Smartcards

Einrichten einer Windows Server 2003-Anmeldungsinfrastruktur mit Smartcards

Christian Zahler

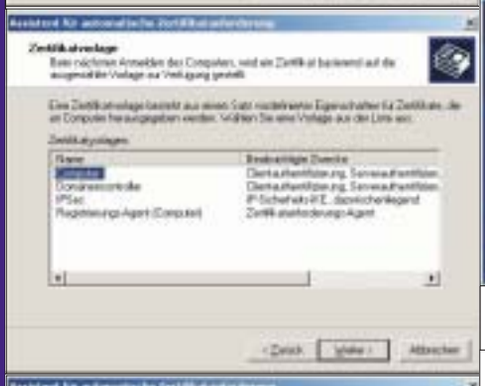
Voraussetzungen

Eine installierte und funktionsfähige Organisations-Zertifizierungsstelle, die so konfiguriert ist, dass automatisch Client-Zertifikate ausgestellt werden können.

Am Windows XP-Client ist ein GEMPlus-Smartcard-Reader am USB-Port angeschlossen.

Schritt 0: Einrichten bzw. Überprüfen der automatischen Zertifikatanforderung für Client-Computer

Annahme: Ein DC ist Organisations-Stammzertifizierungsstelle; dann muss die *„Default Domain Controllers Policy"*-Gruppenrichtlinie bearbeitet werden.



Schritt 1 (am Client): Installieren des CSP *(Cryptography Service Provider)*

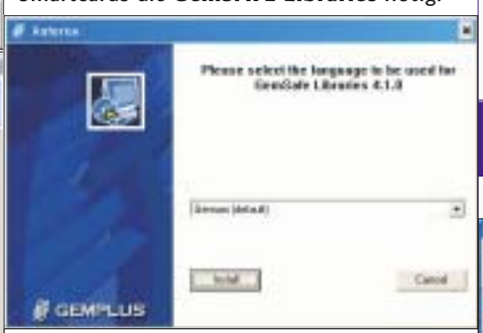
Windows XP und Windows Server 2003 (alle Editionen) unterstützen folgende Smartcards:

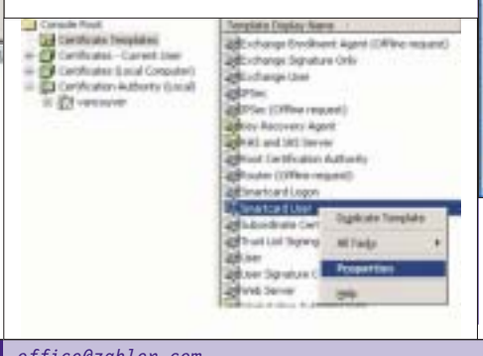
Hersteller	Modell
Gemplus	GemSAFE 4k
Gemplus	GemSAFE 8k
Infineon	SICRYPT v2
Schlumberger	Cryptoflex 4k
Schlumberger	Cryptoflex 8k
Schlumberger	Cyberflex Access 16k

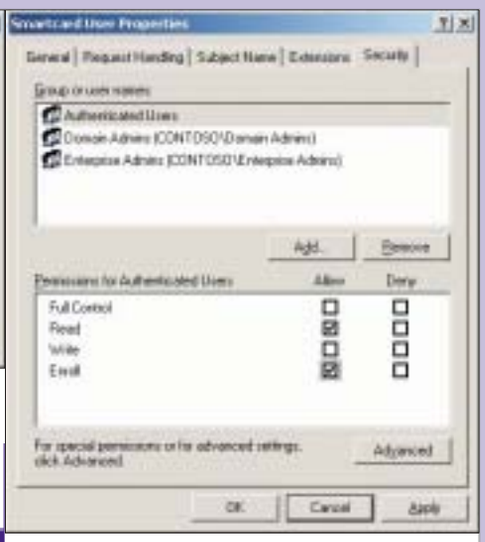
Verwendet man eine von diesen Smartcards, so sind keine zusätzlichen Konfigurationen oder Softwareinstallationen nötig. Trotzdem ist auch die Verwendung anderer Karten auf der Basis des RSA-Verschlüsselungsverfahrens möglich, vorausgesetzt, der Kartenhersteller hat einen *Cryptographic Service Provider* (CSP) für diese Karten entwickelt. (Anmerkung: Dafür stehen die Crypto API und das *Smart Card Software Developer's Kit* zur Verfügung, welchen über MSDN bezogen werden kann.)

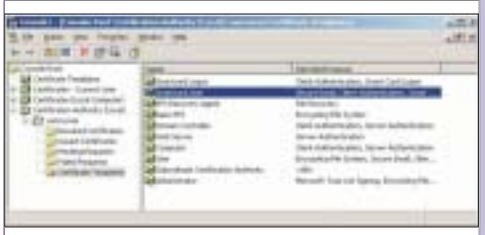
Die Verwaltung von Smartcard PINs (PIN = *personal identification numbers*) ist nur mit einer Software möglich, die der Kartenhersteller zur Verfügung stellen muss.

Dazu sind im Falle von 16-Bit-GemSAFE-Smartcards die **GemSAFE Libraries** nötig.









Schritt 2: Erstellen und Konfigurieren einer Zertifikatsvorlage am Domänencontroller

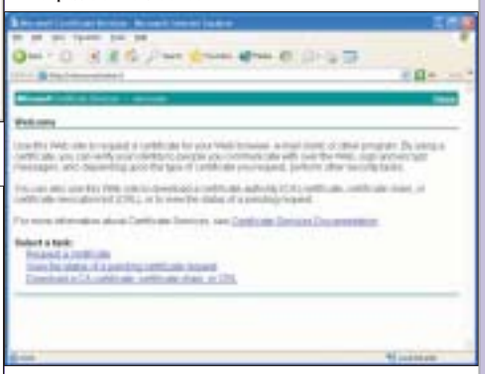
Am DC: ***Zertifikatsvorlagen*** - ***Smart Card User*** - ***Eigenschaften*** - ***Security***

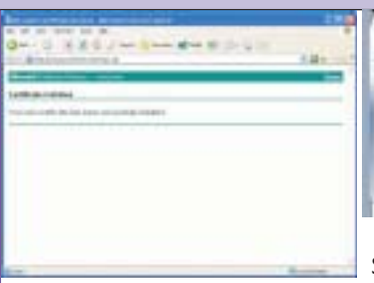
Authentifizierte Benutzer - ***Enrollment erlauben***

Zertifikatsserver: Die konfigurierte Zertifikatsvorlage publizieren

Schritt 3: Am Client: Anforderung eines Smartcard-User-Zertifikats und Speicherung auf der Smartcard

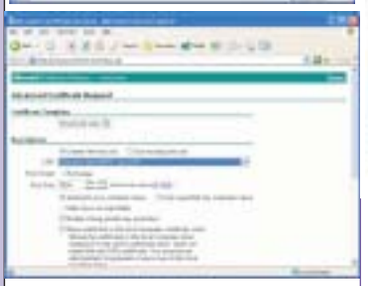
http://server/certsrv





Schritt 4: Am Client - Überprüfung der SmartCard, Setzen des Default-Zertifikats

Mit der korrekten PIN bekommt man auch den *Private Key* zu sehen:

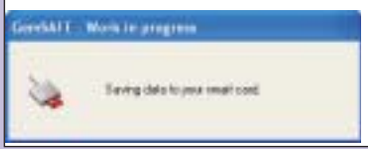


Wichtig: Unter „Als Standard festlegen“: Default Zertifikat setzen (auch wenns nur 1 Zert. gibt!) Die PIN kann auch geändert bzw. entsperrt werden.

Situation: Der Client kann sich nun mit SmartCard an der Windows XP-Workstation anmelden.

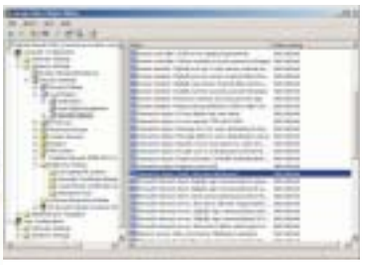
Anmerkung: Zertifikate auf der Karte können nur gelöscht werden, wenn der angemeldete Benutzer im Benutzerprofil die korrekte Berechtigung hat.

Erstellen eines neuen Profils:



Speichern unter ... Es entsteht eine *.gsl-Datei. Damit diese gültig ist, muss die bestehende CONFIG.GSL im GemSAFE-Programmordner durch die neu erstellte Profildatei ersetzt werden.

Schritt 5: Am Domänencontroller: ggf. Erzwingen der Smartcard-Anmeldung, Verhalten beim Entfernen der Smartcard usw.



Für bestimmte Benutzer kann die Anmeldung über Smartcards erzwungen werden: