



SecAuthenticator

Anwenderhandbuch

Version 2.1

5. Februar 2016

© 2001-2016 SecCommerce Informationssysteme GmbH

SecRouter, SecAuthenticator und SecPKI sind eingetragene Warenzeichen
der SecCommerce Informationssysteme GmbH, Hamburg

Dokumentenhistorie

Datum	Version	Inhalt / Änderung	Autor
07.02.2002	1.0	Erste Fassung	marks
13.02.2002	1.1	Korrekturen	marks
25.06.2002	1.2	Review	uhl
16.07.2002	1.3	Ergänzung	uhl
30.10.2002	1.4	Unterstützung Netscape 4.x entfernt	marks
16.07.2009	1.5	Ergänzungen unterstützte Hard-/Software	hl
17.07.2009	1.6	Aktualisierung Screenshots	hl
09.01.2013	1.7	Aktuelle Windows-Systeme	hl
13.11.2015	2.0	Java Webstart statt Applet	tk
05.02.2016	2.1	Zuordnung SecSign ID – SmartCard	tk

Inhaltsverzeichnis

1 Einführung.....	4
1.1 Systemvoraussetzungen Hardware.....	4
1.2 Systemvoraussetzungen Software.....	4
2 Sicherheitshinweise.....	5
3 Authentifikation mittels SecAuthenticator.....	6
3.1 SecSign ID.....	6
3.1.1 Zuordnung einer SecSign ID zu einer Smartcard oder einem Software- Zertifikat.....	6
3.1.2 SecSign ID Login.....	8
3.2 Smartcard-Login.....	8
3.3 Software-Zertifikat Login.....	9
4 Anmeldung neuer Benutzer.....	10

1 Einführung

Der SecCommerce SecAuthenticator sichert beliebige Web-Server durch Authentifizierung mit Hilfe von SmartCards, Software-Zertifikaten oder der SecSign ID ab. Im Zusammenspiel mit SecRouter können hochsichere HTTPS-Sitzungen realisiert werden.

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

1.1 Systemvoraussetzungen Hardware

Eine stets aktuelle Übersicht unterstützter Hard- und Software findet sich im Internet unter:

<https://www.seccommerce.com/> → Produkte → Unterstützte Hard- und Software

1.2 Systemvoraussetzungen Software

Betriebssysteme, jeweils in einer vom Hersteller noch unterstützten Version:

- Microsoft Windows
- Mac OS X
- Linux

Das Anwendersystem erfordert einen Internet-Browser sowie eine Java-VM in einer vom Hersteller Oracle unterstützten Version.

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

2 Sicherheitshinweise

Für die sichere Nutzung des SecAuthenticator sind grundsätzlich allgemeine Sicherheitsempfehlungen zu beachten. Siehe dazu die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik.

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. Bei Fragen zur Realisierung der Einstellungen ist die Dokumentation des verwendeten Internet-Browsers zu Rate zu ziehen.

3 Authentifikation mittels SecAuthenticator

Erfordert ein Webseite einen SmartCard-abgesicherten Zugang, so erscheint zunächst der Initialisierungsbildschirm des SecAuthenticators:



Abbildung 1: SecAuthenticator – Initialisierung

Je nach Konfiguration durch den Betreiber der Webseite stehen folgende Möglichkeiten der Anmeldung zur Verfügung:

- SecSign ID
- Smartcard
- Software-Zertifikat

3.1 SecSign ID

Die SecSign ID ist eine sichere und komfortable Zwei-Faktor-Authentifizierung. Der private Schlüssel des Nutzers befindet sich dabei in der SecSignApp auf seinem Smartphone. Die SecSignApp ist kostenlos in Apples AppStore bzw. Googles PlayStore verfügbar. Der Anwender kann sich in der SecSign App SecSign IDs erstellen, denen er jeweils einen selbst gewählten Namen gibt. Mit diesem Namen kann er sich dann an beispielsweise an Webseiten anmelden oder an seinem Windows-PC.

3.1.1 Zuordnung einer SecSign ID zu einer Smartcard oder einem Software-Zertifikat

An Webseiten, die ein Login mit dem SecAuthenticator ermöglichen, kann der Anwender seine vorhandene Smartcard oder sein Software-Zertifikat mit einer

SecSign ID verbinden. Er authentifiziert sich dabei einmalig mit seiner Smartcard oder seinem Software-Zertifikat sowie seiner SecSign ID:

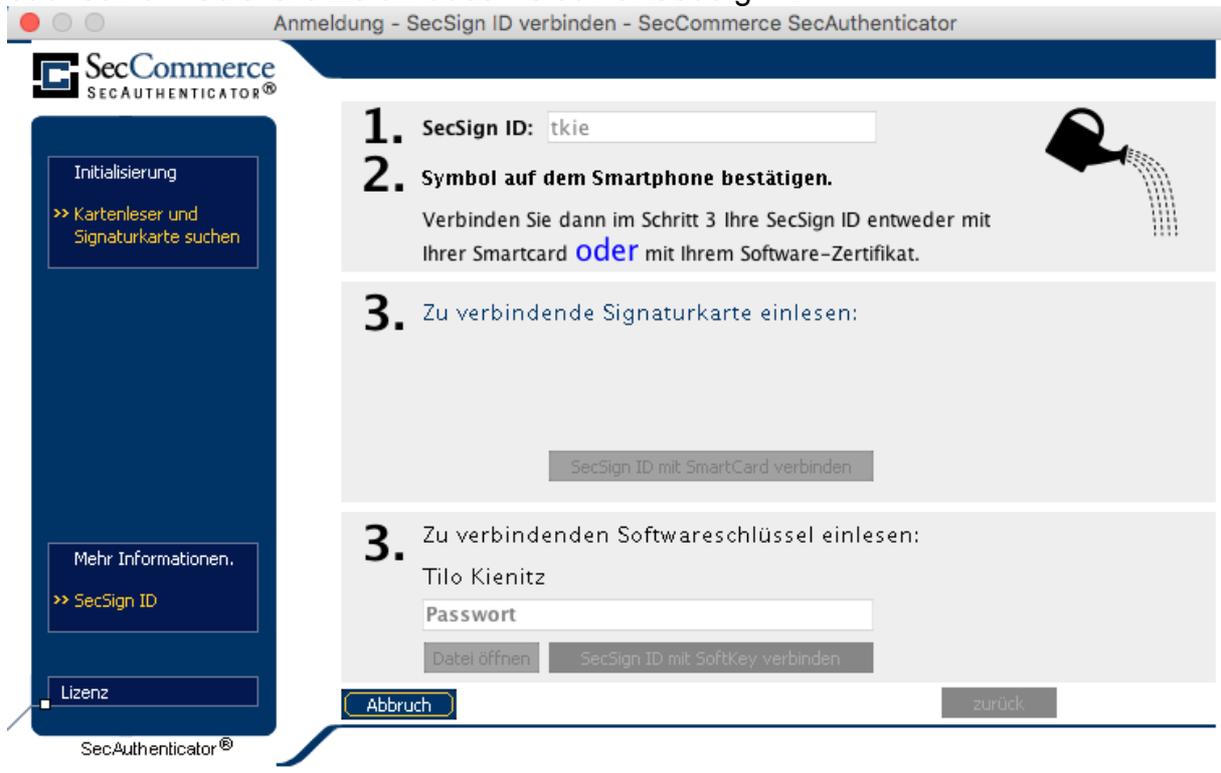


Abbildung 2: SecSign-ID-Authentifizierung für Zuordnung zu einer Smartcard

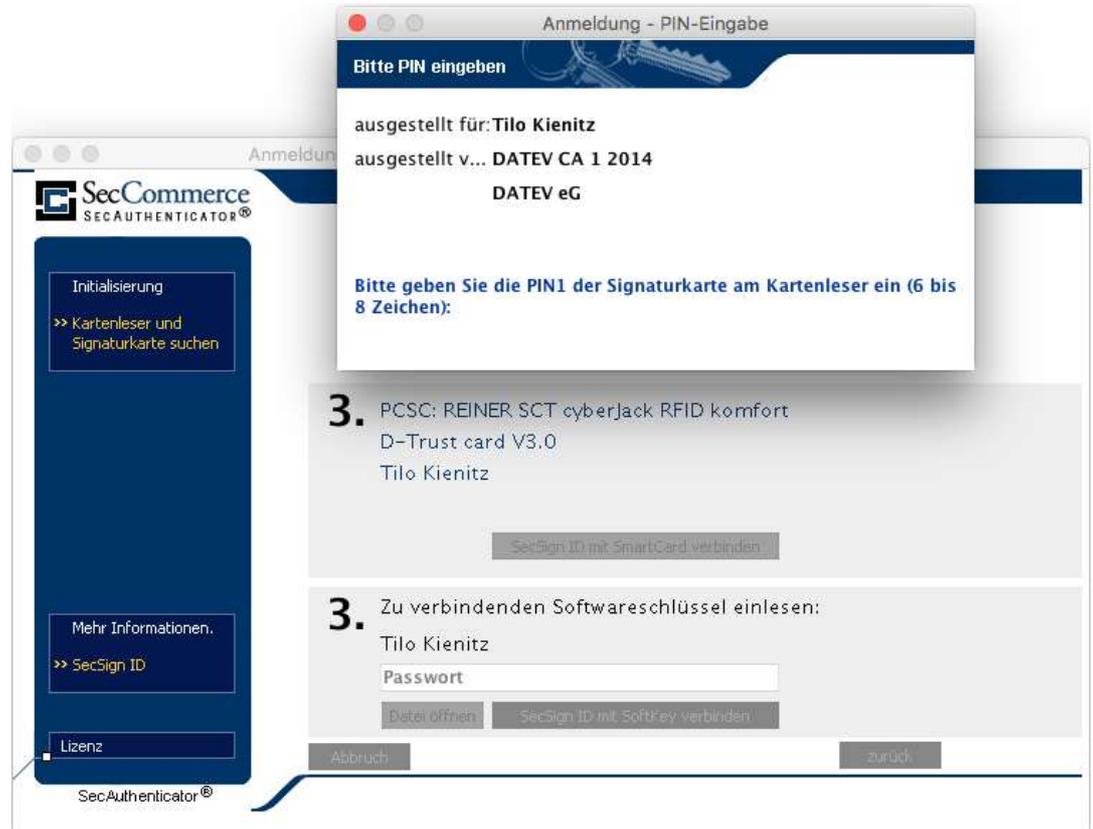


Illustration 3: Smartcard-Authentifizierung für Zuordnung zu einer SecSign-ID

✓ SecSign ID tkie mit Signaturkarte verbunden.
Sie können sich nun auch mit Ihrer SecSign ID anmelden.

Abbildung 4: SecSign ID erfolgreich einer Smartcard zugeordnet

3.1.2 SecSign ID Login

Nach der einmaligen Zuordnung einer SecSign ID zu einer Smartcard oder einem Software-Zertifikat kann zu jedem Login bequem die SecSign ID verwendet werden. Dazu ist der selbst gewählte Name der SecSign ID einzugeben auf „Anmelden“ zu klicken. Es erscheint ein Symbol, welches in der SecSign App bestätigt werden muss, um das Login zu erlauben.

Hinweis an Webseiten-Betreiber: Ein SecSign ID Login lässt sich einfacher auch ohne SecRouter und SecAuthenticator ermöglichen. Dafür stehen Plug-ins zur Verfügung.

<https://www.secsign.com/>

3.2 Smartcard-Login

Nach Anwahl der Schaltfläche „Anmelden“ neben dem Smartcard-Symbol wird automatisch der angeschlossene Kartenleser und die damit verwendete SmartCard ermittelt. Der auf der SmartCard enthaltene, öffentliche Authentifizierungsschlüssel¹ wird nun an Diensteanbieter gesandt², welcher eine Legitimationsprüfung durchführt. Ist diese erfolgreich, wird der Nutzer automatisch zur gewünschten Webseite weitergeleitet.

Anmerkung: Voraussetzung für diese Art der Identifikation ist das Vorhandensein eines Authentifizierungs-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.

¹ im Gegensatz zum Signaturschlüssel und Verschlüsselungsschlüssel.

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 5: SecAuthenticator – PIN-Eingabe

Hinweis: Beachten Sie bitte, dass SmartCards eine unterschiedliche PIN für Signaturzertifikat und Authentifizierungszertifikat besitzen. Gefordert ist stets die PIN des Authentifizierungsschlüssel.

3.3 Software-Zertifikat Login

Analog zu einer Smartcard kann auch ein Software-Zertifikat zum Login benutzt werden. Dieses wird aus einer Datei im Format PKCS#12 eingelesen. Oft haben solche Dateien die Endungen p12 oder pkcs12.

Der SecAuthenticator speichert das zuletzt benutzte Software-Zertifikat, so dass beim nächsten Login die Datei nicht erneut geladen werden muss. Das Passwort muss allerdings jedesmal eingegeben werden, da der SecAuthenticator die PKCS12-Datei zur Sicherheit in verschlüsselter Form speichert.

4 Anmeldung neuer Benutzer

Ist die verwendete SmartCard oder das Software-Zertifikat dem System nicht bekannt und gestattet der Betreiber der Webseite das Anmelden neuer Benutzer, so wird eine weitere Applikation geladen (*SecPKISignOn*), die 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 der Webseite 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.