



Anwendung der Smartcards und deren Zertifikate innerhalb Mozilla Firefox

T-Systems International GmbH

Version 1.0
Stand 29.06.11



Impressum

Herausgeber

T-Systems International GmbH
Untere Industriestraße 20
57250 Netphen

Version	Stand
1.0	29.06.11

Kurzinfo

Anwendung der Smartcards und deren Zertifikate innerhalb Mozilla Firefox

Vorwort

T-Systems übernimmt keine Garantie dafür, dass die in der Anleitung bereitgestellten Informationen vollständig, richtig und in jedem Fall aktuell sind. T-Systems hat bei der Erstellung dieser Anleitung die aktuelle Architektur diverser Softwareanwendungen berücksichtigt. Diese kann sich ändern. Solche Änderungen liegen allein im Ermessen des Herstellers. Auf keinen Fall haftet T-Systems für Schäden, die im Zusammenhang mit der Nutzung der Anleitung stehen, die auf dieser Website zugänglich ist.

Zur Verwendung der TCOS-Chipkarte muss zuerst einmal die Karten-PIN aktiviert werden, hierzu kann das Card Management-Tool von den TeleSec-Seiten verwendet werden.

Inhaltsverzeichnis

1.1) Einbinden eines Kryptographie Moduls: Treiber Installation.....	5
1.2) Einbinden eines Kryptographie Moduls: Einbinden in Mozilla Firefox.....	6
2.1) Importieren von Zertifikaten.....	8

Einbinden eines Kryptographie-Moduls

- 1.1) Um ein Kryptographie-Modul einzubinden, müssen Sie zuerst den Treiber von www.telesec.de herunterladen und installieren. Wenn Sie dies zuvor schon erledigt haben, können Sie direkt zu Punkt 2 springen.

Besuchen Sie die Webseite www.telesec.de und klicken Sie im Untermenü „TCOS-Smartcards“ auf „Schnittstellen und Treiber (PKCS#11 und Microsoft Card Modul)“:

The screenshot shows the T-Systems website with the following elements:

- Header:** T-Systems logo and navigation links (Startseite, Kontakt).
- Navigation:** Signaturkarte (PKS), ServerPass, Shared Business CA, **TCOS-Smartcards**, OneTimePass, PKI, E-Mail Encryption Gateway.
- Left Sidebar:**
 - Public Key Service
 - ServerPass
 - Shared Business CA
 - TCOS-Smartcards** (highlighted)
 - OneTimePass
 - Public Key Infrastructure
 - E-Mail Encryption Gateway
- Main Content:**

Smart Card Technology

Die Erzeugung hochwertiger kryptografischer Schlüssel und deren sichere Aufbewahrung sind technologische und organisatorische Probleme. Als Lösungsangebot wurde bei T-Systems ein Chipkartenbetriebsystem (TeleSec Chipcard Operating System, TCOS) entwickelt, welches in der Lage ist, Schlüssel sicher zu verwahren und den kryptografischen Algorithmus innerhalb des Chips zu berechnen. Einmal sicher eingebrachte Schlüssel müssen die Chipkarte also niemals mehr verlassen.

Bleibt die Frage nach der Herkunft der jeweiligen Schlüssel. Als Antwort wurde durch T-Systems ein Schlüsselgenerator entwickelt, der nachprüfbar sicheres Schlüsselmaterial generieren kann. Unter den Augen von neutralen Evaluatoren entstand ein System, bei dem die generierten Schlüssel über einen sicheren Kanal in unsere TCOS-Chipkarten eingebracht und gespeichert werden.

Durch Zuordnung von Identitätsmerkmalen zu diesen kryptografischen Schlüsseln entstehen digitale Identitäten. Die Smart Card macht aufgrund der zuvor beschriebenen Arbeitsweise diese digitalen Identitäten einmalig, das heißt, es existieren keine Kopien der Schlüssel.

Auf der Basis von TCOS stehen verschiedene Standardprodukte mit oder ohne Schlüsselmaterial zur Verfügung, wobei gängige ISO-Standards selbstverständlich sind.

Daneben bietet die T-Systems die Entwicklung und Konfektionierung von Smart Cards nach individuellen Kundenanforderungen an und begleitet den Kunden innerhalb von Projekten unter Einbeziehung des gesamten Smart Card Know-how.

Sprechen Sie uns an, wenn Sie Fragen haben!

☰ nach oben ↶ zurück 🖨 drucken
- Right Sidebar:**

Next Step

 - ☰ Detaillierte Produktinformationen
 - ☰ Treibersoftware und Support** (circled in red)
- Footer:** © 2010 T-Systems International GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz Glossar

- 1.2) Im Untermenü „PKCS#11 SDK“ wählen Sie den passenden Treiber für Ihr Betriebssystem aus. Das heruntergeladene Treiberpaket (ZIP-Datei) kann sofort installiert werden.

The screenshot shows the T-Systems website with the following elements:

- Header:** T-Systems logo and navigation links (Startseite, Kontakt).
- Navigation:** Signaturkarte (PKS), ServerPass, Shared Business CA, **TCOS-Smartcards**, OneTimePass, PKI, E-Mail Encryption Gateway.
- Left Sidebar:**
 - Public Key Service
 - ServerPass
 - Shared Business CA
 - TCOS-Smartcards** (highlighted)
 - OneTimePass
 - Public Key Infrastructure
 - E-Mail Encryption Gateway
- Main Content:**

PKCS#11 SDK

Es werden je nach Betriebssystem bis zu drei PKCS#11 Module zur TCOS Karte bereitgestellt. Das SigG Modul unterstützt die SigG-Applikation für die qualifizierte Signatur auf der NetKey 3.0 TCOS 3 Chipkarte. Das NetKey-Modul unterstützt die fortgeschrittene Chipkarten Applikation auf den TCOS 3.0 Chipkarten NetKey 3.0 IDKey. Das ELSTER-Modul ist weitestgehend identisch mit dem NetKey-Modul und für die Steuer Software ELSTER vorgesehen. Das Setup der Windows Version des TCOS PKCS#11 SDK enthält C-Beispiel Quellcode zur einfachen Integration der TCOS-Chipkarten.

Beachten Sie bitte vor dem Einsatz unsere **Allgemeinen Geschäftsbedingungen** zum Einsatz der Software.

 - ☰ P11TCOS3-Lib für Windows x86 v.1.4.0.3
 - ☰ P11TCOS3-Lib für Windows x64 v.1.4.0.3
 - ☰ P11TCOS3-Lib für Linux mit PIN-Pad Unterstützung v.1.4.0.3
 - ☰ P11TCOS3-Lib für Linux ohne PIN-Pad Unterstützung v.1.4.0.3
 - ☰ P11TCOS3-Lib für MAC v.1.4.0.3
 - ☰ Beispiel Sourcecode-Zip-Datei

☰ nach oben ↶ zurück 🖨 drucken
- Right Sidebar:**

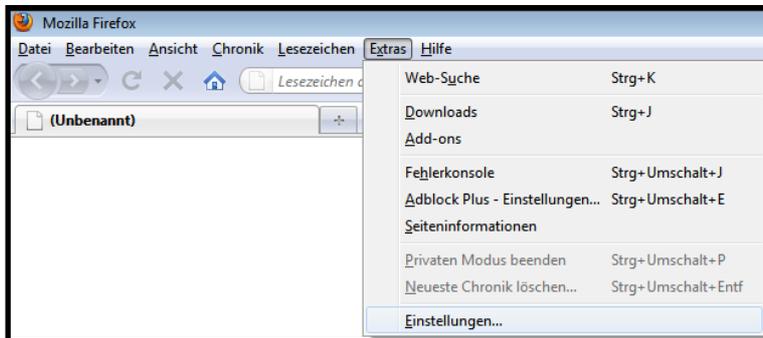
Download

 - ☰ TCOS Card Modul zum Microsoft® Smartcard Base/SP
 - ☰ PKCS#11 SDK** (circled in red)
 - ☰ TeleSec CardManager .NET

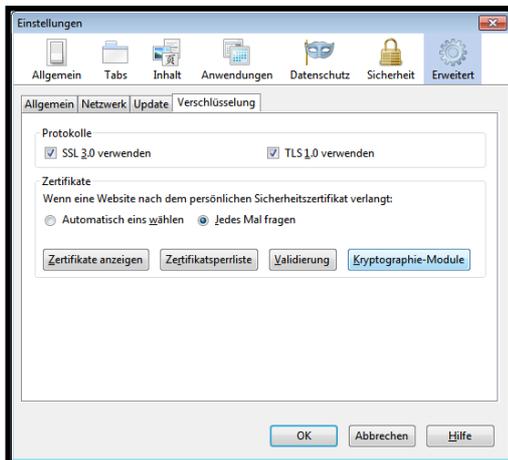
Next Step

 - ☰ Tutorien, How-Tos
 - ☰ Kontaktieren Sie unsere Experten!
- Footer:** © 2010 T-Systems International GmbH. Alle Rechte vorbehalten. Deutsche Telekom Impressum Datenschutz Glossar

- 2.1) Nachdem der Treiber installiert wurde, kann das Modul unter Firefox eingebunden werden. Öffnen Sie die Firefox-Einstellungen: *Klicken Sie hierfür in der Menüleiste auf Extras und im Untermenü auf Einstellungen.*

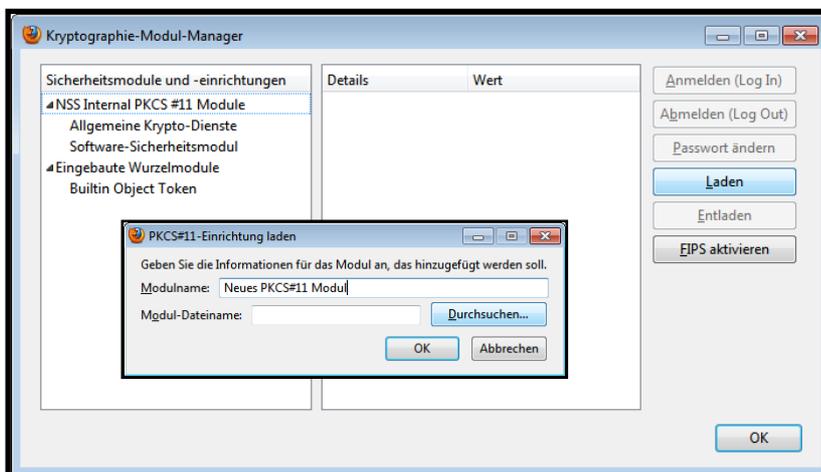


- 2.2) Klicken Sie auf Erweitert und wählen Sie im Register "Verschlüsselung" aus: *Hier findet sich der Button für "Kryptographie-Module", klicken Sie hierauf und der Kryptographie-Modul-Manager wird geöffnet.*



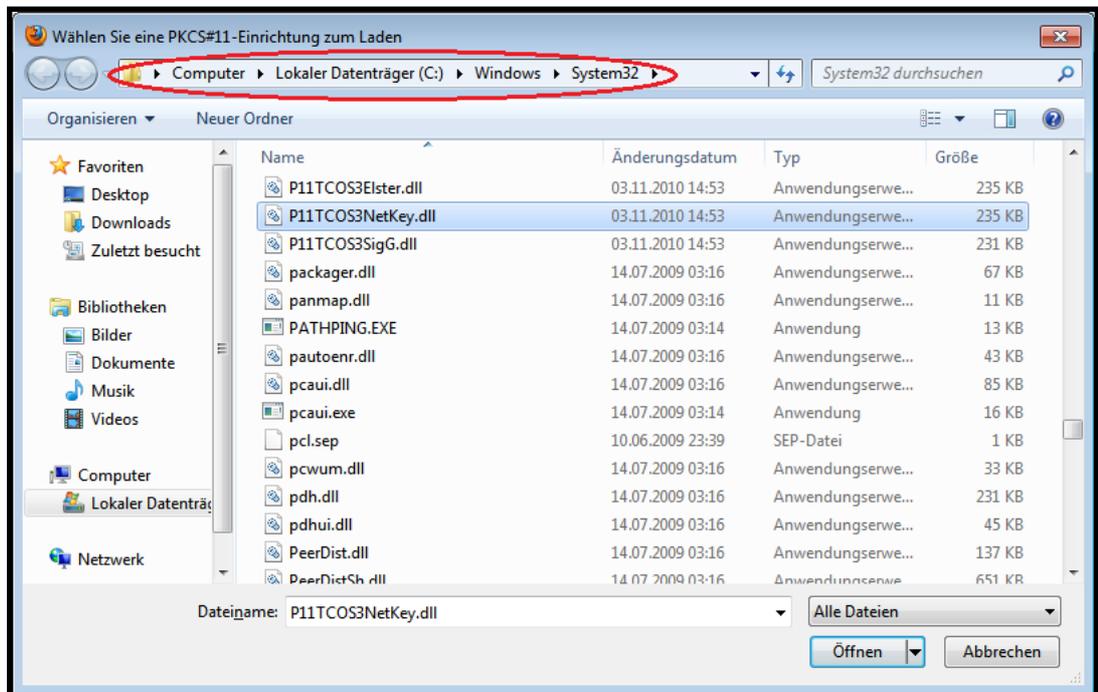
- 2.3) Im Kryptographie-Modul-Manger klicken Sie auf „Laden“.

Es öffnet sich ein Fenster zum Laden von PKCS#11-Einrichtung. Klicken Sie auf „Durchsuchen“.



- 2.4) Es öffnet sich ein Auswahlfenster. Gehen Sie in den Ordner „Laufwerk: Windows/System32“ und suchen Sie nach der Datei P11TCOS3NetKey.dll

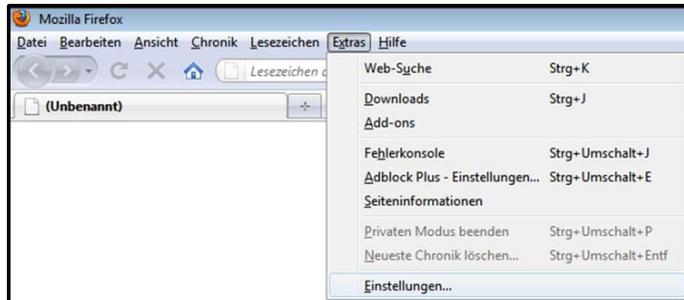
Hier klicken Sie nachdem Sie die Datei ausgewählt haben einfach auf „Öffnen“. Die Datei wird in das Eingabefeld „Modul-Dateiname“ eingetragen. Jetzt müssen Sie nur noch zweimal mit „OK“ bestätigen. Sie können nun die Smartcard-Anwendungen innerhalb Mozilla Firefox nutzen.



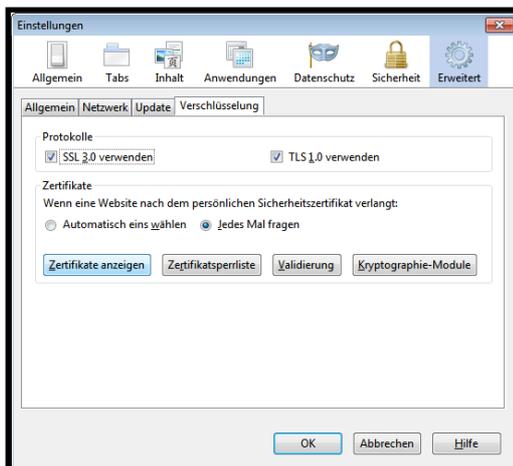
Zertifikate importieren

3.1) Öffnen Sie die Firefox-Einstellungen:

Klicken Sie hierfür in der Menüleiste auf Extras und im Untermenü auf Einstellungen.

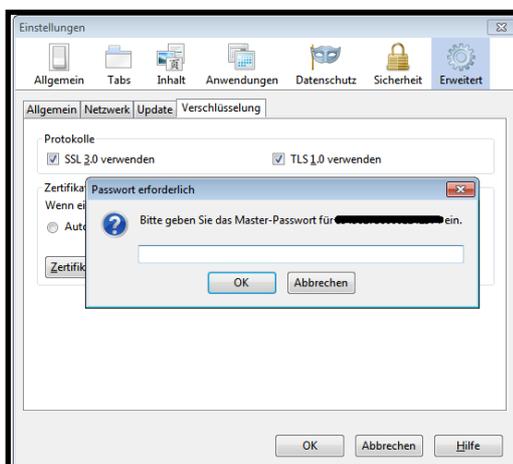


3.2) Klicken Sie auf Erweitert und wählen Sie im Register "Verschlüsselung" aus:



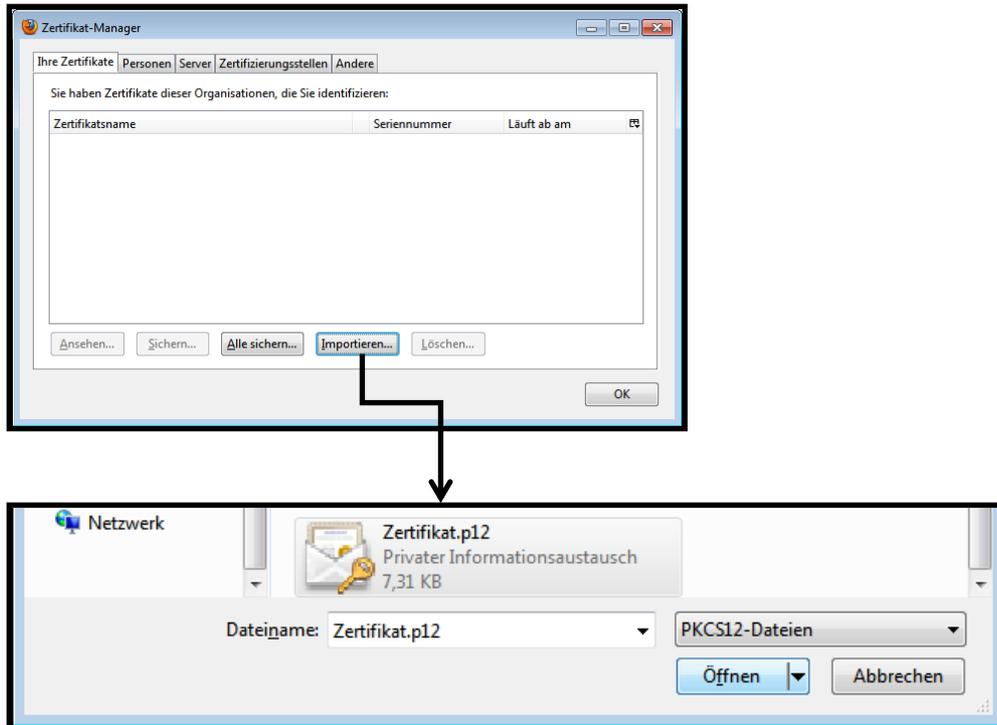
Hier findet sich der Button "Zertifikate anzeigen". Ein Klick hierauf öffnet den Zertifikat-Manager.

Achtung: Wenn sich eine Smartcard im Kartenleser befindet, die bereits mit einem Zertifikat personalisiert und mit einer persönlichen PIN versehen wurde, verlangt Firefox nach einem sogenannten Master-Passwort. Geben Sie hier Ihre PIN für die Smartcard ein.



3.3) Hier wählen Sie Ihr Zertifikat unter Importieren aus:

Wählen Sie aus, von wo Sie Ihr Zertifikat öffnen möchten und klicken Sie auf Öffnen.



3.4) Fertig!

Wenn alles geklappt hat, zeigt der Zertifikat-Manager Ihr Zertifikat folgendermaßen an:

