



crypto vision

cv act *sc/interface* V6.0

Handbuch

Inhaltsverzeichnis

1	Einführung	5
2	Über dieses Handbuch	6
3	Grundlagen der Public Key Kryptographie	7
3.1	Was ist eine Smartcard-Middleware?	7
3.2	Was sind Public Key Kryptographie-Standards?	8
3.3	Was sind kryptografische Schnittstellen?	10
4	Über cv act sc/interface	12
4.1	Die Module von cv act sc/interface	12
5	Unterstützte Hardware	14
5.1	Security Token	14
5.2	Kartenleser	18
5.3	Citrix Terminal Server	22
6	Installation von cv act sc/interface	24
6.1	Installation auf Windows	24
6.2	Installation auf Linux	29
6.3	Installing on OS X	36
7	Das Administrationstool	37
8	Beispiel: Konfiguration einer Smartcard für die erste Nutzung	55
8.2	Erzeugen von Karten-Profilen	56
9	Verwenden von Biometrie	62
9.1	Unterstützte Smartcards und Leser	62
9.2	Profile	62
9.3	Fingerabdruck initialisieren	63
9.4	Fingerabdruck entsperren und löschen	65
9.5	Sensor-Leser-Zuordnung	65
10	Weitere Funktionen	67
10.1	Das Data-Verzeichnis	67
10.2	Die Funktion "Open Token"	69

10.3	Die Funktionen "Delete all" und "Delete Certificate" / "Delete Data" / "Delete Secret key" / "Delete Container"	69
10.4	Funktion "Set Default Container"	70
10.5	Die Funktion "Show Certificate"	70
10.6	Die Funktion "Export Certificate"	71
10.7	Die Funktion "Register Certificate"	71
10.8	Die Funktion "Check Private Key"	72
10.9	Die Funktion "Check Secret Key"	74
11	User Tool	75
12.1	cv act <i>sc/interface</i> Manager und cv act <i>sc/interface</i> Utility starten	78
12.2	PKCS#11 registrieren und abmelden	79
12.3	Unterbrechen und Fortsetzen	79
12.4	Einstellungen	80
12.5	Exit	81
13	Fortgeschrittene Konfiguration der Cryptographic Interfaces	82
13.1	CSP-Modul	82
14	Minidriver	88
14.1	CMCK-Zertifizierung	88
14.2	Minidriver-Unterstützung mit PACE	88
15	PKCS#11-Modul	90
15.1	Allgemeine Vorgehensweise	90
15.2	Smartcard-Login an einem Novell eDirectory	91
15.3	SSL-Smartcard-Authentifizierung mit Firefox / Safari	91
15.4	E-Mail-Sicherheit mit Smartcards für den Mozilla Messenger	91
15.5	cryptovision-Producte, beispielsweise cv act <i>s/mail</i> oder cv act PKIntegrated	91
15.6	Verfahren auf Basis Elliptischer Kurven (ECC)	91
15.7	Initialisierung über PKCS#11	92
15.8	Identifikation einer Smartcard	93
Anhang A:	Referenz für Entwickler	95
	Kurzbeschreibung einzelner Funktionen	95
	Objekte	98

Mechanismen	100
Anhang B: Debug	102
PKCS#11 Logger (win)	102
CSP Logger (win)	102
Anhang C: Zertifikatsattribute (Key Usage)	103
Information / Export Restrictions.....	104

1 Einführung

Vielen Dank, dass Sie sich für cv act *sc/interface* entschieden haben.

Sichere elektronische Identitäten gewinnen immer mehr an Bedeutung. Hierbei reicht es oft nicht mehr aus, für die Identitätsprüfung nur Benutzername und Passwort zu verwenden. Stattdessen sind sicherere und benutzerfreundlichere Methoden in vielen Fällen ein Muss. Digitale Zertifikate, zusammen mit Smartcards oder anderen Security-Tokens, gelten als Ideallösung für diesen Zweck. Smartcards werden bereits seit Jahrzehnten als Bankkarten und seit kurzem auch als elektronische Ausweiskarten eingesetzt. Mit Hilfe eines Kartenlesers sind sie auch am PC nutzbar.

Das inzwischen große Angebot an Smartcards und anderen Security-Tokens hat dafür gesorgt, dass die Hardware in Authentifizierungssystemen meist kein kritischer Faktor mehr ist. Stattdessen hängt der Erfolg von der Smartcard-Middleware ab.

Eine Smartcard-Middleware ist eine Software, die ein Security-Token mit einer PKI-Anwendung verbindet. Eine gute Smartcard-Middleware-Lösung zeichnet sich dadurch aus, dass sie auf verschiedenen Plattformen lauffähig ist und viele Anwendungen auf unterschiedlichen Geräten unterstützt. Darüber hinaus sollte eine Smartcard-Middleware standardisierte Protokolle und moderne kryptografische Methoden verwenden.

cv act *sc/interface* ist eine leistungsfähige Smartcard-Middleware. Sie verbindet nahezu jede PKI-Anwendung (zum Beispiel Windows, Outlook, Safari und Mozilla) mit einem nahezu beliebigen Security-Token. cv act *sc/interface* unterstützt alle relevanten Krypto-Schnittstellen auf allen gängigen Betriebssystemen. Auf Windows werden sowohl Microsoft CSP als auch Minidrivers angesprochen. Für das Mac OS ist die TokenD-Schnittstelle und für Linux-Derivate der PKCS#11-Standard implementiert. Mit der Hardware-Unterstützung von über 50 Kartentypen bietet cv act *sc/interface* außerdem eine weitgehende Unabhängigkeit von einem bestimmten Kartenanbieter und gewährleistet ein Maximum an Interoperabilität.

cv act *sc/interface* unterstützt Krypto-Verfahren, die von der NSA und dem BSI empfohlen werden. Dazu gehören insbesondere RSA und Verfahren auf Basis elliptischer Kurven. Weitere Vorzüge, wie Plattformunabhängigkeit und eine modulare Architektur, machen cv act *sc/interface* zu einem der besten Produkte seiner Art auf dem weltweiten Markt.

2 Über dieses Handbuch

Dieses Dokument ist eine Bedienungsanleitung für Administratoren von Smartcard und Security Token Middleware. Es geht davon aus, dass eine funktionierende Installation von verschiedenen Certificate Authorities und Webservices vorhanden ist, die eine Public Key Infrastructure (PKI) umfasst, in die Security Token integriert werden sollen. Für weitere spezifische Installationsanleitungen und Referenzmaterialien für die vorhandenen PKI-Konfigurationen verwenden Sie bitte die Originaldokumentationen der entsprechenden Hersteller.

Dieses Handbuch enthält Installations- und Anwendungsanleitungen für Administratoren von cv act *sc/interface*. Es würde den Rahmen dieses Handbuchs sprengen, zu erklären, wie Sie 3rd-Party-Software anderer Anbieter konfigurieren müssen. Bitte beachten Sie dazu die Dokumentationen der jeweiligen Produkte vor der Installation und dem Betrieb von cv act *sc/interface*.

Da cv act *sc/interface* ein delegated administration model unterstützt, können verschiedene Module installiert werden, abhängig von den Funktionen, die benötigt werden. Wenn Sie cv act *sc/interface* in der Admin Edition nutzen, lesen Sie bitte die Beschreibung des Administrationstools. Darin wird beschrieben, wie Sie Schlüssel und Zertifikate verwalten, PINs ändern, Smartcards entsperren, initialisieren und personalisieren.

Wenn Sie cv act *sc/interface* in der Benutzer Edition nutzen, lesen Sie bitte die Beschreibung des Benutzertools. Darin wird beschrieben, wie Sie PINs ändern und die Smartcard registrieren.

Weiter finden Sie jeweilige Kapitel zu den anderen Bestandteilen von cv act *sc/interface*, wie das Register Tool, CSP-Modul, Minidriver-Modul, PKCS#11-Modul und das TokenD-Modul sowie Informationen über Fingerabdruck und darüber, welche Anwendungen Sie mit Smartcards verwenden können.

Zur Vertiefung schließt sich ein Referenzteil an: Anwendungsentwickler finden weiterführende Informationen wie man auf Module von cv act *sc/interface* zugreift (z.B. auf PKCS#11) in Anhang A. Dieses ist hilfreich, um Benutzeranwendungen zu entwickeln. Anhang B gibt eine kurze Beschreibung der verwendeten Zertifikatsattribute, d.h. Informationen über die Schlüsselverwendung.

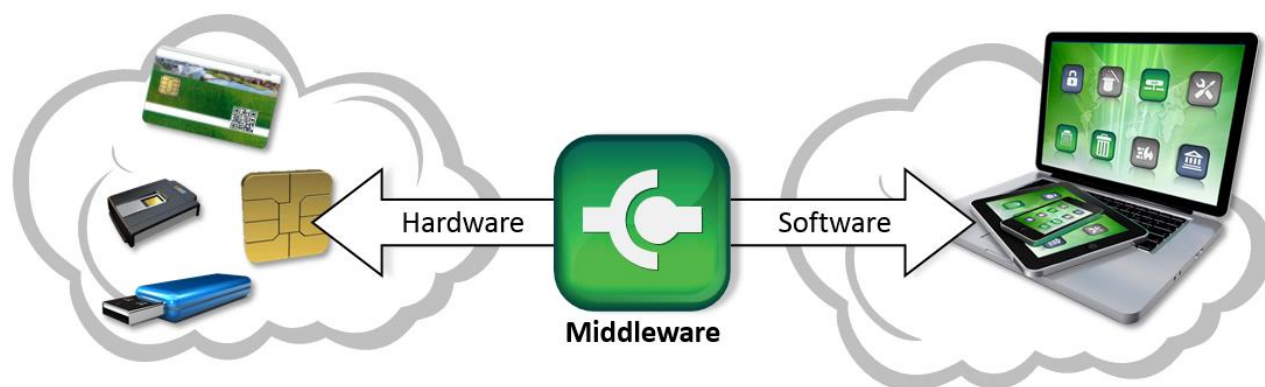
HINWEIS: Zum Verständnis dieses Handbuchs werden Grundkenntnisse in der IT-Sicherheit vorausgesetzt. Speziell sollten Sie vertraut sein mit den Begriffen (digitales) Zertifikat, privater, öffentlicher und geheimer Schlüssel, digitale Signatur, PKI, usw. Falls Sie Ihr Wissen im Bereich IT-Sicherheit und Kryptographie erweitern möchten, finden Sie Informationen in den Bereichen Solutions und Company der cryptovision-Homepage: <http://www.cryptovision.com/>

3 Grundlagen der Public Key Kryptographie

3.1 Was ist eine Smartcard-Middleware?

Betriebssystem-Login, VPN-Zugang, Zugang zu sicheren Web-Portalen und ähnliche Anwendungen müssen geschützt werden. Viele Unternehmen nutzen zu diesem Zweck immer noch Passwörter, obwohl dies weder sicher noch benutzerfreundlich ist. Besser ist es, Smartcards oder andere Security-Tokens an die Nutzer auszugeben. Auf einem solchen Token wird ein geheimer Schlüssel gespeichert. Ein Token mit Schlüssel bietet eine deutlich sicherere Authentifizierung als ein einfaches Passwort. Darüber hinaus lassen sich Security-Tokens auch zum Verschlüsseln und digitalen Signieren nutzen.

Um ein Security-Token auf einem Host (z. B. PC) nutzen zu können, ist eine Smartcard-Middleware (auch als Token-Middleware bezeichnet) notwendig. Eine solche verbindet eine Smartcard oder ein anderes Security-Token mit dem Host-Betriebssystem und einer oder mehreren Anwendungen. Die Smartcard-Middleware erfüllt hierbei die Funktion eines Treibers. Sie stellt den Anwendungen eine Hardware-unabhängige kryptografische Schnittstelle zur Verfügung und kommuniziert mit der Karte über eine Hardware-nahe API. Darüber hinaus enthalten viele Smartcard-Middleware-Lösungen ein Management-Programm für das Formatieren, Personalisieren und ähnliche Administrationsaufgaben.



Die Technik einer Smartcard-Middleware ist erstaunlich komplex. Da viele Anwender ihre Karte auf unterschiedlichen Host-Geräten nutzen (zum Beispiel auf dem PC und dem Tablet), muss die Middleware mehrere Plattformen unterstützen. Darüber hinaus werden mehrere Dutzend Karten und Tokens am Markt angeboten, die meist nicht miteinander kompatibel sind – und dennoch von derselben Smartcard-Middleware unterstützt werden sollten. Und schließlich existieren teilweise sogar auf der gleichen Plattform unterschiedliche Krypto-Schnittstellen – etwa CSP und Minidriver auf Windows. Damit muss die Smartcard-Middleware umgehen können.

3.2 Was sind Public Key Kryptographie-Standards?

Es versteht sich von selbst, dass Formate und Protokolle im Zusammenhang mit Security-Tokens standardisiert werden sollten. In den frühen 1990er-Jahren machte die damalige US-Firma RSA Data Security diesbezüglich den Anfang, indem sie Spezifikationen für das RSA-Verfahren und einige andere Methoden entwickelte – die “PKCS-Standards” waren geboren. Diese gewannen eine große Verbreitung. Zwar wird die Entwicklung der PKCS-Standards bis heute von einem Privatunternehmen geleitet, doch andere Standardisierungsgremien – insbesondere die Engineering Task Force ([IETF](#)) und deren Public Key Infrastructure Working Group ([PKIX WG](#)) – haben große Teile davon übernommen. Die PKCS-Standards sind durchnummeriert und werden als PKCS#1, PKCS#2, PKCS#3 usw. bezeichnet. Im Folgenden werden die wichtigsten davon vorgestellt.

3.2.1 PKCS#7: Cryptographic Message Syntax Standard

Die Cryptographic Message Syntax (CMS) ist der IETF-Standard für kryptografisch geschützte Daten. Mit CMS lassen sich verschlüsselte, digital signierte und gehashte Nachrichten kodieren. CMS bildet die Grundlage für andere Formate, insbesondere für die Secure/Multipurpose Internet Mail Extensions ([S/MIME](#)), die ein Format für verschlüsselte und signierte E-Mails festlegen.

3.2.2 PKCS#10: Certification Request Standard

Das Beantragen eines digitalen Zertifikats bei einer Zertifizierungsstelle ist ein wichtiger Vorgang in einer Public-Key-Infrastruktur. [PKCS#10](#) spezifiziert ein Format für einen solchen Zertifizierungsantrag (Certification Request). Ein PKCS#10-Request besteht aus einem Namen (Distinguished Name nach X.500), einem öffentlichen Schlüssel sowie einigen weiteren Attributen. Der Antrag wird vom Antragssteller digital signiert. Die Zertifizierungsstelle, die den Antrag bearbeitet, prüft die Angaben (insbesondere die Signatur) und stellt im positiven Fall ein X.509-Zertifikat aus.

3.2.3 PKCS#11: Cryptographic Token Interface “Cryptoki”

[PKCS#11](#) beschreibt eine Programmierschnittstelle namens Cryptoki. Diese Schnittstelle ermöglicht den Hardware-unabhängigen Zugriff auf Smartcards, Security-Tokens und andere Krypto-Module. Mehrere Module und mehrere zugreifende Geräte lassen sich über dieselbe Schnittstelle betreiben.

3.2.4 PKCS#12: Personal Information Syntax Standard

[PKCS#12](#) spezifiziert ein Format für das sichere Speichern und Transportieren von privaten Schlüsseln inklusive der zugehörigen Zertifikate. Der Schutz der Informationen erfolgt über eine symmetrische Verschlüsselung, wobei der Schlüssel von einem Passwort abgeleitet wird. PKCS#12 ist ein Nachfolger des PFX-Formats (Microsoft Personal Information Exchange), allerdings werden die Bezeichnungen der beiden Formate oft synonym verwendet.

3.2.5 PKCS#15: Cryptographic Token Information Format Standard

cv act *sc/interface* implementiert ein ISO-7816-kompatibles Dateisystem, das auf unterschiedlichen Plattformen nutzbar ist. Dieses Dateisystem bietet Leistungsmerkmale, die in [PKCS#15](#) -und ISO-7816-15-festgelegt sind. Außerdem ist die Schnittstelle für IAS-Anwendungen (Identification, Authentication, Signatures) nutzbar, wobei optional auch Unterstützung für Fingerabdruckerkennung über das Biomatch J™ Package von Precise Biometrics geboten wird. PKCS#15 definiert eine hierarchische Datei- und Verzeichnisstruktur für den Chip eines Security-Token. Diese wird für das Speichern von Schlüsseln, Zertifikaten und einigen Zusatzinformationen verwendet. Ein Vorteil dieser Standardisierung besteht darin, dass verschiedene Host-Programme (z. B. unterschiedliche Smartcard-Middlewares) auf dieselben Security-Tokens zugreifen können, ohne dass Anpassungen auf der Dateiebene des Chips notwendig sind.

3.2.6 ISO/IEC 7816-15:2004 Cryptographic Information Application

Der PKCS#15-v1.1-Standard wurde inzwischen von ISO 7816-15 abgelöst. Letzteres Format bildet daher de-facto PKCS#15-v2. Es besteht Abwärtskompatibilität zu früheren PKCS-15-Versionen.

[ISO/IEC 7816-15](#) wird in der Spezifikation wie folgt beschrieben:

"ISO / IEC 7816-15:2004 spezifiziert eine Kartenanwendung. Diese Anwendung enthält Informationen zu kryptografischen Funktionen. Außerdem definiert ISO/IEC 7816-15:2004 eine gemeinsame Syntax (ASN.1) und das Format für die kryptografische Informationen und Mechanismen, um diese Informationen zu teilen, wann immer angemessen.

ISO / IEC 7816-15:2004 unterstützt die folgenden Funktionen:

- *Speicherung kryptographischer Informationen auf einer Karte (in mehreren Instanzen)*
- *Verwendung kryptographischer Informationen*
- *Abruf der kryptographischen Informationen*
- *Verlinkung kryptographischer Informationen mit Objekten, die in ISO/IEC 7816 definiert werden*
- *verschiedene Authentifizierungsmechanismen*
- *mehrere Verschlüsselungsalgorithmen*

3.2.7 PACE (Password Authenticated Connection Establishment) nach TR-03110

PACE (Password Authenticated Connection Establishment) ist ein gegenseitiger Authentisierungsmechanismus zwischen Lesegerät und Chip basiert aber auf einem gemeinsamen Passwort, z. B. einer geheimen PIN die nur dem Inhaber bekannt ist, oder einer CAN (Card Access Number, Kartenzugriffsnummer) die auf der Smartcard aufgedruckt ist (wie bei dem deutschen elektronischen Personalausweis). Das Verfahren dient zum initialen Aufbau einer sicheren Verbindung.

Das Protokoll wurde vom Bundesamt für Sicherheit in der Informationstechnik für den Einsatz im neuen Personalausweis entwickelt und wird u.a. in der Technischen Richtlinie [TR-03110](#) beschrieben.

PACE hat den Vorteil, dass sich die Länge des Passwortes nicht auf das Sicherheitsniveau der Verschlüsselung auswirkt. Das heißt, auch bei einer so nicht so sicheren PIN (d.h. mit geringer Entropie) sind die Daten auf dem Chip der Smartcard und während der Übertragung stark geschützt (Secure Messaging), indem ein

sicherer Kanal von cv act *sc/interface* zur Smartcard aufgebaut genutzt wird und eine PIN nirgendwo auf dem PC zwischengespeichert wird.

3.3 Was sind kryptografische Schnittstellen?

In aktuellen IT-Umgebungen sollen die meisten Anwendungen auf vielen verschiedenen Plattformen ausgeführt werden. Zum Beispiel wird eine einzelne Internet-Seite oft von Anwendern auf Windows, Mac OS X, Linux oder anderen genutzt. Weiter nutzen diese unterschiedlichen Browser auf den verschiedenen Betriebssystemen unterschiedliche Mechanismen zur Durchführung kryptographischer Operationen. Um eine unabhängige Entwicklung von Anwendungen für den Einsatz auf unterschiedlichsten Plattformen zu unterstützen, nutzt man eine programmatische Schnittstelle für kryptografische Operationen. Diese spezifische Schnittstelle ist abhängig vom Betriebssystem und der gewünschten Anwendung.

cv act *sc/interface* unterstützt die folgenden kryptografischen Schnittstellen:

3.3.1 Cryptographic Service Provider

Im Microsoft Betriebssystem ist der Cryptographic Service Provider eine Komponente, die kryptographische Funktionen zur Verfügung stellt. Das Betriebssystem selbst stellt spezifische CSPs zur Verfügung, die konfiguriert sind, um mit den entsprechenden Zertifikatstemplate und den definierten kryptografischen Algorithmen verwendet zu werden. Durch die Auswahl eines bestimmten CSP können Administratoren effektiv bestimmen, welche Algorithmen und Schlüssellängen mit den ausgestellten Zertifikaten verwendet werden. Zusätzliche CSPs können hinzugefügt werden, wie die cryptovision cvCSP.DLL aus cv act *sc/interface*, die erweiterte Funktionalität wie Biometrie oder PIN-Caching zur Verfügung stellt.

3.3.2 Minidriver

Microsoft hat eine neue Schnittstelle definiert, die für den Zugriff auf Smartcards genutzt werden kann. Diese Schnittstelle stellt ein konsistentes Interface zur Verwendung von Smartcards über den Base Smart Card Cryptographic Service Provider (Base CSP) oder den Crypto Next Generation (CNG) Key Storage Provider (KSP) und das Smart Card Management Interface zur Verfügung.

Dieser Minidriver wird bei der Installation in den Windows Systemcode eingefügt. Die Funktionalität umfasst wenige, kartenspezifische Bereiche. Die weiteren Code-Bestandteile, die bei einem Smartcard-CSP bisher notwendig waren, sind in das Betriebssystem integriert.

Weitere Informationen sind in der „Smart Card Minidriver Specification“ im Internet verfügbar unter: ["Smart Card Minidriver Specification"](#).

Nähere Erläuterungen zu dem Card Minidriver, der in cv act *sc/interface* enthalten ist, finden sich in dem Kapitel „Minidriver“.

3.3.3 TokenD

TokenD ist die definierte Schnittstelle für den Zugriff auf Smartcards mit Mac OS. Die Schlüssel auf Smartcards können damit von Anwendungen wie Logon, Safari Browser oder dem Mail-Client verwendet werden.

Ein Keychain (Schlüsselbund) ist ein verschlüsselter Container, der Passwörter für verschiedene Anwendungen und sichere Dienste verwahrt. Also sind Keychains sichere Speicherorte, d.h. wenn ein Keychain gelockt ist, kann niemand darauf zugreifen. In Mac OS X können Benutzer ein Keychain entsperren, so dass vertrauenswürdige Anwendungen Zugriff auf den Inhalt haben – durch Eingabe eines einzigen Master-

Passworts. Weitere Informationen finden Sie im "[Keychain Services Programming Guide](#)" von der Apple iOS Developer Library.

3.3.4 PKCS#11 Library

Die PKCS#11 library von cv act *sc/interface* wird entweder als Dynamic Link Library für Windows (cvP11.dll) oder als shared Object (libcvP11.so) für Linux und Mac OS X geliefert. Diese Bibliotheken ermöglichen Betriebssystem oder dem Kernel Level-Interaktionen mit dem kryptografischen Token über die Cryptoki API.

3.3.4.1 Virtuelle Slots

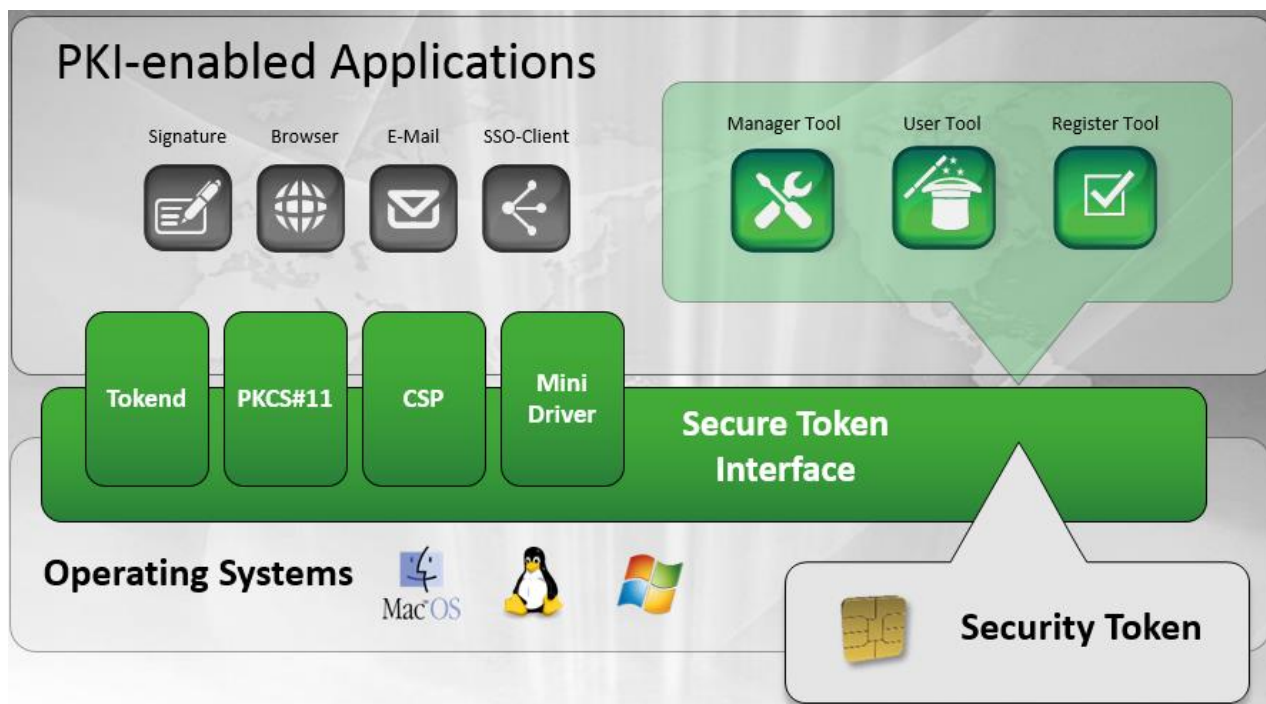
cv act *sc/interface* unterstützt Smartcards, bei denen mehrere Anwendungen auf der Smartcard zur Verfügung stehen, oder mehrere PINs pro Application, so wie D-Trust oder SwissSign.

Weil PKCS#11 nicht dazu bestimmt ist, mit mehr als einer User-PIN benutzt zu werden, wurde von Nexus eine Lösung für multi-application Szenarios eingeführt, die sogenannten Virtuellen Slots (siehe PKCS#11 v2.10 <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/pkcs11-v2-10/pkcs11v2-10.pdf>). Durch die Aufteilung eines Slots in mehrere "virtuelle Slots" kann genau eine Benutzer-PIN pro virtuellem Slot für jede Anwendung, die PKCS#11 nutzen kann, definiert werden. Dies ermöglicht eine einzige Smartcard mehrere Benutzer-PINs für Schlüsselmateriale bereitzustellen. Dies wird durch einen einzigen logischen Slot innerhalb von cv act *sc/interface* realisiert, aber für eine Anwendung scheint es, dass es mehrere Slots und Token gibt.

4 Über cv act *sc/interface*

4.1 Die Module von cv act *sc/interface*

Die folgende Abbildung zeigt Ihnen die architektonischen Komponenten der Middleware:



cv act *sc/interface* besteht aus verschiedenen Modulen:

- **Administrationstool:** Das Administrationstool stellt volle Karten-, Schlüssel- und Zertifikatsmanagement Funktionen zur Verfügung. Zum Funktionsumfang gehört Schlüsselerzeugung, Importieren und Exportieren von Zertifikaten sowie andere Funktionen wie die Erzeugung von Zertifikatsanfragen. Mit diesem Manager Tool ist es möglich, verschiedene Kartenprofile zu erzeugen, das Setzen und Ändern der Smartcard-PINs, das Entsperren einer Karte und das Ausrollen von biometrischen Credentials.
- **Usertool:** Diese spezielle Schnittstelle erlaubt nur Benutzerfunktionen: die Benutzer-PIN Ihrer Smartcard ändern und die Zertifikate Ihrer Smartcard registrieren.
- **Register Tool:** Dieses Tool registriert die Benutzerzertifikate von einer Smartcard nahtlos in den Windows-Zertifikatspeicher. Es kann auch verwendet werden, um das PKCS#11-Modul für die Browser-Integration zu registrieren.
- **CSP Module:** Das CSP (Cryptographic Service Provider) Modul ermöglicht ein Smartcard Login am Betriebssystem und an Windows Domänen und erweitert den Gebrauch von Token für andere Anwendungen.

- **GINA-Integration:** Dieses Modul ermöglicht die Smartcard-Anmeldung an Windows durch die Erweiterung der Windows Graphical Identification and Authentication (GINA) Bibliothek. Dieess ermöglicht sowohl Smartcard als auch biometrischen Login durch den CSP für 32-Bit Windows XP.
- **PKCS#11 Module:** Die PKCS#11-Modul Applikationen und Services für Anwendungen unterstützen über den PKCS#11 Cryptographic Token Interface Standard und die Verwendung der Cryptoki Anwendungsprogrammierschnittstelle. Beispiele für solche Programme sind Mozilla-basierte Anwendungen, wie Firefox oder Thunderbird, sowie Linux und Novell-Umgebungen. Das PKCS#11-Modul von cv act *sc/interface* unterstützt kryptographische Algorithmen, die auf RSA und auf elliptischen Kurven basieren (ECC). Nähere Erläuterungen finden sich in dem Kapitel „PKCS#11-Modul“.
- **Minidriver Module:** Mit diesem Interface können Smartcards über den Base Smart Card Cryptographic Service Provider (Base CSP) oder den Crypto Next Generation (CNG) Key Storage Provider (KSP) verwendet werden und stellt das Smartcard Management Interface zur Verfügung. Nähere Erläuterungen finden sich in dem Kapitel „Card Minidriver“. Für 32- und 64-bit Plattformen steht jeweils ein eigenes Modul zur Verfügung.
- **TokenD Module:** Dieses Plugin ermöglicht die Verwendung von Smartcards mit dem nativen kryptographische Token Handling in Mac OS Betriebssystem (Mac OS X 10.4 und höher). Nähere Erläuterungen finden Sie im Abschnitt „TokenD“.

Das Administrationstool und das Usertool befinden sich im Lieferumfang jeder Plattform. Die Module werden jedoch nur unter bestimmten Plattformen unterstützt, wie die folgende Tabelle zeigt:

	PKCS#11	Register Tool	CSP	Minidriver	GINA	TokenD
Win 32-Bit	✓	✓	✓	✓	nur für Windows XP	--
Win 64-Bit	✓	✓	✓	✓	--	--
Linux	✓	--	--	--	--	--
Mac OS X	✓	--	--	--	--	✓

5 Unterstützte Hardware

5.1 Security Token

Hier finden Sie eine Liste der Smartcards und Smartcard-Betriebssysteme, die erfolgreich mit diesem Release von cv act *sc/interface* getestet wurden. Diese Security Token werden als von cv act *sc/interface* unterstützt.

	cvProfile	PKCS#15	Biometric	Minidriver	TokenD
<i>AustriaCard ACOS EMV A04 / A05</i>	✓	✓		✓	
<i>AustriaCard JCOP 21 V2.2</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 21 V2.3.1</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31 V2.2</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31 V2.2 contactless</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31 V2.3.1</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31 V2.3.1 contactless</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31/72 V2.3.1</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 31/72 V2.3.1 contactless</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.2.1</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.2.1 contactless</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.3.1</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.3.1 contactless</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.4</i>	✓	✓		✓	✓
<i>AustriaCard JCOP 41 V2.4 contactless</i>	✓	✓		✓	✓
<i>E.ON Card V1</i>		✓		✓	✓
<i>E.ON Card V1 contactless</i>		✓		✓	✓

	cvProfile	PKCS#15	Biometric	Minidriver	TokenD
<i>ePasslet-Suite 1.1 on JCOP V2.4.1R3</i>	✓	✓	✓	✓	✓
<i>ePasslet-Suite 1.1 on JCOP V2.4.1R3 with PACE Profile</i>	✓	✓	✓	✓	✓
<i>ePasslet-Suite 1.2 on JCOP V2.4.1R3</i>	✓	✓	✓	✓	✓
<i>ePasslet-Suite 1.2 on JCOP V2.4.1R3 with PACE Profile</i>	✓	✓	✓	✓	✓
<i>ePasslet-Suite 2.0 on JCOP V2.4.2R3</i>	✓	✓	✓	✓	✓
<i>ePasslet-Suite 2.0 on JCOP V2.4.2R3 with PACE Profile</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 3.1</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 3.1 contactless</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 3.2</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 4.0</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 5.0</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 6.0</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 6.0 SCP 03</i>	✓	✓	✓	✓	✓
<i>G&D STARCOS 3.0</i>		✓		✓	✓
<i>G&D STARCOS 3.1</i>		✓		✓	✓
<i>G&D STARCOS 3.2</i>		✓		✓	✓
<i>G&D STARCOS 3.4 (Swiss Health Card eGK)</i>		✓		✓	✓
<i>Gemalto TOP IM GX4</i>	✓	✓		✓	✓
<i>HID Crescendo C700</i>	✓	✓		✓	✓
<i>HID Crescendo C700 contactless</i>	✓	✓		✓	✓
<i>Infineon JCLX80 jTOP</i>		✓	✓	✓	✓
<i>Infineon JCLX80 jTOP contactless</i>		✓	✓	✓	✓

	cvProfile	PKCS#15	Biometric	Minidriver	TokenD
<i>NXP JCOP V2.1</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.2</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.2 Contactless</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.3.1</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.2.1 IDptoken 200</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.4</i>	✓	✓	✓		✓
<i>NXP JCOP V2.4.1</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.4.2 R1</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.4.2 R2</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.4.2 R3</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.4.2 R3 SCP 03</i>	✓	✓	✓	✓	✓
<i>NXP JCOP V2.2 Certgate microSD</i>	✓	✓	✓	✓	✓
<i>Siemens CardOS M4.01a</i>	✓		✓	✓	
<i>Siemens CardOS V4.2</i>	✓	✓		✓	✓
<i>Siemens CardOS V4.2B</i>	✓	✓		✓	✓
<i>Siemens CardOS V4.2C</i>	✓	✓		✓	✓
<i>Siemens CardOS V4.3</i>	✓	✓		✓	✓
<i>Siemens CardOS V4.3B</i>	✓	✓		✓	✓
<i>Siemens CardOS V4.4</i>	✓	✓		✓	✓
<i>SwissSign SwissStick (CardOS M4.3B)</i>	✓	✓		✓	✓
<i>SwissSign suisseID (CardOS M4.3B)</i>	✓	✓		✓	✓
<i>SwissSign suisseID (CardOS M4.4)</i>	✓	✓		✓	✓

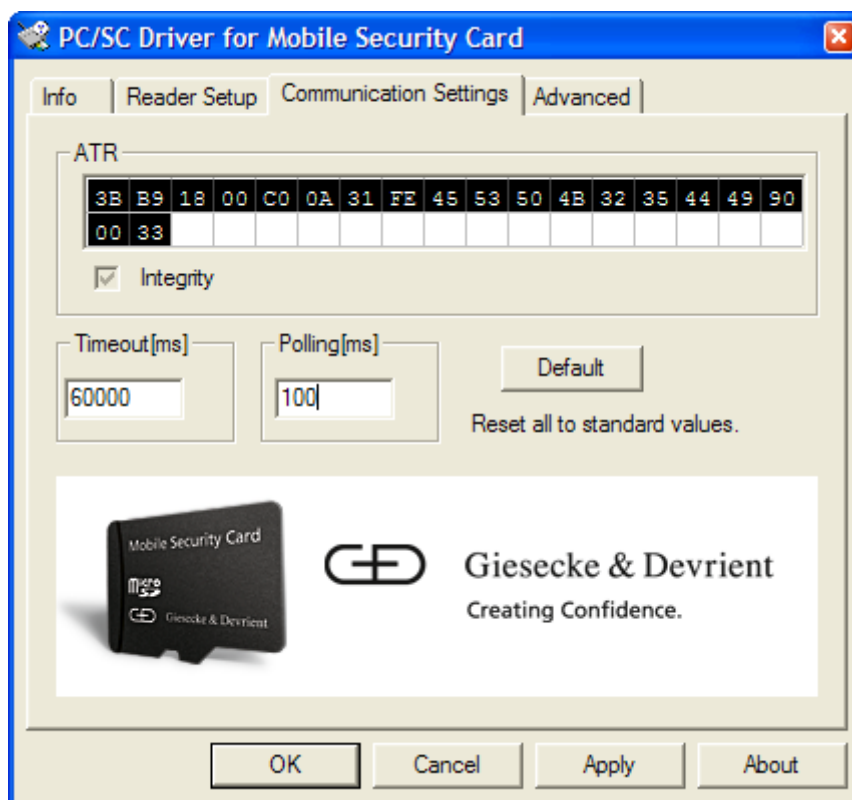
Hier finden Sie eine Liste von Smartcards und Smartcard-Betriebssysteme, die mit cv act *sc/interface* arbeiten sollten, aber in diesem Release nicht getestet wurden. Zusätzliche Hardware Tests können auf Kundenwunsch durchgeführt werden.

	cvProfile	PKCS#15	Biometric	Minidriver	TokenD
<i>AustriaCard ACOS EMV D01</i>	✓	✓			✓
<i>AustriaCard JACOS 2.4.1</i>	✓	✓	✓		✓
<i>G&D Mobile Security Card 3.x microSD™</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 3.2 StarSign Card Token 550 (USB)</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 64 cfg3</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 64 cfg8</i>	✓	✓	✓	✓	✓
<i>G&D Sm@rtCafé Expert 64 StarKey400 USB Token</i>	✓	✓	✓	✓	✓
<i>Gemalto GemXpresso Pro R3</i>	✓	✓		✓	✓
<i>Oberthur Cosmo V5.2D</i>		✓		✓	✓
<i>Siemens CardOS M4.01</i>	✓		Readonly		
<i>Siemens CardOS V4.2B contactless</i>	✓	✓		✓	✓

Hinweise:

- Ein Token oder eine Smartcard, die mit Fremd-Middleware konfiguriert wurde, kann eventuell auch mit cv act *sc/interface* verwendet werden. Für weitere Informationen bzgl. der Konfiguration der cryptovision Middleware kontaktieren Sie bitte Ihren Ansprechpartner bei cryptovision.
- Für alle JavaCards wird SCP 02 unterstützt. Für G&D Sm@rtCafé Expert 6.0 wird zusätzlich SCP 03 unterstützt.
- Bei Verwendung von G&D Sm@rtCafé Expert 3.1 und G&D Sm@rtCafé Expert 3.2 auf StarSign Card Token 550 (USB) werden die „Visa Fixed Keys“ und die Schlüsselableitung „CPG2.04“ unterstützt. Für die G&D Sm@rtCafé Expert64 werden nur die „Visa Fixed Keys“ unterstützt.
- Bei der Verwendung des Biometric-Profiles wird für CardOS M4.01a das Match-on-Card Package benötigt, für die G&D Smartcards das BiomatchJ 3.0 Applet. In letzterem Fall wird nur das PKCS#15-Profil mit Biometrie unterstützt.

- All Für alle o. g. Smartcards werden alle PINs und damit auch die Verwendung aller Schlüssel auf der Smartcard unterstützt. Nähere Erläuterungen finden sich in dem Kapitel „Einführung“ → „Virtuelle Slots“.
- Für G&D StarSign Version 1.0, Siemens HiPath ab Version 1.6.2.1 (und höher), A.E.T. SafeSign ab Version 2.3.0 (und höher) und Nexus Personal ab Version 4.6.1 (und höher) wird die Verwendung von CardOS M4.01a nicht unterstützt.
- Für Gemalto TOP IM GX4 und Infineon JTOP wird die Triple-DES Funktion auf der Smartcard nicht unterstützt.
- Für Starcos 3.0 werden nur 128Bit Triple-DES Schlüssel unterstützt.
- Wenn Sie die G&D Mobile Security Card nutzen wollen, stellen Sie bitte in der G&D Konfigurationssoftware „PC/SC Driver for Mobile Security Card“ unter „Communication Settings“ folgenden ATR ein:
3B B9 18 00 C0 0A 31 FE 45 53 50 4B 32 35 44 49 90 00 33



5.2 Kartenleser

cv act *sc/interface* benutzt die PC/SC-Schnittstelle des jeweiligen Betriebssystems für den Datenaustausch zwischen Smartcard, Reader und Betriebssystem. Entsprechend funktionieren alle PC/SC-2.0 konformen Karten-Lesegeräte mit den geeigneten Treibern. Unter Apple OS X und Linux Derivativen wird „pcsc-lite“ ab Version 1.1.2 (oder höher) verlangt.

In einigen Fällen sind die Anforderungen des PC/SC-Standards in den Treibern der Reader nicht vollständig implementiert. In der Folge können Auffälligkeiten bei bestimmten Kombinationen aus Smartcard, Treiber des Smartcard-Readers und Firmware des Smartcard-Readers auftreten. Diese Auffälligkeiten führen zu entsprechenden Hinweisen (z. B. send error). In diesem Fall wenden Sie sich bitte an den Hersteller des Smartcard-Readers, um ein Update des Treibers bzw. der Firmware zu erhalten.

Bei Verwendung von virtuellen Maschinen gibt es eine zusätzliche Hardware-Schicht. So können sich Abhängigkeiten ergeben und die Funktion der Reader nicht 100% gewährleistet werden.

Hier finden sie die Smartcard Reader, die erfolgreich mit diesem Release von cv act *sc/interface* getestet wurden. Diese Kartenleser werden von cv act *sc/interface* unterstützt:

- Omnikey Cardman 3121 USB
- Identive SCR3310v2.0

In den folgenden Unterkapiteln finden Sie Listen von Smartcard Readern, die mit cv act *sc/interface* arbeiten sollten, aber in diesem Release nicht getestet wurden. Zusätzliche spezielle Hardware kann auf Kundenwunsch getestet werden.

5.2.1 Kartenleser ohne Pinpad bzw. USB-Token

- ACS ACR100 SIMFlash (CCID)
- ACS ACR100 SIMFlash (HID)
- ACS ACR101 SIMicro (CCID)
- ACS ACR38 Smart Card Reader
- ACS ACR38DT DualKey
- ACS ACR38ET DualKey2
- ACS ACR38T Plug-in (SIM Sized) Card Reader
- Cherry SmartTerminal ST-1044U
- Cherry SmartTerminal ST-1210
- Gemalto GemPC Express
- Gemalto PC Twin Reader (USB/Serial)
- Omnikey Cardman 2020 USB
- Omnikey Cardman 3620 USB
- Omnikey 6121 USB
- Eutronsec SIMReader Combo
- Identive CLOUD 2700 F
- Identive CLOUD 4700 F
- Identive @MAXX® lite
- Identive @MAXX® NFC
- Identive @MAXX® prime
- Identive @MAXX® token SCT3511
- Identive SCT3522
- Identive SCR3311
- Identive SCR335
- Identive SCR241
- Identive SCR243
- Identive SCR331

- Identive SCR3310
- Identive SCR3320
- Identive SCR3321
- Identive SCR333
- Identive SCR3340
- Identive SCR335 USB
- Identive SPR532 serial/USB

5.2.2 Keyboard mit integrierten Kartenlesern

- ACS ACR38k Smart Keyboard
- Cherry FingerTIP ID Board G83-14400
- Cherry FingerTIP ID Board G83-14500
- Cherry FingerTIP ID Board G83-14600
- Cherry MultiBoard contactless G81-8072LUC
- Cherry SmartBoard G83-6610
- Cherry SmartBoard G83-6644
- Cherry SmartBoard Twin G83-6675

5.2.3 Kontaktlose Kartenleser

Bei der Verwendung von Smartcards mit kontaktloser Schnittstelle bzw. Dual-Interface Smartcards kann auch ein kontaktloser Kartenleser verwendet werden.

- ACS ACR120
- ACS ACR122L VisualVantage NFC
- ACS ACR122S NFC
- ACS ACR122T NFC
- ACS ACR122U NFC
- ACS ACR1281U nPA
- ACS ACR128U Dual-Interface
- Cherry SmartTerminal ST-1275
- Omnikey CardMan 5321 RFID
- Identive CLOUD 4700 F
- Identive SCL010
- Identive SCL3711
- Identive SDI010
- Identive SDI110
- REINER SCT cyberJack® RFID basis

5.2.4 Smartcard Reader mit Fingerprint-Sensors

Ein Smartcard Reader mit Fingerprint-Sensor benutzt den Fingerabdruck für die Authentifizierung anstatt der PIN:

- ACS AET52
- ACS AET63
- ACS AET65
- Omnikey 7121 Biometric
- Precise Biometrics 250 MC
- Precise Biometrics SENSE™ MC
- Precise Biometrics SENSE™ MC-S
- Precise Biometrics Tactivo™ for iPhone (mit unterstützter Konfiguration und spezieller Software - bitte kontaktieren Sie ihren Ansprechpartner bei cryptovision)
- Precise Biometrics Tactivo™ for iPad (mit unterstützter Konfiguration und spezieller Software - bitte kontaktieren Sie ihren Ansprechpartner bei cryptovision)

5.2.5 Kartenleser mit PINpad

cv act *sc/interface* unterstützt die Verwendung von Kartenlesern mit Pinpad und die Verwendung des Pinpad zur sicheren Eingabe der PIN. Es müssen folgende Voraussetzungen erfüllt sein:

- Es muss sich um einen PC/SC Reader handeln.
- Der Kartenleser muss FEATURE_VERIFY_PIN_DIRECT unterstützen.

Secure PIN entry wird mit einem Registry-Key konfiguriert:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]
"Enable_Secure_PIN_Entry"=dword:00000001
```

Wenn dieser Key den Wert „0“ hat, steht das Pinpad nicht zur Verfügung, bei „1“ kann das Pinpad verwendet werden. Die Konfiguration wirkt sich auf das CSP- und das PKCS#11-Modul aus, nicht jedoch auf das Administrationstool oder das Usertool. Fehlt der Key wird, der Standard-Wert „1“ verwendet. Wenn also ein Pinpad-Reader angeschlossen wird, kann dieser nun automatisch genutzt werden!

Bemerkungen:

- Bitte beachten Sie, dass es Problem geben, wenn man Outlook mit einem PinPad Reader benutzt. Die Anwendung kann einfrieren.
- Smartcard Logon erfordert immer eine PIN, so dass dafür kein PinPad Reader unterstützt wird.

Hier ist eine Liste von Kartenlesern mit PinPad:

- ACS ACR83 PINeasy Smart Card Reader
- ACS ACR88 PIN-Pad Reader
- ACS ACR880 GPRS Portable Smart Card Terminal
- Cherry SmartTerminal ST-2000U
- Omnikey 3821

- REINER SCT cyberJack® RFID comfort
- REINER SCT cyberJack® RFID standard
- REINER SCT cyberJack® e-com plus
- REINER SCT cyberJack® secoder
- Gemalto PC Pinpad Reader
- KAAN TriB@nk

Anmerkungen (Known Issues):

- KAAN TriB@nk wird nicht unterstützt in Kombination mit den Smartcards G&D Smartcafe Expert 64 und Gemalto TOP IM GX4.
- Der Gemalto PC Pinpad-Reader unterstützt eine maximale PIN-Länge von 8 Stellen, d.h. längere PINs können nicht eingegeben werden. Es gibt unter Windows (zum jetzigen Zeitpunkt) keine Möglichkeit diese maximale PIN-Länge abzufragen. Unter Linux funktioniert dies ab der CCID-Version 1.3.12 release 8 May 2010. Eine umfassende Erklärung zu diesem Thema finden Sie auch unter: <http://ludovicrousseau.blogspot.com/2010/05/how-to-know-pin-sizes-supported-by.html>

5.2.6 ExpressCard & PCMCIA Reader

- ACS ACR92
- Cherry SmartReader SR-4044
- Cherry SmartReader SR-5044
- Omnikey 4040 PCMCIA
- Omnikey 4321 ExpressCard 54
- Identive SCR243
- Identive SCR3340

5.2.7 Mobile Reader

- Identive @MAXX ID-1
- Identive SCR3500
- Identive SCL3711
- Precise Biometrics Tactivo™ for iPhone (with supported card configurations)
- Precise Biometrics Tactivo™ for iPad (with supported card configurations)

5.3 Citrix Terminal Server

cv act *sc/interface* wurde in der folgenden Konfiguration mit den entsprechenden Komponenten getestet:

5.3.1 Getestete Konfiguration von XenDesktop 5

- Windows 2008 R2 Server
- XenDesktop 5 auf Windows 7 64bit (via VMWare)

- CSP-Modul von cv act *sc/interface* (cvCSP) – **Wichtig:** der cvCSP muss als erstes auf dem Client und auf dem Server installiert werden, bevor die Citrix Komponenten installiert werden. Dafür starten Sie bitte die Installation von cv act *sc/interface*. Mehr Informationen zu den Anforderungen von Citrix lesen Sie unter <http://support.citrix.com/proddocs/topic/xendesktop-71/cds-smart-cards-sys-reqs.html>
- Reader: Idemetric SCR 3310
- JCOP2.4.1 und CardOS 4.3
- Anwendungen:
 - Smartcard logon an XenApp 5 via WebInterface (Internet Explorer 10 und Firefox 24.0)
 - Smartcard logon an Windows 7 und Windows XP
 - Zertifikats-Enrollment (Internet Explorer 10 und Firefox 24.0)
 - SSL (Internet Explorer 10 und Firefox 24.0)
 - PDF Signatur mit Adobe 11

5.3.2 Getestete Konfiguration von XenApp 6.5

- Windows 2008 R2 Server
- XenApp 6.5 auf Windows 7 FatClient(VM)
- CSP-Modul von cv act *sc/interface* (cvCSP) – **Wichtig:** der cvCSP muss als erstes auf dem Client und auf dem Server installiert werden, bevor die Citrix Komponenten installiert werden. Dafür starten Sie bitte die Installation von cv act *sc/interface*. Mehr Informationen zu den Anforderungen von Citrix lesen Sie unter <http://support.citrix.com/proddocs/topic/xendesktop-71/cds-smart-cards-sys-reqs.html>
- Reader: Idemetric SCR3310v2
- JCOP2.4.1 und CardOS 4.3
- Anwendungen:
 - Smartcard logon an XenApp 6.5 via WebInterface (Internet Explorer 10 und Firefox 24.0)
 - Zertifikats-Enrollment (Internet Explorer 10 und Firefox 24.0)
 - SSL (Internet Explorer 10 und Firefox 24.0)
 - PDF-Signatur mit Adobe 9

Bemerkung: Die Treiber der USB Token müssen HotPlugEnable sein (Citrix requirement).

5.3.3 Getestete Version von CitrixReceiver

- CitrixReceiver: 4.1.0.56 (Fileversion: 14.1.0)

6 Installation von cv act *sc/interface*

cv act *sc/interface* wurde entwickelt, um auf allen gängigen Desktop-Betriebssystemen eingesetzt zu werden. So hängt die Installation von der Plattform ab. In den folgenden Abschnitten werden die Installationsverfahren für die verschiedenen Betriebssysteme in weiteren Einzelheiten beschrieben.

6.1 Installation auf Windows

Die Funktionalität von cv act *sc/interface* richtet sich an zwei Haupt-Zielgruppen: sowohl an Administratoren von Sicherheits-Token, die volle Token Lifecycle Management Funktionen ausführen wollen, wie die initiale Konfiguration der Token für den ersten Einsatz, Schlüssel- und Zertifikatsmanagement als auch an die Endnutzer der Token. Aufgrund dieser Rollen sind das Manager- und das Benutzer-Modul aufgeteilt in unterschiedliche Anwendungen und verwenden unterschiedliche Software Setup-Dateien. Diese Setup-Dateien sind weiter aufgeteilt in bestimmte Versionen für 32-Bit und 64-Bit-Chip-Architekturen. Das cv act *sc/interface* Installationsmedium wird als komprimierte Archiv-Datei komplett mit Unterordnern geliefert. Unter Windows sind die relevanten Unterordner wie folgt:

- installation_admin
- installation_admin_x64
- installation_user
- installation_user_x64
- minidriver
- support
- windows

Die Setup-Dateien sind in den Foldern installation_admin oder installation_user für die entsprechenden Chiparchitekturen. Die andern Subfolder enthalten Dateien und Ressourcen, die für die fortgeschrittene Installation notwendig sind oder für ausführliche Protokollierungsversionen, nützlich für Anwendungsprogrammierer und diagnostische Fehlersuche.

6.1.1 Unterstützte Windows Versionen

Hier finden Sie eine Liste der Microsoft-Betriebssysteme, die erfolgreich mit diesem Release von cv act *sc/interface* getestet wurden. Diese Microsoft-Betriebssysteme werden von cv act *sc/interface* unterstützt.

- Windows XP mit Service Pack 3
- Windows 7 mit Service Pack 1
- Windows Server 2008 R2 mit Service Pack 1
- Windows 8.0 (nur Minidriver)
- Windows 8.1 (nur Minidriver)

Hier finden Sie eine Liste von Microsoft-Betriebssysteme, die mit cv act *sc/interface* arbeiten sollten, aber in diesem Release nicht getestet wurden. Zusätzliche Tests können auf Kundenwunsch durchgeführt werden:

- Windows Server 2003 with Service Pack 3
- Windows Vista with Service Pack 2

- Windows Server 2008 mit Service Pack 2
- Windows 8.0 (CSP)
- Windows 8.1 (CSP)
- Windows Server 2012

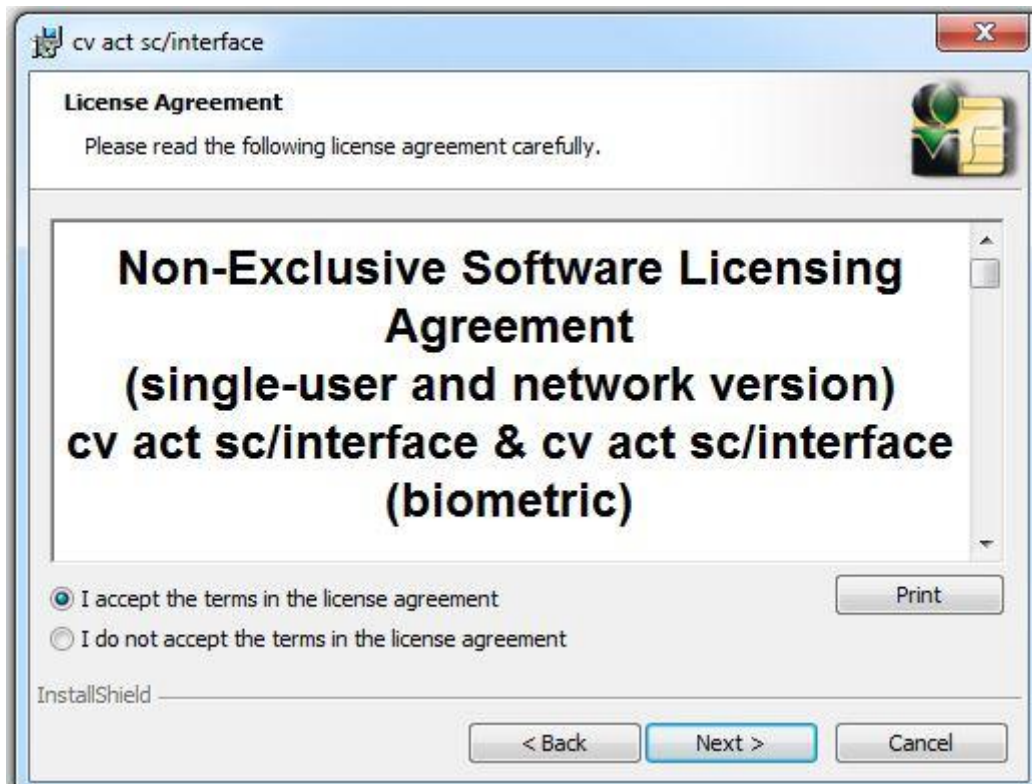
6.1.2 Ausführen des Windows Administrator Setup

Bitte führen Sie mit Administrator-Rechten die Datei SETUP.EXE aus und folgen Sie den Installationsanweisungen des Setup Wizards. Die folgenden Screenshots veranschaulichen diesen Prozess.

Bitte beachten Sie: Die Installation von cv act *sc/interface* erfordert Administrator-Rechte. Falls Sie als regulärer Benutzer bei der Installation möglicherweise nach weiteren Credentials gefragt werden. Für nähere Informationen halten Sie sich bitte an die Dokumentation des Betriebssystems oder wenden Sie sich an Ihren Systemadministrator



Klicken Sie auf Next oder Enter, um den Installationsprozess zu starten.



Wenn Sie fortfahren, akzeptieren Sie das license agreement.



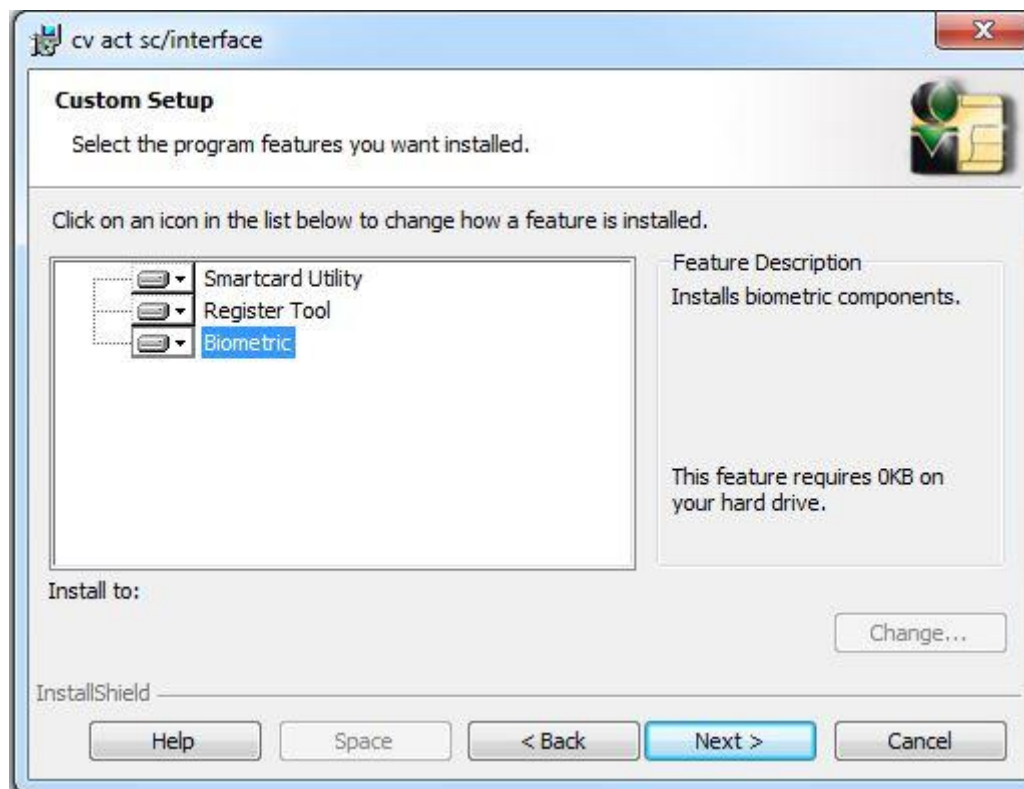
Für Anwendungen, die erweiterte Funktionalität für den Cryptographic Service Provider benötigen, wie die Verwendung der Klasse 2 oder 3 sicheren PIN-Pad Kartenleser oder erweitertes PIN-Caching, wird der cryptovision Cryptographic Service Provider empfohlen. Für Legacy-Unterstützung von Standard-Installationen von Windows XP, Windows 2000 oder Windows Server 2003 ist es erforderlich, dass Sie den cryptovision Cryptographic Service Provider nutzen.

Wenn Sie die Minidriver auf Windows XP, Windows 2000 oder Windows Server 2003 installieren möchten, müssen Sie zuerst die Microsoft Base Smart Card Cryptographic Service Provider Paket x86 (KB909520) installieren. Sie finden die relevanten Updates für Chip-Architekturen als Download unter: <http://www.microsoft.com/en-us/download/search.aspx?q=KB909520>

Wenn Sie cv act *sc/interface* mit mehr als einer Art von Sicherheits-Token benutzen wollen oder eine automatische Verteilung der Benutzer-Modul planen, dann ist es empfehlenswert, dass Sie die Smartcard Mindriver Option auswählen, da so die relevanten Minidriver-Dateien für alle unterstützten Token installiert werden. Obwohl diese Option mehr Speicherplatz auf dem Client benötigt, sorgt sie für die maximale Kompatibilität für Systeme, die mehrere Arten von Token unterstützen. Für diese Systeme, bei denen die Verteilung der Minidriver automatisiert ist, wird empfohlen, dass der Windows "Smart Card Plug and Play" Dienst deaktiviert ist, um Windows von dem Versuch abzuhalten, einen Treiber zu reinstallieren, wenn Sie wieder eine Smartcard einlegen. Dieser Dienst kann über Gruppenrichtlinien deaktiviert werden, in Windows 2008 Server mit dem folgenden Beispiel:

Administrative Templates | Windows Components | Smart Card "Plug & Play smart card enabled services

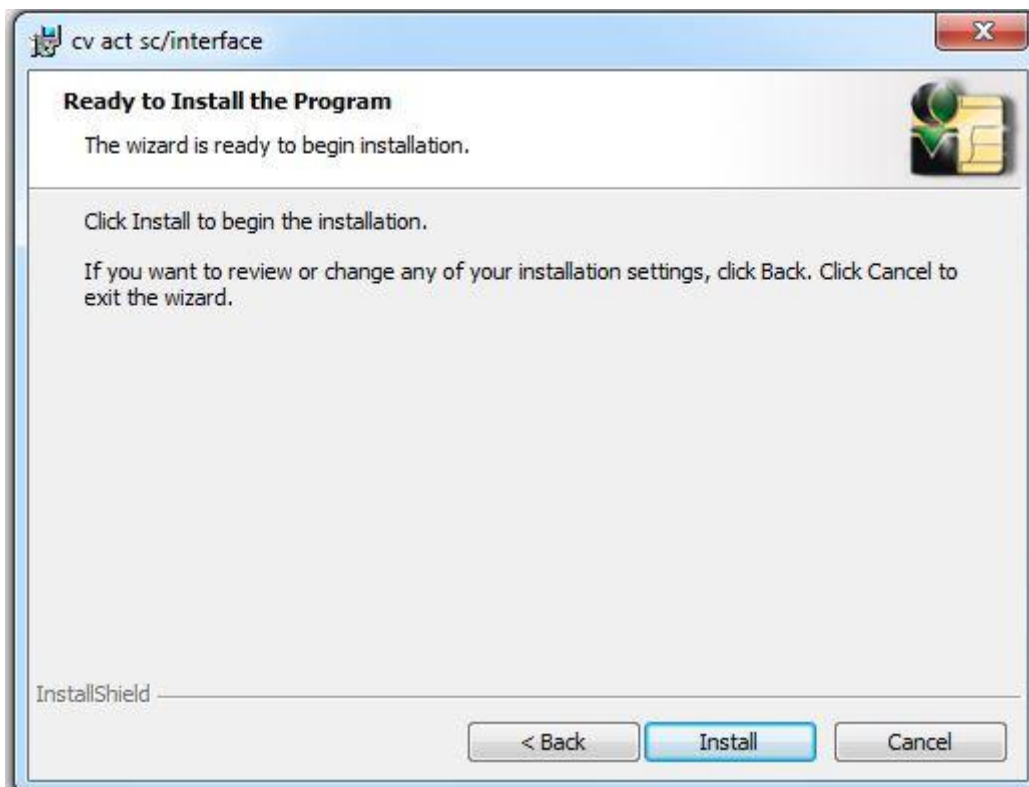
Für eine minimale Installation, wo nur die Token-spezifischen Dateien installiert werden, kann das Smart Card Minidriver - Device Driver Setup ausgewählt werden. Da jedoch diese Methode das automatische Downloaden von Token-spezifischen Dateien erfordert, bedarf es Online-Zugriff auf Windows Update.



Wenn Sie eine Lizenz erworben haben, die das Precise Match-on-Card™ Paket beinhaltet, können Sie wahlweise diese Dateien auswählen.



Zusätzlich zu der Middleware-Lizenzvereinbarung, müssen Sie die die zusätzlichen Lizenzbestimmungen der zusätzlichen biometrischen Komponenten akzeptieren.



Klicken Sie auf Install, um die Setup Wizard Konfiguration zu beenden und beginnen Sie den aktuellen Installationsprozess.



Sobald der Setup-Assistent beendet ist, klicken Sie auf Finish, um den Installationsassistenten zu schließen.

6.1.3 Ausführen des Windows User Setup

Bitte führen Sie als Benutzer mit Administrator-Rechten die Datei SETUP.EXE aus und folgen Sie den Installationsanweisungen des Setup Wizards. Da die Setup-Wizard Dateien auf dem gleichen Installationsprozess wie des Administrator Setups im vorhergehenden Kapitel basieren, nur mit einem kleinen Unterschied der Installation der Smartcard Utility anstelle des Manager Tool, haben wir die Screenshots für diesen Prozess weggelassen.

Bitte beachten Sie: Die Installation von cv act *sc/interface* erfordert Administrator-Rechte. Falls Sie als regulärer Benutzer bei der Installation möglicherweise nach weiteren Credentials gefragt werden. Für nähere Informationen halten Sie sich bitte an die Dokumentation des Betriebssystems oder wenden Sie sich an Ihren Systemadministrator

6.2 Installation auf Linux

Anders als die Windows Prozedur, basiert die Linux Installation nicht auf administrativen Rollen, sondern auf Zieldistribution und Chiparchitektur. In dem cv act *sc/interface* Installationsmedien ist ein Linux Unterverzeichnis, das die verschiedenen Installationsdateien für die unterschiedlichen Linux Derivate enthält.

6.2.1 Unterstützte Linux Versionen

Die aktuellen cv act *sc/interface* Installationsmedien enthalten ein .deb basierte Installationsdatei. Zusätzlich kann eine .rpm basierte Installationsdatei bei Bedarf produziert werden.

Hier finden Sie die Linux Distribution basierend auf Linux (Kernel 2.6, 3.2), die erfolgreich mit diesem Release von cv act *sc/interface* getestet wurden. Dieses wird als von cv act *sc/interface* unterstützt.

- Ubuntu 12.04.3 LTS (32/64 bit)

Hier finden Sie eine Liste von Distributionen, basierend auf Linux (Kernel 2.6, 3.2), die mit cv act *sc/interface* arbeiten sollten, aber in diesem Release nicht getestet wurden. Zusätzliche Tests können auf Kundenwunsch durchgeführt werden:

- Ubuntu 10, 11, 12 LTE
- SLES 11 (OpenSuse 11.2) (64 bit)
- Fedora 15-19
- Debian 6, 7
- Red Hat Enterprise Linux 6

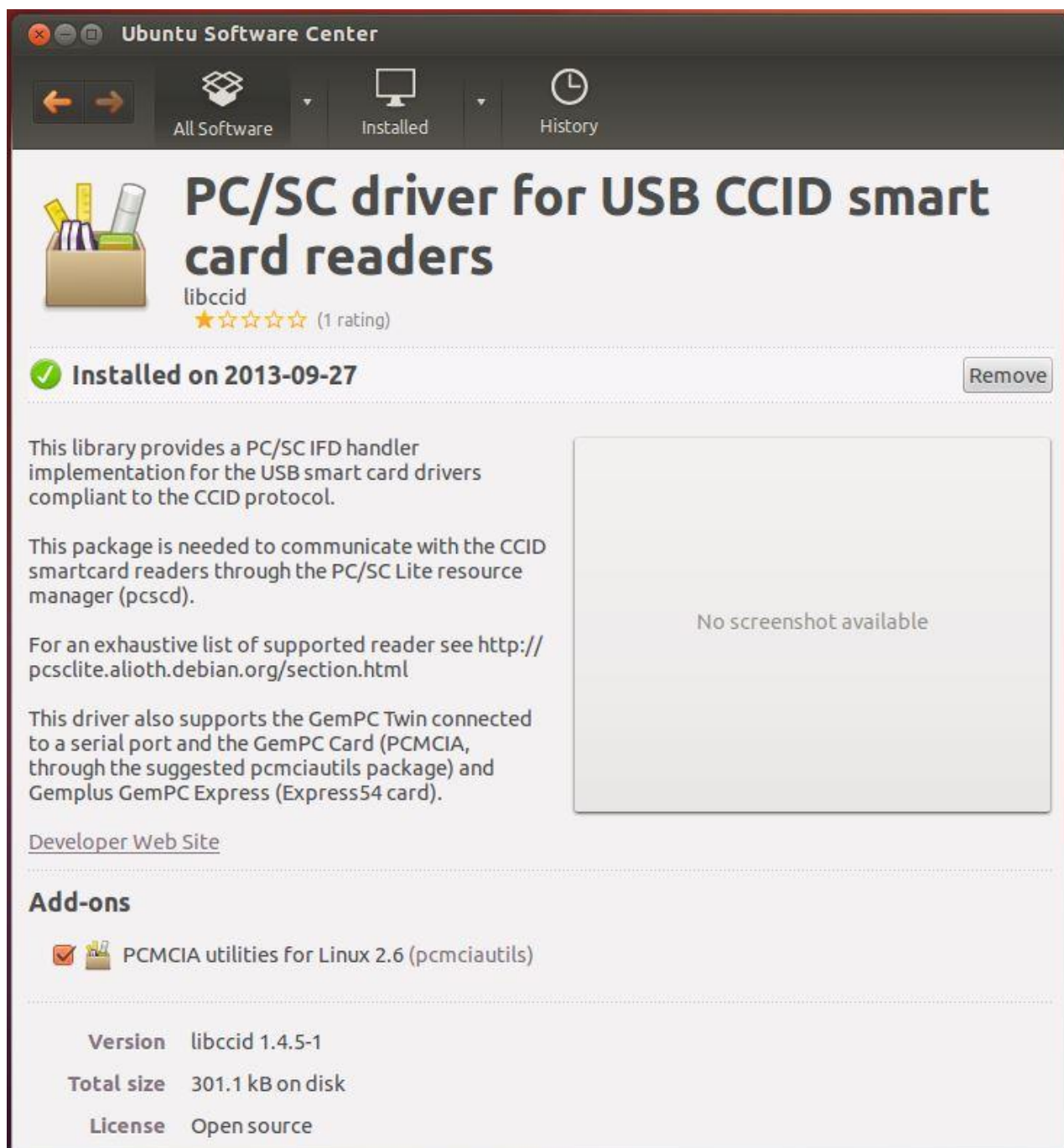
6.2.2 Beispiel Linux Distribution Installation: Ubuntu Setup

Kopieren Sie zunächst die benötigten Installationsdateien vom Installationsmedium auf die Ziel-Workstation. Rufen Sie hierzu das Linux-Unterverzeichnis des Installationsmediums auf, das die unterschiedlichen Installations-Dateien für die verschiedenen Linux-Derivate abhängig von der Zielverteilung und der Chip-Architektur enthält. Im folgenden Beispiel führen wir eine Installation von cv act *sc/interface* Utility und des cv act *sc/interface* Manager auf Ubuntu Linux (Release 12.4 LTS) durch.

Für die Installation von cv act *sc/interface* muss ein PC/SC-Dämon vorhanden sein. Suchen Sie hierzu im Ubuntu Software Center das pcscd-Paket und installieren Sie dieses. Der PC/SC-Daemon ist notwendig, damit Lesertreiber zur Laufzeit zugeordnet werden können. Nur so ist eine Verbindung zum Leser möglich.

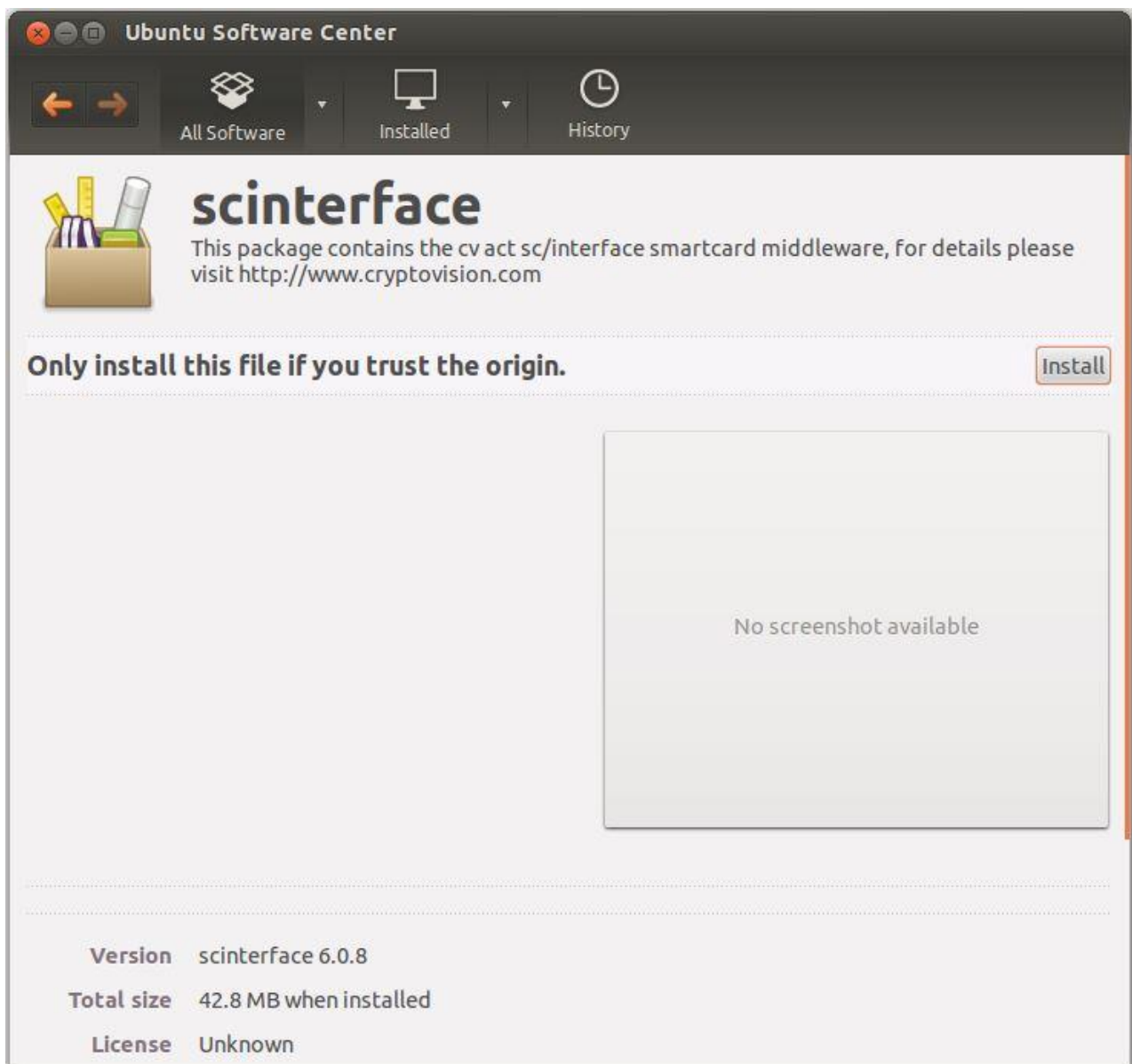


Zusätzlich zu PC/SC müssen auch die USB-Smartcard-Treiber installiert werden, die das CCID-Protokoll unterstützen (libccid-Paket). Dieses Paket kann auch vom Ubuntu Software Center aus installiert werden.

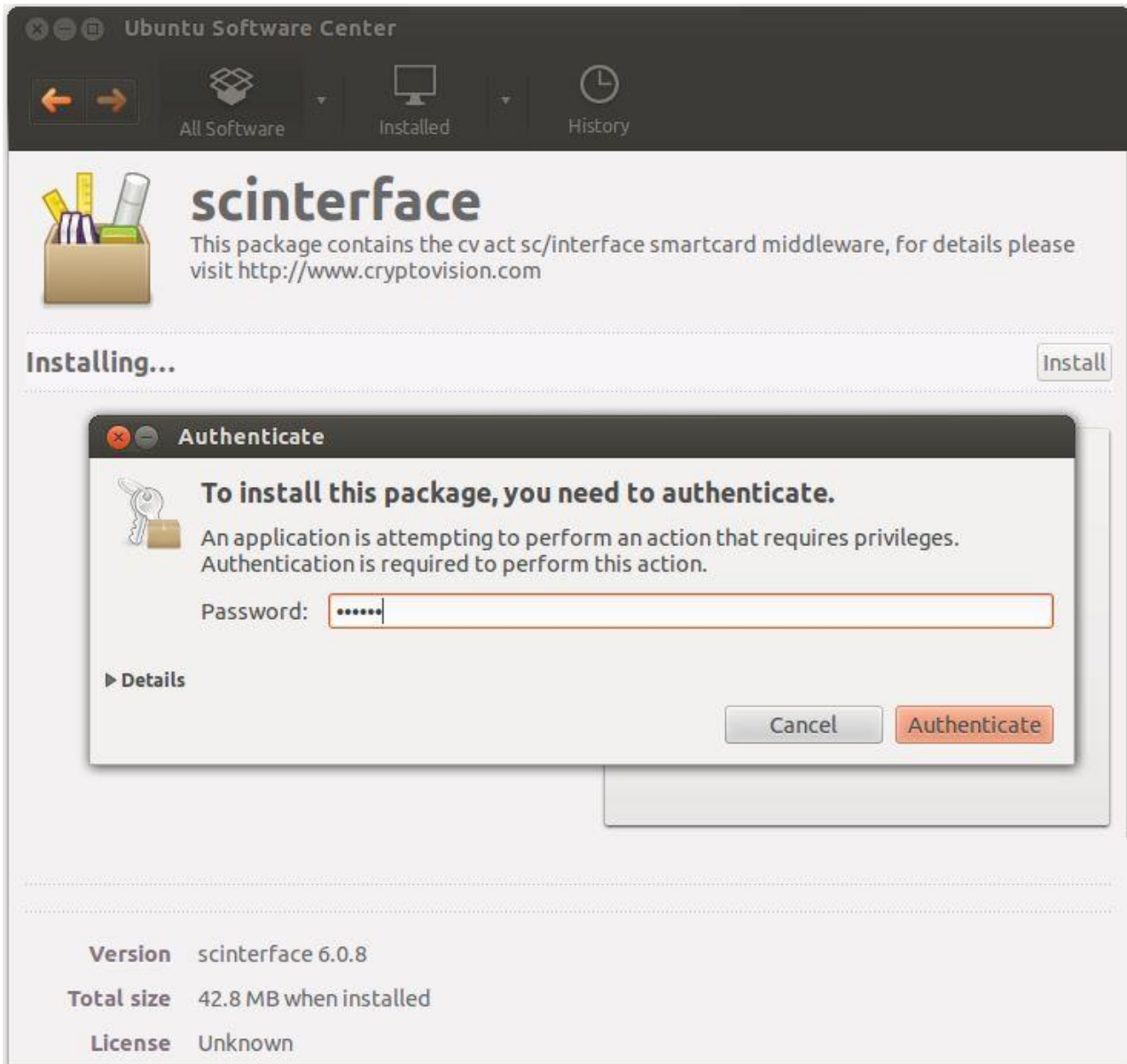


Wird der Smartcard-Leser, den Sie nutzen wollen, nicht unterstützt (siehe <http://pcsc-lite.alioth.debian.org/ccid/section.html> für eine Übersicht), müssen Sie einen proprietären Treiber für Ihren speziellen Leser installieren. Wenden Sie sich dazu an den Hersteller.

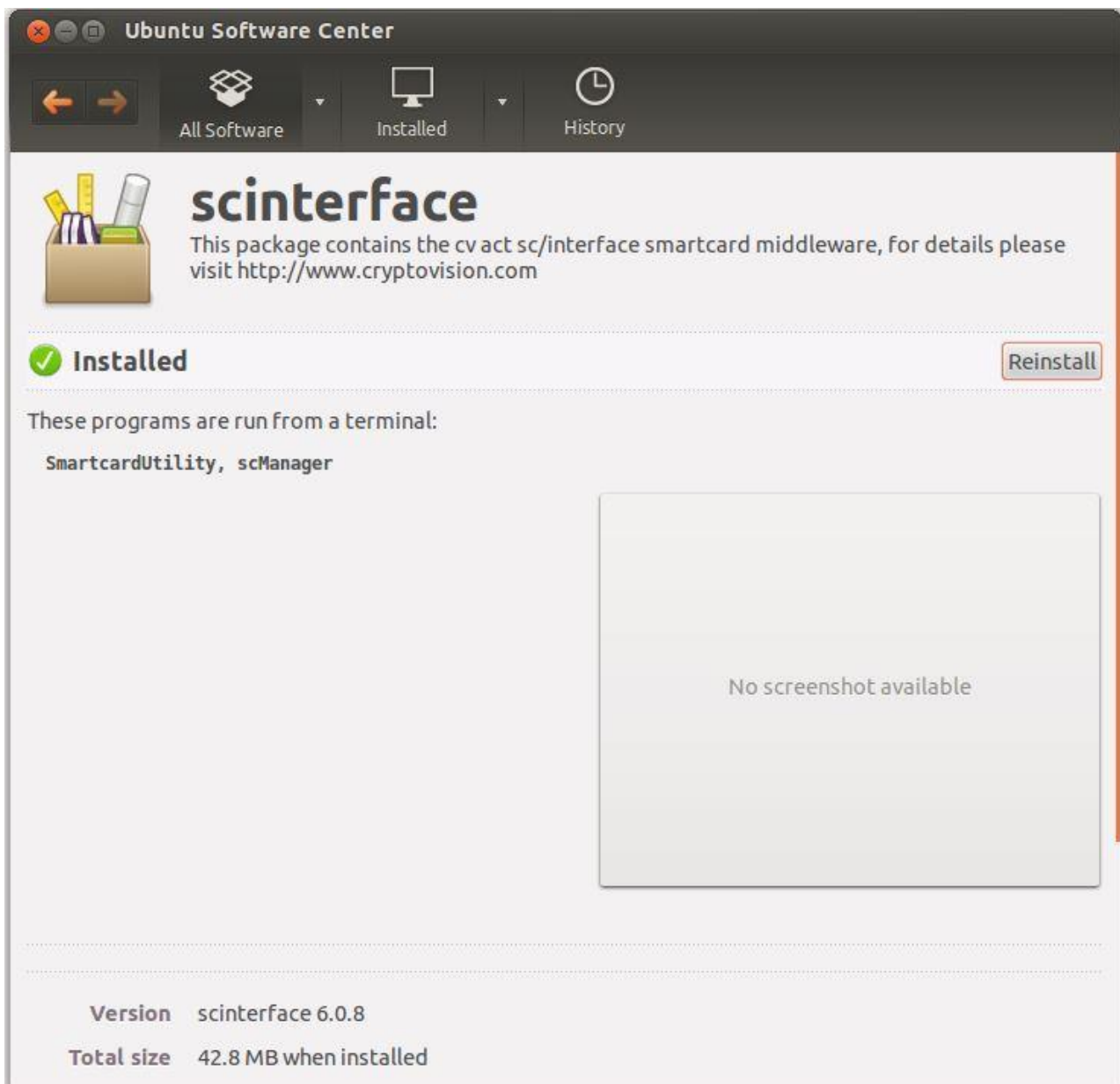
Sind die genannten Vorbedingungen erfüllt und die entsprechenden Treiber installiert, kann die Installation von cv act *sc/interface* beginnen. Kopieren Sie hierzu die benötigten Installationsdateien vom Linux-Unterverzeichnis des Installationsmediums auf die Workstation. Im Beispiel wird (auf einer Intel-basierten Ubuntu-Maschine) die Datei `scInterface-6.0.x.x-Ubuntu12-i686.deb` verwendet. Machen Sie einen Rechtsklick auf diese Datei und wählen Sie "Open with Ubuntu Software Center" aus, um die Installation zu starten.



Sie werden zur Authentifizierung aufgefordert. Ihr Account muss die zur Installation der Software notwendigen Rechte besitzen. Geben Sie Ihr Passwort ein und klicken Sie "Authenticate".



Wenn die Installation abgeschlossen ist, erhalten Sie eine Bestätigung, dass die Benutzeroberflächen des scManager und der SmartcardUtility nun von der Terminal-Konsole aus nutzbar sind.



6.3 Installation auf OS X

Ähnlich wie bei Linux ist auch bei der OS-X-Installation nicht die administrative Rolle, sondern die Betriebssystem-Version des Zielrechners entscheidend. Auf dem Installationsmedium gibt es ein Unterverzeichnis namens "macosx", das verschiedene Installationsdateien für die verschiedenen Mac-OS-X-Versionen enthält.

6.3.1 Supported OS X Versions

Hier finden Sie OS X Versionen, die erfolgreich mit diesem Release von cv act *sc/interface* getestet wurden. Diese werden von cv act *sc/interface* unterstützt:

- 10.7.x Lion (Intel 64 Bit)
- 10.8.x Mountain Lion (Intel 64 Bit)
- 10.9.x OS X Mavericks (Intel 64 Bit)

Hier finden Sie eine Liste der OS X Versionen, die mit cv act *sc/interface* arbeiten sollten, aber in diesem Release nicht getestet wurden. Zusätzliche Tests können auf Kundenwunsch durchgeführt werden:

- 10.5.x Leopard (Intel 32Bit)
- 10.6.x Snow Leopard (Intel 32/64Bit)

Bitte beachten Sie, dass seit dem Release 10.7 enthält das Mac OS in der Standard-Installation keine SmartCard-Services-Komponenten mehr. Wer dennoch Smartcards nutzen will, muss daher zusätzliche Komponenten installieren. Diese sind über folgenden Link erhältlich:

<http://smartcardservices.macosforge.org/trac/wiki/installers>

Bitte beachten Sie, dass TokenD von Apple nicht mehr unterstützt wird.

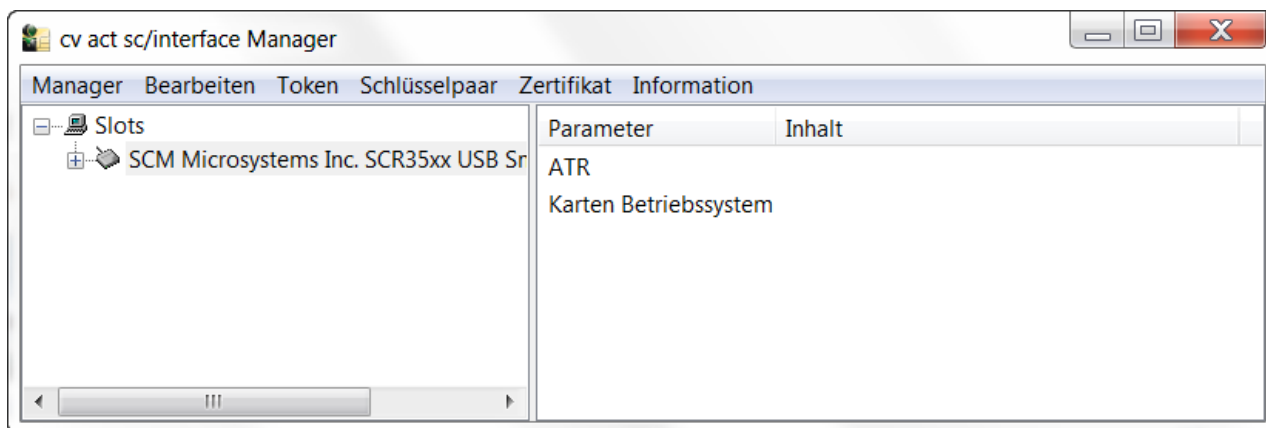
7 Das Administrationstool

Wenn Sie cv act *sc/interface* in der Admin Edition installiert haben, stehen Ihnen mit dieser Verwaltungsoberfläche die für einen Administrator relevanten Funktionen wie das Ändern von PINs, Entsperren von Smartcards, Anlegen von Profilen inklusive Erzeugen oder Importieren und Exportieren von Zertifikaten zur Verfügung.

In diesem Kapitel wird zunächst die Benutzeroberfläche, also die Bedienung jeder Registerkarte erklärt. Danach werden die Anwendungen, die Sie mit dem Administrationstool vornehmen können, näher beschrieben.

7.1 Benutzeroberfläche von cv act *sc/interface* Manager

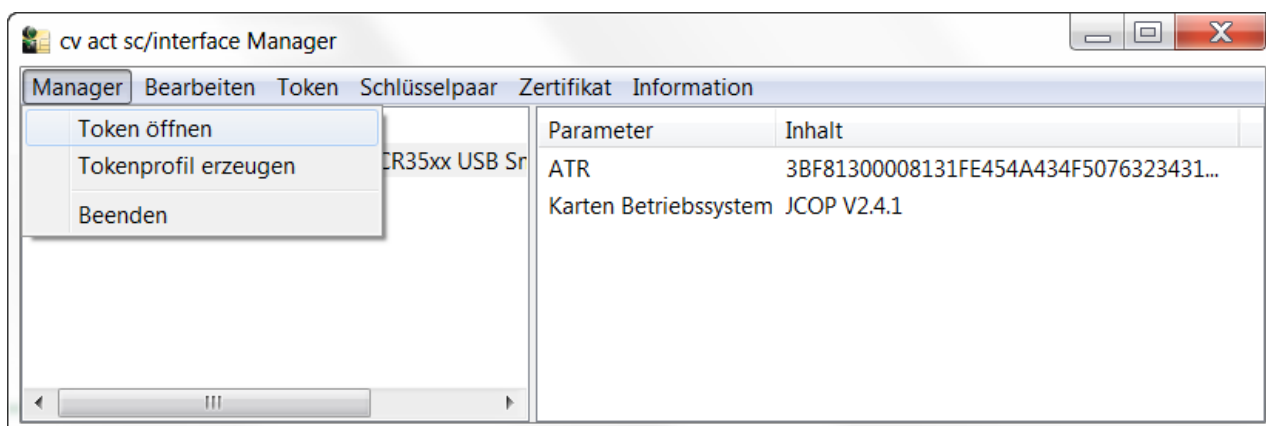
Nach dem Öffnen des Administrationstools von cv act *sc/interface* sehen Sie folgende Oberfläche:



Hinweis: Das Administrationstool unterstützt die Verwendung von Strg+C zum Kopieren. Auf diese Weise lässt sich z. B. der ATR oder das Token Label aus dem rechten Fenster kopieren.

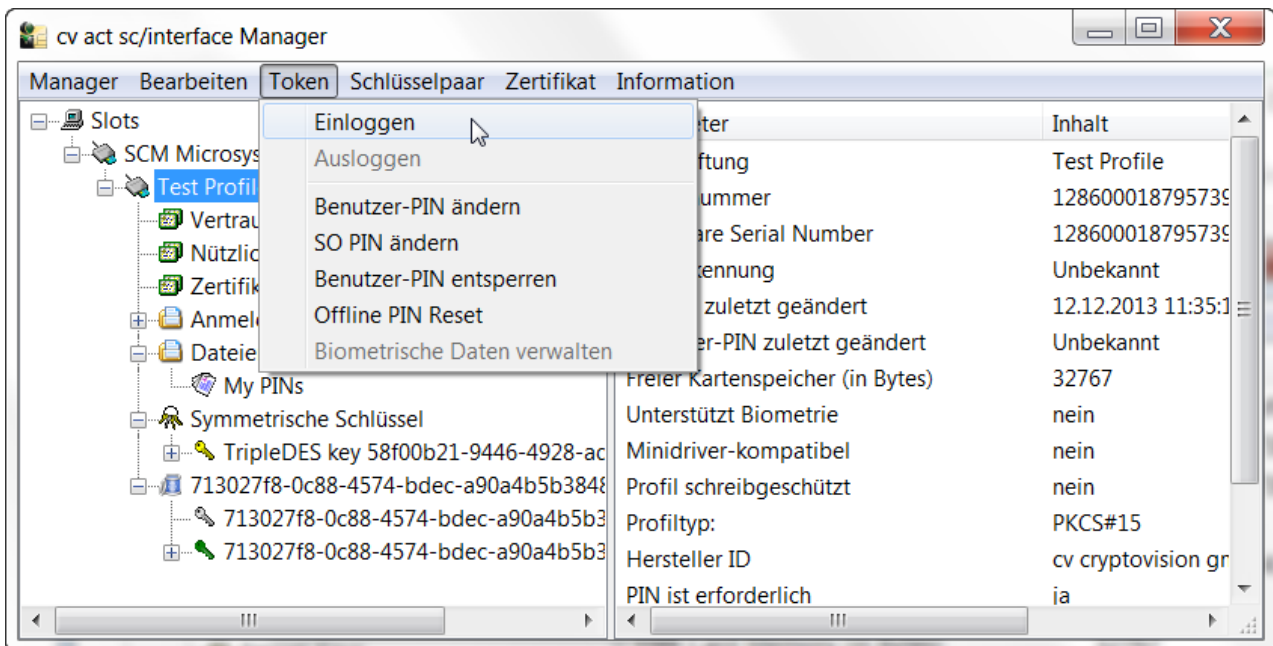
Hinweis: Sie können im laufenden Betrieb Kartenleser anschließen und entfernen. Das Administrationstool erkennt dies automatisch.

Nachdem Sie die Smartcard in den Reader eingelegt haben, können Sie nach einem Klick auf den Smartcard Reader mit der rechten Maustaste die Funktion „Token öffnen“ anwählen. Alternativ haben sie auch die Möglichkeit diese Funktion unter dem Menüpunkt „Manager“ auszuwählen:

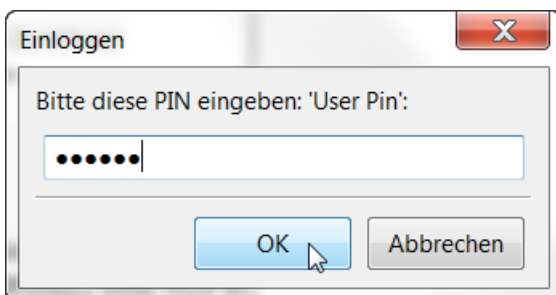


Es werden zunächst die vorhandenen öffentlichen Informationen, wie Name der Smartcard, Name des Profils und freier Speicherplatz angezeigt. Des Weiteren sehen Sie Zertifikate, öffentliche Schlüssel, Container und Daten. In diesem Fall handelt es sich um eine Smartcard, die zwei Anwendungen enthält, demgemäß sind zwei virtuelle Slots dargestellt.

Um sich die sensiblen Daten der Smartcard anzeigen zu lassen, müssen Sie sich auf die Karte einloggen. Dazu wählen Sie im Menü „Token“ den Punkt „Einloggen“:

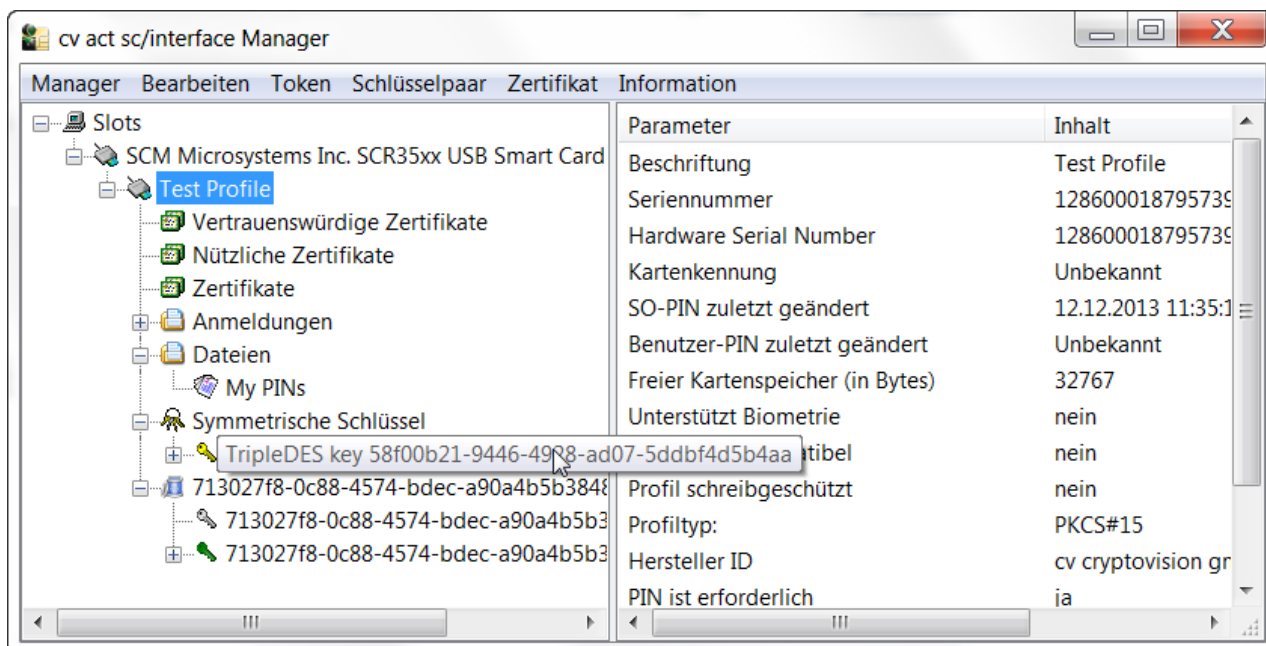


Geben Sie Ihre Benutzer-PIN ein:



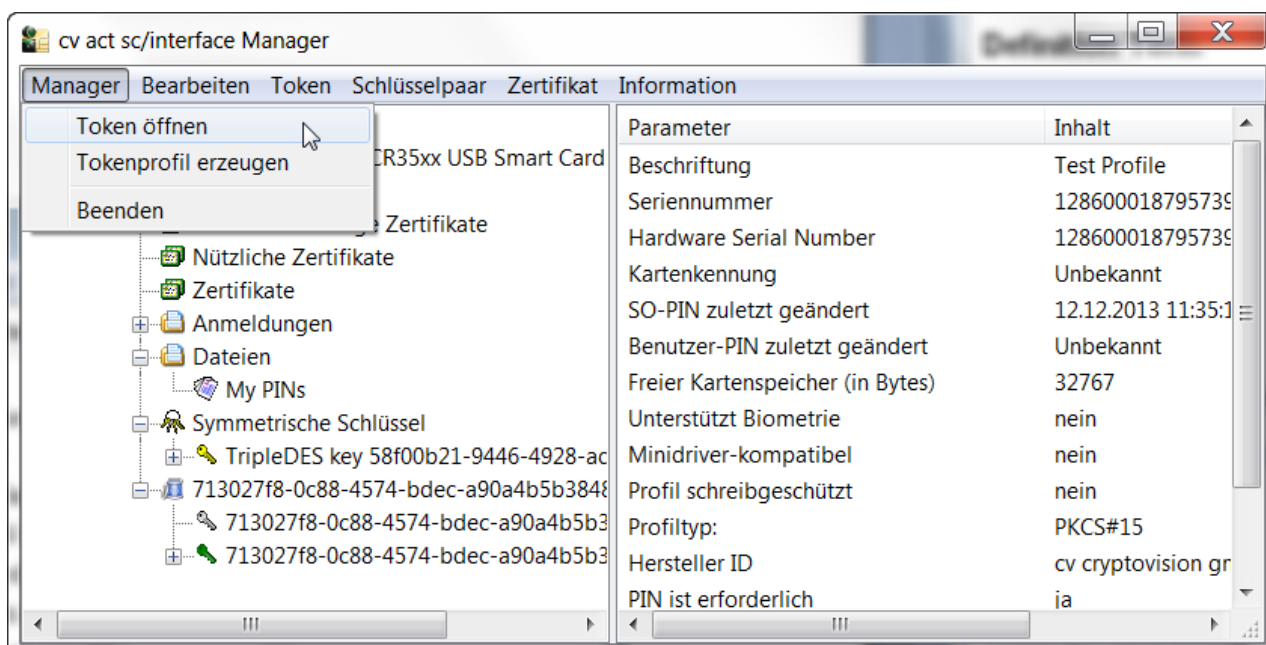
An dieser Stelle gibt Ihnen cv act *sc/interface* die Möglichkeit, Ihre Zertifikate im Windows Zertifikatsspeicher zu registrieren. Dadurch können Sie sich später das Importieren von Zertifikaten in das Betriebssystem ersparen. Die Registrierung erfolgt über einen Dialog, der für jedes Zertifikat abfragt, ob die Zertifikatsregistrierung erwünscht ist.

Nachdem Login erscheinen in der Oberfläche weitere Daten, darunter private und geheime Schlüssel (Private Keys und Secret Keys):



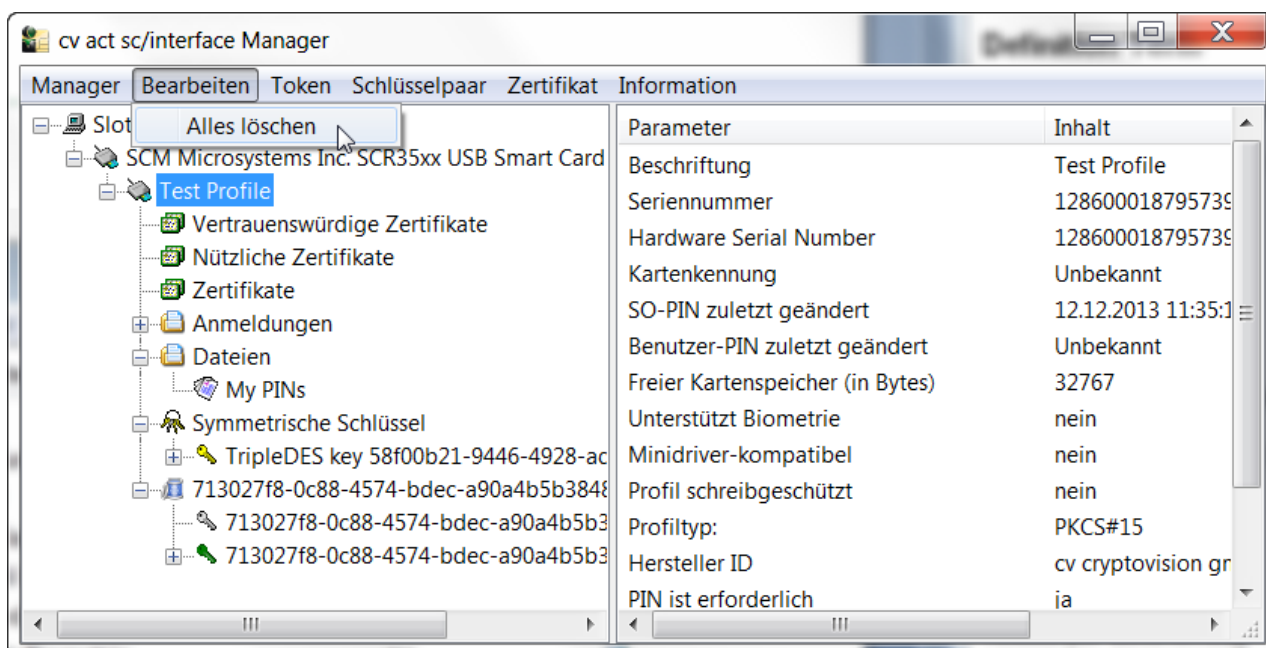
Sie können mehrere Schlüssel mit zugehörigen Zertifikaten auf der Karte anlegen. Diese werden dann jeweils in Containern zusammengefasst. Die Funktionen, die Ihnen zur Verfügung stehen, werden in den folgenden Abschnitten näher beschrieben.

7.1.1 Registerkarte "Manager"



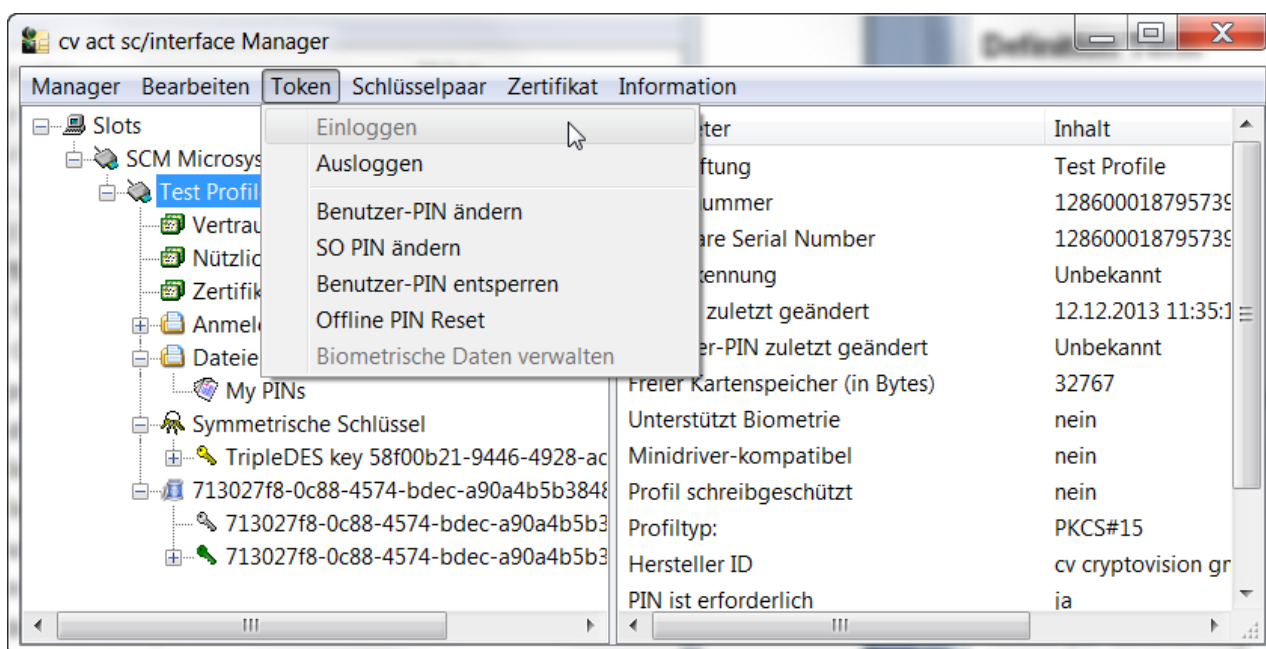
Über diese Registerkarte können Sie auf allgemeine Funktionen zugreifen, die die Arbeit mit cv act *sc/interface* Manager betreffen.

7.1.2 Registerkarte „Bearbeiten“



Über diese Registerkarte können Sie die spezifischen Funktionen aufrufen, die die Smartcard zur Verfügung stellt.

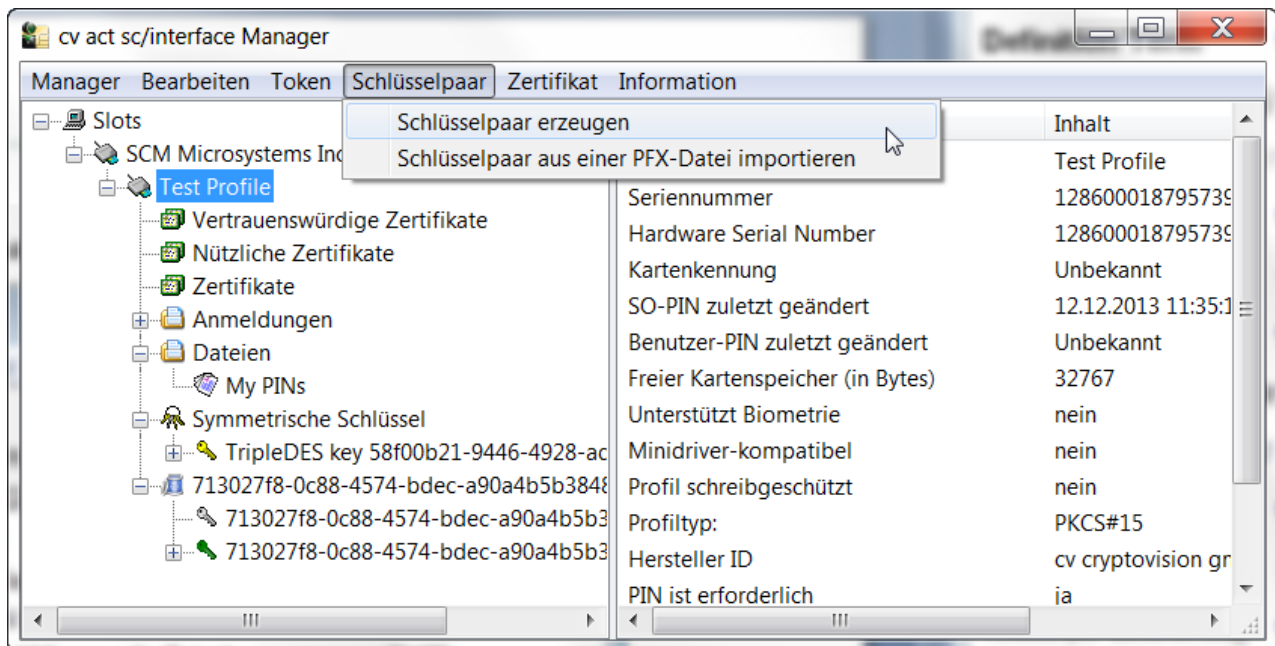
7.1.3 Registerkarte "Token"



Über diese Registerkarte können Sie die Funktionen nutzen, die das Token selber betreffen.

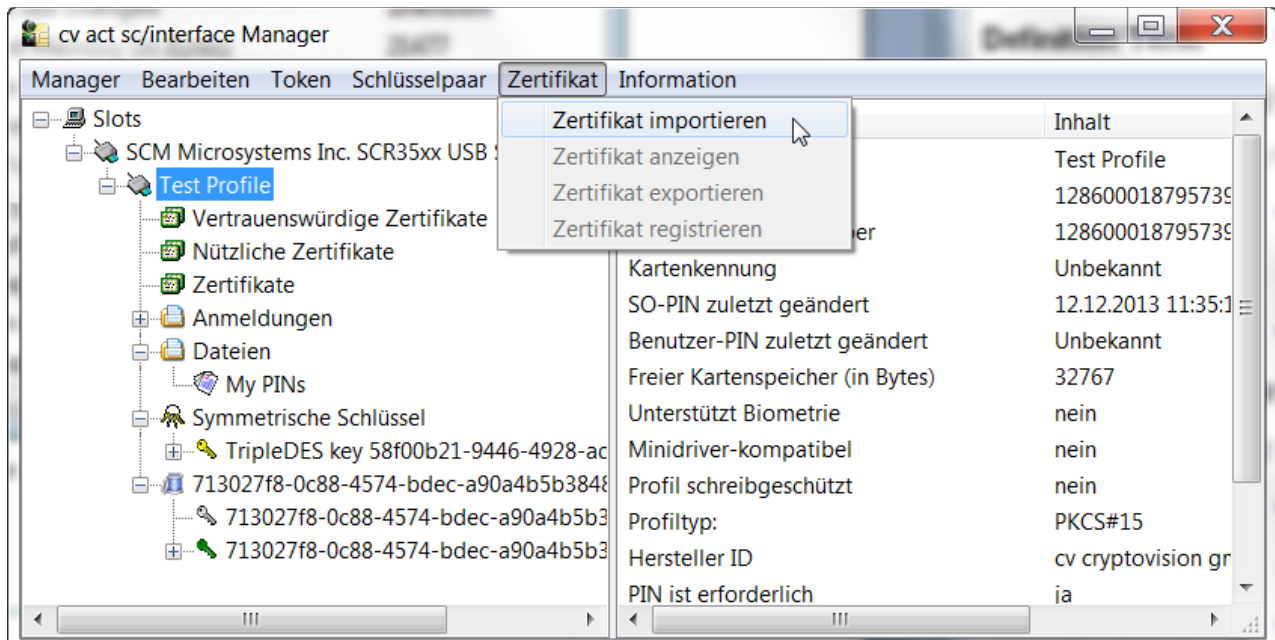
Benutzer-PIN und SO-PIN werden pro (virtuellem) Slot verwaltet, aus diesem Grunde ist „Entsperren einer Smartcard“ bei Verwendung einer Smartcard mit mehreren Anwendungen als „Entsperren eines Slots“ zu verstehen.

7.1.4 Registerkarte „Schlüsselpaar“



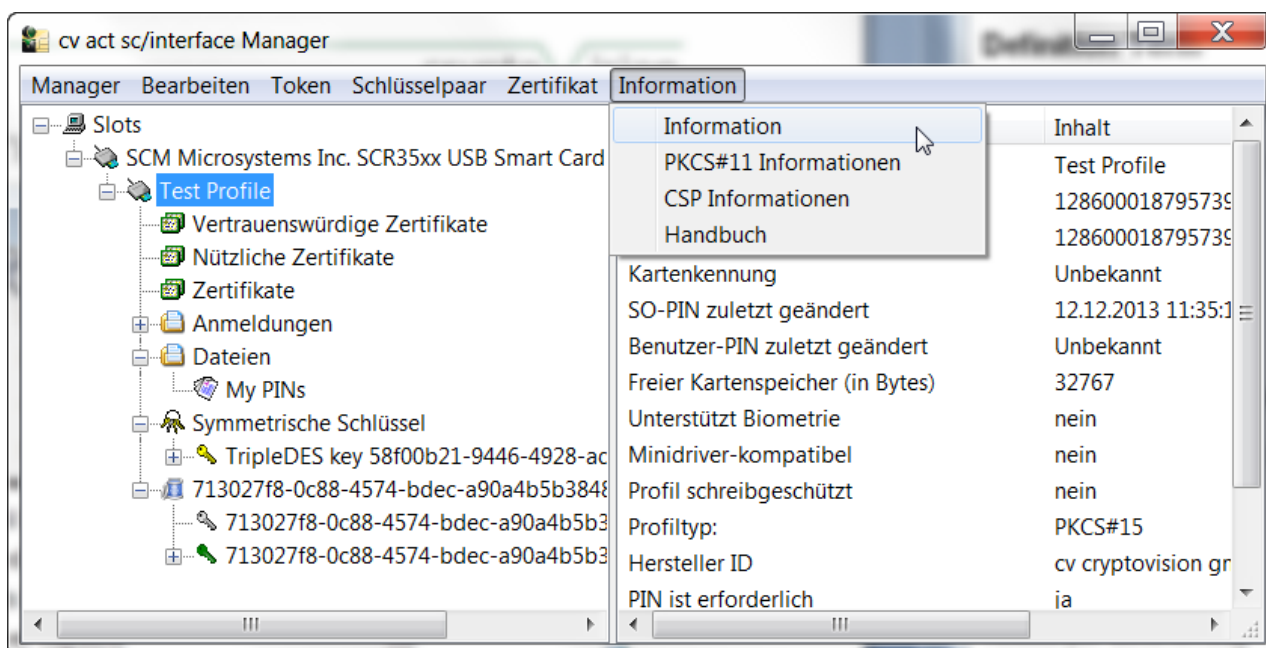
Diese Registerkarte stellt Ihnen die Funktionen zur Verfügung, die das Schlüsselpaar auf der Smartcard betreffen, sowie die Schlüsselpaarerzeugung und den Import eines Schlüsselpaars von einem Passwortgeschütztem File.

7.1.5 Registerkarte „Zertifikat“



Über diese Registerkarte haben Sie Zugriff auf die Funktionen, die Sie für die Arbeit mit Zertifikaten auf der -Smartcard benötigen.

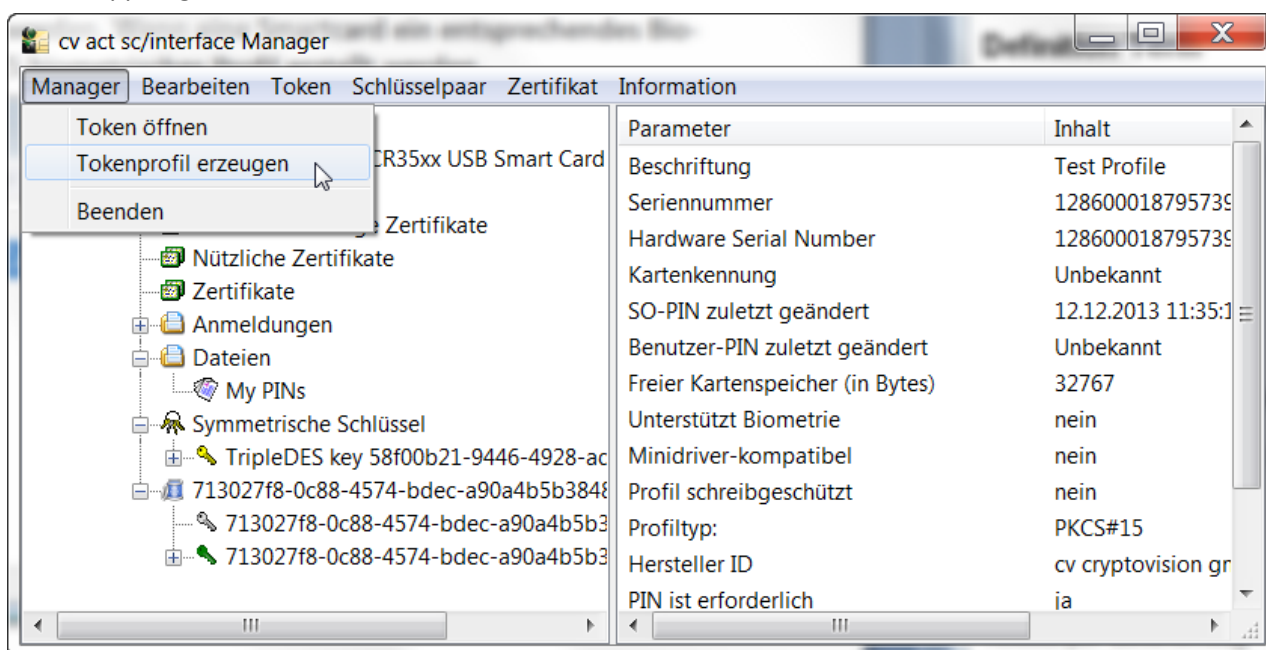
7.1.6 Registerkarte „Informationen“



Über die Registerkarte „Informationen“ bekommen Sie Informationen zu den Versionen der Module von cv act *sc/interface* und zum Hersteller cv cryptovision GmbH angezeigt, sowie einen Link zu diesem Handbuch.

7.2 Erzeugen von Profilen

Damit Sie eine Smartcard verwenden können, muss auf dieser Smartcard ein Profil vorhanden sein. Diese Profile können mit dem "Manager" Menüpunkt "Tokenprofil erzeugen" erzeugt werden. Beide PKCS#15 und cv Profile können standardmäßig ausgewählt werden. Wenn eine Smartcard ein entsprechendes Biometrie-Applet geladen hat, kann auch ein PKCS#15 biometrisches Profil erstellt werden.

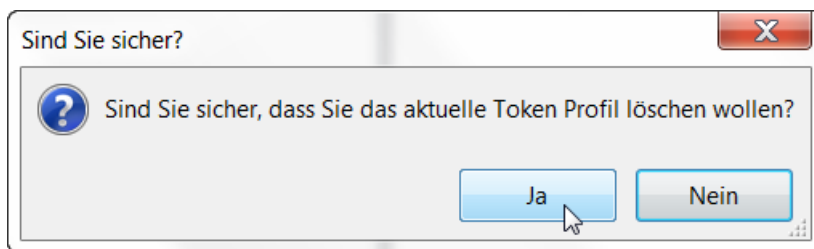


7.2.1 Smartcard mit vorhandenem Profil

Falls sich bereits ein Profil auf der Karte befindet und Sie nun ein neues Profil erzeugen wollen, wird das vorhandene in einem ersten Schritt gelöscht.

Abhängig davon welches Profil sich bereits auf der Karte befindet gehen Sie folgendermaßen vor:

- Haben Sie dieses Profil selber angelegt, müssen Sie die von Ihnen vergebene Karten-PIN eingeben
- Handelt es sich um das Siemens-Profil, geben Sie die Default-Karten-PIN "0987654321" von Siemens ein
- Handelt es sich um das STARCOS-Profil, geben Sie die Default-Karten-PIN "87654321" von Siemens ein
- Bei allen anderen Profilen lesen Sie bitte die Herstellerangaben oder dieser Dialog erscheint nicht oder das Profil kann nicht gelöscht werden.
- Handelt es sich um ein Nexus Profil auf der Smartcard, kann das Profil nicht gelöscht werden.



Die weitere Vorgehensweise ist die gleiche, wie im folgenden Abschnitt "Bei einer leeren Smartcard" erklärt.

7.2.2 Bei einer leeren Smartcard

- Beim Aufspielen des Profils (Initialisierung) auf eine Smartcard müssen folgende Parameter festgelegt werden (dabei werden die Parameter „Token-Label“, „Benutzer-PIN“, „SO-PIN“ und „Karten-PIN“ standardmäßig vorgegeben):
- Profile (die unterstützten Profile werden angezeigt, beispielsweise „PKCS#15 profile“ und „cv profile“)
- Token Label (Standardwert ist kartenabhängig)
- Karten-PIN
- SO-PIN
- Benutzer-PIN (Standardwert „11111111“, das sind 8 Einsen)
- Serial Number
- Challenge Response PIN (Erläuterung im Kapitel Minidriver)
- Minidriver kompatibel

7.2.3 Unterstützte PIN-Längen

Die folgenden minimalen und maximalen PIN-Längen stehen bei der Initialisierung einer Smartcard unter Verwendung des Administrationstools zur Verfügung:

	Benutzer	SO	Admin/Card
ACOS	4/8	8/8	8/8
CardOS	4/10	8/10	10/10
JavaCard	4/10	8/10	10/10 (nur cvProfile)
StarCOS	4/8	8/8	8/8

7.2.4 Standardwerte

Die folgenden, in der unten dargestellten Maske vorhandenen Felder sind bestimmten Werten vorbelegt:

[illegible]

Für diese Vorbelegung können eigene Werte eingestellt werden. Diese Konfiguration kann an zwei Stellen vorgenommen werden:

- scManager.ini:

Diese Datei gehört zum Lieferumfang von cv act *sc/interface* und kann entsprechend den eigenen Anforderungen angepasst werden. Sie muss in demselben Verzeichnis gespeichert werden, in dem auch scManager.exe liegt.

- Konfiguration über die Registry:

Die folgenden Registry-Schlüssel stehen zur Verfügung und können entsprechend den eigenen Anforderungen angepasst werden:

```
[HKEY LOCAL MACHINE\SOFTWARE\cv cryptovision\sc interface]
```

```
[HKEY LOCAL MACHINE\SOFTWARE\cv cryptovision\sc interface\keys]
```

```
"crkey" = "000000000000000000000000000000000000000000"
```

```
[HKEY LOCAL MACHINE\SOFTWARE\cv cryptovision\sc interface\profile]
```

```
"userpin"="11111111"  
"cardpin"="sopin"  
"#cardpin"="0987654321"  
"remindpinchange"="true"  
"minidriver"="true"  
"usehwsnr"=dword:00000001
```

Die Konfiguration über die Registry wird vorrangig verwendet.

Bei der Einstellung der eigenen Werte sind die folgenden Rahmenbedingungen zu beachten:

1. Bei der Challenge Response PIN (crkey) handelt es sich im Fall der ACOS-Smartcards um einen Zwei-Schlüssel (ABA) TripleDES Schlüssel. Für alle anderen Smartcards ist es ein Drei-Schlüssel (ABC) TripleDES Schlüssel. In beiden Fällen sind dreimal Acht Hex-Bytes, für ACOS müssen die ersten und die letzten acht Bytes übereinstimmen.
2. Benutzer PIN, Card PIN und SO PIN müssen innerhalb der kartenspezifischen Grenzen gewählt werden.
3. Falls in der Datei keine SO-PIN bzw. keine Card-PIN angegeben ist, bleiben diese Felder in der unten stehenden Maske leer.
4. Falls in der Datei keine Benutzer-PIN angegeben ist, wird der in der obigen Tabelle genannte Standardwert verwendet.
5. Falls die Option „use HW serial number“ auf true gesetzt ist, ist in der unten stehenden Maske die entsprechende Checkbox ausgewählt und das Feld zur Eingabe einer Seriennummer deaktiviert.
6. Für „Remind pin change“ kann der Wert false eingestellt werden. In diesem Fall wird nach dem Erstellen des Profils keine Warnung durch das Register Tool ausgegeben, wenn die BenutzerPIN durch den Benutzer nicht geändert wird.
7. Seit cv act *sc/interface* 4.0.1 können auch Smartcards mit Java-Betriebssystem mit einem Profil versehen werden, die nicht die Java Fixed Keys verwenden. In diesem Fall müssen die entsprechenden Schlüssel in die Datei o. g. Datei scmanager.ini eingetragen werden. Es können beliebig viele Schlüsselsätze hinzugefügt werden, wobei ein Schlüsseldatensatz wie folgt aufgebaut sein muss:

```
[javacard]  
# VISA-Fixed Keyset  
#      enc                               mac                               dek  
Keyset=404142434445464748494a4b4c4d4e4f,404142434445464748494a4b4c4d4e4f,404142434445464748494a4b4c4d4e4f  
keyset=...  
keyset=...
```

Die Karten-PIN und die SO PIN sind wichtige PINs: Mit Hilfe der Karten-PIN kann später die Karte wieder gelöscht werden und mit der SO-PIN kann eine Karte entsperrt werden. Deshalb sollten Sie keine „einfachen“ PINs vergeben. Die Eingabe der SO-PIN **erscheint auch nicht im Klartext**, sondern wird als * in der Eingabemaske angezeigt. Die Eingabe muss danach auch bestätigt werden.

Insgesamt befinden sich auf der Karte drei PINs (neben der Karten-PIN und der SO-PIN noch die Benutzer-PIN). Die Benutzer-PIN ist nun die Default-PIN und zwar „11111111“ (das sind 8 Einsen). Diese sollte dann von dem Administrator oder dem Benutzer geändert werden.

Die Verwendung der Hardware-Seriennummer als Seriennummer der Smartcard wird durch die Auswahl der entsprechenden Checkbox konfiguriert.

Anwendungen und Dienste benötigen Zugriff auf die Smartcard, z.B. ein Browser, der ein Schlüsselpaar und Zertifikat auf eine Smartcard ausrollen möchte, muss gestartet werden, nachdem das Profil erzeugt wurde.

7.2.5 PKCS#15-Profil-Karten anderer Hersteller

cv act *sc/interface* unterstützt existierende ISO7816 basierende PKCS#15-Profil-Karten.

Dabei wird zwischen ReadWrite und ReadOnly Zugriff unterschieden.

1. ReadWrite
 - Alle Operationen sind möglich.
 - Importierte Zertifikate werden nur unter „Zertifikate“ abgelegt
2. ReadOnly
 - Schreibzugriffe nicht möglich

Depending on the smart cards and vendors the following points are important:

3. Siemens HiPath ab Version 1.6.2.1
 - ReadWrite bei CardOS V-Serie

- ReadOnly bei CardOS M-Serie
 - Achtung: Von cv act *sc/interface* angelegte oder importierte Schlüsselpaare werden in Siemens HiPath ab Version 1.6.2.1 nicht angezeigt.
4. A.E.T. SafeSign ab Version 2.3.0
 - ReadOnly
 5. A.E.T. SafeSign ab Version 2.3.0 with StarCOS
 - ReadWrite
 6. G & D StarSign 1.0
 - ReadWrite
 7. Nexus Personal ab Version 4.6.1
 - ReadOnly

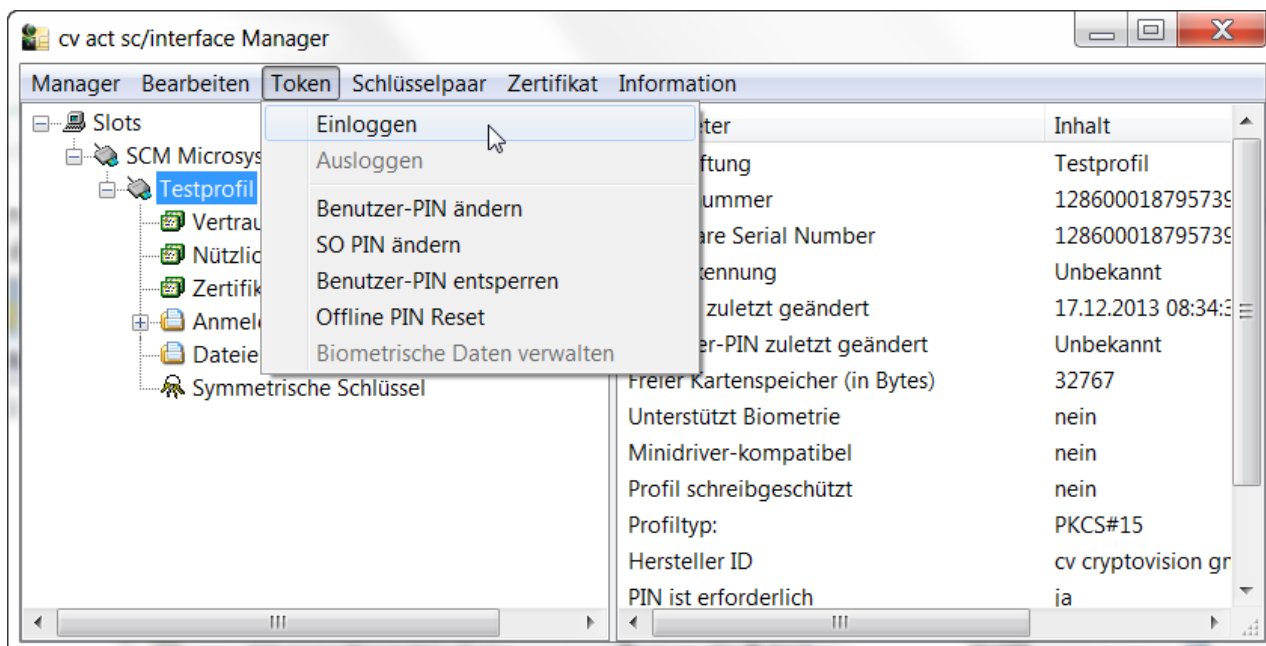
7.3 Erzeugen und Importieren von Schlüsseln

Um die Smartcard für digitale Signaturen oder Verschlüsselung zu nutzen, brauchen Sie ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel (Private Key und Public Key). Der private Schlüssel muss sicher aufbewahrt werden und der öffentliche Schlüssel durch ein Zertifikat den Kommunikationspartnern zugänglich gemacht werden. Dann gibt es noch einen Schlüssel für die Verschlüsselung, den so genannten Secret Key. Diese Schlüssel und Zertifikate können Sie mit dem Administrationstool anlegen und verwalten.

Grundsätzlich gibt es verschiedene Möglichkeiten:

1. Sie können Schlüsselpaare (Schlüssel bestehend aus privatem und öffentlichem Schlüssel als auch Secret Keys) mit diesem Administrationstool von cv act *sc/interface* erzeugen
2. Sie erzeugen Schlüssel unter Verwendung des PKCS#11-Moduls oder des CSP oder des Minidriver (sind Bestandteil von cv act *sc/interface*). Diese Vorgehensweise wird in den Kapiteln 13, 14 oder 15 näher beschrieben.
3. Sie haben bereits einen Schlüssel und/oder ein Schlüsselpaar. Dann können Sie ein Schlüsselpaar, gegebenenfalls zusammen mit dem Zertifikat als PFX-Datei importieren. Secret Keys können Sie speichern, indem Sie diese, z.B. mit Copy and Paste importieren.

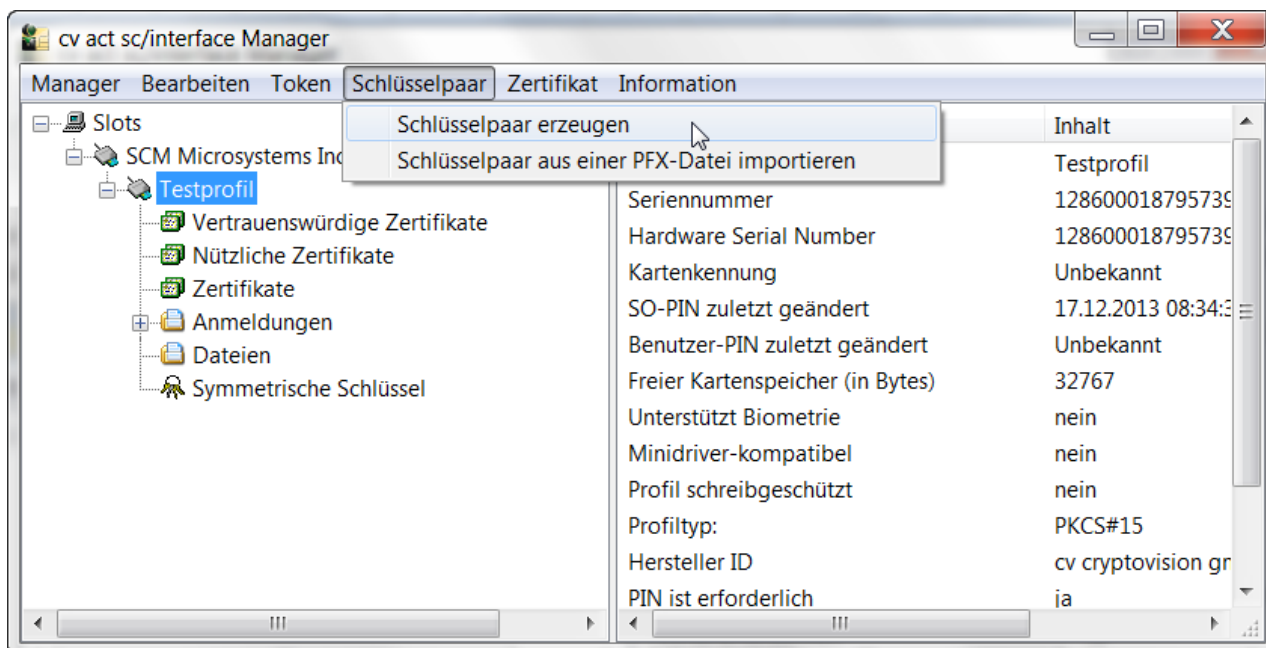
Wenn Sie diese Funktionen nutzen wollen, müssen Sie sich zuerst auf die Smartcard einloggen: Betätigen Sie das Menü „Token“ -> „Einloggen“:



Alle Funktionen zum Erzeugen und Importieren von Schlüsseln finden Sie im Menü „Schlüsselpaar“ und zum Importieren von Zertifikaten im Menü „Zertifikat“, wie in den folgenden Kapiteln erklärt wird.

7.3.1 Erzeugen eines Schlüsselpaares

Das Erzeugen eines Schlüsselpaares (privater und öffentlicher Schlüssel) erfolgt im Menü „Schlüsselpaar“ über den Menüpunkt „Schlüsselpaar erzeugen“. Diese Schlüssel sehen Sie dann im Administrationstool im zugehörigen Container.



Die verfügbare RSA-Schlüssellänge hängt von der Smartcard bzw. dem verwendeten Smartcard-Betriebssystem ab:

- G&D Sm@rtCafé Expert 3.1, G&D Sm@rtCafé Expert3.2 auf StarSign Card Token 550 (USB), G&D Sm@rtCafé Expert64:
 - 512, 1024, 1536 oder 2048 Bit
- CardOS M4.01, M4.01a oder V4.20 Smartcard:
 - 512 oder 1024 Bit
- CardOS V4.30 oder V4.20 mit zusätzlichem Package:
 - 512, 1024, 1536 oder 2048 Bit
 - Um bei einer CardOS V4.20 Smartcard ebenfalls RSA-Schlüssel mit 2048 Bit erzeugen zu können, benötigen Sie dafür ein so genanntes nachladbares Package.

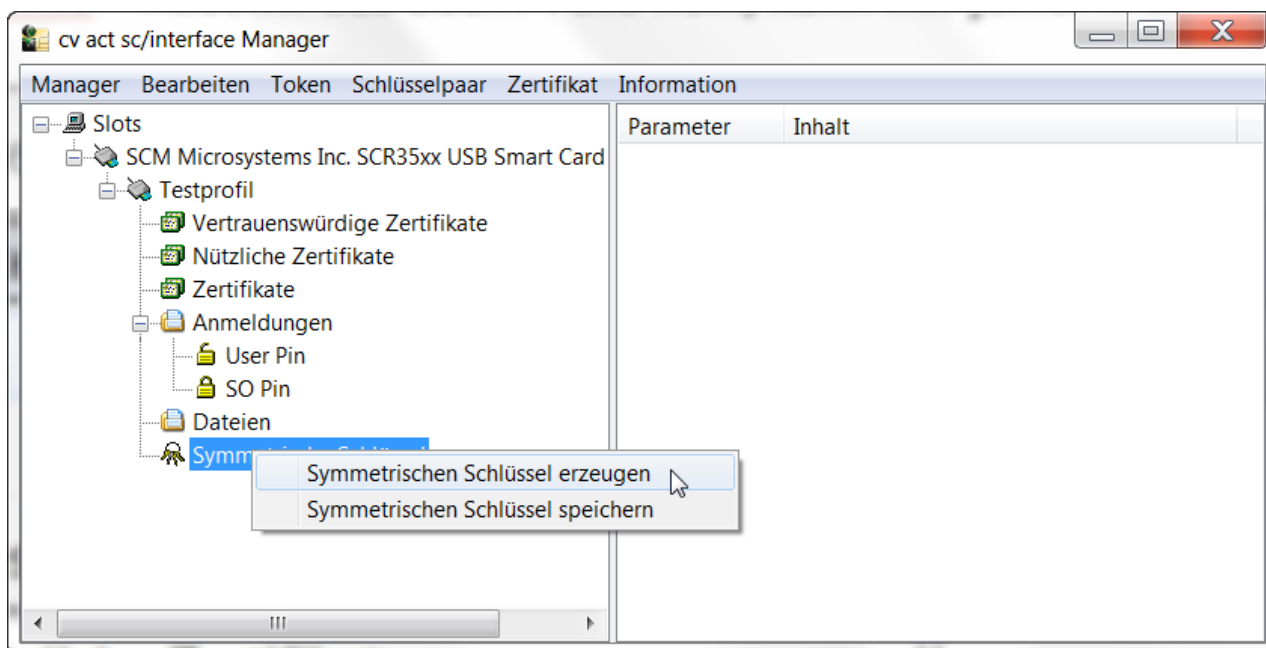
7.3.2 Importieren eines Schlüsselpaars

Falls Sie bereits ein Schlüsselpaar besitzen, das Sie verwenden möchten, können Sie dieses im Menü „Key Pair“ („Schlüsselpaar“) über den Menüpunkt „Import Key Pair from PFX-File“ („Schlüsselpaar aus einer PFX-Datei importieren“) importieren. Dabei werden Sie aufgefordert, den Pfad zu dem PFX-File und Ihr Passwort, das Sie zum Sichern dieser Datei benutzen, einzugeben.

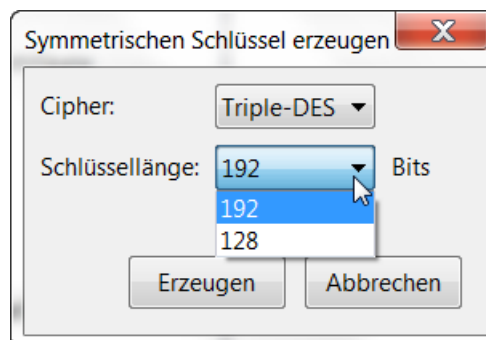
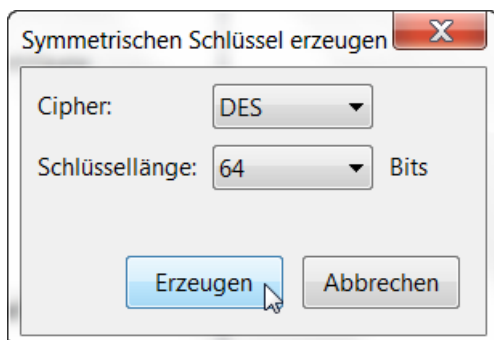
Bemerkung: Die Schlüssellänge beim Importieren von Schlüsselpaaren unterliegt denselben Rahmenbedingungen, die im vorhergehenden Abschnitt für das Erzeugen eines Schlüsselpaares genannt sind. Der Schlüssel muss ein RSA-Schlüssel sein und im pfx- oder p12-Format vorliegen

7.3.3 Erzeugen eines Secret Keys

Zum Erzeugen eines geheimen Schlüssels zum Verschlüsseln markieren Sie „Secret Keys“ und wählen im Menü „Bearbeiten“ den Menüpunkt „Symmetrischen Schlüssel erzeugen“ oder auch über das Kontextmenü der rechten Maustaste:



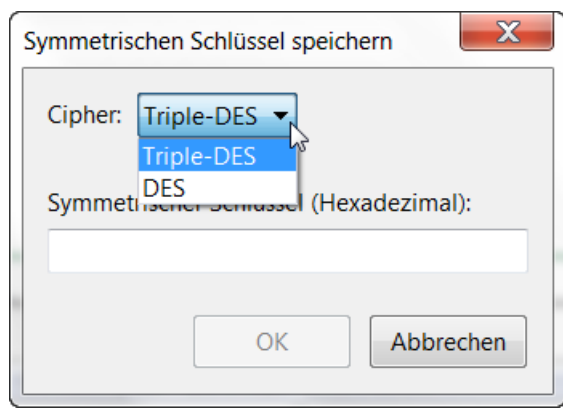
Dabei können Sie einen Triple-DES-Schlüssel mit 192 Bit oder 128 Bit oder einen DES-Schlüssel mit 64 Bit erzeugen.



HINWEIS: Empfohlen werden Algorithmen ab 128 Bit (Triple-DES). Nach dem heutigen Stand können Algorithmen mit Schlüssellängen von weniger als 128 Bit nicht als sicher angesehen werden.

Importieren eines symmetrischen Schlüssels / Secret Key

Falls Sie bereits einen symmetrischen Schlüssel (Secret Key) besitzen, den Sie verwenden möchten, können Sie diesen im Menü „Bearbeiten“ über den Menüpunkt „Symmetrischen Schlüssel speichern“ importieren. Der symmetrische Schlüssel muss hexadezimal angegeben werden und bei Triple-DES 192 oder 128 Bit und bei DES 64 Bit groß sein. Das Importieren erfolgt über das Einfügen der Bits in das Feld „Symmetrischer Schlüssel (Hexadezimal)“, z.B. per Kopieren und Einfügen.



7.4 Ändern von PINs

Insgesamt befinden sich auf der Smartcard drei PINs: die User-PIN, die SO-PIN (PIN des System Operators, bzw. des Security Operators) und die Karten-PIN. Es gibt verschiedene Funktionen, um diese 3 PINs zu verwenden:

Benutzer-PIN: Diese muss eingegeben werden, wenn auf die Karte geschrieben wird (z.B. Schlüsselgenerierung, Speicherung eines Zertifikats), Objekte gelöscht werden sollen oder wenn die kryptographischen Funktionen (wie Signieren oder Entschlüsseln) benutzt werden. Die minimale Länge der Benutzer-PIN beträgt vier Zeichen, die maximale Länge beträgt zehn Zeichen. Die Default-PIN ist „11111111“ (das sind 8 Einsen).

Wichtig: Die Benutzer-PIN wird nach dreimaliger Falscheingabe gesperrt.

SO-PIN: Eine gesperrte Benutzer-PIN kann mit Hilfe der SO-PIN (auch PUK genannt) entsperrt werden. Die minimale Länge der SO-PIN beträgt acht Zeichen, die maximale Länge beträgt zehn Zeichen. Die Default-SO-PIN ist „1111111111“ (das sind 10 Einsen).

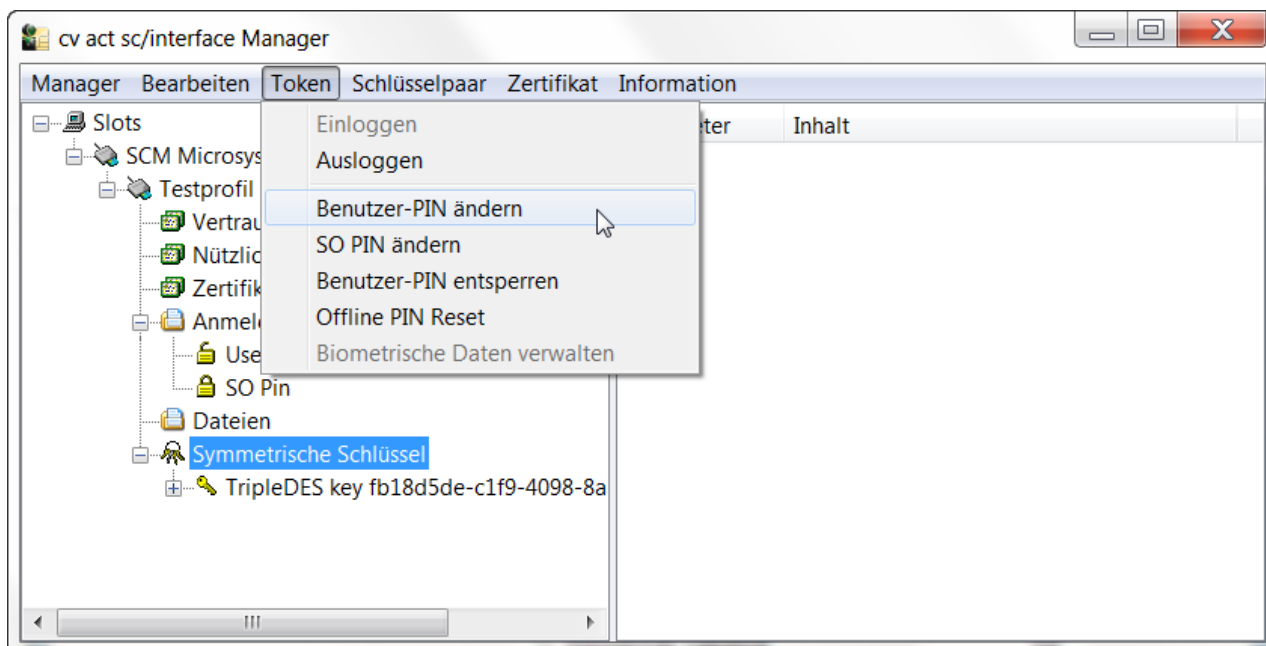
Die SO-PIN wird nur für das Entsperren der Benutzer-PIN verwendet und für das Ausrollen von biometrischen Fingerprint-Daten. Ansonsten kann man keine weiteren Funktionen, wie Create oder Delete verwenden.

Wichtig: Abhängig von Betriebssystem wird die SO-PIN nach einer gewissen Anzahl von Falscheingabe gesperrt. Falls dieses Limit überschritten wurde und die SO-PIN gesperrt ist, muss das Profil gelöscht und mit der Karten-PIN neu angelegt werden.

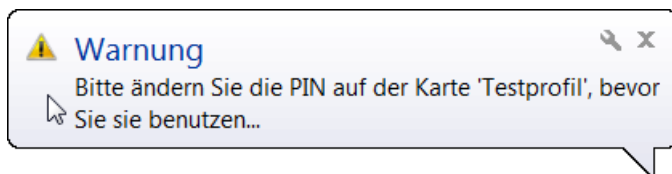
Karten-PIN: Mit der Karten-PIN kann eine Karte, auf der sich bereits ein Profil befindet, gelöscht werden, indem Sie ein neues Profil aufspielen. Die Karten-PIN wird bei der Initialisierung der Karte festgelegt und kann danach nicht mehr geändert werden. Die Länge der Karten-PIN ist auf zehn Zeichen festgelegt.

Wichtig: Nach einer gewissen Anzahl von Falscheingabe ist die Karten-PIN gesperrt und die Karte kann nicht mehr gelöscht werden (Bei zB. StarCOS 3.0 wird die Karten-PIN nach der dritten Fehleingabe gesperrt). Wenn sowohl Karten-PIN, SO-PIN als auch die Benutzer-PIN gesperrt sind, ist die Karte unbrauchbar!

Alle Funktionen zum Ändern der SO- oder der Benutzer-PIN finden Sie im Menü „Token“, wie in der folgenden Abbildung dargestellt:



Anmerkung: Bei einer Smartcard mit PKCS#15-Profil wird auf der Smartcard das Datum der letzten Änderung gespeichert. Falls hier der Wert „00000“ gespeichert ist, wird über einen Balloon Tipp eine Aufforderung ausgegeben, die Benutzer-PIN zu ändern. D.h. wurde die Benutzer-PIN, mit der die Smartcard ausgeliefert wurde, nicht geändert, wird der Benutzer über diesen Balloon Tipp dazu aufgefordert (falls die Smartcard diese Funktion unterstützt).

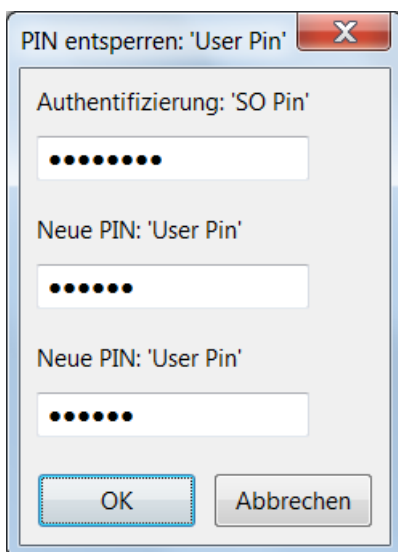
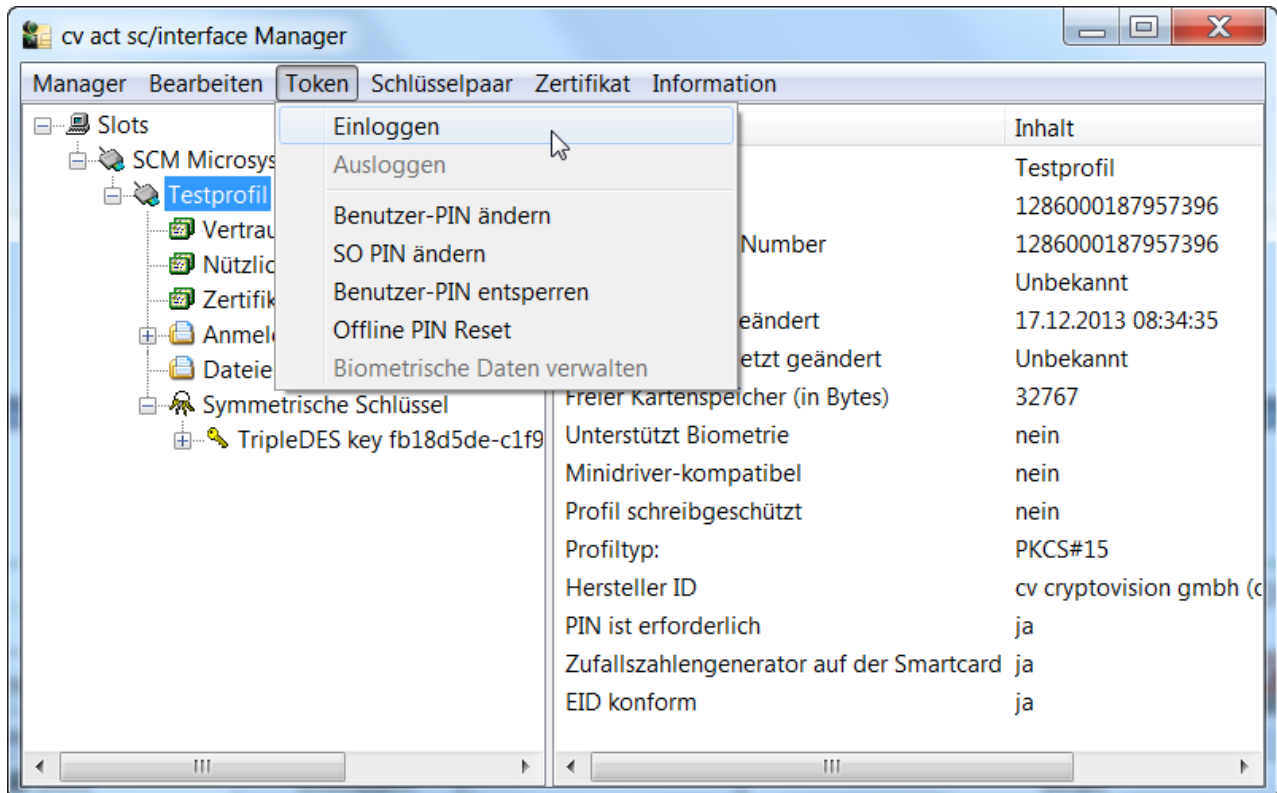


7.5 Entsperren von Smartcards

Als Schutzmechanismus wird eine Smartcard gesperrt, wenn ein Benutzer dreimal die falsche Benutzer-PIN eingegeben hat. Der Schutz besteht darin, dass ein Unbefugter nicht durch Ausprobieren aller möglichen PINs (brute force) die Benutzer-PIN herausfinden kann, wenn Sie die Smartcard verloren haben oder sie Ihnen entwendet wurde.

Benutzer-PIN und SO-PIN werden pro (virtuellem) Slot verwaltet, aus diesem Grunde ist „Entsperren einer Smartcard“ bei Verwendung einer Smartcard mit mehreren Anwendungen als „Entsperren eines Slots“ zu verstehen.

Um eine Benutzer-PIN zu entsperren, benötigen Sie dazu die SO-PIN. Die Funktion zum Entsperren finden Sie im Menü „Token“, wie in der folgenden Abbildung dargestellt:



8 Beispiel: Konfiguration einer Smartcard für die erste Nutzung

Im Folgenden wird ein typischer Smartcard-Initialisierungsprozess beschrieben. Zu Beginn ist die Smartcard leer. Zunächst wird daher ein Profil erstellt. Dies erfolgt mit Hilfe des scManager auf einem Windows-Desktop-PC mit Standard-Kartenleser. Nach der Profilerstellung wird auf der Smartcard ein Schlüsselpaar generiert, und ein PKCS#10-Request für den öffentlichen Schlüssel wird erstellt. Beides wird exportiert. Der PKCS#10-Request wird dann an einen CA-Betreiber geschickt, der den Antrag prüft und im positiven Fall ein Zertifikat ausstellt. Das Zertifikat wird anschließend zurückgeschickt und auf der Chipkarte gespeichert. Wenn dieser Prozess abgeschlossen ist, kann die Chipkarte an den Anwender übergeben werden.

8.1 Vorbereiten einer Smartcard (Initialisieren und Personalisieren)

Damit ein Benutzer seine Smartcard verwenden kann, muss diese dafür vorbereitet werden, d.h. die Smartcard muss für den Benutzer initialisiert und personalisiert werden. In der Regel müssen Sie ein Profil auf die Smartcard aufspielen und danach bringen Sie Schlüssel und Zertifikate auf die Smartcard.

Erster Schritt: Anlegen eines Profils (Initialisierung)

Als ersten Schritt müssen Sie ein Profil auf die leere Smartcard aufspielen. Dazu gehen Sie vor, wie in Abschnitt 4.6 „[Erzeugen von Profilen](#)“ beschrieben.

Zweiter Schritt: Anlegen von Schlüsseln und Zertifikaten (Personalisierung)

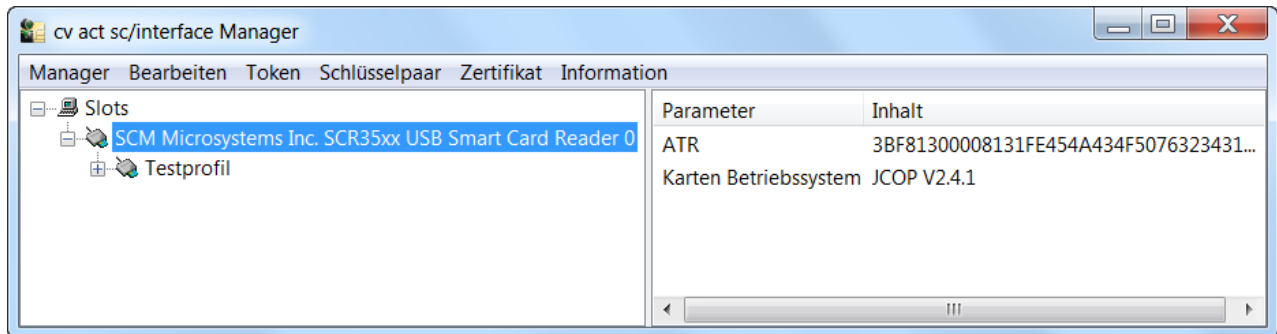
Als zweiten Schritt müssen Sie für einen Benutzer Schlüssel und Zertifikat auf der Smartcard anlegen. Dabei haben Sie die Möglichkeit, Schlüssel und Zertifikate entweder zu erzeugen oder zu importieren. Dazu finden Sie die Beschreibung jeweils in Abschnitt 4.4 „[Erzeugen und Importieren von Schlüsseln](#)“ und in Abschnitt 4.5 „[Erzeugen und Importieren von Zertifikaten](#)“.

8.2 Erzeugen von Karten-Profilen

Um ein Kartenprofil zu erstellen, starten Sie den scManager (er befindet sich normalerweise im Verzeichnis "Programme → cv cryptovision → cv act sc interface") mit dem folgenden Befehl:

```
C:\Program Files (x86)\cv cryptovision\cv act sc interface\scManager.exe
```

Wenn ein Smartcard-Leser mit eingelegter Karte festgestellt wird, öffnet sich ein Fenster wie das folgende (in diesem Fall werden der Leser "SCM Microsystems Inc. SCR35xx USB Smart Card Reader 0" und die Karte JCOP V2.4.1 angezeigt):



Bevor Sie ein Schlüsselpaar auf der Smartcard generieren können, muss diese initialisiert werden. Dieser Vorgang wird als Profilierung bezeichnet. Um die Profilierung zu starten, markieren Sie den Kartenleser und wählen Sie den Menüpunkt "Manager → Create Token Profile" aus.

Falls die Smartcard nicht leer ist, wird eine Warnung angezeigt, dass alle Daten auf der Karte gelöscht werden, wenn Sie den Vorgang fortsetzen. Stellen Sie sicher, dass Sie den Inhalt der eingelegten Karte nicht mehr benötigen.

Im Dialog "Create Token Profile" müssen Sie folgende Felder ausfüllen:

Feld	Wert	Anmerkungen
Profile	PKCS#15-Profile	In der Regel ist das Standard-PKCS#15-Profile zu empfehlen.
Token Label	Name oder Kennung der Smartcard	Dieses Feld wird von zahlreichen Anwendungen genutzt, um die Karte eindeutig zu identifizieren. Die Kennung kann beispielsweise den Namen oder die Personalnummer des Nutzers enthalten. Eine andere Möglichkeit ist eine kurze Beschreibung des Verwendungszwecks.
Card PIN	Deaktiviert	Eine Karten-PIN wird in diesem Beispiel nicht verwendet.
SO PIN	PIN des Security Officers	<p>Ist die Karte nach mehrfacher falscher PIN-Eingabe gesperrt, kann sie der Security Officer mit der SO-PIN wieder entsperren. Die SO-PIN darf dem Benutzer nicht ausgehändigt werden. Die Aufbewahrung sollte an einem sicheren Ort mit Zugangskontrolle erfolgen.</p> <p>Wir empfehlen die Verwendung einer numerischen SO-PIN, damit die Eingabe an einem Kartenleser mit integrierter Tastatur erfolgen kann (ein solcher hat normalerweise keine Buchstabentasten).</p> <p>Auf der rechten Seite des Dialogs wird angezeigt, wie lange die SO-PIN mindestens sein muss und höchstens sein darf.</p> <p>Die SO-PIN muss über das Feld "Confirm SO PIN" bestätigt werden.</p>
User PIN	PIN des Anwenders	<p>Wir empfehlen, auch die User-PIN numerisch zu wählen, damit ein Kartenleser mit integrierter Tastatur verwendet werden kann.</p> <p>An dieser Stelle bietet es sich an, eine einfache Standard-PIN wie 11111111 zu wählen. Bevor die Karte dem Anwender ausgehändigt wird, kann ein</p>

Registrator die PIN ändern. Durch dieses Vorgehen wird kein PIN-Brief benötigt.

Die Länge der PIN muss innerhalb der auf der rechten Seite angezeigten Grenzen liegen.

Wenn der Anwender mehrfach eine falsche PIN eingibt (die Obergrenze ist konfigurierbar, meist liegt sie bei 3), sperrt sich die Karte. Nur ein Security Officer mit Zugang zur SO-PIN kann eine gesperrte Karte wieder entsperren.

Serial Number Seriennummer (frei definierbar)

Bitte prüfen Sie, ob die Box "Hardware SN benutzen" aktiviert ist.

Ist keine Hardware-Seriennummer vorhanden, dann sollte eine gewählt werden, die zuvor festgelegten Vorgaben entspricht. Es bietet sich beispielsweise an, die Personalnummer des Anwenders mit der Kartenfolgennummer (diese entspricht der Anzahl der Karten, die eine Person bisher erhalten hat) zu kombinieren.

Challenge Response PIN Deaktiviert

Eine Challenge-Response-PIN wird in diesem Beispiel nicht verwendet.

Minidriver compatible Deaktiviert

Diese Option ist nur verfügbar, wenn eine Challenge-Response-PIN verwendet wird.

Session PIN support Deaktiviert

Diese Option ist nur verfügbar, wenn die Smartcard Session PIN unterstützt

Wenn in allen Zeilen ein grüner Haken angezeigt wird, klicken Sie "OK". Nun wird ein neues Profil generiert. Dieser Prozess kann einige Minuten dauern.

Das Hauptfenster sollte ähnlich wie auf dem folgenden Screenshot aussehen. Auf der linken Seite werden einige leere Container, wie "Vertrauenswürdige Zertifikate" oder "Dateien", dargestellt. Auf der linken Seite sind verschiedene Informationen zur Karte zu sehen.

8.3 Erzeugen und Importieren von Zertifikaten

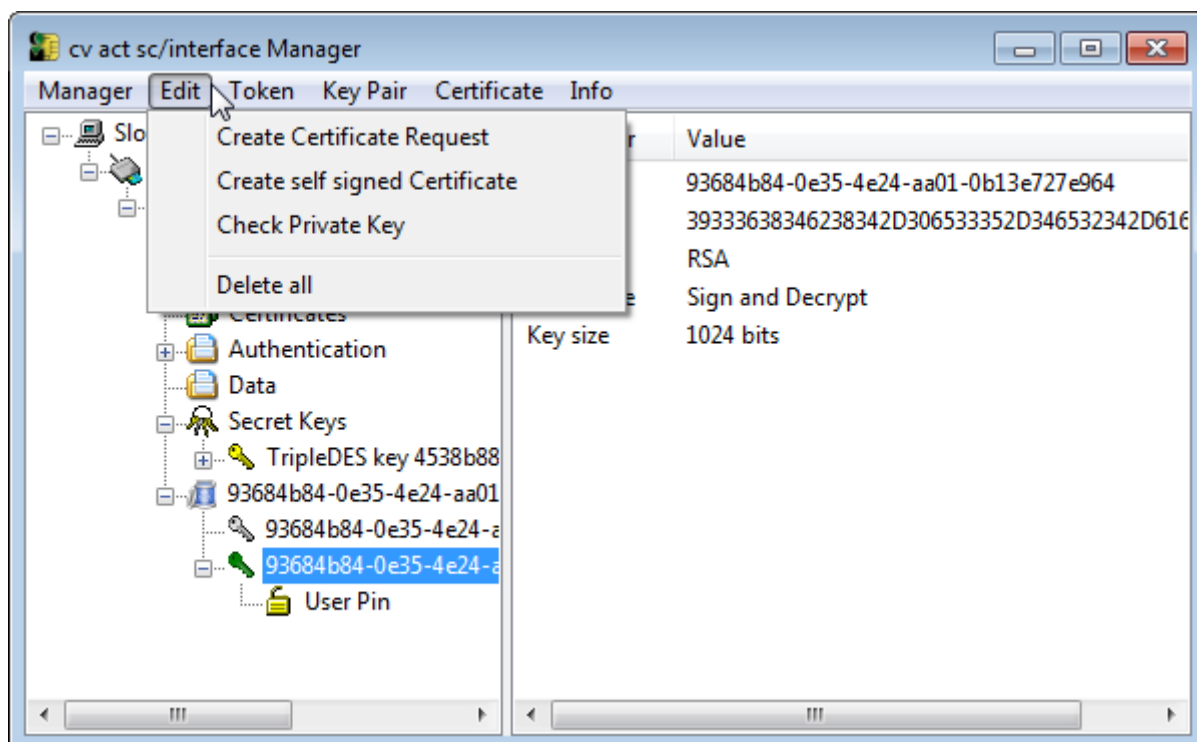
Um die Smartcard für digitale Signaturen und Verschlüsselung verwenden zu können, müssen Sie ein Schlüsselpaar (bestehend aus einem privaten und einem öffentlichen Schlüssel) generieren. Der öffentliche Schlüssel sollte in Form eines digitalen Zertifikats für Kommunikationspartner zugänglich sein. Digitale Zertifikate können Sie mit dem scManager generieren und verwalten.

Grundsätzlich gibt es zwei Möglichkeiten:

1. Sie können Ihr Zertifikat selbst signieren oder einen Certificate Signing Request an eine Zertifizierungsstelle schicken, die ein Zertifikat für Sie generiert.
2. Falls Sie bereits ein Zertifikat haben, können Sie dieses zusammen mit dem zugehörigen Schlüssel importieren.

8.3.1 Selbstsignierte Zertifikate und Certificate Signing Requests

Sie können das Zertifikat, das zu einem öffentlichen Schlüssel gehört, entweder selbst generieren, oder Sie können einen Certificate Signing Request erstellen und diesen an eine Zertifizierungsstelle schicken. Um einen dieser Schritte durchzuführen, wählen Sie den privaten Schlüssel aus und klicken Sie auf "Bearbeiten" -> **Create Self Signed Certificate** für ein selbstsigniertes Zertifikat.



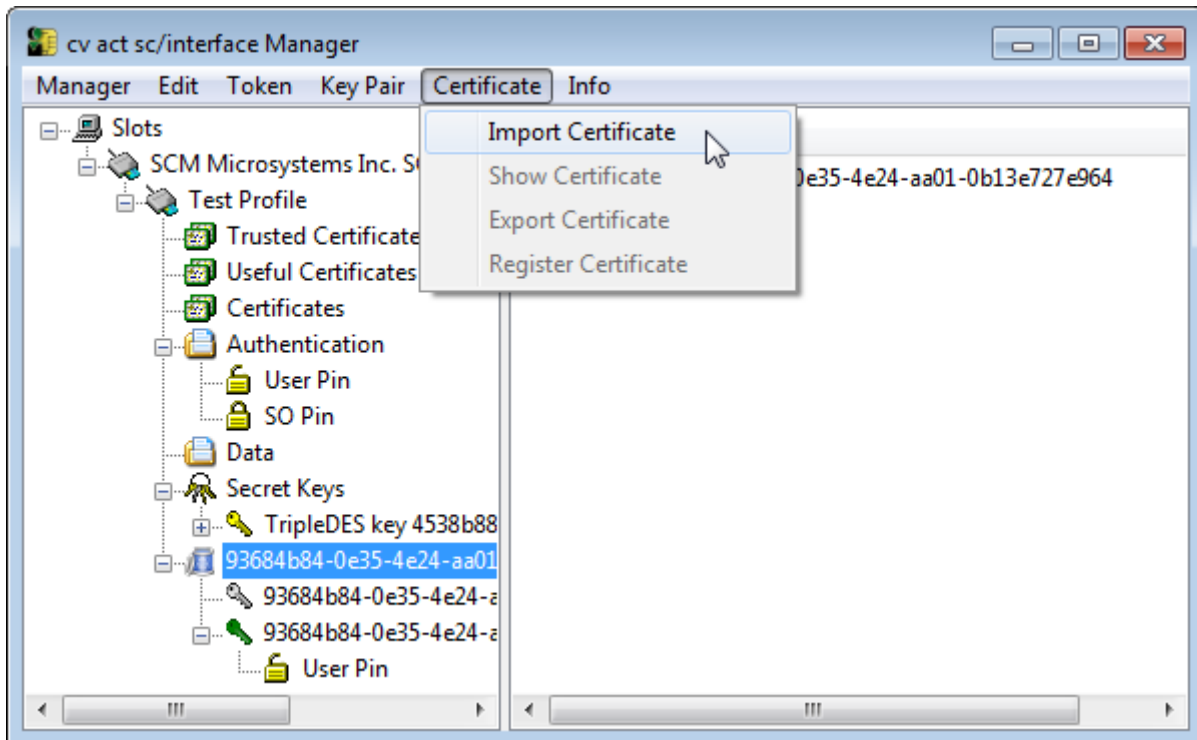
Um den Request zu generieren, müssen Sie verschiedene Daten in die entsprechenden Felder eingeben. Typischerweise wird ein Request als Datei an die Zertifizierungsstelle gesendet. Sie können den Request daher in den meisten Fällen als p10-Datei auf Ihrem PC abspeichern und als E-Mail-Anhang verschicken. Hierbei müssen Sie die Bestimmungen der jeweiligen Zertifizierungsstelle beachten.

Wenn die Zertifizierungsstelle das beantragte Zertifikat geliefert hat, müssen Sie dieses über den Menüpunkt "Import Certificate" importieren.

Hinweis: In Anhang C dieses Handbuchs werden verschiedene Zertifikatsattribute und deren Anwendung erklärt.

8.3.2 Import von Zertifikaten

Wenn Sie bereits ein Zertifikat besitzen, können Sie dieses über den Menüpunkt "Certificate->Import Certificate" importieren. Wenn das Zertifikat zu einem bereits vorhandenen Schlüsselpaar gehört, wird es automatisch dem entsprechenden Container zugewiesen. Zertifikate ohne Schlüssel, zum Beispiel CA-Zertifikate, werden dem Knoten "Certificates" zugeordnet.



9 Verwenden von Biometrie

cv act *sc/interface* ermöglicht einen durch Biometrie geschützten Zugang zu Windows-Umgebungen. Dabei wird eine Smartcard verwendet, die statt einer PIN ein Fingerabdruck-Muster entgegen nimmt.

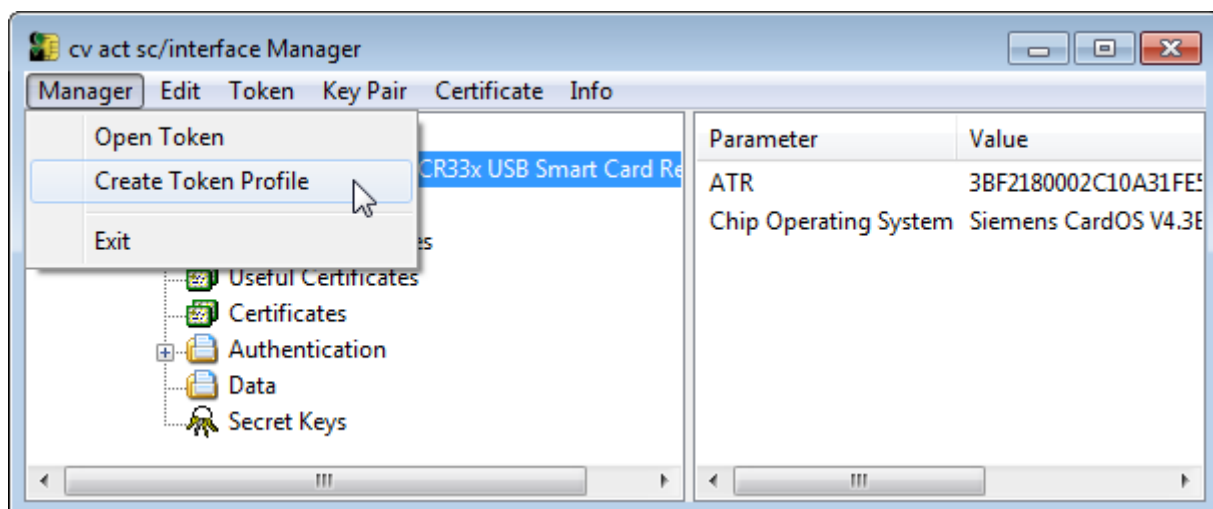
9.1 Unterstützte Smartcards und Leser

cv act *sc/interface* unterstützt derzeit nur Fingerabdruck-Leser von Precise Biometrics. Eine Liste der getesteten Lesegeräte findet sich im Abschnitt "Smart Kartenleser mit Fingerprint-Sensor" im Kapitel über die Installation. Folgende Karten werden unterstützt:

- CardOS 4.01a
- Alle aufgeführten Java Cards mit dem Match-on-Card™-Package von Precise Biometrics (siehe [Kapitel 3.3 "Unterstützte Smartcards"](#))

9.2 Profile

Wenn Sie eine Smartcard mit Biometrie nutzen wollen, muss die Karte mit einem biometrischen Profil versehen werden. Ist bereits ein nicht-biometrisches Profil installiert, so muss dieses gelöscht werden, bevor ein biometrisches Profil erstellt werden kann. Zu diesem Zweck muss die Karten-PIN eingegeben werden. Wenn Sie das Profil selbst erstellt haben, müssen Sie die selbst gewählte PIN verwenden. Ist das Profil ein cryptovision-Standardprofil, dann lautet die Karten-PIN "0987654321". Um ein biometrisches Profil zu erstellen, wählen Sie (nachdem ein Leser ausgewählt ist) "Create Token-Profil" im Menü "Manager".



Wenn Sie ein neues Profil generieren (initialisierung), öffnet sich das folgende Fenster:

Create Token Profile

Profile: PKCS#15 biometric profile

Token Label: Biometric test profile

Card PIN:

SO PIN:

Confirm SO PIN:

User PIN:

Confirm User PIN:

Serial Number: ☒ Use Hardware SN

Challenge Response PIN: ☐

Minidriver compatible: ☐

Session PIN support: ☒

The Card PIN is defined to consist of 10.

- ✓ The SO-PIN has to consist of at least 4.
- ✓ The SO-PIN shall not exceed 10.
- ✓ The SO-PIN was correctly verified.
- ✓ The user PIN has to consist of at least 4.
- ✓ The user PIN shall not exceed 10.
- ✓ The user PIN was correctly verified.

The serial number shall have not more than 16 and at least one alpha-numeric digits.

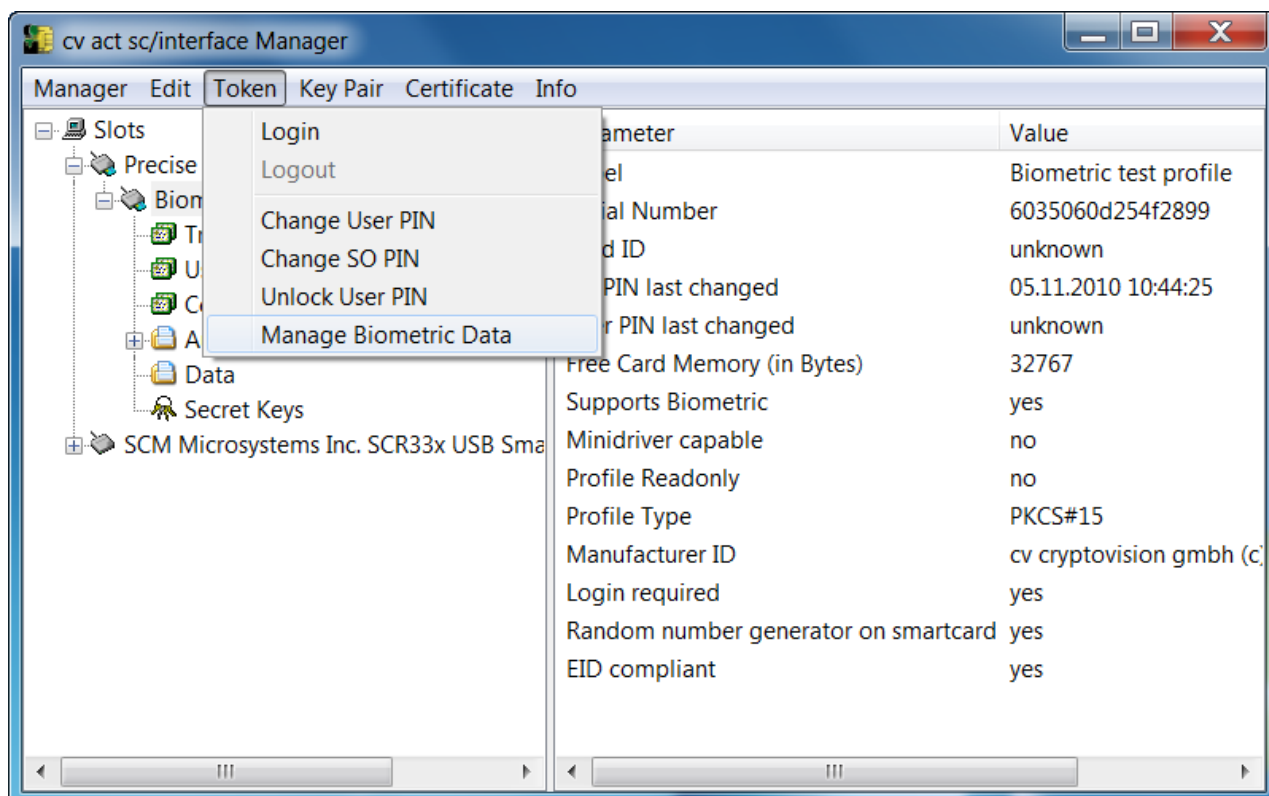
- ✓ No challenge response PIN needed.

OK Cancel

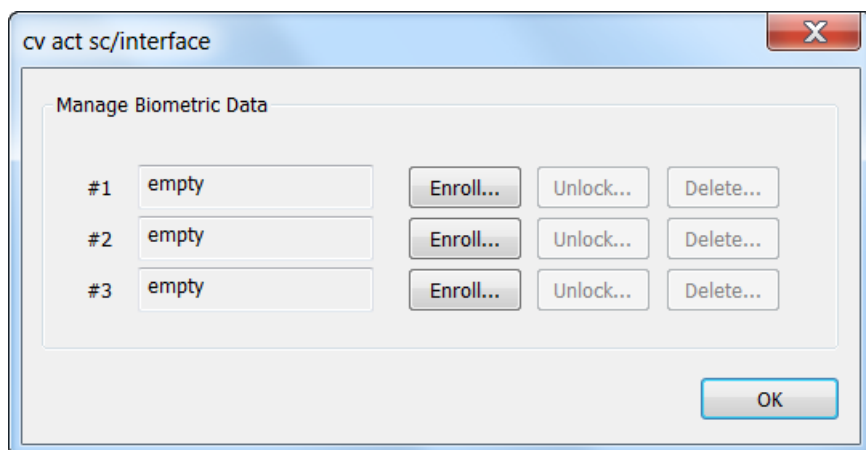
Wählen Sie "PKCS#15 biometric profile" und geben Sie eine Karten-PIN, die SO-PIN und eine Seriennummer ein. Im rechten Teil des Fensters werden die Anforderungen angezeigt, diese Werte erfüllen müssen. Ein grünes Häkchen steht für "in Ordnung", ein rotes Häkchen für "Anforderungen nicht erfüllt".

9.3 Fingerabdruck initialisieren

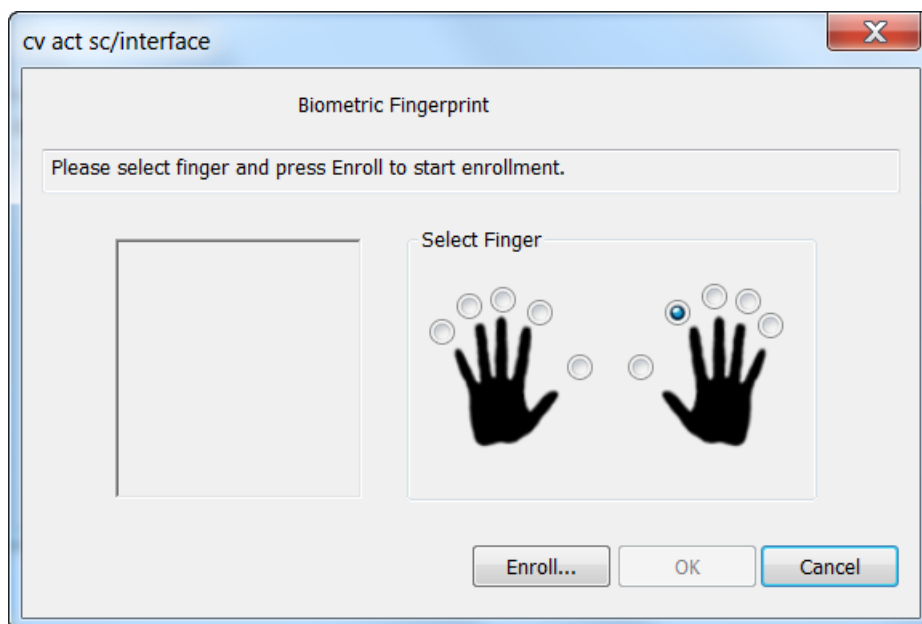
Nun können Sie Ihren Fingerabdruck eingeben und ihn auf der Smartcard speichern. Wählen Sie dazu "Manage Biometric Data" im Menü "Token":



Diese Funktion ist nur verfügbar, wenn die eingegebene Smartcard ein biometrisches Profil enthält. Wenn Sie diesen Menüpunkt ausgewählt haben, erscheint ein Fenster, über das Sie bis zu drei Fingerabdrücke speichern können:



Jetzt können Sie einen neuen Fingerabdruck einlesen (jeder Finger kann nur einmal gespeichert werden), entsperren oder löschen. Um einen Fingerabdruck zu registrieren, klicken Sie auf die Schaltfläche "Enroll ..." in einer Zeile, die mit "empty" gekennzeichnet ist. Gibt es keine leere Zeile, dann müssen Sie einen der registrierten Fingerabdrücke löschen. Nach dem Klick auf "Enroll ..." öffnet sich ein neues Fenster. Wenn Sie bereits Fingerabdrücke registriert haben, sind die entsprechenden Finger nicht mehr wählbar. Wenn Sie einen Fingerabdruck überschreiben wollen, dann müssen Sie diesen zunächst löschen:



Wählen Sie den Finger, der eingelesen werden soll, und klicken Sie auf "Enroll". Folgen Sie den Anweisungen in der Zeile unter "Biometric Fingerprint Enrollment". Wenn der Fingerabdruck eingelesen ist und die Qualitätsprüfung erfolgreich war, klicken Sie auf "OK". Geben Sie die PIN-SO ein, um die biometrischen Daten auf der Smartcard zu speichern.

Nach Eingabe der SO-PIN können die Daten auf der Smartcard gespeichert werden.

9.4 Fingerabdruck entsperren und löschen

Geben Sie mehr als dreimal einen falschen Fingerabdruck ein, dann wird die Karte gesperrt (ähnlich wie bei einer falschen PIN). Sie können die Smartcard anschließend mit der SO-PIN entsperren. Wie oben beschrieben, erfolgt dies mit dem "Unlock"-Menüpunkt. Klicke Sie diesen an, erscheint ein Popup-Fenster, in dem Sie nach der SO-PIN gefragt werden.

Zum Löschen eines Fingerabdrucks drücken Sie die Schaltfläche "Delete" hinter dem registrierten Finger. Auch hier erscheint ein Popup-Fenster für die SO-PIN.

9.5 Sensor-Leser-Zuordnung

cv act *sc/interface* kann so konfiguriert werden, dass es ein biometrisches Gerät ohne integrierten Kartenleser nutzt. Hierzu muss eine logische Zuordnung zweier unterschiedlicher Geräte hergestellt werden. Zum Beispiel kann ein Laptop mit integriertem Fingerabdruck-Swipe-Sensor in Verbindung mit einem USB-Chipkartenleser verwendet werden. Auch einige biometrische Geräte, die integrierte Kartenleser enthalten, erfordern eine solche Sensor-Leser-Zuordnung.

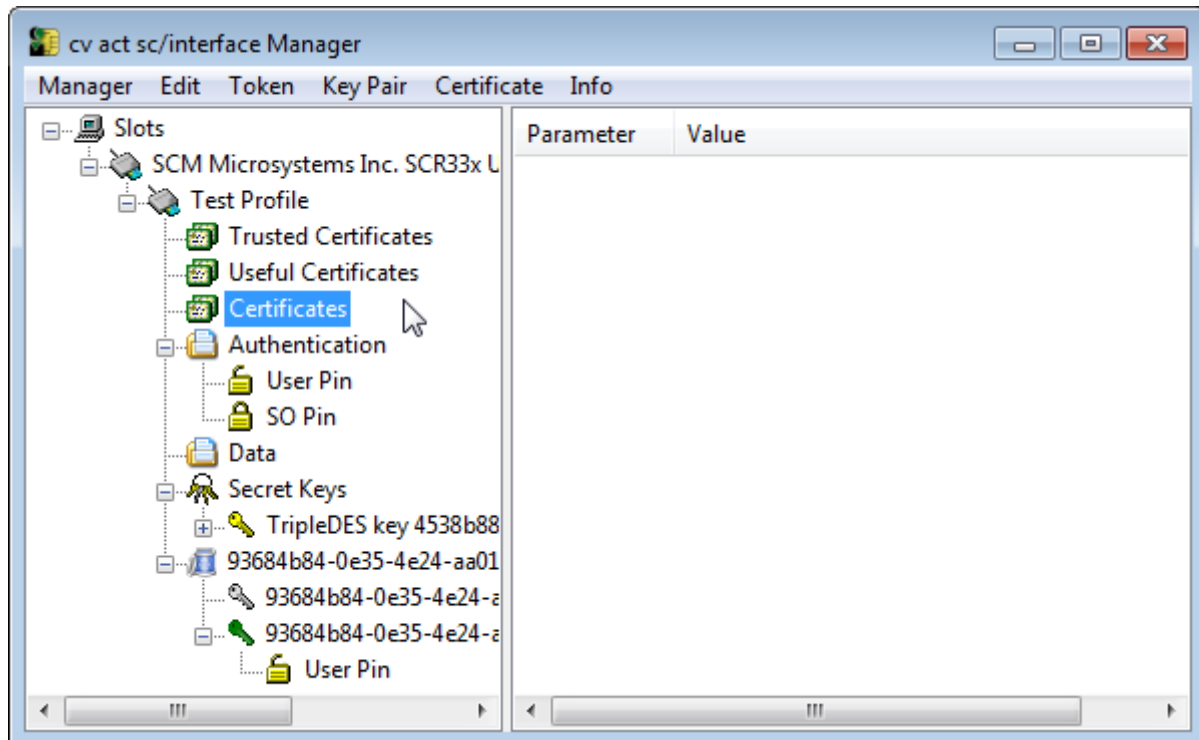
Erstellen Sie den Ordner "reader mapping" in "HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface"

1. Erstellen Sie einen String Value (RegSZ) mit dem Namen des Kartenlesers, der keine Biometrie unterstützt (z. B. "SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0").
2. Weisen Sie dem String Value den Namen des biometrischen Kartenlesers zu (z. B. "Precise Biometrics Precise 250 MC 0").

cv act sc/manager zeigt Ihnen die Namen der angeschlossenen Kartenleser an. Diese Option ist für CardOS 4.01a nicht verfügbar.

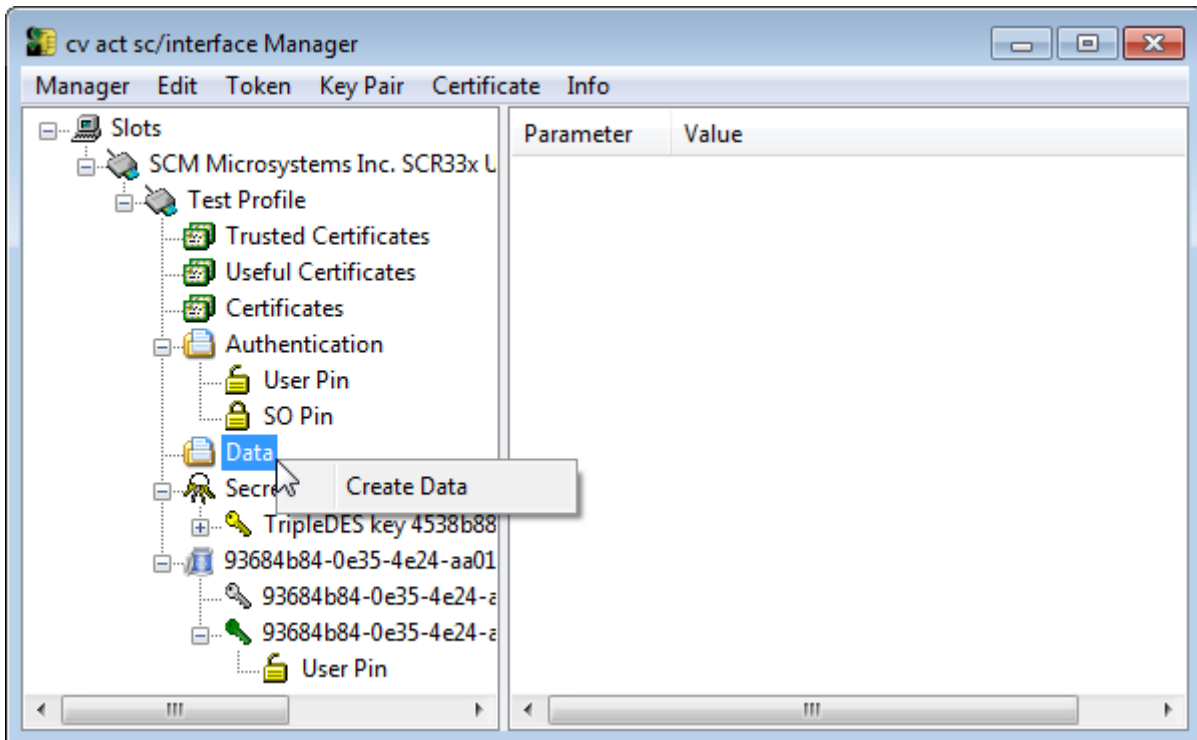
10 Weitere Funktionen

Auf einer profilierten Smartcard gibt es Verzeichnisse mit den Bezeichnungen "Trusted Certificates", "Useful Certificates" und "Certificates". Diese Verzeichnisse sind für Zertifikate gedacht, die nicht zu einem privaten Schlüssel gehören - also Wurzel- und Zwischenzertifikate, die in die jeweiligen Verzeichnisse importiert werden. Zu diesem Zweck wählen Sie den Punkt "Import Certificate " im Menü "Zertifikat" oder nutzen Sie das Kontextmenü über die rechte Maustaste.

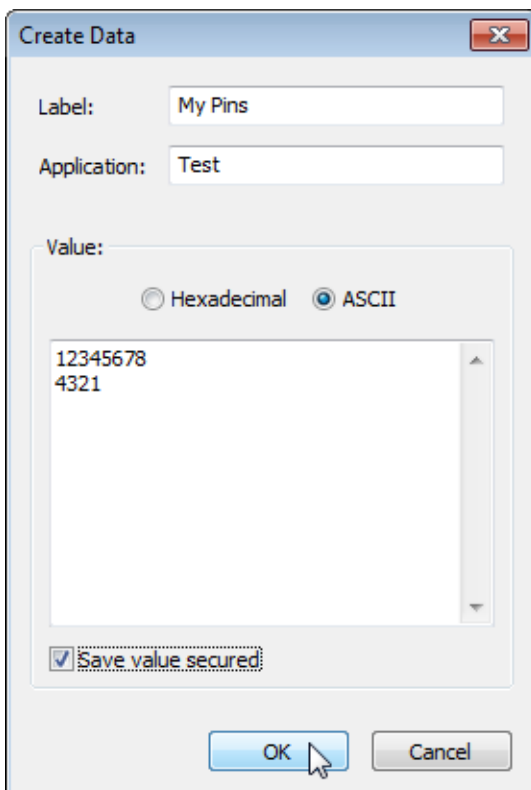


10.1 Das Data-Verzeichnis

Eine Chipkarte ist die sicherste Umgebung für einen privaten Schlüssel. Zusätzlich können andere sensible Daten auf der Smartcard gespeichert werden. Um Daten auf die Karte zu schreiben, loggen Sie sich mit der Benutzer-PIN ein und wählen Sie das Verzeichnis "Data". Nach der Eingabe von "Create Data->Bearbeiten" wird folgendes Fenster angezeigt:



Hier können Sie entweder hexadezimale Daten oder Text eingeben. Optional können die Daten durch Auswahl der Checkbox "Save value secured" gesichert werden. Nach dem Speichern können die vorhandenen Daten gelöscht, aktualisiert oder exportiert werden:



10.2 Die Funktion "Open Token"

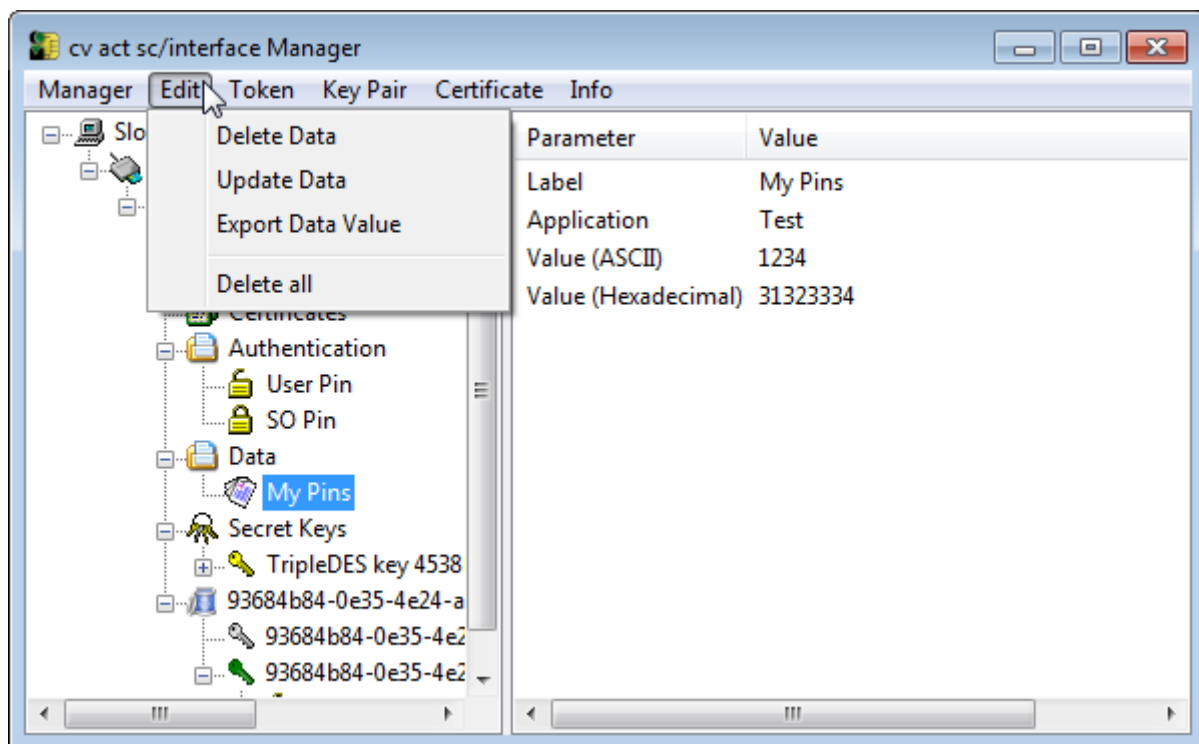
Die Funktion "Open Token" im Menü "Manager" überträgt Daten von der Smartcard auf die Benutzeroberfläche. Dies wird empfohlen, wenn Sie mit mehreren Karten oder Lesern arbeiten.

10.3 Die Funktionen "Delete all" und "Delete Certificate" / "Delete Data" / "Delete Secret key" / "Delete Container"

Sie können alle Objekte, einschließlich Schlüsseln und Zertifikaten, mit der Funktion "Delete all" im Menü "Edit" löschen.

Andere "Delete"-Funktionen bieten die Möglichkeit, bestimmte Objekte, Schlüssel oder Zertifikate zu löschen. Diese Funktionen sind über das Kontextmenü verfügbar. Klicken Sie auf das zu löschende Objekt mit der rechten Maustaste und wählen Sie den Punkt "Delete Certificate" oder "Delete Data" oder "Delete Secret Key" oder "Delete Container".

Hinweis: Die Funktion "Delete all" stützt sich auf spezifische Funktionen des Smartcard-Betriebssystems. Typischerweise unterstützen native Betriebssysteme diese Funktion, während dies bei Java-Card-basierten Betriebssystemen nicht der Fall ist. Wenn die Chipkarte diese Funktion nicht unterstützt, ist der Kontextbefehl ausgegraut und kann nicht ausgewählt werden.

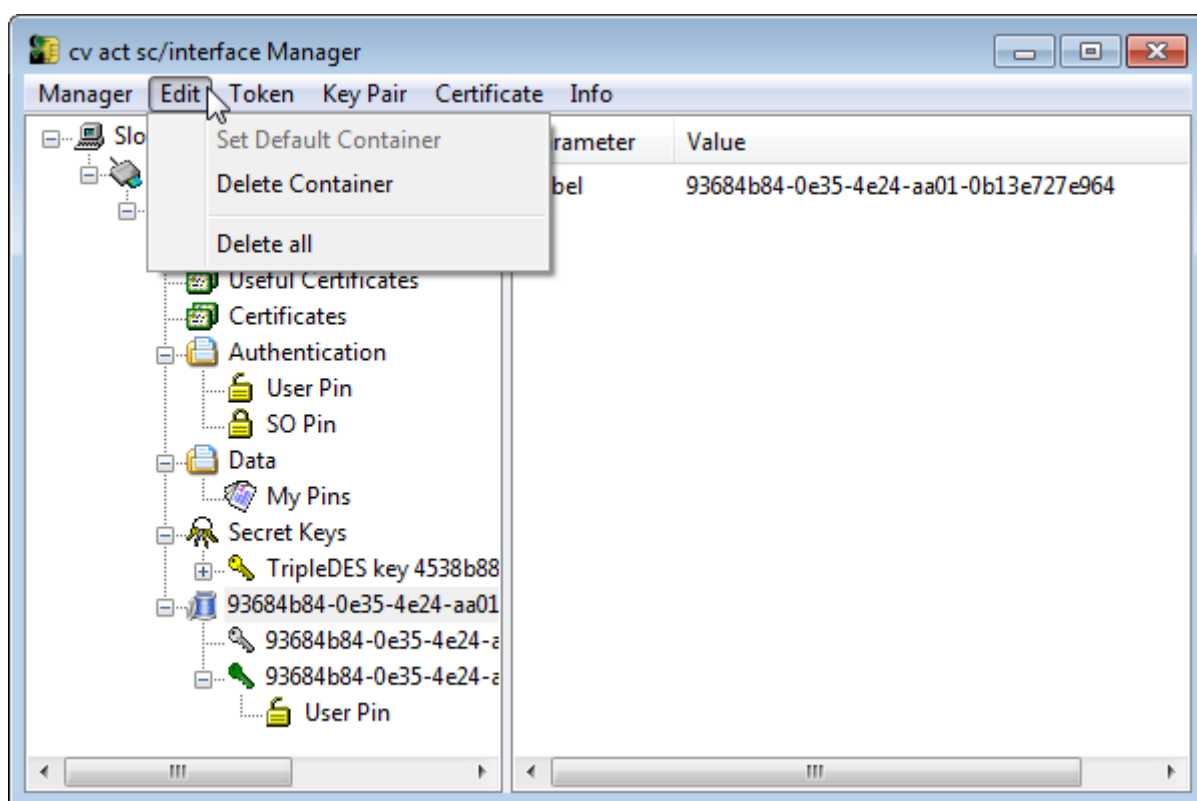


10.4 Funktion "Set Default Container"

Die Funktion "Set Default Container" im Menü "Edit" wird für die Smartcard-Anmeldung an einer Windows-2000/2003/2008 Domain über CSP benötigt.

Wenn Sie keinen Container als Default-Container angeben, wird für die Anmeldung an der Domain erste Windows-Schlüssel aus der Liste verwendet. Chipkarten mit mehreren Benutzer-Containern müssen dieses Vorgehen durch die Auswahl der gewünschten Container und einem Rechtsklick im Kontextmenü auf die Option "Set Default Container" ändern.

Die Standard-Container wird auf der Benutzeroberfläche des Administrationstools fett angezeigt:

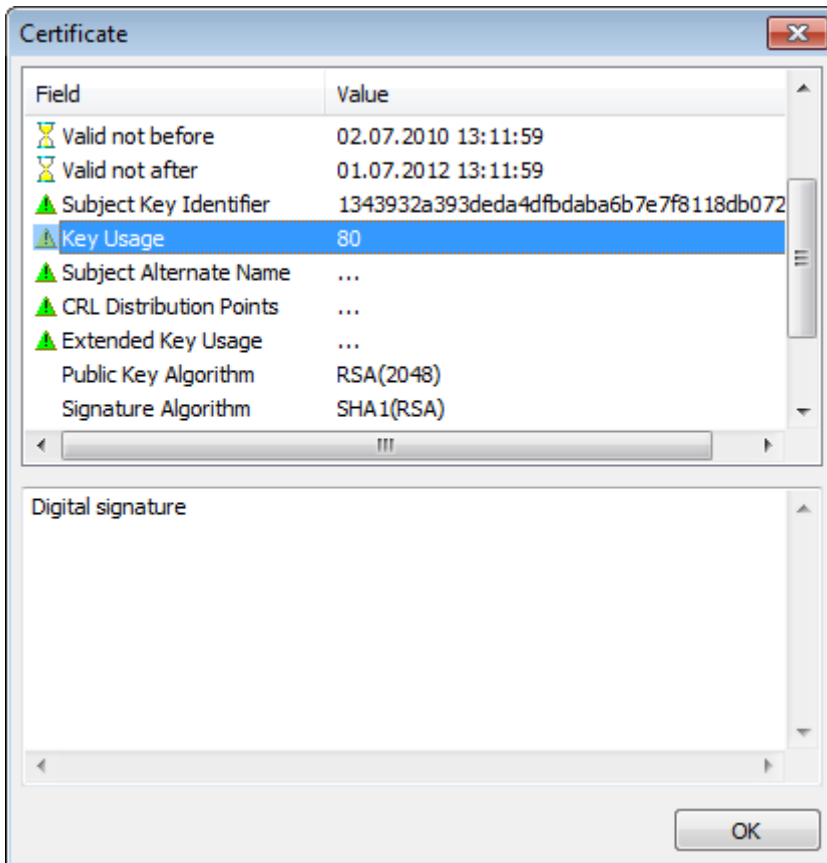


Verwendet man für die Zertifikatregistrierung einen CSP, dann wird ein Container auf der Chipkarte generiert, in dem das Zertifikat gespeichert wird. Wenn das Zertifikat für die Smartcard-Anmeldung geeignet ist, wird der Container automatisch zum Standard-Container.

10.5 Die Funktion "Show Certificate"

Um Zertifikate anzeigen zu lassen, verwenden Sie die Funktion "Show Certificate" aus dem Menü "Certificate".

Diese Funktion wird über das Kontextmenü aufgerufen. Wählen Sie das Zertifikat aus, das Sie anzeigen lassen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie "Show Certificate". Nun werden die Zertifikatsinhalte dargestellt:



10.6 Die Funktion "Export Certificate"

Wenn Sie ein Zertifikat für andere Anwendungen nutzen möchten, können Sie es von der Smartcard mit Hilfe der Funktion "Export Certificate" aus dem Menü "Certificate" exportieren. Diese Funktion kann auch über das Kontextmenü aufgerufen werden. Wählen Sie hierzu das Zertifikat mit der rechten Maustaste aus und wählen Sie den Punkt "Export Certificate".

10.7 Die Funktion "Register Certificate"

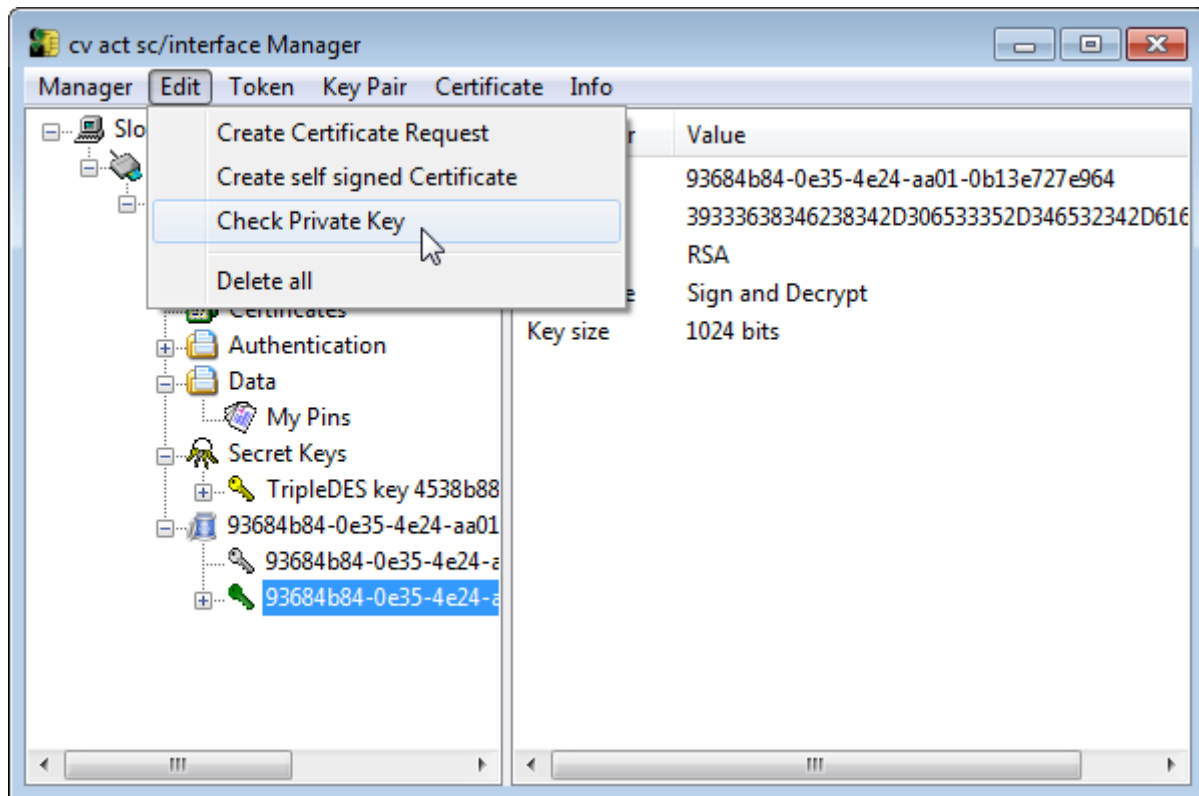
Die Funktion "Register Certificate" aus dem Menü "Certificate" installiert das Zertifikat im Windows-Zertifikatspeicher, um es für Windows-Anwendungen (z. B. Internet Explorer oder Outlook Express) zugänglich zu machen.

Diese Funktion ist auch über ein Kontextmenü aufrufbar. Wählen Sie hierzu das Zertifikat mit der rechten Maustaste aus und klicken Sie dann auf den Punkt "Register Certificate".

Die Zertifikatsregistrierung kann (mit dem Register Tool) auch automatisiert werden. Die Details hierzu werden in Kapitel 6: [Register Tool](#) beschrieben.

10.8 Die Funktion "Check Private Key"

Mit dieser Funktion können Sie erzeugte Schlüssel testen, beispielsweise zum Signieren oder Entschlüsseln. Um dies durchzuführen, loggen Sie sich das Token ein, wählen Sie den privaten Schlüssel, den Sie testen möchten, und wählen Sie die Funktion "Check Private Key" aus dem Menü "Bearbeiten". Diese Funktion ist auch über ein Kontextmenü verfügbar. Wählen Sie hierzu den privaten Schlüssel mit der rechten Maustaste und klicken Sie dann auf den Punkt "Check Private Key".



Um einen Entschlüsselungsschlüssel zu testen, geben Sie einen Text in das Feld "Plaintext" ein und klicken Sie auf "Start". Wenn der entschlüsselte Text dem Klartext entspricht, war der Test erfolgreich.

The screenshot shows the 'Check Private Key' dialog box with the 'Encrypt/Decrypt' section active. The 'Plaintext' field contains 'This is a secret'. The 'Ciphertext' field contains a long hexadecimal string: '1E21A20E9587985D8944236F82AAD23D11CCF2A6BA9DFD5'. The 'Decrypted text' field also contains 'This is a secret'. A blue 'Start' button is highlighted with a mouse cursor. Below this section is the 'Sign/Verify' section, which is currently inactive. It has a 'Hash' dropdown set to 'SHA-512', and empty fields for 'Plaintext', 'Signature', and 'Verify Result'. A 'Start' button is at the bottom right of the 'Sign/Verify' section, and a 'Close' button is at the very bottom of the dialog.

The screenshot shows the 'Check Private Key' dialog box with the 'Sign/Verify' section active. The 'Hash' dropdown is set to 'SHA-512'. The 'Plaintext' field contains 'This is also a secret'. The 'Signature' field contains a long hexadecimal string: '1607E56DDD6A305F48A52BD2864DAB1BD87449FA13A44B1'. The 'Verify Result' field contains 'True'. A blue 'Start' button is highlighted with a mouse cursor. A 'Close' button is at the bottom of the dialog.

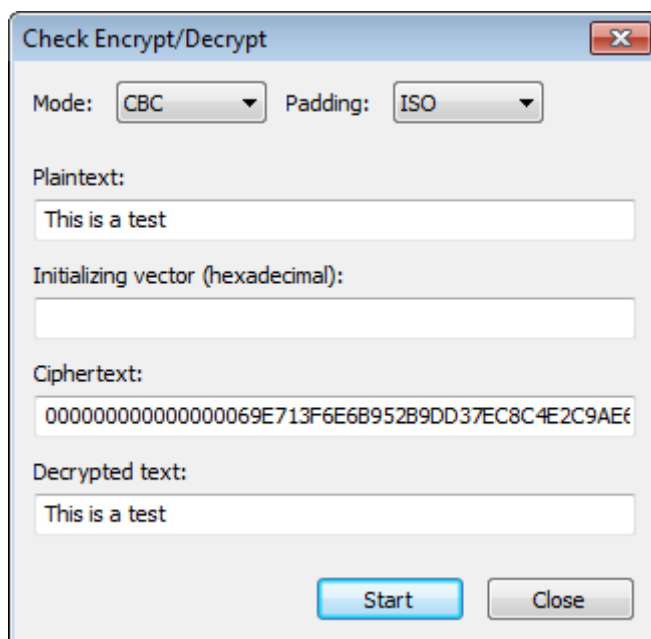
Um den Signaturschlüssel zu testen, legen Sie einen Hash-Algorithmus fest, geben Sie einen Text in das Feld "Plaintext" ein und klicken Sie auf "Start". Wenn das Feld "Verify Result" als "True" angezeigt wird, ist der Test erfolgreich verlaufen.

10.9 Die Funktion "Check Secret Key"

Mit dieser Funktion können Sie einen symmetrischen Verschlüsselungsschlüssel testen. Melden Sie sich am Token an, markieren Sie dann den geheimen Schlüssel, den Sie testen wollen, und wählen Sie die Funktion "Check Secret Key" aus dem Menü "Edit".

Es stehen zwei Blockchiffren-Betriebsarten zum Testen der Schlüssel zur Verfügung: Cipher Block Chaining (CBC) und Electronic Code Book (ECB). Als Padding-Verfahren kann entweder ISO oder PKCS#5 ausgewählt werden.

Um den Test zu starten, geben Sie einen Text in das Feld "Plaintext" ein und klicken Sie auf "Start". Sie können einen Initialisierungsvektor angeben. Lassen Sie das Feld leer, dann wird eine Folge von Nullen verwendet. Wenn der entschlüsselte Text dem Klartext entspricht, ist der Test erfolgreich verlaufen.



Check Encrypt/Decrypt

Mode: CBC Padding: ISO

Plaintext:
This is a test

Initializing vector (hexadecimal):

Ciphertext:
000000000000000069E713F6E6B952B9DD37EC8C4E2C9AE

Decrypted text:
This is a test

Start Close

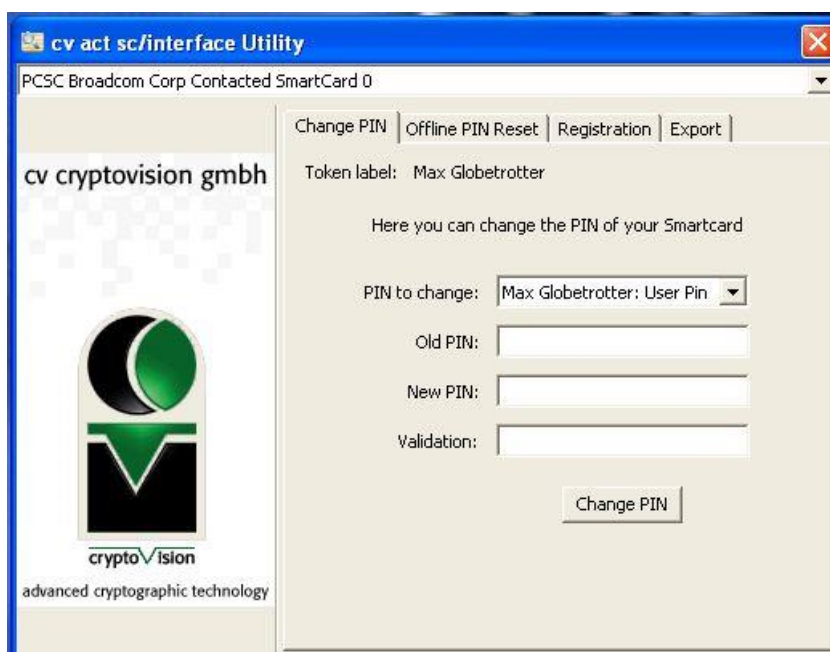
11 Das Usertool

cv act *sc/interface* bietet mit dem User Tool ein einfaches Administrationswerkzeug mit begrenztem Funktionsumfang. Das User Tool unterstützt einige typische Benutzerfunktionen: PIN-Änderung, Schlüsselregistrierung und den Export von Zertifikaten.

11.1 PIN-Änderung

Legen Sie Ihre Smartcard in den Leser und öffnen Sie cv act *sc/interface* Utility (klicken Sie dazu auf "Start" und folgen Sie dem Pfad "Programs"->"cv cryptovision"->"cv act sc/interface"->"cv act sc/interface Utility").

Um Ihre PIN zu ändern, geben Sie zuerst die alte PIN ein. Geben Sie dann eine neue PIN (doppelt) ein. Die minimale Länge der Benutzer-PIN beträgt vier Zeichen, die maximale zehn Zeichen.



Klicken Sie auf die Schaltfläche "Change PIN". Sie erhalten dann ein Fenster mit einer Bestätigung. Datum und Uhrzeit der PIN-Änderung werden gespeichert.

WICHTIG: Nach drei Fehleingaben wird die Benutzer-PIN gesperrt. Bitte wählen Sie eine PIN, die Sie sich gut merken können, die aber nicht leicht erraten werden kann. Vermeiden Sie insbesondere Geburtstage oder einfache Zahlenfolgen wie 1234 oder 1111.

Hinweis: Bei Verwendung einer Smartcard mit PKCS#15-Profil wird das Datum der letzten Änderung der Nutzer-PIN auf der Smartcard gespeichert. Wenn der Wert "00000" gespeichert ist, wird vor der Änderung eine Warnung angezeigt. Wenn die Benutzer-PIN seit der Lieferung noch nicht geändert wurde, fordert eine Pop-up-Nachricht den Benutzer auf, dies zu tun, sofern die Karte dies unterstützt.

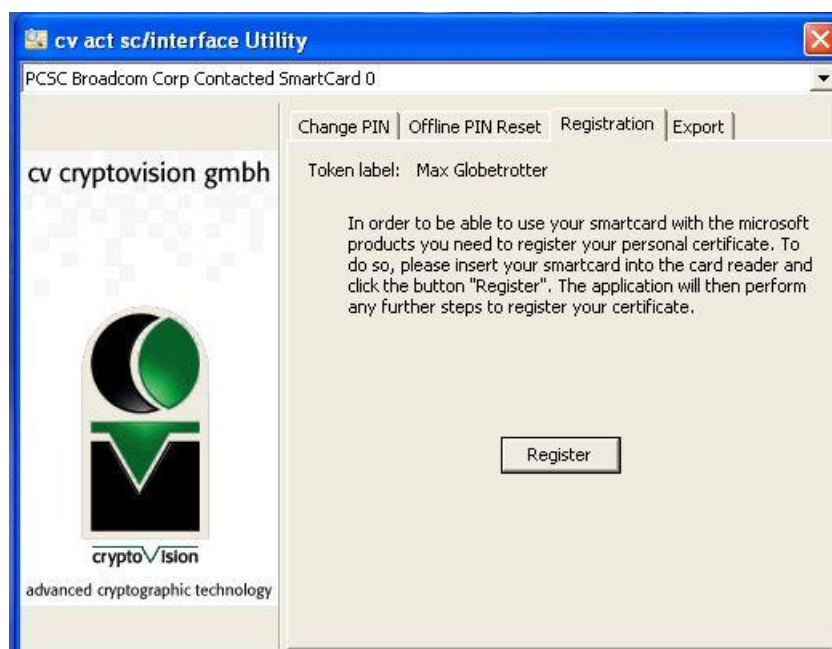
11.2 Smartcard-Registrierung

Ihre Smartcard enthält Zertifikate und Schlüssel. Diese Zertifikate müssen registriert sein, damit Anwendungen diese verwenden können. Die Registrierung eines Zertifikats/Schlüssels im Windows-Zertifikatsspeicher ermöglicht es, dass Anwendungen wie Internet Explorer, Outlook und andere sie verwenden.

WICHTIG: Die Registrierung muss nur einmal durchgeführt werden.

Legen Sie Ihre Karte in den Leser und starten Sie *cv act sc/interface* Utility. Klicken Sie hierzu auf "Start" und folgen Sie dem Pfad "Programms -> cv cryptovision -> cv act sc interface -> cv act sc/interface Utility".

Klicken Sie nun auf den Reiter "Registration" und wählen Sie "Register now". Folgen Sie den Anweisungen auf dem Monitor.



Die Registrierung ist nun abgeschlossen.

11.3 Zertifikate exportieren

"Export" ermöglicht es, Zertifikate extern in Dateien abzuspeichern. Hierzu muss ein Zertifikat markiert werden. Anschließend wird der Button "Export ..." geklickt.

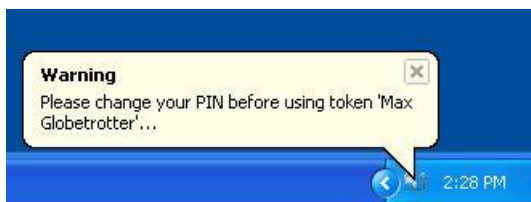


12 Das Register Tool

Wenn Sie cv act *sc/interface* unter Windows in der Admin- oder Benutzer-Version verwenden, kann das Register-Tool einige Vorgänge automatisieren.

Um Zertifikate Windows-Anwendungen, wie Internet Explorer oder Outlook Express, zugänglich zu machen, können Sie diese automatisch mit dem Register-Tool im Windows-Zertifikatsspeicher registrieren.

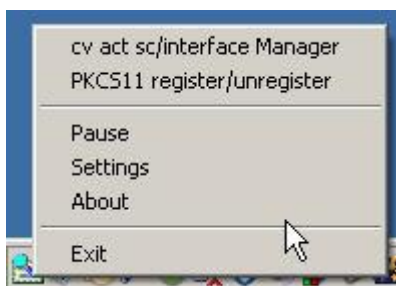
Das voreingestellte Verhalten besteht darin, dass Zertifikate automatisch registriert werden, wenn eine Karte in den Kartenleser eingelegt und das Register-Tool aktiv ist. Optional können Zertifikate beim Entfernen der Karte auch automatisch abgemeldet werden. Ist dies gewünscht, dann können Sie diese Funktion über die "Settings" aktivieren.



Sie können das cv act *sc/interface* Register Tool über das Startmenü aufrufen. Es kann außerdem automatisch gestartet werden. Die Benutzeroberfläche wird über den Infobereich aufgerufen:



Die Benutzeroberfläche bietet folgende Funktionen: Starten des Administrations-Tools cv act *sc/interface* Manager, Starten des Anwenderprogramms cv act *sc/interface* Utility, Registrieren des PKCS#11-Moduls im Netscape-Browser, Deaktivieren des Register-Tools, Ändern der Konfigurationseinstellungen, Informationen Lesen und Beenden.



oder



12.1 cv act *sc/interface* Manager und cv act *sc/interface* Utility starten

In der Admin-Version können Sie das Administrations-Tool über "Start *sc/interface* Manager" starten. In der User-Version können Sie entsprechend das cv act *sc/interface* User Tool starten. Weitere Erläuterungen zum User Tool finden Sie in den entsprechenden Abschnitten dieses Dokuments.

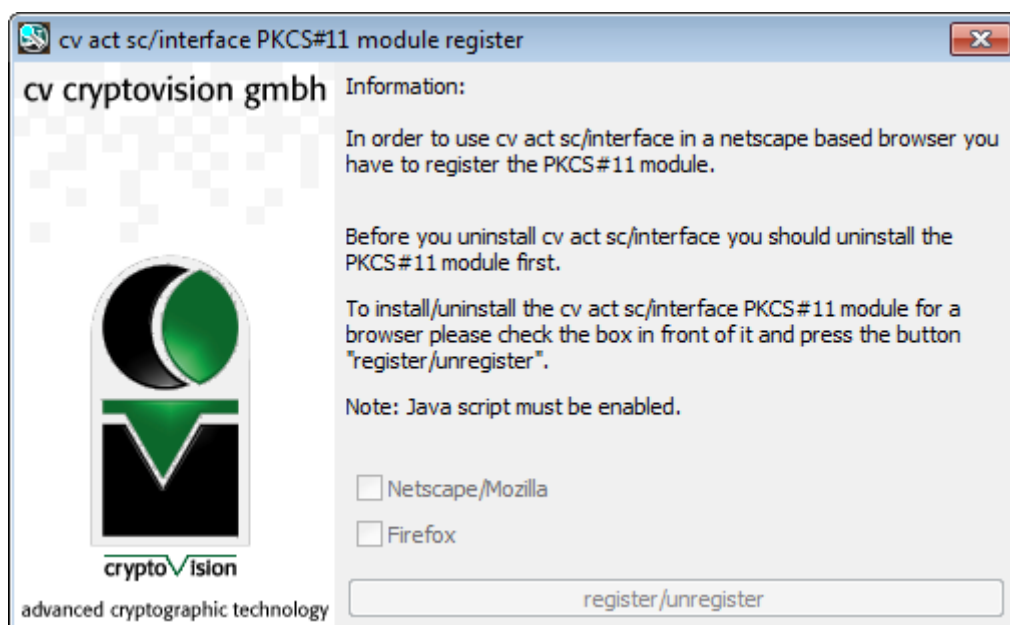
12.2 PKCS#11 registrieren und abmelden

Firefox unterstützt die PKCS#11-Schnittstelle und kann so konfiguriert werden, dass er die cv act *sc/interface* PKCS#11-Bibliotheken nutzt. Damit lassen sich Anwendungen wie gegenseitige SSL-Authentifizierung oder E-Mail-Sicherheit mit Netscape realisieren. Weitere Erläuterungen finden Sie in den Abschnitten über das PKCS#11-Modul.

HINWEIS: Mit Mozilla Firefox Version 3.6.6 wurden einige Richtlinien geändert. Es ist seitdem nicht mehr möglich, einer HTML-Seite das Registrieren und Abmelden von PKCS11-Modulen zu erlauben. Bitte führen Sie daher die Registrierung manuelle durch.

Über die Funktion "PKCS11-/ Abmelden" können Sie das Modul starten. Ein Fenster zur Registrierung und Abmeldung wird angezeigt.

Wenn Sie das cv-PKCS#11-Modul im Firefox-Browser registrieren wollen, wählen Sie den Browser und klicken Sie auf die Schaltfläche "register/unregister".



Sie werden nun gefragt, ob Sie das PKCS#11-Modul installieren wollen. Der Name und Pfad des Moduls werden angezeigt.

Für die Bestätigung der Aktion erscheint ein weiteres Dialogfeld.


Nachdem Sie auf den Button "register /unregister" geklickt haben, öffnet sich der Browser. Wenn alle Aktionen beendet sind, wird eine Bestätigung oder eine Fehlermeldung angezeigt.

Wenn Sie das Modul abmelden möchten, entfernen Sie die Aktivierung des entsprechenden Browsers und klicken Sie auf die Schaltfläche "register /unregister".

12.3 Unterbrechen und Fortsetzen

Wenn die Zertifikate auf der Smartcard nicht automatisch registriert werden sollen, kann das Register Tool unterbrochen werden. Klicken Sie dazu auf "Pause" im Pop-up-Menü des Icons im Infobereich.



Beachten Sie, dass sich das Icon nun ändert . Es zeigt nun an, dass das Register Tool unterbrochen ist. Um die Unterbrechung zu beenden, klicken Sie auf "Continue" im Pop-up-Menü des Icons im Infobereich.



12.4 Einstellungen



Wenn auf der Karte gespeicherte Zertifikate automatisch im Windows-Zertifikatsspeicher registriert werden sollen, muss die erste Checkbox ausgewählt werden (Standard).

Der "Friendly Name" wird während der Registrierung eines Zertifikats gesetzt, wenn das entsprechende Kontrollkästchen ausgewählt ist.

Um Zertifikate im Windows-Zertifikatsspeicher wieder abzumelden, wählen Sie das letzte Kästchen aus.

12.4.1 Configuration via registry

Die genannten Konfigurationseinstellungen lassen sich nicht nur über die Benutzeroberfläche, sondern auch über Einträge in der Registry-Einstellungen festlegen. Der folgende Registry Key bezieht sich auf diese Einstellungen:

[HKEY_LOCAL_USER\SOFTWARE\cv cryptovision\sc interface]

Jede Einstellung hat einen zugehörigen Binärwert.

[DeactivateRegister]

Mögliche Werte: 00, 01 (voreingestellt)

Der Wert 00 deaktiviert den automatischen Zertifikatsimport von der Smartcard in den in den Windows-Zertifikatsspeicher beim Einstecken der Karte.

[SetFriendlyName]

Mögliche Werte: 00, 01 (voreingestellt)

Der Wert 00 deaktiviert die Verwendung eines "Friendly Name" für die Zertifikatsregistrierung.

[DeactivateUnregister]

Mögliche Werte: 00, 01 (voreingestellt)

Der Wert 00 deaktiviert das automatische Entfernen der Zertifikate aus dem Windows Zertifikatsspeicher nach dem Entfernen der Karte aus dem Leser.

12.5 Exit

Beenden Sie das Register Tool mit "Exit".

13 Fortgeschrittene Konfiguration der Cryptographic Interfaces

13.1 CSP-Modul

Das Windows-Betriebssystem unterstützt kryptografische Funktionen wie Verschlüsselung oder digitale Signatur über eine kryptografische Schnittstelle (Crypto-API). Die Nutzung von Smartcards erfolgt über einen Cryptographic Service Provider (CSP). Im Rahmen der Installation von cv act *sc/interface* wird der cryptovision-CSP (abgekürzt cv-CSP) zu den vorhandenen CSPs hinzugefügt.

WICHTIG: Der cv-CSP ist eine DLL mit dem Namen "cvcsp.dll". Diese wird nach der Installation im Systemordner gespeichert, beispielsweise in WINDOWS\system32.

Mit dem cv-CSP können Sie bestimmte Programme und Funktionen mit einer Smartcard nutzen, die Windows 2000, XP, 2003, Vista, Windows 7 und 2008 bieten. Dazu gehören Outlook Express, Internet Explorer, Netzwerkanmeldung und VPN-Login.

***HINWEIS:** Im vorliegenden Dokument wird nicht beschrieben, wie Sie Ihre Microsoft-Umgebung für den Einsatz von Smartcards konfigurieren. In der Dokumentation der jeweiligen Programme finden Sie die entsprechenden Informationen. Um den Netzzugang und den VPN-Login für Smartcards zu konfigurieren, informieren Sie sich bitte über die entsprechenden Microsoft-Web-Seiten.*

Wenn Sie für die Windows-Konfiguration oder zusätzliche Software-Entwicklung Unterstützung benötigen, ist Ihnen das Beraterteam der cryptovision gerne behilflich. Kontaktieren Sie Ihren Account-Manager für weitere Informationen.

13.1.1 Allgemeines

Als minimale Anforderung muss der cv-CSP installiert sein. Dies erfolgt bei der Installation von cv act *sc/interface* automatisch. Folgendes gibt es hierbei zu beachten:

- > Wenn Sie ein Microsoft-Produkt in Verbindung mit einem CSP zum ersten Mal auf einem bestimmten Computer verwenden, müssen Sie das Zertifikat, das Sie nutzen möchten, registrieren. In Kapitel 6 "Register Tool" sowie im Abschnitt 4.9.8 "Register Certificate" erfahren Sie, wie Sie Ihre Zertifikate registrieren können.
- > Als Nutzer benötigen Sie Schlüssel und Zertifikate auf der Smartcard. Es gibt mehrere verschiedene Möglichkeiten. Die gängigsten sind folgende:
 - Generierung eines Schlüsselpaars mit zugehörigem Zertifikat direkt auf der Karte, wobei die entsprechenden Funktionen der Standard-Browser (Internet Explorer oder Netscape) genutzt werden. Dieses Vorgehen gewährleistet einen Zugriff auf die Module von cv act sc / interface, in diesem Fall also auf den cv-CSP oder das cv-PKCS#11-Modul.

- Generierung eines Schlüsselpaars mit zugehörigem Zertifikat direkt auf der Smartcard mit cv act PKIntegrated oder Microsoft Certificate Server (im "Enterprise CA" und im "Stand Alone"-Modus).
- Import vorhandener Schlüssel und Zertifikate auf die Smartcard, die von anderen Zertifizierungsstellen oder Trustcentern wurden, inklusive Bentragung der Zertifikate von einer Zertifizierungsstelle.
- Generierung eines Schlüsselpaars mit selbstsigniertem Zertifikat direkt auf der Karte mit cv act *sc/interface*. Bitte beachten Sie, dass selbstsignierte Zertifikaten nur in Umgebungen ohne PKI oder zum Testen sinnvoll sind.

Hinweis: Wenn Sie ein Zertifikat von einer Zertifizierungsstelle beantragen, werden Sie möglicherweise aufgefordert, ein Sicherheitsmodul auszuwählen, z. B. ein Token. In diesem Fall wählen Sie ein cv-Profil, also den cv-CSP oder das cv-PKCS#11-Modul. Darüber hinaus muss die Smartcard in den Kartenleser eingelegt sein, damit Zertifikate auf sie geschrieben werden können.

- > Programme müssen in geeigneter Weise konfiguriert werden, damit sie mit einer Smartcard arbeiten.
- > Programme müssen zudem konfiguriert werden, damit sie mit Schlüsseln und Zertifikaten arbeiten. Hierbei müssen die Voraussetzungen der jeweiligen Programme berücksichtigt werden. Einige Programme benötigen beispielsweise Root-Zertifikate, die in bestimmte Verzeichnisse kopiert werden müssen. Andere Programme verlangen, dass Sie Ihr Zertifikat registrieren lassen.

13.1.2 Smartcard-Login an einer Windows-2000- oder Windows-2003-Domäne

Anwender, die diese Funktion aktivieren, sollten ein fundamentals Verständnis von der Administration eines Windows-Servers haben. Folgen Sie den folgenden Schritttten:

Einrichten von Active Directory Services. Bitte achten Sie auf die korrekte Konfiguration des DNS-Servers.

1. Möglichkeit 1: verwenden Sie cv act PKIntegrated.

Weitere Informationen finden sich auf folgender Web-Seite:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q281245>

2. Möglichkeit 2: Installation der Enterprise CA und mindestens der Templates "Enrollment Agent", "Smart card Logon" und "Smart card User".

Beachten Sie außerdem, dass "Set Default Private Key" auf den privaten Schlüssel des Clients gesetzt werden muss (siehe [Kapitel 4.8](#)).

13.2 Biometrie-Login, GINA-integration

Die GINA-Integration, die Teil von cv act *sc/interface* ist, bietet Unterstützung für eine Biometrie-basierte Smartcard-Anmeldung an Windows XP. Sie unterstützt alle von cv act *sc/interface* bereitgestellten biometrischen Smart-Card-Profilen in Verbindung mit dem cv-CSP.

Wenn keine Smartcard für das Login verwendet wird, erscheint der übliche Anmeldedialog mit Username und Passwort.



Wenn eine Smartcard ohne biometrische Daten zum Login verwendet wird, erscheint der entsprechende PIN-Abfrage-Dialog.



Unterstützt die Smartcard biometrische Daten, dann sieht der Anmeldedialog wie folgt aus (Sie können für das Login auch die PIN eingeben).



Hinweis: Das-Biometrie-Login funktioniert nicht mit dem Card Minidriver.

Hinweis: Die GINA-integration wird nur von den 32-Bit-Versionen von Windows XP unterstützt.

13.3 Konfigurationsparameter

13.3.1 PIN-Cache-Modus (PIN-Cache deaktivieren)

In der Standard-Konfiguration nutzt der CSP PIN-Caching. Nach Eingabe der PIN wird diese im RAM gespeichert. Der Benutzer muss daher nicht jedes Mal die PIN eingeben, wenn der private Schlüssel auf der Smartcard genutzt wird. Wenn die Chipkarte aus dem Chipkartenleser entfernt wird, wird die PIN im RAM gelöscht.

PIN-caching kann über einen Registry Key deaktiviert werden:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]
"CSP_Disable_PIN_Cache"=dword:00000000
```

Hat der Registry Key den Wert "0", dann ist PIN-Caching aktiv. Der Wert "1" deaktiviert das PIN-Caching. Ist der Registry Key nicht vorhanden, dann wird als voreingestellter Wert "0" angenommen, und das PIN-Caching ist aktiv.

Hinweis: Bestimmte Verhaltensweisen von Microsoft Windows basieren auf einem CSP, der PIN-Caching unterstützt. Wenn "CSP_Disable_PIN_Cache" eingestellt ist, kann dies dazu führen, dass sich der CSP nicht wie in den Microsoft-Spezifikationen festgelegt verhält.

Dies bedeutet, dass Anwendungen, die ihren eigenen PIN-Eingabe-Dialog mit deaktiviertem PIN-Caching nutzen, unerwünschte Ergebnisse produzieren. Zum Beispiel könnte eine Anwendung nur eine PIN-Eingabe Dialog präsentieren, und später, es könnte die PIN an die CSP geben und erwarten, dass die CSP,

die PIN zwischenspeichern. In einem solchen Fall könnte es unmöglich sein, die CSP mit der Anwendung ermöglicht, ohne PIN-Caching.

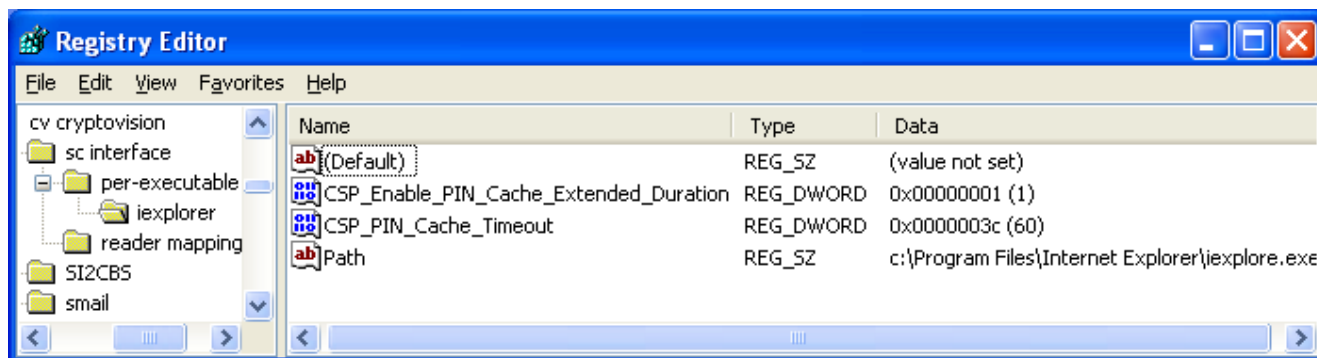
Dies ist der Fall wenn z.B. auf die Chipkarte mehrere Male während der Authentifizierungsprozedur gegriffen wird und daher die PIN mehrmals benötigt wird. Für Windows-Smartcard-Anmeldung und Windows VPN wurde dieses Verhalten getestet. Es ist nicht möglich, sich an einer Windows-Domäne oder an einer Windows VPN mit Smartcards anzumelden, wenn PIN-Cache deaktiviert ist (registry key set to "1"). In einer Umgebung, in der Smartcard-Anmeldung an einer Windows-Domäne oder an einem Windows VPN mit Smartcards verwendet wird, sollte der PIN-Cache-Modus daher nicht deaktiviert werden.

13.3.2 Extended PIN-Caching

Der cv-CSP bietet die Möglichkeit, die Dauer der PIN-Speicherung zu verlängern. Da dies nicht den Microsoft-Vorgaben entspricht und zudem die Sicherheit beeinträchtigt, muss eine solche Verlängerung über die Registry manuell konfiguriert werden.

Das Verlängern für eine bestimmte ausführbare Datei geschieht wie folgt (<Programmname> ist eine Variable):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface\per-executable\<Program name>]
```



Für eine Anwendung (z. B. Internet Explorer) müssen folgende Parameter festgelegt werden:

CSP_Enable_PIN_Cache_Extended_Duration <REG_DWORD>(0|1)

- Aktiviere (1) oder deaktiviere (0) verlängertes PIN-Caching.

CSP_PIN_Cache_Timeout <REG_DWORD>(1-N)

- Speicherzeit in Sekunden

Path <REG_SZ>

- Pfad der Anwendung:
 - vollständig, z. B. c:\Program Files\Internet Explorer\iexplore.exe
 - nur der Name der Anwendung, z. B.: iexplore.exe

Hinweis: Sie können erweitertes PIN-Caching auch global (und nicht nur für eine bestimmte ausführbare Datei) aktivieren. Hierbei ist jedoch beachten: Wenn für ein einzelnes Programm Einstellungen festgelegt sind, werden die globalen Einstellungen ignoriert. Möglicherweise müssen Sie daher die Registry-Einträge vom Hauptbaum in die Per-Executable-Einstellungen kopieren, wenn diese beachtet werden sollen.

13.3.3 Session-Modus

Ein CSP kann von verschiedenen Anwendungen gleichzeitig verwendet werden. Ist dies nicht erwünscht, können Sie die Beschränkung auf eine Anwendung mit einem Registry Key konfigurieren:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]
```

"CSP_Enable_Session_Mode"=dword:00000000

Wird der Wert "0" festgelegt, ist der CSP von mehreren Anwendungen gleichzeitig nutzbar. Beim Wert "1" steht die Karte nur derjenigen Anwendung zur Verfügung, die zuerst darauf zugreift (Session-Modus). Erst wenn diese Anwendung beendet wird, kann die Chipkarte von einer anderen aufgerufen werden. Wenn der Registry Key nicht vorhanden ist, wird der Wert "0" verwendet.

Die exklusive Nutzung einer Karte verhindert, dass andere Anwendungen über CSP, PKCS#11 oder direkt darauf zugreifen. Als Folge ist beispielsweise das Register Tool nicht nutzbar, solange eine Karte vom Internet Explorer für eine SSL-Client-Authentifizierung verwendet wird. Im Falle eines Windows-Smartcard-Logins oder eines Windows-VPN-Logins gibt es diesen Effekt ebenfalls. Andere Anwendungen können auf die Smartcard erst wieder zugreifen, nachdem diese aus dem Kartenleser entfernt und wieder eingesteckt worden ist. Dies sollten beachtet werden, wenn der Session-Modus konfiguriert wird.

14 Minidriver

Der Card Minidriver wurde für die Nutzung mit dem Microsoft Identity Lifecycle Management (ILM) / Certificate Lifecycle Management (CLM) und weitere Anwendungen entwickelt.

14.1 CMCK-Zertifizierung

Der Card Minidriver Certification Kit (CMCK) ist ein Testwerkzeug, das Funktions-, Belastungs-, Leistungs- und Zuverlässigkeitsprüfungen an einem Smartcard Minidriver durchführt. Der CMCK ruft den Microsoft BaseCSP und den Microsoft Smart Card Key Storage Provider auf und greift außerdem direkt auf die Minidriver-Methoden zu, um das korrekte Funktionieren des Mini-Card-Treibers und der zugehörigen Karte zu testen. Der CMCK verwendet den Smart Card Resource Manager, um direkt auf die Karte zuzugreifen.

Die 32-Bit- und die 64-Bit-Version des Minidrivers von cv act *sc/interface* haben alle CMCK-Tests erfolgreich bestanden. Für die Tests unter Windows XP (32 und 64 Bit-Version) wurde die Version 6.0.6001.17031 der Testsuite verwendet. Für Windows Vista (32 und 64 Bit-Version) kam die CMCK-Version 6.1.7000.0 zum Einsatz.

Weitere Informationen zu diesem Thema sind auf folgender Web-Seite verfügbar:
[http://msdn.microsoft.com/de-de/library/dd327365\(en-us\).aspx](http://msdn.microsoft.com/de-de/library/dd327365(en-us).aspx).

14.2 Minidriver-Unterstützung mit PACE

Um das Sicherheitsniveau zu erhöhen, können Sie die Übertragung der PIN zwischen Karte und Anwendung mit PACE realisieren. PACE hat den Vorteil, dass auch bei einer unsicheren PIN (d.h. mit geringer Entropie) die Daten auf dem Chip der Smartcard und während der Übertragung stark geschützt (Secure Messaging) sind, indem ein sicherer Kanal von cv act *sc/interface* zur Smartcard aufgebaut genutzt wird und eine PIN nirgendwo außerhalb der Karte zwischengespeichert wird.

Dabei ist die User-PIN vom Typ PIN-PACE, die SO-PIN vom Typ PUK-PACE und beim Minidriver gibt es noch den Admin-Key und eine Session-PIN.

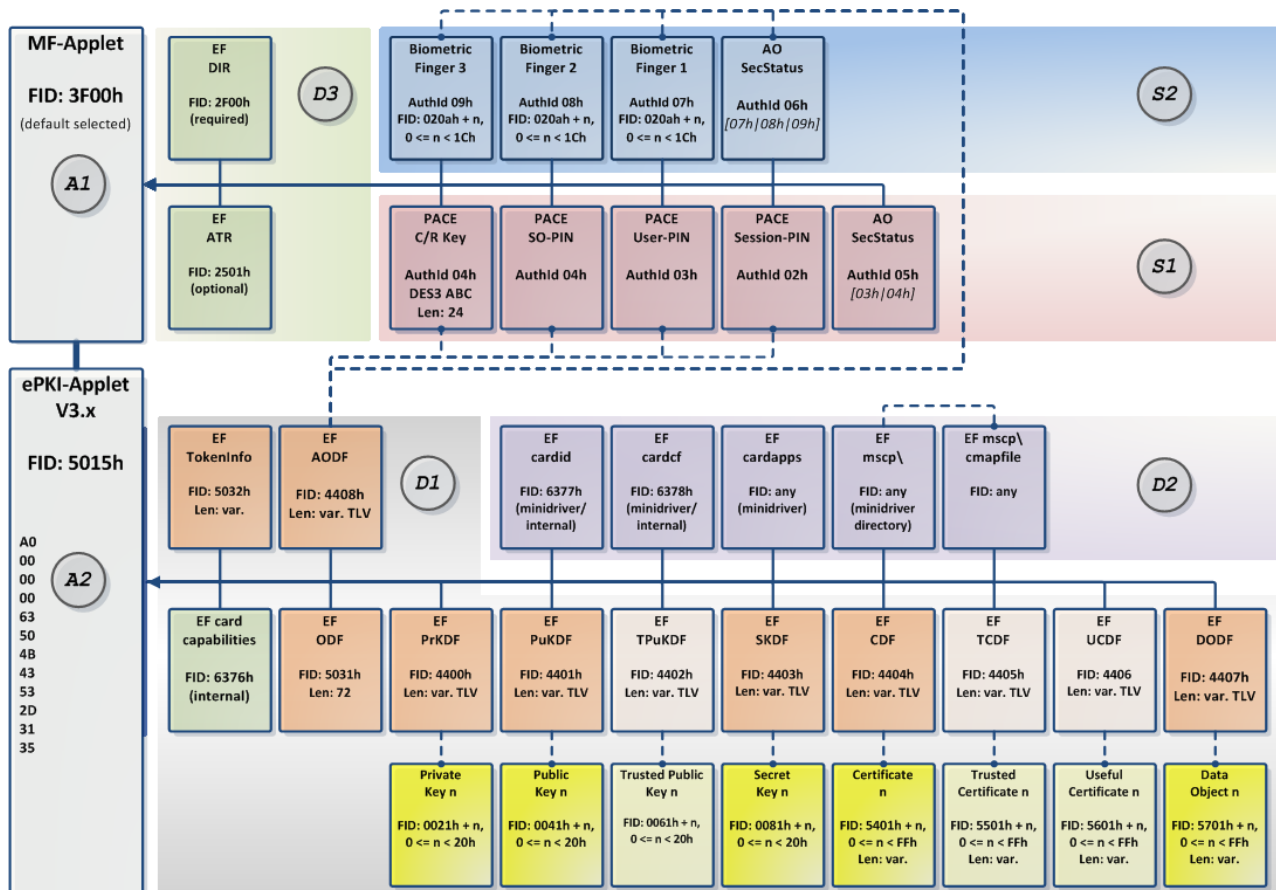
cv act *sc/interface* unterstützt nun mit PACE Session-PINs, die der Minidriver-Spezifikation Version 7.06 entsprechen. Eine Session-PIN ist eine temporäre PIN, die von der Karte generiert wird und nach der Session gelöscht wird. Wird eine Session-PIN verwendet, wird die aktuelle PIN nicht durchgereicht und der Minidriver muss die Session-PIN nutzen, um die Karte zu authentifizieren. Die Smartcard muss das Erzeugen von Session-PINs unterstützen.

Bemerkung: Durch die zusätzlichen Funktionen zur Erhöhung des Sicherheitsniveaus dauert die Nutzung der Karte ca. zwei Sekunden länger (bei Session Key noch ein wenig länger).

Weiter wird beim Challenge-Response die PACE-PIN statt dem Challenge Response Key verwendet.

PACE können Sie mit cv act *sc/interface* mit den Karten nutzen, die PACE unterstützen, d.h. die das cv act ePasslet-Suite Aplett geladen haben und zwar aus der cv act ePasslet-Suite 1.1, 1.2 und 2.0.

Zur Veranschaulichung für technischere Details finden Sie nun folgendes Diagramm:



Eine Sitzungs-PIN ist als temporäre PIN definiert. Dieser PIN-Typ wird von der Karte generiert und verfällt bei Beendigung der Sitzung. In dieser Situation wird die eigentliche PIN nicht weitergegeben und der Minidriver muss Sitzungs-PIN verwenden, um die Karte zu authentifizieren.

Karten, die die Sitzungs-PIN unterstützen, können die generierte Sitzungs-PIN zurückgeben.

15 PKCS#11-Modul

Wenn Sie eine Anwendung nutzen, die PKCS#11 unterstützt, können Sie das cv act *sc/interface*-**PKCS#11** – Modul (cv-PKCS#11) zur Ansteuerung der Smartcard verwenden. Es gibt zahlreiche Anwendungen, die diesen Standard nutzen. Dazu gehören beispielsweise VPN-Programme, Web-Browser und E-Mail-Clients.

Hinweis: An dieser Stelle wird nicht beschrieben, wie Sie bestimmte Anwendungen für die Nutzung mit PKCS#11 konfigurieren. Wenden Sie sich hierzu bitte an die entsprechenden Dokumentationen.

WICHTIG: *cv-PKCS#11 ist als DLL mit dem Namen "cvP11.dll" realisiert. Nach der Installation liegt es in einem Verzeichnis, beispielsweise in \WINDOWS\system32.*

15.1 Allgemeine Vorgehensweise

Im Folgenden werden einige allgemeine Hinweise zur Nutzung von cv-PKCS#11 gegeben. Naturgemäß muss cv-PKCS#11 installiert sein. Bei der Installation von cv act *sc/interface* ist dies automatisch der Fall.

Wenn die Anwendung das Initialisieren einer Karte nicht unterstützt (meist ist die nur bei einem Karten-Management-System der Fall), muss ein Profil generiert werden, bevor die Karte genutzt werden kann.

Als Anwender benötigen Sie Schlüssel und Zertifikate auf der Karte. Dazu gibt es mehrere Möglichkeiten. Die folgenden sind die wichtigsten:

- Generierung eines Schlüsselpaars mit zugehörigem Zertifikat direkt auf der Karte über einen Browser. Hierbei können Sie die entsprechenden Funktionen der Standard-Browser (Internet Explorer oder Firefox) nutzen. Dieses Vorgehen gewährleistet einen Zugriff auf die Module von cv act *sc/interface*, in diesem Fall also auf den cv-CSP oder das cv-PKCS#11-Modul.
- Generierung eines Schlüsselpaars mit zugehörigem Zertifikat direkt auf der Smartcard mit cv act PKIntegrated.
- Import eines vorhandenen Schlüssels und Zertifikats. Hierbei stammen Schlüssel und Zertifikat typischerweise von einer Zertifizierungsstelle.
- Generierung eines Schlüsselpaars mit selbstsigniertem Zertifikat direkt auf der Karte mit cv act *sc/interface*. Bitte beachten Sie, dass selbstsignierte Zertifikaten nur in Umgebungen ohne PKI oder zum Testen sinnvoll sind.

HINWEIS: *Wenn Sie einen Browser oder cv act PKIntegrated verwenden oder ein Zertifikat von einer öffentlichen Zertifizierungsstelle beantragen, müssen Sie möglicherweise ein Sicherheitsmodul auswählen. Bitte wählen Sie in diesem Fall das cryptovision-Profil, also cv-PKCS#11. Darüber hinaus muss die Smartcard in den Kartenleser gesteckt sein, damit Zertifikate auf sie geschrieben werden können.*

Wie in Abschnitt 6.2 beschrieben, kann das PKCS#11-Modul auf einfache Weise im Mozilla Firefox installiert werden. Verwenden Sie dazu bitte das Register Tool.

Programme müssen in der Regel konfiguriert werden, damit Sie mit Ihrer Smartcard arbeiten.

Programme müssen in der Regel konfiguriert werden, so damit Sie mit Schlüsseln und Zertifikaten arbeiten. Hier müssen Sie die Voraussetzungen der Programme berücksichtigen. Beispielsweise benötigen einige Programme Root-Zertifikate, die in bestimmten Verzeichnissen vorhanden sein müssen. In anderen Programmen müssen Sie Ihre Zertifikate registrieren.

15.2 Smartcard-Login an einem Novell eDirectory

Benutzer, die beabsichtigen, diese Funktion zu aktivieren, sollten sich gut mit dem Administrieren eines Novell-Servers auskennen und die Installationsvoraussetzungen beachten. Zusätzlich benötigen Sie für die Smartcard-Anmeldung an einem eDirectory das Produkt NMAS und die Enhanced Smart Card Login Method. Diese Funktionen sind auch im Identity Assurance-Client enthalten.

15.3 SSL-Smartcard-Authentifizierung mit Firefox / Safari

Wenn Sie Ihre Smartcard mit einem der genannten Browser verwenden wollen, registrieren Sie bitte cv-PKCS#11 in diesem Browser. Die notwendigen Funktionen werden vom Register Tool von cv act *sc/interface* bereitgestellt. Eine Beschreibung findet sich in Kapitel 6.2.

15.4 E-Mail-Sicherheit mit Smartcards für den Mozilla Messenger

Hinweise für die Verwendung von Mozilla-Produkten inklusive Screenshots zum Management der Module und Zertifikate werden im Beispiel zu Version 7 im vorhergehenden Abschnitt gegeben.

Normalerweise gibt es in den E-Mail-Fenstern Pull-Down-Fenster, in denen man festlegen kann, ob eine E-Mail verschlüsselt und/oder signiert werden sollte. Dazu gehört außerdem eine Funktion zur Verifizierung empfangener E-Mails.

15.5 cryptovision-Produkte, beispielsweise cv act *s/mail* oder cv act PKIntegrated

Alle cryptovision-Produkte können Smartcards direct ansprechen oder den cv-PKCS#11 verwenden. Wir empfehlen Letzteres.

Ausführliche Informationen zur Konfiguration der cryptovision-Produkte finden Sie in den jeweiligen Handbüchern.

15.6 Verfahren auf Basis Elliptischer Kurven (ECC)

Das PKCS#11-Modul von cv act *sc/interface* unterstützt kryptografische Algorithmen, die auf elliptischen Kurven basieren (ECC-Verfahren). Die entsprechenden Methoden sind in das PKCS#11-Modul eingebettet und können bei Bedarf mit geeigneten Parametern verwendet werden.

Hierbei ist es notwendig, dass die Anwendung, die das PKCS#11-Modul anspricht, ECC-Verfahren unterstützt. Auch die Smartcards müssen ECC-Verfahren unterstützen. Informationen über derartige Smartcards können Sie beim cryptovision-Support anfordern: support@cryptovision.com.

15.7 Initialisierung über PKCS#11

Einige Anwendungen, beispielsweise Karten-Management-Systeme, können eine Smartcard über PKCS#11 initialisieren. In einem solchen Fall ist es nicht notwendig, die entsprechende Funktion von cvManager zu verwenden.

15.7.1 Unterstützte PIN-Längen

Die folgenden minimalen und maximalen PIN-Längen sind bei der Initialisierung einer Smartcard über das PKCS#11-Modul notwendig:

	User	SO	Admin/Karte
ACOS	4/8	8/8	8/8
CardOS	4/10	8/10	10/10
JavaCard	4/10	8/10	10/10 (nur cvProfil)
StarCOS	4/8	8/8	8/8

15.7.2 Voreingestellte Werte

Ein Challenge-Response-Schlüssel und Minidriver-Kompatibilität können ebenfalls konfiguriert werden, wenn das Profil mit PKCS#11 erstellt wurde. Es gibt zwei Optionen für diese Konfiguration:

- cvP11.ini:

Diese Datei ist ein Teil von cv act *sc/interface* und muss modifiziert werden. Die Datei muss im selben Verzeichnis wie scManager.exe gespeichert werden.

- Konfiguration über die Registry:

Die folgenden Registry Keys können verwendet werden. Möglicherweise müssen sie an die jeweiligen Anforderungen angepasst werden:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]

[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface\keys]
"crkey"="0000000000000000000000000000000000000000000000000000000000000000"

[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface\profile]
"userpin"="11111111"
"cardpin"="sopin"
"#cardpin"="0987654321"
"remindpinchange"="true"
"minidriver"="true"
"virtual_slots"=dword:00000002
```

Die Konfigurationseinstellungen der Registry überschreiben die der Datei scManager.ini

Die Datei cvP11.ini enthält per Voreinstellung die folgenden Werte. Wird eines der Felder leer gelassen, werden diese Werte verwendet.

	Voreingestellter Wert
Challenge Response PIN	00
Minidriver compatible	TRUE
Card PIN	0987654321
Card PIN (für ACOS oder StarCOS)	87654321

User PIN	11111111
Remind PIN change	TRUE
Card PIN = SO PIN	deaktiviert
Virtual Slots	deaktiviert

Die folgenden Rahmenbedingungen sind zu beachten:

- Im Gegensatz zu den möglichen Vorbelegungen für das Administrationstools wird die Einstellung SO-PIN nicht genutzt. Diese Einstellung muss von der aufrufenden Anwendung über das PKCS#11-Modul übergeben werden.
- Card-PIN und SO-PIN müssen innerhalb der kartenspezifischen Grenzen gewählt werden.
- Bei Aufruf der Methode C_InitToken bewirkt die Option cardpin=sopin, dass auch als Karten-PIN die PIN verwendet wird, die von der aufrufenden Anwendung als SO-PIN übergeben wurde. Diese Option ist standardmäßig deaktiviert und sollte nur aktiviert werden, wenn dieses unbedingt notwendig ist und es sichere Aufzeichnungen o. ä. zu den verwendeten SO-PIN gibt. Solche Aufzeichnungen werden typischerweise von CMS-Systemen im Rahmen der Verwaltung von Smartcards geführt.
- Bei der Challenge Response-PIN handelt es sich im Fall der ACOS-Smartcards um einen Zwei-Schlüssel (ABA) TripleDES Schlüssel. Für alle anderen Smartcards ist es ein Drei-Schlüssel (ABC) TripleDES Schlüssel. In beiden Fällen sind dreimal Acht Hex-Bytes, für ACOS müssen die ersten und die letzten acht Bytes übereinstimmen. Für weitere Information lesen Sie bitte <http://msdn.microsoft.com/en-us/library/windows/desktop/bb468064%28v=vs.100%29.aspx>
- Für „Remind pin change“ kann der Wert false eingestellt werden. In diesem Fall wird nach dem Erstellen des Profils keine Warnung durch das Register Tool ausgegeben, wenn die Benutzer-PIN durch den Benutzer nicht geändert wird.
- Seit cv act *sc/interface* 4.0.1 können auch Smartcards mit Java-Betriebssystem mit einem Profil versehen werden, die nicht die Java Fixed Keys verwenden. In diesem Fall müssen die entsprechenden Schlüssel in die Datei Datei cvP11.ini eingetragen werden. Es können beliebig viele Schlüsselsätze hinzugefügt werden, wobei ein Schlüsseldatensatz wie folgt aufgebaut sein muss:

```
[javacard]
# VISA-Fixed Keyset
#      enc      mac      kek
keyset=4041...4e4f,4041...4e4f,4041...4e4f
keyset=...
```

15.8 Identifikation einer Smartcard

Bei der Verwendung von Smartcards und Zertifikaten muss das zu verwendende Zertifikat bzw. die zu verwendende Smartcard identifiziert werden. Für diese Identifizierung gibt es keine standardisierte Vorgehensweise, d. h. verschiedenen Anwendungen verwenden unterschiedliche Identifizierungsmerkmale.

Neben den Mechanismen, die cv act *sc/interface* in der Standardkonfiguration zur Verfügung stellt (u. a. ATR, Label, Zertifikat), kann mit der folgenden Konfiguration der Parameter Modell bzw. ModellID als weiteres Identifizierungsmerkmal zur Verfügung gestellt werden. Diese Konfiguration ist z. B. für die unterstützten Anwendungen der Firma Secude notwendig, falls cv act *sc/interface* mit A.E.T. SafeSign Profil genutzt wird.

Die Konfiguration kann alternativ in der Registry oder durch Einträge in cvP11.ini vorgenommen werden. Unten findet sich beispielhaft die Konfiguration für Smartcards mit dem Betriebssystem StarCOS 3.0.

15.8.1 Konfigurationsdatei

In der Datei cvP11.ini müssen die folgenden Einträge hinzugefügt werden:

```
[pkcs11]
# cardid (historical bytes) fixed CK_TOKEN_INFO.model mapping
# model=cardid,model[1-16]
  model=80670412b003030000,3384110107000000      # G&D STARCOS 3.0 contactless
  model=80670412b00303000008105,3384110107000000 # G&D STARCOS 3.0
  model=c808,disabled                            # Disable standard CardOS 4.3B
```

Der Begriff „cardid“ ist in diesem Zusammenhang nicht zu verwechseln mit der Anzeige der Card ID für eine Smartcard mit Minidriver-kompatiblen Profil im cv act *sc/interface* Manager. Bei letzterem handelt es sich um die GUID entsprechend der Microsoft Minidriver Spezifikation.

15.8.2 Verwendung der Registry

Die folgenden Registry-Einträge haben dieselbe Auswirkung:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface\pkcs11\model]
"80670412b003030000"="3384110107000000"
"80670412b00303000008105"="3384110107000000"
```

Anhang A: Referenz für Entwickler

In diesem Anhang finden Sie nähere Angaben bzgl. der unterstützten Funktionen des PKCS#11-Standards, eine Kurzbeschreibung einzelner Funktionen und eine Auflistung der Objekte und Mechanismen. Diese Informationen sind nützlich und notwendig für Anwendungsentwickler, die eigene Anwendungen entwickeln, die das PKCS#11-Modul unterstützen.

Funktionen nach PKCS#11-Standard

cv act *sc/interface* unterstützt den PKCS#11-Standard nach Version 2.20. Im Folgenden werden die Funktionen nach PKCS#11-Standard aufgelistet, die von cv act *sc/interface* nicht oder abweichend unterstützt werden.

Folgende Funktionen werden momentan nicht unterstützt

`C_VerifyRecoverInit`

`C_VerifyRecover`

`C_SeedRandom`

Folgende Funktionen werden nur mit Abweichungen zum Standard unterstützt:

`C_Initialize`

`C_OpenSession`

`C_GetObjectSize`

`C_GetTokenInfo`

`C_CreateObject`

`C_GenerateKeyPair`

Kurzbeschreibung einzelner Funktionen

`C_Initialize`

Parameter:	<code>CK_VOID_PTR_PTR</code>	<code>CinitArg</code>
Beschreibung:	Library wird initialisiert. Slots werden erstellt. Eingelegte Karten werden gelesen.	
Abweichungen:	<code>CinitArg</code> wird im Format <code>CK_C_INITIALIZE_ARGS</code> erwartet. Aus diesen werden die Flags ausgelesen. Insbesondere <code>CKF_LIBRARY_CANT_CREATE_OS_THREADS</code> welches über Multithreading entscheidet. Der Rest wird ignoriert.	

Wird C_Initialize mehrmals aufgerufen wird CKR_CRYPTOKI_ALREADY_INITIALIZED zurückgegeben. Die Anzahl wird mitgezählt.

C_OpenSession

Parameter:	CK_SLOT_ID	slotID
	CK_FLAGS	flags
	CK_VOID_PTR	pApplication
	CK_NOTIFY	Notify
	C_SESSION_HANDLE_PTR	phSession

Beschreibung: Öffnet eine neue Session auf den Slot.

Abweichung: Notify und pApplication werden ignoriert und sollten auf NULL_PTR gesetzt werden. Sessions können nur geöffnet werden, wenn eine Karte eingelegt ist.

Besonderheit: Ist eine Session geöffnet und wird dann die Karte entfernt, geben alle Sessions auf den Slot CKR_DEVICE_REMOVED zurück. Gibt es einen Fehler mit CKR_DEVICE_REMOVED, CKR_TOKEN_NOT_RECOGNIZED oder CKR_TOKEN_NOT_PRESENT wird automatisch ein pauseAllSessions auf diesem Slot erzeugt. Wenn eine pausierte Session wieder genutzt wird, wird diese Session automatisch wieder geöffnet.

Wird eine Karte im Slot eingelegt oder entfernt, so stellt dieses ein Event da (siehe C_WaitForSlotEvent). Wird die C_OpenSession aufgerufen, wird das Event beendet, auch wenn die Karte rausgenommen wurde und C_OpenSession CKR_TOKEN_NOT_PRESENT zurückgibt.

C_GetObjectSize

Parameter:	CK_SESSION_HANDLE	hSession
	CK_OBJECT_HANDLE	hObject
	CK_ULONG_PTR	pulSize

Beschreibung: Es wird die Größe eines Objektes zurückgegeben

Abweichungen: Die zurückgegebene Größe ist die minimale Größe des Objektes, d. h. es enthält nicht die Größe von Extra-Attributen wie Label oder ID. Die Größe von privaten Objekten sind Standardwerte.

C_GetTokenInfo

Parameter:	CK_SLOT_ID	slotID
	CK_TOKEN_INFO_PTR	pInfo
Beschreibung:	Gibt Informationen über die Karte im Slot zurück. Ist keine Karte eingelegt, wird CKR_TOKEN_REMOVED zurückgegeben.	
Besonderheit:	Wird eine Karte in den Slot eingelegt oder entfernt, so stellt dieses ein Event dar (siehe C_WaitForSlotEvent). Wird C_GetTokenInfo aufgerufen, wird das Event beendet, auch wenn die Karte rausgenommen wurde und C_GetTokenInfo CKR_TOKEN_NOT_PRESENT zurückgibt. Die Seriennummer, die in CK_TOKEN_INFO zurückgegeben wird, ist nicht die Hardware Seriennummer der Karte. Wenden Sie sich kurz per e-Mail an support@cryptovision.com und fordern die Dokumentation der PKCS#11-Modul-Erweiterungen an.	

C_CreateObject

Parameter:	CK_SESSION_HANDLE	hSession,
	CK_ATTRIBUTE_PTR	pTemplate,
	CK_ULONG	ulCount,
	CK_OBJECT_HANDLE_PTR	phObject
Beschreibung:	Erzeugt anhand des Templates Objekte.	
Abweichung:	C_CreateObject für RSA Schlüssel („Import von RSA Schlüsseln“) weicht stark von der normalen Verwendung ab. Spezielles Verhalten der cv act sc/interface Implementierung: <ol style="list-style-type: none">Der Import nur des öffentlichen Schlüssels wird nicht unterstützt. C_GenerateObject für ein entsprechendes Template (d.h. mit Eintrag CKA_CLASS = CKO_PUBLIC_KEY) liefert CKR_FUNCTION_NOT_SUPPORTED.Beim Erzeugen des privaten Schlüssels muss neben Modulus und privatem Exponenten auch immer prim_p und prime_q (CKA_PRIME_1 und CKA_PRIME_2) sowie der öffentliche Exponent (CKA_PUBLIC_EXPONENT) mit angegeben werden.Es werden immer beide (privater und öffentlicher) Schlüssel erzeugt: der eigentliche C_CreateObject-Aufruf erfolgt für ein Template für einen privaten Schlüssel (CKA_CLASS = CKO_PRIVATE_KEY), der öffentliche Schlüssel wird aber gleichzeitig bei dem C_CreateObject-Aufruf mit erzeugt. phObject zeigt auf den	

privaten Schlüssel, man erhält nicht direkt ein Handle für den öffentlichen Schlüssel.

4. Man kann über das Template keine weiteren Attribute des öffentlichen Schlüssel (z.B. CKA_VERIFY und CKA_ENCRYPT) setzen, entsprechende Einträge in dem Template werden ignoriert.

5. Um Flags für den öffentlichen Schlüssel zu setzen muss man diesen nach der Erzeugung manuell suchen (C_FindObject anhand z.B. CKA_ID) und ggf. mit C_SetAttributes gewünschte Attribute setzen.

Objekte

cv act *sc/interface* unterstützt eine weite Auswahl der in PKCS#11 vorgesehenen Objekte. Bei einigen der Objektattribute gibt es aber Abweichungen vom Standard in ihrer Handhabung. Diese sollen im Folgenden aufgeführt werden.

Bemerkung: Alle PKCS#11-Funktionen, die ein Objekt erzeugen, erwarten einen Parameter der Form „CK_ATTRIBUTE_PTR pTemplate“. Dieser Parameter wird genutzt, um die verschiedenen Attribute des zu erzeugenden Objekts festzulegen. Wenn im Folgenden von „dem Template“ die Rede ist, ist stets dieser Parameter gemeint.

Bemerkung: Für alle Objekte gilt: wird CKA_TOKEN in dem Template nicht gesetzt, so wird als Default-Wert CK_FALSE verwendet, es wird also nur ein Session-Objekt erzeugt. Soll das Objekt auf die Karte geschrieben werden, so muss CKA_TOKEN explizit in dem Template auf CK_TRUE gesetzt werden.

CKO_CERTIFICATE (CKC_X_509)

cv act *sc/interface* unterstützt Zertifikate im X.509 Format. Dabei gibt's es für einige Attribute folgende Abweichungen:

- CKA_URL: Dieses Attribut wird nicht unterstützt. Dementsprechend muss CKA_VALUE immer gesetzt sein.
- CKA_VALUE: Da CKA_URL nicht unterstützt wird, muss dieses Attribut immer gesetzt sein, ansonsten gibt der entsprechende C_CreateObject-Aufruf die Fehlermeldung CKR_TEMPLATE_INCOMPLETE zurück.
- CKA_SUBJECT: Setzt man dieses Attribut in dem Template nicht explizit, so wird es automatisch aus dem Subject-Feld des in CKA_VALUE enthaltenen Zertifikats erzeugt.
- CKA_ISSUER: Setzt man dieses Attribut in dem Template nicht explizit, so wird es automatisch aus dem Issuer-Feld des in CKA_VALUE enthaltenen Zertifikats erzeugt.
- CKA_SERIAL_NUMBER: Setzt man dieses Attribut in dem Template nicht explizit, so wird es automatisch aus der Seriennummer des in CKA_VALUE enthaltenen Zertifikats erzeugt.

C_GenerateKeyPair

Parameter:	CK_SESSION_HANDLE	hSession,
	CK_MECHANISM_PTR	pMechanism,
	CK_ATTRIBUTE_PTR	pPublicKeyTemplate,
	CK_ULONG	ulPublicKeyAttributeCount,
	CK_ATTRIBUTE_PTR	pPrivateKeyTemplate,
	CK_ULONG	ulPrivateKeyAttributeCount,
	CK_OBJECT_HANDLE_PTR	phPublicKey,
	CK_OBJECT_HANDLE_PTR	phPrivateKey

Beschreibung: Erzeugt ein öffentlicher Schlüssel / privater Schlüssel Paar.

Abweichung: Im Gegensatz zu anderen Implementierungen müssen die folgenden Attribute immer zusätzlich zu den obligatorischen Attribute angegeben werden.

1. Public key template: CKA_ENCRYPT und CKA_VERIFY.
2. Private key template: CKA_DECRYPT und CKA_SIGN.
3. Um nur einen Signaturschlüssel zu erzeugen, setzt man CKA_ENCRYPT und CKA_DECRYPT auf false, aber CKA_VERIFY und CKA_SIGN auf true.

RSA Key Pair (CKO_PRIVATE_KEY and CKO_PUBLIC_KEY with CKK_RSA)

Es gibt 2 verschiedene PKCS#11-Funktionen, um ein RSA-Schlüsselpaar zu erzeugen: C_GenerateKeyPair („Schlüsselerzeugung“) und C_CreateObject („Import eines Schlüsselpaars“). Die cv act sc/interface Implementierung von der C_CreateObject Funktion unterscheidet sich stark vom Standardgebrauch der RSA-Schlüsselerzeugung. Lesen Sie auch im vorherigen Kapitel „[Kurzbeschreibung einzelner Funktionen](#)“. In beiden Fällen wird immer das komplette Schlüsselpaar erzeugt, bestehend aus beiden Schlüsseln (öffentlich und privat). Nur einen einzigen Schlüssel zu erzeugen, sei es der private oder der öffentliche Schlüssel, wird von cv act sc/interface nicht unterstützt.

- **C_CreateObject:** Ob das Schlüsselpaar auf der Karte gespeichert wird, wird durch die CKA_TOKEN-Einstellung des privaten Schlüssels bestimmt. Setzt man in dem Template des privaten Schlüssels CKA_TOKEN = CK_TRUE so wird dadurch auch automatisch der zugehörige öffentliche Schlüssel auf der Karte gespeichert.
- **C_GenerateKeyPair:** Diese Funktion hat 2 Templates als Parameter, einen für den öffentlichen und einen für den privaten Schlüssel. Die CKA_TOKEN Einstellungen in beiden Templates müssen gleich sein – falls vorhanden.

Mechanismen

cv act *sc/interface* unterstützt verschiedene Mechanismen, wie in der folgenden Tabelle gezeigt wird.

Bemerkung:

Mechanismen, die hier nicht explizit erwähnt werden, werden auch nicht unterstützt. Speziell unterstützt cv act *sc/interface* nicht die Mechanismen aus PKCS#11 v2.20 amendments (1-3).

Mechanism	Functions						
	Encrypt / Decrypt	Sign / Verify	SR / VR	Digest	Generate Key	Wrap / Unwrap	Derive
CKM_RSA_PKCS_KEY_PAIR_GEN					X		
CKM_RSA_PKCS	X	X				X	
CKM_RSA_X_509	X	X				X	
CKM_MD2_RSA_PKCS		X					
CKM_MD5_RSA_PKCS		X					
CKM_SHA1_RSA_PKCS		X					
CKM_SHA224_RSA_PKCS		X					
CKM_SHA256_RSA_PKCS		X					
CKM_SHA384_RSA_PKCS		X					
CKM_SHA512_RSA_PKCS		X					
CKM_RIPEMD128_RSA_PKCS		X					
CKM_RIPEMD160_RSA_PKCS		X					
CKM_EC_KEY_PAIR_GEN (CKM_ECDSA_KEY_PAIR_GEN)					X		
CKM_ECDSA		X					

CKM_ECDSA_SHA1		X					
CKM_DES_KEY_GEN					X		
CKM_DES_ECB	X						
CKM_DES_CBC	X						
CKM_DES_CBC_PAD	X						
CKM_DES3_KEY_GEN					X		
CKM_DES3_ECB	X						
CKM_DES3_CBC	X						
CKM_DES3_CBC_PAD	X						
CKM_MD2				X			
CKM_MD5				X			
CKM_SHA_1				X			
CKM_SHA224				X			
CKM_SHA256				X			
CKM_SHA384				X			
CKM_SHA512				X			
CKM_RIPEMD128				X			
CKM_RIPEMD160				X			

Anhang B: Debug

PKCS#11 Logger (win)

Beschreibung: Loggt alle PKCS11 Funktionsaufrufe in eine Datei. Ein Eintrag enthält den Funktionsnamen, die Parameter vor und nach dem Funktionsaufruf und das Ergebnis der Funktion. Private Informationen sind verdeckt durch einen statischen String „[-----]“, so dass nur die Länge lesbar ist.

Einstellungen: Die Einstellungen werden in der Registry unter HKEY_LOCAL_MACHINE, Software\cv cryptovision\sc interface.

Der PKCS11_LogFile_name ist der Name des Logfiles.

LogFile_mode kann 0 für off oder 1 für on sein.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]
    "PKCS11_LogFile_name"="c:\cvPKCS11_log.txt"
    "LogFile_mode"=dword:00000064
```

Besonderheit: Eine Debug-Library loggt private Information als Klartext.

CSP Logger (win)

Beschreibung: Loggt alle CSP Funktionsaufrufe in eine Datei. Ein Eintrag enthält den Funktionsnamen, die Parameter vor und nach dem Funktionsaufruf und das Ergebnis der Funktion. Private Informationen sind verdeckt durch einen statischen String „[-----]“, so dass nur die Länge lesbar ist.

Einstellungen: Die Einstellungen werden in der Registry unter HKEY_LOCAL_MACHINE, Software\cv cryptovision\sc interface.

Der CSP_LogFile_name ist der Name des Logfiles.

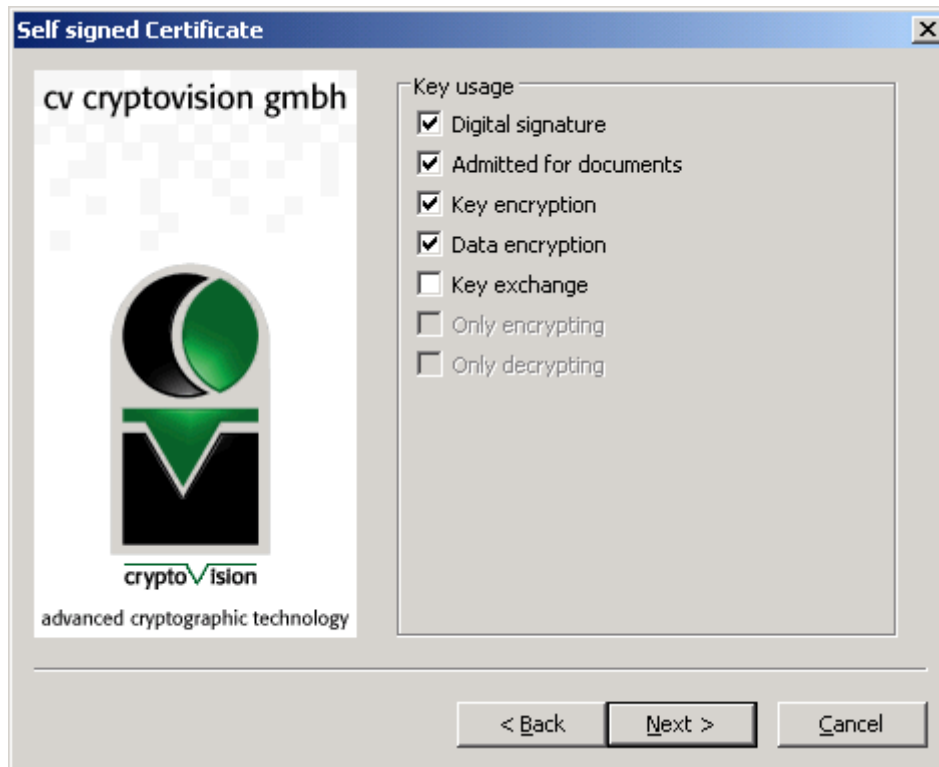
LogFile_mode kann 0 für off oder 1 für on sein.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\cv cryptovision\sc interface]
    "CSP_LogFile_name"="c:\cvCSP_log.txt"
    "LogFile_mode"=dword:00000064
```

Besonderheit: Eine Debug-Library loggt private Information als Klartext.

Anhang C: Zertifikatsattribute (Key Usage)

Die einzelnen Verwendungen eines Schlüsselpaars sehen Sie am Beispiel der Erstellung eines selbstsignierten Zertifikats:



Bemerkung; Diese Funktionalität ist nur für Testzwecke geeignet.

Im Einzelnen haben diese folgende Bedeutung:

1. Digitale Signatur: Hiermit können Sie digitale Signaturen prüfen (außer die für unter zwei genannten Zwecken) z.B. zur Authentifizierung.
2. Zugelassen für Dokumente: Hiermit können Sie digitale Signaturen verifizieren, die zur Prüfung der Verbindlichkeit von Dokumenten dienen (außer bei Signaturen von Zertifikaten und Sperrlisten von CA).
3. Schlüsselverschlüsselung: Verschlüsselung von Schlüsseln zum Zwecke des Transports von diesen.
4. Datenverschlüsselung: Verschlüsselung von Daten zum Zwecke des Transports, aber nicht von Schlüsseln.
5. Schlüsselaustausch: Verwendung des Schlüssels zur Vereinbarung von Schlüsseln, z.B. für einen Diffie-Hellman-Schlüssel.

Information / Export Restrictions

Please observe!

The product delivered to you is liable to export control. Please observe the legal requirements of specific countries. For export out of the EU an export approval is necessary. To obtain such approval contact

cv cryptovision GmbH

Munscheidstr. 14

45886 Gelsenkirchen

Germany

© Copyright cv cryptovision GmbH 2002-2013

All rights reserved. Without the express prior written consent of cryptovision you must not distribute, edit or translate copyrighted material.

Trade Mark

All mentioned software and hardware names are in most of the cases trademarks and are liable to legal requirements.