cryptoshop®

HOWTO
Lokales Windows Logon mit Chipkarte

Erstellt von
Silvia Straihammer, BSc
Silvia.straihammer@cryptas.com

Dokument Version – Erstellungsdatum
v1.0 – 08/2011

Franzosengraben 8 : A-1030 Wien
Tel +43 (1) 798 96 96-0 : Fax +43 (1) 798 96 96-99
E-Mail info@cryptas.com : Web www.cryptas.com

cryptoshop®

Inhaltsverzeichnis

Abbildungsverzeichnis

cryptoshop®

Einleitung

Microsoft hat in seinen Betriebssystemen die Möglichkeit eines Chipkarten-Logon eingebaut. Jedoch ist es nur möglich dieses Feature zu verwenden, wenn der Computer einer Domäne angehört. Man steht vor einer Herausforderung, wenn man sich auch auf seinem privaten Computer mit einer Smartcard einloggen und damit die Vorteile eines solchen Logons genießen möchte.

In diesem Guide wird Schritt für Schritt erklärt, wie man auch seinen privaten PC dazu bringt eine Chipkarte mit PIN anstatt eines Passworts anzunehmen. Außerdem kann man mit einer Chipkarte noch andere Vorteile genießen (siehe HOWTO Keepass mit Chipkarte).

Voraussetzungen

Folgendes wird benötigt um einen Chipkarten-Logon zu realisieren:

- Kartenlesegerät
- Chipkarte mit CSP Unterstützung (Bsp.: Gemalto .NET, Athena ASE Card,…)
- EIDAuthenticate Software (Diese Software steht unter http://www.mysmartlogon.com/products/eidauthenticate.html gratis zum Download bereit)

Um das Kartenlesegerät und die Chipkarte verwenden zu können sind oft noch die passenden Treiber notwendig. Diese werden entweder von Windows automatisch bei der ersten Inbetriebnahme des Geräts heruntergeladen und installiert. Die andere Möglichkeit ist eine manuelle Installation. Die Treiber sind meistens im Lieferumfang enthalten oder können von der Herstellerhomepage heruntergeladen werden.

Personalisierung

Bei der Installation von EIDAuthenticate einfach dem Wizard folgen.

EIDAuthenticate fügt der Systemsteuerung einen Menüpunkt unter System und Sicherheit hinzu (Start – Systemsteuerung – System und Sicherheit – Smart Card Logon)

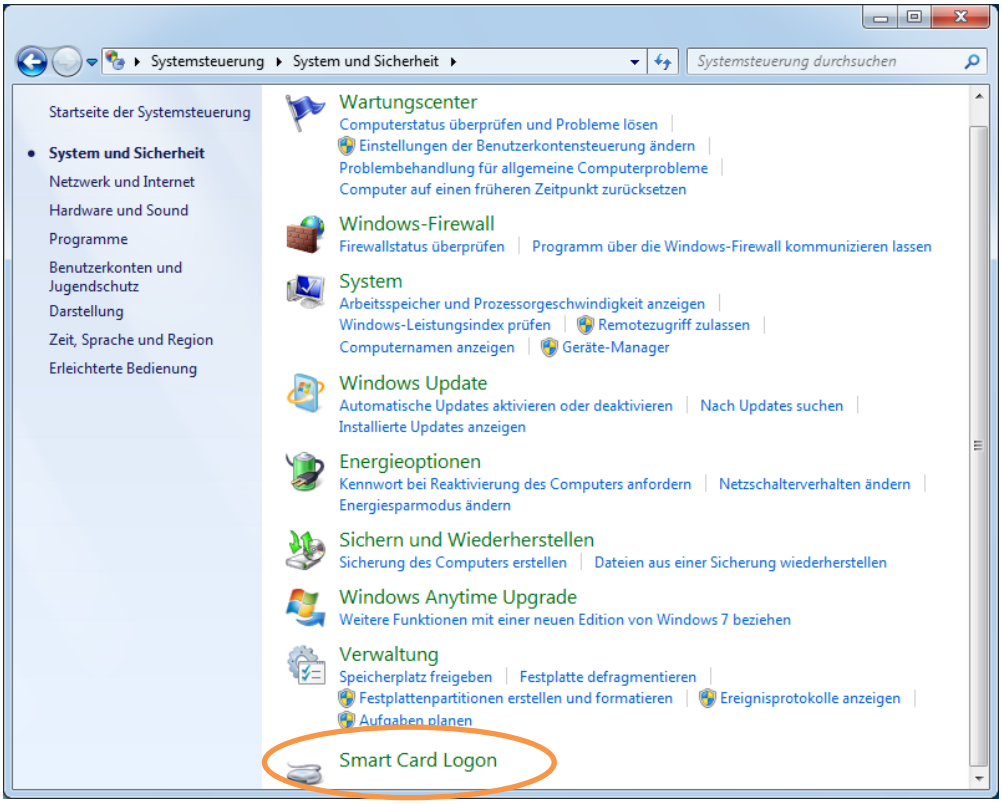

Abbildung 1: Systemsteuerung

Mit einem Klick auf diesen Menüpunkt kann der Computer und die Chipkarte konfiguriert werden. Bei der ersten Verwendung ist es notwendig eine neue Certification Authority (CA) zu erstellen. Will man weitere Chipkarten für einen Logon ausrollen, so kann die bestehende CA verwendet werden. Dieser Dialog erscheint nur, wenn eine Chipkarte im Lesegerät vorhanden ist und alle Treiber erfolgreich installiert wurden.

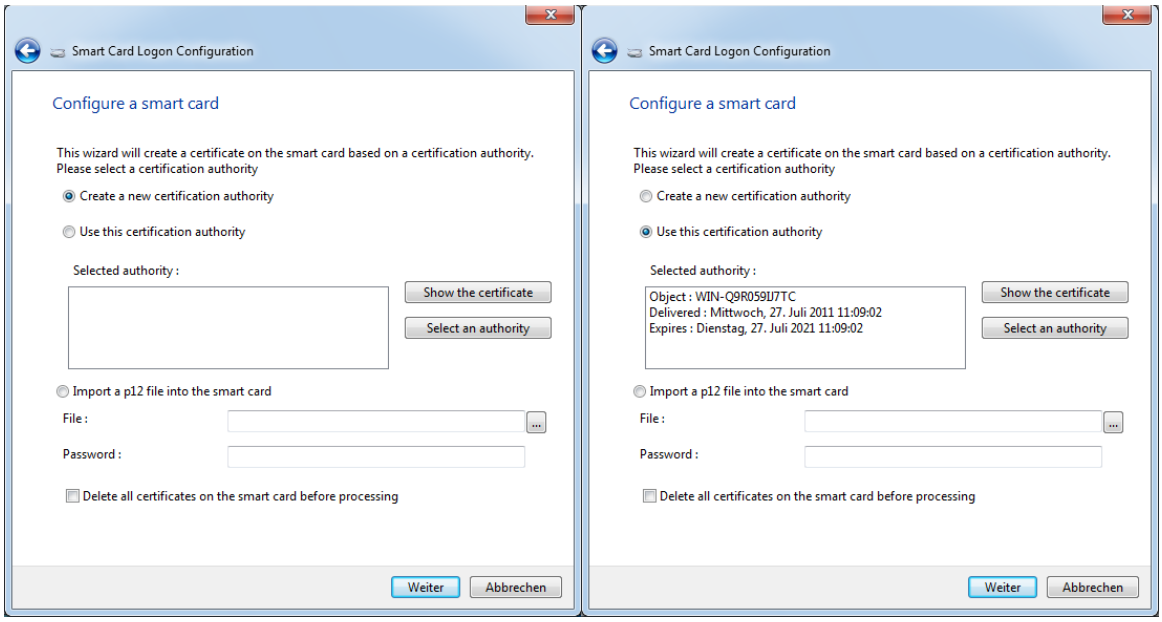

Abbildung 2: Smart Card Logon Konfiguration

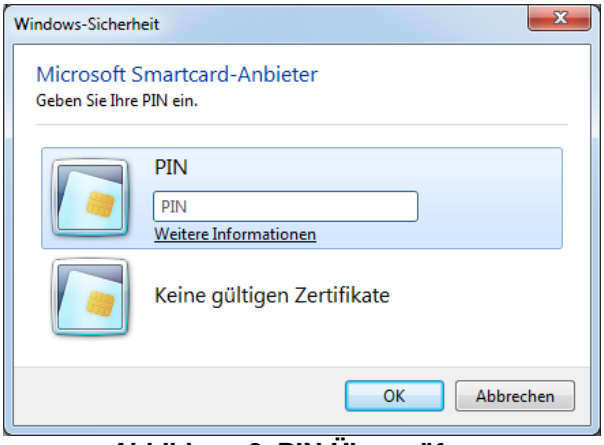

Abbildung 3: PIN Überprüfung

Damit das Zertifikat auf der Chipkarte abgelegt werden kann muss der Benutzer erst den PIN eingeben und damit die Karte entsperren. Bei Gemalto .NET Karten ist 0000 der default PIN.

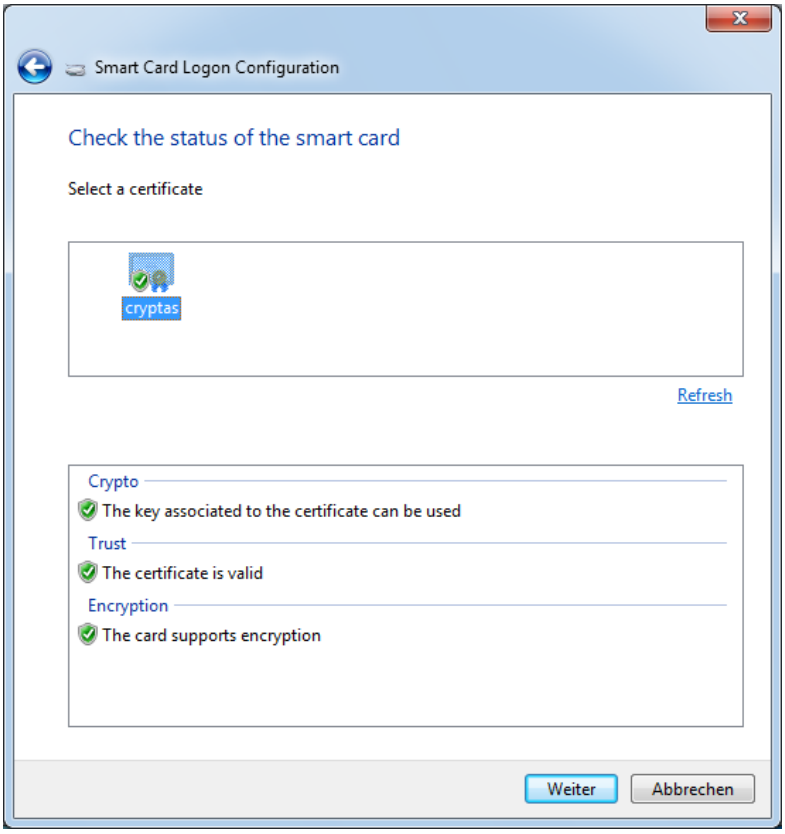

Abbildung 4: Zertifikatsauswahl

Ist die Karte entsperrt, so überprüft die Software, ob die Karte den Anforderungen entspricht und das ausgewählte Zertifikat darauf abgelegt werden kann.

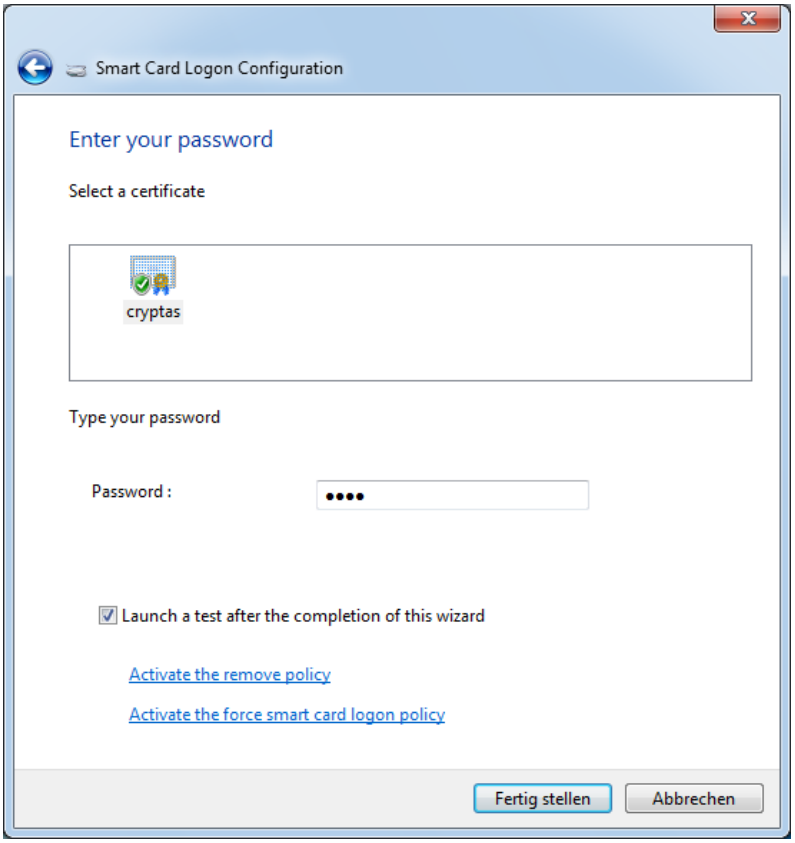

Abbildung 5: Passwortverifikation und Optionen

Das Windows Passwort wird dazu verwendet das Zertifikat abzusichern. Hier können auch zwei Policies aktiviert oder deaktiviert werden.

- Remove Policy – Wenn diese Option aktiviert ist wird der Computer gesperrt, sobald die Smartcard aus dem Lesegerät entfernt wird.
- Force Smart Card Logon Policy – Ist diese Option aktiviert, so muss sich der Benutzer immer mit der Chipkarte am System anmelden. Es ist nicht mehr möglich sich mit Benutzername und Passwort anzumelden.

Nach vollendeter Personalisierung wird ein Test durchgeführt. Dazu ist die Eingabe des PINs notwendig.

PIN ändern

Das Ändern des PINs funktioniert auf die gleiche Weise wie das Ändern eines Windows Passworts. Mit der Tastenkombination ***Strg+Alt+Entf*** erscheint ein Menü in dem der Punkt *‚Kennwort ändern‘* ausgewählt wird. Zuerst erscheint der Dialog zum Ändern des Benutzerpassworts. Mit einem Klick auf *‚Andere Anmeldeinformationen‘* stehen alle konfigurierten Anmeldeinformationen zur Auswahl.

Abbildung 6: Kennwort ändern

‚*Änderung der Smartcard PIN*' auswählen und im folgenden Dialog den alten und den neuen PIN eingeben.

Abbildung 7: PIN ändern

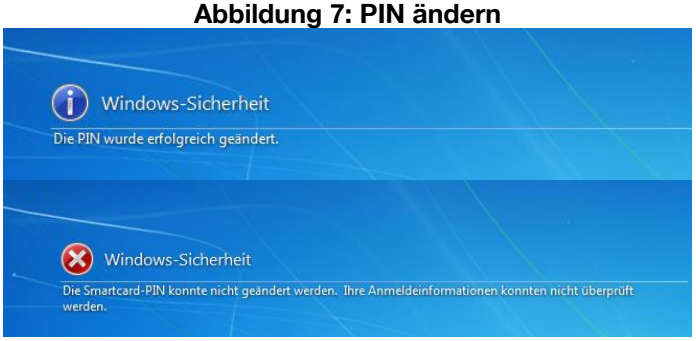

Abbildung 8: Erfolgs- / Fehlermeldung

Es kann nur der BenutzerPIN der Chipkarte geändert werden, nicht aber der Admin PIN. Nur bei Chipkarten, die Base Smart Card CSP enabled sind kann der PIN geändert werden.

Getestet mit Gemalto .NET und Athena ASE Card CRYPTO Karten

Funktionsweise

Die Software hat folgende Bestandteile

- Credential Provider: für die PIN Abfrage
- Authentication Package: Authentifikation des Benutzers
- Password Filter: Passwortmanagement
- Wizard: Damit kann alles konfiguriert werden.

Die Software installiert auf dem PC eine so genannte Certificate Authority. In einer Domäne übernimmt diese Rolle meist ein zentraler Server. Die Certificate Authority ist dafür verantwortlich Zertifikate auszustellen und eine Sperrliste für ungültige Zertifikate zu verwalten. Während der Konfiguration wird ein Zertifikat von dieser CA angefordert, welches dann auf der Chipkarte abgelegt wird.

Bei einem Login-Versuch wird das Zertifikat auf der Karte ausgelesen und kann mit Hilfe der CA auf dem Computer auf Gültigkeit überprüft werden.

Fazit

Mit dem EIDAuthenticate Software ist es ganz einfach möglich sich auch ohne Domäne mit einer Chipkarte an seinem PC anzumelden. Damit erhöht sich nicht nur die Sicherheit der Daten auf dem PC, auch der Logon-Vorgang ist viel schneller. Anstatt eines mindestens acht Zeichen langen Passworts muss nur mehr ein vier Zeichen langer PIN eingeben werden.

Quelle

MySmartLogon http://www.mysmartlogon.com/

cryptoshop®

CRYPTAS it–Security
Franzosengraben 8
A–1030 Wien, Austria
T +43 (1) 798 96 96 – 0
F +43 (1) 798 96 96 – 99
info@cryptas.com

www.cryptoshop.com
www.cryptas.com