IT-SECURE.COM

The Swiss E-Security Company.

VPN Remote Access auf Terminal Services mit Smart Cards basierend auf Windows Server Technology

Einleitung

Heim-Arbeitsplätze, Application Service Provider, zentralisierte EDV-Dienstleister müssen heute meist umständlich und teuer Lösungen implementieren um den neuen Anforderungen gerecht zu werden.

Sichere Remote Access Lösungen waren schon immer sehr komplex und teuer, meist auch für die Benutzer umständlich zu bedienen. Wir stellen Ihnen eine Möglichkeit vor, die nicht nur sicher ist, sondern auch einfach zu bedienen und bescheiden im Preis: **die Kosten für einen VPN-Zugang auf Ihre Services betragen lediglich pro Benutzer sFr. 60.40**. In diesem Preis sind alle Lizenzen, Hardware und Smart Cards enthalten.

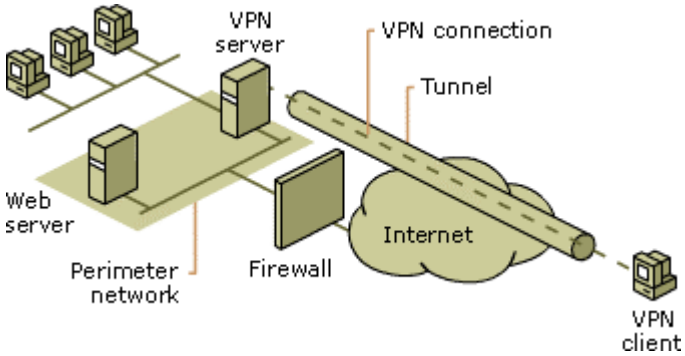
Technische Voraussetzungen

Sie benötigen folgende Komponenten für den VPN Remote Access auf Terminal Services mit Smart Card Login:

1. Windows Server 2003 mit Active Directory Services und Certification Authority (Microsoft bietet eine Gratis-Testlizenz an).
2. Terminal Services konfiguriert.
3. VPN-Remote Access konfiguriert.
4. Smart Card USB-Token Crypto- oder Cyberflex 32k E-Gate mit Dongle.
5. Middleware Schlumberger.

Labor Beispiel

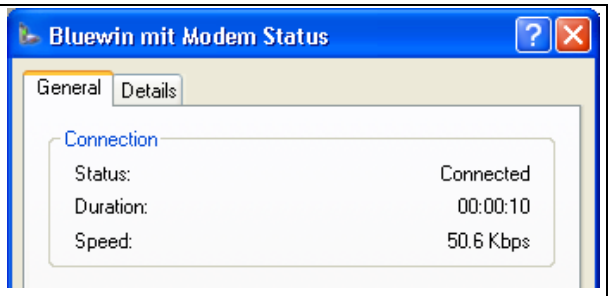
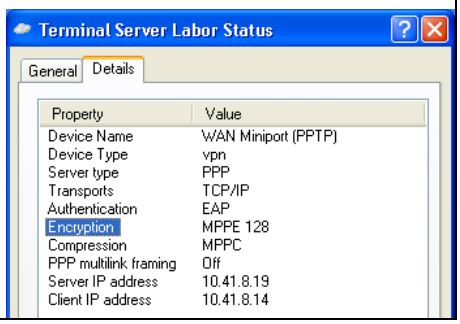
Im Labor von IT-Secure.com wurde folgende Testinstallation für Demo-Zwecke aufgebaut:



Beim VPN-Client handelt es sich um einen Laptop mit Microsoft Windows XP Professional SP1 mit der COVE Middleware und Treiber für Cyberflex E-Gate Smart Cards. Der Firewall ist ein handelsüblicher Zywall auf dem die Ports für PPTP-Maintenance und PPTP mit incoming allow auf unseren VPN-Server konfiguriert wurde. Beim VPN-Server handelt es sich um einen Windows 2003 Server als DC mit Aktiv

Directory Services und Certificate Services konfiguriert. Vorgängig wurde dem VPN-Benutzer das Zertifikat auf die Smart Card ausgestellt und der Benutzer als Dial-In Benutzer konfiguriert. Die Middleware unterstützt sowohl Lokale Authentisierung über Smart Card sowie auch Remote im Terminal Services Window!

Beispiel der VPN-Connection

Wir verwenden für unser Beispiel eine relativ langsame Modem-Verbindung über den Provider Bluewin mit 50 kbits um auch die Dial-Up Connectivität bei niedriger Bandbreite zu testen.	
1. Wir starten den Dialer für die Modem-Verbindung zu unserem Provider und erhalten eine wirklich kleine Bandbreite von 50.6 Kbps. 2. Als nächstes starten wir die VPN-Verbindung mit unserem Labor-Server über das mit dem VPN-Connection-Wizard erstellte Icon und messen die Zeit.	 Terminal Server Labor.lnk
3. Wir werden aufgefordert die Smart Card einzustecken und klicken auf OK.	
4. Wir werden nun aufgefordert den PIN einzugeben, der uns als berechtigter Benutzer dieser Smart Card und den dazugehörenden digitalen Zertifikates identifiziert. **Nach der Eingabe des PIN's wird die VPN Verbindung in weniger als 3 Sekunden aufgebaut!**	
Wir kontrollieren lokal, ob wir auch wirklich eine verschlüsselte Verbindung haben: tatsächlich, mit dem Zertifikat wurden wir Identifiziert (1028 Bit) und es wurde eine verschlüsselte Verbindung aufgebaut mit 128 Bit. Dies entspricht der Verschlüsselungsstärke heutiger E-Banking Lösungen.	

Jetzt wollen wir versuchen über diese dürftige Bandbreite eine Terminal-Session aufzubauen und uns mit dem Zertifikat auf der Smart Card, das sich am lokalen USB-Port befindet, remote zu authentisieren. **Tatsächlich verlangt der Login-Screen nun den PIN der Smart Card**	

Wir überprüfen im Eventviewer den Remote Access und sehen folgende Meldung:
The user Administrator@xxxx.yyyy.com has connected and has been successfully authenticated on port VPN4-127. Data sent and received over this link is strongly encrypted.

Fazit

Dieser Test beweist, dass es immer einfacher wird, sichere, auf digitalen Zertifikaten mit Smart Cards basierende Lösungen im Bereich Secure Single Sign on, zu etablieren und diese auch Benutzerfreundlich zu gestalten. Die Sicherheit mit digitalen Zertifikaten und Public Key Längen von 1024 Bit sowie die symmetrisch verschlüsselte Verbindung mit 128 Bit genügen heute internationalen Standards und wird im E-Banking-Bereich Tag für Tag eingesetzt.

Gerne demonstrieren wir Ihnen die Vorteile von Cyberflex oder Cryptoflex Smart Cards in Ihrem Hause oder bei uns.

smartcards@it-secure.com