SecCommerce
INFORMATIONSSYSTEME GMBH

SecAuthenticator

Anwenderhandbuch

Version 9.1.44

20. August 2019

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	Aktualisiertung 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
11.12.2018	9.1	Web-Run statt Java Webstart	tk
20.03.2019	9.1.32	gematik Konnektor	tk
20.08.2019	9.1.44	User-ID-Parameter im gematik-Konnektor-Dialog ergänzt	tk

Inhaltsverzeichnis

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. Der SecAuthenticator bringt bei der Installation ein OpenJDK von Azul Systems Inc. mit.

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 wenige Versuche, nach einigen Falscheingaben 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 Installation

Die Installation des SecAuthenticators erfolgt unter Windows durch das bereitgestellte Installationsprogramm SecAuth-9-Setup.exe, bzw. SecAuth-9-Setup.msi.

Unter MacOS muss die in SecAuthenticator.zip enthaltene SecAuthenticator-App in das Applications-Verzeichnis gezogen werden.

Unter Debian-Linux, bzw. Ubuntu erfolgt die Installation mit:

sudo dpkg -i secauthenticator_9.1.x_amd64.deb

Unter OpenSUSE erfolgt die Installation mit:

sudo zypper install SecAuthenticator-9.1.x-1.x86_64.rpm

Dem System ist dann bekannt, dass der SecAuthenticator für das Öffnen von secauthwr-Dateien zuständig ist. Beim Login bietet der SecRouter dem Browser eine ebensolche secauthwr-Datei zum Download und somit zum Start des SecAuthenticators an.

4 gematik Konnektor Einrichtung

Der SecAuthenticator kann sowohl lokal angeschlossene Kartenleser verwenden als auch solche, die über das Netzwerk mittels eines Konnektors nach gematik-Spezifikation erreichbar sind.

Für lokal angeschlossene Kartenleser ist nur die Installation des Treibers vom Kartenleser-Hersteller erforderlich.

Soll ein Konnektor verwendet werden, so muss im Konnektor ein Zugang für den SecAuthenticator eingerichtet werden. Support zu diesem Schritt kann nur der Hersteller des Konnektors oder ein spezieller Dienstleister übernehmen.

Der Dialog zum Einstellen der Parameter für den Konnektorzugriff öffnet sich nach einem Mausklick auf den Menüpunkt „Konnektor Konfig.“:

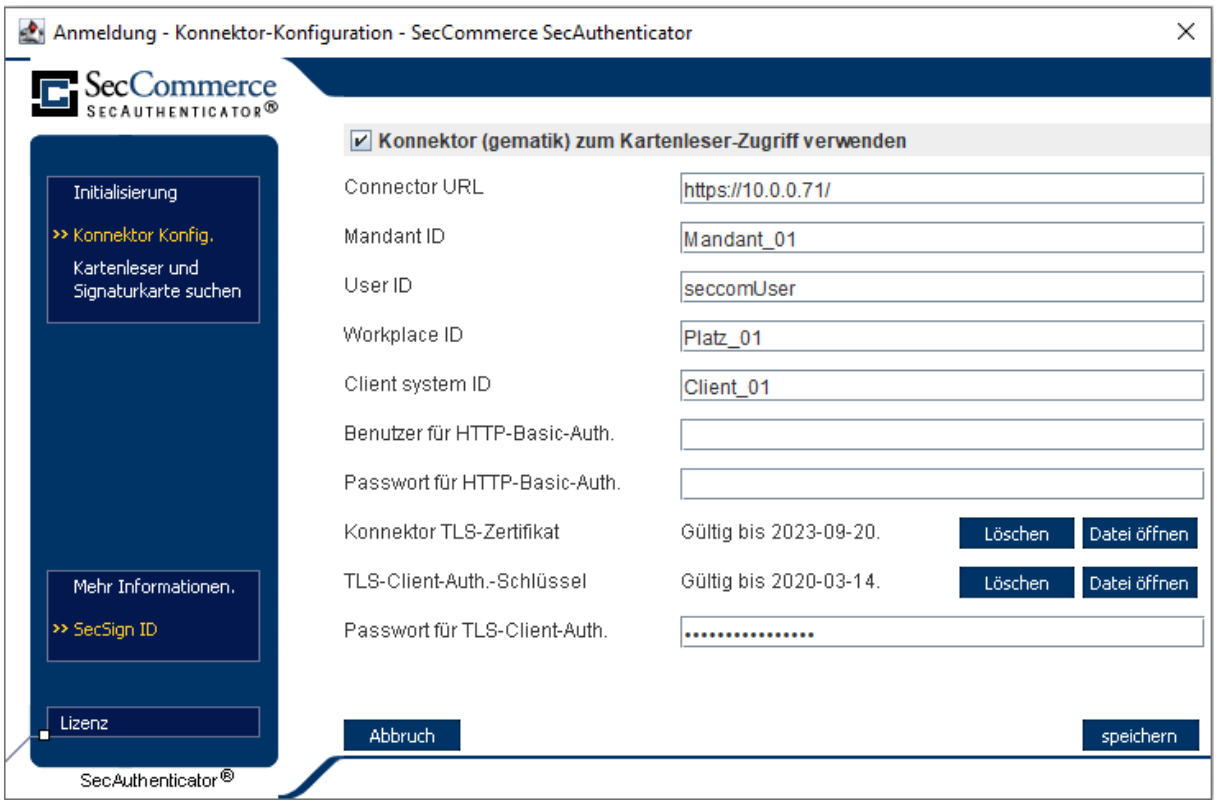

Abbildung 1: Konnektor Parameter

Im einzelnen sind folgende Parameter einzustellen:

- Connector-URL gibt die URL an, unter der der Konnektor im lokalen Netzwerk erreichbar ist.
- Mandant ID, User ID, Workplace ID und Client-System ID geben den technischen Benutzer für den SecAuthenticator im Konnektor an.
- Falls im Konnektor eingestellt wurde, dass für den Zugriff ein HTTP-Benutzername und -Passwort erforderlich sind, sind diese bei „Benutzer für HTTP-Basic-Auth“ und „Passwort für HTTP-Basic-Auth“ einzutragen.
- Um die Übertragung zwischen SecAuthenticator und Konnektor abzusichern, kann das Zertifikat, mit dem der Konnektor sich ausweist, aus einer Datei geladen werden. Die Datei muss im DER-Format sein. Der SecAuthenticator bricht Verbindungen zum Konnektor ab, falls dieser nicht das hier konfigurierte Zertifikat verwendet.
  Das Konnektor-Server-Zertifikat hat eine begrenzte Gültigkeitszeit. Das Ablaufdatum wird hier

angezeigt. Es muss rechtzeitig vorher ein neues Zertifikat eingetragen werden, sonst ist keine Verbindung zum Konnektor mehr möglich.
Ist hier kein Zertifikat angegeben, erfolgt die Übertragung der Daten zum Konnektor zwar trotzdem TLS-verschlüsselt, es wird jedoch jedes Server-Zertifikat akzeptiert. Ein sogenannter Man-in-the-Middle-Angriff ist möglich.

- Falls im Konnektor eingestellt wurde, dass für die Zugriff eine TLS-Client-Authentifizierung erforderlich ist, muss der entsprechende Schlüssel hier aus einer Datei im PKCS#12-Format geladen werden. Das Passwort zur Entschlüsselung dieser Datei wird bei „Passwort für TLS-Client-Auth.“ angegeben.
  Die PKCS#12-Datei kann vom Konnektor erstellt werden. Sie enthält ein Zertifikat, das ein Ablaufdatum hat, welches hier angezeigt wird. Rechtzeitig vor Ablauf muss eine neue PKCS#12-Datei erstellt und hier eingelesen werden, mit die Kommunikation mit dem Konnektor weiterhin möglich ist.

5 Authentifikation mittels SecAuthenticator

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

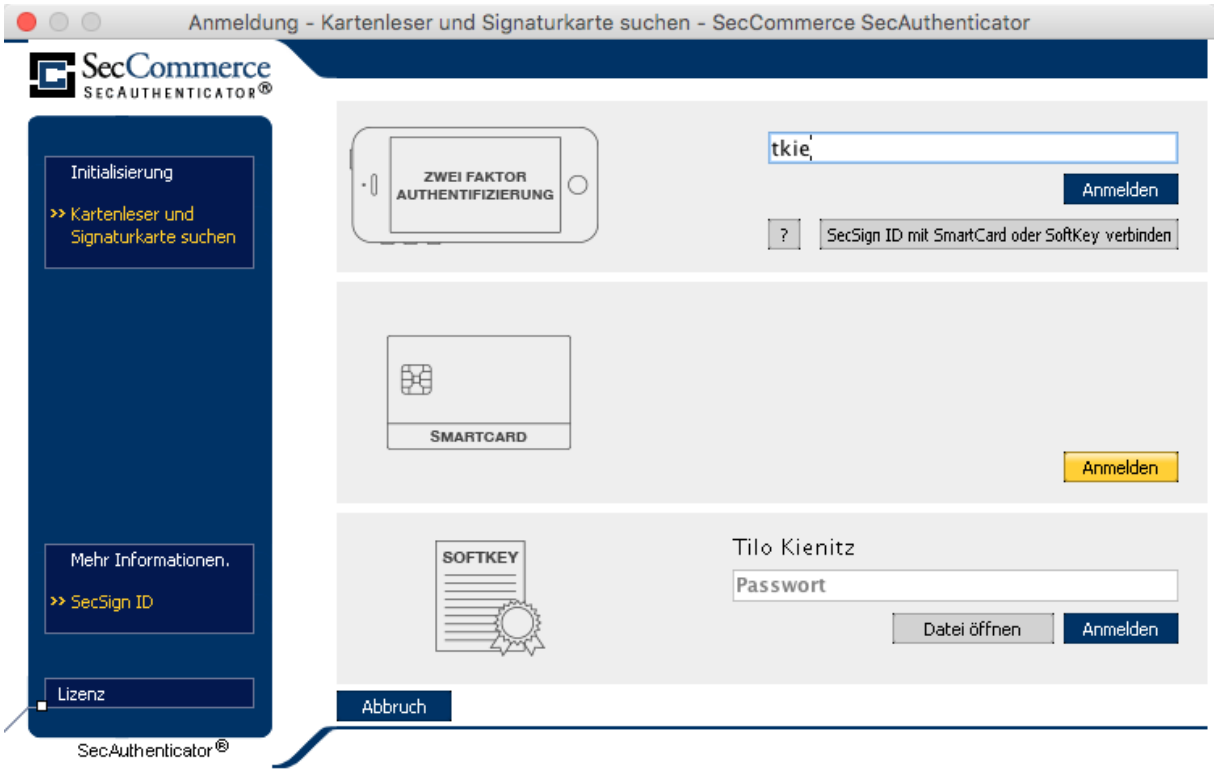

Abbildung 2: SecAuthenticator – Initialisierung

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

- SecSign ID
- Smartcard
- Software-Zertifikat

5.1 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.

5.1.1 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 3: SecSign-ID-Authentifizierung für Zuordnung zu einer Smartcard

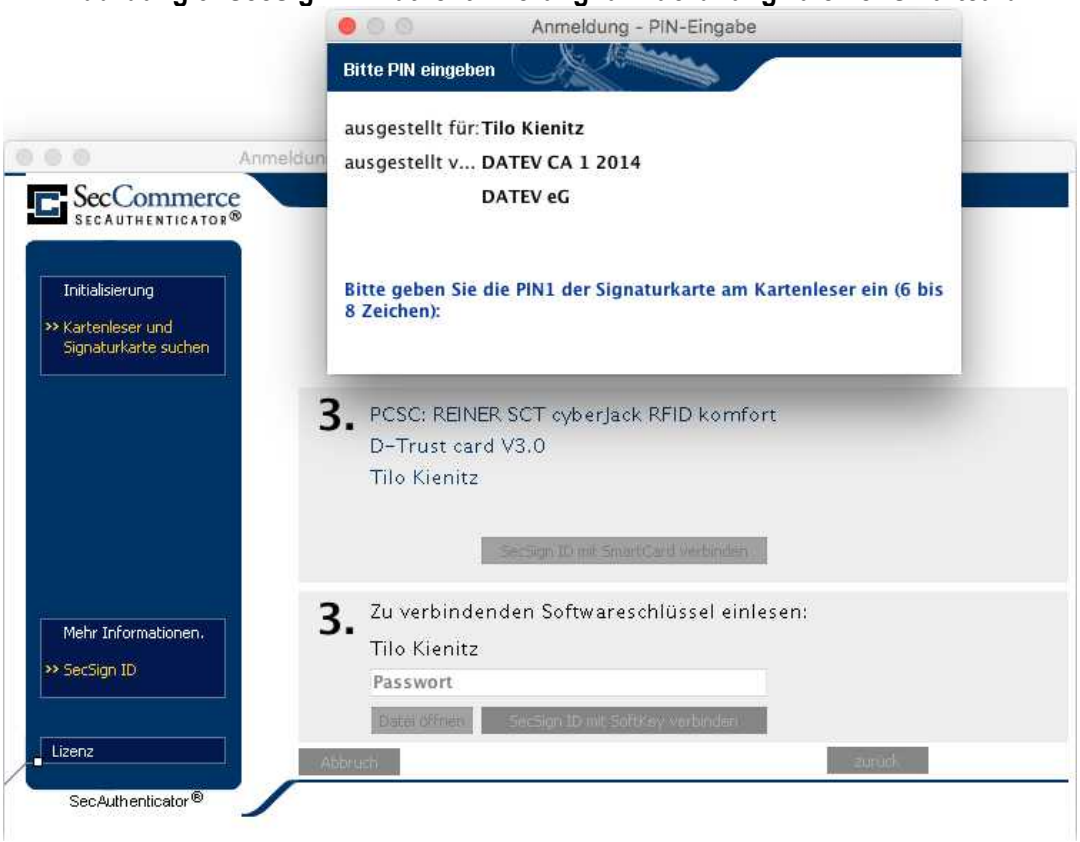

Illustration 4: Smartcard-Authentifizierung für Zuordnung zu einer SecSign-ID

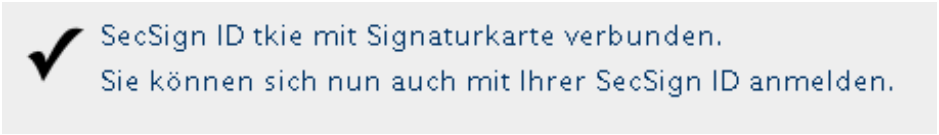

Abbildung 5: SecSign ID erfolgreich einer Smartcard zugeordnet

5.1.2 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/

5.2 Smartcard-Login mit lokal angeschlossenem Kartenleser

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 Authentifizierungsschlüssel[1] wird nun an Diensteanbieter gesandt[2], 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 6: SecAuthenticator – PIN-Eingabe

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

5.3 Smartcard-Login über Konnektor

Wurde eingestellt, dass der SecAuthenticator über einen Konnektor auf Kartenleser zugreift, wie in Abschnitt beschrieben, so fragt der SecAuthenticator beim Konnektor die gesteckten Signaturkarten in allen mit dem Konnektor verbundenen Kartenlesern ab. Unterstützt werden nur die Kartentypen Heilberufsausweis (z.B. für einen Arzt) und SMC-B (z.B. für eine Arztpraxis).

Der SecAuthenticator zeigt die gefundenen Signaturkarten in einer Auswahlliste an. Nach Auswahl einer Karte in der Liste kann das Login mit einem Mausklick auf „Anmelden“ gestartet werden.

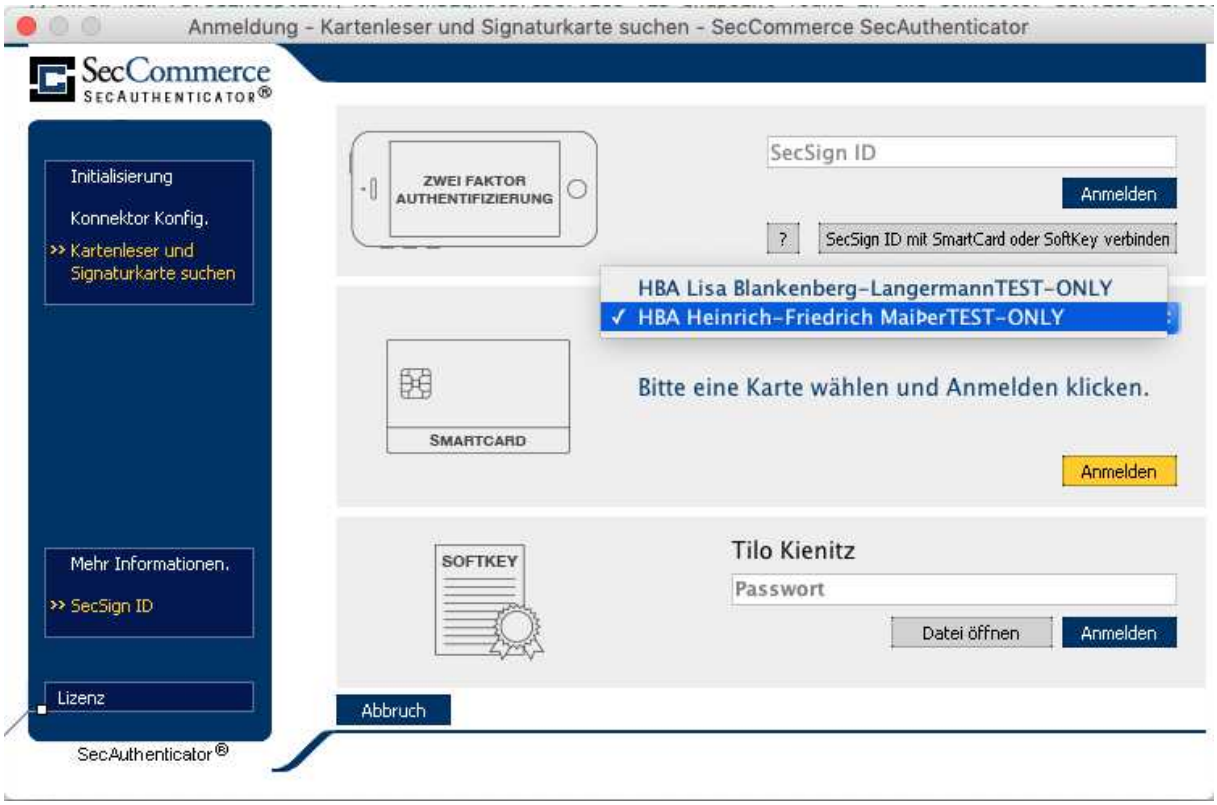

Abbildung 7: Anmeldung über den Konnektor (gematik)

5.4 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.

6 Log-Dateien

Der SecAuthenticator schreibt Meldungen über durchgeführte Aktionen und dabei aufgetretete Fehler in die Log-Dateien secauthenticatorXX.log und seccommerceXX.log. XX steht dabei für den Tag des Monats. Die Log-Dateien befinden sich im Verzeichnis .seccommerce/temp im Home-Verzeichnis des Anwenders. Sie enthalten Informationen, die für die Fehlerbehebung durch den technischen Support hilfreich sind.

7 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 (Sec*PKISignOn*), 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.