7.2.2 Data Services

7.2.2.1 CDMA2000® Packet Data

Some operators use a Network Access Identifier (NAI) of the format ESN@realm. Default provisioning of this value should be changed to a unique value, such as MEID@realm.

Origination and PLCM assignment is as for voice.

Either MEID or pESN (or both) is included in the airlink record sent from the PCF to the PDSN[35], and included in the PDSN UDR sent to the AAA. If MEID is sent, the receiving entity must be capable of accepting it (and if the pESN is absent the receiving entity must not consider it required).

7.2.2.2 1xEV-DO Packet Data

An AT can provide its Hardware ID in response to a HardwareIDRequest Message. When the AT is provisioned with an MEID, it will include this value as its Hardware-ID, with a specific HardwareIDType.

In order to include this identifier on the A12 interface, the AN must recode the HardwareIDType to the value specified in A.S0008-A. in other words, the AN cannot simply pass the information received from the AT transparently – it must explicitly understand the “MEID” HardwareIDType, and recode this to the “Type of Identity” coding for MEID, as specified in A.S0016-C (referenced from A.S0008-A Annex E) in order to build a properly formatted A12 message.

Only the MEID is available to be included into an airlink record and subsequently into the PDSN UDR (assuming derivation of the pESN is not performed). The PCF, PDSN and AAA must all be capable of receiving the MEID instead of an ESN field.

7.2.2.3 Other Applications

Any applications (e.g. Java, LBS, MediaPlayer for DRM etc) that today use ESN as a unique equipment identifier should be modified to use MEID instead. In the event that the application uses IMSI, or IMSI+ESN as a unique (subscriber and/or equipment) identifier, this scheme can be retained with the move to MEID.

---

[35] See A.S0017-C v2 sections 2.3 and 4.2.13, and X.S0011-005-D v1 section 3.2.1

7.2.3 Lost/Stolen Phone

A subscriber whose phone has been lost or stolen typically contacts Customer Service from an alternate number. Assuming the subscriber's identity is verified satisfactorily, the HLR subscription may be call-barred to prevent charges to the subscriber's account.

To prevent the stolen phone later being reprogrammed with a new number, the ESN is typically logged as stolen in the provisioning system. For an MEID-equipped device, the MEID should be logged instead (since using the pESN may incorrectly affect other, legitimate phones with the same pESN). This implies that the MEID of the device must be known to the network – possible mechanisms for this include:

- Recording the MEID at the point of sale
- Recording the MEID during an OTASP session (see Section 7.2.4)
- Capturing the MEID in billing records (see Section 7.2.1.5)
- Support of [X.S0008] and provisioning of the MEID in the HLR
- Support of X.S0008 and implementation of an Equipment Identity Register (see Section 7.3.3)

7.2.4 Over the Air Service Provisioning

Over-the-air Service Provisioning (OTASP) is a process by which a prospective subscriber buys a new, unprogrammed device, and has the necessary information (e.g. IMSI) downloaded to the device while making a call to the Customer Service Center (CSC).

At the start of the programming session, the MEID may be the only unique identifier available for the device.

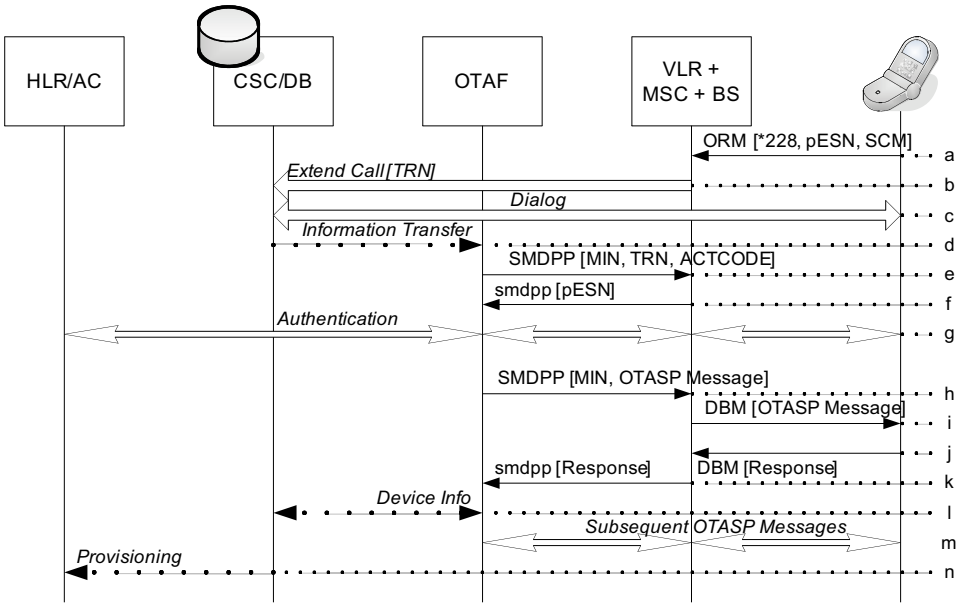

Figure 7-8 shows a simplified typical message flow for an OTASP call. For more detail see IS-725-A[36]. Note that the exact steps are to some extent implementation-dependent, and will depend on the way the operator has integrated the OTAF and the OTASP sales channel into their business processes.

[36] http://www.3gpp2.org/Public_html/specs/N.S0011-0_v1.0.pdf

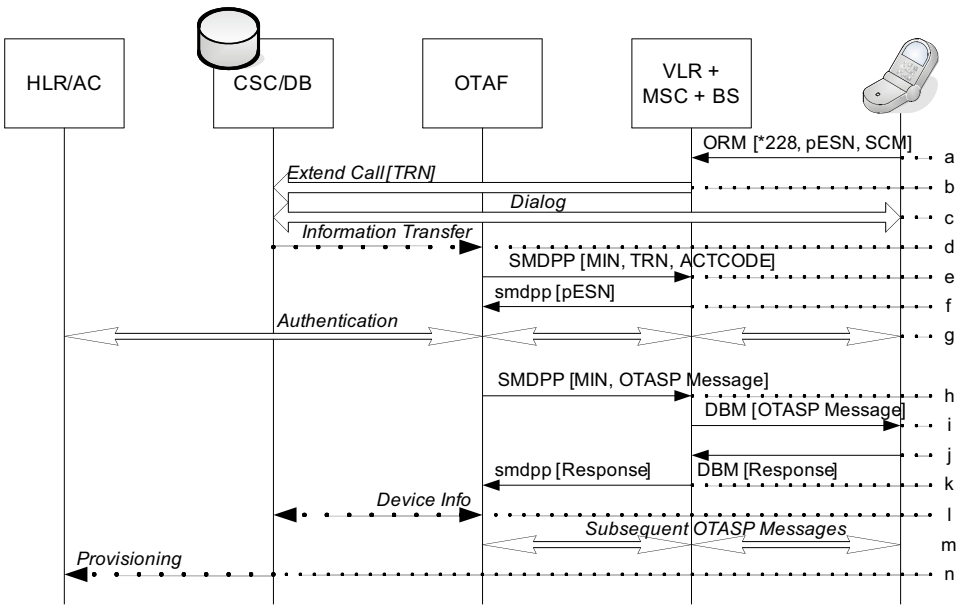

Figure 7-8 - OTASP Data Flow

Steps are as follows:

a) The MS originates a call to the OTASP feature code (typically *228), including its pESN and SCM as with other originations

b) Recognizing the OTASP code, the MSC assigns a Temporary Reference Number (TRN) from a pool and sets this as the Calling Party Number (CgPN). It extends the call to the CSC.

c) The CSC (shown here co-located with a provisioning database for simplicity) answers the call. The prospective subscriber may enter into a dialog with a Customer Service Representative, or an automated system. Subscribers provide sufficient information (e.g. credit card number, or code allocated at point of sale) to allow the operator to authorize them for service.

d) The CSC provides the TRN to the OTAF.

e) The OTAF sends a SMDPP to the MSC. The message includes the TRN (to identify the call in progress), and a temporary Activation_MIN assigned by the OTAF.
Note: At this point, the OTAF has no knowledge of the device MEID, or even the pESN. If two handsets with the same pESN made simultaneous OTASP calls, the OTAF would still be able to distinguish them based on the TRNs assigned by the MSC, and assign unique Activation_MINs.

f) The MSC returns the pESN of the device. Optionally, if the network requested the device MEID via an earlier STRQM, the MEID could be included here as per X.S0008/X.S0033. Note however that the MEID can be transferred to the OTAF without the need for X.S0008 or X.S0033 (see below). Another SMDPP at this point (not shown) releases the TRN back

into the MSC's pool. From this point the Activation_MIN is used to identify the call.

g) Optionally, the OTAF may, in conjunction with the HLR/AC, instruct the MS to generate a new A-key. The same A-key value is securely generated in both the AC and MS so that it does not need to be transferred over the air.

h) The OTAF sends an SMDPP containing an OTASP *Protocol Capability Request Message*. Based on the presence of a pESN (identifiable by its manufacturer code), the OTAF includes in the message a request for the MEID.

i) The MSC passes the message on to the MS encapsulated in a DBM.

j) The MS returns its MEID (together with other capabilities requested)

k) The MSC returns the MEID to the OTAF. The MEID is embedded in the SMS_BearerData of the smdpp and does not explicitly require ANSI-41 / IS-725 modifications.

l) The OTAF may query a database for information about the device, for example the Service Programming Code (SPC). The contents of the database are typically provided by the handset manufacturer, and are indexed by ESN/MEID (but should not be indexed by pESN).

m) Multiple SMDPP/DBM messages may be used to program the desired IMSI, download Preferred Roaming List information, and other tasks. At the conclusion of the OTASP session, the Activation_MIN is released for re-use.

n) The CSC (via the provisioning system) creates an entry in the HLR to match the information in the device just programmed. The entry associates a MIN/IMSI with the pESN and/or MEID. If the A-key has not been generated during the OTASP session, a pre-programmed value may be retrieved from the device information database. Again, a unique device identifier is required here to ensure the correct record is retrieved.

IS-725-A (3GPP2 N.S0011-0) defines the temporary call record that may exist during an OTASP session at any/all of the MSC, VLR, HLR or AC, and names it the OTASPCallEntry. The standard provides several methods to identify this record, including the Activation MIN and the ESN (extended by X.S0033 to include MEID). The identifier needs to be unique, so ESN is not recommended as a method. Use of MEID requires X.S0008/X.S0033 support in the network.

7.2.5 Roaming

The following scenarios describe cases when a device is not in its home network. Due to varying levels of operator readiness, network support for MEID-equipped mobiles may be different in the visited network to that experienced at home, and expected by other elements in the home network. More information is available in [CDG Ref Doc 137].

7.2.5.1 Outbound Roaming

The following scenarios may occur when an operator's MEID-equipped devices roam into another network:

- **No support for MEID devices**. Some networks have been identified which cannot serve MEID-equipped mobiles at all. Until these networks are upgraded, subscribers with MEID devices may not be able to roam in these markets. See the [MEID Failure Bulletin] for more detail.
- **No C.S0072 support in visited network**. If the visited network does not support C.S0072, the roamer may be at risk of PLCM collisions. Collisions could occur with other roamers, or with the visited network's own subscribers (e.g. if the serving operator had chosen to deploy only unique pESNs for its own subscribers – see Section 6.). Furthermore, the MEID will not be available on any interface.
- **No X.S0008 support in visited network**. Even if C.S0072 is implemented, the visited network may not support the transfer of the MEID in ANSI-41 messages. Alternatively, the home network may not support X.S0008, but the serving network does, and MEID is received unexpectedly in internetwork messages. This should have no consequences as long as unrecognized parameters in ANSI-41 are properly ignored, and as long as MEID-capable networks properly treat MEID as an optional parameter.
- **MEID presence in CIBER.** The CIBER record contains only one field for MEID or pESN. Different roaming partners may populate this field differently. It is recommended that MEID be accepted but that the field is populated with pESN if MIN/ESN validation is performed or it is verified that all roaming partners will accept MEID.
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pESN) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.
- **MEID in 1X Packet Data UDR.** The MEID may be included in the UDR instead of the ESN, or vice versa, which may differ from the home operator's own network practice.

7.2.5.2 Inbound Roaming

An operator serving roamers from other networks has no control over the deployment timeframe and options implemented by the home operator – the roamers could be using R-UIMs equipped with UIMIDs or EUIMIDs even if the serving operator's own subscribers only use non-R-UIM devices. The relevant issues are addressed in the Outbound Roaming sections of the various operator configurations.

Assuming the serving operator has already deployed MEID-equipped devices and C.S0072 support, inbound roamers with pESN/pUIMID should not cause issues for the serving operator. Communication and negotiation with roaming partners may be useful to address the implementation differences described in Section 7.2.5.1 .

7.3 R-UIM Operator – existing R-UIM in MEID device

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. Here, an existing R-UIM with a unique UIMID has been inserted into a new, MEID-equipped device.

7.3.1 Basic Operation

7.3.1.1 Registration – No X.S0008 support

Without support for X.S0008, this scenario is indistinguishable at the HLR from the existing case (i.e. unique UIMID in unique ESN device). The steps are shown in Figure 7-9:

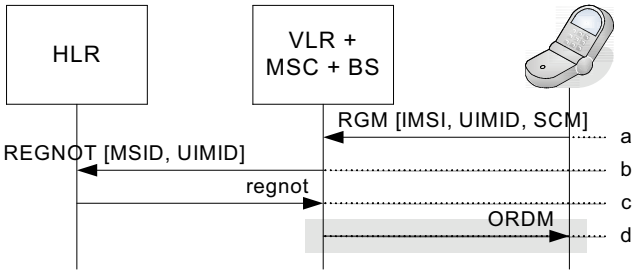

Figure 7-9 - UIMID Registration - no X.S0008 support

Steps are as follows:

a) MS sends a *Registration Message*, including its IMSI, UIMID, and Station Class Mark set to indicate MEID support. The MS cannot include its MEID in this message.

b) Although the MSC is aware that the MS has a MEID, it takes no specific action. It proceeds with the RegistrationNotification INVOKE message, including the UIMID and the Mobile Station Identity (MSID – either MIN or IMSI)

c) The HLR validates the subscription on the basis of MSID-UIMID. This is the same information the HLR receives if the subscriber had inserted their R-UIM in an ESN-equipped device. The HLR returns the subscriber profile to the MSC

d) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.3.1.2 Registration – X.S0008 supported

When the serving network does support X.S0008, the MEID can be included in the REGNOT. The ability to receive information relating both to the card and the device is new: the device ESN is not available to the HLR today. The steps are shown in Figure 7-10:

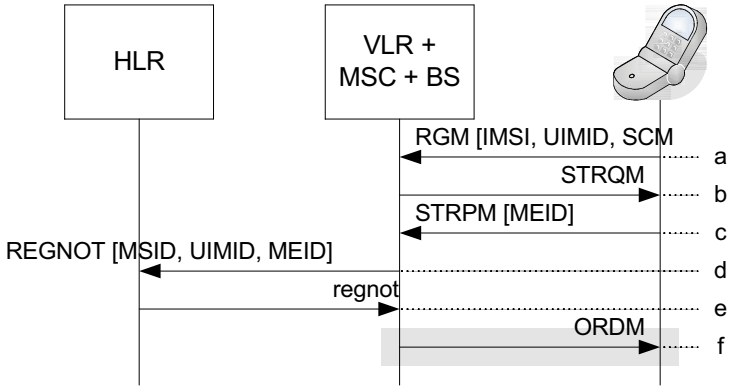

Figure 7-10 - UIMID Registration - X.S0008 supported

Steps are as follows:

a) MS sends a *Registration Message*, including its IMSI, UIMID and Station Class Mark set to indicate MEID support. The MS cannot include its MEID in this message.

b) Based on the SCM, the MSC recognizes that the mobile has a MEID, and that the MSC does not know this value. It solicits the MEID via the *Status Request Message*

c) The MS returns its MEID in the *Status Response Message*

d) The MSC sends a RegistrationNotification to the HLR, including the MSID, UIMID, and the MEID. The UIMID is not hash-related to the MEID, so no checking should be performed by the MSC to ensure this.

e) The HLR will presumably not track the MEID value, as the subscriber may transfer the R-UIM to another ME at any time (although it may be recorded to assist in a future lost/stolen report – see Section 7.2.3). In any case, the HLR should not perform a hash-relation check between the two values. Even if the HLR supports X.S0008, it will not include the MEIDValidated parameter in the regnot.

f) Optionally, the BS sends a *Registration Accepted Order* to the MS. Since the MEIDValidated parameter was not present in the regnot, the MEID retrieved from the mobile in step c is not used by the MSC in validating subsequent system accesses.

7.3.1.3 Authentication

Authentication is unchanged from existing operation. The UIMID is used as an input to various CAVE computations. The MEID may be included in various network operations if X.S0008 is supported, but it is not used as an authentication input.

7.3.1.4 Call Origination/Termination

Although the traditional (in this case UIMID-based) PLCM would not be susceptible to collisions, the network is expected to use a BS-assigned PLCM instead, due to the SCM bit 4 being set to 1.

Note: The MSC could in theory examine the first 8 bits of the received ESN to determine whether this was a unique (ESN/UIMID) or non-unique (pESN/pUIMID) value. However the ESN is not a mandatory field in the MSID (as defined in C.S0004), so C.S0072 implies that the decision is made solely on the basis of the SCM. An equipment vendor may choose to require *both* SCM bit 4 = 1 and an "ESN" beginning with 0x80 before assigning a non-UIMID-based PLCM. Similarly, some MEID-equipped handsets have been observed to set the SCM bit 4 to 0 when a unique UIMID-equipped R-UIM is inserted. This behavior is not explicitly covered in existing standards – the "default" behavior expected is that the SCM bit 4 will be set to 1 if the ME has an MEID, irrespective of the type of R-UIM inserted. This custom handset/network behavior will deactive EIR capabilities for the mobile but will not result in any collision problems as the PLCM derived from the UIMID will be unique.

7.3.1.5 Call Detail Record Production

Similar to the registration case in Section 7.3.1.2 , both the MEID and UIMID may be available in the MSC CDR, a change from current operation where only the UIMID is available and not the handset ESN. Billing system changes would presumably be needed if the operator wished to take advantage of this new information (e.g. for statistical information on handset usage). This does not apply to some billing record formats such as the CIBER inter-carrier format, in which only one hardware identifier can be included. In this case it may be desirable to include the pUIMID instead of the MEID to allow validation of a matched pair of identifiers (the MEID will change if the R-UIM is moved but the pUIMID comes from the card along with the IMSI).

7.3.1.6 Mobile Terminated SMS

MT-SMS and other paging-channel messages are not susceptible to the mis-addressing problem described in Section 7.2.1.6 for this scenario, as message addressed by 'ESN' will actually contain the unique UIMID.

7.3.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM (assuming the SCM bit 4 is set to 1).

7.3.2 Data Services

7.3.2.1 CDMA2000® Packet Data

Operator provisioning using an NAI constructed as UIMID@realm is unaffected by insertion into an MEID-equipped ME.

Origination and PLCM assignment is as for voice.

In 1X mode the UIMID or MEID or both may be included in the airlink record and the subsequent PDSN UDR. For EVDO, the MEID may be included but the UIMID will not be included unless it is calculated from the MEID.

7.3.2.2 1xEV-DO Packet Data

Devices obtain the HardwareID from the device (MEID in this scenario), not the R-UIM[37]. In this scenario the network must be upgraded to handle the new MEID HardwareIDType, as described in Section 7.2.2.2 .

7.3.2.3 Other Applications

Applications would typically be expected to honor the R-UIM usage indicator bit, and therefore use the UIMID as the “ESN” value. In this case no change from existing behavior would be required for this scenario.

If the application used the device ESN, then use of the MEID instead as per Section 7.2.2.3 is recommended, although note that “subscription mobility” (moving the R-UIM to a different ME) may be compromised in this case regardless of MEID issues.

7.3.3 Lost/Stolen Phone

A subscriber whose phone has been lost or stolen typically contacts Customer Service from an alternate number. Assuming the subscriber’s identity is verified satisfactorily, the HLR subscription may be call-barred to prevent charges to the subscriber’s account.

R-UIM devices present a particular challenge for the stolen phone case, as the thief can replace the legitimate subscriber’s R-UIM with their own (e.g. if the device had more functionality than the thief’s). Prior to the introduction of MEID, there was no way for the network to track the device independently of the R-UIM (assuming the usage indicator was set to replace the ESN with the EUIMID).

---

[37] The 3GPP2 specification for EV-DO was not clear on this point. To rectify this 3GPP2 contribution C23-20080512-004R1 was introduced and accepted in May, 2008. It makes it absolutely clear that the intent of the EV-DO specification is that Hardware ID comes from the phone (ESN or MEID) not from the R-UIM.

X.S0008 and C.S0072 address this issue by allowing the device MEID to be retrieved, and checked against a record held in a new network element, the Equipment Identity Register (EIR). The new CheckMEID operation is defined for this purpose, as shown in Figure 7-11. Note that in order for the MEID to be listed as stolen in the EIR, the network must have previous knowledge of which MEID was in use for the stolen IMSI (see Section 7.2.3):

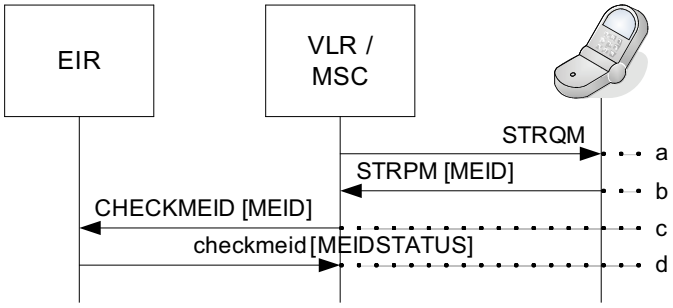

Figure 7-11 - CheckMEID Operation

Steps are as follows:

a-b) The VLR/MSC does not have the current MEID, and so retrieves it via *Status Request/Response Message*.

c) The VLR sends the CheckMEID message to the EIR containing the MEID.

d) The EIR returns the MEID Status (e.g. Normal, Block, Track).

Ultimately, the success of EIR deployment to identify stolen phones depends on the extent to which EIRs of different operators are interconnected – from GSM experience, the “SIM/R-UIM lock” which restricts a device to a particular operator can often be defeated by the thief. At the time of writing, no CDMA operators were known to have deployed or be actively pursuing deployment of an EIR.

7.3.4 Over the Air Service Provisioning

OTASP provisioning for the “UIMID in MEID” scenario is the same as the existing “UIMID in ESN” flow (assuming the MSC does not autonomously include the MEID in the initial smdpp to the OTAF). The unique UIMID would not trigger the OTAF to request the MEID from the handset. The unique UIMID can be used to index a database to retrieve card-specific information (e.g. A-key, SPC).

7.3.5 Roaming

7.3.5.1 Outbound Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. The “UIMID in MEID” configuration is susceptible to this issue.
- **No C.S0072 support in visited network**. Since the UIMID is unique, there is no risk of PLCM collision even if C.S0072 is not supported.
- **No X.S0008 support in visited network**. X.S0008 support is of limited use in this scenario, as the subscriber may move their R-UIM between MEs without advising the operator. X.S0008 support would be beneficial to address stolen phone scenarios while roaming.
- **MEID presence in CIBER.** The two identifiers (UIMID and MEID) potentially available for inclusion in the CIBER record are not hash-related. Use of the UIMID is recommended in this case (see Section 6.)
- **No MEID in A12 authentication**. Some operators may not send HardwareID in A12 at all. Others may support ESN as HardwareID, but not MEID.
- **MEID in UDR.** In 1x mode the MEID may be included in the UDR instead of the UIMID, or vice versa, which may differ from the home operator’s own network practice. In EVDO mode the MEID may be included but the UIMID cannot be included unless it is calculated from the MEID.

7.3.5.2 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network’s ability to serve roamers from other markets. Operators who themselves use R-UIMs may be more cognizant of the potential CIBER ramifications of including the MEID rather than the UIMID.

7.4 R-UIM Operator – Short-Form EUIMID

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. The operator has chosen to deploy Short-Form EUIMID. Following the argument in Section 5.2 , the assumption here is that Bit 2 of the Usage Indicator is set to 1, i.e. the SF_EUIMID overrides the device MEID if present. The EUIMID-equipped R-UIMs may be inserted into devices that are equipped with either an ESN, or an MEID. MEID equipped devices are assumed to be C.S0023-C/C.S0065 capable (see Section 5.2), unless otherwise noted.

Note that in the case where an ESN-equipped handset includes the necessary software to support MEID, it might be thought that the handset would use the SF_EUIMID and report MEID availability. However C.S0023-C specifically prohibits an ESN-equipped ME from interpreting the SF_EUIMID Usage Indicator bit. Such a device will operate as a pure ESN device and SF_EUIMID will not be used.

In general, insertion of a SF_EUIMID card into an ESN-equipped device is shown to create potential for PLCM collisions, regardless of the network support for C.S0072.

7.4.1 Basic Operation

7.4.1.1 Registration – No X.S0008 support

This scenario is equivalent to that shown in Section 7.2.1.1 , except that pUIMID is sent in the ESN parameter instead of pESN. HLR validation is performed on the basis of the MIN/IMSI – pUIMID combination.

7.4.1.2 Registration – X.S0008 supported

In this scenario, the SF_EUIMID can be included in the registration message, as shown in Figure 7-12. This is only possible if the handset has an MEID (even though the MEID itself is not sent to the network), since only an MEID-equipped device will understand the *Status Request* for the MEID, and advertise this fact via the SCM.

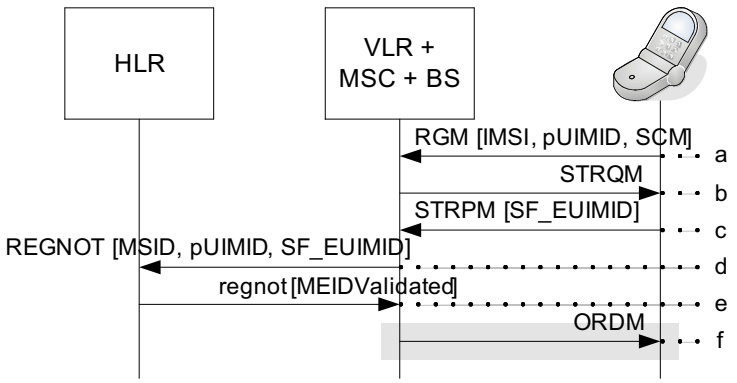

Figure 7-12 - SF_EUIMID Registration with X.S0008 support

Steps are as follows (for MEID-equipped ME):

a) MS sends a *Registration Message*, including its IMSI, pUIMID and Station Class Mark set to indicate MEID support. The MS cannot include its MEID or the SF_EUIMID in this message.

b) Based on the SCM, the MSC recognizes that the mobile has a MEID, and that the MSC does not know this value. It solicits the MEID via the *Status Request Message* (new Information Record in C.S0072).

c) The MS responds with a *Status Response Message*. Based on the value of the Usage Indicator, the SF_EUIMID is returned instead of the MEID.

d) The MSC sends a RegistrationNotification to the HLR, including the MSID, pUIMID (required for backwards compatibility) and the SF_EUIMID.

e) Text extracted from X.S0008: “Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the REGNOT, the HLR includes an MEID comparison in the validation of the subscription. The HLR then registers the indicated MS and returns a regnot to the Serving VLR. The regnot includes the MEIDValidated parameter to inform the Serving VLR/MSC that the MEID associated with the system access has been validated.” In this case, the value included in the MEID parameter will be the SF_EUIMID. Even if the subscriber transfers the R-UIM to another (MEID-equipped) device, this value will remain constant, and can therefore be reasonably expected to be stored in the HLR.

f) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.4.1.3 Authentication

Authentication is performed on the basis of the pUIMID. The SF_EUIMID, if included, will not be used for authentication calculations.

A-key checksum calculations should use the pUIMID as an input for verification.

7.4.1.4 Call Origination/Termination

If the SF_EUIMID-equipped R-UIM is inserted in an MEID-equipped ME, PLCM assignment will be as per Section 7.2.1.4 (i.e. network recognizes SCM and provides BS-assigned PLCM). pUIMID and SF_EUIMID replace pESN and MEID respectively from the earlier scenario.

If however the card is inserted in an ESN-equipped ME, this device will not understand the new PLCM types or set the SCM bit flag. The pUIMID-based PLCM will be used, and there is a risk of PLCM collision.

7.4.1.5 Call Detail Record Production

The two identifiers available (pUIMID and SF_EUIMID) for inclusion in the CDR are hash-related, but since both are associated with the R-UIM, there is no opportunity to capture information about specific hardware usage.

It is recommended that operators include the pUIMID since it is more compatible with existing billing systems until it can be verified that all roaming partners will accept a 56-bit identifier for billing. Note that an operator serving a roamer cannot determine whether the 56-bit identifier is SF_EUMID (and therefore associated with the subscription) or an MEID (and therefore not associated with the subscription, but with the phone hardware).

Note that some billing record formats, notably CIBER, do not support the inclusion of two hardware identifiers.

7.4.1.6 Mobile Terminated SMS

ESN-addressed messages over the paging channel would in this configuration use the pUIMID derived from the SF_EUIMID. Regardless of whether the card was inserted in an ESN- or MEID-equipped device, messages could be received by other mobiles in addition to the intended recipient due to pUIMID duplication.

7.4.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM. If the R-UIM is inserted in an ESN-equipped device, BS-assigned PLCM is not possible, regardless of the status of C.S0072 support in the network.

7.4.1.8 Handset Compatibility Issues

If the R-UIM is inserted in a device affected by the issue described in Section 5.4 , the device may indicate “Service Required”, or otherwise refuse to operate.

If the R-UIM is inserted into an MEID-equipped device without C.S0023-C support, it will return the handset shell (ME) MEID rather than the desired SF_EUIMID.

7.4.2 Data Services

7.4.2.1 CDMA2000® Packet Data

Data originations when an ESN-equipped device is used are subject to the same potential for PLCM collision as for voice.

NAI assignment using UIMID@realm will no longer be unique – an upgrade to another value that is unique, such as SF_EUIMID@realm is necessary.

For 1x packet data SF_EUIMID or pUIMID or both may be included in the airlink record and subsequent PDSN UDR.

7.4.2.2 1xEV-DO Packet Data

HardwareID handling (if implemented) should be upgraded to accept the MEID format as described in Section 7.2.2.2 . This parameter will be the MEID or ESN not the UIMID or EUIMID.

If an MEID-equipped handset is used, then the handset MEID will be present in the airlink record and subsequent PDSN UDR (unless the associated pESN is calculated from the MEID by the PCF/PDSN).

7.4.2.3 Other Applications

Applications should use the EUIMID in preference to the pUIMID as a unique identifier. The exact access method for the application to obtain the EUIMID is beyond the scope of this document.

7.4.3 Lost/Stolen Phone

Overriding the ME's MEID with the SF_EUIMID means that a stolen device cannot be tracked/blocked independently of its R-UIM. A thief would be able to replace the legitimate subscriber's R-UIM with their own without the network being aware of the change.

This limitation is essentially equivalent to the situation today with UIMID cards in ESN devices.

7.4.4 Over the Air Service Provisioning

OTASP (when the SF_EUIMID R-UIM is inserted into an MEID ME) is essentially equivalent to the non-R-UIM MEID device scenario shown in Section 7.2.4 , with pUIMID and SF_EUIMID replacing pESN and MEID respectively.

When the card is inserted into an ESN device, it may not be possible to retrieve the SF_EUIMID[38]. In fact, the OTASP session may fail, as the ESN-equipped handset may not handle the additional fields in the *Protocol Capability Request Message*[39]. A solution is to store the SF_EUIMID or a unique provisioning identifier in fields that are accessible to ESN mobiles but not filled with data until the time of provisioning, fields such as MDN and IMSI_T.

The new capabilities introduced in C.S0066 v2.0 and the forthcoming C.S0016-C v2.0 allow the retrieval of both the SF_EUIMID and the handset MEID during the OTASP session.

[38] C.S0023-C Section 4.3.2.1 implies the ME is required to process the additional fields in the *Protocol Capability Request Message* (including the request for MEID) not the R-UIM.

[39] C.S0066 (Section 4.3.1) states “The base station shall not send the *Protocol Capability Request Message* with additional fields to the mobile stations which don’t support the additional fields”, yet the presence of the pUIMID means that OTAF may assume the mobile does support these fields.

7.4.5 Roaming

7.4.5.1 Outbound Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. When inserted in a MEID-equipped device, the SF_EUIMID R-UIM is susceptible to this issue.
- **No C.S0072 support in visited network**. In this case the pUIMID will be used to form the PLCM, with the associated risk of collision.
- **No X.S0008 support in visited network**. As per Section 7.2.5.1 , the SF_EUIMID may not be available in ANSI-41 messaging.
- **SF_EUIMID presence in CIBER.** The two identifiers (pUIMID and SF_EUIMID) potentially available for inclusion in the CIBER record are hash-related. There may be a preference for the unique identifier (i.e. SF_EUIMID), although it is likely that roaming partner behavior will vary.
- **No MEID in A12 authentication**. Some operators may not send HardwareID in A12 at all. Others may support ESN as HardwareID, but not MEID.
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pUIMID) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.
- **MEID in UDR.** The SF_EUIMID may be included in a 1X UDR instead of the pUIMID, or vice versa, which may differ from the home operator's own network practice. For EVDO modes, the serving network may not be able to include the MEID or pUIMID in the UDR.

7.4.5.2 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network's ability to serve roamers from other markets.

7.5 R-UIM Operator – Long-Form EUIMID

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. The operator has chosen to deploy Long-Form EUIMID. The full LF_EUIMID can only be retrieved remotely from the MS via C.S0066-0 v2.0 messaging or through the use of a special CCAT/UTK application (see Section 5.3). The EUIMID-equipped R-UIMs may be inserted into devices that are equipped with either an ESN or an MEID

In general, insertion of a LF_EUIMID card into an ESN-equipped device is shown to create potential for PLCM collisions, regardless of the network support for C.S0072.

7.5.1 Basic Operation

7.5.1.1 Registration – No X.S0008 support

This scenario is equivalent to that shown in Section 7.2.1.1 , except that pUIMID is sent in the ESN parameter instead of pESN. HLR validation is performed on the basis of the MIN/IMSI – pUIMID combination.

7.5.1.2 Registration – X.S0008 supported

When X.S0008 is supported, the registration scenario is equivalent to that shown in Section 7.3.1.2 , except that pUIMID replaces the UIMID. No checking for a hash relationship between the received 32- and 56-bit identifiers should be performed.

7.5.1.3 Authentication

Authentication is performed on the basis of the pUIMID.

A-key checksum calculations should use the pUIMID as an input for verification, although other implementations may be possible – the standards in this area predate the introduction of MEID/EUIMID.

7.5.1.4 Call Origination/Termination

If the LF_EUIMID-equipped R-UIM is inserted in an MEID-equipped ME, PLCM assignment will be as per Section 7.2.1.4 (i.e. network recognizes SCM and provides BS-assigned PLCM). pUIMID replaces pESN from the earlier scenario, but the ME MEID may still be retrieved via the *Status Request/Response Messages*.

If however the card is inserted in an ESN-equipped ME, this device will not understand the new PLCM types or set the SCM bit flag. The pUIMID-based PLCM will be used, and there is a risk of PLCM collision.

7.5.1.5 Call Detail Record Production

Similar to the registration case in Section 7.5.1.2 , both the MEID and pUIMID may be available in the MSC CDR, a change from current operation where only the UIMID is available and not the handset ESN. Billing system changes would presumably be needed if the operator wished to take advantage of this new information (e.g. for statistical information on handset usage). The unique LF_EUIMID is not available. The inclusion of two hardware identifiers may not be supported by all CDR formats, and is not supported by the CIBER billing record format. In this case it may be desirable to include the pUIMID instead of the MEID to allow validation of a matched pair of identifiers (the MEID will change if the R-UIM is moved but the pUIMID comes from the card along with the IMSI).

7.5.1.6 Mobile Terminated SMS

ESN-addressed messages over the paging channel would in this configuration use the pUIMID derived from the LF_EUIMID. Regardless of whether the card was inserted in an ESN- or MEID-equipped device, messages could be received by mobiles in addition to the intended recipient due to pUIMID duplication. IMSI-addressed messages significantly reduce this problem.

7.5.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM. If the R-UIM is inserted in an ESN-equipped device, BS-assigned PLCM is not possible, regardless of the status of C.S0072 support in the network.

7.5.1.8 Handset Compatibility Issues

If the R-UIM is inserted in a device affected by the issue described in Section 5.4 , the device may indicate “Service Required”, or otherwise refuse to operate.

7.5.2 Data Services

7.5.2.1 CDMA2000® Packet Data

Data originations when an ESN-equipped device is used are subject to the same potential for PLCM collision as for voice.

NAI assignment using UIMID@realm will no longer be unique – an upgrade to a unique value such as LF_EUIMID@realm is necessary.

Either MEID or pUIMID or both may be included in the airlink record and subsequent PDSN UDR.

7.5.2.2 1xEV-DO Packet Data

HardwareID handling (if implemented) should be upgraded to accept the MEID format as described in Section 7.2.2.2 . Devices should source the HardwareID from the device (ESN or MEID), not the R-UIM.

If an MEID-equipped handset is used, then the handset MEID will be present in the airlink record and subsequent PDSN UDR (unless the associated pESN is calculated from the MEID by the PCF/PDSN).

7.5.2.3 Other Applications

Applications should use the EUIMID in preference to the pUIMID as a unique identifier. The exact access method for the application to obtain the EUIMID is beyond the scope of this document.

7.5.3 Lost/Stolen Phone

The stolen phone scenario for LF_EUIMID is equivalent to the “UIMID in MEID” case shown in Section 7.3.3 , provided the lost phone is MEID-equipped. If the MEID has been previously recorded, it could be marked as stolen in the EIR, and blocked from further usage within the scope of connectivity to that EIR.

If the device is ESN-equipped, its ESN is not transmitted to the network, and therefore the device cannot be barred from operating using a different R-UIM.

7.5.4 Over the Air Service Provisioning

OTASP using LF_EUIMID can present some challenges, as the LF_EUIMID can often not be retrieved from the card (only the new capabilities recently added in C.S0066 v2.0 and C.S0016-C v2.0 provide standard methods for this). If there is any card-specific information stored in a database (e.g. A-key and/or SPC) but no IMSI on the R-UIM it is difficult to retrieve data for provisioning accurately. In addition, subsidy protection may present a challenge as it may not be possible to determine that a particular card was sold by a particular operator.

An alternative to retrieving pre-programmed card-specific information is to generate it during the OTASP session (after which it can be associated with the programmed IMSI). IS-725-A and IS-683 contain procedures for securely creating the A-key in the AC and MS during the OTASP session. Similarly, the SPC could be initially set to a default value, and then changed to a random value using existing OTASP procedures. A PIN issued at the point of sale (as well as the default Preferred Roaming List in the card) can help ensure that the prospective subscriber ultimately obtains service from the correct operator.

Another approach is to provision the LF_EUIMID in fields that are accessible to all mobiles supporting R-UIM, and not required to be filled with valid information prior to provisioning, such as the MDN and IMSI_T fields.

7.5.5 Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. When inserted in a MEID-equipped device, the LF_EUIMID R-UIM is susceptible to this issue.
- **No C.S0072 support in visited network**. In this case the pUIMID will be used to form the PLCM, with the associated risk of collision.
- **No X.S0008 support in visited network**. X.S0008 support is of limited use in this scenario, as the subscriber may move their R-UIM between MEs without advising the operator. X.S0008 support would be beneficial to address stolen phone scenarios while roaming.
- **MEID presence in CIBER.** The two identifiers (pUIMID and MEID) potentially available for inclusion in the CIBER record are not hash-related. Use of the pUIMID is recommended in this case (see Section 6.).
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pESN) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.

7.5.5.1 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network's ability to serve roamers from other markets.

8. Terminology

0x	Hexadecimal (base 16) format indicator
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AC	Authentication Center
A-key	Authentication Key
AMPS	Advanced Mobile Phone Service
AN	Access Network
ANSI-41	American National Standards Institute 41 – mobile standard (also known as 3GPP2 X.S0004)
AT	Access Terminal
AUTHR	AuthenticationResponse
AUTHREQ	AuthenticationRequest Invoke
authreq	AuthenticationRequest Return Result
BCD	Binary Coded Decimal
BS	Base Station
CAVE	Cellular Authentication and Voice Encryption algorithm
CCAT	CDMA Card Application Toolkit
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CIBER	Cellular Intercarrier Billing Exchange for Roamer
CSC	Customer Service Center

CSIM	CDMA Subscriber Identity Module
DBM	*Data Burst Message*
DRM	Digital Rights Management
EF	Elementary File
EIR	Equipment Identity Register
ESN	Electronic Serial Number
EUIMID	Expanded (Removable) User Identity Module Identifier
f-csch	Forward common signaling channel
GDA	Global Decimal Administrator (currently BABT)
GHA	Global Hexadecimal Administrator (currently TIA)
GPM	General Page Message
GSM	Global System for Mobile
HLR	Home Location Register
HOCM	*Handoff Complete Message*
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
IOS	Interoperability Specification
IRM	International Roaming MIN
ITU-T	International Telecommunication Union – Standardization Sector
LAC	Link Access Control
LBS	Location-Based Services
LF_EUIMID	Long Form EUIMID
MAP	Mobile Application Part

ME	Mobile Equipment (phone 'shell' without R-UIM or CSIM)
MECAM	*MEID Enhanced Channel Assignment Message*
MEID	Mobile Equipment Identifier
MIN	Mobile Identification Number
MS	Mobile Station
MSC	Mobile Switching Center
MT	Mobile Terminated
MUHDM	*MEID Universal Handoff Direction Message*
NAI	Network Access Identifier
ORM	*Origination Message*
OTAF	Over-The-Air Function
OTASP	Over The Air Service Provisioning
PCF	Packet Control Function
PDSN	Packet Data Serving Node
pESN	Pseudo-ESN
PIN	Personal Identification Number
PLCM	Public Long Code Mask
PRL	Preferred Roaming List
PRM	*Page Response Message*
pUIMID	Pseudo-EUIMID
r-csch	Reverse common signaling channel
R-UIM	Removable User Identity Module
SCM	Station Class Mark
SF_EUIMID	Short Form EUIMD

SHA	Secure Hash Algorithm
SMDPP	ShortMessageDeliveryPointToPoint Invoke
smdpp	ShortMessageDeliveryPointToPoint Return Result
SPC	Service Programming Code
SSD	Shared Secret Data
STRPM	*Status Response Message*
STRQM	*Status Request Message*
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TMSI	Temporary Mobile Station Identity
TRN	Temporary Reference Number
UDR	Usage Data Record
UHDM	*Universal Handoff Direction Message*
UICC	Universal Integrated Circuit Card
UIM	User Identity Module
UIMID	(Removable) User Identity Module Identifier
UMTS	Universal Mobile Telephone Service
USIM	Universal Subscriber Identity Module
UTK	UIM Tool Kit

1

9. References

[A.S001x]	3GPP2 A.S001*x*-D (TIA-2001.*x*). Interoperability Specification (IOS) for CDMA2000® Access Network Interfaces. V1.0. June 2007. http://www.3gpp2.org/Public_html/specs/tsga.cfm. • A.S0011. *Overview* • A.S0012. *Transport* • A.S0013. *Features* • A.S0014. *A1, A1p, A2, and A5 Interfaces* • A.S0015. *A3 and A7 Interfaces* • A.S0016. *A8 and A9 Interfaces* • A.S0017. *A10 and A11 Interfaces*
[A.S0008]	3GPP2 A.S0008-C (TIA-878). *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*. v1.0. July 2007. http://www.3gpp2.org/Public_html/specs/A.S0008-C_v1.0_070801.pdf
[C.S0005]	3GPP2 C.S0005 (IS-2000). *Upper Layer (Layer 3) Signaling Standard for CDMA2000 Spread Spectrum Systems*. v3.0. June 15, 2000. www.3gpp2.org/Public_html/specs/C.S0005-0_v3.0.pdf
[C.S0016]	3GPP2 C.S0016-C (TIA-683-D). *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*. v1.0. November, 2004. www.3gpp2.org/Public_html/specs/C.S0016-C_v1.0_041025.pdf *Version 2.0 is under development.*
[C.S0023]	3GPP2 C.S0023-C (TIA-820-C). *Removable User Identity Module for Spread Spectrum Systems*. v1.0. May 26, 2006. www.3gpp2.org/Public_html/specs/C.S0023-C_v1.0_060530.pdf *Version 2.0 is under development.*
[C.S0024]	3GPP2 C.S0024-A (TIA-856-A). *CDMA2000 High Rate Packet Data Air Interface Specification*. v3.0. September 2006. www.3gpp2.org/Public_html/specs/C.S0024-A_v3.0_060912.pdf

[C.S0035]	3GPP2 C.S0035-A. *CDMA Card Application Toolkit (CCAT).* v2.0. August 2007. http://www.3gpp2.org/public_html/specs/C.S0035-A_v2.0_070731.pdf
[C.S0065]	3GPP2 C.S0065-0 (TIA-1080). *CDMA2000 Application on UICC for Spread Spectrum Systems*. v2.0 July 2008 http://www.3gpp2.org/Public_html/specs/C.S0065-0_v2.0_080729.pdf
[C.S0066]	3GPP2 C.S0066-0 (TIA-158). *Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems*. v2.0. July, 2008. http://www.3gpp2.org/Public_html/specs/C.S0066-0_v2.0_080729.pdf
[C.S0072]	3GPP2 C.S0072-0 (TIA-1082). *Mobile Station Equipment Identifier (MEID) Support for CDMA2000 Spread Spectrum Systems*. v1.0. July 22, 2005. www.3gpp2.org/Public_html/specs/C.S0072-0_v1.0_050727.pdf
[C.S0073]	3GPP2 C.S0073-0. *Signaling Test Specification for Mobile Station Equipment Identifier (MEID) Support for CDMA2000 Spread Spectrum Systems*. v1.0. September 2005. www.3gpp2.org/Public_html/specs/C.S0073-0_v1.0_051004.pdf
[CDG Ref Doc 137]	CDG Reference Document #137, Mobile Equipment Identifier Roaming Recommendations. v1.0, December 2006.http://www.cdg.org/members_only/refdocs/137.zip
[Collisions WP]	Pellegrino, Gary; Quick, Frank. *White Paper on Pseudo-ESN Collisions*. TIA TR-45 ESN/UIM Ad Hoc Group. May 26, 2005. www.tiaonline.org/standards/resources/esn/documents/Collisions_pESN_wp.pdf
[GSMA TW.06]	GSMA PRD TW.06. IMEI Allocation and Approval Guidelines. December 2004. http://www.gsmworld.com/documents/twg/tw06.pdf
[E.118]	ITU-T Recommendation E.118. *The international telecommunication charge card*. May 2006. www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.118-200605-I!!PDF-E&type=items
[MEID Failure Bulletin]	CDG Technical Bulletin 070301IRT. *MEID IOS Issue*. v1.0, March 2007. http://www.cdg.org/members_only/teams/IntRoaming/docs/CDG%20Tech%20Bulletin%20070301IRT%20MEID%20IOS%20Issue%20v1_0.doc

[SC.R4001]	3GPP2 SC.R4001-0. *Global Wireless Equipment Numbering Administration Procedures.* V1.0. February, 2004. http://www.3gpp2.org/public_html/Specs/SC.R4001-0_v1.0_Wireless_Equipment_Numbering_Admin_Procedures_040420.pdf
[SC.R4002]	3GPP2 SC.R4002-0. *Mobile Equipment Identifier (MEID) GHA (Global Hexadecimal Administrator), Assignment Guidelines and Procedures.* v4.0. July 26, 2007. http://www.3gpp2.org/public_html/Specs/SC.R4002-0_v4.0_MEID_GHA_Guidelines_070730.pdf
[SC.R4003]	3GPP2 SC.R4003. *Expanded R-UIM Numbering Administration Procedures*. v1.0. May 2007. http://www.3gpp2.org/public_html/Specs/SC.R4003-0_v1.0_EUIMID_Procedures_070521.pdf
[S.R0111]	3GPP2 S.R0111-0. *Expanded R-UIM Identifier, Stage 1 Requirements*. v2.0. 17 May 2007. http://www.3gpp2.org/public_html/specs/S.R0111-0_v2.0_070521.pdf
[S.R0048]	3GPP2 S.R0048-A (TIA-928). *3G Mobile Equipment Identifier (MEID), Stage 1*. v4.0. June 23, 2005. *www.3gpp2.org/Public_html/specs/S.R0048-A_v4.0_050630.pdf*
[X.S0008]	3GPP2 X.S0008-0 (TIA-928). *MAP Support for the Mobile Equipment Identity (MEID)*. v2.0. October 2005. www.3gpp2.org/Public_html/specs/X.S0008-0_v2.0_051018.pdf
[X.S0011]	3GPP2 X.S0011-xxx-D (TIA-835). *CDMA2000 Wireless IP Network Standard*, v1.0, March 2006 http://www.3gpp2.org/Public_html/specs/tsgx.cfm
[X.S0033]	3GPP2 X.S0033-0 (TIA-1074). *OTA Support for MEID*. v2.0. February 2006. www.3gpp2.org/Public_html/specs/X.S0033-0_v2.0_060301.pdf

1