15 April 2012 Article · Digital Identity · Web & Cloud

Smart Card Applet

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/smart-card-applet-en/

The Smart Card Applet identifies cards according to their ATR (Answer to Reset). In addition to the cards specified here the applet also recognizes eID cards from member states of the European Union (Austrian e-card, Finnish eID card etc.).

For some cards the applet displays card specific data, like for the Austrian e-card (G2 to G3) and further Austrian Citizen Cards. In addition you can retrieve signature certificates from European eID cards.

Requirements

- Java from version 6
- connected card reader with the corresponding PC/SC driver installed
- Broswer supporting Java-Applets (**Note**: As browser-vendors retire Java-Applet support, this tool is just usable with few current browsers like Internet Explorer 11)

How to execute simple commands

To demonstrate the interaction with the card, we provide you with commands needed to read the social insurance number from your e-card. In order to execute commands, please change into the tab „Befehle".

Note that these sample commands only work with an Austrian e-card up to generation 3 (G3). In order to execute them with other cards, they have to be adapted according to the cards specification.

- Select the application „SV Personendaten"

Therefor enter the following APDU command:

CLA: 00 INS: A4 (SELECT command) P1: 04 (Specifies that the selected file is a "Dedicated File", and that we select it with its "DF Name") P2: 00 (Specifies that we expect the card to return "File Control Information") LE: FF (Maximum number of bytes that can be returned) Daten: D0 40 00 00 17 01 01 01 (The application identifier of "SV Personendaten") Response:

As response you should receive the status code 9000 (Success).

- Next we select the file „Grunddaten“.

Therefor enter the following APDU command:

CLA: 00 INS: A4 (SELECT command) P1: 02 (Specifies that the file is an “Elementary File” and that it resides in the currently selected “Dedicated File”) P2: 04 (Specifies that we expect the card to return “File Control Information”) LE: FF (Maximum number of bytes that can be returned) Daten: EF 01 (The “File identifier” for the file “Grunddaten”) Response:

As response you should receive the status code 9000 (Success).

- Read the content of the file

Therefor enter the following APDU command:

CLA: 00 INS: B0 (READ BINARY command, this command reads data from “transparent” files, “transparent” files are files without an inner structure of the content) P1: 00 (Offset) P2: 00 (Offset) LE: FF (Specifies how many bytes should be read, 0xFF correspondes to the maximum number of bytes that can be returned) Response:

The response includes the content of the file and the status code 9000. The returned data is ASN.1 encoded. In order to decode them you can use an ASN.1 Parser.

Here you can find further information and detailed instructions about all possible commands (ISO 7816-4) and their parameters .