



VirtuoSimo Card Plug-in

Requirements for Implementation

Overview

This document provides the requirements to implement and test a card plug-in for a specific SIM card within the VirtuoSimo development environment.

Most of the SIM card commands are standards and comply with the 3GPP TS 11.11 and 3GPP TS 11.14. But some administrative commands like the creation and deletion of file and not standardised. Therefore each SIM card supplier designs its own set of administrative commands. The document summarises the required information about these proprietary administrative commands.

The document gives also a few requirements about the personalisation of the SIM cards required to test the plug-in software.

Administrative Commands Documentation

In order to implement such a plug-in, we therefore need get the documentation about the following administrative commands or mechanisms.

File Creation

We need to know the process to manage a file creation. Generally the creation of files (EF and DF) is handled through a single APDU command. In this case, we need to know the format of this APDU command.

We also need to know the specific access conditions attached to the file creation. Generally access conditions for file creation are attached to the parent DF. We therefore need to know how to retrieve this access condition. Generally this is through the response to the standard SELECT command (field "GSM Specific Data") or through a specific command like GET FILE INFORMATION.

File Deletion

We need to know the process to manage a file deletion. Generally the deletion of files (EF and DF) is handled through a single APDU command. In this case, we need to know the format of this APDU command.

We also need to know the specific access conditions attached to the file deletion. Generally access conditions for file deletion are attached to the parent DF. We therefore need to know how to retrieve this access condition. Generally this is through the response to the standard SELECT command (field "GSM Specific Data") or through a specific command like GET FILE INFORMATION.

Administrative Code Verification

3GPP TS 11.11 specifies the VERIFY CHV command for card holder codes CHV1 and CHV2. The verification of an administrative code is not specified nor the number of available administrative code within the SIM card.

We need to know the format of the command available to verify an administrative code. We also need to know the maximum number of administrative codes available in the SIM card as well as their coding both in the verification command and in the response to SELECT command (field "Access Conditions").

Setting the Authentication Key (Ki)

Each card has a different mechanism to set the GSM authentication key known as "Ki". Generally this key is stored into a specific file together with the mode of operation for the authentication procedure (COMP128-V1, COMP128-V2, etc.) In this case, we need to know the location and format of this file.

The setting of the key can also be done through a specific APDU command in which case we need to know the format of this command.

Sometimes a procedure is also required to activate the key after it has been updated. This is also important for us to know.

Test Cards Personalisation

In order to test the plug-in software, we need to get a few SIM cards personalised in a way that would allow us to:

- create and delete files under the MF, DF Telecom and DF GSM,
- modify the value of the key Ki (if stored into a file, the update access condition must not be set to NEVER),
- download a SIM Toolkit applet using the SIM Alliance Interoperable Loader (minimum security level for OTA downloading must not be over 1).

The exact SIM personalisation is not of real importance and can be a very standard personalisation. We just need to know the following:

- the value of CHV1 and UNBLOCK CHV1,
- the value CHV2 and UNBLOCK CHV2,
- the number of administrative codes initialised on the card and their values,
- the value and key set of the OTA download key known as "KID".

If required, a detailed card profile requirement can be provided.