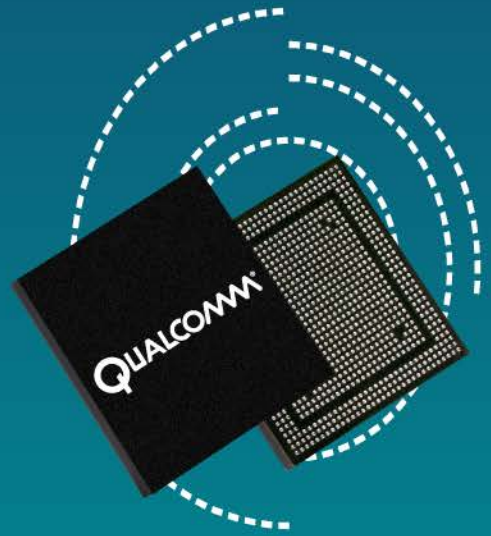
Qualcomm
TECHNOLOGIES, INC



USB UICC Overview

80-NN611-1 B

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

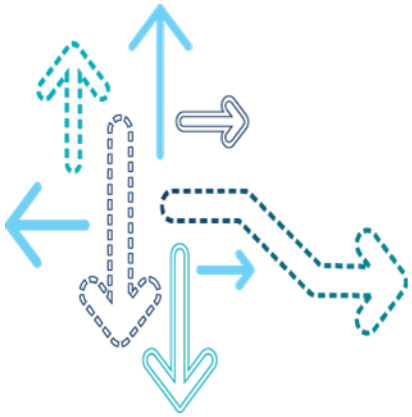
Revision History

Revision	Date	Description
A	Apr 2014	Initial release
B	Jun 2014	Updated NV Item and Feature Support; added USB UICC Log Analysis

Contents

- Introduction
- Card Architecture and Functional Interfaces
- IC-USB Hardware Characteristics
- Product Requirements
- Software Block Diagram
- Software Implementation of Interface Selection, Powerup, and ISO Fallback
- NV Item and Feature Support
- USB UICC Call Flow
- USB UICC Log Analysis
- References
- Questions?

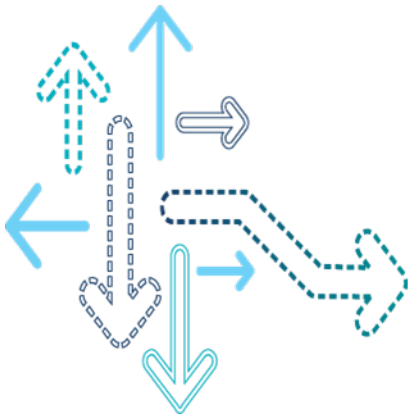
Introduction to USB UICC



Introduction

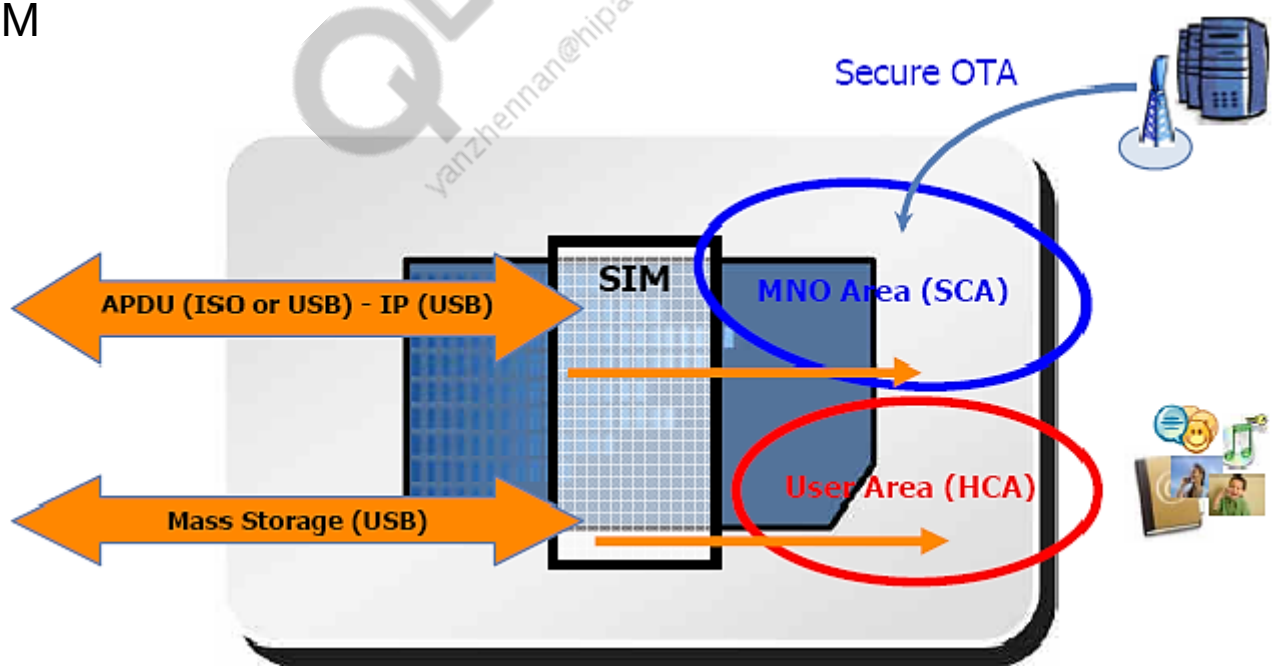
- Transformation of the UIM from an “identity” to a “multimedia” card
- Faster data transfer rates between terminal and card
- Execute, install, or store specific MNO applications or games
- Manage an operator menu
- Provide a storage solution to end users
  - Mass storage drive with more flexibility for the end user
- Enable use of protected content stored in the SIM card
- Provide carriers with a Smart Card Web Server (SCWS) solution
  - Alternative to SCWS over Bearer Independent Protocol (BIP)
  - Facilitates offline browsing
  - Allows MNO to provide targeted preloaded websites for easy service discovery and content teasing
  - Allows end user to personalize a portable web home page

Card Architecture and Functional Interfaces



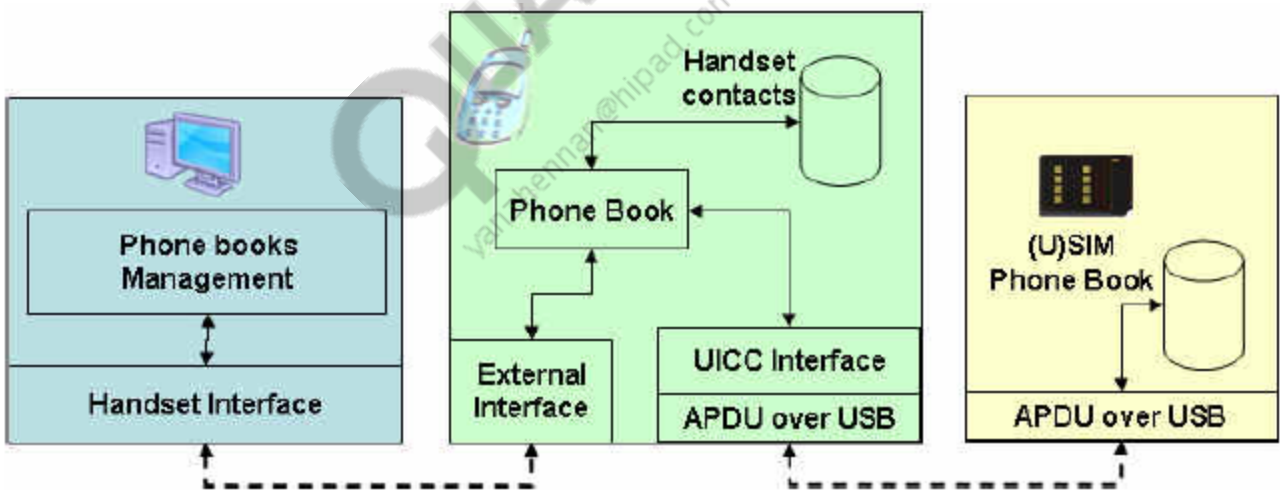
Card Architecture

- Two partitions
  - Mobile network operator area (SIM controlled area)
  - User area (handset controlled area)
- Three interfaces
  - ICCD
  - MS
  - CDC-EEM



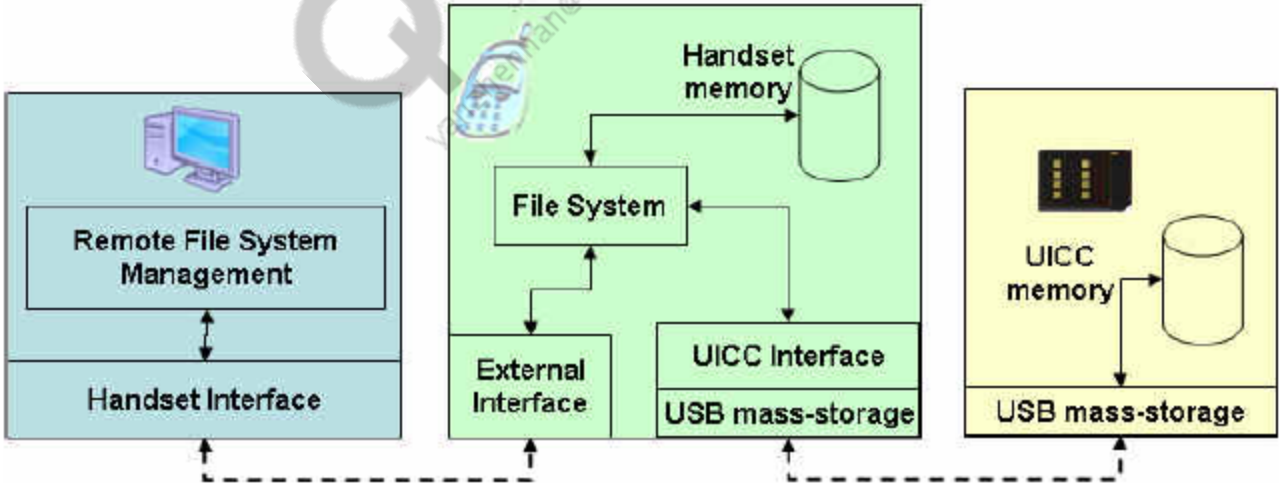
Integrated Circuit Card Device (ICCD) Interface

- Provides access to the internal file system in the SIM controlled area
- Allows exchange of APDUs over USB
- Supports all APDUs defined in [S1]



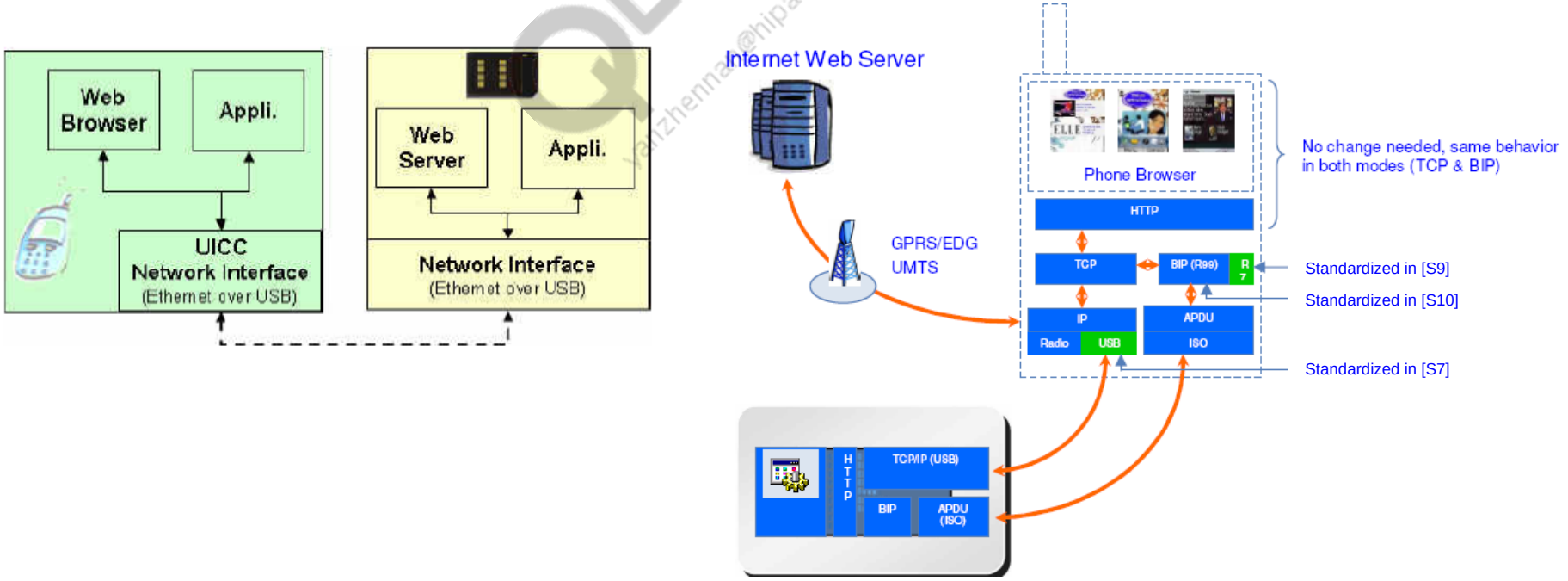
Mass Storage (MS) Interface

- Provides access to handset controlled area via a file system driver
- Allows file system applications to place and retrieve files
- Allows media applications to access and render media files directly
- Storage area may have one or more partitions and shall be formatted as a FAT 32 file system (for cards with < 2 GB capacity)

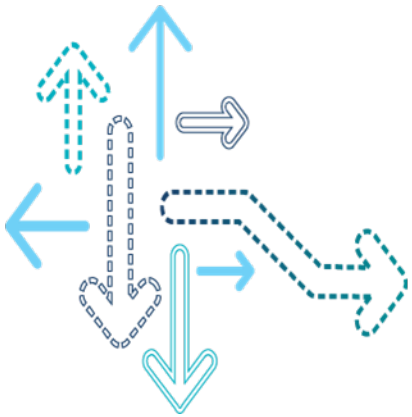


Communication Device Class-Ethernet Emulation Model (CDC-EEM) Interface

- Allows IP connection between terminal and card as defined in [S2]
- Allows access to SIM controlled area via IP connectivity
- UICC configurations supported
  - Server for a client located on the terminal (currently supported)

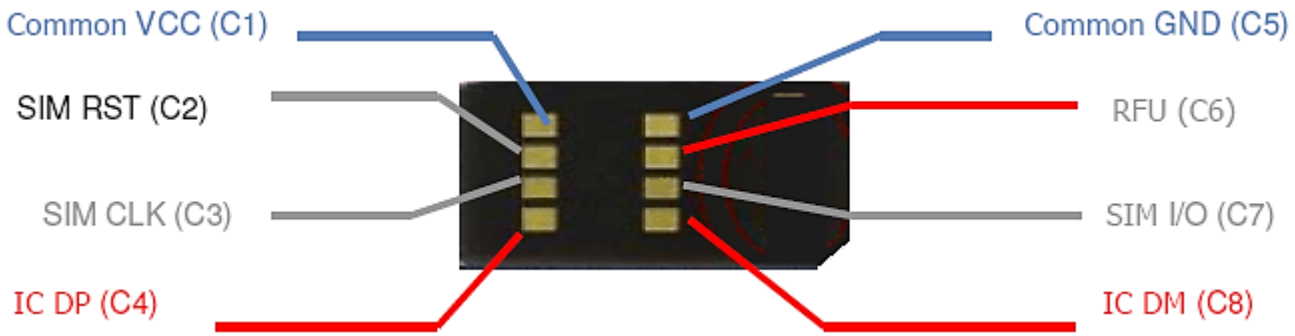


IC-USB Hardware Characteristics

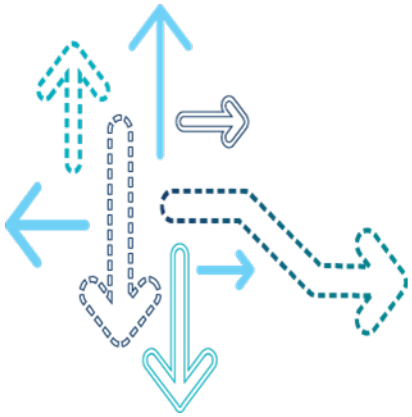


Inter-Chip USB (IC-USB) Hardware Characteristics

- Specified in [S8]
- Handset must integrate an 8-pin connector compliant with [S6]
- USB D+/D- signals are located on C4 and C8 contacts
- Legacy ISO contacts, e.g., RST, CLK, and I/O shall be supported, but not concurrently with the USB interface
- Plug-in UICC form factor
- Class B and Class C voltages supported
- Current draw compliant with ISO specification for idle (< 200 uA) and active

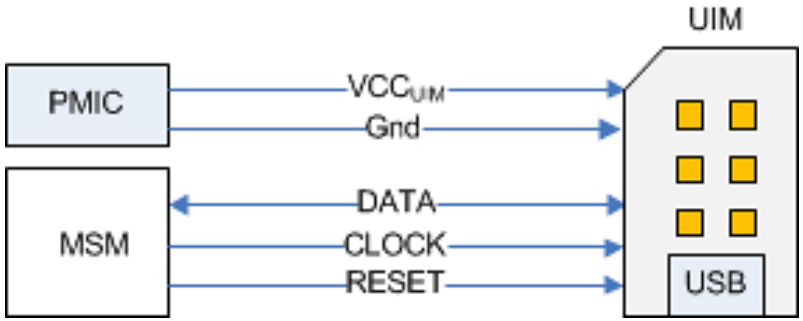


Product Requirements



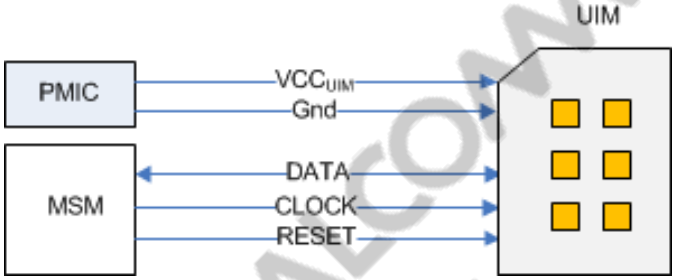
Product Requirements

- UICC terminal interoperability
- Terminal shall support a high-speed protocol over USB
- Terminal shall be fully backward-compatible with legacy ISO cards
- Three possible configurations
  - Terminal not capable of USB (legacy ISO interface used)
  - UICC not capable of USB (legacy ISO interface used)
  - Terminal and UICC capable of USB (IC-USB interface used)
- Terminal not capable of USB

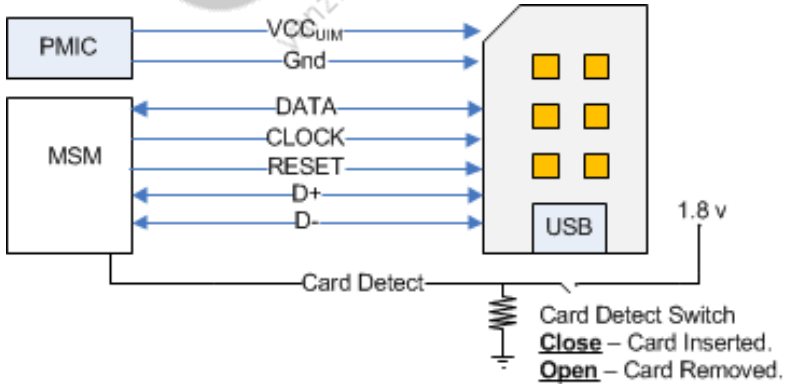


Product Requirements (cont.)

- UICC not capable of USB



- Terminal and UICC capable of USB



Product Requirements (cont.)

- The ICCD interface shall be used for reading subscription information and performing other SIM-related procedures, i.e., PIN verification, authentication, etc. The physical layer differences for the ICCD interface shall be abstracted from the higher layers. The upper layers see and operate the ICCD interface just as they do for legacy SIMs.
- The mobile device can operate the USB UICC in either legacy mode (see [S5]) *or* USB mode at any given time, but it cannot operate it in legacy mode *and* USB mode at the same time. When operating in legacy mode, the mobile device should turn off any USB signaling and when operating in USB mode, it should not use any of the legacy signals.
- The mobile device should support concurrent operation of ICCD and MS interfaces. The device should allow different applications to use ICCD and MS interfaces simultaneously for sending and receiving data from the USB UICC.
- The mobile device should handle error conditions for ICCD and MS interfaces independently without affecting the other interface, e.g., SIM recovery/reset procedures on the ICCD interface should not affect MS transactions while operating in USB mode.

Product Requirements (cont.)

- USB UICC memory is divided into four partitions:
  - Area 0 – Card OS file
  - Area 1 – NAND Flash to store card system files and security-related information
  - Area 2 – NAND Flash to store carrier applications and data
  - Area 3 – NAND Flash to store end user data
- Area 2 and Area 3 will be visible to the device while Area 0 and Area 1 will be hidden.
- Area 2 and Area 3 may be mounted as mass storage partitions with FAT32 file system. Area 2 must be hidden from the standard user interface. Special permissions must be put in place so that the end user cannot read/write/modify files in this partition. Only specific carrier applications (background/frontend) can access this region of the memory.
- There is no restriction on the type of data that the user can store in Area 3.
- User-accessible USB mass storage partitions should be available for all UI applications listed as “SIM Storage Area” with read/write/modify permissions. Carrier-accessible USB mass storage partitions should be hidden for end user applications. Each UI application should be able to make a selection between the SD card, USB MS, and eMMC for offline storage needs.

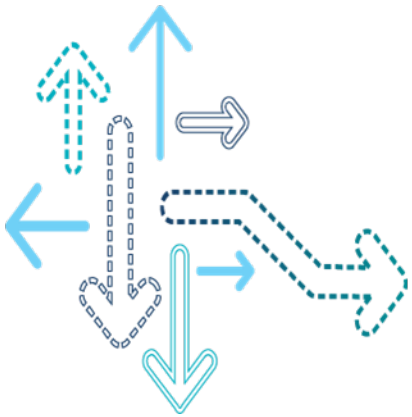
Product Requirements (cont.)

- When the user connects the mobile device to the PC, the user should be able to see the mass storage areas enumerating as the disk drive. The user should see two disk drives being enumerated on the PC and should be able to read/write/modify files in the storage area meant for general access. The user should be able to perform format operations on this disk drive as provided by the desktop operating system. The carrier partition may not be available for the user for reading and writing files.
- The USB UICC is a hot-pluggable device. The mobile device should handle a loss of connection due to the user plugging out of the card, or any other error condition, in a graceful manner. For an MS connection, the software should report it as a USB device eject to the UI and PC connection. Also, the terminal should handle use cases where:
  - The user plugs in/out of the USB UICC at any point during regular operation.
  - The user swaps the USB UICC with a normal SIM and vice versa.

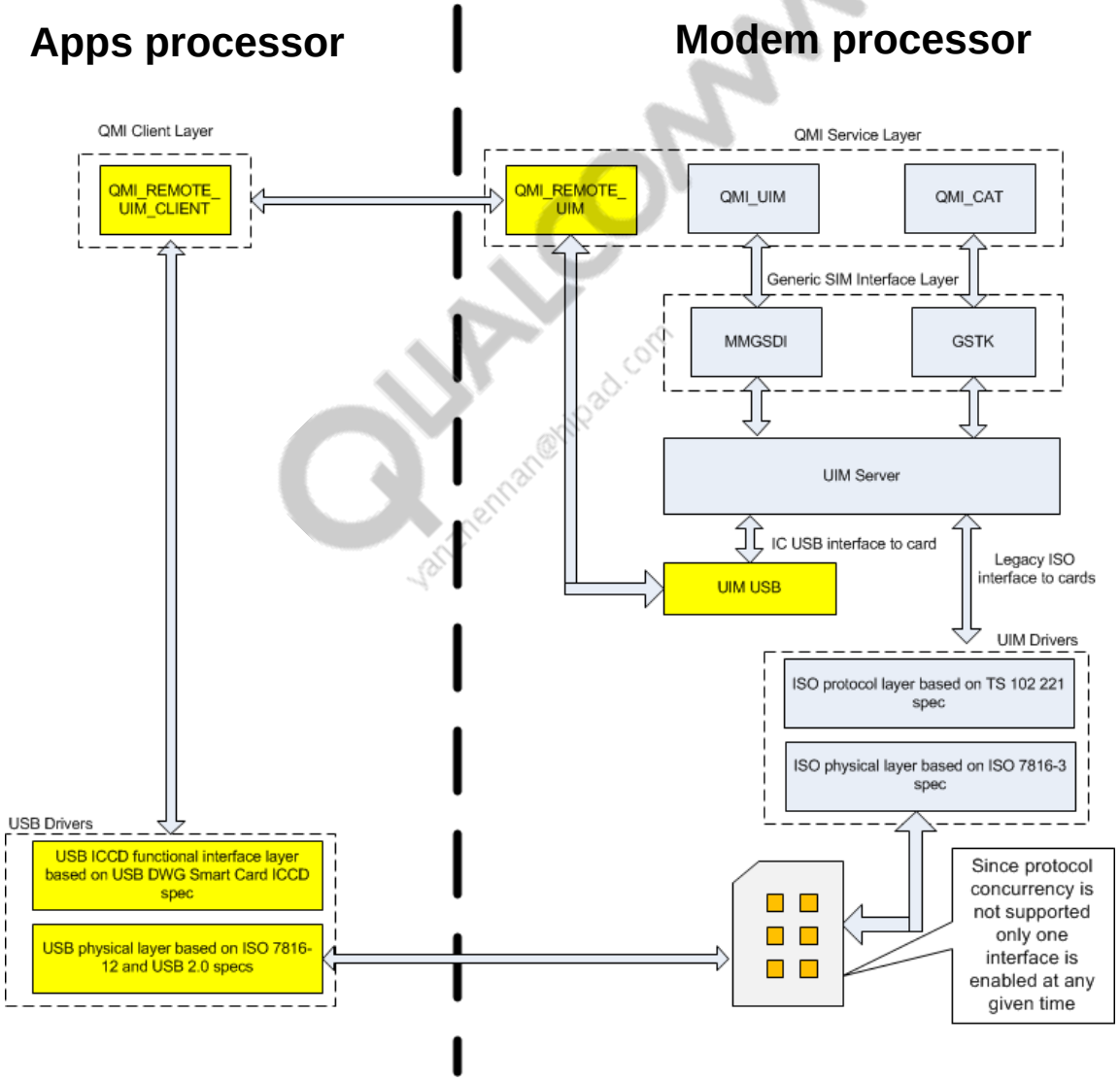
Product Requirements (cont.)

- While the mobile device is in Airplane mode, the user should still be able to access the mass storage memory.
- For a card power-down initiated by AT commands or Airplane mode, the software will initiate logical shutdown of the ICCD interface. The UIM driver shall put the card in an error state for ICCD functionality. Mass storage functionality shall still be available.
- The terminal should support read and write speeds as follows:
  - Write speed should be no less than 190 KBps (1500 kbs).
  - Read speed should be no less than 375 KBps (3000 kbps).

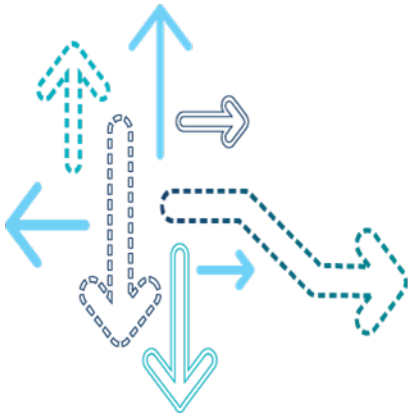
Software Block Diagram



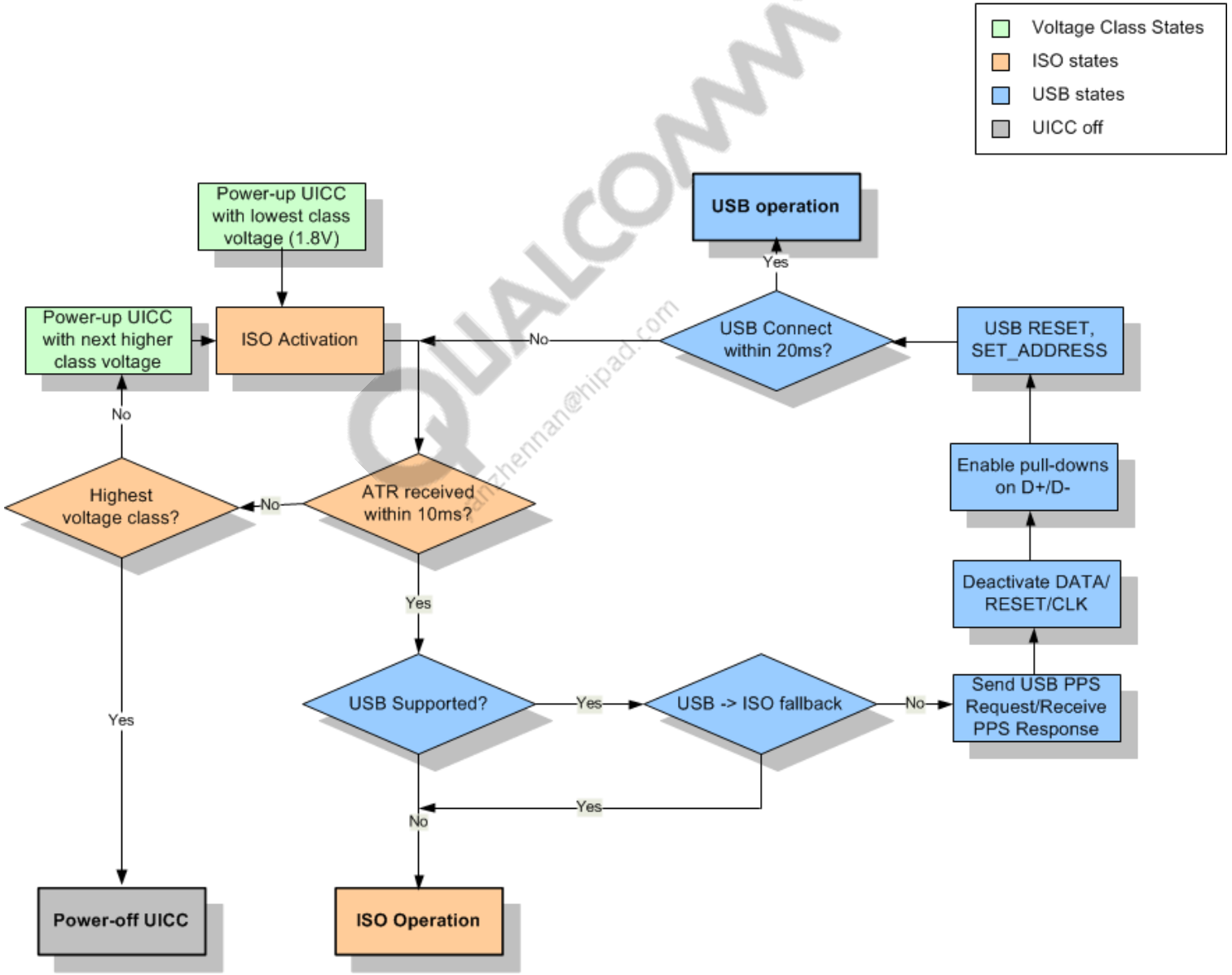
Software Block Diagram



Software Implementation of Interface Selection, Powerup, and ISO Fallback



Voltage and Interface Selection Flowchart

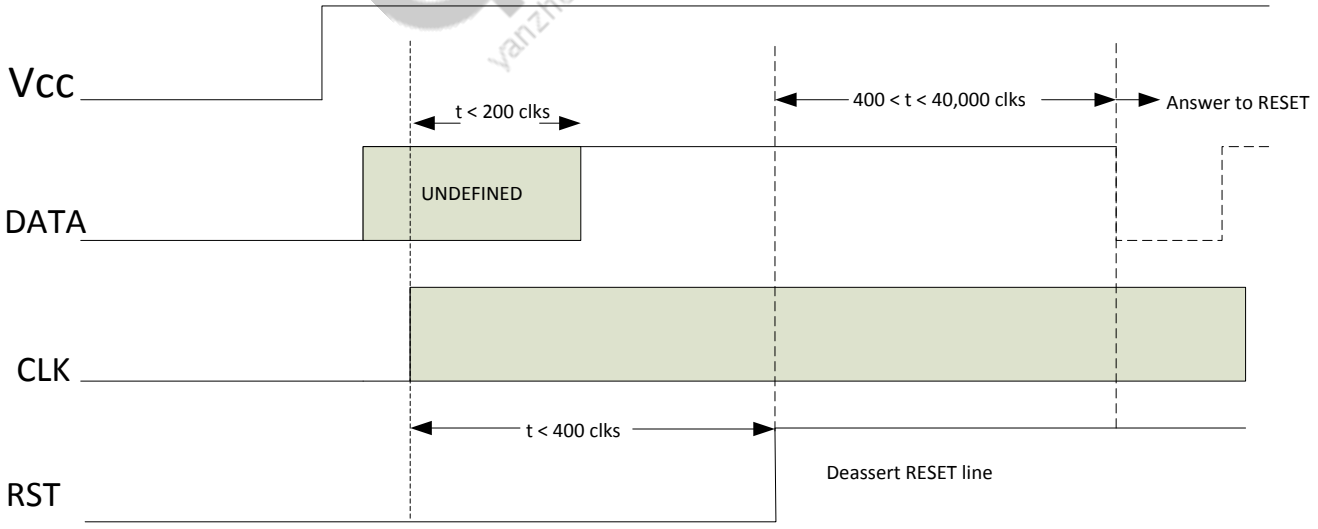


Supply Voltage and Interface Selection

- The terminal shall support voltage classes B and C.
- Cards from some manufacturers may not enumerate mass storage drive at voltage class C.
- The terminal shall initially select voltage class C and start the interface selection procedure.
- If no USB attach occurs or no ATR is received or the card returns “Class B activation preferred” during power negotiations, the UICC shall be deactivated and activated with voltage class B.
- Two interface selection procedures are allowed by the standard:
  - Procedure using ATR
  - Procedure using USB
- Qualcomm Technologies, Inc. (QTI) implementation supports the procedure using ATR, which has three steps:
  1. ISO activation
  2. USB attachment
  3. USB activation

ISO Activation

- The terminal shall begin activation in ISO mode. The activation sequence shall be:
  1. All the lines shall be in low state.
  2. Vcc shall be powered. I/O in the terminal should be put in the reception mode. CLK shall be provided.
  3. After 400 clock cycles, the RESET line shall be brought up.
  4. The card should respond to RESET by sending Answer to Reset information.



ATR and PPS

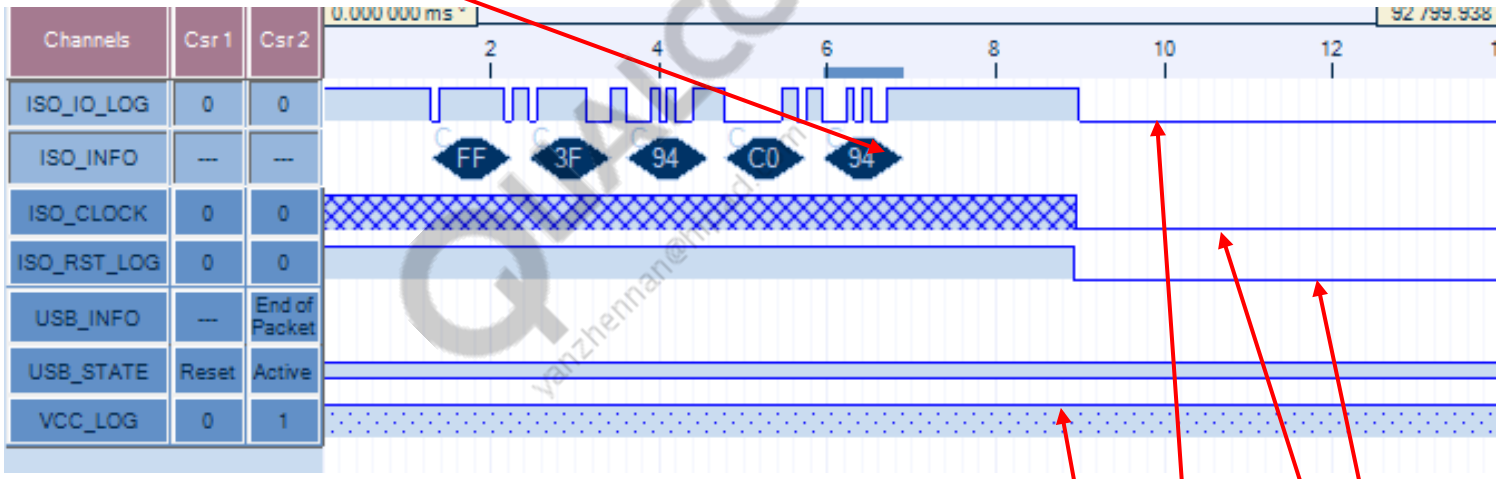
- If TB3 byte has a value of C0, then it indicates support for USB UICC. The ATR also tells the terminal about supported voltage classes.
- For USB protocol operation, the terminal shall send a PPS request as follows:
  - PPS1 byte with bit 5 set to 1 to indicate the presence of the PPS2 byte. Bits 4 to 1 are set to 1 to indicate T=15 protocol. Other bits are set to 0 (PPS1 = 0x3F).
  - PPS2 byte will be set to 0xC0 to indicate USB protocol.
  - Upon receiving the PPS response, the terminal shall start USB activation.

IT3 Logs (ISO Activation)

Cold reset		Event			Reset card interface
Warm reset		Event			Reset card interface
ATR	C	TS	3B		Direct convention
	C	T0	9F	etu	Following interface chars: TA1, TD1 Number of historical chars: 15
	C	TA1	94	etu	F = 512 D = 8
	C	TD1	80	etu	Following interface chars: TD2 Transfer protocol T=0
	C	TD2	3F	etu	Following interface chars: TA3, TB3 Interface character qualifier: T=15
	C	TA3	C2	etu	X = No preference U = Class B only
	C	TB3	C0	etu	Global Interface: Inter-Chip USB UICC-Terminal interface supported as defined in TS 102600.
	C	T1	80	etu	
	C	T2	31	etu	
	C	T3	E0	etu	
	C	T4	73	etu	
	C	T5	FE	etu	
	C	T6	21	etu	
	C	T7	13	etu	
	C	T8	67	etu	
	C	T9	80	etu	
	C	T10	32	etu	
	C	T11	40	etu	
	C	T12	13	etu	
	C	T13	56	etu	
	C	T14	C1	etu	
	C	T15	01	etu	
	C	TCK	48	etu	Check character
PPS reques	T	PPSS	FF	etu	Initial character
	T	PPSC	3F	etu	Following parameter chars: PPS1, PPS2 Transfer protocol: T=15
	T	PPS1	94	etu	F = 512 D = 8
	T	PPS2	C0	etu	Global Interface: Inter-Chip USB UICC-Terminal interface supported as defined in TS 102600.
	T	PCK	94	etu	Check character
PPS respon	C	PPSS	FF	etu	Initial character
	C	PPSC	3F	etu	Following parameter chars: PPS1, PPS2 Transfer protocol: T=15
	C	PPS1	94	etu	F = 512 D = 8
	C	PPS2	C0	etu	Global Interface: Inter-Chip USB UICC-Terminal interface supported as defined in TS 102600.
	C	PCK	94	etu	Check character

IT3 Logs Switching from ISO to USB

PPS response from card

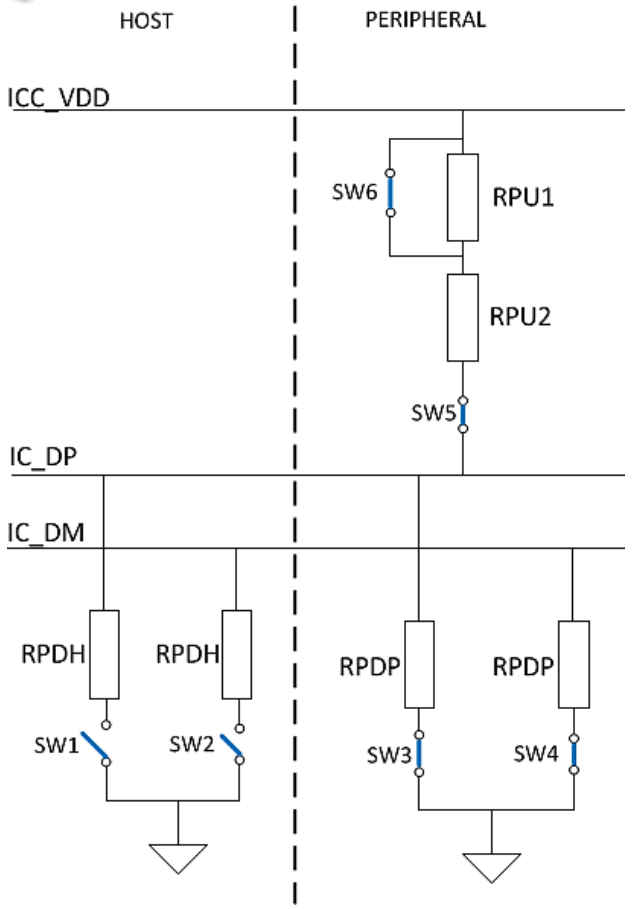


Data, CLK, and RST lines turned low; Vcc stays high

IC-USB Implementation

- The card can leave DP floating (high impedance) or pull it up by keeping SW5 open or closed, respectively.
- The card can enable pull-down with the help of SW3 and SW4.
- The host can also enable pull-down on DP and DM with the help of SW1 or SW2.

IC-USB configuration as mentioned in USB 2.0 spec

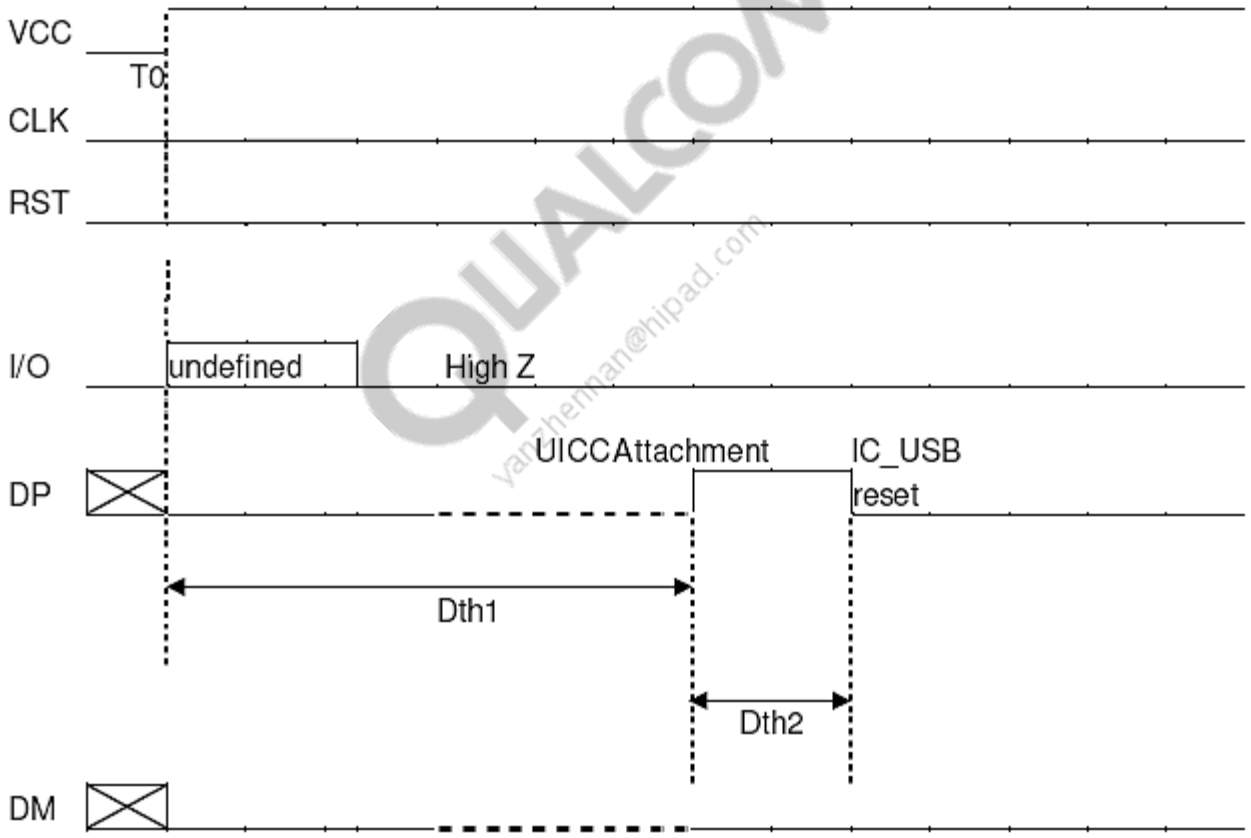


USB Activation

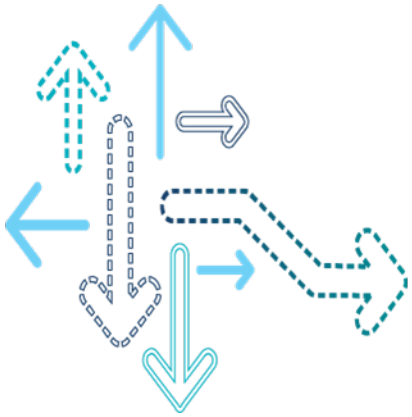
- USB attachment
  - Before attachment, the terminal shall activate its pull-down resistors on C4 and C8, and the UICC shall present high impedance on C4 and C8.
  - If C4 and C8 are maintained in state L for at least 20 ms by the terminal, the UICC shall continue with the attachment procedure.
  - The USB UICC attaches itself as a USB full-speed terminal by pulling the C4 line to state H for a maximum of 10 ms.
  - The terminal shall detect the UICC when the C4 line is driven to state H.
  - The terminal shall perform a USB RESET.
  - No clock shall be provided by the terminal.
- USB activation
  - The terminal shall assign a unique address to the USB UICC.
  - The terminal and UICC shall exchange information about voltage classes and current consumption.
  - The terminal shall configure the USB UICC for applications that it is running (ICCD power-up sequence).

IC-USB Host Timing Requirements

- Activation of USB UICC (Dth1 = 20 ms min; Dth2 = 10 ms max)



NV Item and Feature Support



NV Item Support

- NV 70210 (UIM hardware configuration) is updated to support a USB UICC card type. Currently, USB UICC is supported on slot 1 only.
- If NV hw_config.USB_UICC_SUPPORTED[slot] is set to FALSE, USB UICC enumeration is not attempted and the legacy ISO drivers are used to communicate with the card.
- The compile time feature FEATURE_UIM_REMOTE_UIM can be used to enable QMI UIM REMOTE service.

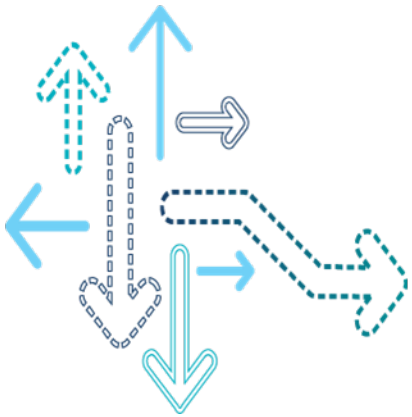
ID	Description	Full Path Name	Category
70202	QIPCall Is Conference Aware Mode	/nv/item_files/ims/qipcall_is_...	VOIP Sup.
70203	GNSS TLE Downloaded CellDb Pages	/cgps/nv/item_files/ulp/tle/g...	GPS
70204	GNSS TLE Downloaded RegionDb Pag...	/cgps/nv/item_files/ulp/tle/g...	GPS
70205	GNSS TLE Self Learned PosDb Pages	/cgps/nv/item_files/ulp/tle/g...	GPS
70206	GNSS TLE Write To Storage Enabled	/cgps/nv/item_files/ulp/tle/g...	GPS
70207	GNSS XTRA-T Simultaneous XTRA/XT...	/cgps/nv/item_files/ulp/tle/g...	GPS
70208	NAS CSFB Force LAU On AC Barred Cell	/nv/item_files/modem/nas/n...	Factory
70209	MCS TCXOMGR Field Aging Data	/nv/item_files/mcs/tcxomgr/f...	MCS
70210	UIM HW Config	/nv/item_files/modem/uim/u...	UIM
70211	UIM System Information	/nv/item_files/modem/uim/u...	UIM

Input	Value	Name (Partial)	Size	Type
2	VER_2	version	8	Signed Enum
1	TRUE	hw_config.USB_UICC_SUPPORTED[0]	8	Unsigned Enum
0	FALSE	hw_config.USB_UICC_SUPPORTED[1]	8	Unsigned Enum
0	FALSE	hw_config.USB_UICC_SUPPORTED[2]	8	Unsigned Enum
0	FALSE	hw_config.USB_UICC_SUPPORTED[3]	8	Unsigned Enum

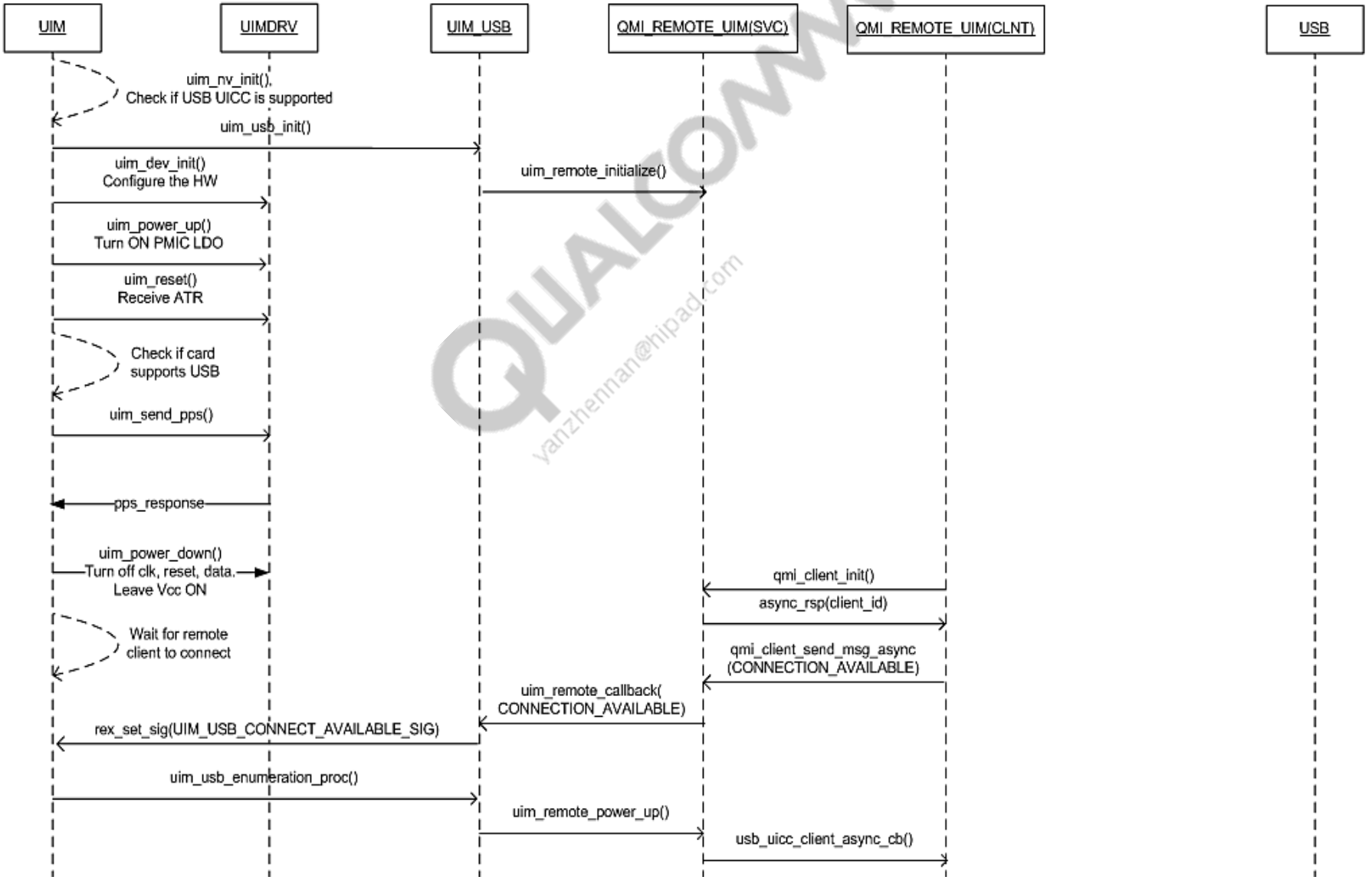
Feature Support

- In MSM8916 chipsets, the following featurization is also added:
  - FEATURE_UIM_USB_UICC

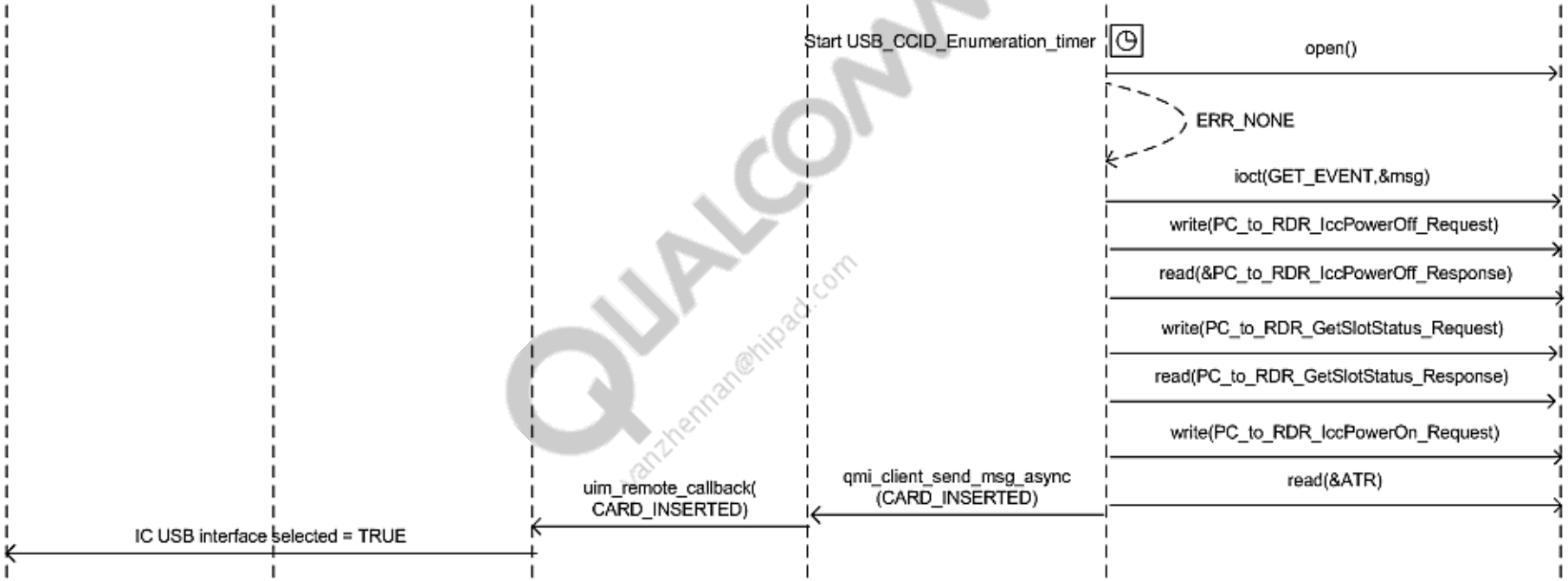
USB UICC Call Flow



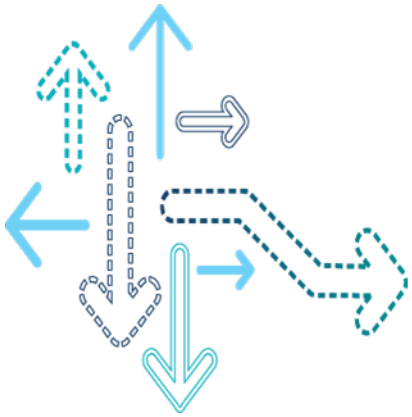
Call Flow



Call Flow (cont.)



USB UICC Log Analysis



Interaction Between Apps and Modem

- The following interaction occurs:

==========

Apps processor Modem processor

USB Driver <--> USB UICC QMI Client |||| <--> QMI Modem Service <-->
USB UICC <--> UIM Server <--> MMGSDI

==========

Scenario 1 – USB_NV_USB_UICC_INSERTED

18:46:45.430 uim.c 11314 UIM_1: Attempting power up at 3V
18:46:45.771 uimdrv.c 01932 UIM_1: uim power up @ 3 v
18:46:45.794 uimdrv.c 02058 UIM_1: uim_reset

//ATR indicates that card supports USB protocol.
18:46:45.824 uimgen.c 09563 UIM_1: USB MODE SUPPORTED = TRUE

// You send PPS that indicates USB protocol will be used. Else you will see message like "Sending Default PPS".
18:46:45.825 uimgen.c 05640 UIM_1: Sending USB PPS

//You turn off CLK/DATA/RESET and keep UIM Vcc ON
18:46:45.841 uimdrv.c 03581 UIM_1: uim_iso_power_down_before_usb_attach

// event = 0x2 indicates remote client has connected. Details of event enum can be found in qmi_uim_remote.h.
18:46:45.871 uimusb.c 00419 UIM_1: receive event: evt_ptr->evt=0x2

//We go to a stage where we wait for client to connect. If client has not connected, then we wait for duration of UIM_USB_POWERUP_WAITING_TIME. If client does not connect in this time, then we fall back to ISO T = 0/1, protocol
18:46:45.942 uimgen.c 07844 UIM_1: Waiting for AP client to connect....

Scenario 1 – USB_NV_ON_USB_UICC_INSERTED (cont.)

// At this point we know remote client has made a connection with QMI Remote UIM service and link is available. We send a command to the remote client to start USB activation.

18:46:45.942 uimusb.c 00565 UIM_1: UIM USB: Power up ICCD issued

18:46:48.114 uimusb.c 00419 UIM_1: receive event: evt_ptr->evt=0x6

// USB activation was successful and card sent an ATR over USB interface.

18:46:48.114 uimusb.c 00275 UIM_1: UIM USB ICCD attach occurred

18:46:48.114 uimgen.c 11847 UIM_1: UIM USB UICC ICCD POWER ON complete

//Select MF

18:46:48.114 uimdrv.c 02976 UIM_1: UIM in USB mode.Calling remote API's to send cmd

// Get response for Select

18:46:48.332 uim_remote.c 00784 UIM_1: Received get response command. Issuing new command

// Final response for Select MF

18:46:48.359 uim.c 05104 UIM_1: Response status 0, slot 0x1 uim_cmd_mode 0x1

18:46:48.444 uimgen.c 08608 UIM_1: generic_state_ptr 0xb, uim_reselect_mf 0x0

18:46:48.444 uimgen.c 08740 UIM_1: Processsing uim_generic_command_response for state 0xb

Scenario 1 – USB_NV_ON_USB_UICC_INSERTED (cont.)

18:46:48.488 uimgen.c 08608 UIM_1: generic_state_ptr 0xa, uim_reselect_mf 0x0

18:46:48.488 uimgen.c 08740 UIM_1: Processsing uim_generic_command_response for state 0xa

// Link Established

18:46:48.489 uim.c 07927 UIM_1: UIM link established with card over USB UICC interface

Scenario 2 – USB_NV_ON_ISO_CARD_INSERTED

//Since USB NV is enabled we do USB Initialization

00:00:00.263 uimusb.c 00153 UIM_1: uim_usb_init

//Register with QMI Remote UIM

00:00:00.263 uimusb.c 00208 UIM_1: UIM USB registering with remote qmi at power up

//Start USB UICC PUP STATE machine

00:00:00.263 uim.c 07628 UIM_1: Internal command to Reset the UIM for slot 0x1
00:00:00.263 uimdrv.c 03443 UIM_1: uim power down @ 1.8 v
00:00:00.279 uimgen.c 02583 UIM_1: Received internal USB UICC powerup command 0x100
00:00:00.302 uimdrv.c 02056 UIM_1: uim_reset

//Analyze the ATR and see if TB3 is set to C0. Since it is not set to C0, we continue with ISO powerup.

00:00:00.408 uimgen.c 05638 UIM_1: usb enabled 0x1 usb mode supported 0x0 fallback occured 0x0
00:00:00.408 uimgen.c 05664 UIM_1: Sending Default PPS
00:00:00.846 uim.c 07966 UIM_1: UIM link established with card over legacy ISO interface
00:00:00.848 uim.c 04418 UIM_1: Last DF1,DF2,EF 3f00 ffff 2fe2
00:00:00.848 uim.c 04422 UIM_1: New path 3f00 ffff 2f05

Scenario 3 – Hotswap – Replace USB Card with ISO

//Process USB card removal

22:24:04.315 uimdrv.c 09507 UIM_1: HOTSWAP: Start, For CARD REMOVED Interrupt

22:24:04.325 uimdrv.c 09771 UIM_1: HOTSWAP: Debounce logic Sample Count 0x1, Max Count 0x1, RT Card Staus = 0x0 [1: Card Inserted]

22:24:04.325 uimdrv.c 09791 UIM_1: HOTSWAP:Debounce logic ended successfully, processing card removal

//Send command to remote end to power down card, it may not necessarily power down the card since it was already removed but it will clean up the USB driver and close the USB driver bridge. It also informs the remote entity of card removal so that they can clear their state machine.

22:24:04.328 uimusb.c 00529 UIM_1: UIM USB UICC ICCD POWER OFF issued POWER DOWN CARD

22:24:04.328 uimusb.c 00548 UIM_1: UIM USB UICC ICCD POWER OFF issued, mode is 0x2

22:24:04.328 uimgen.c 07826 UIM_1: Turning off UIM USB UICC with QMI_UIM_REMOTE_POWER_DOWN_CARD

22:24:04.730 uimusb.c 00372 UIM_1: UIM USB:Remote card power down success

//Process Card Insertion (ISO - Process ISO power up state machine)

22:24:41.190 uimdrv.c 09502 UIM_1: HOTSWAP: Start, For CARD INSERTED Interrupt

22:24:09.078 uimdrv.c 09771 UIM_1: HOTSWAP: Debounce logic Sample Count 0x1, Max Count 0x1, RT Card Staus = 0x1 [1: Card Inserted]

22:24:09.078 uimdrv.c 09814 UIM_1: HOTSWAP: Debounce logic End, Unstable status: 0 [0=REMOVED 1=INSERTED]

Scenario 3 – Hotswap – Replace USB Card with ISO (cont.)

22:24:43.208 uimgen.c 03332 UIM_1: Received Reset command for UIM_HOTSWAP_CARD_INS_F
22:24:43.209 uimdrv.c 01926 UIM_1: uim power up @ 1.8 v
22:24:43.232 uimdrv.c 02056 UIM_1: uim_reset
22:24:43.338 uimdrv_clk.c 00374 UIM_1: FI and DI are supported
22:24:43.339 uimgen.c 05664 UIM_1: Sending Default PPS
22:24:43.777 uim.c 07966 UIM_1: UIM link established with card over legacy ISO interface

//Rest of the ISO powerup follows as mentioned before

Scenario 4 – Hotswap ISO Card Replaced with USB UICC

//Process Card Removal(ISO)

22:50:03.968 uimdrv.c 09507 UIM_1: HOTSWAP: Start, For CARD REMOVED Interrupt

22:50:03.978 uim.c 12821 UIM_1: HOTSWAP: uim_hotswap_send_card_removed_cmd is successfully send to uim

22:50:03.980 uimgen.c 03492 UIM_1: Received power down command

22:50:03.980 uimdrv.c 03443 UIM_1: uim power down @ 1.8 v

//Process card insertion (USB)

22:50:31.691 uimdrv.c 09502 UIM_1: HOTSWAP: Start, For CARD INSERTED Interrupt

22:50:31.792 uimdrv.c 09771 UIM_1: HOTSWAP: Debounce logic Sample Count 0x1, Max Count 0x14, RT Card Staus = 0x1 [1: Card Inserted]

//Finish debounce logic

22:50:33.708 uimdrv.c 09771 UIM_1: HOTSWAP: Debounce logic Sample Count 0x14, Max Count 0x14, RT Card Staus = 0x1 [1: Card Inserted]

22:50:33.708 uimdrv.c 09786 UIM_1: HOTSWAP: Debounce logic ended successfully, processing card insertion

//Start power up @ 1.8 V

22:50:33.710 uimdrv.c 01926 UIM_1: uim power up @ 1.8 V

22:50:33.733 uimdrv.c 02056 UIM_1: uim_reset

Scenario 4 – Hotswap ISO Card Replaced with USB UICC (cont.)

```
//Timeout on reset @ 1.8 V (since this is a 3.0 V card)
22:50:34.713          uim.c          10861  UIM_1: Timed out on the command response
22:50:34.713          uimdrv.c       03443  UIM_1: uim power down @ 1.8 V

//Switch voltage class to class B
22:50:34.716          uim.c          11320  UIM_1: Attempting power up at 3 V
22:50:34.728          uimdrv.c       03447  UIM_1: uim power down @ 3 V
22:50:34.759          uimdrv.c       01930  UIM_1: uim power up @ 3 V

//Perform reset @ 3.0 V
22:50:34.782          uimdrv.c       02056  UIM_1: uim_reset
22:50:34.813          uimdrv_clk.c   00374  UIM_1: FI and DI are supported

//Parse ATR and see if card supports USB
22:50:34.813          uimgen.c       09567  UIM_1: USB MODE SUPPORTED = TRUE

//Send USB specific PPS req
22:50:34.814          uimgen.c       05642  UIM_1: Sending USB PPS

//Power down ISO lines
22:50:34.830          uimdrv.c       03576  UIM_1: uim_iso_power_down_before_usb_attach

//Follow rest of the USB UICC power up state machine.
22:50:34.932          uimgen.c       07862  UIM_1: Turning on UIM USB UICC
22:50:37.278          uimusb.c       00284  UIM_1: UIM USB ICCD attach occurred
22:50:37.279          uimgen.c       11851  UIM_1: UIM USB UICC ICCD POWER ON complete
22:50:37.681          uim.c          07929  UIM_1: UIM link established with card over USB UICC interface
```


Scenario 5 – USB NV Off, Insert USB Card

- This should look like a 3.0 V UICC powerup.

```
//Power up in 1.8 V mode.
00:03:27.115        uim.c       07789  UIM_1: Internal command to Reset the UIM for slot 0x1
00:03:27.115        uimdrv.c    03441  UIM_1: uim power down @ 1.8 v
00:03:27.130        uimgen.c    02610  UIM_1: Received internal Powerup command 0x100
00:03:32.130        uimdrv.c    01911  UIM_1: uim power up @ 1.8 v

//Timed out waiting for ATR
00:03:33.086        uim.c       11132  UIM_1: Timed out on the command response
00:03:33.086        uimdrv.c    03441  UIM_1: uim power down @ 1.8 v

//Switch voltage class to 3.0 V
00:03:33.088        uim.c       11595  UIM_1: Attempting power up at 3V

//Card sends ATR
00:03:33.130        uimdrv.c    01915  UIM_1: uim power up @ 3 v
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[0]:0x3b
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[1]:0x9f
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[2]:0x94
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[3]:0x80
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[4]:0x3f
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[5]:0xc2
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[6]:0xc0
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[7]:0x80
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[8]:0x31
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[9]:0xe0
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[10]:0x73
00:03:33.183        uimgen.c    08824  UIM_1: atr byte[11]:0xfe
```


Scenario 5 – USB NV Off, Insert USB Card (cont.)

//Card sends ATR (continued)

```
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[12]:0x21
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[13]:0x13
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[14]:0x67
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[15]:0x80
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[16]:0x32
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[17]:0x40
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[18]:0x13
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[19]:0x56
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[20]:0xc1
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[21]:0x1
00:03:33.183        uimgen.c  08824  UIM_1: atr byte[22]:0x48
```

//Since the USB mode is turned off in NV, send default PPS

```
00:03:33.184        uimgen.c  05679  UIM_1: Sending Default PPS
00:03:33.200        uimgen.c  09781  UIM_1: The UIM is operating under T=0x0
```

//Select MF

```
00:03:33.542        uimgen.c  08659  UIM_1: generic_state_ptr 0x7, uim_reselect_mf 0x0
00:03:33.542        uimgen.c  08791  UIM_1: Processsing uim_generic_command_response for state 0x7
00:03:33.618        uimgen.c  08659  UIM_1: generic_state_ptr 0xb, uim_reselect_mf 0x0
00:03:33.618        uimgen.c  08791  UIM_1: Processsing uim_generic_command_response for state 0xb
```

Scenario 5 – USB NV Off, Insert USB Card (cont.)

//Send link established message to MMGSDI.

```
00:03:33.655        uim.c      08135  UIM_1: UIM link established with card over legacy ISO interface
00:03:33.656        uim.c      09519  UIM_1: Setting POLL timer upon successfull completion of the
command
00:03:33.658        uim.c      04462  UIM_1: Last DF1,DF2,EF 3f00 ffff 2fe2
00:03:33.658        uim.c      04466  UIM_1: New path 3f00 ffff 2f05
```

//MMGSDI gets card inserted event.

```
00:03:34.000        mmgsdi.c   07774  Received event: 0x0 in mmgsdi_evt_cb
00:03:34.000        mmgsdi.c   07947  MMGSDI_CARD_INSERTED_EVT, slot: 0x1
```


Scenario 6 – Fall Back to ISO Mode

- Slot 2 does not have support for USB UICC. If NV for USB UICC support is enabled and a USB card is inserted in slot 2, it falls back to ISO mode.

```
//Timed out on ATR at 1.8 V
00:10:31.183        uim.c       11132  UIM_2: Timed out on the command response
00:10:31.183        uimdrv.c    03441  UIM_2: uim power down @ 1.8 V
00:10:31.212        uim.c       11703  UIM_2: Cold Reset after timeout Rx-state 0x1 Tx-state 0x0

//Switch voltage class to 3.0 V
00:10:31.212        uimdrv.c   03445  UIM_2: uim power down @ 3 V
00:10:31.226        uimdrv.c   01915  UIM_2: uim power up @ 3 V
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[0]:0x3b
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[1]:0x9f
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[2]:0x94
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[3]:0x80
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[4]:0x3f
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[5]:0xc2
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[6]:0xc0
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[7]:0x80
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[8]:0x31
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[9]:0xe0
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[10]:0x73
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[11]:0xfe
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[12]:0x21
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[13]:0x13
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[14]:0x67
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[15]:0x80
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[16]:0x32
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[17]:0x40
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[18]:0x13
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[19]:0x56
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[20]:0xc1
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[21]:0x1
00:10:31.280        uimgen.c  08824  UIM_2: atr byte[22]:0x48
```

Scenario 6 – Fall Back to ISO Mode (cont.)

//Fallback has not occured yet and card supports USB mode so send USB specific PPS
00:10:31.281 uimgen.c 05663 UIM_2: usb enabled 0x1 usb mode supported 0x1 fallback occured 0x0
00:10:31.281 uimgen.c 05669 UIM_2: Sending USB PPS

// Waiting for remote AP client (QMI USB UICC Client) to connect.
00:10:31.297 uimgen.c 07895 UIM_2: Waiting for AP client to connect....

//After 4 seconds the timer expires and we fallback to ISO. The other fallback conditions are when USB enumeration fails (due to some error conditions in USB layer). or during normal operation any attempts to recover on USB interface fail too.
00:10:35.212 uimusb.c 01095 UIM_2: uim usb init timer expired
00:10:35.212 uimusb.c 00671 UIM_2: Initiating Fallback to ISO
00:10:35.212 uim.c 10594 UIM_2: Falling back to legacy ISO from IC USB interface

//After fallback we initiate a cold reset and try to power up the card in ISO mode.
// Power up the card at 1.8 V
00:10:35.212 uimdrv.c 03441 UIM_2: uim power down @ 1.8 V
00:10:35.227 uimgen.c 02610 UIM_2: Received internal Powerup command 0x100
00:10:35.227 uimdrv.c 01911 UIM_2: uim power up @ 1.8 V

//Timed on ATR at 1.8 V
00:10:36.183 uim.c 11132 UIM_2: Timed out on the command response
00:10:36.183 uimdrv.c 03441 UIM_2: uim power down @ 1.8 V

Scenario 6 – Fall Back to ISO Mode (cont.)

```
//Switch voltage class to 3.0 V
00:10:36.227        uimdrv.c       01915  UIM_2: uim power up @ 3 V
00:10:36.280        uimgen.c       08659  UIM_2: generic_state_ptr 0x1, uim_reselect_mf 0x0
00:10:36.280        uimgen.c       08791  UIM_2: Processsing uim_generic_command_response for state 0x1

//Received ATR at 3.0 V
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[0]:0x3b
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[1]:0x9f
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[2]:0x94
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[3]:0x80
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[4]:0x3f
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[5]:0xc2
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[6]:0xc0
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[7]:0x80
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[8]:0x31
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[9]:0xe0
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[10]:0x73
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[11]:0xfe
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[12]:0x21
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[13]:0x13
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[14]:0x67
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[15]:0x80
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[16]:0x32
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[17]:0x40
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[18]:0x13
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[19]:0x56
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[20]:0xc1
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[21]:0x1
00:10:36.280        uimgen.c       08824  UIM_2: atr byte[22]:0x48
00:10:36.280        uimdrv_clk.c   00380  UIM_2: FI and DI are supported
```

Scenario 6 – Fall Back to ISO Mode (cont.)

//Since the fallback occurred flag is set to true, we will not attempt USB mode powerup or PPS anymore. We will continue with ISO mode powerup state machine.

00:10:36.281 uimgen.c 05663 UIM_2: usb enabled 0x1 usb mode supported 0x1 fallback occured 0x1
00:10:36.281 uimgen.c 05679 UIM_2: Sending Default PPS

//Select MF over ISO interface, further go on to process card capabilities, read iccid states.

00:10:36.317 uim.c 05266 UIM_2: SW1 0x0,SW2 0x0, Response data length 0x4
00:10:36.317 uimgen.c 08659 UIM_2: generic_state_ptr 0x5, uim_reselect_mf 0x0
00:10:36.639 uim.c 05266 UIM_2: SW1 0x90,SW2 0x0, Response data length 0x28
00:10:36.639 uimgen.c 08659 UIM_2: generic_state_ptr 0x7, uim_reselect_mf 0x0
00:10:36.715 uim.c 05266 UIM_2: SW1 0x90,SW2 0x0, Response data length 0x19
00:10:36.715 uimgen.c 08659 UIM_2: generic_state_ptr 0xb, uim_reselect_mf 0x0

//Send link established to MMGSDI.

00:10:36.752 uim.c 08135 UIM_2: UIM link established with card over legacy ISO interface

//MMGSDI card inserted event.

00:10:37.098 mmgsdi.c 07774 Received event: 0x0 in mmgsdi_evt_cb
00:10:37.098 mmgsdi.c 07947 MMGSDI_CARD_INSERTED_EVT, slot: 0x2

Scenario 7 – USB Mode Recovery

//At the power up USB attach occurs and link established is sent for USB interface.

```
22:50:43.203    uimusb.c              00284  UIM_1: UIM USB ICCD attach occurred
22:50:43.203    uimgen.c              11851  UIM_1: UIM USB UICC ICCD POWER ON complete
22:50:43.575    uim.c                 07929  UIM_1: UIM link established with card over USB UICC interface
```

//Recovery triggerred

```
22:50:55.191    mmgsdi_common.c  02820  Sending down SEARCH command to UIM
22:50:55.191    mmgsdi_uim_uicc.c  04063  UICC SEARCH RECORD NUMBER: 0x1, SEARCH TYPE: 0x2
22:50:55.191    qmi_uim_remote.c    02028  Successfully queued qmi uim remote cmd 0x4
22:50:55.191    qmi_uim_remote.c    01721  Card operation req 0x4 send indication status : 0x0
```

//1st recovery

```
22:50:55.715    uim_remote.c          00185  UIM_1: Invalid resp 0x1 received setting command resp time out sig
22:50:55.715    uim.c                 10861  UIM_1: Timed out on the command response
22:50:55.739    uimusb.c              00525  UIM_1: UIM USB UICC ICCD POWER OFF issued TELECOM INTERFACE
22:50:56.000    uimusb.c              00350  UIM_1: Receive card error. evt_ptr->evt_data.card_error=0x3.
22:50:56.000    uimgen.c              11844  UIM_1: UIM USB UICC ICCD POWER OFF complete
22:50:56.000    uimgen.c              07862  UIM_1: Turning on UIM USB UICC
22:50:56.103    uimgen.c              11851  UIM_1: UIM USB UICC ICCD POWER ON complete
22:50:56.559    mmgsdilib.c           03195  In mmgsdi_get_recovery_data_sync
22:50:56.559    uimgen.c              08100  UIM_1: Sending Terminal Profile for UICC
22:50:56.816    uimgen.c              04384  UIM_1: UIM Recovery Complete
```

//Retry the command

```
22:50:56.857    uimgen.c              02661  UIM_1: Received internal Select command 0x103
22:50:57.494    qmi_uim_remote.c    01050  qmi_uim_remote_apdu_req_handler
22:50:57.494    uim_remote.c          00185  UIM_1: Invalid resp 0x1 received setting command resp time out sig
22:50:57.495    uim.c                 10861  UIM_1: Timed out on the command response
```

Scenario 7 – USB Mode Recovery (cont.)

```
//2nd recovery
22:50:57.518    uimgen.c      07832  UIM_1: Turning off UIM USB UICC with
QMI_UIM_REMOTE_POWER_DOWN_TELECOM_INTERFACE
22:50:57.787    uimgen.c      11844  UIM_1: UIM USB UICC ICCD POWER OFF complete
22:50:57.787    uimgen.c      07843  UIM_1: Waiting for AP client to connect....
22:50:57.787    uimgen.c      07862  UIM_1: Turning on UIM USB UICC
22:50:57.867    uimusb.c      00432  UIM_1: receive event: evt_ptr->evt=0x6
22:50:57.867    uimgen.c      11851  UIM_1: UIM USB UICC ICCD POWER ON complete
22:50:58.333    mmgsdilib.c   03195  In mmgsdi_get_recovery_data_sync
22:50:58.333    uimgen.c      08100  UIM_1: Sending Terminal Profile for UICC
22:50:58.573    uimgen.c      04384  UIM_1: UIM Recovery Complete

//Retry the same command
22:50:59.254    qmi_uim_remote.c  01050  qmi_uim_remote_apdu_req_handler
22:50:59.255    uim.c             10861  UIM_1: Timed out on the command response

//3rd recovery
22:50:59.255    uim.c          10861  UIM_1: Timed out on the command response
22:50:59.278    uimgen.c       07832  UIM_1: Turning off UIM USB UICC with
QMI_UIM_REMOTE_POWER_DOWN_TELECOM_INTERFACE
22:50:59.546    uimgen.c       11844  UIM_1: UIM USB UICC ICCD POWER OFF complete
22:50:59.625    uimgen.c       11851  UIM_1: UIM USB UICC ICCD POWER ON complete
22:51:00.321    uimgen.c       04384  UIM_1: UIM Recovery Complete

// UIM dequeue the command and check if the command has reached max number of attempts and then we
send a error response for this command
to MMGSDI
22:51:00.460    uimgen.c       01484  UIM_1: Reporting error for generic command 0x106
22:51:00.461    mmgsdi.c       05008  MMGSDI_PROCESS_RESPONSE IN TASK 0x1, cmd: 0x29, slot: 0x1
22:51:00.461    mmgsdi_common_rsp.c  02234  UIM Response parsing failed for Search
```

References

Ref.	Document	
Qualcomm Technologies		
Q1	*Application Note: Software Glossary for Customers*	CL93-V3077-1
Standards		
S1	*Smart Cards; UICC-Terminal Interface; Physical and Logical Characteristics*	ETSI TS 102 221 v7.8.0 (Feb 2007)
S2	*Smart Cards; UICC-Terminal Interface; Internet Protocol Connectivity between UICC and Terminal*	ETSI TS 102 483 V8.1.0 (Apr 2009)
S3	*Smart Cards; UICC-Terminal Interface; Characteristics of the USB Interface*	ETSI TS 102 600 v7.1.0 (Nov 2007)
S4	*Universal Serial Bus, Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices*	USB-ICC ICCD Rev 1.0 (Apr 2005)
S5	*Identification Cards – Integrated Circuit Cards – Part 3: Cards with Contacts – Electronic Interface and Transmission Protocols*	ISO 7816-3 (2006)
S6	*Identification Cards – Integrated Circuit Cards – Part 2: Cards with Contacts – Dimensions and Location of the Contacts*	ISO 7816-2 (2007)
S7	*Universal Serial Bus Specification Revision 2.0*	USB-IF (Apr 2000)
S8	*Inter-Chip USB Supplement to the USB 2.0 Specification Revision 1.0*	USB-IF (Mar 2006)
S9	*Smart Cards; Card Application Toolkit (CAT) (Release 7)*	ETSI TS 102 223 v7.2.0 (Jan 2006)
S10	*Digital Cellular Telecommunications System (Phase 2+) (GSM); Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface*	GSM 11.14 Rel.99 (1999)
Resources		
R1	*USB Multimedia SIM Card Handset Requirements, Handset Technical Team, Telecom Business Unit,* V 2.2	Gemalto (Jan 2008)

Questions?

https://support.cdmatech.com