3GPP2 X.S0008-A v2.0

March 2014

MAP Support for the Mobile Equipment Identity (MEID)

© **2014 3GPP2**
3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

REVISION HISTORY

Version		Date
Rev. 0 v1.0	Initial Publication	June 2004
Rev. 0 v2.0	Annexes A & B added; clarifications	October 2005
Rev. 0 v3.0	Annex A & B footnotes updated	January 2009
Rev. 0 v4.0	Annex B check digit calculation clarified	February 2012
Rev. A v1.0	Introduction of MEID_ME and SF_EUIMID terminology to replace MEID	June 2013
Rev. A v2.0	Support for MEID Device Binding	March 2014

MAP Support for the Mobile Equipment Identity (MEID)

Contents

LIST OF TABLES

FOREWORD

This foreword is not part of this document.

This document was prepared by 3GPP2 TSG-SX.

1 INTRODUCTION

1.1 Scope

This document specifies the MAP modifications needed for support of the Mobile Equipment Identifier (MEID).

1.2 Document Conventions

"Shall" and "shall not" identify requirements to be followed strictly to conform to this document and from which no deviation is permitted. "Should" and "should not" indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. "May" and "need not" indicate a course of action permissible within the limits of the document. "Can" and "cannot" are used for statements of possibility and capability, whether material, physical or causal.

1.3 Normative References

This section provides references to other specifications and standards that are necessary to implement this document. References are either specific (identified by date of publication, revision identifier, and version number) or non-specific.

- For a specific reference, subsequent revisions may not apply.
- For a non-specific reference, the latest revision applies.

[GSM MAP] 3GPP TS 29.002. 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Application Part (MAP) Specification.

[CDMA] 3GPP2 C.S000[1,2,3,4,5,6]-E v3.0. cdma2000 Spread Spectrum Systems. June 2011.

[MAP] 3GPP2 X.S0004-E. Mobile Application Part (MAP).

Note: 3GPP2 X.S0004-E is a set of specifications and is a non-specific reference.

3GPP2 N.S0005-0 v1.0. Wireless Radiotelecommunications Intersystem Operations. 1997.

[MEID Binding] 3GPP2 S.S0152-0 v1.0. Security Framework for Binding of Access Subscription with Devices. December 2013.

1.4 Informative References

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

[EUIMIDStg1] 3GPP2 S.R0111 v2.0. Expanded R-UIM Identifier, Stage 1 Requirements. May 2007.

[MEIDStg1] 3GPP2 S.R0048-A v2.0. 3G Mobile Equipment Identifier (MEID) Stage 1. April 2004.

[RUIM] 3GPP2 C.S0023-B v1.0. Removable User Identity Module for Spread Spectrum Systems. May 2004.

[23.003] 3GPP TS 23.003 10.2.0. Numbering, addressing and identification. June 2011.

1.5 Assumptions

1. MEID-equipped mobiles do not have a true ESN. They transmit either UIMID (including pUIMID) or pseudo-ESN as ESN

   These MSs may also transmit an MEID_ME or SF_EUIMID under some circumstances.

2. The MEID_ME and SF_EUIMID are not used for authentication.

3. The CheckMEID operation is optional.

1.6 Editorial Conventions

The following editorial conventions are used for this document:

- ~~red cross-out~~ with change bars indicates text that is being deleted from X.S0004.
- Changes to X.S0004 are shown in blue, underlined text with change bars.
- Entirely new sections for X.S0004 just have a change bar.

In figures, blue dashed arrows indicate interfaces outside the scope of X.S0004 and N.S0005, and are included for illustrative purposes only.

2 *X.S0004-000-E* MODIFICATIONS

This section provides additional definitions for the introductory matter for *X.S0004-E* (part 000). See Annex C for further information regarding some of the terms used in this specification.

Card

A subscriber identity module, either *R-UIM* or *CSIM*.

Expanded UIMID (EUIMID)

A unique *CDMA* Card identifier that is longer than the unique UIMID it replaces and that is used in conjunction with pUIMID. May be an SF_EUIMID.

Mobile Equipment (ME)

A wireless transceiver device, without the Card.

Mobile Equipment Identifier (MEID)

A protocol element that is either an MEID_ME or an SF_EUIMID.

MEID_ME

A 56-bit number that, in conjunction with pESN, replaces ESN as the unique identifier of an ME.

MEID_SIG

An electronic signature cryptographically computed using the credentials associated with the MEID_ME (see *MEID Binding*). This signature is used by the network to enforce the binding of a cdma2000 1x subscription to a specific Mobile Station or to a group of Mobile Stations.

Pseudo-ESN (pESN)

A 32-bit number derived from the MEID_ME and used in place of the electronic serial number. The high order 8 bits are always 0x80 and the remaining 24 bits are derived using the SHA-1 algorithm as defined in *CDMA*.

Pseudo-UIMID (pUIMID)

A 32-bit number derived from the EUIMID and used in place of the UIMID. The high order 8 bits are always 0x80 and the remaining 24 bits are derived using the SHA-1 algorithm as defined in *CDMA*.

Short Form Expanded UIMID (SF_EUIMID)

A 56-bit number that, in conjunction with pUIMID, may replace UIMID as the unique identifier of a *CDMA* Card (see *EUIMIDStg1*).

UIMID

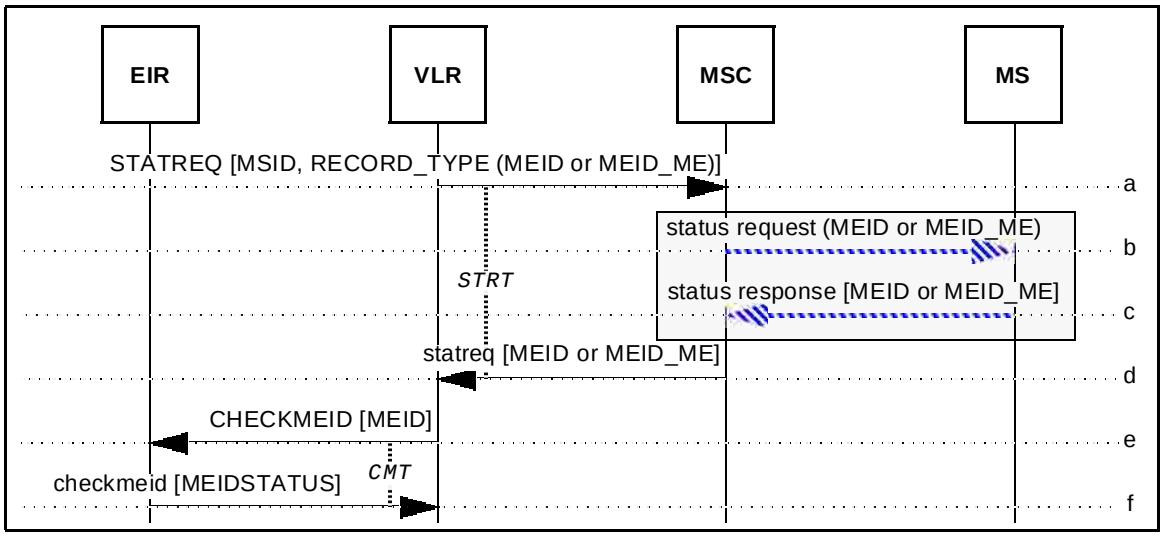
A 32-bit number used to uniquely identify a *CDMA* Card or a pUIMID (that satisfies some protocol requirements but does not uniquely identify a CDMA Card).

3 *N.S0005-0* CHAPTER 3 MODIFICATIONS

This section provides information flows for MEID support according to the structure of *N.S0005-0 Parts 3xx*.

3.1 Check MEID Procedure (new)

This scenario illustrates the Check MEID procedure. In this case, the VLR does not have the MEID of the MS and initiates the Status Request operation to retrieve it.



a. The VLR sends a `STATREQ` to the Serving MSC with the MSID parameter set to identify the target MS. The RECORD_TYPE parameter is set to request the MEID or MEID_ME information record.

b. Optionally, the MSC sends a *status request* message to the MS requesting the MEID or MEID_ME information record.

c. The MS returns its MEID or MEID_ME in the *status response* message. If MEID is returned, it may be MEID_ME or SF_EUIMID and the protocol does not identify which type of identifier is being returned.

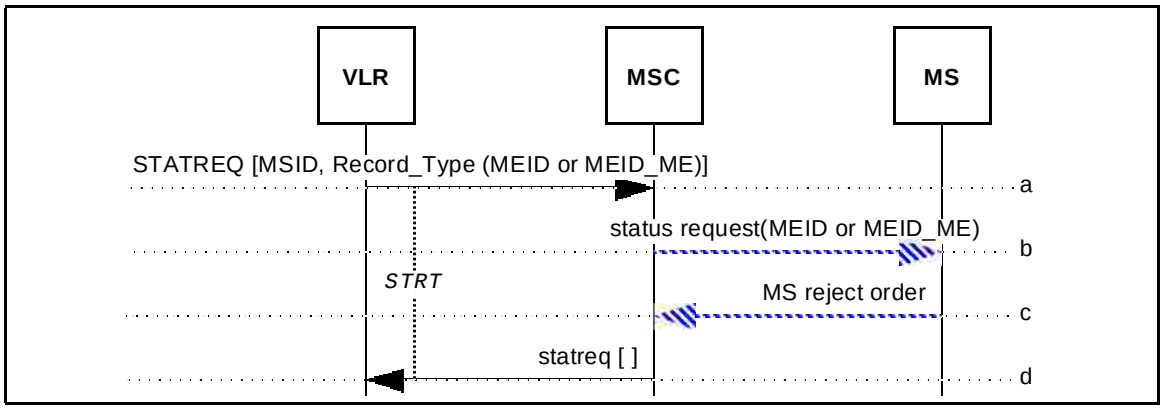
d. The MSC sends a `statreq` with the requested MEID to the VLR.

e. The VLR can now check the MEID or MEID_ME in the EIR database. The VLR sends the MEID to the EIR in the `CHECKMEID`.

f. The EIR returns the requested equipment status to the VLR in the `checkmeid`. The status may be *Normal*, *Block*, *Track*, or *No Entry*.

3.2 Unsuccessful Status Request (new)

This scenario illustrates an unsuccessful StatusRequest operation.



a. The VLR sends a STATREQ to the Serving MSC with the MSID parameter set to identify the target MS. The Record_Type parameter is set to request the MEID or MEID_ME information record.

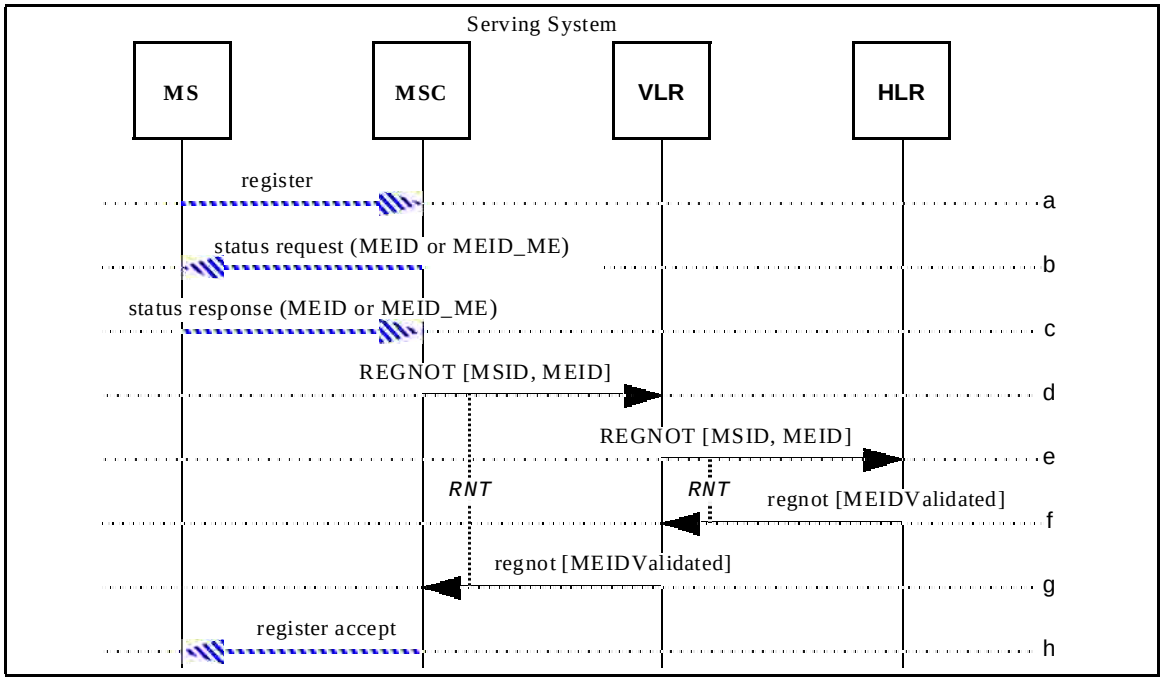
b. The MSC sends a *status request* message to the MS requesting the MEID or MEID_ME information record.

c. The MS cannot provide the requested information (e.g. because it does not support the correct revision of *CDMA*) and sends the *MS reject order*.

d. The MSC sends an empty statreq to the VLR to indicate that the *status response* message was not received from the MS.

3.3 MEID-Based Subscription Validation in the Visited Network - Authentication Not Active in Serving MSC (new)

This scenario illustrates the use of a provisioned MEID value in validating an MS (subscription). In this scenario the Serving MSC utilizes the Status Request/Status Response operation on the CDMA radio interface as a means to obtain the MEID of the MS so that a comparison can be made.



a. The MS acquires a CDMA system and registers based on SID/NID change. The MS does not include MEID in the *register* message (e.g., because the acquired system does not indicate support of MEID). The MS is not solicited to provide authentication parameters. The MS supplies an indication of its own support of MEID.

b. Because the MS supplied an indication of its own support of MEID, yet the MSC does not have the MEID of the MS, the MSC solicits the MEID or MEID_ME of the MS by way of a *status request* message over the radio interface.

c. The MS responds with a *status response* message that includes the MEID or MEID_ME.

d. The MSC sends a `REGNOT` to the VLR. The `REGNOT` includes the MEID value transmitted by the MS.

e. The VLR forwards the `REGNOT` to the MS' HLR.

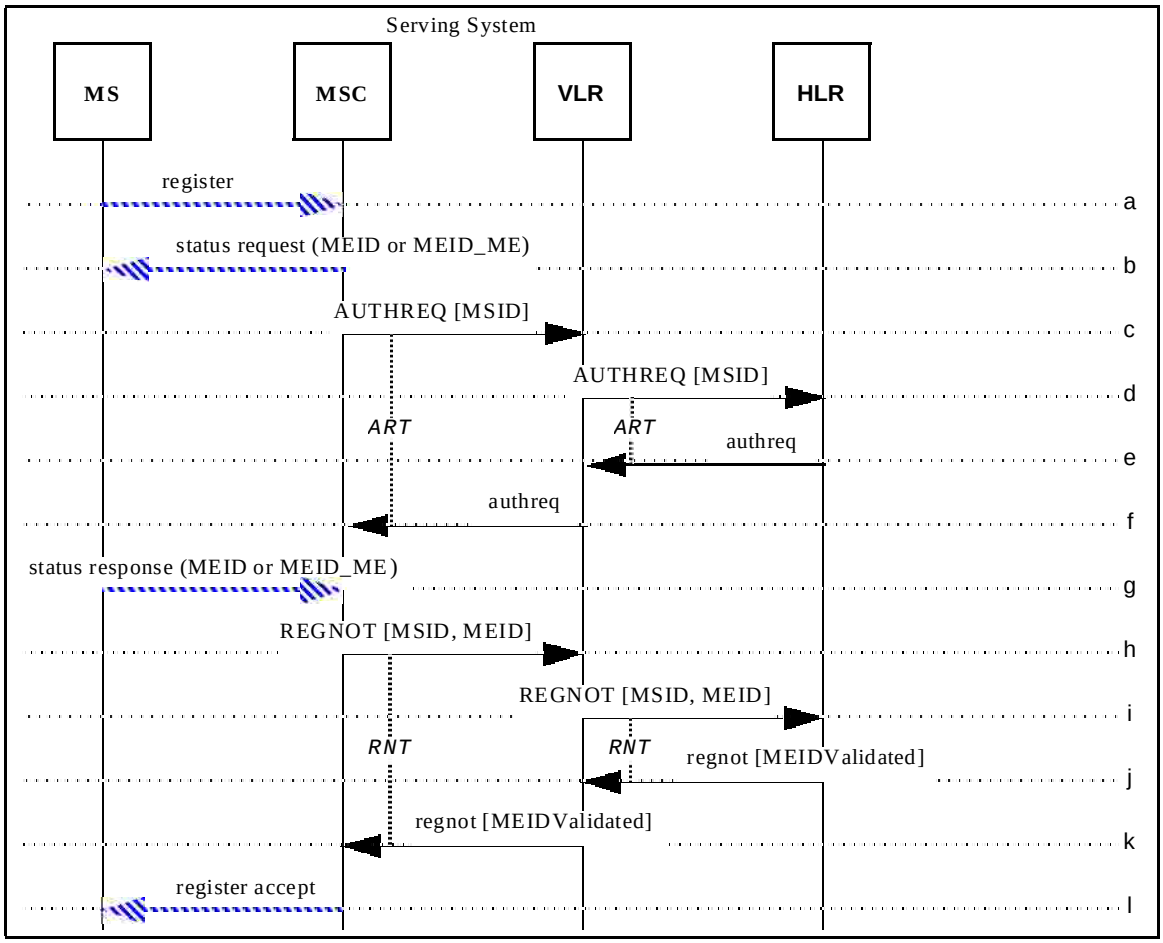
f. Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the `REGNOT`, the HLR includes an MEID comparison in the validation of the subscription. The HLR then registers the indicated MS and returns a `regnot` to the Serving VLR. The `regnot` includes the MEIDValidated parameter to inform the Serving VLR/MSC that the MEID associated with the system access has been validated.

g. The VLR sends a `regnot` to the MSC. The MEID received at step-c is stored at the Serving MSC for use in validating subsequent system accesses by the MS.

h. Optionally, the MSC confirms the success of the registration event to the MS.

3.4 MEID-Based Subscription Validation in the Visited Network -Authentication Active in Serving MSC (new)

This scenario illustrates the use of a provisioned MEID value in validating an MS (subscription). In this scenario the Serving MSC utilizes the Status Request/Status Response operation on the CDMA radio interface as a means to obtain the MEID of the MS so that a comparison can be made. Authentication is active in the visited system, yet the MS is marked as 'No authentication required' in the AuthenticationCapability parameter received from the HLR as part of the subscriber service profile.



a. The MS acquires a CDMA system and registers based on SID/NID change. The MS includes CAVE-related authentication parameters in the radio interface *register* message as mandated by the acquired system by way of broadcast system information. The MS does not include MEID in the *register* message (e.g., because the acquired system does not indicate support of MEID). The MS supplies an indication of its own support of MEID.

b. Because the MS supplied an indication of its own support of MEID, yet the MSC does not have the MEID of the MS, the MSC solicits the MEID or MEID_ME of the MS by way of a *status request* message over the radio interface.

c. The MSC sends an AUTHREQ to the VLR.

d. The VLR forwards the AUTHREQ to the MS' HLR.

e. The HLR determines that authentication is not required for this particular MS and returns an `authreq` to the Serving VLR.

f. The VLR sends an `authreq` to the MSC.

g. The MS responds with a *status response* message that includes the MEID or MEID_ME.

h. The MSC sends a `REGNOT` to the VLR. The `REGNOT` includes the MEID value transmitted by the MS.

i. The VLR forwards the `REGNOT` to the MS' HLR.

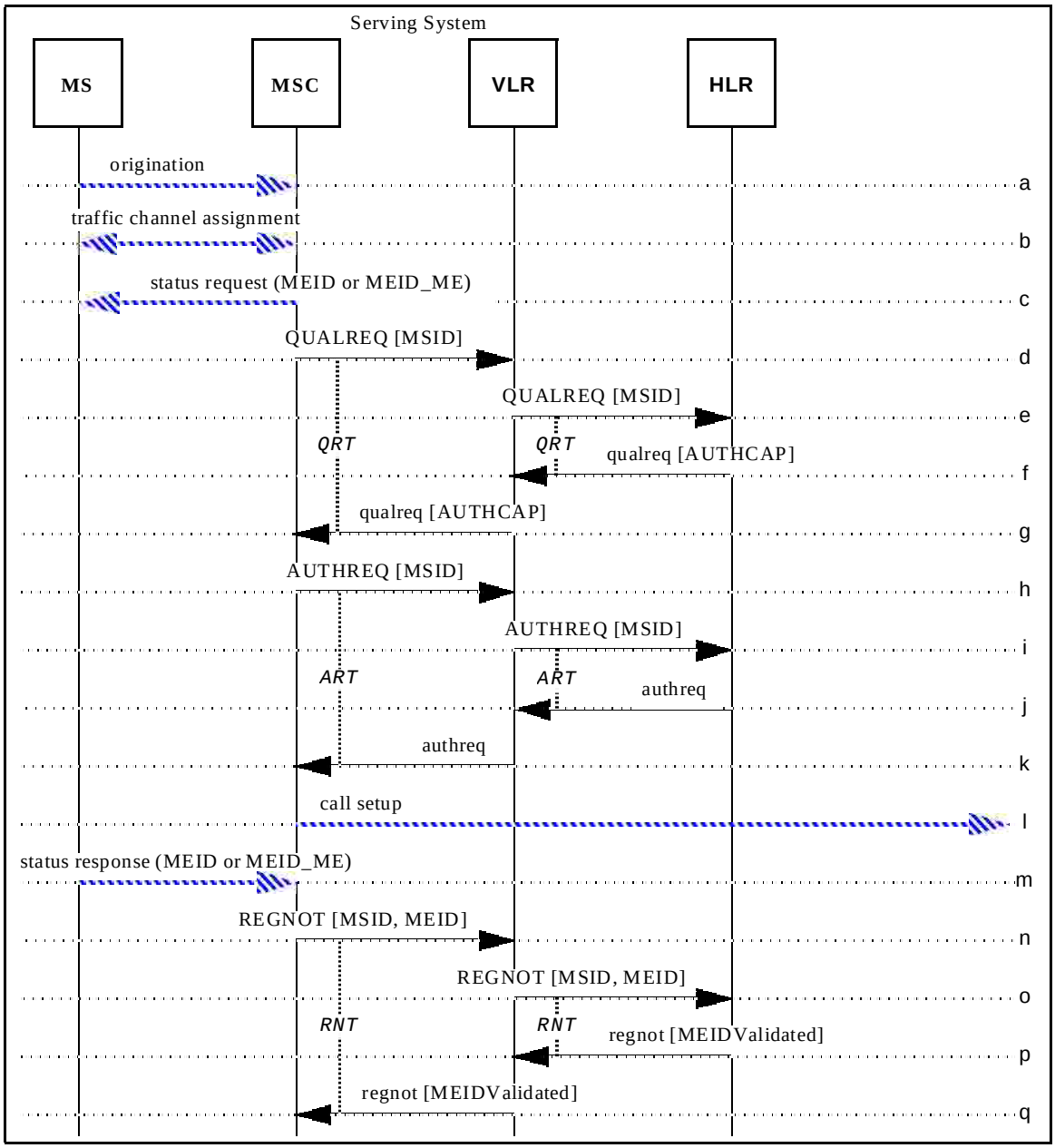
j. Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the REGNOT, the HLR includes an MEID comparison in the validation of the subscription. The HLR registers the indicated MS and returns a `regnot` to the Serving VLR. The `regnot` includes the MEIDValidated parameter to inform the Serving VLR/MSC that the MEID associated with the system access has been validated. The AUTHCAP parameter is also included in the `regnot` (as part of the subscriber service profile) and is set to *No authentication required*.

k. The VLR sends a `regnot` to the MSC. The MEID received at step-g is stored at the Serving MSC for use in validating subsequent system accesses by the MS.

l. Optionally, the MSC confirms the success of the registration event to the MS.

3.5 MEID-Based Subscription Validation in the Visited Network - Origination with Authentication (new)

This scenario illustrates the use of a provisioned MEID value in validating an MS (subscription). In this scenario the Serving MSC utilizes the Status Request/Status Response operation on the CDMA radio interface as a means to obtain the MEID of the MS so that a comparison can be made. The MS originates a call as the initial system access.



a. The MS acquires a CDMA system and, prior to any other system access, originates a call. The MS includes CAVE-related authentication parameters in the radio interface *origination* message as mandated by the acquired system by way of broadcast system information. The MS does not include MEID in the *origination* message (e.g., because the acquired system does not indicate support of MEID). The MS supplies an indication of its own support of MEID.

b. The MS is assigned to a traffic channel (TCH).

c. Because the MS supplied an indication of its own support of MEID, yet the MSC does not have the MEID of the MS, the MSC solicits the MEID or MEID_ME of the MS by way of a *status request* message over the radio interface. Proceed with steps d-g. Optionally, in parallel, initiate steps h-k.

d. The MSC sends a QUALREQ to the VLR.

e. The VLR forwards the QUALREQ to the MS' HLR.

f. The HLR returns an qualreq to the Serving VLR. The AUTHCAP parameter is included in the qualreq (as part of the subscriber service profile) and is set to *No authentication required*.

g. The VLR sends a qualreq to the MSC.

h. The MSC sends an AUTHREQ to the VLR.

i. The VLR forwards the AUTHREQ to the MS' HLR.

j. The HLR determines that authentication is not required for this particular MS and returns an authreq to the Serving VLR.

k. The VLR sends an authreq to the MSC.

l. The Serving MSC continues with call origination. *Note:* This step and the next (receipt of the MEID from the MS) could occur in either order.

m. The MS responds with a *status response* message that includes the MEID or MEID_ME.

n. The MSC sends a REGNOT to the VLR. The REGNOT includes the MEID value transmitted by the MS.

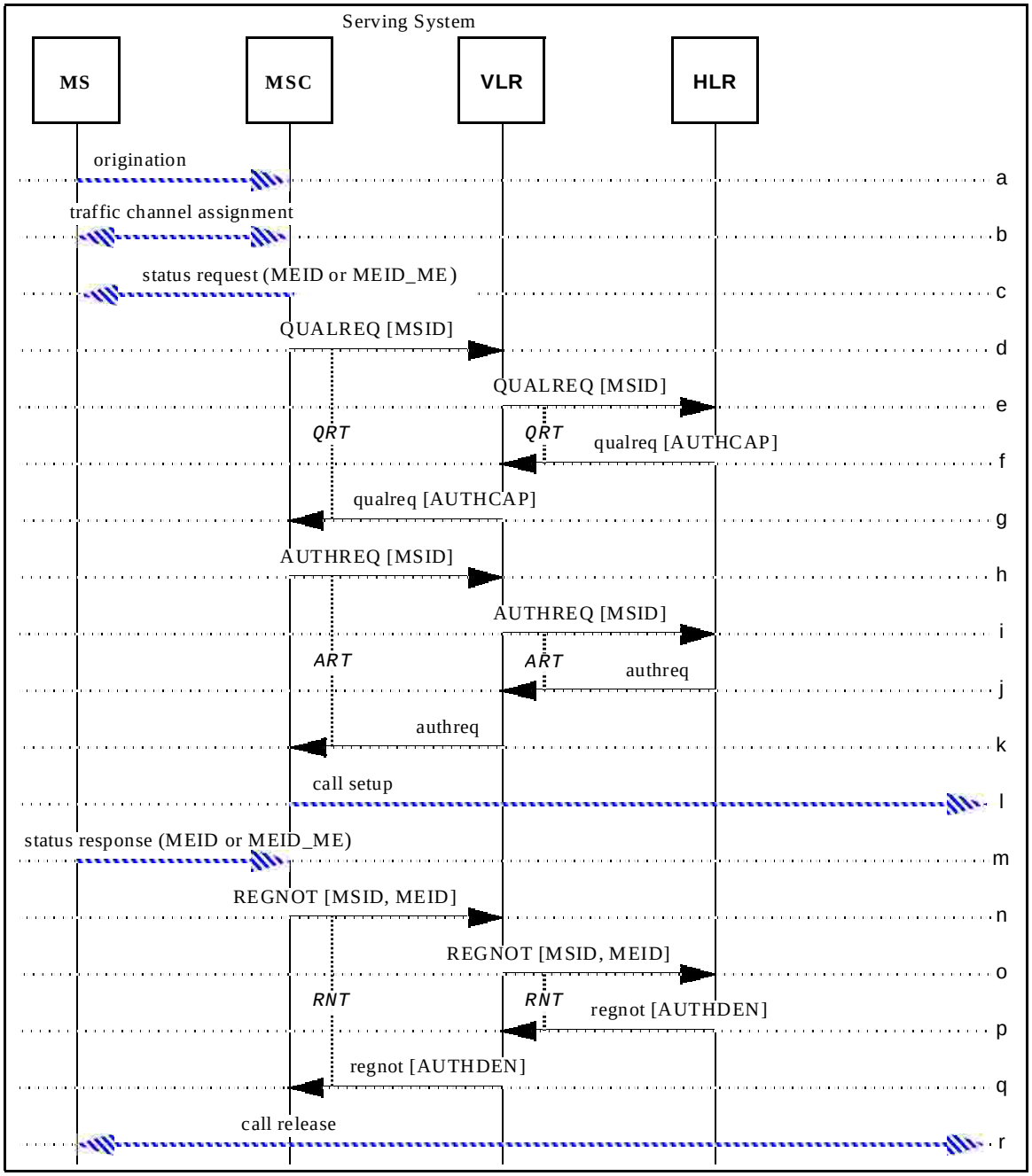
o. The VLR forwards the REGNOT to the MS' HLR.

p. 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 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.

q. The VLR sends a regnot to the MSC. The MEID received at step-m is stored at the Serving MSC for use in validating subsequent system accesses by the MS.

3.6 MEID-Based Subscription Validation in the Visited Network - Validation Fails (new)

This scenario illustrates the use of a provisioned MEID value in validating an MS (subscription). The MS originates a call as the initial system access. In this scenario the MEID received from the MS and the provisioned MEID for the MS do not match. The call in progress is cleared.



a-k. Same as 3.5, steps a-k.

l. The serving MSC continues with call origination.

m. The MS responds with a *status response* message that includes the MEID or MEID_ME.

n. The MSC sends a REGNOT to the VLR. The REGNOT includes the MEID value transmitted by the MS.

o. The VLR forwards the REGNOT to the MS' HLR.

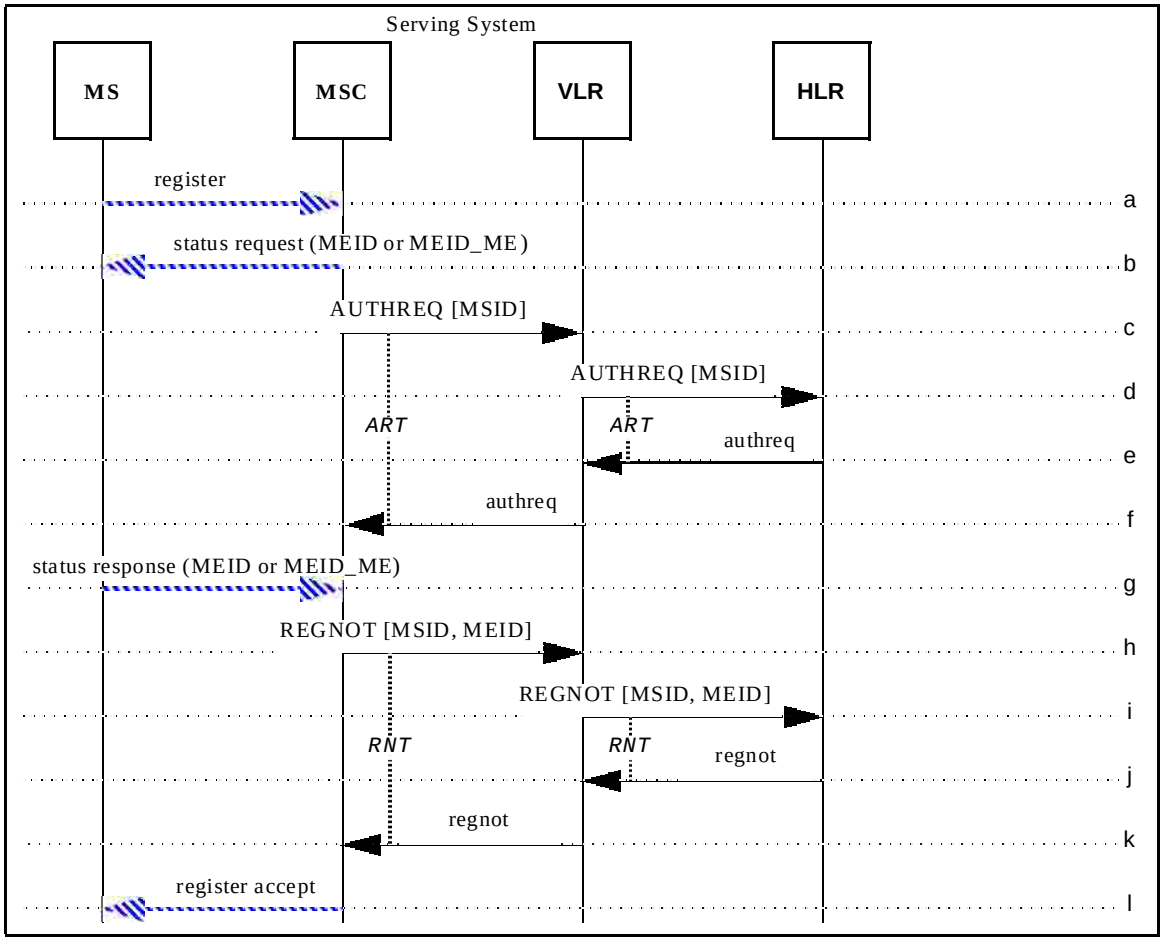
p. Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the REGNOT, the HLR includes an MEID comparison in the validation of the subscription. The HLR fails to validate the subscription due to an invalid MEID, and thus returns a regnot to the Serving VLR that includes the AuthorizationDenied (AUTHDEN) parameter set to value *Invalid serial number*.

q. The VLR sends a regnot to the MSC.

r. The call in progress is cleared; resources toward both the MS and the called party are released.

3.7 MEID Support in Visited Network But Not in HLR (new)

This scenario illustrates the inter-working of a Serving MSC and VLR that support MEID with an HLR that does not support MEID subscription validation. The Serving MSC utilizes the Status Request/Status Response operation on the CDMA radio interface as a means to obtain the MEID of the MS. No MEID-based subscription validation occurs within the HLR, thus the Serving MSC has no basis to validate the MEID of the MS.



a. The MS acquires a CDMA system and registers based on SID/NID change. The MS includes CAVE-related authentication parameters in the radio interface *register* message as mandated by the acquired system by way of broadcast system information. The MS does not include MEID in the *register* message (e.g., because the acquired system does not indicate support of MEID). The MS supplies an indication of its own support of MEID.

b. Because the MS supplied an indication of its own support of MEID, yet the MSC does not have the MEID of the MS, the MSC solicits the MEID or MEID_ME of the MS by way of a *status request* message over the radio interface.

c. The MSC sends an AUTHREQ to the VLR.

d. The VLR forwards the AUTHREQ to the MS' HLR.

e. The HLR determines that authentication is not required for this particular MS and returns an `authreq` to the Serving VLR.

f. The VLR sends an `authreq` to the MSC.

g. The MS responds with a *status response* message that includes the MEID or MEID_ME.

h. The MSC sends a `REGNOT` to the VLR. The `REGNOT` includes the MEID value transmitted by the MS.

i. The VLR forwards the `REGNOT` to the MS' HLR.

j. The HLR validates the subscription (e.g., using the ESN present in the `REGNOT`), then registers the indicated MS and returns a `regnot` to the Serving VLR. The AUTHCAP parameter is included in the `regnot` (as part of the subscriber service profile) and is set to *No authentication required*.

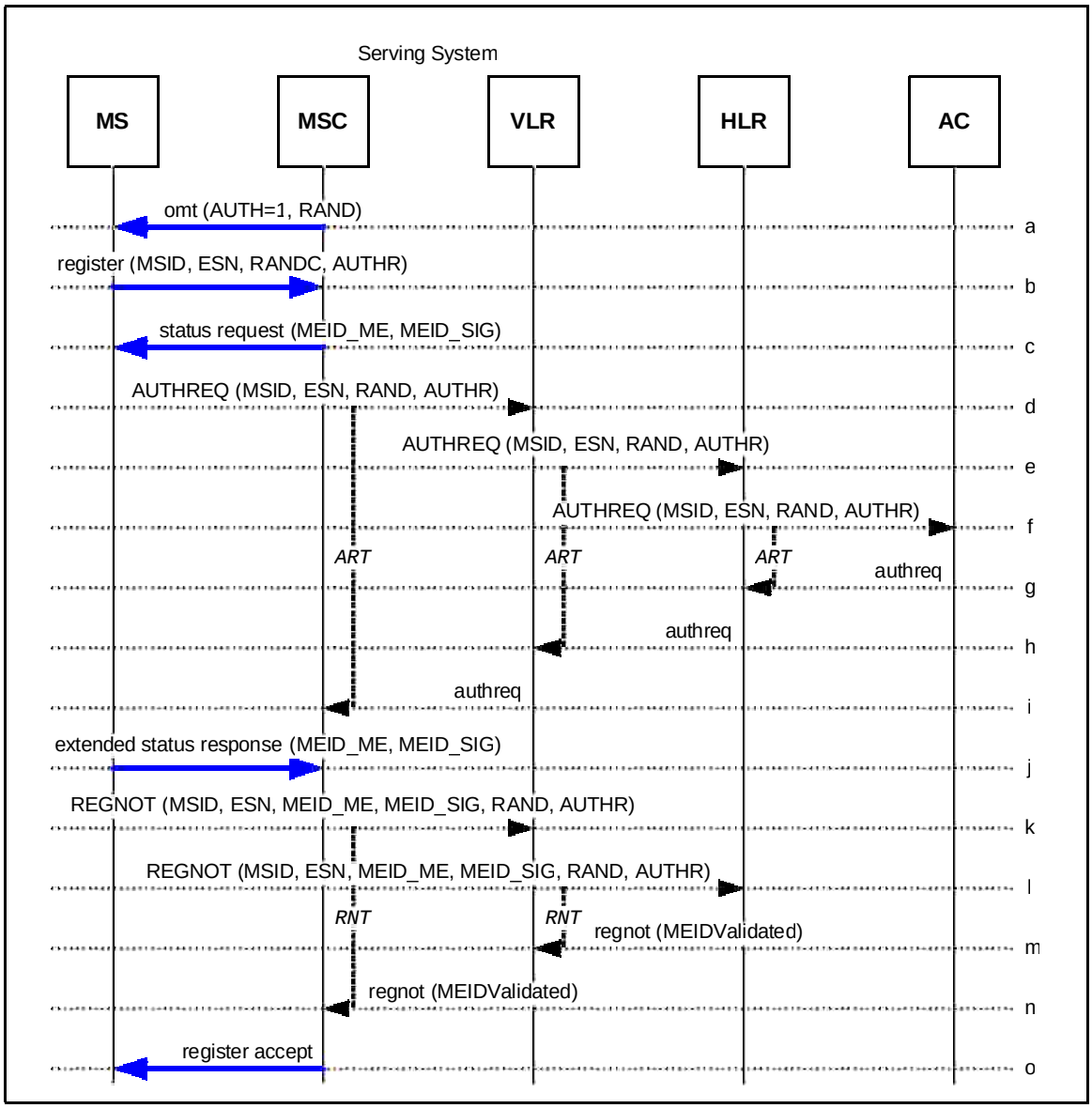
k. The VLR sends a `regnot` to the MSC. Since the MEIDValidated parameter is not present in the `regnot`, the MEID received at step-g is **not** used by the Serving MSC in validating subsequent system accesses by the MS.

l. Optionally, the MSC confirms the success of the registration event to the MS.

3.8 MEID Device Binding with Global Challenge (new)

This scenario illustrates the binding of an access subscription to an ME when global channel is used in the serving system. This scenario is applicable for a Serving System that supports MEID device binding (see *MEID Binding*).

Only those information flows relevant for MEID device binding are shown.



a. The MS determines from the Overhead Message Train (OMT) that a new serving system has been entered and that authentication is required on all system accesses (AUTH=1). The Random Number (RAND) to be used for authentication may also be obtained by the MS at this time.

   The MS executes CAVE using the SSD-A currently stored and the RAND value to produce a registration Authentication Result (AUTHR).

b. The MS sends a *register* to the Serving MSC providing its MSID, ESN, AUTHR, and RANDC derived from the RAND used to compute AUTHR.

c. The Serving MSC sends a *status request* with the new RECORD_TYPE to the MS (see *MEID Binding*). The RECORD_TYPE requests the MEID_ME and MEID_SIG.

d. The Serving MSC verifies the RANDC supplied by the MS and sends the appropriate value of RAND in an AUTHREQ to the Serving VLR.

e. The Serving VLR forwards the AUTHREQ to the HLR associated with the MSID.

f. The HLR forwards the AUTHREQ to the AC.

g. The AC verifies the MSID and ESN reported by the MS. The AC then executes CAVE using the SSD-A currently stored and the RAND value to produce a registration Authentication Result (AUTHR).

The AC verifies that the AUTHR received from the MS matches its CAVE results.

The AC sends an authreq to the HLR. The AC includes the DenyAccess if authentication was not successful.

h. The HLR forwards the authreq to the Serving VLR.

i. The VLR forwards the authreq to the Serving MSC.

j. The MS computes an MEID_SIG using its Device Binding Credentials (see *MEID Binding*) and the RAND and AUTHR from Step-a. The MS sends an *extended status response* to the Serving MSC and includes the MEID_SIG and MEID_ME.

k. The Serving MSC sends a REGNOT to the Serving VLR and includes the MEID, ESN, MEID_ME, MEID_SIG, and the RAND and AUTHR used to compute the received MEID_SIG.

l. The Serving VLR forwards the REGNOT to the HLR.

m. Based on the parameters included in the received REGNOT, the HLR verifies that the MSID is expected to be paired with an authorized MEID_ME (see *MEID Binding*). The HLR verifies that the received MSID is allowed to be paired with the received MEID_ME. Then the HLR computes the expected value of MEID_SIG using the Device Binding Credentials associated with the MEID and the received RAND and AUTHR to validate the reported MEID_ME.

The HLR registers the MS and sends a regnot to the Serving VLR. The regnot includes the MEIDValidated parameter to indicate successful MEID binding to the MSID.

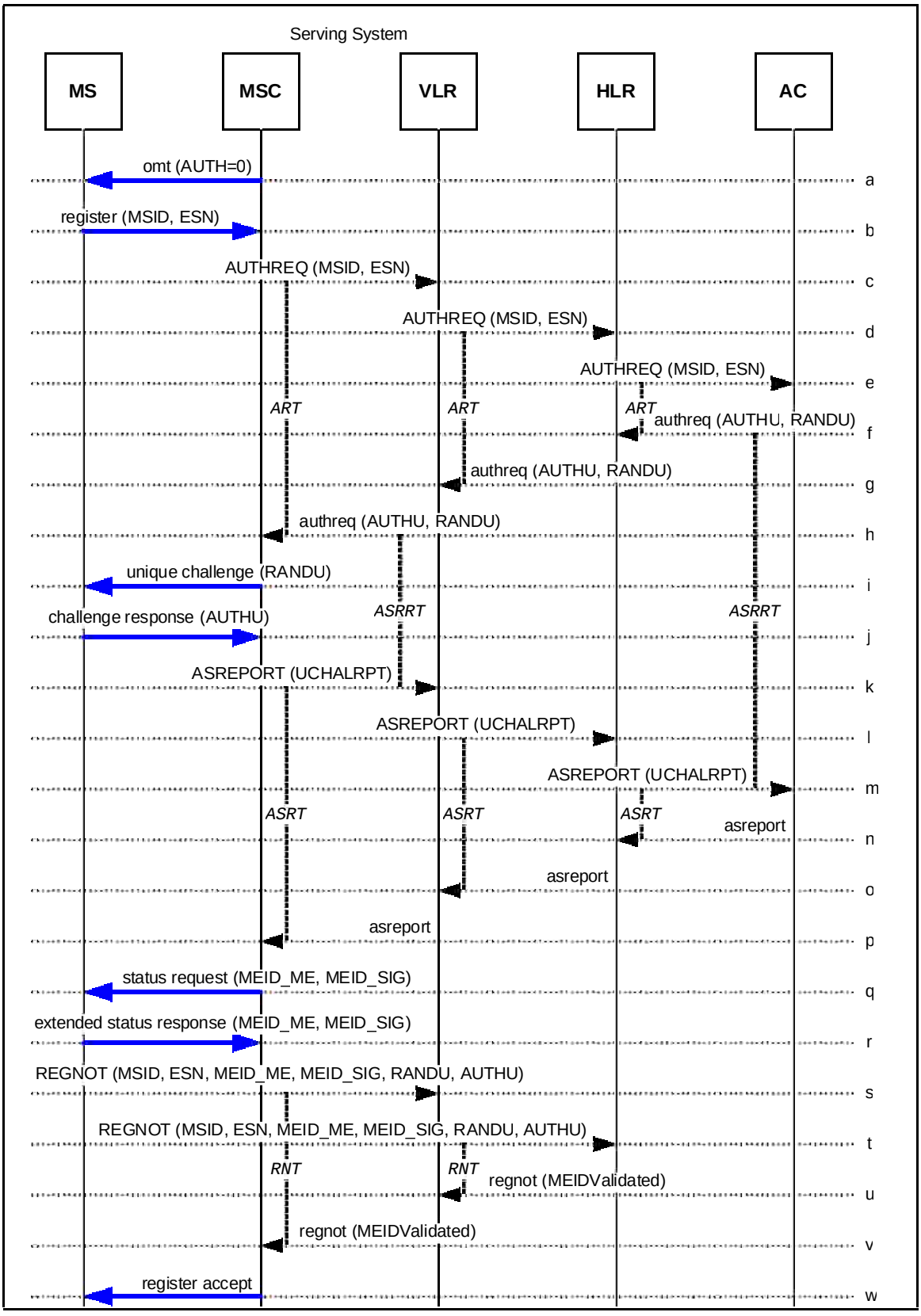
n. The Serving VLR registers the MS and forwards the regnot to the Serving MSC.

o. Upon successful registration of the MS, the Serving MSC sends a *register accept* to the MS.

3.9 MEID Device Binding with Unique Challenge (new)

This scenario illustrates the binding of an access subscription to an ME when global challenge is not used by the serving system (i.e., unique challenge is performed on a control or traffic channel). This scenario is applicable for a Serving System that support MEID device binding (see *MEID Binding*).

Only those information flows relevant for MEID device binding are shown.



a. The MS determines from the Overhead Message Train (OMT) that authentication is not required on system accesses (AUTH=0).

b. The MS sends a *register* message to the Serving MSC, providing its MSID and ESN only.

c. The Serving MSC sends an AUTHREQ to the Serving VLR.

d. The VLR forwards the AUTHREQ to the HLR associated with the MSID.

e. The HLR forwards the AUTHREQ to its AC.

f. The AC verifies the MSID and ESN reported by the MS. The AC chooses a Unique Random Variable (RANDU) and executes CAVE using the SSD-A currently stored to produce a Unique Authentication Response (AUTHU).

The AC sends an authreq to the HLR including RANDU and the expected AUTHU result.

g. The HLR forwards the authreq to the Serving VLR.

h. The Serving VLR forwards the authreq to the Serving MSC.

i. The Serving MSC sends a *unique challenge order* to the MS using the RANDU provided in the authreq.

j. The MS executes CAVE using RANDU and the SSD-A currently stored to generate an Authentication Result (AUTHU) which is then sent to the Serving MSC.

The Serving MSC compares the value of AUTHU provided in the authreq with that received from the MS.

k. The Serving MSC sends an ASREPORT to the Serving VLR indicating success or failure of the unique challenge.

l. The VLR forwards the ASREPORT to the HLR.

m. The HLR forwards the ASREPORT to its AC.

n. The AC responds with an asreport that may include SSD and directives to deny access according to the AC local administrative practices.

o. The HLR forwards the asreport to the Serving VLR.

p. The Serving VLR sends an asreport to the Serving MSC.

q. Following successful authentication of the MS, the Serving MSC sends a *status request* with the new RECORD_TYPE to the MS (see *MEID Binding*). The RECORD_TYPE requests the MEID_ME and MEID_SIG.

r. The MS computes an MEID_SIG using its Device Binding Credentials (see *MEID Binding*) and the RANDU and AUTHU from Step-j. The MS sends an *extended status response* to the Serving MSC and includes the MEID_SIG and MEID_ME.

s. The Serving MSC sends a REGNOT to the Serving VLR and includes the MEID, ESN, MEID_ME, MEID_SIG, and the RANDU and AUTHU used to compute the received MEID_SIG.

t. The Serving VLR forwards the REGNOT to the HLR.

u. Based on the parameters included in the received REGNOT, the HLR verifies that the MSID is expected to be paired with an authorized MEID_ME (see *MEID Binding*). The HLR verifies that the received MSID is allowed to be paired with the received MEID_ME. Then the HLR computes the expected value of MEID_SIG using the Device Binding Credentials associated with the MEID and the received RANDU and AUTHU to validate the reported MEID_ME.

The HLR registers the MS and sends a regnot to the Serving VLR. The regnot includes the MEIDValidated parameter to indicate successful MEID binding to the MSID.

v. The Serving VLR registers the MS and forwards the regnot to the Serving MSC.

w. Upon successful registration of the MS, the Serving MSC sends a *register accept* to the MS.

4 *X.S0004-5xx-E* MODIFICATIONS

This section provides the additions and modifications to *X.S0004-E* Parts 5xx signaling protocol for MEID support.

4.1 Application Services

4.1.1 MAP Operations

4.1.1.2 Operation Specifiers

(See X.S0004-540-E § 1.3)

Table 1 MAP Operation Specifiers

Operation Name	Operation Specifier								
	H	G	F	E	D	C	B	A	Decimal
CheckMEID	0	1	1	0	1	0	0	0	104
StatusRequest	0	1	1	0	1	0	1	1	107

4.1.2 Operation Definitions

(See X.S0004-540-E § 2)

Table 2 Summary of MAP Operations

Operation	Reference
CheckMEID	see 4.1.2.1
StatusRequest	see 4.1.2.2

4.1.2.1 CheckMEID (new)

(New for X.S0004-540-E)

The CheckMEID (CHECKMEID) operation is used to request information from an EIR on the status of a specific MEID.

The following table lists the possible combinations of invoking and responding NEs.

Table 3 FE Combinations for CheckMEID

	INVOKING NE	RESPONDING NE
Case 1	VLR	EIR

The CheckMEID operation is initiated with a TCAP INVOKE (LAST). This is carried by a TCAP QUERY WITH PERMISSION package. The Parameter Set is encoded as follows:

CheckMEID INVOKE Parameters			**Timer: CMT**	
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.3.2.1	
Length	variable octets	M	6.3.2.1	
Contents				
MEID		M	X.S0004-550	a

Notes:

a. Include to identify the MEID to be checked.

The CheckMEID operation success is reported with a TCAP RETURN RESULT (LAST). This is carried by a TCAP RESPONSE package. The Parameter Set is encoded as follows:

CheckMEID RETURN RESULTParameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.3.2.1	
Length	variable octets	M	6.3.2.1	
Contents				
MEIDStatus		M	X.S0004-550	a, b

Notes:

a. Include to specify the status of the ME identified by the given MEID.

b. If the MEID to be checked is within a valid SF_EUIMID range and is not individually listed, the status returned should be “Normal” as this indicates that the MEID_ME is not available.

4.1.2.2 StatusRequest (new)

(New for X.S0004-540-E)

The StatusRequest (STATREQ) operation is used to request information (such as MEID or MEID_ME) about a specific MS.

The following table lists the possible combinations of invoking and responding NEs.

Table 4 FE Combinations for StatusRequest

	INVOKING NE	RESPONDING NE
Case 1	VLR	MSC

The StatusRequest operation is initiated with a TCAP INVOKE (LAST). This is carried by a TCAP QUERY WITH PERMISSION package. The Parameter Set is encoded as follows:

StatusRequest INVOKE Parameters				**Timer: STRT**
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.3.2.1	
Length	variable octets	M	6.3.2.1	
Contents				
MSID		M	X.S0004-550	a
Record_Type		M	X.S0004-550	b

Notes:

a. Include to identify the MS.

b. Include to identify the information record requested (e.g., MEID or MEID_ME).

The StatusRequest operation success is reported with a TCAP RETURN RESULT (LAST). This is carried by a TCAP RESPONSE package. The Parameter Set is encoded as follows:

StatusRequest RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.3.2.1	
Length	variable octets	M	6.3.2.1	
Contents				
Information_Record		O	X.S0004-550	a

Notes:

a. Include the requested information record.

4.1.2.3 RegistrationNotification

(see X.S0004.540-E §2.50)

The RegistrationNotification operation is used to report the location of an MS and, optionally, to (a) validate the MS or (b) validate the MS and obtain its profile information. It is also used for delivering the Serving MSC's routing address to the Desired OTAF in support of TDMA OTASP.

The following table lists the valid combinations of invoking and responding FEs.

	INVOKING FE	RESPONDING FE
Case 1	Serving (or Bordering) MSC	Serving (or Bordering) VLR
Case 2	Serving (or Bordering) VLR-~~HLR~~	HLR
Case 3 (Note 1)	Serving VLR	OTAF

Note:

1. Case 3 is only applicable to TDMA OTASP.

The RegistrationNotification operation is initiated with a TCAP INVOKE (LAST). This is carried by a TCAP QUERY WITH PERMISSION package. The Parameter Set is encoded as follows:

RegistrationNotification INVOKE Parameters				**Timer: RNT**
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	520-1.3.2.1	
Length	variable octets	M	520.1.3.2.1	
Contents				
...				
MEID_ME		O	4.2.2.100	a
MEID_SIG		O	4.2.2.101	a
RandomVariable		O	X.S0004-550	b
AuthenticationResponse		O	X.S0004-550	b
RandomVariableUniqueChallenge		O	X.S0004-550	c
AuthenticationResponseUniqueChallenge		O	X.S0004-550	c
...				

Notes:

a. Include if the MSID is expected to be paired with an authorized MEID_ME.

b. Include if the MSID is expected to be paired with an authorized MEID_ME and authentication is performed on every system access (i.e., global challenge).

c. Include if the MSID is expected to be paired with an authorized MEID_ME and a unique challenge was used to authenticate the MS.

All other parameters are per X.S0004. Note 1

The RegistrationNotification operation success is reported with a TCAP RETURN RESULT (LAST). This is carried by a TCAP RESPONSE package. The Parameter Set is encoded as follows:

RegistrationNotification RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	520-1.3.2.2	
Length	variable octets	M	520-1.3.2.2	
Contents				
...				
MEIDValidated		O	4.2.2.98	a
...				

Notes:

a. Include for an MEID-capable MS to indicate that MEID-based subscription validation has succeeded.

All other parameters are per X.S0004. Note 2

4.2 Map Parameters

4.2.1 General

4.2.1.1 Parameter Identifiers

(See X.S0004-550-E § 1.2)

Table 5 MAP Parameter Identifiers

Parameter Identifier Name	Parameter Identifier Code								Reference
	H	G	F	E	D	C	B	A	
Information_Record	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	0	0	1	0	1	
MEID	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	0	0	1	1	0	
MEIDStatus	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	0	0	1	1	1	
Record_Type	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	0	1	0	0	0	
MEIDValidated	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	1	0	0	0	1	
MEID_ME	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	1	1	0	0	1	
MEID_SIG	1	0	0	1	1	1	1	1	X.S0004-550
	1	0	0	0	0	0	1	1	
	0	0	0	1	1	0	1	0	

4.2.2 Parameter Definitions

4.2.2.1 ElectronicSerialNumber

(See X.S0004-550-E § 2.112)

This parameter was named MobileSerialNumber prior to this revision of the Interim Standard.

The ElectronicSerialNumber (ESN) parameter is used to indicate the unique 32-bit electronic serial number of an MS, a UIMID (including pUIMID) of a card, or the Pseudo-ESN of an MS equipped with an MEID_ME.

Field	Value	Type	Reference	Notes
Identifier	ElectronicSerialNumber IMPLICIT OCTET STRING	M	Part 550 Section 1.2	
Length	4 octets	M	Part 550 Section 1.1	

Contents

H	G	F	E	D	C	B	A	Octet	Notes
Manufacturer's Code								1	a
MSB								2	a
Serial Number								3	
							LSB	4	

Notes:

a. See *AMPS*, *NAMPS*, *TDMA*, or *CDMA* for encoding of this field.

4.2.2.2 Information_Record (new)

(New for X.S0004-550-E)

The Information_Record parameter carries specific information requested from an ME.

Field	Value	Type	Reference	Notes
Identifier	INFORMATION_RECORD IMPLICIT OCTET STRING	M	6.5.1.2	
Length	variable	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
Status Information Record Type								1	a
Status Information Record Length								2	b
Type-specific fields								3-n	c,d

Notes:

a. Encoding is the same as the RECORD_TYPE in *CDMA*.

b. Encoding is the same as the RECORD_LENGTH in *CDMA*.

c. Encoding is the same as the Status Information Record Type-specific fields in *CDMA*.

d. Ignore extra octets, if received. Send only defined (or significant) octets.

4.2.2.3 MEID (new)

(New for X.S0004-550-E)

The MEID parameter specifies the unique 56-bit Mobile Equipment Identifier for an ME or the unique 56-bit SF_EUIMID for a card. See *MEIDStg1 and EUIMIDStg1*.

Field	Value	Type	Reference	Notes
Identifier	MEID IMPLICIT OCTET STRING	M	6.5.1.2	
Length	7 octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
MSB								1	
								2	
								3	
				MEID				4	
								5	
								6	
							LSB	7	

4.2.2.97 MEIDStatus (new)

(New for X.S0004-550-E)

The MEIDStatus (MEIDSTATUS) parameter specifies the current status of a given MEID in the EIR.

Field	Value	Type	Reference	Notes
Identifier	MEIDStatus IMPLICIT OCTET STRING	M	6.5.1.2	
Length	variable	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
MEID_Status								1	
• • •								n	a

Notes:

a. Ignore extra octets, if received. Send only defined (or significant) octets.

MEID_Status (octet 1, bits A-H)	
Decimal Value	Meaning
0	**Normal.** Same as GSM White Listed - see *GSM MAP*.
1	**Block.** Same as GSM Black Listed - see *GSM MAP*.
2	**Track.** Same as GSM Grey Listed - see *GSM MAP*.
3	**No Entry.** There is no entry covering this MEID.
Other values	Reserved for *MAP* protocol extension. If received treat as value 3, *No Entry*.

4.2.2.98 MEIDValidated (new)

The MEIDValidated (MEIDVAL) parameter informs the receiving network entity that MEID-based subscription validation has succeeded.

Field	Value	Type	Reference	Notes
Identifier	MEIDValidated IMPLICIT NULL	M	Part 550 Section 1.2	
Length	zero octets	M	Part 550 Section 1.1	
Contents				

4.2.2.99 Record_Type (new)

(New for X.S0004-550-E)

The Record_Type parameter specifies the information record type.

Field	Value	Type	Reference	Notes
Identifier	Record_Type IMPLICIT OCTET STRING	M	6.5.1.2	
Length	variable octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
Status Information Record Type								1	a
• • •								n	b

Notes:

a. Encoding is the same as the RECORD_TYPE in *CDMA*.

b. Ignore extra octets, if received. Send only defined (or significant) octets.

4.2.2.100 MEID_ME (new)

(New for X.S0004-550-E)

The MEID_ME parameter is used to indicate the unique 56-bit number that replaces the ESN as the unique identifier of an ME.

Field	Value	Type	Reference	Notes
Identifier	MEID_ME IMPLICIT OCTET STRING	M	6.5.1.2	
Length	7 octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
MSB								1	
								2	
								3	
			MEID_ME					4	
								5	
								6	
							LSB	7	

4.2.2.101 MEID_SIG (new)

(New for X.S0004-550-E)

The MEID_SIG parameter contains the electronic signature cryptographically computed using the credentials associated with the MEID_ME (see *MEID Binding*).

Field	Value	Type	Reference	Notes
Identifier	MEID_SIG IMPLICIT OCTET STRING	M	6.5.1.2	
Length	variable octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
MSB								1	
MEID_SIG								. . .	a
							LSB	n	

Notes:

a. See *MEID Binding* for the encoding of this field.

5 X.S0004-6xx-E SIGNALING PROCEDURES

5.1 Autonomous or Power-On Registration

When the MSC becomes aware of the presence of an MS through registration, the Serving MSC should do the following:

1 IF the MS is not authenticated and authentication is active:

1-1 IF the MS's AuthenticationCapability indicates the MS shall be authenticated[1]:

1-1-1 Include the SystemAccessType parameter set to *Autonomous registration*.

1-1-2 Execute the "MSC Initiating an Authentication Request" task (see Part 640, sec. 5.1).

1-1-3 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

1-1-3-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

1-1-3-2 Exit this task.

1-1-4 ENDIF.

1-1-5 IF authentication fails:

1-1-5-1 Execute "Local Recovery Procedures" task (see Part 630, sec. 5.1).

1-1-5-2 Exit this task.

1-1-6 ENDIF.

1-2 ENDIF.

2 ENDIF.

3 IF the MS is not registered:

3-1 Execute the "MSC Initiating MS Registration" task (see Part 640, sec. 57.1).

3-2 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

3-2-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

3-2-2 Exit this task.

3-3 ENDIF.

3-4 IF the MS is not authorized:

3-4-1 Execute "Local Recovery Procedures" task (see Part 630, sec. 5.1).

3-4-2 Exit this task.

3-5 ENDIF.

3-6 Send the MS the RoamingIndication parameter if received, in addition to other messages.

4 ENDIF.

5 IF the last received MessageWaitingNotificationType is *MWI ON* and the MessageWaitingNotificationCount indicates that at least one message is waiting:

[1] In addition the MSC shall initiate authentication procedures if there is no AuthenticationCapability information for the MS.

5-1 Execute the "MSC MWN Status Change Invocation" task (see Part 651, sec. 16.9) indicating that message waiting notification is required.

6 ENDIF.

7 Exit this task.

5.2 Idle MS Origination

When the MS attempts to originate a call, the Serving MSC shall do the following:

1 IF an appropriate *idle* voice or traffic channel is available for the identified air interface control channel, the MSC may pre-seize the channel by:

1-1 Reserve the available voice or traffic channel.

1-2 Order the MS to acquire the reserved voice or traffic channel.

1-3 Verify the MS has properly tuned to this voice or traffic channel.

2 ENDIF.

3 IF the MS is not registered AND IF local policy requires MEID validation of this call:[1]

3-1 IF the MEID of the MS is not received in the call origination:

3-1-1 Request the MEID of the MS (e.g., by means of the CDMA Status Request operation).

3-2 ENDIF.

4 ELSEIF the MS is already registered AND IF a stored MEID value exists for this MS AND IF local policy requires MEID validation of this call:

4-1 IF the MEID of the MS was not received in the call origination:

4-1-1 Request the MEID of the MS (e.g., by means of the CDMA Status Request operation).

4-1-2 IF the MEID is received from the MS AND IF the stored MEID was previously validated:

4-1-2-1 Execute the "MSC Receives MEID of MS" task (see 2.2).

4-1-3 ENDIF.

4-2 ELSE (the MEID of the MS was received in the call origination):

4-2-1 IF the stored MEID was previously validated:

4-2-1-1 Execute the "MSC Receives MEID of MS" task (see 2.2).

4-2-2 ENDIF.

4-3 ENDIF.

5 ENDIF.

6 IF the MS is not authenticated and authentication is active:

6-1 IF the MS's AuthenticationCapability indicates that the MS shall be authenticated[2]:

6-1-1 Include the SystemAccessType parameter set to *Call origination*.

6-1-2 IF the MS is not registered OR the location of the MS has changed since the last registration (i.e., the MS has left the location for which it is geographically authorized):

6-1-2-1 Set a *pending registration* flag for the MS.

---

1 Steps 3 through 5 may occur in parallel with steps 6 though 7.

2 In addition the MSC shall initiate authentication procedures if there is no AuthenticationCapability information for the MS.

6-1-3 ENDIF.

6-1-4 IF a *pending registration* flag is set for the MS OR the MSC requires the MS's profile (e.g., per call authorization required or the profile is not present):

6-1-4-1 IF the MSC requests qualification and authentication in parallel when a system access is received from an MS for which it does not have a valid service profile:

6-1-4-1-1 Execute the "MSC Initiating an Authentication Request" task (see Part 640, sec. 5.1) and the "MSC Initiating Qualification Request" task (see Part 640, sec. 52.1) in parallel.

6-1-4-1-2 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

6-1-4-1-2-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

6-1-4-1-2-2 Exit this task.

6-1-4-1-3 ENDIF.

6-1-4-1-4 IF authentication fails:

6-1-4-1-4-1 Clear the *pending registration* flag for the MS.

6-1-4-1-4-2 IF the MS dialed an OTASP Feature Code (e.g., *FC) AND CDMA is being used:

6-1-4-1-4-2-1 GOTO Pre-screening completed.

6-1-4-1-4-3 ELSEIF the MS dialed a locally allowed number (e.g., 9-1-1, *-9-1-1, N11, *N11):

6-1-4-1-4-3-1 Process the dialed number locally and route the call.

6-1-4-1-4-3-2 Exit this task.

6-1-4-1-4-4 ELSE:

6-1-4-1-4-4-1 Execute the "Local Recovery Procedures" task (see Part 630, sec. 5.1).

6-1-4-1-4-4-2 Exit this task.

6-1-4-1-4-5 ENDIF.

6-1-4-1-5 ELSE (authentication successful):

6-1-4-1-5-1 GOTO Pre-screening completed.

6-1-4-1-6 ENDIF.

6-1-4-2 ELSE:

6-1-4-2-1 Execute the "MSC Initiating Qualification Request" task (see Part 640, sec. 52.1).

6-1-4-2-2 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

6-1-4-2-2-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

6-1-4-2-2-2 Exit this task.

6-1-4-2-3 ENDIF.

6-1-4-2-4 IF the MS's AuthenticationCapability indicates that the MS shall be authenticated:

6-1-4-2-4-1 Execute the "MSC Initiating an Authentication Request" task (see Part 640, sec. 5.1).

6-1-4-2-5 ENDIF.

6-1-4-2-6 IF authentication fails:

6-1-4-2-6-1 Clear the *pending registration* flag for the MS.

6-1-4-2-6-2 IF the MS dialed an OTASP Feature Code (e.g., *FC) AND CDMA is being used:

6-1-4-2-6-2-1 GOTO Pre-screening completed.

6-1-4-2-6-3 ELSEIF the MS dialed a locally allowed number (e.g., 9-1-1, *-9-1-1, N11, *N11):

6-1-4-2-6-3-1 Process the dialed number locally and route the call.

6-1-4-2-6-3-2 Exit this task.

6-1-4-2-6-4 ELSE:

6-1-4-2-6-4-1 Execute the “Local Recovery Procedures” task (see Part 630, sec. 5.1).

6-1-4-2-6-4-2 Exit this task.

6-1-4-2-6-5 ENDIF.

6-1-4-2-7 ELSE (authentication successful):

6-1-4-2-7-1 GOTO Pre-screening completed.

6-1-4-2-8 ENDIF.

6-1-4-3 ENDIF.

6-1-5 ENDIF.

6-1-6 Execute the “MSC Initiating an Authentication Request” task (see Part 640, sec. 5.1).

6-1-7 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

6-1-7-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

6-1-7-2 Exit this task.

6-1-8 ENDIF.

6-1-9 IF authentication fails:

6-1-9-1 IF the MS dialed an OTASP Feature Code (e.g., *FC) AND IF CDMA is being used:

6-1-9-1-1 GOTO Pre-screening completed.

6-1-9-2 ELSEIF the MS dialed a locally allowed number (e.g., 9-1-1, *-9-1-1, N11, *N11):

6-1-9-2-1 Process the dialed number locally and route the call.

6-1-9-2-2 Exit this task.

6-1-9-3 ELSE:

6-1-9-3-1 Execute “Local Recovery Procedures” task (see Part 630, sec. 5.1).

6-1-9-3-2 Exit this task.

6-1-9-4 ENDIF.

6-1-10 ENDIF.

6-1-11 GOTO Pre-screening completed.

6-2 ENDIF.

7 ENDIF.

8 IF the MS is not registered OR IF the location of the MS has changed since the last registration:

8-1 Execute the “MSC Initiating MS Registration” task (see Part 640, sec. 57.1).

8-2 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

8-2-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

8-2-2 Exit this task.

8-3 ENDIF.

8-4 Send the MS the RoamingIndication parameter if received, in addition to other messages.

9 ELSEIF the MSC requires the MS’s service profile (e.g., per call authorization required or the service profile is not present):

9-1 Execute the “MSC Initiating Qualification Request” task (see Part 640, sec. 52.1).

9-2 IF the AnalogRedirectRecord parameter is received OR IF the CDMARedirectRecord parameter is received (MS is being redirected):

9-2-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

9-2-2 Exit this task.

9-3 ENDIF.

9-4 Send the MS the RoamingIndication parameter if received, in addition to other messages.

10 ENDIF.

Pre-screening completed:

11 Execute “Initialize the OneTimeFeatureIndicator Parameter” task (see Part 630, sec. 2.8).

12 IF a *pending registration* flag is set for the MS:

12-1 Clear the *pending registration* flag for the MS.

12-2 Execute the “MSC Analyze MS Dialed Number” task (see Part 630, sec. 2.3) to set the PointOfReturn and spawn the “MSC Initiating MS Registration” task (see Part 640, sec. 57.1) in parallel.

13 ELSE:

13-1 Execute the “MSC Analyze MS Dialed Number” task (see Part 630, sec. 2.3) to set the PointOfReturn.

14 ENDIF.

15 IF the PointOfReturn is *ToneTermination*:

15-1 Execute “Apply Access Denial Treatment” task (see Part 630, sec. 4.5).

15-2 Exit this task.

16 ENDIF.

17 IF the MS is not authorized:

17-1 IF the MS did not dial an OTASP Feature Code (*FC) AND IF CDMA is being used:

17-1-1 Execute “Apply Access Denial Treatment” task (see Part 630, sec. 4.5).

17-1-2 Exit this task.

17-2 ENDIF.

18 ENDIF.

19 Execute the “MSC PACA Call Origination Invocation” task (see Part 651, sec. 20.2).

20 IF unsuccessful:

20-1 Execute “Apply Access Denial Treatment” task (see Part 630, sec. 4.5).

20-2 Exit this task.

21 ELSE (seize the channel by):

21-1 Reserve the available voice or traffic channel.

21-2 Order the MS to acquire the reserved voice or traffic channel.

21-3 Verify the MS has properly tuned to this voice or traffic channel.

21-4 IF unsuccessful:

21-4-1 Execute “Apply Access Denial Treatment” task (see Part 630, sec. 4.5).

21-4-2 Exit this task.

21-5 ENDIF.

22 ENDIF.

23 Execute the “MSC MWN Call Origination Invocation” task (see Part 651, sec. 16.7).

24 IF the AnnouncementList parameter is received:

24-1 Execute the “Play All Announcements in the AnnouncementList” task (see Part 630, sec. 2.5).

25 IF the TerminationList parameter is received:

25-1 Execute the “MSC Routing Points Of Return” task (see Part 630, sec. 2.6).

26 ELSEIF the PointOfReturn is *PSTNTermination*:

26-1 Execute the “MSC Select a Route for the Call” task (see Part 630, sec. 3.9).

27 ELSEIF the the MS dialed an OTASP Feature Code (*FC) AND IF CDMA is being used:

27-1 Include the TRN.

27-2 Route the call to the Customer Service Center.

28 ELSE:

28-1 Execute “Apply Access Denial Treatment” task (see Part 630, sec. 4.5).

29 ENDIF.

30 Exit this task.

5.3 MSC Receives MEID of MS (new)

When the MSC receives a message (e.g., CDMA Status Response) that contains the MEID of an MS that is accessing the system, the MSC shall do the following:

1 IF a stored (i.e., previously validated) MEID value exists for this MS:

1-1 IF the received MEID and the stored MEID do not match:

1-1-1 Apply treatment that is appropriate for the system access (e.g., permit locally allowed calls but deny other calls).

1-2 ENDIF.

2 ENDIF.

3 Exit this task.

6 REGISTRATION NOTIFICATION

6.1 MSC Initiating MS Registration

When an MSC determines that a roaming Mobile Station (MS) is now within its service (through autonomous registration, call origination, call termination (e.g., a page response following a call to the roamer access number), or other mechanism, except for detection by a call handoff), or if instructed to do so for OTASP, this new Serving MSC shall start the registration notification process by doing the following:

1 Include the QualificationInformationCode parameter set according to the information needed from the VLR.

2 Include the SystemAccessType parameter set to the type of access performed by the MS (for e.g., Autonomous Registration, SMS Page Response, OTASP).

3 IF the MS enters a CDMA OTASP session (initiated by either the MS or the Serving MSC):

3-1 Include the SystemAccessType parameter set to *OTASP*.

4 ENDIF.

5 IF the access occurred in a border cell:

5-1 Include the BorderCellAccess parameter with a value of *Border cell access*.

5-2 The MSC should include the ReceivedSignalQuality parameter set to the signal strength of the received access.

5-3 The MSC should include the ControlChannelData parameter set to the Control Channel Identification information.

5-4 The MSC should include the SystemAccessData parameter set to the cell site information.

6 ENDIF.

7 IF the MSC is authentication capable:

7-1 Include the SystemCapabilities (SYSCAP) parameter set to indicate the authentication-related capabilities of this system.

8 ENDIF.

9 IF authentication parameters were requested (i.e., AUTH=1 in the Overhead Message Train), but were not received from the MS on the system access:

9-1 Include the ReportType (RPTTYP) parameter indicating *Missing authentication parameters*.

10 ENDIF.

11 Include the ElectronicSerialNumber parameter set to identify the MS.

12 IF MS support for MEID was indicated in the access message AND IF local policy requires MEID validation:

12-1 IF the MSC does not have the MEID of the MS:

12-1-1 Obtain the MEID of the MS (e.g., by means of the CDMA Status Request operation)[1].

12-1-2 IF the MEID_SIG ANDIF the MEID_ME were received from the MS:

12-1-2-1 Include the MEID_SIG parameter.

[1] If, by the time of expiration of a local timer, the MSC has not received a message containing the MEID of the MS, then the MSC sends the RegistrationNotification INVOKE without the MEID parameter.

12-1-2-2 Include the MEID_ME parameter.

12-1-2-3 IF authentication parameters were received from the MS on the system access (i.e., AUTH=1 in the Overhead Message Train):

12-1-2-3-1 Include the AUTHR parameter set to the Authentication Response received from the MS.

12-1-2-3-2 Include the RAND parameter set to the Random Variable used by the MS to compute the Authentication Response.

12-1-2-4 ELSE (Unique Challenge was used to request authentication parameter from the MS):

12-1-2-4-1 Include the AUTHU parameter set to the Authentication Response Unique Challenge received from the MS.

12-1-2-4-2 Include the RANDU parameter set to the Random Variable Unique Challenge used by the MS to compute the Authentication Response Unique Challenge.

12-1-2-5 ENDIF.

12-2 ENDIF.

12-3 Include the MEID parameter.

13 ENDIF.

14 Include the MSID parameter set to identify the MS.

15 Include the MSCID parameter set to the identity of the MSC.

16 Include the TransactionCapability parameter set to the current capabilities of the system.

17 IF the MSC supports WIN operations:

17-1 Include the WINCapability parameter to indicate current capabilities.

18 ENDIF.

19 IF the MSC is NDSS capable:

19-1 Include the ControlChannelMode (CCM) parameter set to indicate the operating mode of the MS.

19-2 Include the CDMANetworkIdentification (CDMANID) parameter set to identify the serving network.

19-3 Include the ServiceRedirectionCause parameter set to the reason of MS registration or access.

20 ENDIF.

21 Include the SystemMyTypeCode parameter set to the MSC's manufacturer.

22 Include the TerminalType (TERMTYP) parameter as declared by the MS.

23 IF the MSC is sending the message to an SS7 network:

23-1 Include the PC_SSN parameter with the Type set to *Serving MSC* and the PC and SSN fields set to the MSC's point code and subsystem number.

24 ENDIF.

25 IF the MSC is SMS capable:

25-1 Include the SMS_Address parameter set to be used to route SMS messages to the MS.

26 ELSEIF the MSC supports any other service (e.g., CDMA OTAPA) for which the current routing address of Serving MSC is needed:

26-1 Include the MSC_Address parameter set to a value that can be used to route SMDPP messages to the MSC.

27 ENDIF.

28 IF the MS is intentionally inaccessible for normal Call Delivery for periods of time (e.g., using a slotted mode, paging frame class, or sleep mode):

28-1 Include the AvailabilityType parameter set to AvailabilityType: *Unspecified mobile inactivity type*.

29 ENDIF.

30 Send a RegistrationNotification INVOKE to the MSC's associated VLR.

31 Start the Registration Notification Timer (RNT).

32 WAIT for a Registration Notification response:

33 WHEN a RETURN RESULT is received:

33-1 Stop timer (RNT).

33-2 IF the message can be processed:

33-2-1 IF the AnalogRedirectRecord or the CDMARedirectRecord parameter is received (i.e., the MS is being redirected):

33-2-1-1 Return to the invoking process.

33-2-2 ENDIF.

33-2-3 IF the message contained an AuthorizationDenied parameter:

33-2-3-1 IF the indicated MS is involved in a call or service operation anchored by this MSC:

33-2-3-1-1 The Serving System may optionally discontinue the call or service operation currently in progress.

33-2-3-2 ENDIF.

33-2-3-3 IF a record exists for the indicated MS:

33-2-3-3-1 Clear the subscriber's profile.

33-2-3-4 ENDIF.

33-2-4 ELSE:

33-2-4-1 Update the MS's service profile and qualification information with the received parameters.

33-2-4-2 IF the SMS_MessageWaitingIndicator parameter was received:

33-2-4-2-1 Set the *SMS Delivery Pending Flag* for this MS.

33-2-4-3 ENDIF.

33-2-4-4 Execute the "MSC MWN Status Change Invocation" task (see Part 651, sec. 16.9).

33-2-4-5 IF the indicated MS is involved in a call or service operation anchored by this MSC:

33-2-4-5-1 IF the service profile parameters do not authorize the current call or service operation:

33-2-4-5-1-1 The Serving System may optionally discontinue the call or service operation currently in progress.

33-2-4-5-2 ENDIF.

33-2-4-6 ENDIF.

33-2-4-7 IF the MEIDValidated parameter is received:

33-2-4-7-1 Store the MEID of the MS for use in validating subsequent system accesses by the MS.

33-2-4-8 ENDIF.

33-2-5 ENDIF.

33-3 ELSE (the message cannot be processed):

33-3-1 Execute the “Local Recovery Procedures” task (see Part 630, sec. 5.1).

33-4 ENDIF.

34 WHEN a RETURN ERROR OR REJECT is received:

34-1 Stop timer (RNT).

34-2 Execute the “Local Recovery Procedures” task (see Part 630, sec. 5.1).

35 WHEN timer (RNT) expires:

35-1 Execute the “Local Recovery Procedures” task (see Part 630, sec. 5.1).

36 ENDWAIT.

37 Exit this task.

6.2 HLR Receiving RegistrationNotification INVOKE

When an HLR receives a RegistrationNotification INVOKE, it shall perform the following:

1 IF the received message can be processed and the requested information can be made available for the indicated MS:

1-1 IF the received SystemAccessType parameter indicates *Autonomous registration*:[1]

1-1-1 IF this RegistrationNotification is part of a multiple access situation (based on internal algorithms and local operating procedures):

1-1-1-1 IF this is not the most desirable access:

1-1-1-1-1 Include the AuthorizationDenied parameter set to *Multiple Access*.

1-1-1-1-2 IF the measurement data is available:

1-1-1-1-2-1 Include the ReceivedSignalQuality, ControlChannelData and SystemAccessData parameters set according to values received with the best RegistrationNotification INVOKE received for this access.

1-1-1-1-3 ENDIF.

1-1-1-1-4 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-1-1-1-5 Send a RETURN RESULT to the requesting VLR.

1-1-1-1-6 Exit this task.

1-1-1-2 ENDIF.

1-1-2 ENDIF.

1-2 ENDIF.

1-3 If the MS identity is within the range of the HLR:

1-3-1 IF the MSC is NDSS capable, and the NDSS procedure has not been performed for the MS on this MSC and the NDSS feature is not suppressed for the MS:

1-3-1-1 IF the HLR determines there is a more preferable system for the MS and decides to select the system for NDSS redirection:

1-3-1-1-1 IF the selected system is a CDMA system:

1-3-1-1-1-1 Include the CDMARedirectRecord of the selected system:

1-3-1-1-2 ELSEIF the selected system is an analog system:

1-3-1-1-2-1 Include the AnalogRedirectRecord of the selected system:

1-3-1-1-3 ENDIF

1-3-1-1-4 Include the ServiceRedirectionInfo of the selected system if available.

1-3-1-1-5 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-3-1-1-6 Send a RETURN RESULT to the requesting VLR.

1-3-1-1-7 Exit this task.

1-3-1-2 ENDIF.

1-3-2 ENDIF.

1-4 ENDIF.

1-5 IF the MS is authorized for service on this MSC:

[1] The HLR may record the time at which the message was received as described in informative Part 691 Annex E.

1-5-1 IF the MEID parameter is received:
1-5-1-1 IF a Mobile Equipment Identifier (MEID) value is provisioned for this MS:
1-5-1-1-1 IF the received MEID and the provisioned MEID match:
1-5-1-1-1-1 Include the MEIDValidated parameter.
1-5-1-1-2 ELSEIF the MEID_ME AND the MEID_SIG parameters are received, AND IF the received MSID parameter value is expected to be paired with an authorized MEID_ME:
1-5-1-1-2-1 Compute the ME digital signature using the received authentication parameters (see *MEID Binding*).
1-5-1-1-2-2 IF the computed ME digital signature matches the received MEID_SIG parameter value:
1-5-1-1-2-2-1 Bind the received MSID to the received MEID_ME.
1-5-1-1-2-2-2 Include the MEIDValidated parameter.
1-5-1-1-2-3 ELSE:
1-5-1-1-2-3-1 Include the AuthorizationDenied parameter set to *Invalid serial number*.
1-5-1-1-2-3-2 IF applicable:
1-5-1-1-2-3-2-1 Include the DeniedAuthorizationPeriod parameter set appropriately.
1-5-1-1-2-3-3 ENDIF.
1-5-1-1-2-3-4 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.
1-5-1-1-2-3-5 Send a RETURN RESULT to the requesting VLR.
1-5-1-1-2-3-6 Exit this task.
1-5-1-1-2-4 ENDIF.
1-5-1-1-3 ELSE:
1-5-1-1-3-1 Include the AuthorizationDenied parameter set to *Invalid serial number*.
1-5-1-1-3-2 IF applicable:
1-5-1-1-3-2-1 Include the DeniedAuthorizationPeriod parameter set appropriately.
1-5-1-1-3-3 ENDIF.
1-5-1-1-3-4 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.
1-5-1-1-3-5 Send a RETURN RESULT to the requesting VLR.
1-5-1-1-3-6 Exit this task.
1-5-1-1-4 ENDIF.
1-5-1-2 ENDIF.
1-5-2 ENDIF.
1-5-3 IF the MS is registered with a different VLR:
1-5-3-1 IF the received SystemAccessType parameter indicates *Autonomous registration*:
1-5-3-1-1 IF the measurement data is available:
1-5-3-1-1-1 Include the ReceivedSignalQuality, ControlChannelData and SystemAccessData parameters according to the values received with the best RegistrationNotification INVOKE received for this access.

1-5-3-1-2 ENDIF.

1-5-3-2 ENDIF.

1-5-3-3 Execute the “HLR Initiating Registration Cancellation” task (see Part 640, sec. 56.1).

1-5-3-4 IF the CancellationDenied parameter is received:

1-5-3-4-1 IF the CancellationDenied parameter was set to *Multiple Access*.

1-5-3-4-1-1 Include the AuthorizationDenied parameter ~~to~~ set to *Multiple Access.*

1-5-3-4-1-2 IF the measurement data is available:

1-5-3-4-1-2-1 Relay the ReceivedSignalQuality, ControlChannelData, and SystemAccessData parameters.

1-5-3-4-1-3 ENDIF.

1-5-3-4-2 ELSEIF the CancellationDenied parameter is set to *Busy*:

1-5-3-4-2-1 Include the AuthorizationDenied parameter set to *Duplicate Unit.*

1-5-3-4-3 ENDIF.

1-5-3-4-4 Include the SystemMyTypeCode parameter set to the HLR’s manufacturer.

1-5-3-4-5 Send a RETURN RESULT to the requesting VLR.

1-5-3-4-6 Exit this task.

1-5-3-5 ELSE (no CancellationDenied parameter received):

1-5-3-5-1 Relay any received parameters, except the SMS_MessageWaitingIndicator parameter, from the RegistrationCancellation RETURN RESULT.

1-5-3-6 ENDIF.

1-5-4 ELSE:

1-5-4-1 IF an SMS_MessageWaitingIndicator parameter was received:

1-5-4-1-1 Set the *SMS Delivery Pending Flag* for this MS.

1-5-4-2 ENDIF.

1-5-5 ENDIF.

1-5-6 IF the TransactionCapability parameter was received:

1-5-6-1 Store the value of the TransactionCapability parameter for later use in the messaging on behalf of the subscriber.

1-5-7 ENDIF.

1-5-8 IF the QualificationInformationCode indicates *Profile only* or *Validation and profile:*

1-5-8-1 Execute the “Loading of Profile Parameters” task (see Part 630, sec. 1.3).

1-5-9 ENDIF.

1-5-10 IF the QualificationInformationCode indicates *Validation only* or *Validation and profile:*

1-5-10-1 Include the AuthorizationPeriod parameter set appropriately.

1-5-11 ENDIF.

1-5-12 IF an SMS_Address parameter is received with the RegistrationNotification INVOKE:

1-5-12-1 IF an AvailabilityType parameter is NOT received with the RegistrationNotification INVOKE:

1-5-12-1-1 IF SMS service is authorized for the MS on the current serving system:

1-5-12-1-1-1 IF the *SMS Delivery Pending Flag* is set for this MS:

1-5-12-1-1-1-1 Include the SMS_MessageWaitingIndicator parameter.

1-5-12-1-1-2 ENDIF.

1-5-12-1-2 ENDIF.

1-5-12-2 ENDIF.

1-5-13 ENDIF.

1-5-14 IF the registration pointer is cleared (i.e., there is no VLR identified as the VLR serving the MS).

1-5-14-1 Set the registration pointer to identify the VLR for which the RegistrationNotification INVOKE was received.

1-5-15 ENDIF.

1-6 ELSE (the MS is not authorized for service):

1-6-1 Include the AuthorizationDenied parameter set to the proper value (see the following table):

1-6-2 IF applicable:

1-6-2-1 Include the DeniedAuthorizationPeriod parameter set appropriately.

1-6-3 ENDIF.

1-7 ENDIF.

1-8 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-9 Send a RETURN RESULT to the requesting VLR.

1-10 IF the TransactionCapability for the current Serving MSC indicates that CDMA OTAPA Service is supported:

1-10-1 IF an AvailabilityType parameter was NOT received with the RegistrationNotification INVOKE:

1-10-1-1 IF the CDMA OTAPA Service is authorized for the MS on the current Serving MSC:

1-10-1-1-1 Set the status of CDMA OTAPA Service as *available*.

1-10-1-1-2 IF the SMS Address parameter has been received:

1-10-1-1-2-1 Set the temporary MSC routing address to the received SMS Address value.

1-10-1-1-3 ELSEIF the MSC Address parameter has been received:

1-10-1-1-3-1 Set the temporary MSC routing address to the received MSC Address value.

1-10-1-1-4 ENDIF.

1-10-1-1-5 IF the OTA *Delivery Pending Flag* is set for this MS and the OTAPA Service is *available*:

1-10-1-1-5-1 Retrieve the routing address of the OTAF stored with the OTA *Delivery Pending Flag* for the MS to use in routing an SMSNotification message toward the OTAF.

1-10-1-1-5-2 Clear the OTA *Delivery Pending Flag*.

1-10-1-1-5-3 Execute the "HLR inititating SMSNotification INVOKE" task.

1-10-1-1-6 ENDIF.

1-10-1-2 ELSE (Service is not authorized for the current system):

1-10-1-2-1 Set the CDMA OTAPA Service status to *unavailable*.

1-10-1-3 ENDIF.

1-10-2 ELSE (AvailabilityType parameter was received):

1-10-2-1 Set the CDMA OTAPA Service status to *unavailable*.

1-10-3 ENDIF.

1-11 ELSE (TransactionCapability indicates CDMA OTAPA Service not supported):

1-11-1 Set the CDMA OTAPA Service status to *unavailable*.

1-12 ENDIF.

1-13 IF an SMS_Address parameter was received in the RegistrationNotification INVOKE (this sequence is repeated only so that the SMSNotification is sent after the RegistrationNotification RETURN RESULT):

1-13-1 IF an AvailabilityType parameter was NOT received with the RegistrationNotification INVOKE:

1-13-1-1 IF SMS service is authorized for the MS on the current serving system:

1-13-1-1-1 Optionally set the temporary SMS routing address to the received SMS_Address.

1-13-1-1-2 IF the *SMS Delivery Pending Flag* is set for this MS:

1-13-1-1-2-1 Clear the *SMS Delivery Pending Flag*.

1-13-1-1-2-2 Execute the "HLR Initiating SMSNotification INVOKE" task (see Part 641, sec. 5.2).

1-13-1-1-3 ENDIF.

1-13-1-2 ELSE (SMS service is not authorized for the current system):

1-13-1-2-1 GOTO SMS Not Available.

1-13-1-3 ENDIF.

1-13-2 ELSE (AvailabilityType parameter was received:

1-13-2-1 GOTO SMS Not Available.

1-13-3 ENDIF.

1-14 ELSE (no SMS_Address parameter was received):

SMS Not Available:

1-14-1 Set the SMS status to *unavailable*.

1-14-2 Clear the temporary SMS routing address.

1-14-3 Optionally, IF the MC is to be informed of MS unavailability:

1-14-3-1 Include the SMS_AccessDeniedReason parameter set to *Unavailable*.

1-14-3-2 Execute the "HLR Initiating SMSNotification INVOKE" task (see Part 641, sec. 5.2).

1-14-4 ENDIF.

1-15 ENDIF.

1-16 IF an AvailabilityType parameter was received in the RegistrationNotification INVOKE:

1-16-1 Set the MS's state to *inactive*.

1-17 ELSE:

1-17-1 Set the MS's state to *active*.

1-18 ENDIF.

2 ELSE (the received message cannot be processed or the requested information cannot be made available for the indicated MS):

2-1 Send a RETURN ERROR with a proper Error Code value (see the following table) to the requesting VLR.

3 ENDIF.

4 Exit this task.

Table 6 HLR RegistrationNotification Response

Problem Detection and Recommended Response from HLR to VLR	
RETURN ERROR Error Code	**Problem Definition**
ID/HLRMismatch	The supplied MSID is not in the HLR's range of MSIDs or directory numbers (suspect routing error).
ResourceShortage	A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion).
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized. ***Note: It is recommended that an HLR supports RegistrationNotification transactions.***
ParameterError	A supplied parameter has an encoding problem (e.g., the supplied MSID parameter digit values do not meet the BCD specification). ***Note: Include the Parameter Identifier in question as the FaultyParameter parameter.***
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution.
UnrecognizedParameter-Value	A supplied parameter value is unrecognized or has nonstandard values. ***Note: Use default value, if specified, otherwise ignore the parameter.***
MissingParameter	An expected, or required, optional parameter was not received. ***Note: Include the Parameter Identifier in question as the FaultyParameter parameter.***
RETURN RESULT AuthorizationDenied	***Note: Only RETURN RESULT parameter values needing clarification have been included.***
Delinquent Account	The supplied MSID is within the range of the HLR, but the MSID is a delinquent account.
Invalid Serial Number	The supplied MSID is within the range of the HLR, but the supplied ElectronicSerialNumber or MEID parameter is not valid for the MSID's record.
Stolen Unit	The supplied MSID is within the range of the HLR, but the MSID is a stolen unit.
Duplicate Unit	The supplied MSID is within the range of the HLR, but the MSID is a duplicate unit.
Unassigned Directory Number	The supplied MSID is within the range of the HLR, but the MSID is not presently assigned to a subscriber.
Unspecified	The supplied MSID is within the range of the HLR, but the MSID is unspecified.
Multiple access	The supplied MSID is within the range of the HLR, but the MSID is a multiple access.

Not Authorized for the MSC	The supplied MSID is within the range of the HLR, but the MSID is not authorized for the MS
Missing authentication parameters	The supplied MSID is within the range of the HLR, but the MSID is missing authentication parameters.
TerminalType mismatch	The supplied MSID is within the range of the HLR, but the MSID is a terminal type mismatch.

7 CHECK MEID (NEW)

(New for X.S0004-640-E)

7.1 VLR Initiating a Check MEID

Note that support for these procedures in a given operator's network is optional.

When a VLR determines that an MEID shall be verified, it shall perform the following:

5 IF the MEID is not known:

5-1 Execute the "VLR Initiating a Status Request" task (see ~~5.2.1~~7.1) indicating that an MEID or MEID_ME information record is to be requested.

5-2 IF the MEID or MEID_ME is not returned:

5-2-1 Execute "Local Recovery Procedures" task (see X.S0004-~~TIA-41.~~630-E § 5.1).

5-2-2 Exit this task.

5-3 ENDIF.

6 ENDIF.

7 Send a CheckMEID INVOKE to the EIR.

8 Start the Check MEID Timer (CMT).

9 Wait for a Check MEID response:

10 WHEN a RETURN RESULT is received:

10-1 Stop the timer (CMT).

10-2 IF the MEIDStatus is *Normal* (same as GSM white listed):

10-2-1 Store the MEID with *Normal* status in the VLR.

10-3 ELSEIF the MEIDStatus is *Block* (same as GSM black listed):

10-3-1 Store the MEID with *Block* status in the VLR.

10-3-2 Optionally, use local procedures to indicate an illegal equipment status to the user (e.g., announcement or SMS).

10-3-3 IF the serving system will deny service from the MS that reported this MEID[1]:

10-3-3-1 Send a QualificationDirective INVOKE to the MSC, including the AuthorizationDenied and DeniedAuthorizationPeriod parameters (local procedures may allow voice originations to be routed to customer service).[2]

10-3-3-2 Send a MSInactive INVOKE to the HLR with DeregistrationType parameter set to indicate *Deregistration for an administrative reason.*

10-3-4 ENDIF.

10-4 ELSEIF the MEIDStatus is *No Entry*:

10-4-1 Store the MEID with *No Entry* status in the VLR.

---

1 Emergency calls will be exempt.

2 The VLR will suppress re-registrations for the MS for the DeniedAuthorizationPeriod or until the MS disassociates with this MEID.

10-4-2 Optionally, use local procedures to indicate an illegal equipment status to the user (e.g., announcement or SMS).

10-4-3 IF the serving system will deny service from the MS that reported this MEID[1]:

10-4-3-1 Send a QualificationDirective INVOKE to the MSC, including the AuthorizationDenied and DeniedAuthorizationPeriod parameters (local procedures may allow voice originations to be routed to customer service). Note that the VLR will suppress re-registrations for the MS for the DeniedAuthorizationPeriod or until the MS diassociates with this MEID.

10-4-3-2 Send a MSInactive INVOKE to the HLR with DeregistrationType parameter set to indicate *Deregistration for an administrative reason*.

10-4-4 ENDIF.

10-5 ELSEIF the MEIDStatus is *Track* (same as GSM grey listed):

10-5-1 Store the MEID with *Track* status in the VLR.

10-5-2 Optionally, record system accesses from any ME that reports this MEID.

10-6 ENDIF.

11 WHEN a RETURN ERROR or REJECT is received:

11-1 Stop the timer (CMT).

11-2 Execute “Local Recovery Procedures” task (see X.S0004-~~TIA-41.~~630-E § 5.1).

12 WHEN the timer (CMT) expires:

12-1 Execute “Local Recovery Procedures” task (see X.S0004-~~TIA-41.~~630-E § 5.1).

13 ENDWAIT.

14 Exit this task.

7.2 EIR Receiving a Check MEID Request

1 When an EIR receives a CheckMEID INVOKE, it shall perform the following:

2 If the received message can be processed:

2-1 Include the MEIDStatus parameter set appropriately:

2-2 Send a RETURN RESULT to the requesting network entity.

3 ELSE:

3-1 Send a RETURN ERROR with the proper error code value (see the following table).

4 ENDIF.

5 Exit this task.

[1] Emergency calls will be exempt.

Table 7 CheckMEID Response

Problem Detection and Recommended Response from EIR to VLR	
RETURN ERROR Error Code	**PROBLEM DEFINITION**
ResourceShortage	A required EIR resource (e.g., internal memory record) is temporarily not available (e.g., congestion).
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving EIR, or the requesting VLR is not authorized.
ParameterError	A supplied parameter has an encoding problem. ***Note: Include the Parameter Identifier in question as the FaultyParameter parameter.***
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution.

8 STATUS REQUEST (NEW)

(New for X.S0004-640-E)

8.1 VLR Initiating a Status Request

This task assumes that it is called by a higher function capable of acting upon returned MS information records appropriately. Upon request, the VLR shall do the following:

1 Send a StatusRequest INVOKE to the MSC.

2 Start the Status Request Timer (STRT).

3 Wait for a Status Request response:

4 WHEN a RETURN RESULT is received:

4-1 Stop the timer (STRT).

4-2 IF the requested MS information record is received:

4-2-1 Return to the calling task with the requested MS information record.

4-3 ELSE:

4-3-1 Return to the calling task with a failure indication.

4-4 ENDIF.

5 WHEN a RETURN ERROR or REJECT is received:

5-1 Stop the timer (STRT).

5-2 Return to the calling task with a *failure* indication.

6 WHEN the timer (STRT) expires:

6-1 Return to the calling task with a *failure* indication.

7 ENDWAIT.

8 Exit this task.

8.2 MSC Receiving a StatusRequest INVOKE

When an MSC receives a StatusRequest INVOKE, it shall perform the following:

1 IF the received message can be processed:

1-1 If the MS has been handed off:

1-1-1 Send an empty RETURN RESULT to the requesting network entity.

1-1-2 Exit this task.

1-2 ENDIF.

1-3 Send a CDMA Status Request message to the MS identified by the MSID, including the record type to be returned.

1-4 WAIT for a response from the MS:

1-5 WHEN a Status Response is received from the MS:

1-5-1 Include the received information record or records.

1-5-2 Send a RETURN RESULT to the requesting network entity.

1-6 WHEN an MS Reject order is received from the MS:

1-6-1 Send an empty RETURN RESULT to the requesting network entity.

1-7 WHEN no response is received from the MS:

1-7-1 Send an empty RETURN RESULT to the requesting network entity.

1-8 ENDWAIT.

2 ELSEIF the message cannot be processed:

2-1 Send a RETURN ERROR with the proper error code value (see the following table).

3 ENDIF.

4 Exit this task.

Table 8 StatusRequest Response

Problem Detection and Recommended Response from MSC to VLR	
RETURN ERROR Error Code	**PROBLEM DEFINITION**
UnrecognizedMIN	A Serving MSC record does not presently exist for the supplied MobileIdentificationNumber parameter
ResourceShortage	A required MSC resource (e.g., internal memory record, MSC is fully occupied) is temporarily not available (e.g., congestion).
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving MSC, or the requesting functional entity is not authorized.
ParameterError	A supplied parameter has an encoding problem. ***Note: Include the Parameter Identifier in question as the FaultyParameter parameter.***
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution.
UnrecognizedIMSI/TMSI	An MSC record does not presently exist for the supplied IMSI parameter.

9 OPERATION TIMER VALUES

(See X.S0004-690-E)

Table 9 Operation Timer Values (continued)

Timer	Default (sec.)	Started when	Normally stopped when	Action when timer expires
• • •	• • •	• • •	• • •	• • •
CMT Check MEID Timer	6	Check MEID INVOKE is sent.	Check MEID RETURN RESULT or RETURN ERROR is received.	Execute recovery procedures.
STRT Status Request Timer	10	Status Request-INVOKE is sent.	Status Request RETURN RESULT or RETURN ERROR is received.	Return a failure indication to the invoking task.
• • •	• • •	• • •	• • •	• • •

10 X.S0004-540-E OPERATION CHANGES FOR MEID

Only those operation parameter sets (INVOKE or RETURN RESULT) that contain the ElectronicSerialNumber parameter have been included in this section. The "Note" column specifies the text for the Note accompanying the MEID parameter. Operations with a note of "[Not Applicable]" will not have MEID added to their parameter list.

Messages Containing ESN		
Operation Name	**I(nvoke) or R(esult)**	**Note**
AnalyzedInformation	I	[Not Applicable]
AuthenticationDirective	I	Include if available AND if being transmitted for OTASP or OTAPA.
AuthenticationFailureReport	I	Include if available.
AuthenticationRequest	I	Include if available.
AuthenticationStatusReport	I	Include if available.
BaseStationChallenge	I	Include if available.
ChangeFacilities	I	[Not Applicable]
ChangeService	I	[Not Applicable]
CountRequest	I	Include if available.
FacilitiesDirective	I	[Not Applicable]
FacilitiesDirective2	I	Include if available.
FacilitySelectedAndAvailable	I	[Not Applicable]
FeatureRequest	I	Include if available when initiated by an MSC or VLR.
FlashRequest	I	[Not Applicable]
HandoffToThird	I	[Not Applicable]
HandoffToThird2	I	Include if available.
InformationDirective	I	[Not applicable].
InformationForward	I	Include if available.
InterSystemAnswer	I	[Not Applicable]
InterSystemPage	I	[Not Applicable]
InterSystemPage2	I	[Not Applicable]
InterSystemSetup	I	Include if available (existing note a)
LocationRequest	R	Include if available for recording purposes.
MSInactive	I	Include if available
OriginationRequest	I	Include if available when sent to the HLR or OTAF.
OTASPRequest	I	Include if available.
ParameterRequest	I	[Not Applicable]
	R	[Not Applicable]

Messages Containing ESN		
Operation Name	**I(nvoke) or R(esult)**	**Note**
QualificationDirective	I	[Not Applicable]
QualificationRequest	I	Include if known to identify the Mobile Equipment.
RedirectionDirective	I	[Not Applicable]
RedirectionRequest	I	[Not Applicable]
RegistrationCancellation	I	[Not Applicable]
RegistrationNotification	I	Include if known to identify the Mobile Equipment.
RoutingRequest	I	[Not Applicable]
	R	[Not Applicable]
SMSDeliveryBackward	I	[Not Applicable]
SMSDeliveryForward	I	[Not Applicable]
SMSDeliveryPointToPoint	I	Include if available for OTA or OTAPA.
	R	Include if available for OTA or OTAPA.
SMSNotification	I	Include if available.
SMSRequest	I	[Not Applicable]
	R	[Not Applicable]
TBusy	I	[Not Applicable]
TMSIDirective	I	[Not Applicable]
	R	Include if available.
TNoAnswer	I	[Not Applicable]
TransferToNumberRequest	I	Include if available when initiated by the Serving MSC.
UnsolicitedResponse	I	Include if available.

11 X.S0004-550-E PARAMETER CHANGES FOR MEID

Only those parameters that contain the ElectronicSerialNumber have been included in this section. The "Note" column specifies the text for the Note accompanying the MEID field. Parameters with a note of "[Not Applicable]" will not have MEID added as a sub-parameter.

Parameter Identifier Name	Note
AnnouncementCode	Add new code "Invalid MEID" (7).
AuthorizationDenied	Add new code point values "Blocked MEID" (12) and "Unknown MEID" (13).
CDMA2000HandoffInvokeIOSData	[Not applicable]
DenyAccess	Value 10, "MIN, IMSI or ESN authorization failure" should be changed to "MIN, IMSI, MEID or ESN authorization failure".
IntersystemTermination	Re-use note e for MEID. (Include for recording purposes).
LocalTermination	Include if available.
PSTNTermination	Re-use note c for MEID (Optional, for recording purposes).
ReportType	[Not Applicable] (This is a CAVE authentication parameter. There is no MEID equivalent to "MSID/ESN mismatch")
RequiredParametersMask	[Not Applicable]
SMS_CauseCode	"Address translation failure" value should be reworded to include mention of MEID for OTA as: The SMS Destination Address is invalid (e.g., address is not a recognized address type, address is not for a known or possible SMS functional entity, the MSID associated with a destination MS address does not correspond to its HLR, the ESN associated with a destination MS does not match the expected value, the SMS_DestinationAddress, SMS_OriginalDestinationAddress, destination MSID, or original destination subaddress does not match the address of a destination SME). For CDMA OTASP, the TRN, the Activation_MIN, the MEID or the ESN is currently not allocated to an OTASP call.

Annex A: Decimal Representation of MEID (Informative)

This annex is informative and is not part of this standard.

The MEID is a 14 digit hexadecimal value with the following format:

MEID													
Manufacturer Code								Serial Number					
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z
14	13	12	11	10	9	8	7	6	5	4	3	2	1

The decimal representation is calculated as follows[1]:

a. Separate the 14-digit hexadecimal MEID into two parts:

   Part 1: 8 digits representing the manufacturer code (digits RRXXXXXX in the figure).

   Part 2: 6 digits representing the serial number (digits ZZZZZZ in the figure).

b. Convert the hexadecimal value of each part into the decimal equivalent:

   Part 1: 10 decimal digits zero filled.

   Part 2: 8 decimal digits zero filled.

   If the decimal equivalent of each part is less than the number of required digits, right align and zero fill to create the required length.

c. Concatenate Part 1 and Part 2 to create an 18 digit decimal number.

Example:

Hex MEID = AF 01 23 45 0A BC DE

Part 1, manufacturer code is 0xAF012345 = 2936087365

Part 2, serial number is 0x0ABCDE = 00703710

Therefore, the decimal representation of the MEID is 29360 87365 0070 3710.

[1] If all digits are in the range 0-9 (i.e., the MEID is an IMEI for use with multi-mode phones), the 18-digit decimal format is not recommended.

Annex B: Check Digit Calculation (Informative)

This annex is informative and is not part of this standard.

A check digit (CD) may be calculated for use when an MEID is printed (e.g., on packaging or on the exterior of an MS). The check digit is not part of the MEID and is not transmitted when the MEID is transmitted.

There are three different methods of calculating the check digit:

- The check digit for an MEID containing all decimal digits (i.e., an IMEI – International Mobile Equipment Identity – assigned to a multi-mode phone) is calculated using the method described in [23.003].
- The check digit for an MEID containing at least one digit in the range 'A'–'F'[1] is calculated using a slight modification of the ISO/IEC 7812-1:2000(E) method used in [23.003] ('Luhn formula'). The modification is that all arithmetic is performed in base 16 instead of base 10. This preserves many of the desirable error detection properties of this formula. The result of the calculation is a single *hexadecimal* digit.
- The check digit for the decimal representation of an MEID uses the standard (decimal) 'Luhn formula' from ISO/IEC 7812-1:2000(E) performed on all 18 digits resulting in a single decimal digit.[2]

B.1 Example MEID Hexadecimal Check Digit Calculation

The format of the MEID with associated hexadecimal check digit is:

MEID														
Manufacturer Code								Serial Number						CD
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z	C
14	13	12	11	10	9	8	7	6	5	4	3	2	1	

This calculation is for AF 01 23 45 0A BC DE (an MEID containing one or more hexadecimal digits in the range 'A'–'F'). This follows the algorithm in ISO/IEC 7812-1:2000(E) with the exception that *all arithmetic is in base 16*:

- Step 1: "Double the value of alternate digits beginning with the first right-hand digit (low order)" converts (F, 1, 3, 5, A, C, E) to (1E, 2, 6, A, 14, 18, 1C).
- Step 2: "Add the individual digits comprising the products obtained in Step 1 to each of the unaffected digits in the original number" produces A + (1+E) + 0 + 2 + 2 + 6 + 4 + A + 0 + (1+4) + B + (1+8) + D + (1+C) = 64.
- Step 3: "Subtract the total obtained in Step 2 from the next higher number ending in 0. If the total obtained in Step 2 is a number ending in zero (30, 40, etc.), the check digit is 0." Therefore, the Check Digit for this example MEID including at least one hexadecimal digit is C (70-64).

[1] At the time of publication of this document, hexadecimal MEID assignments were limited to codes where the first digit is in the range 'A'–'F'. All other digits may have any hexadecimal value '0'–'9', 'A'–'F'.

[2] If all digits are in the range 0-9 (i.e., the MEID is an IMEI for use with multi-mode phones), the 18-digit decimal format is not recommended.

B.2 Example Decimal Representation Check Digit Calculation

The format of the decimal representation of the MEID, with associated decimal check digit is:

MEID																	
Manufacturer Code										Serial Number								CD
A	A	A	A	A	A	A	A	A	A	B	B	B	B	B	B	B	B	C
18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	

This calculation is for 29360 87365 0070 3710, the decimal representation of the MEID used in the previous example. This follows the algorithm in ISO/IEC 7812-1:2000(E) exactly (i.e., using decimal arithmetic:

- Step 1: “Double the value of alternate digits beginning with the first right-hand digit (low order)” converts (9,6,8,3,5,0,0,7,0) to (18,12,16,6,10,0,0,14,0).
- Step 2: “Add the individual digits comprising the products obtained in Step 1 to each of the unaffected digits in the original number” produces 2 + (1+8) + 3 + (1+2) + 0 + (1+6) + 7 + 6 + 6 + (1+0) + 0 + 0 + 7 + 0 + 3+ (1+4) + 1 + 0 = 60.
- Step 3: “Subtract the total obtained in Step 2 from the next higher number ending in 0. If the total obtained in Step 2 is a number ending in zero (30, 40, etc.), the check digit is 0.” Therefore, the Check Digit for this example decimal representation is 0.

Annex C: MEID, MEID_ME and SF_EUIMID (Informative)

The MEID (Mobile Equipment Identifier) is used to uniquely identify a wireless hardware unit, such as a mobile phone.

SF_EUIMID (Short Form Expanded UIM Identifier) is an identifier with the same format as MEID (14 digits/56 bits), and allocated from the same set of values, but with the purpose of uniquely identifying a card (R-UIM or CSIM) rather than a wireless hardware unit. The SF_EUIMID was designed so that it could be placed into an MEID protocol element when the card is configured to transmit the card identifier instead of the hardware identifier. Note that the alternative EUIMID format, LF_EUIMID, is longer, and therefore cannot fit within the MEID protocol element.

To distinguish between the MEID as a hardware identifier and the protocol element called MEID within 3GPP2 specifications, in some specifications, including this one, MEID_ME is used for the hardware identifier and “MEID” is used only as the protocol element name.