15. April 2012 Artikel · Digitale Identität · Web & Cloud

Smart-Card Applet

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/smart-card-applet/

Das SmartCard Applet erkennt Chipkarten anhand des ATR (Answer to Reset). Zusätzlich zu den hier angeführten Karten werden auch eID Karten aus EU Staaten erkannt (österreichische e-card, finnische eID Karte, etc.).

Für einige Karten werden spezifische Informationen angezeigt. Diese sind aktuell die österreichische e-card (G2 bis G3) und weitere österreichischen Bürgerkarten. Zusätzlich können Signaturzertifikate europäischer eID Karten ausgelesen werden.

Voraussetzungen

- Java ab Version 6
- ein angeschlossener Kartenleser mit PC/SC Treiber
- Browser mit Java-Applet Unterstützung (**Anmerkung**: nachdem Browser-Hersteller zunehmend die Unterstützung von Java-Applets einstellen, ist dieses Tool nur mehr mit wenigen aktuellen Browsern nutzbar, z.B. Internet Explorer 11).

Einfache Befehle ausführen

Um kurz die Funktionsweise der Interaktion mit der Karte zu demonstrieren, finden Sie hier die Befehle um die Sozialversicherungsnummer auf Ihrer e-card auszulesen. Um Befehle auszuführen, wechseln Sie bitte in die Registerkarte „Befehle“.

Bitte beachten Sie, dass diese Beispiel-Befehle nur für die österreichische e-card bis zu Generation 3 (G3) funktionieren. Für andere Karten müssen die Befehle der jeweiligen Kartenspezifikation verwendet werden.

- Anwendung „SV Personendaten“ auswählen

Dazu geben Sie bitte folgenden APDU Befehl ein:

CLA: 00 INS: A4 (SELECT Befehl) P1: 04 (Gibt an dass die Datei ein Dedicated File ist und diese mit dem DF Namen selektiert wird) P2: 00 (Gibt an, dass eine File Control Information zurückgegeben werden soll) LE: FF (Maximum an Bytes das zurückgegeben werden kann) Daten: D0 40 00 00 17 01 01 01 (Der Anwendungsidentifier der Anwendung SV Personendaten) Antwort:

Als Antwort sollte nun der Status 9000 (Kommando erfolgreich ausgeführt) angezeigt werden.

- Anschließend die Datei „Grunddaten“ auswählen

Dazu geben Sie bitte folgenden APDU Befehl ein:

CLA: 00 INS: A4 (SELECT Befehl) P1: 02 (Gibt an, dass die Datei ein Elementary File ist und sich im momentan selektierten Dedicated File befindet) P2: 04 (Gibt an, dass ein File Control Parameter zurückgegeben werden soll) LE: FF (Maximum an Bytes das zurückgegeben werden kann) Daten: EF 01 (Der Fileidentifier für die Datei Grunddaten) Antwort:

Als Antwort sollte nun der Status 9000 (Kommando erfolgreich ausgeführt) angezeigt werden.

- Abschließend wird der Inhalt dieser Datei gelesen

Dazu geben Sie bitte folgenden APDU Befehl ein:

CLA: 00 INS: B0 (READ BINARY Befehl, liest Daten aus Dateien der Struktur “transparent”, “transparente” Dateien sind Dateien ohne innerer Struktur) P1: 00 (Offset) P2: 00 (Offset) LE: FF (gibt an, wie viele Bytes gelesen werden sollen, 0xFF ist das Maximum an Bytes das zurückgegeben werden kann) Antwort:

Die Antwort besteht aus dem Inhalt der Datei und dem Status 9000. Die Antwortdaten sind in ASN.1 kodiert. Um diese nun zu dekodieren kann unter anderem dieser ASN.1 Parser verwendet werden.

Eine ausführliche und übersichtliche Aufstellung der möglichen Befehle (ISO 7816-4) und ihren Parametern finden Sie hier.