IT-SECURE.COM

The Swiss E-Security Company.

Anleitung: Smart Card basiertes Login mit Zertifikaten basierend auf Windows 2003 Server Technology

Einleitung

Die sichere Identifizierung der Benutzer und Administratoren wird immer wichtiger. Dies kann mit verschiedenen Technologien und Prozessen umgesetzt werden. Der Erfolg oder Return on Investment einer sicheren Identifizierung basiert auf folgenden Konzepten:

- Einführen einer 2-Stufigen Identifizierung
- Trennung der Identifikation von der Autorisation

Die Identifizierung wird in folgende Stufen eingeteilt:

1. *Etwas dass man weiss*. (Username und Passwort). Die sicher „schwächste" Identifizierung, ist doch der Benutzername immer statisch und das Passwort je nach Komplexität mit einer Brute force Attacke mit einem gewissen Zeitaufwand zu knacken. Meist werden die Identifikationsparameter auch unverschlüsselt über das Netzwerk übertragen.
2. *Etwas dass man weiss und etwas dass man besitzt*. Sicher ist uns das Beispiel der Online Bank bekannt mit einer Vertragsnummer, einem Passwort und einer Streichliste oder einem Token. Meist werden die Identifikationsparameter während dem Transit verschlüsselt. Diese Technologie ist meist sehr teuer und kann nicht für alle Zwecke eingesetzt werden, da nicht alle Applikationen diese Technologie erkennen. Auch ist die Verwaltung der „Tokens" meist Aufwändig und Proprietär implementiert was zu höheren Produktionskosten führt.
3. *Etwas dass man weiss und etwas dass man besitzt sowie etwas dass man ist*. Bei diesem Konzept wird auf Biometrische Erkennungsmerkmale gesetzt. Sicher eine der aktuellen Themen auch bei der Einreise in die USA wobei sich die Investition kaum lohnt, wenn Daten der Schutzklasse 3 (gemäss DSG) bearbeitet werden, da gute Leser heute immer noch sehr teuer sind. Dabei ist darauf zu achten, dass sich die beiden Parameter FAR (Benutzerfreundlichkeit) und FRR (Sicherheit) konfliktär verhalten.

Die Trennung von der Identifikation von der Autorisation: Ziel eines jedes Unternehmens sollte es sein, dass jede zu identifizierende Entität nur eine digitale Identität im Gesamtsystem hat. Dabei wird die Identifizierung (Registrierung der natürlichen Identität mit einer digitalen Identität) von der Autorisierung (welche Rechte hat die Identität im System) getrennt. Diese digitale Identität muss allen Applikationen in einem sogenannten Meta-Directory verfügbar gemacht werden. Was hier so kompliziert beschrieben ist, wird in der Praxis heute schon sehr oft Angewandt: in einer Microsoft-Umgebung ist dies das Active Directory, häufig werden auch X500 Directory oder LDAP Verzeichnisse dafür eingesetzt.

Mit der Einführung der Certification Authority und dem Active Directory von Microsoft wurde die Voraussetzung geschaffen, dass sich Entitäten nun mit Zertifikaten Identifizieren können und die ganze Anmeldung verschlüsselt erfolgen kann. Diese Anleitung zeigt in einer Schritt für Schritt Anleitung auf, wie Sie diese Technologie in Ihrem Unternehmen nutzen können.

Technische Voraussetzungen

Sie benötigen folgende Komponenten für den Smart Card Login:

1. Windows Server 2003 Enterprise Edition mit Active Directory und Certification Authority (Microsoft bietet eine Gratis-Testlizenz an).
2. Smart Card USB-Token Cryptoflex 32k E-Gate mit Dongle (Aktionspreis: CHF 20.--)
3. Middleware Schlumberger (Einzelplatzlizenz CHF 22.40)

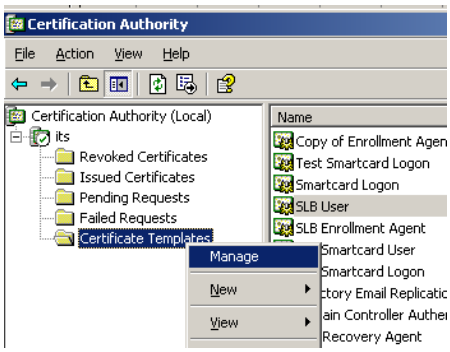
Vorgehen

Installation Treiber und Middleware

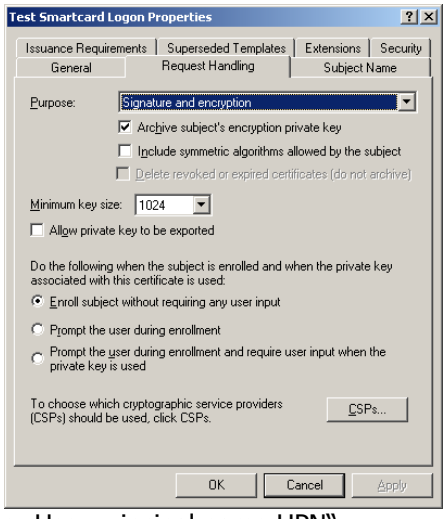
1. Installieren Sie die Middleware mit dem Installationsscript auf Ihrem Test-Server
2. Laden Sie sich die neuesten Treiber für die Cryptoflex Smart Cards auf Ihren Testserver (http://www.it-secure.com/Downloads/e-gate_W2k_XP_24.zip)
3. Schliessen Sie den USB-Dongle an Ihren Test-Server an und Installieren Sie die Treiber.

Führen Sie einen reboot durch. Das System kennt jetzt die USB-Smart Card und die Middleware ist bereit.

Konfiguration Windows Server Certification Authority

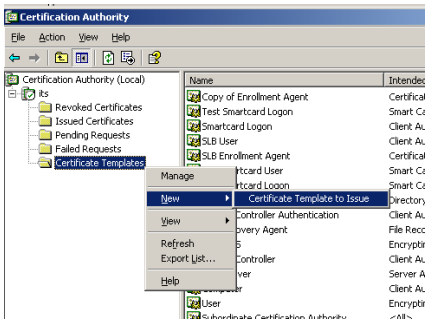


Starten Sie das Windows Certification Authority MMC Snap In. Wählen Sie die Certificate Templates aus und halten Sie die rechte Maustaste gedrückt. Das Kontextsensitive Menu zeigt Ihnen eine Position „Manage" auf. Wählen Sie diese aus. Das MMC Snap In für die Certificate Templates wird gestartet. Wählen Sie das Template Smart Card Logon aus und halten Sie die rechte Maustaste gedrückt. Wählen Sie „dublicate Template" aus. Geben Sie dem Smart Card Template den Namen SLB Smart Card Logon. Aktivieren Sie „Publish certificate in Active Directory".



Auf der nächsten Seite wählen Sie bei "Purpose" "Signature and encryption" aus, aktivieren "Archive subject's encryption private key und stellen den „Minimum key size" auf 1024. Bei den „Enrollment" Eigenschaften wählen Sie „Enroll subject without requiring any user input" und ganz unten wählen Sie den CSP (Cryptographic Service Provider) aus. Aus Benutzerfreundlichkeit wählen Sie „Requests must use one of the following CSP's" und aktivieren den „Schlumberger Cryptographic Service Provider".

Auf der nächsten Seite „Subject Name" aktivieren Sie „Build from this Active Directory infomation" aus und wählen Sie bei „Subject name format" den „Fully distinguished name" aus. Je nach dem, wenn Sie die E-Mail Adresse ebenfalls im Active Directory haben, empfiehlt es sich, die E-Mail Adresse im Feld „alternate subject name" zu aktivieren (Sie können dann verschlüsselte E-Mails senden und empfangen). Aktivieren Sie den „User principal name UPN".



Unter „Issuance Requirements" können Sie die Anzahl der benötigten Bestätigungen durch Administratoren bestimmen.

Unter dem „Security-Tab" wählen Sie für die Benutzer-Gruppe oder den einzelnen Benutzer die Optionen „Enroll" und „Autoenroll" aus.

Klicken Sie auf OK und schliessen Sie das Window mit den „Certificate Templates" und kehren Sie zurück zur „Certification Authority". Wählen Sie „Certificate Templates" aus und drücken Sie die rechte Maustaste und wählen aus dem Menu → New → „Certificate Template

to use" aus. Ein Window erscheint, aus dem Sie das oben kreierte Template „SLB Smart Card Logon" auswählen können. Klicken Sie auf OK.

Jetzt müssen Sie nur noch die „Default Domain Controller Security Settings" anpassen, um das Verhalten des Servers bei einem „Smart Card removal" fest zu legen. Gehen Sie hierfür auf „Start" → „Administrative Tools" → „Domain Controller Security Settings". Das MMC Snap-In erscheint. Unter „Security Settings" → „Local Policy" → „Security Options" finden Sie den Eintrag "Interactive logon: Smart card removal behaviour". Klicken Sie darauf und wählen Sie "Lock Workstation" aus.

Certificate Enrollment

Schliessen Sie das Token an den Server an und öffnen Sie eine MMC Konsole (Run → MMC). Unter „File" und „Add/Remove Snap-in" wählen Sie „Add" aus. Im folgenden Window aktivieren Sie „Certificates" und unter Certificates Snap-in aktivieren Sie „My user account". Klicken Sie auf „finish" und „close". Das Fenster sollte jetzt „Certificates – Current User" anzeigen. Klicken Sie auf OK. Öffnen Sie „Certificates – Current User" → „Personal". Mit der rechten Maustaste unter „All Tasks" → „Request New Certificate" auswählen. Jetzt sollte der Certificate Request Wizard erscheinen. Wählen Sie das Template „SLB Smart Card Login aus" und klicken Sie auf weiter. Geben Sie dem Zertifikat einen Namen zum Beispiel Test Smart Card. Sie werden jetzt aufgefordert die Smart Card einzustecken und ein Dialog für die PIN-Abfrage erscheint. Der Wizard führt Sie durch das Ausstellen des Zertifikates.

Anmelden mit Smart Card

Starten Sie Ihren Server neu. Beim nächsten Logon sollten nicht nur User Name und Passwort erscheinen sondern auch Smart Card based logon. Schliessen Sie den Token an, Sie werden aufgefordert den PIN einzugeben und werden mittels einem Zertifikat angemeldet. Fertig.

Gerne demonstrieren wir Ihnen die Vorteile dieses neuen Produktes in Ihrem Hause oder bei uns.

smartcards@it-secure.com