SecCommerce
INFORMATIONSSYSTEME GMBH

SecCommerce

SecAuthenticator®

Benutzerhandbuch

Version 1.6
17.07.2009

Autor:
Rainer Marks, Jens Uhl, Ulrich Heller

www.seccommerce.de info@seccommerce.de

Dokumentenhistorie

Datum	Version	Inhalt / Änderung	Autor
07.02.2002	1.0	Erste Fassung	Rainer Marks
13.02.2002	1.1	Korrekturen	Rainer Marks
25.06.2002	1.2	Review	Jens Uhl
16.07.2002	1.3	Ergänzung	Jens Uhl
30.10.2002	1.4	Unterstützung Netscape 4.x entfernt	Rainer Marks
16.07.2009	1.5	Ergänzungen unterstützte Hard-/Software	Ulrich Heller
17.07.2009	1.6	Aktualisiertung Screenshots	Ulrich Heller

Inhaltsverzeichnis

1 Einführung

Der SecCommerce SecAuthenticator sichert beliebige SSL/TLS-Angebote durch Authentifizierung mit Hilfe von SmartCards ab. Im Zusammenspiel mit SecRouter® können hochsichere HTTPS-Sitzungen mit und ohne den Einsatz von Cookies realisiert werden.

Dieses Dokument richtet sich an die Anwender, die sich mittels SecAuthenticator authentifizieren möchten.

1.1 Systemvoraussetzungen Hardware

Es werden folgende Signaturkarten (mit Bestätigungsnummer) unterstützt:

- TCOS 3.0 Signature Card, Version 1.1, T-Systems (TUVIT.93146.TE.12.2006)
- STARCOS 3.0 V3.0, SignTrust, BNotK (TUVIT.93100.TE.09.2005, Anhang 4)
- Chipkarte mit Prozessor SLE66CX322P (bzw. SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature, D-Trust card V2.1/V2.2/V2.3/V2.4, Mirabeiterkarte Deutsche Rentenversicherung,
- TC Trustcenter TC Qsign (T-Systems.02182.TE.11.2006, Anhang 2)
- ZKA Banking Signature Card, Version 6.6 (TUVIT.93130.TU.05.2006, Anhang 2)
- ZKA Banking Signature Card, Version 7.1.2 (TUVIT.93166.TE.06.2008)
- STARCOS 3.2 QES Version 1.1, SignTrust, BnotK (BSI.02102.TE.11.2008)
- STARCOS 3.2 QES Version 2.0, SignTrust, BnotK (BSI.02114.TE.12.2008)

Es werden folgende Kartenleser unterstützt:

- REINER cyberJack e-com, Version 2.0, Firmware 2.0.22
- REINER cyberJack e-com (a), Version 3.0, Firmware 3.0.69
- REINER cyberJack pinpad (a), Version 3.0, Firmware 3.0.12
- REINER cyberJack secoder, Version 3.0, Firmware 3.0.14
- Cherry SmartBoard G83-6744, Firmware 1.04
- Cherry SmartTerminal ST-2000, Firmware 5.08
- Fujitsu Siemens-Tastatur KB SCR Pro, Firmware 1.06
- KOBIL KAAN Advanced, Firmware Version 1.19
- KAAN TriB@nk, Firmware 79.22
- OMNIKEY CardMan 3621, Firmware 6.00
- OMNIKEY CardMan 3821, Firmware 6.00
- SCM Microsystems SPR532, Firmware 5.10

Eine stets aktuelle Übersicht unterstützter Hard- und Software findet sich im Internet unter:
http://www.seccommerce.de/de/produkte/unterstuetze/unterstuetze.html

1.2 Systemvoraussetzungen Software

Betriebssysteme:

- Microsoft Windows XP SP3
- Microsoft Windows Vista
- Mac OS X
- SuSe Linux 10
- Ubuntu Linux 9
- Fedora Linux 11

Das Anwendersystem erfordert einen JAVA-fähigen Internet-Browser mit einer JAVA-Version ab Version 1.4.2.

Ein für den Browser konfigurierter http-Proxy, wie er in Firmennetzwerken häufig Verwendung findet, wird vom SecAuthenticator erkannt und für die Kommunikation verwendet.

Ist für den Web-Browser keine Java-VM installiert, ist der Download und die Installation des SUN Java-Plugin für den Web-Browser erforderlich:

http://www.java.com/de/download/

2 Sicherheitshinweise

Für die sichere Nutzung des SecAuthenticator sind grundsätzlich allgemeine Sicherheitsempfehlungen zu beachten. Die Regulierungsbehörde für Telekommunikation und Post (RegTP) als zuständige Behörde hat z.B. unter der folgenden URL entsprechende Hinweise veröffentlicht:

http://www.regtp.de/tech_reg_tele/00432/01/index.html

Beachten Sie bitte auch folgendes:

- Durch einen eventuellen Virenbefall eines Microsoft Windows- Anwendersystems können Tastatureingaben und somit auch die geheime PIN ausgespäht werden. Ein Kartenleser mit integrierter PIN- Eingabe macht das unmöglich. Bei sicherheitskritischen Dokumenten sollte daher immer ein Leser dieser Bauart verwendet werden.

- Beachten Sie bitte unbedingt die Benutzungshinweise Ihres Trustcenters zur Nutzung Ihrer Signaturkarte.

- Lassen Sie die Signaturkarte nicht offen herumliegen.

- Ändern Sie die PIN Ihrer Signaturkarte regelmäßig, insbesondere wenn Sie befürchten, dass jemand unberechtigterweise die PIN erfahren hat.

- Wählen Sie eine PIN, die sich nur schwer erraten lässt. Ein Dieb hat drei Versuche, nach dreimaliger Falscheingabe wird Ihre Signaturkarte automatisch unbrauchbar.

- Teilen Sie die PIN Ihrer Signaturkarte niemandem mit, auch nicht auf Verlangen unserer „Mitarbeiter“.

- Notieren Sie die PIN nicht, insbesondere nicht auf der Signaturkarte!

- Melden Sie den Verlust Ihrer Signaturkarten sofort der kartenausgebenden Stelle (Ihrem Trustcenter) und lassen Sie die Karte sperren. Damit sind Signaturen, die nach der Sperrung erfolgen nicht mehr rechtsverbindlich.

- Bei ungültiger PIN oder abgelaufener Signaturkarte wenden Sie sich bitte an den Herausgeber oder Provider der Karte (Ihr Trustcenter).

- Darüber hinaus sind die Sicherheitseinstellungen des verwendeten Internet-Browsers zu überprüfen und gegebenenfalls gemäß den nachfolgenden Anweisungen einzurichten. Bei Fragen zur Realisierung der Einstellungen ist die Dokumentation des verwendeten Internet-Browsers zu Rate zu ziehen.

2.1 Sicherheitseinstellungen im Web-Browser

- Vor dem Laden des SecAuthenticator ist der Cache des Internet-Browsers zu löschen.
- Es ist einzustellen, dass immer die aktuelle Seite geladen wird, auch wenn sich im Cache bereits eine entsprechende Seite befindet.
- Der Dialog zur Anforderung zusätzlicher Rechte durch Java-Applets darf nicht deaktiviert sein.
- Das Ausführen von Java muss aktiviert sein.
- Wird ein Proxy-Server verwendet, so ist dieser ggfs. zu konfigurieren.

3 Authentifikation mittels SecAuthenticator

Erfordert ein SSL-Angebot einen SmartCard-abgesicherten Zugang, so erscheint zunächst der Initialisierungsbildschirm des SecAuthenticator (Abbildung 1). Nach Anwahl der Schaltfläche „SmartCard suchen“ wird automatisch der angeschlossene Kartenleser und die damit verwendete SmartCard ermittelt. Konnte eine gültige SmartCard gefunden werden, so wird die Schaltfläche „anmelden“ aktiviert, mit der der Benutzer seine Identifikation abschließen kann. Der auf der SmartCard enthaltene, öffentliche Verschlüsselungsschlüssel[1] wird nun an Diensteanbieter gesandt[2], welcher eine Legitimationsprüfung durchführt. Ist diese erfolgreich, wird der Nutzer automatisch zum gewünschten SSL-Angebot weitergeleitet.

> **Anmerkung**: Voraussetzung für diese Art der Identifikation ist das Vorhandensein eines Verschlüsselungs- oder Utility-Zertifikates auf der SmartCard. Ist ausschließlich ein Signaturzertifikat vorhanden, so ist die SmartCard-basierte Authentifikation nicht möglich und der SecAuthenticator bricht den Anmeldevorgang mit einer entsprechenden Meldung ab.

> **Hinweis**: Ist das Verschlüsselungszertifikat der Karte durch eine PIN geschützt, wo wird diese nach Drücken der Schaltfläche „anmelden“ in einem gesonderten Dialog abgefragt.

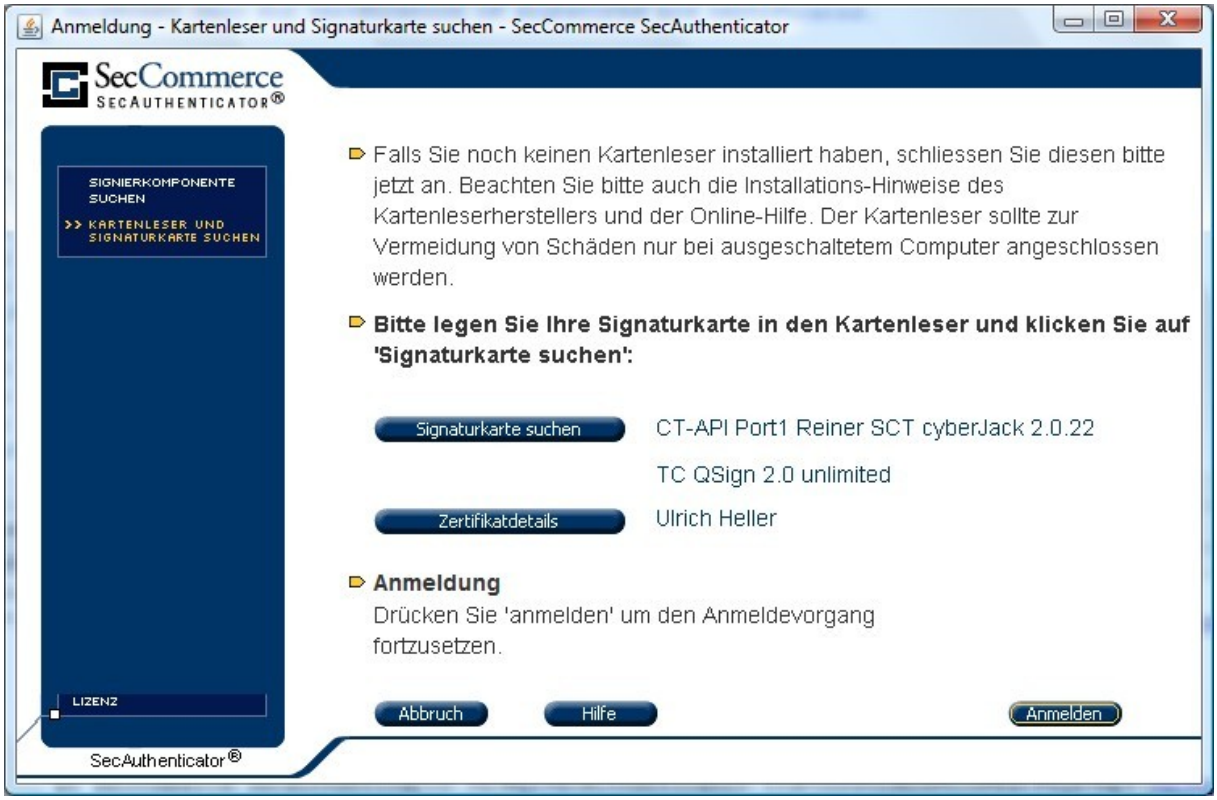

Abbildung 1: SecAuthenticator – Initialisierung

[1] im Gegensatz zum Signaturschlüssel.
[2] es werden ausschließlich für die Öffentlichkeit bestimmte Daten von der SmartCard ausgelesen, welche verschlüsselt an die überprüfende Instanz geschickt werden. Vertrauliche Daten der SmartCard (der private Schlüssel) können die Karte nie verlassen!

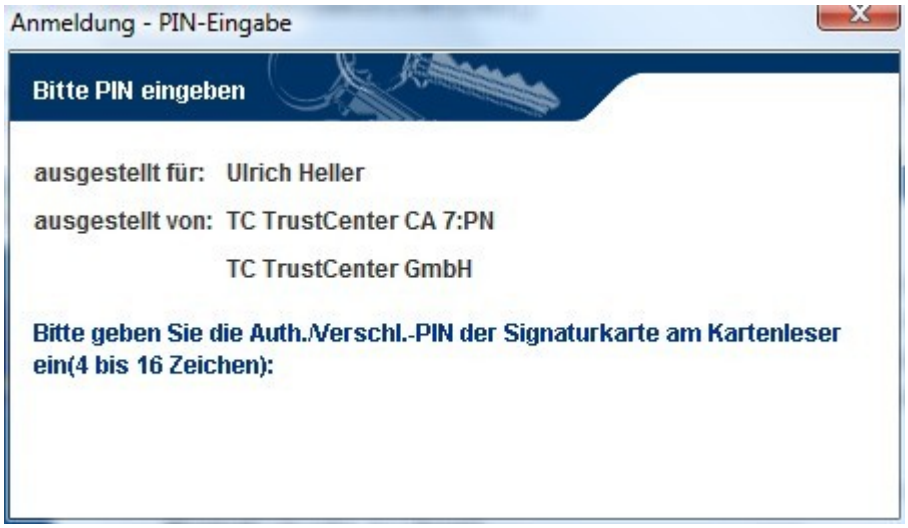

Abbildung 2: SecAuthenticator – PIN-Eingabe

> **Hinweis**: Beachten Sie bitte, dass manche SmartCards eine unterschiedliche PIN für Signaturzertifikat und Verschlüsselungszertifikat besitzen. Gefordert ist stets die PIN des Verschlüsselungs-/ Authentifizierungsschlüssel.

Ist die verwendete SmartCard dem System nicht bekannt und gestattet der Betreiber des SSL-Angebotes das Anmelden neuer Benutzer, so wird ein weiteres Applet geladen (Sec*PKISignOn*), das eine Neuanmeldung gestattet. Neben den auf der SmartCard verankerten Daten wie z.B. Seriennummer und Hersteller, können diese Daten durch Freitextbeschreibungen ergänzt werden. Es hängt stets vom Betreiber des SSL-Angebotes ab, welche zusätzlichen Informationen dieser vom Inhaber der SmartCard fordert.

> **Hinweis**: Nach einer Neuanmeldung steht der Zugang zum System i.d.R. nicht sofort zur Verfügung, sondern erst nach Sichtung und Bearbeitung des Antrages.