CSIM-Capable Device Requirements

CDG Document 200

Version 1.0

April 2011

CDMA Development Group
575 Anton Boulevard, Suite 560
Costa Mesa, California 92626
PHONE +1 888 800-CDMA
+1 714 545-5211
FAX +1 714 545-4601
http://www.cdg.org
cdg@cdg.org

Notice

Each CDG member acknowledges that CDG does not review the disclosures or contributions of any CDG member nor does CDG verify the status of the ownership of any of the intellectual property rights associated with any such disclosures or contributions. Accordingly, each CDG member should consider all disclosures and contributions as being made solely on an as-is basis. If any CDG member makes any use of any disclosure or contribution, then such use is at such CDG member's sole risk. Each CDG member agrees that CDG shall not be liable to any person or entity (including any CDG member) arising out of any use of any disclosure or contribution including any liability arising out of infringement of intellectual property rights.

<page left blank intentionally>

Contents

Figures and Tables

Revision History

Date	Version	Description
April 2011	1.0	Initial release version (jointly authored, developed, reviewed and submitted by China Telecom and Qualcomm).

1. *Introduction*

1.1 Scope

This document defines the requirements for devices that support CSIM. They are consistent with 3GPP2 standard requirements and enable a uniform device implementation to ensure that devices complying with these requirements can be leveraged by all CDMA operators that use CSIMs and/or R-UIMs.

1.2 Requirements Overview

This document focuses on CSIM related device requirements which also allow R-UIM fallback. The specified requirements include two key components:

1. Capability of devices to use the operator configuration information on the CSIM. When a CSIM-capable device is used with a CSIM from any operator, the device requirements defined in this document apply.
2. Fallback capability of devices to ensure compatibility with both UICC and ICC cards in order to support all versions of CSIM and R-UIM applications on those cards.

The minimum device requirements include the following areas:

- General support for CSIM/UICC
- Device Operations, including support for:
    - BIP data download
    - 3G Phonebook
    - Fallback to work with an R-UIM
    - UTK/CCAT SMS-PP Download
- Voice Services
- Short Message Service (SMS)
- 3G Packet Data (3GPD)
- High Rate Packet Data (HRPD) (EV-DO)
- Applications, including support for WAP, MMS, Java, BREW Application Manager and Location Based Services (LBS)

1.3 Conventions

Each requirement in this document has a requirement number in this format: **DCn-m**, where **DC** represents a device that is CSIM capable, **n** represents the feature set or functional area and **m** represents the requirement number within that feature set or functional area. These requirements are also formatted in blue so the reader can visually identify the requirements more easily.

Verbal terms "***shall***" and "***shall not***" identify mandatory requirements that must be satisfied, "should" and "should not" indicate optional requirements that are preferred, and "may" and "may not" indicate optional requirements that may be followed.

Unless otherwise specified, 'device' means the CSIM-capable device.

1.4 Card Evolution

The following diagram depicts the CSIM-capable device that can interwork with different versions of R-UIM and CSIM on UICC and ICC.

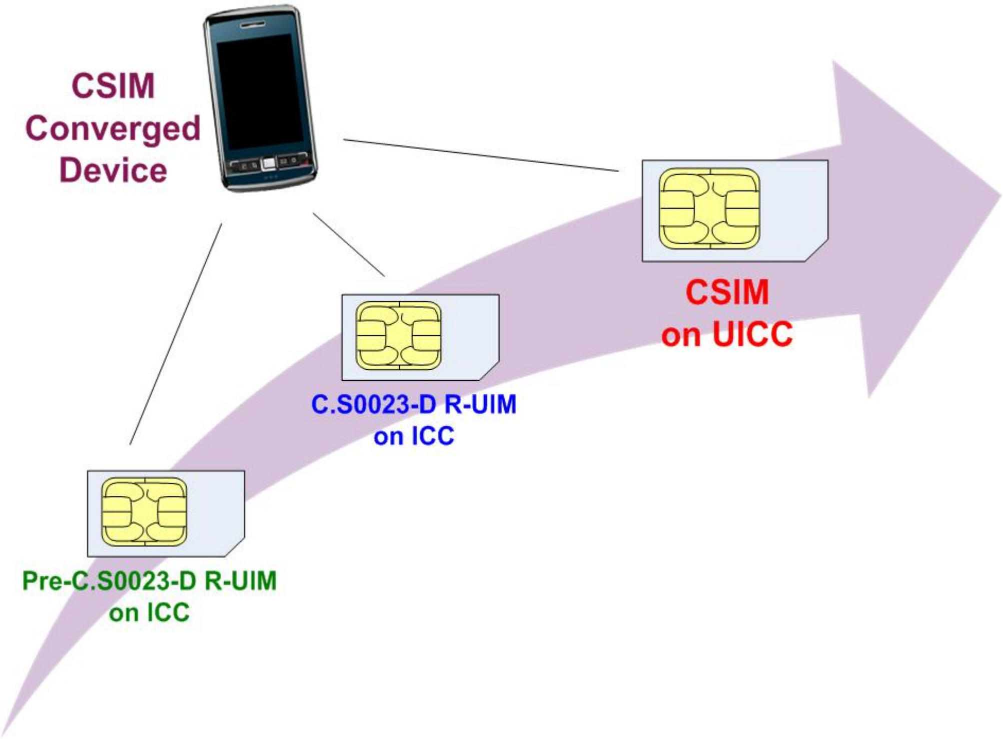
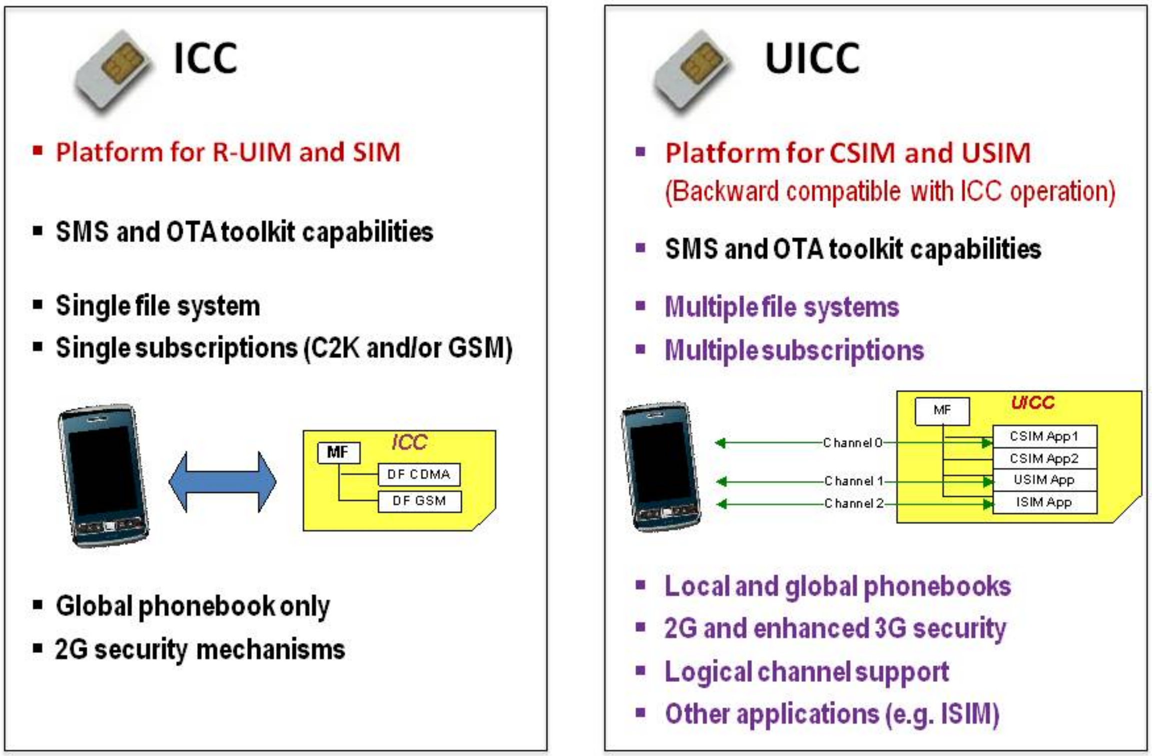


Figure 1 CSIM-Capable Device and Card Evolution

The following diagram shows some differences between an ICC and a UICC. CSIM is the CDMA Application on the UICC, and R-UIM is the CDMA Application on the ICC. R-UIM is present on the UICC too for interworking with devices that are not CSIM capable yet.



ICC

- Platform for R-UIM and SIM
- SMS and OTA toolkit capabilities
- Single file system
- Single subscriptions (C2K and/or GSM)
- Global phonebook only
- 2G security mechanisms

UICC

- Platform for CSIM and USIM
  (Backward compatible with ICC operation)
- SMS and OTA toolkit capabilities
- Multiple file systems
- Multiple subscriptions
- Local and global phonebooks
- 2G and enhanced 3G security
- Logical channel support
- Other applications (e.g. ISIM)

Figure 2 ICC versus UICC

2. CSIM Mechanisms

This section contains the fundamental device requirements for general CSIM and UICC support, security functions, carrier customization, UTK and CCAT, SMS-PP download and BIP download, device model and identification, and OTASP/OTAP support.

2.1 CSIM and UICC (DC1)

DC1-1 The device ***shall*** support UICC physical and logical characteristics as defined in [CS0074].

DC1-5 The device ***shall*** support the CSIM application on the UICC as defined in [CS0065].

DC1-10 The device ***shall*** support the following CSIM commands:

- SELECT
- STATUS
- READ BINARY
- UPDATE BINARY
- READ RECORD
- UPDATE RECORD
- SEARCH RECORD
- INCREASE
- VERIFY PIN
- CHANGE PIN
- DISABLE PIN
- ENABLE PIN
- UNBLOCK PIN
- DEACTIVATE FILE
- ACTIVATE FILE
- TERMINAL PROFILE
- ENVELOPE
- FETCH
- TERMINAL RESPONSE
- MANAGE CHANNEL
- GET RESPONSE

2.2 Security (DC5)

DC5-1 The device ***shall*** support the following voice and SMS security commands as defined [CS0065]:

- Manage SSD (Update & Confirm SSD)
- Base Station Challenge
- Generate Key / VPM
- Authenticate

DC5-5 The device ***shall*** support the following 3G Packet Data security commands as defined in [CS0065]:

- Compute IP Authentication

2.3 Carrier Customization (DC10)

DC10-1 If the service provider name is provisioned in EF_{SPN} on the CSIM, the device ***shall*** display that information on the idle screen.

DC10-5 The device shall support decoding of the following encoding types defined in [CR1001] for the character string data present in EF_{SPN}:

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters[1]
- "Unicode"[2]

DC10-10 If an application label has been provisioned for a particular application in $EF_{AppLabels}$, the device's user interface ***shall*** display this text label with the associated icon or menu item used to launch that application (e.g., "Content World").

DC10-15 The device shall support decoding of the following encoding types defined in [CR1001] for the character string data present in $EF_{AppLabels}$:

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters
- "Unicode"

DC10-20 If an application label has not been provisioned for a particular application in $EF_{AppLabels}$, the device's default label ***shall*** be displayed (e.g., "MMS").

---

[1] The characters are encoded the same way when the encoding type is Octet, Unspecified, or 7-bit ASCII.

[2] Per Clause D98, Section 3.10 "Unicode Encoding Schemes" in [UNICODE], if BOM (byte order mark) is not present, the bytes for each character are in big-endian order. Otherwise, BOM indicates the byte order explicitly.

2.4 Toolkit Support (DC15)

DC15-1 The device ***shall*** provide an icon and/or a menu item for the user to select so that the user will be able to access the UTK or CCAT menus from the applications on the CSIM.

2.4.1 UTK with SMS-PP Download

DC15-50 The device ***shall*** support the proactive and envelope commands defined in the UIM Toolkit specification [CDG76].

DC15-55 The device ***shall*** support the UIM Toolkit (UTK) SMS-PP data download mechanism as defined in [CDG76].

2.4.2 CCAT with SMS-PP and BIP Download

DC15-100 The device ***shall*** support the proactive and envelope commands defined in the CCAT specification [CS0035].

DC15-105 The device ***shall*** support the CCAT SMS-PP data download mechanism as defined in [CS0035].

DC15-110 The device ***shall*** support the following CCAT Bearer Independent Protocol (BIP) commands and events for Remote File Management and Remote Application Management as defined in [CS0035]:

- OPEN CHANNEL
- CLOSE CHANNEL
- RECEIVE DATA
- SEND DATA
- GET CHANNEL STATUS
- Event: Data Available
- Event: Channel Status

DC15-115 The device ***shall*** support the CCAT BIP OPEN CHANNEL command with the following parameter options as defined in *section 6.4.27* in [TS102.223]:

- Default Bearer with both UDP and TCP in Client Mode
- Link Establishment:
  - On demand
  - Immediate
- Destination Address:
  - IPv4
  - IPv6 [3]

---

[3] This depends on the device’s overall support for IPv6. If the device supports IPv6, requirement for BIP’s IPv6 address is mandatory.

- Destination Port number
- Buffer Size
- Alpha Text display
    - If it is present with non-null text, user confirmation is required.
    - If it is present with null text, no display to the user occurs.
    - If it is absent, it is up to the device to decide whether to display any text or not.

DC15-120 The device may support the CCAT BIP OPEN CHANNEL command with other bearer types and transport level types.

DC15-125 The device ***shall*** support the CCAT BIP SEND DATA command with the following parameter options as defined in *section 6.4.30* of [TS102.223]:

- Send Mode
    - Immediate
    - Buffered
- Alpha Text display

DC15-130 The device ***shall*** support the CCAT BIP RECEIVE DATA command with the following parameter options as defined in *section 6.4.29* of [TS102.223]:

- Alpha Text display

DC15-135 The device ***shall*** support the CCAT BIP CLOSE CHANNEL command with the following parameter options as defined in *section 6.4.28* of [TS102.223]:

- Alpha Text display

DC15-140 The device ***shall*** support the CCAT BIP Channel Status event with the following parameter options as defined in *section 7.5.11* of [TS102.223]:

- Channel Identifier
- Channel Status
    - Link not established or Packet data service not activated
    - Link established or Packet data service activated

DC15-145 The device ***shall*** support the CCAT BIP Data Available event with the following parameter options as defined in *section 7.5.10* of [TS102.223]:

- Data Length
- Channel Status
    - Link not established or Packet data service not activated
    - Link established or Packet data service activated

2.5 Device Model and Identification (DC20)

DC20-1 The device ***shall*** support MEID.

DC20-5 The device ***shall*** be provisioned with a properly formed MEID.

DC20-10 The device ***shall*** be provisioned with an ESN containing the pESN value derived from the device's MEID

DC20-15 The device ***shall*** support EUIMID, which is either SF_EUIMID or LF_EUIMID.

DC20-20 If service n34 (SF_EUIMID-based EUIMID) is activated in EF_{CST} (CDMA Service Table), the device ***shall*** use EF_{USGIND} (Usage Indicator) to determine whether to use the Short Form Expanded UIM Identifier (SF_EUMID) or MEID for network identification.

DC20-25 Just as the device writes its ESN/MEID to the CSIM during power-up, it ***shall*** also write its manufacturer information, model information, and software version information to EF_{Model} on the CSIM.

DC20-30 The device ***shall*** support the following encoding types defined in [CR1001] for the character strings in EF_{Model}:

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters
- "Unicode": See [UNICODE] for allowed characters

2.6 Service Provisioning (DC35)

DC35-1 The device ***shall*** support the following OTASP/OTAPA commands:

- Generate Public Key
- Key Generation Request
- Commit
- Validate
- Configuration Request
- Download Request
- SSPR Configuration Request
- SSPR Download Request
- OTAPA Request

DC35-5 The device ***shall*** support the download of Concatenated Preferred Roaming List (cPRL) to EF_{PRL} on CSIM using OTASP/OTAPA.

DC35-10 The device ***shall*** support the download of EPRL (Extended PRL) to EF_{EPRL} on CSIM using OTASP/OTAPA.

2.7 Configuration Data Sources (DC45)

A CSIM-capable device can work with a CSIM that is provisioned with 1x and HRPD configurations specific to a subscriber (i.e., subscription and access network authentication credentials). The CSIM also contains 3GPD configuration. All the other operator specific configurations come from the following sources in the following priority order:

a. CSIM
b. Device memory
c. User input

DC45-1 The device ***shall*** always use the configuration for 1x subscription and access network authentication from the CSIM.

DC45-5 If the device supports HRPD, the device ***shall*** always use the configuration for HRPD access network authentication from the CSIM.

DC45-10 The device ***shall*** always use the 3GPD configuration from the CSIM.

DC45-15 The device ***shall*** use the following parameters from the CSIM if they are available on the CSIM. If the CSIM is not configured with these parameters, the device ***shall*** fallback to obtain these parameters from the device memory or from user input, in that priority order:

- SMS configuration
- WAP Browser configuration, if WAP Browser is supported on the device
- MMS configuration, if MMS is supported on the device
- Java Download URL, if Java Download is supported on the device
- BREW Mobile Shop configuration, if BREW Mobile Shop is supported on the device
- LBS configuration, if LBS is supported on the device

DC45-25 If the device does not read a configuration (e.g. configuration for MMS) from the CSIM because it is absent from the CSIM, the device ***shall*** try to read the configuration from the device memory, and should allow the user to modify the configuration stored in the device memory.

DC45-30 If the device does not read a configuration (e.g. configuration for MMS) from the CSIM or the device because it is absent from both the CSIM and the device, the device ***shall*** allow the user to manually enter the configuration into the device memory, and should allow the user to modify the configuration stored in the device memory.

DC45-35 Any configuration that is entered by the user manually ***shall*** be stored in the device's non-volatile memory so that the configuration persists across device power cycles.

3. *Fallback to R-UIM (DC50)*

This section contains requirements for the device to work with an R-UIM for the purpose of supporting backward compatibility of the cards.

DC50-1	When a CSIM-capable device is used with a pre-C.S0023-D R-UIM, it ***shall*** support voice and SMS based on the provisioning in the R-UIM and support all the other features based on provisioning in the device.
DC50-5	When a CSIM-capable device is used with a C.S0023-D R-UIM, it ***shall*** support voice, SMS, 3GPD and other features enabled by C.S0023-D based on the provisioning in the R-UIM, as defined in [CDG167].
DC50-10	When a CSIM-capable device using a pre-C.S0023-D R-UIM sets up a tethered data call using Password Authentication Protocol (PAP) authentication in Relay Model, it ***shall*** perform PAP authentication using credentials from the terminal.[4]
DC50-15	When a CSIM-capable device using a pre-C.S0023-D R-UIM sets up a tethered data call using the Challenge Handshaking Authentication Protocol (CHAP) authentication in Relay Model, it ***shall*** perform CHAP authentication using credentials from the terminal.

---

[4] In this document, Terminal means a laptop or some other computing device that is connected to the device in tethered mode.

4. Voice (DC55)

This section contains the device requirements for supporting voice operations.

DC55-1 Voice services on the device ***shall*** retrieve and use the Voice configuration information provisioned on the CSIM.

DC55-5 The device ***shall*** support Abbreviated Dialing Numbers (i.e., phonebook) stored on the CSIM.

DC55-10 The device may support Fixed Dialing Numbers stored on the CSIM.

DC55-15 The device ***shall*** have the capability to store and retrieve internationally formatted numbers to and from the CSIM.

DC55-18 The device ***shall*** support a user interface menu for the user to select among calling features.

DC55-20 The device ***shall*** read all applicable calling feature codes from the CSIM, and map them to the appropriate calling features displayed in the user interface menu.

DC55-25 The device may allow the user to manually enter the calling feature codes to be mapped to calling features in the user interface menus, if those calling feature codes are not present on the CSIM. Alternatively the device may fall back to the default set of calling feature codes valid for the respective operator.

DC55-30 The device ***shall*** be provisioned with a list of emergency numbers.

DC55-35 The device ***shall*** always permit calls to emergency numbers, even if no CSIM is inserted.

DC55-40 The device ***shall*** allow the user to dial emergency numbers stored on the CSIM and device when CSIM is present.

DC55-45 The device should allow the user to add emergency numbers, but should disallow the user to delete emergency numbers provisioned by the manufacturer.

DC55-50 The device should support SDN (Service Dialing Numbers).

DC55-55 The device should support ICI (Incoming Call Information).

DC55-60 The device should support OCI (Outgoing Call Information).

4.1 3G Phonebook

DC55-100 The device shall support 3G Phonebook stored under DF$_{\text{PHONEBOOK}}$ as defined in [CS0065].

DC55-105 If the device supports 3G Phonebook, it ***shall*** support the Global Phonebook stored under the MF.

DC55-110 If the device supports 3G Phonebook, it may support the Local Phonebook stored under the CSIM ADF.

5. SMS (DC60)

This section contains the device requirements for supporting SMS operations.

DC60-1 The SMS client on the device ***shall*** retrieve and use the SMS configuration information provisioned on the CSIM.

DC60-5 The device should perform SMS retries using the retry parameters provisioned on the CSIM.

DC60-10 The device ***shall*** allow the user to store SMS messages to the CSIM.

DC60-15 The device should automatically store received SMS messages to CSIM.

DC60-20 The device should allow the user to modify the messages on the CSIM.

DC60-25 The device ***shall*** allow the user to delete the messages from the CSIM.

DC60-30 The device should allow the user to store SMS Parameters to the CSIM.

DC60-35 The device should allow the user to modify SMS Parameters on the CSIM.

DC60-40 The device should allow the user to delete SMS Parameters from the CSIM.

DC60-45 The device should use SMS Parameters from the CSIM when sending MO SMS messages.

DC60-50 The device should allow the user to choose one of the SMS Preferences records for use with SMS.

DC60-55 The device should use MESSAGE_ID from the CSIM when sending MO SMS messages and increment it by 1.

6. *3G Packet Data (DC65)*

This section contains the device requirements for supporting 3G Packet Data operations.

6.1 General

DC65-1 3GPD services on the device ***shall*** retrieve and use the 3GPD configuration information provisioned on the CSIM.

DC65-5 The device ***shall*** support both PAP and CHAP authentication for Simple IP using credentials and authentication algorithms on the CSIM.

DC65-10 If the device supports Mobile IP, the device ***shall*** support Mobile IP authentication using credentials and authentication algorithms on the CSIM.

DC65-15 If the device supports Mobile IP, the device ***shall*** support Mobile IP to Simple IP fallback based on the flag in $EF_{3GPDOPM}$.

DC65-20 The device should support the following features based on the parameters on the CSIM:

- Extended Packet Zone Identifiers (EPZID)
- Hysteresis Activation Timer (HAT)
- TCP Keep-alive Idle Timer

DC65-25 The device ***shall*** restore the dormant timer to the value contained in EF_{DGC} when an application exits. This prevents an application from changing the dormant timer to a value that may be inappropriate for other applications.

DC65-30 The device ***shall*** support tethered-mode data calls in Relay Model using PAP credentials from the terminal.

DC65-35 The device ***shall*** support tethered-mode data calls in Relay Model using CHAP credentials from the terminal.

DC65-40 The device ***shall*** support tethered-mode data calls in Network Model using PAP credentials from the CSIM.

DC65-45 The device ***shall*** support tethered-mode data calls in Network Model using CHAP credentials from the CSIM.

6.2 Multiple Profiles

DC65-200 The device ***shall*** support Multiple User Profiles for Simple IP based on provisioning information in $EF_{3GPDUPPExt}$[5], as well as EF_{SIPUPP}.

DC65-205 The device ***shall*** support Multiple User Profiles for Mobile IP based on provisioning information in $EF_{3GPDUPPExt}$[6], as well as EF_{MIPUPP}.

---

[5] $EF_{SIPUPPExt}$ has been renamed to $EF_{3GPDUPPExt}$ in the to-be-published 3GPP2 C.S0065-B v2.0.

[6] $EF_{MIPUPPExt}$ has been removed in the to-be-published 3GPP2 C.S0065-B v2.0. Instead, the extension block in $EF_{3GPDUPPExt}$ is used for both Mobile IP profiles and SIP profiles.

DC65-210 The devices ***shall*** resolve the proper user profile identifier (i.e., the NAI index) based on the identifier of the application to be launched.

DC65-215 When performing Mobile IP to Simple IP fallback, the device ***shall*** fall back from a Mobile IP profile to a corresponding Simple IP profile that has the same Network Address Identifier (NAI) index.

6.2.1 Profile Arbitration for Concurrent Applications

DC65-300 The device ***shall*** reuse the existing data session if the newly launched application uses the same profile as the one being used by the existing data session.

DC65-305 The device ***shall*** preempt the existing data session and set up a new data session if the priority of the profile associated with the newly launched application is higher than the priority of the profile being used by the existing data session.

DC65-310 The device ***shall*** reject the data session setup request from a newly launched application if the priority of the profile associated with the newly launched application is lower than the priority of the profile being used by the existing data session.

DC65-325 When an LBS data session needs to be established but there is no existing data session active, the default LBS profile ***shall*** be used for establishing a data session.

Note: If $EF_{3GPDUPPExt}$ *in the CSIM has more than one profile with the LBS application type set in the application bit mask, the LBS profile with the lowest priority is treated as the default profile.*

DC65-330 If the LBS data session is released due to the launch of an application using a higher priority profile, the device may re-launch the LBS application if the profile associated with the newly established data session also supports the LBS application type.

DC65-335 The device ***shall*** perform device specific arbitration for concurrent applications based on its own policy, when the profile associated with a newly launched application is different from the profile associated with the existing data session but the priorities of these two profiles are the same.

NOTE: For example, the device may perform one of the following actions:

- *Reject data session setup for the newly launched application and continue with the existing data session;*
- *Close or suspend the applications that use the current data session, release the current data session, establish a new data session using the profile associated with the newly launched application;*
- *Prompt the user (e.g. via a pop-up menu) to let user decide whether to launch the new application with a new data session or not..*

7. HRPD (1xEV-DO) (DC70)

DC70-1 For HRPD, the device ***shall*** perform A12 (AN-AAA) authentication for HRPD access using access credentials and authentication algorithms on the CSIM.

DC70-5 The device should support HRPD Rev 0.

DC70-10 The device should support HRPD Rev A.

DC70-15 The device should support 1x and HRPD hybrid operations.

DC70-20 The device should support Receive Diversity.

8. *Applications*

This section contains the device requirements for supporting various applications and services.

8.1 WAP Browser (DC75)

DC75-1 The device should support OMA WAP 2.0 Browser.

DC75-5 The device ***shall*** retrieve and use the WAP browser configuration provisioned on the CSIM.

DC75-10 If the operator provisions bookmarks on the CSIM, the device ***shall*** present these bookmarks to the user.

DC75-15 The device should allow the user to save additional bookmarks on the CSIM.

DC75-20 The device ***shall*** be capable of displaying the web pages based on the bookmarks on the CSIM.

DC75-25 The device ***shall*** allow the user to change any bookmark on the CSIM.

8.2 MMS (DC80)

DC80-1 The device should support MMS.

DC80-5 The MMS client on the device ***shall*** retrieve and use the MMS configuration information provisioned on the CSIM.

DC80-7 If the CSIM does not contain the MMS WAP gateway configuration, the device may use that information from the device memory.

DC80-10 The device ***shall*** support MMS WAP gateway provisioned as either a domain name (PXADDR-FQDN) or IP address (PXADDR) on the CSIM.

DC80-15 If there are more than one MMS connectivity parameter sets including the WAP gateway provisioned on the CSIM, the device should fall back to the next MMS connectivity parameter set if the device fails to connect to the MMS server using the current connectivity parameter set.

DC80-20 The device ***shall not*** send MMS messages larger than the Max Message Size provisioned on the CSIM.[7]

DC80-25 The device ***shall*** perform MMS retries based on retry times and retry interval values provisioned on the CSIM.

DC80-30 The device ***shall*** wait for a duration indicated in the Mobile Messaging Service Center (MMSC) timeout value provisioned on the CSIM before declaring an MMSC timeout.

---

[7] The maximum MMS message size sent by a device should be the lower of the Max Message Size Value in $\text{EF}_{\text{MMSConfig}}$ and the maximum message size value in the device's User Agent Profile.

DC80-35 The device should read and use MMS User Preferences, if they are present on the CSIM.

DC80-40 The device should support the capability of updating MMS User Preferences on the CSIM.

DC80-45 The device should provide an option for the user to specify which MMS User Preferences record will be used when there are multiple User Preferences records on the CSIM.

DC80-50 If there are MMS Notifications present on the CSIM, the device should read them from the CSIM, present them to the user, and use those notifications to receive MMS messages from the network.

DC80-55 The device should support the capability of storing MMS Notifications on the CSIM.

DC80-60 If the device supports the capability of storing MMS Notifications on the CSIM, it should provide an option for the user to specify where the received MMS Notifications are stored (i.e., on the device or on the CSIM).

DC80-65 If the device supports the capability of storing MMS Notifications on the CSIM, it ***shall*** follow the procedure defined in [XS0016-0] to update the status fields on the CSIM.

DC80-70 If the device supports the capability of storing MMS Notifications on the CSIM, it ***shall*** record the time it receives the MMS notification into the MMS Notification PDU on the CSIM using the RFC2822 Date header.

Reason: If the Date header is not added to the MMS Notification PDU, the expiry time displayed to the user would be relative (e.g., “The message will expire in 2 days”) and would not be valid when the same notification is read sometime later (e.g. after two days, the user would still see “The message will expire in 2 days”).

DC80-75 The device should allow the user to preview the message before it is sent.

DC80-80 The device should display a progress bar when a message is being submitted.

DC80-85 The device should allow the user to access the phonebook when the device displays the MMS application menus.

DC80-90 The device should allow the user to distinguish between read and unread messages.

DC80-95 The device should allow the user to enter multiple recipient addresses when a message is composed.

DC80-100 The device should allow the pictures and audios stored in the device’s gallery or downloads folder to be attached while sending a message.

DC80-105 The device should use MMS to upload a picture taken by the camera to a server when selected.

8.3 Java (DC85)

DC85-1 The device should support Java Virtual Machine (JVM) required to support Java applications.

DC85-5	If the operator has provisioned a Java download URL in EF_{JDL} on the CSIM, the Java download client on the device ***shall*** use this URL..
DC85-10	For Java application download, the 3GPD user profile to be used for establishing a data session for the download ***shall*** be the one having the Java bit enabled in the application bitmask or the one having the Unspecified bit enabled in the application bitmask if the Java bit is not enabled in any profiles.

8.4 BREW (DC90)

DC90-1	The BREW client on the device ***shall*** retrieve and use the BREW configuration information provisioned on the CSIM.
DC90-5	The device may support the fallback of BREW configuration from the CSIM to those on the device when the CSIM does not have BREW configuration.
DC90-10	If the device falls back to NV for BREW configuration, the device ***shall*** delete all applications downloaded from the previous carrier due to Carrier ID mismatch.
DC90-15	The device ***shall*** use BREW provisioning data only from the card when BREW service in the EF_{CST} on the CSIM is enabled.
DC90-20	The device ***shall*** allow the user to use a BREW icon or menu item to connect to the BREW download server provisioned on the CSIM.
DC90-25	The device ***shall*** perform BREW download based on BREW Download Flag values provisioned on the CSIM.
DC90-30	The device ***shall*** perform BREW authentication based on the BREW Download Authentication Policy value provisioned on the CSIM.
DC90-35	The device ***shall*** use the BREW Carrier ID, Teleservice ID, Subscriber ID values provisioned on the CSIM.
DC90-40	The device ***shall*** ensure that previously downloaded BREW configuration data and applications are not accessible when a CSIM with a different BREW Carrier ID value is used.
DC90-45	The device ***shall*** perform BREW application execution based on the BREW Application Execution Policy provisioned on the CSIM.
DC90-50	When a CSIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall*** prevent the applications downloaded by the previous subscriber from being launched.
DC90-55	When a CSIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall*** retain the applications downloaded by the previous subscriber.
DC90-60	When a CSIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall*** allow the user to manually delete the applications associated with the previous subscriber ID if the RUIM_DEL_OVERRIDE flag on the CSIM is enabled.
DC90-65	The OEM ***shall*** obtain a single Platform ID for a device that will be used among all operators.

8.5 LBS (DC95)

LBS User Plane architectures use IP bearer to exchange services layer and positioning layer signaling information between the device and the location servers.

There are 2 types of User Plane LBS architectures deployed by CDMA operators:

- V2 Non-Trusted Model, in which the device is required to communicate with a Mobile Positioning Center (MPC) for LBS service authorization prior to communicating with a Position Determination Entity (PDE) server
- Trusted Model, in which the device is not required to communicate with a Mobile Positioning Center (MPC) for LBS service authorization prior to communicating with a Position Determination Entity (PDE) server

There are 3 types of positioning modes that can be invoked by an application on the device:

- A-GPS MS-Assisted Mode, in which the device communicates with the PDE to exchange assistance data for every position fix request. The final position is calculated and sent to the device by the PDE.
- A-GPS MS-Based Mode, in which the device communicates with the PDE intermittently (typically every 60 or 90 minutes) to exchange assistance data. The final position is calculated by the device.
- Standalone Mode, in which the device autonomously calculates its own position without any assistance data from the PDE. The performance of Standalone Mode can be improved by using XTRA assistance information. To download XTRA assistance information the device connects via internet to a XTRA server and downloads an updated XTRA data file which contains 7 days of orbital predictions.

DC95-1 The device ***shall*** retrieve and use the LBS configuration information provisioned on the CSIM.[8]

DC95-5 The device should allow the user to turn on/off all LBS functions.

8.5.1 A-GPS

DC95-200 The device should support V2 Non-Trusted Model for User Plane LBS functions.

DC95-205 The device should support Trusted Model for User Plane LBS functions.

DC95-210 If the device supports V2 Non-Trusted Model or Trusted Model, the device ***shall*** support IS-801-1 LBS User Plane call flows for MS-Assisted and MS-Based positioning mode operations.

---

[8] See the 3GPD section of this document for the special cases of LBS working with multiple user profiles.

DC95-215 If the device supports LBS User Plane Trusted Model and the CSIM has valid configuration for the PDE address, the device ***shall*** perform Trusted Model LBS operations.

DC95-220 If the device supports V2 Non-Trusted Model and the CSIM has valid configuration for MPC address, the device ***shall*** perform V2 Non-Trusted Model LBS operations.

DC95-225 If the device supports V2 Non-Trusted Model, the device ***shall*** support SMS Teleservice 65001 for receiving the LBS trigger from the network.

DC95-230 If the device supports V2 Non-Trusted Model, the device ***shall*** support the notification and verification procedure involving the user's response.

DC95-235 If the device supports V2 Non-Trusted Model or Trusted Model, the device ***shall*** support WAP Pull as the trigger from the network to initiate an LBS session.

DC95-245 The device ***shall*** use a 3GPD user profile associated with the LBS application type for setting up a data session only when the requested data session is for A-GPS services.

8.5.2 Standalone GPS

DC95-300 The device should support Standalone GPS.

DC95-305 If the device supports Standalone GPS, it should support XTRA.

DC95-310 If the device supports XTRA and the CSIM has valid configuration for XTRA, the device ***shall*** be able to perform Standalone GPS with XTRA data.

DC95-315 If the device supports XTRA and the CSIM has valid configuration for XTRA, the device ***shall*** download XTRA data using the XTRA configuration from the CSIM.

DC95-320 The device ***shall*** support Dynamic Mode as configured on the CSIM (i.e., falling back to standalone GPS as needed if Standalone GPS is supported).

DC95-325 When the device is out of CDMA coverage, the device should continue to support LBS using mechanisms not requiring CDMA service.

DC95-330 The device ***shall*** use a 3GPD user profile associated with the Unspecified application type for setting up a data session when the requested data session is for XTRA.

9. *Appendix: Arbitration of Multiple Profiles*

This chapter provides information on different levels of arbitration for concurrent applications and describes some typical scenarios related to arbitration of multiple profiles, as a design guideline for device vendors.

9.1 Example Multiple Profiles on CSIM

Below are some example configuration of multiple profiles provisioned in EF_{SIPUPP} and $EF_{3GPDUPPExt}$ on the CSIM.

Table 9-1 Example of Multiple Profiles Parameters

Fields	**Profile 1** **(for private IP access)**	**Profile 2** **(for public IP access)**
NAI_ENTRY_INDEX	1	2
NAI	“private@doamin.com”	“public@domain.com”
Priority	100	100
Applications	• ‘MMS’ • ‘WAP Browser’	• ‘Unspecified’ • ‘Terminal’
Auth. Algorithm	CHAP & PAP	CHAP & PAP
…	…	…

Application types MMS and WAP Browser are associated with Profile 1, while all the other applications and tethered data calls are associated with Profile 2.

In this example, when an application specifically identifies itself as “MMS” or “WAP Browser”, Profile 1 is used to set up the data session. When an application identifies itself as any other valid application type including the “Unspecified” application type or does not specify any application type, Profile 2 will be used to set up the data session.

The diagram below illustrates how the data applications are mapped to the profiles stored on the CSIM.

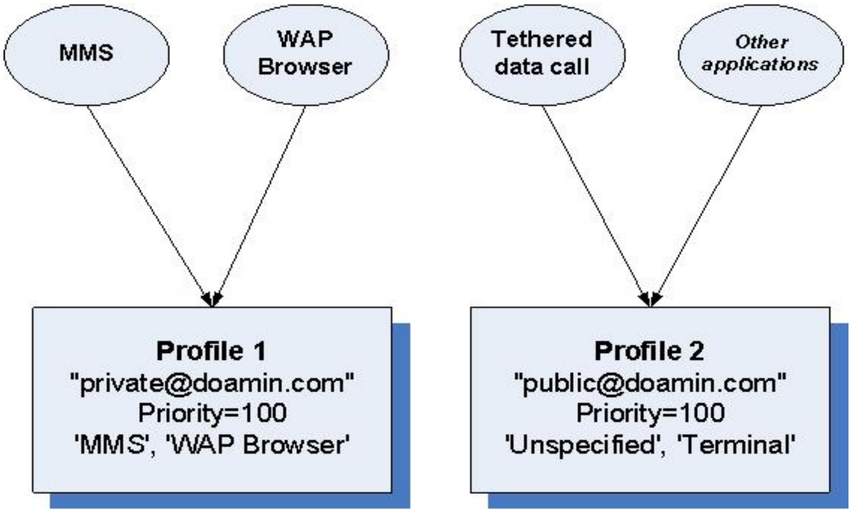


Figure 3 Mapping from Applications to Profiles

9.2 Profile Level Arbitration

Here are some informative descriptions of the requirements defined in *6.2.1 Profile Arbitration for Concurrent Applications.*

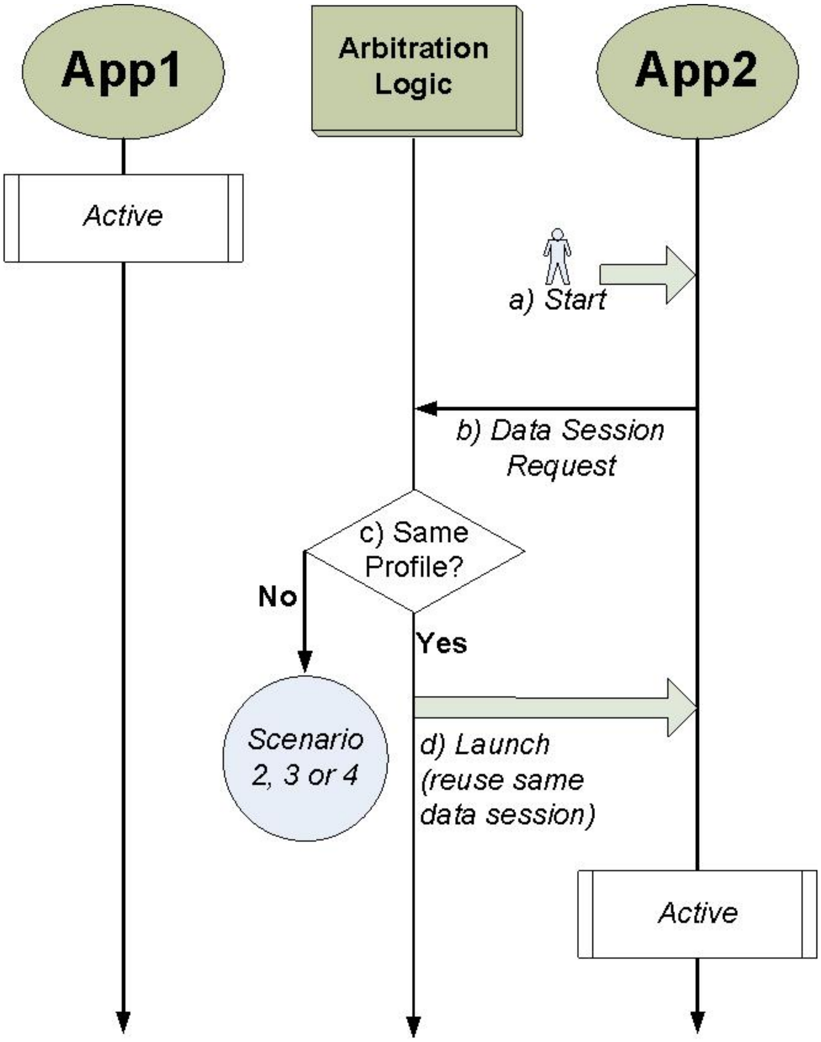
The device performs profile level arbitration based on the priorities and application types in the profiles stored on the CSIM. Each scenario below is further illustrated in the scenario diagrams in sections 9.2.1 to 9.2.4.

Table 9-2 Scenarios of Profile Level Arbitration

Scenario	**Newly Requested Session Profile ID**	**Newly Requested Session Profile Priority**	**Device Behavior**	**Scenario Section**
1	Same as existing session profile ID	Same as existing session profile priority	• Keep existing data session • Allow newly launched application to use the existing data session	9.2.1
2	Different…	Same..	*See 9.3 Device Specific Arbitration*	9.2.2
3	Different	Higher	• Abort the existing data session • Establish a new data session by using the new profile for the newly launched application	9.2.3
4	Different	Lower	• Keep the existing data session • Abort the new application	9.2.4

9.2.1 Scenario 1: Same Profile, Same Priority

In the following scenario diagram, App1 is MMS and App2 is WAP Browser, both using Profile 1. The newly launched App2 can reuse the existing data session.

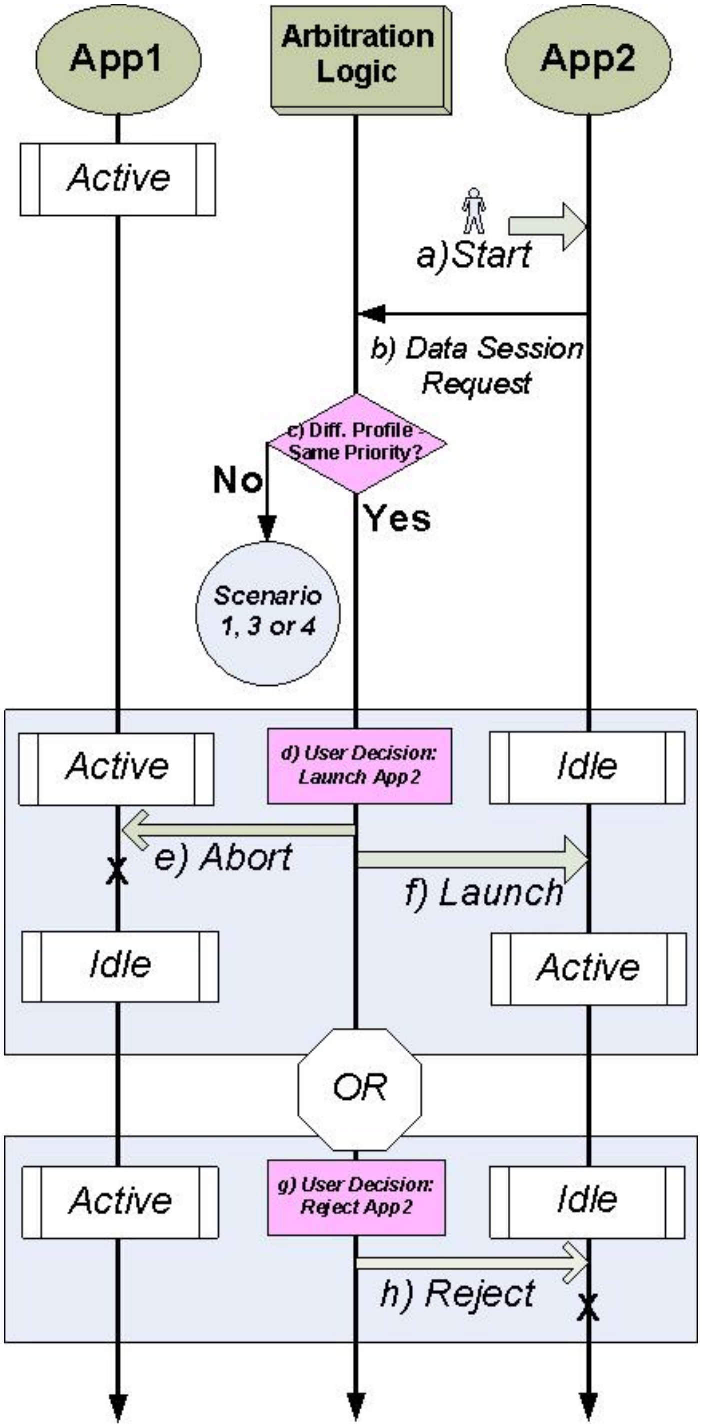


Scenario 1 steps:

a) While App1 is running with a data session active, App2 is launched.
b) App2 requests access to a data session.
c) The arbitration logic on the device checks whether the profile associated with App2 is the same as the one associated with App1.
d) The result of this checking is Yes, so the launch of App2 is completed which will reuse the existing data session.

9.2.2 Scenario 2: Different Profile, Same Priority

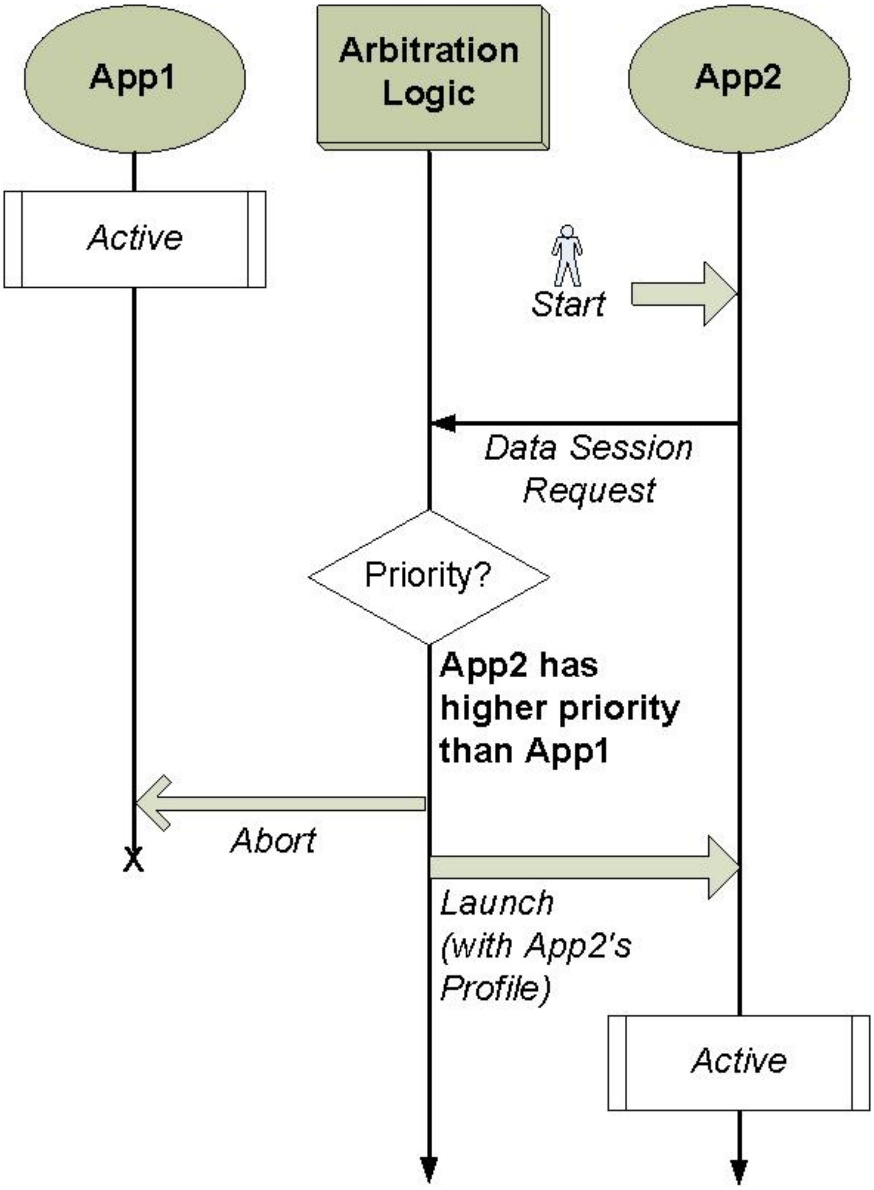
In the following scenario diagram, App1 is MMS using Profile 1, and App 2 is a 3rd-party app using Profile 2. Profile 1 and Profile 2 have the same priority.



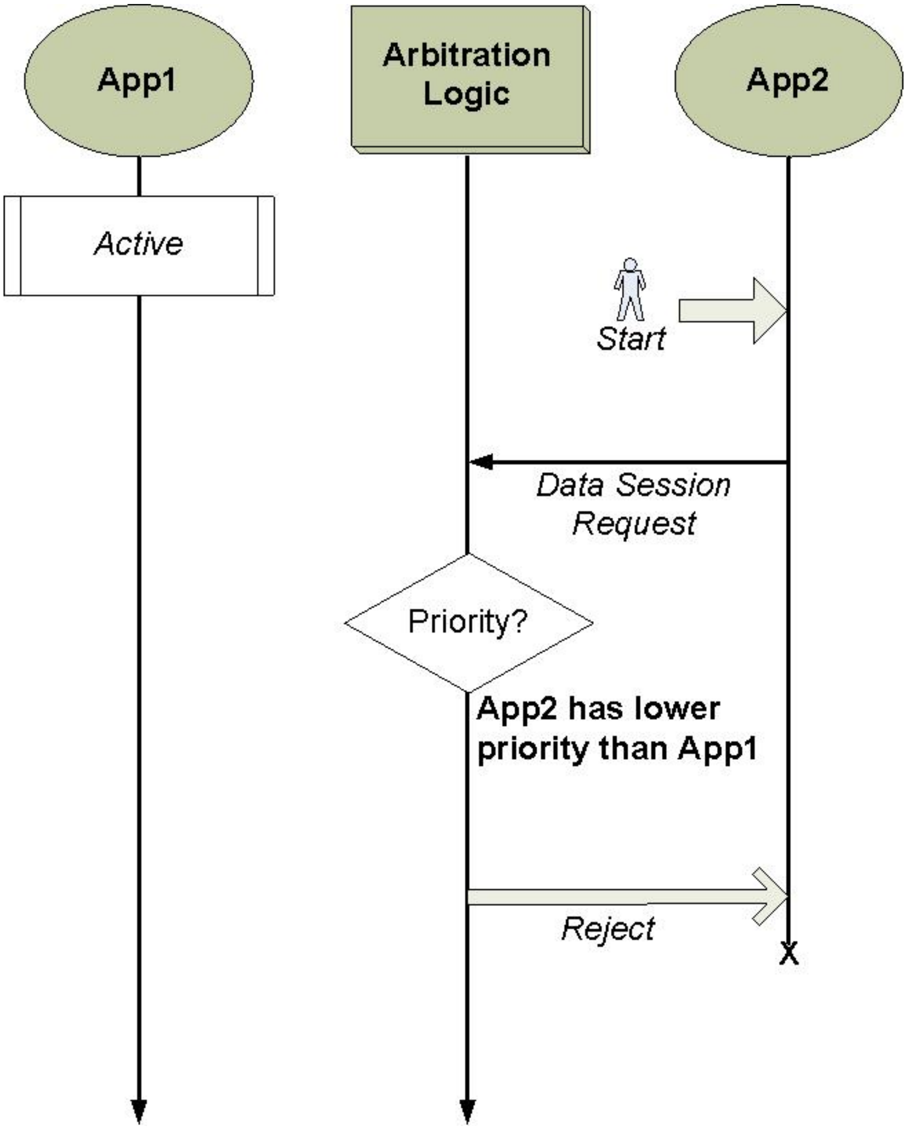
Scenario 2 steps:

a) While App1 is running with a data session active, App2 is launched.
b) App2 requests access to a data session.
c) The arbitration logic on the device checks whether the profile associated with App2 is different from the one associated with App1 and whether they have the same priority.
d) **The result of this checking is Yes, and the user decides to complete the launch of App2.**
e) The existing data session is aborted.
f) The launch of App2 is completed by establishing a new data session using the profile associated with App2.
g) Or, the result of this checking is Yes, but the user decides to reject the launch of App2.
h) The newly launched App2 is rejected. The existing data session for App1 continues.

9.2.3 Scenario 3: Different Profile, Higher Priority



9.2.4 Scenario 4: Different Profile, Lower Priority



9.3 Device Specific Arbitration

In the case where the newly launched application uses a profile that is different from the profile associated with the existing data session, but the priorities for both profiles are the same, the arbitration behavior is left up to the device manufacturer. For example, the device manufacturer may prompt the user to reject the new application request or accept the new application request (see table below). The device manufacturer may use some other means to make arbitration decisions without explicit user input.

Table 9-3 Scenarios of User Level Arbitration

Scenario	**User Decision**	**Device Behavior**
1	Reject the new application request	• Retain the existing data session • Abort the newly launched application
2	Accept the new application request	• Tear down the existing data session • Establish a new data session using the profile associated with the newly launched application • Complete the launching of the new application

10. Appendix: CSIM Provisioning and Profile

The following table summarizes how the device obtains application configurations from various configuration sources.

Table 10-1 Provisioning Scenarios

Scenario	Application Configuration present on CSIM?	Application Configuration present on device?	Application Configuration comes from…
1	Yes	No	CSIM
2	Yes	Yes	CSIM
3	No	Yes	Device
4	No	No	User Input

The following table provides the typical CSIM card profile with the list of EFs to be provisioned.

Table 10-2 Typical CSIM Card Profile

CSIM ADF
Device Operation
A-Key
SSD
COUNT
IMSI_M
IMSI_T
TMSI
CDMAHOME
ZNREGI
SNREGI
DISREGI

ACCOLC
TERM
SSCI
PRL
RUIMID
CST
SPC
OTASPSPC
NAMLOCK
OTA
SP
ESNME
LI
SPN
USGIND
AD
MDN
MAXPRL
SPCS
MECRP
ATC
EPRL
SF_EUIMID
EST
AppLabels
Model
RC
Voice
FDN
EXT2

SSFC
ECC
ICI
OCI
SMS
SMS
SMSP
SMSS
SMSCAP
3GPD
ME3GPDOPC
3GPDOPM
SIPCAP
MIPCAP
SIPUPP
MIPUPP
SIPSP
MIPSP
SIPPAPSS
SimpleIP CHAP SS
MobileIP SS
MIPFlags
SIPUPPExt
IPV6CAP
TCPConfig
DGC
HRPD
HRPDCAP
HRPDUPP
HRPD AA CHAP SS

MMS
MMSN
EXT8
MMSICP
MMSUP
MMSConfig
WAP Browser
WAPBrowserCP
WAPBrowserBM
Java
JDL
LBS
LBSXTRAConfig
LBSXSURL
LBSV2Config
LBSV2PDEADDR
LBSV2MPCADDR
BREW
BREWDownload
BREWSID
BREWAEP
MF
DIR
ICCID
PL
3G Phonebook
PBR
IAP
ADN
EXT1

PBC
GRP
AAS
GAS
ANR
SNE
EMAIL

11. Appendix: R-UIM Fallback Scenarios

The following table provides a high-level view of behavior for different combinations of R-UIMs and devices that support CSIM, C.S0023-D or pre-C.S0023-D.

Table 11-1 Device and R-UIM Compatibility Matrix

Scenario	User Inserts…	Into...	Device Behavior
1	Pre-C.S0023-D R-UIM	Pre-C.S0023-D R-UIM based Device	• Existing behavior, i.e., Voice and SMS based on provisioning in the RUIM and all other features (including 3GPD) based on provisioning in the device or user input.
2	C.S0023-D R-UIM	Pre-C.S0023-D R-UIM based Device	(Same as Scenario 1)
3	Pre-C.S0023-D R-UIM	CSIM-capable Device	(Same as Scenario 1)
4	C.S0023-D R-UIM	CSIM-capable Device	• Voice, SMS, 3GPD, and C.S0023-D enabled features based on provisioning in the R-UIM.

12. Terminology

Acronyms	***Meaning***
3GPD	3G Packet Data
ADF	Application Dedicated File
AMR NB	Adaptive Multi-Rate Narrow Band
BCD	Binary Coded Decimal
BIP	Bearer Independent Protocol
BOM	Byte Order Mark
BREW	Binary Runtime Environment for Wireless
BS	Base Station
CATPT	Card Application Toolkit Protocol Teleservice
CAVE	Cellular Authentication and Voice Encryption
CCAT	CDMA Card Application Toolkit
CDR	Call Detail Records
CHAP	Challenge Handshaking Authentication Protocol
CO	Cache Operation
cPRL	Concatenated PRL
CRC	Cyclical Redundancy Checking
CSIM	CDMA SIM
DELI	Delivery Context Library for CC/PP and UAProf
DNS	Domain Name Server
DRM	Digital Rights Management
DTMF	Dual Tone Multi Frequency
EF	Elementary File
EIR	Equipment Identity Register
EPRL	Extended PRL

Acronyms	***Meaning***
EPZID	Extended Packet Zone Identifier
ESN	Electronic Serial Number
ESN/MEID	Electronic Serial Number/Mobile Equipment Identifier
EUMID	Expanded UIM Identifier
FTAP	Forward Test Application Protocol
HAT	Hysteresis Activation Timer
HRPD	High-Rate Packet Data
ICC	Integrated Circuit Card
ICCID	Integrated Circuit Card Identifier
IMSI	International Mobile Subscription Identifier
IOT	Inter-Operability Test
IP	Internet Protocol
JVM	Java Virtual Machine
LBS	Location Based Services
MEID	Mobile Equipment Identifier
MF	Master File
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Center
MO	Mobile Originated
MPC	Mobile Positioning Center
MSC	Mobile Switching Center
MT	Mobile Terminated
NAI	Network Address Identifier
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OMH	Open Market Handsets
OTA	Over-the-Air
OTAPA	Over-the-Air Parameter Administration
OTASP	Over-the-Air Service Provisioning
PAP	Password Authentication Protocol

Acronyms	***Meaning***
PDE	Position Determination Entity
PDU	Protocol Data Unit
pESN	Pseudo Electronic Serial Number
pUMID	Pseudo UIM Identifier
PKI	Public Key Infrastructure
PLCM	Public Long Code Mask
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
QCIP	Quarter Common Intermediate Format (176 pixels x 144 pixels)
RTAP	Reverse Test Application Protocol
R-UIM	Removable User Identity Module
SI	Service Indication
SIR	Session Initiation Request
SMIL	Synchronized Multimedia Integration Language
SMS	Short Message Service
SMSC	Short Message Service Center
SMS-PP	Short Message Service Point to Point
TLS	Transport Layer Security
UAProf	User Agent Profile
UI	User Interface
UICC	Universal Integrated Circuit Card
UIMID	UIM Identifier
UTK	UIM Toolkit
VPM	Voice Privacy Mask
WAP	Wireless Application Protocol
WBMP	Wireless Bitmap
WML	Wireless Markup Language
WTA	Wireless Telephony Application
xHTML	eXtensible Hypertext Markup Language

<page left blank intentionally>

13. *References*

[CDG76] User Identity Module ToolKit (UTK), Enhanced Ver Vol. 2, October 2001

[CDG167] CDG Reference Document 167, *OMH Device Specification with R-UIM*.

www.cdg.org/omh

[CR1001] 3GPP2 C.R1001-E (TSB-58E), *Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards,* v1.0, September 30, 2005.

www.3gpp2.org/Public_html/specs/C.R1001-E_v1.0_051004.pdf

[CS0014] 3GPP2 C.S0014-C, *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems*, v1.0, January 2007.

www.3gpp2.org/Public_html/specs/C.S0014-C_v1.0_070116.pdf

[CS0015] 3GPP2 C.S0015-A (TIA-637B), *Short Message Service (SMS) for Wideband Spread Spectrum Systems*, v2.0, September 30, 2005.

www.3gpp2.org/Public_html/specs/C.S0015-A_v2.0_051006.pdf

[CS0016] 3GPP2 C.S0016-C (TIA-683C), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*, v1.0, October 22, 2004.

www.3gpp2.org/Public_html/specs/C.S0016-C_v1.0_041025.pdf

[CS0023] 3GPP2 C.S0023-D, *Removable User Identity Module for Spread Spectrum Systems*, v1.0, June 29, 2009.

http://www.3gpp2.org/Public_html/specs/C.S0023-D_v1.0_R-UIM-090720.pdf

[CS0035] 3GPP2 C.S0035-A, *CDMA Card Application Toolkit (CCAT),* v1.0, February 18, 2005.

www.3gpp2.org/Public_html/specs/C.S0035-A_v1.0_050224.pdf

[CS0072] 3GPP2 C.S0072-0, *Mobile Station Equipment Identifier (MEID) Support for cdma2000 Spread Spectrum Systems*, v1.0, July 22, 2005.

http://www.3gpp2.org/Public_html/specs/C.S0072-0_v1.0_050727.pdf

[CS0065] 3GPP2 C.S0065-B, *cdma2000 Application on UICC for Spread Spectrum Systems*, v2.0, January 2011.

[CS0074] 3GPP2 C.S0074-A, *UICC-Terminal interface - Physical and Logical Characteristics for cdma2000 Spread Spectrum Systems*, v1.0, January 2010.

[TS102.223] ETSI TS 102 223, *Smart Cards; Card Application Toolkit (CAT)*, V8.3.0, April 2009

[UNICODE] *Unicode standard*, version 5.2.0, October 2009.

http://www.unicode.org/versions/Unicode5.2.0/

[XS0016-0] 3GPP2 X.S0016, *MMS Specification Overview, Messaging System Specification*, Rev B, v1.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-000-B_v1.0_040616.pdf

[XS0016-2] 3GPP2 X.S0016-200-0 (TIA-934-200), *MMS Stage 2 Functional Description,* v2.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-200-0_v2.0_040707.pdf

[XS0016-3] 3GPP2 X.S0016-310-0 (TIA-934-310), *MMS MM1 Stage 3 Using OMA/WAP,* v2.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-310-0_v2.0_040617.pdf

<page left blank intentionally>