3GPP2 N.S0010-0

Version 1.0

Advanced Features in Wideband Spread Spectrum Systems

CONTENTS

LIST OF FIGURES v

LIST OF TABLES vii

FOREWORD ix

ASSUMPTIONS x

REVISION HISTORY x

1. INTRODUCTION 1
   - 1.1 Objective 1
   - 1.2 Scope 1
   - 1.3 Organization 1

2. REFERENCES 2

3. WIRELESS FEATURES DESCRIPTIONS 3
   - 3.1 Network Directed System Selection (NDSS) 3
     - 3.1.1 Normal Procedures With Successful Outcome 3
     - 3.1.2 Exception Procedures or Unsuccessful Outcome 4
     - 3.1.3 Alternative Procedures 5
     - 3.1.4 Interactions With Other Services 5

4. NETWORK SERVICE DESCRIPTIONS 9
   - 4.1 Subscriber Confidentiality (SC) 9

5. N.S0005-0 v 1.0 Chapter 1 "Functional Overview" Modifications 10
   - 5.1 Definitions 10
   - 5.2 Symbols and Abbreviations 11

6. N.S0005-0 v 1.0 Chapter 2 "Intersystem Handoff" Modifications 12
     - 4.2.1 Successful FacilitiesDirective2 12
     - 4.5.1 Successful HandoffBack2 15
     - 4.9.1 Successful HandoffToThird2 18

7. N.S0005-0 v 1.0 Chapter 3 "Automatic Roaming" Modifications 21

7.1 N.S0005-0 v 1.0 Chapter 3, Section 4 "Automatic Roaming Operations" Modifications 21
   - 4.4 AuthenticationRequest 21
     - 4.4.1 Successful Authentication on Initial Access 22
     - 4.4.A NDSS Procedure As a Result of AuthenticationRequest 25
   - 4.14 InterSystemPage 26
     - 4.14.1 Successful InterSystemPage: Border MSC Routing Information Returned 27
   - 4.15 InterSystemPage2 28
     - 4.15.1 Successful InterSystemPage2: MS Presence Confirmed in Border MSC 28
   - 4.A ParameterRequest 30

4.A.1 Successful ParameterRequest....30
4.A.2 Successful ParameterRequest....32
4.A.3 Unsuccessful ParameterRequest....33
4.A.4 Unsuccessful ParameterRequest....34
4.20 QualificationDirective....35
4.20.3 Successful QualificationDirective: Update Profile Only....36
4.21 QualificationRequest....37
4.21.1 Successful QualificationRequest: Authorization Confirmed....38
4.26 RegistrationNotification....40
4.26.1 Successful RegistrationNotification: Confirmed at the VLR....40
4.26.2 Successful RegistrationNotification: Confirmed at the HLR....43
4.B TMSIDirective....45
4.B.1 Successful TMSIDirective....45
4.B.2 Unsuccessful TMSIDirective....46
7.2 N.S0005-0 v 1.0 Chapter 3, Section 5 "Basic Automatic Roaming Scenarios" Modifications....48
5.A NDSS at Explicit Registration - Successful Scenarios....48
5.A.1 Initial Registration....49
5.A.2 Initial Registration with Authentication....51
5.B NDSS at Call Origination - Successful Scenarios....55
5.B.1 Call Origination without Authentication....55
5.B.2 Call Origination with Authentication....58
5.B.3 NDSS Call Origination without Profile....61
5.B.4 NDSS Feature Suppression....62
5.B.5 NDSS Feature Activation....63
5.C NDSS - Failure Operations....65
5.C.1 No Preferred System Found....65
5.C.2 Registration Rejection from the Directed System....65
5.C.3 Directed System with a Wrong SID/NID....65
5.D TMSI Registration....66
5.D.1 Normal Registration with TMSI_CODE....66
5.D.2 Normal Registration with Full TMSI....67
5.D.3 Normal Registration with Full TMSI (Unavailable at VLR)....69
5.D.4 Normal Registration with Full TMSI (Full-TMSI Timer expired)....71
5.D.5 Normal Registration with Full TMSI (Service Redirection)....73
5.E TMSIDirective....75
5.E.1 Successful TMSIDirective....75
5.E.2 Unsuccessful TMSIDirective with MS failed authentication....76
5.4 Authentication....78
5.4.A Normal Registration with Full TMSI (with Authentication)....78
5.4.A.1 Successful Scenario....79
5.4.A.2 Unsuccessful Scenario: New Serving VLR obtains incorrect MSID and ESN from the Old Serving VLR....82
5.4.A.3 Full TMSI Origination with Authentication....85
7.3 N.S0005-0 v 1.0 Chapter 3, Section 6 "Voice Feature Scenarios" Modifications....87
6.1 Call Delivery....87
6.1.A CD Invocation with Unsolicited Page Response with a Full TMSI....87

8. N.S0005-0 v 1.0 Chapter 5 "Signaling Protocols" Modifications 90
6.4 MAP OPERATIONS 92
6.4.1.2 Operation Specifiers 92
6.4.2 Operation Definitions 93
6.4.2.4 AuthenticationRequest 94
6.4.2.12 FacilitiesDirective2 98
6.4.2.17 HandoffBack2 100
6.4.2.21 HandoffToThird2 102
6.4.2.25 InterSystemPage 104
6.4.2.26 InterSystemPage2 107
6.4.2.e ParameterRequest 109
6.4.2.32 QualificationDirective 111
6.4.2.33 QualificationRequest 113
6.4.2.38 RegistrationNotification 115
6.4.2.f TMSIDirective 119
6.5 MAP PARAMETERS 120
6.5.1 General 120
6.5.1.1 Parameter Format 120
6.5.1.2 Parameter Identifiers 120
6.5.2 Parameter Definitions 123
6.5.2.30 CDMAChannelData 123
6.5.2.32 CDMACodeChannelInformation 125
6.5.2.37 CDMASearchWindow 125
6.5.2.160 TransactionCapability 126
6.5.2.bc AnalogRedirectInfo 128
6.5.2.bd AnalogRedirectRecord 130
6.5.2.be CDMAChannelNumber 130
6.5.2.bf CDMAChannelNumberList 131
6.5.2.bg CDMAPowerCombinedIndicator 131
6.5.2.bh CDMARedirectRecord 132
6.5.2.bi CDMASearchParameters 133
6.5.2.bk CDMANetworkIdentification 134
6.5.2.ac ControlChannelMode 134
6.5.2.bl NetworkTMSI 135
6.5.2.bm NetworkTMSIExpirationTime 136
6.5.2.bn NewNetworkTMSI 137
6.5.2.aw ReasonList 138
6.5.2.bo RequiredParametersMask 140
6.5.2.bp ServiceRedirectionCause 141
6.5.2.bq ServiceRedirectionInfo 142
6.5.2.br RoamingIndication 143

9. N.S0005-0 v 1.0 Chapter 6 "Signaling procedures" Modifications 144
3.1 Registration Call Tasks 144
3.1.1 Autonomous or Power-On Registration 144
3.2 Origination Call Tasks 145
3.2.1 Idle MS Origination 145

4.4 Authentication Request 147
4.4.1 MSC Initiating an Authentication Request INVOKE 147
4.4.2 VLR Receiving AuthenticationRequest INVOKE 149
4.4.3 HLR Receiving AuthenticationRequest INVOKE 157
4.32 Qualification Directive 161
4.32.1 HLR Initiating a Qualification Directive INVOKE 161
4.32.3 VLR Initiating a Qualification Directive INVOKE 162
4.32.4 MSC Receiving QualificationDirective INVOKE 163
4.33 Qualification Request 166
4.33.1 MSC Initiating a QualificationRequest INVOKE 166
4.33.4 HLR Receiving QualificationRequest INVOKE 167
4.38 Registration Notification 171
4.38.1 MSC Initiating MS Registration INVOKE 171
4.38.3 HLR Receiving RegistrationNotification INVOKE 173
4.E Parameter Request 179
4.E.1 Serving MSC Initiation of a ParameterRequest INVOKE 179
4.E.2 Serving VLR Receiving ParameterRequest INVOKE 179
4.E.3 New Serving VLR Initiation of a ParametersRequest 181
4.E.4 Old Serving VLR Receiving ParameterRequest INVOKE 181
4.F TMSI DIRECTIVE 183
4.F.1 Serving VLR Initiation of a TMSI Directive INVOKE 183
4.F.2 MSC Receiving TMSI Directive INVOKE 184
7 Operation Timer values 187

ANNEX A Information Stored in Databases 188
1. Basic assumption 188

LIST OF FIGURES

Figure 4 Successful FacilitiesDirective2 12
Figure 9 Successful HandoffBack2 15
Figure 15 Successful HandoffToThird2 18
Figure 9 Successful Authentication on Initial Access 22
Figure 4.4.A-1 NDSS Procedure as a Result of AuthenticationRequest 25
Figure 29 Successful InterSystemPage: Border MSC Routing Information Returned 27
Figure 32 Successful InterSystemPage2: MS Presence Confirmed in Border MSC 28
Figure 4.A.1-1 Successful ParameterRequest 30
Figure 4.A.2-1 Successful ParameterRequest 32
Figure 4.A.3-1 Unsuccessful ParameterRequest 33
Figure 4.A.4-1 Unsuccessful ParameterRequest 34
Figure 49 Successful QualificationDirective: Update Profile Only 36
Figure 51 Successful QualificationRequest: Authorization Confirmed 38
Figure 64 Successful RegistrationNotification: Confirmed at the VLR 40
Figure 65 Successful RegistrationNotification: Confirmed at the HLR 43
Figure 4.B.1-1 Successful TMSIDirective 45
Figure 4.B.2-1 Unsuccessful TMSIDirective 46
Figure 5.A.1-1 Initial Registration 49
Figure 5.A.2-1 Initial Registration with Authentication 52
Figure 5.B.1-1 Call Origination without Authentication 56
Figure 5.B.2-1 Call Origination with Authentication 58
Figure 5.B.3-1 NDSS Call Origination without Profile 61
Figure 5.B.4-1 NDSS Feature Suppression 62
Figure 5.B.5-1 NDSS Feature Activation 63
Figure 5.D.1-1 Normal Registration with TMSI_CODE 66
Figure 5.D.2-1 Normal Registration with Full TMSI 67
Figure 5.D.3-1 Normal Registration with Full TMSI (Unavailable at VLR) 69
Figure 5.D.4-1 Normal Registration with Full TMSI (Full-TMSI Timer expired) 71
Figure 5.D.5-1 Normal Registration with Full TMSI (Service Redirection) 73
Figure 5.E.1-1 SuccessfulTMSIDirective 75
Figure 5.E.2-1 Unsuccessful TMSIDirective 76
Figure 5.4.A.1-1 Successful Scenario 79
Figure 5.4.A.2-1 Unsuccessful Scenario 83
Figure 5.4.A.3-1 Full TMSI Origination with Authentication 85
Figure 6.1.A-1 CD Invocation with Unsolicited Page Response with Full TMSI 88
Figure 37 CDMAChannelData parameter 124
Figure 39 CDMACodeChannelInformation parameter 125
Figure 44 CDMASearchWindow parameter 125

Figure 177 TransactionCapability parameter....126
Figure 6.5.2.bc-1 AnalogRedirectInfo parameter....128
Figure 6.5.2.bd-1 AnalogRedirectRecord parameter....130
Figure 6.5.2.be-1 CDMAChannelNumber parameter....130
Figure 6.5.2.bf-1 CDMAChannelNumberList parameter....131
Figure 6.5.2.bg-1 CDMAPowerCombinedIndicator parameter....131
Figure 6.5.2.bh-1 CDMARedirectRecord parameter....132
Figure 6.5.2.bi-1 CDMASearchParameters parameter....133
Figure 6.5.2.ac-1 ControlChannelMode parameter....134
Figure 6.5.2.bk-1 CDMANetworkIdentification parameter....134
Figure 6.5.2.bl-3 NetworkTMSI parameter....135
Figure 6.5.2.bm-1 NetworkTMSIExpirationTime parameter....136
Figure 6.5.2.bn-1 NewNetworkTMSI parameter....137
Figure 6.5.2.aw-1 ReasonList parameter....138
Figure 6.5.2.bo-1 RequiredParametersMask parameter....140
Figure 6.5.2.bp-1 ServiceRedirectionCause parameter....141
Figure 6.5.2.bq-1 ServiceRedirectionInfo parameter....142
Figure 6.5.2.br-1 RoamingIndication parameter....143

LIST OF TABLES

Table 5 FE Combinations for AUTHREQ 21
Table 15 FE Combinations for ISPAGE 26
Table 16 FE Combinations for ISPAGE2 28
Table 4.A-1 FE Combinations for PARMREQ 30
Table 21 FE Combinations for QUALDIR 35
Table 22 FE Combinations for QUALREQ 37
Table 27 FE Combinations for REGNOT 40
Table 4.B-1 FE Combinations for TMSIDIR 45
Table 6 Error Codes 91
Table 8 N.S0005-0 v 1.0 MAP Operation Specifiers 92
Table 10 Summary of MAP Operations 93
Table 17 AuthenticationRequest INVOKE Parameters 94
Table 18 AuthenticationRequest RETURN RESULT Parameters 96
Table 34 FacilitiesDirective2 RETURN RESULT Parameters 98
Table 44 HandoffBack2 RETURN RESULT Parameters 100
Table 52 HandoffToThird2 RETURN RESULT Parameters 102
Table 59 InterSystemPage INVOKE Parameters 105
Table 61 InterSystemPage2 INVOKE Parameters 107
Table 6.4.2.e-1 ParameterRequest INVOKE Parameters 109
Table 6.4.2.e-2 ParameterRequest RETURN RESULT Parameters 110
Table 72 QualificationDirective INVOKE Parameters 111
Table 74 QualificationRequest INVOKE Parameters 113
Table 75 QualificationRequest RETURN RESULT Parameters 114
Table 84 RegistrationNotification INVOKE Parameters 115
Table 85 RegistrationNotification RETURN RESULT Parameters 117
Table 6.4.2.f-1 TMSIDirective INVOKE Parameters 119
Table 6.4.2.f-2 TMSIDirective RETURN RESULT Parameters 119
Table 112 N.S0005-0 v 1.0 MAP Parameter Identifiers 120
Table 37 CDMAChannelData value 124
Table 192 TransactionCapability value 126
Table 6.5.2.bc-1 AnalogRedirectInfo value 129
Table 6.5.2.ac-1 ControlChannelMode value 135
Table 6.5.2.bl-1 NetworkTMSI value 136
Table 6.5.2.aw-1 Reason List value 139
Table 6.5.2.bo-1 RequiredParametersMask value 140
Table 6.5.2.bp-1 ServiceRedirectionCause value 141
Table 6.5.2.bq-1 ServiceRedirectionInfo value 142
Table 8 VLR AuthenticationRequest Response 156

Table 9 HLR AuthenticationRequest Response 159
Table 43 MSC QualificationDirective Response 164
Table 45 HLR QualificationRequest Response 169
Table 52 HLR RegistrationNotification Response 177
Table 4.E.2-1 Serving VLR ParametersRequest Response 180
Table 4.E.4-1 Old Serving VLR ParametersRequest Response 182
Table 4.F.2-1 MSC TMSI Directive Response 186
Table 63 Operation Timer Values 187
Table A-1: Overview of information stored in IS-41 Functional Entities 189

FOREWORD

This Standard contains modifications and additions to *ANSI/N.S0005-0 v 1.0* and *ANSI/TIA/EIA-664* that are required to support advanced features for CDMA. For this revision of this Standard, these features include: Network Directed System Selection (NDSS), and Subscriber Confidentiality (SC) supported by Temporary Mobile Station Identity (TMSI).

The *N.S0005-0 v 1.0* recommendation upon which this Standard builds are:

- *ANSI/N.S0005-0 v 1.0 Cellular Radiotelecommunications Intersystem Operations, 1997*.

ASSUMPTIONS

This Standard assumes that:

1. MSs are identified by MobileStationIdentity (MSID) as defined in *N.S0005-0 v 1.0 Modifications to Support IMSI* which may contain the MobileIdentificationNumber (MIN), or InternationalMobileStationIdentity (IMSI).
2. This Standard is backward compatible with *TSB76* and is built upon the functionality supported in *TSB76*.
3. This Standard is backward compatible with *IS-737* and is built upon the functionality supported in *IS-737*.
4. The IMSI associated with an MS's TMSI should be stored at the MSC for future paging of the MS. The MS should be paged with a valid TMSI (e.g., an invalid TMSI is one which is erroneously assigned to multiple MSs causing authentication to fail).
5. The network supports full TMSI (i.e., TMSI_CODE and TMSI_ZONE) referred to as a NetworkTMSI. If the MS registers with a TMSI_CODE, the TMSI_ZONE is added to create a full TMSI (i.e., NetworkTMSI) before it is sent across the network.

REVISION HISTORY

Revision	Date	Remarks
0	January 1998	Initial Publication

1. INTRODUCTION

1.1 Objective

This Standard contains modifications and additions to *N.S0005-0 v 1.0* and *TIA/EIA-664* that are required to support advanced features for CDMA.

1.2 Scope

For this revision of this Standard, the advanced CDMA features include: Network Directed System Selection (NDSS) and Subscriber Confidentiality (SC) supported by TMSI.

1.3 Organization

This document is organized as per *TIA/EIA-664* and *N.S0005-0 v 1.0*.

2. REFERENCES

N.S0005-0 v 1.0 Chapter 1, page 2 line 48: TIA/EIA:

[*IS-41-C*] *TIA/EIA-IS41-C Cellular Radiotelecommunications Intersystem Operations, January 1996.*

[*ANSI-41*] *ANSI/N.S0005-0 v 1.0 Cellular Radiotelecommunications Intersystem Operations, 1998.*

[*ANSI-664*] *ANSI/TIA/EIA-664 Cellular Features Description June 1996.*

[*IMSI*] *N.S0005-0 v 1.0 Modifications to Support IMSI, approved for publishing.*

[*IS-737*] *TIA/EIA/IS-737 IS-41-C Enhancements for Circuit Mode Services, approved for publishing.*

[*TSB29*] *TSB29 B International Implementation of Wireless Telecommunications Systems Compliant with N.S0005-0 v 1.0, July 1997.*

[*TSB76*] *TSB76 PCS Multi-band Support, September 1996.*

N.S0005-0 v 1.0 Chapter 1, page 3 line 15: CDMA:

[*IS-95-A*] *TIA/EIA/IS-95-A Mobile Station – Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*; Telecommunications Industry Association; May 1995.

[*J-STD-008*] *ANSI J-STD-008 Personal Station-Base Station Compatibility Requirements for 1.8 to 2.0 GHz Code Division Multiple Access (CDMA) Personal Communications Systems, approved for publishing.*

[*TSB58*] *TSB58 Administration of Parameter Value Assignments for TIA/EIA Wideband Spread Spectrum Standards, December 1995.*

[*TSB64*] *TSB64 IS-41-B Support for Dual-Mode Wideband Spread Spectrum Systems, December 1993.*

[*TSB74*] *TSB74 Support for 14.4 kbps Data Rate and PCS Interaction for Wideband Spread Spectrum Cellular Systems, December 1995.*

N.S0005-0 v 1.0 Chapter 1, page 3 line 46: TDMA:

[*IS-136.1*] *TIA/EIA IS-136.1-A TDMA Cellular/PCS - Radio Interface - Mobile Station - Base Station Compatibility - Digital Control Channel, Rev. A, October 1996.*

[*IS-136.2*] *TIA/EIA IS-136.2-A TDMA Cellular/PCS - Radio Interface - Mobile Station - Base Station Compatibility - Traffic Channels and FSK Control Channel, Rev. A, October 1996.*

3. WIRELESS FEATURES DESCRIPTIONS

This section provides Stage 1 Feature Descriptions (according to the structure in *TIA/EIA-664*) for the Features supported by this Standard.

3.1 Network Directed System Selection (NDSS)

The Network Directed System Selection (NDSS) feature is a network capability that provides a network based mechanism for a service provider, based on various customer and service provider specified criteria, to automatically direct a subscriber's Mobile Station (MS) to a desired serving system. The serving system could be any system available to the MS, regardless of frequency band (cellular A/B or PCS bands A/B/C/D/E/F) or technology (analog or digital).

NDSS consists of procedures that allow wireless subscribers to register upon a preferred system while they are roaming (i.e., outside of their home system) without manual intervention by the subscriber. NDSS allows an MS to automatically register with a preferred serving system or to be automatically directed by their home system to a suggested system based on bilateral agreements between the serving system and home system. When an MS registers on a visited system, the network may direct the MS from that system to another system. The network may provide information which controls the status of the Enhanced Roaming Indicator in the MS. NDSS may override system selection procedures in the MS. The subscriber should have the ability, however, to suppress NDSS, and use the MS's system selection procedure. The status of NDSS (i.e., Active, Suppressed) is maintained in the home system, and may be changed upon request by the subscriber.

Applicability to Telecommunications Services

NDSS is applicable to all telecommunications services.

3.1.1 Normal Procedures With Successful Outcome

Authorization

NDSS may be made generally available for all subscribers by their service provider.

De-Authorization

NDSS may be withdrawn by the service provider.

Registration

NDSS has no registration.

De-Registration

NDSS has no de-registration.

Activation

NDSS is activated upon authorization.

De-Activation

NDSS is de-activated upon de-authorization.

Invocation

NDSS is invoked by the home system upon receipt of a registration message.

Normal Operation With Successful Outcome

This section describes a typical sequence of procedures for a subscriber, whose home and serving systems offer NDSS, which results in a successful outcome.

a. The MS may scan a list of preferred systems. If no preferred systems are found, the MS registers with any available system, provided the system is not on the MS's negative system list. A negative system list is defined as a short list of unacceptable system identifications that is stored in the memory of an MS. These procedures are utilized for all contexts for which registration may occur.

b. The serving system requests authorization from the subscriber's home system.

c. The home system determines whether another system is preferable to the current serving system.

d. If the home system determines that another system is preferable, and the subscriber has not suppressed NDSS, it may return information to the serving system requesting it to redirect the MS to a different system. If the redirection attempt is unsuccessful, the current serving system, while not preferred, is always assumed to be acceptable.

e. If redirection has been requested by the home system, the NDSS capable serving system shall redirect the MS to the preferred system.

f. The MS receives the redirection message and attempts registration with the new system.

3.1.2 Exception Procedures or Unsuccessful Outcome

This section lists some of the more probable abnormal situations not described in Normal Procedures With Successful Outcome.

Registration

None identified.

De-Registration

None identified.

Activation

NDSS is considered activated when suppression of NDSS is turned off in the home system. NDSS may be activated by an authorized subscriber specifying the NDSS activation feature code as in:

* FC + SEND .

De-Activation

NDSS is considered de-activated when the suppression of NDSS is turned on in the home system. The MS then reverts to its internal system selection procedure which was used upon initial system access.

NDSS may be de-activated by an authorized subscriber specifying the NDSS de-activation suppression feature code as in:

* FC + SEND .

Invocation

If, for some reason, the MS cannot complete service redirection (e.g., registration rejection, invalid system identification, no system found, etc.), it re-attempts to register with the original visited system and indicates the failure condition.

Exceptions While Roaming

None identified.

Exceptions During Intersystem Hand-off

None identified.

3.1.3 Alternative Procedures

None identified.

3.1.4 Interactions With Other Services

Asynchronous Data Service (ADS)

None identified.

Call Delivery (CD)

None identified.

Call Forwarding—Busy (CFB)

None identified.

Call Forwarding—Default (CFD)

None identified.

Call Forwarding—No Answer (CFNA)

None identified.

Call Forwarding—Unconditional (CFU)

None identified.

Call Transfer (CT)

None identified.

Call Waiting (CW)

None identified.

Calling Name Presentation (CNAP)

None identified.

Calling Name Presentation Restriction (CNAR)

None identified.

Calling Number Identification Presentation (CNIP)

None identified.

Calling Number Identification Restriction (CNIR)

None identified.

Conference Calling (CC)

None identified.

Data Privacy (DP)

None identified.

Do Not Disturb (DND)

None identified.

Emergency Services (9-1-1)

Emergency calls are not subject to NDSS.

Flexible Alerting (FA)

None identified.

Group 3 Facsimile (G3 Fax)

None identified.

Incoming Call Screening (ICS)

None identified.

Message Waiting Notification (MWN)

None identified.

Mobile Access Hunting (MAH)

None identified.

Network Directed System Selection (NDSS)

Not applicable.

Non-Public Mode Service (NP)

None identified.

Over-the-Air Service Provisioning (OTASP)

OTASP calls are not subject to NDSS.

Password Call Acceptance (PCA)

None identified.

Preferred Language (PL)

None identified.

Priority Access and Channel Assignment (PACA)

None identified.

Remote Feature Control (RFC)

None identified.

Selective Call Acceptance (SCA)

None identified.

Service Negotiation (SN)

None identified.

Subscriber PIN Access (SPINA)

None identified.

Subscriber PIN Intercept (SPINI)

None identified.

Subscriber Confidentiality (SC)

None identified.

Three-Way Calling (3WC)

None identified.

User Group ID (UGID)

None identified.

Voice Controlled Services (VCS)

None identified.

Voice Message Retrieval (VMR)

None identified.

Voice Privacy (VP)

None identified.

Voice-based User Identification (VUI)

None identified.

4. NETWORK SERVICE DESCRIPTIONS

This section describes services used by the wireless system and network operators. Subscribers may or may not be directly aware of the use of services that are independent of subscriber involvement.

4.1 Subscriber Confidentiality (SC)

Subscriber Confidentiality (SC) allows the wireless system to assign an MS a Temporary Mobile Station Identity (TMSI) to be used in subsequent communications with the MS. The TMSI should not have an externally visible association with the MS's permanent identity (MIN or IMSI). SC conceals the MS's permanent identity on the air interface and thereby protects the subscriber from fraudulent use of the MS's permanent identity.

The wireless system should periodically reassign the TMSI. This further reduces the possibility of associating the TMSI with the subscriber's permanent identity. The TMSI should be reassigned in a manner that does not reveal the MS's permanent identity.

When an MS with a previously assigned TMSI roams into a new system that is SC capable, the MS may not send its permanent identity over the air interface to the new system. It may send its TMSI only. The new system should uniquely identify the MS using this TMSI to obtain the MS's permanent identity and subscriber information through intersystem transactions. On the other hand, if an MS's TMSI is re-established in each new system, intersystem transactions will not be needed.

The wireless serving system shall provide system integrity when assigning TMSIs such that each assigned TMSI uniquely identifies a single subscriber within that wireless serving system. If the wireless system is not able to support SC, the wireless system shall allow the MS to operate with the permanent identity even though a TMSI was previously assigned in another system.

5. *N.S0005-0 v 1.0* Chapter 1 "Functional Overview" Modifications

5.1 Definitions

(*N.S0005-0 v 1.0* Chapter 1, page 6)

Full TMSI

The combination of TMSI zone and TMSI code. It is a globally unique address for the MS.

Full TMSI Timer

The full-TMSI timer is used to automatically deassign the assigned TMSI when the MS roams into a different TMSI zone. The MS starts the full-TMSI timer whenever it first accesses the system in a new TMSI zone. If the timer expires before a new TMSI is assigned, the MS deletes the TMSI and registers again using the IMSI.

Network Identification (NID)

A number that uniquely identifies a network within a wireless system.

Mobile Station Identity (MSID)

The identification for a MS, which may be the MIN, or IMSI.

Negative List

A short list of unacceptable system identifications that is stored in the memory of the MS.

NetworkTMSI

The full TMSI transported over the N.S0005-0 v 1.0 network. The NetworkTMSI is mapped to the subscriber's MIN or IMSI at either the Serving VLR, or the prior Serving VLR.

Temporary Mobile Station Identity (TMSI)

An identification number assigned to an MS on a temporary basis by a serving system (e.g., MSC or VLR.)

TMSI Code

A temporarily assigned MS identification of length up to 32-bits within a TMSI Zone. A TMSI with only a TMSI Code will not provide a globally unique address for an MS.

TMSI Expiration Time

The TMSI expiration time is used to automatically deassign the assigned TMSI. It allows a TMSI to be reassigned periodically and prevents an MS from "holding" a TMSI during extended periods of inactivity. It also helps protect against inadvertent VLR faults which would result in duplicate TMSI assignments. The MS obtains the expiration time value in the message which assigns the TMSI. If the expiration time has passed, the MS deletes the TMSI and uses the IMSI as its identification.

TMSI Zone

The administrative area that allows the TMSI Code to be reused. The TMSI Code is unique only within a TMSI Zone and may be reused in a different TMSI Zone. A TMSI consisting of both the TMSI Zone and TMSI Code, however, provides a globally unique address of an MS.

5.2 Symbols and Abbreviations (*N.S0005-0 v 1.0* Chapter 1, pages 14 through 22)

ADS	Asynchronous Data Service
CNAP	Calling Name Presentation
DP	Data Privacy
EIA	Electronic Industry Association
FAX	Facsimile
ICS	Incoming Call Screening
IMSI	International Mobile Station Identity
ISLP	Intersystem Link Protocol
MSID	Mobile Station Identity
NDSS	Network Directed System Selection
NID	Network Identity
NP	Non-Public Service
OTASP	Over-the-Air Service Provisioning
PCS	Personal Communication Service
SC	Subscriber Confidentiality
SN	Service Negotiation
TIA	Telecommunications Industry Association
TMSI	Temporary Mobile Station Identity
UG	User Group
UGID	User Group ID
VCS	Voice Controlled Services
VUI	Voice-based User Identification

6. *N.S0005-0 v 1.0* Chapter 2 "Intersystem Handoff" Modifications

The following sections refer to *N.S0005-0 v 1.0* Chapter 2.

4.2.1. Successful FacilitiesDirective2 (*N.S0005-0 v 1.0* Chapter 2, page 13)

This scenario describes the successful use of the FacilitiesDirective2 operation.

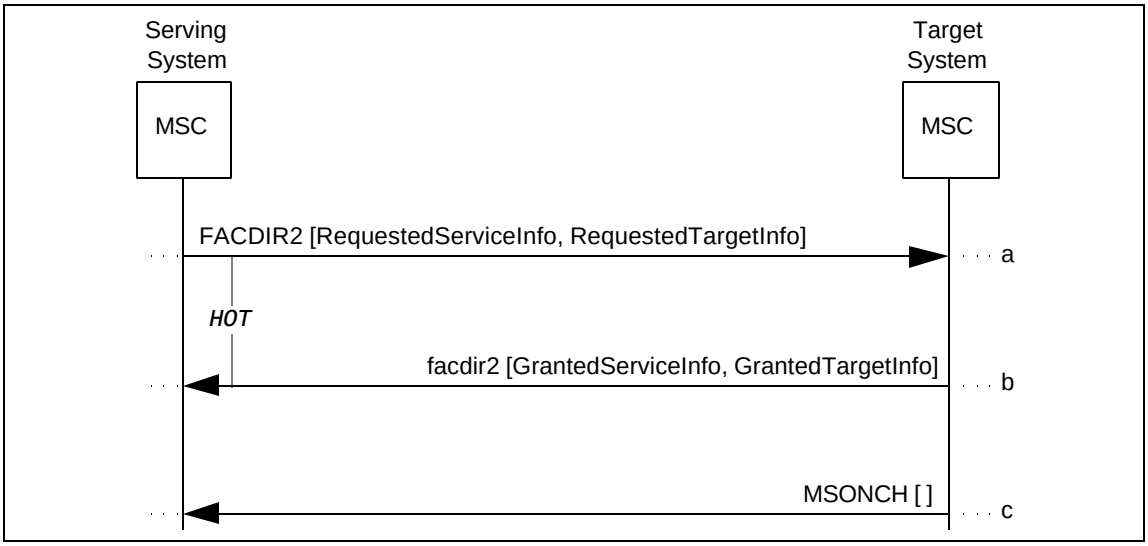

Figure 4 Successful FacilitiesDirective2

a. The Serving MSC determines that a call should be handed off to a target system. It sends a `FACDIR2` to the Target MSC, directing the Target MSC to initiate a Handoff-Forward task.

Parameters	Usage	Type
RequestedServiceInfo:	Set of parameters for Requested Service Information	
[CDMACallMode]	Indicates the acceptable mode of the current call = {AMPS | NAMPS | CDMA}.	O
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the serving channel, if CDMA.	O
[CDMAStationClass-Mark][1]	Identifies certain characteristics of a dual-mode CDMA MS.	O
[CDMAStationClass-Mark2][2]	Identifies certain characteristics of a CDMA MS (e.g., dual-band, dual-mode).	O
...		
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the serving channel, if TDMA.	O

...

b. If a voice channel on the designated target cell is available, the Target MSC increases the Segment Counter in the received BillingID parameter by one and uses the new BillingID for the new call segment. It then returns a `facdir2` to the requesting MSC, and initiates a Handoff-Forward task.

[1] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMAStationClassMark is used.

[2] For [*TSB76*] and later, CDMAStationClassMark2 is used.

Parameters	Usage	Type
GrantedServiceInfo:	Set of parameters for Granted Service Information.	
[CDMACodeChannel-List]	Identifies the code channels in a Forward CDMA Channel used for the call. Included if target channel is CDMA.	O
[CDMASearchPara-meters][1]	Specifies search information (SearchWindow, T_ADD, T_DROP, T_COMP, T_TDROP) that a CDMA MS should use to search for pilots. Included if target channel is CDMA.	O
[CDMASearchWindow][2]	Specifies the number of PN chips that a CDMA MS should use to search for usable multipath components of the pilots in the Active Set and the Candidate Set. Included if target channel is CDMA.	O
[ConfidentialityModes]	Identifies the status of Signaling Message Encryption and Voice Privacy features for the MS actually used for call. Included if the TerminalType value is '2' or greater.	O
[TDMABurstIndicator]	Indicates whether or not the MS is required to transmit shortened burst (as defined in *TDMA*) after handoff. Included if a TDMA channel is in use.	O
GrantedTargetInfo:	Set of parameters for Target Service Information.	
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the target channel, if CDMA.	O
[ChannelData]	Indicates the SAT Color Code, Voice Mobile Attenuation Code, and the channel number of the target channel, if analog.	O
[NAMPSChannelData]	Indicates the Digital SAT Color Code and the narrow voice channel assignment associated with the target analog channel, if NAMPS.	O
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the target channel, if TDMA.	O
[TargetCellID]	Specifies the ID of the actual target cell site selected (AMPS, NAMPS, TDMA).	O

[1] For this Standard and later, CDMASearchParameters is used.

[2] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMASearchWindow is used.

c. After having initiated the Handoff-Forward task, if the MS is received on the designated voice channel, the Target MSC completes the voice path between the voice channel and the inter-MSC trunk and then sends a MSONCH to the initiator of the Handoff-Forward task (the Serving MSC in this scenario).

4.5.1. Successful HandoffBack2

(*N.S0005-0 v 1.0* Chapter 2, page 20)

This scenario describes the successful use of the HandoffBack2 operation.

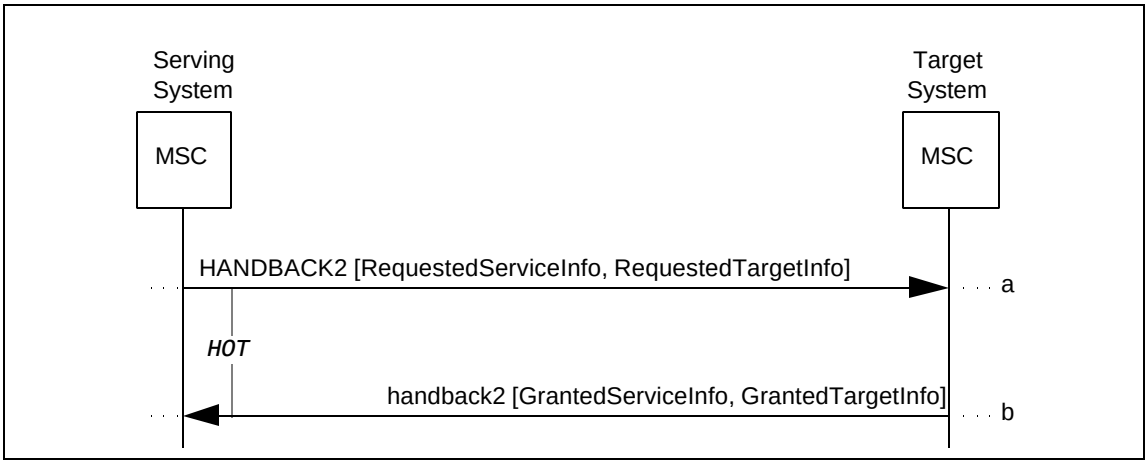

Figure 9 Successful HandoffBack2

a. The Serving MSC determines that a call should be handed off to a target system to which it is already connected, for the call in question, via an inter-MSC trunk. It sends a HANDBACK2 to the Target MSC, directing the Target MSC to initiate a Handoff-Back task.

Parameters	Usage	Type
RequestedServiceInfo:	Set of parameters for Requested Service Information	
[CDMACallMode]	Indicates the acceptable mode of the current call = {AMPS | NAMPS | CDMA}.	O
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the serving channel, if CDMA.	O
[CDMAStationClass-Mark][1]	Identifies certain characteristics of a dual-mode CDMA MS.	O
[CDMAStationClass-Mark2][2]	Identifies certain characteristics of a CDMA MS (e.g., dual-band, dual-mode).	O
...		
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the serving channel, if TDMA.	O

...

[1] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMAStationClassMark is used.

[2] For [*TSB76*] and later, CDMAStationClassMark2 is used.

b. The Target MSC increases the Segment Counter in the received BillingID parameter by one. If a voice channel on the designated target cell is available, it returns a handback2 to the requesting MSC, and initiates a Handoff-Back task.

Parameters	Usage	Type
GrantedServiceInfo:	Set of parameters for Granted Service Information.	
[CDMACodeChannel-List]	Identifies the code channels in a Forward CDMA Channel used for the call. Included if target channel is CDMA.	O
[CDMASearchPara-meters][1]	Specifies search information (SearchWindow, T_ADD, T_DROP, T_COMP, T_TDROP) that a CDMA MS should use to search for pilots. Included if target channel is CDMA.	O
[CDMASearchWindow][2]	Specifies the number of PN chips that a CDMA MS should use to search for usable multipath components of the pilots in the Active Set and the Candidate Set. Included if target channel is CDMA.	O
[ConfidentialityModes]	Identifies the status of Signaling Message Encryption and Voice Privacy features for the MS actually used for call. Included if the TerminalType value is '2' or greater.	O
[TDMABurstIndicator]	Indicates whether or not the mobile is required to transmit shortened burst (as defined in *TDMA*) after handoff. Included if a TDMA channel is in use.	O
GrantedTargetInfo:	Set of parameters for Target Service Information.	
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the target channel, if CDMA.	O
[ChannelData]	Indicates the SAT Color Code, Voice Mobile Attenuation Code, and the channel number of the target channel, if analog.	O
[NAMPSChannelData]	Indicates the Digital SAT Color Code and the narrow voice channel assignment associated with the target analog channel, if NAMPS.	O
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the target channel, if TDMA.	O

[1] For this Standard and later, CDMASearchParameters is used.

[2] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMASearchWindow is used.

[TargetCellID]	Specifies the ID of the actual target cell site selected (AMPS, NAMPS, TDMA).	O

4.9.1. Successful HandoffToThird2 (*N.S0005-0 v 1.0* Chapter 2, page 34)

This scenario describes the successful use of the HandoffToThird2 operation.

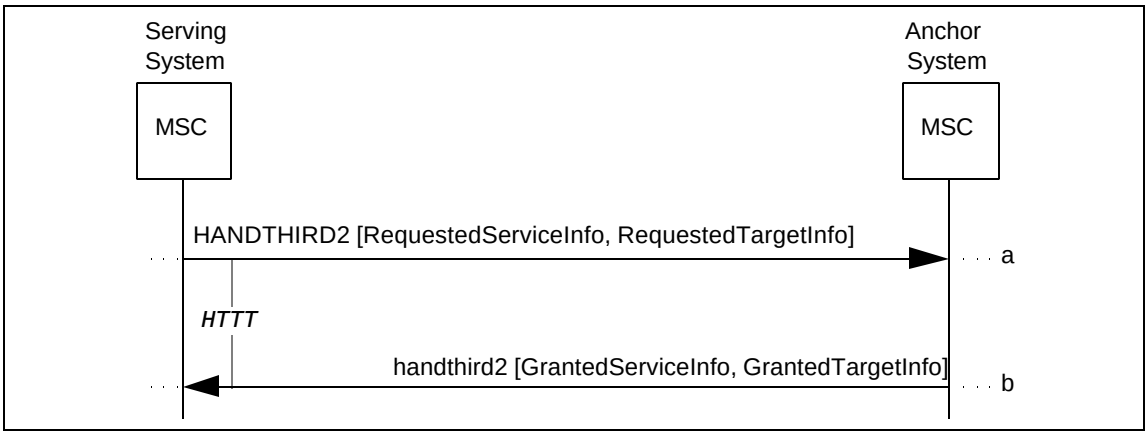

Figure 15 Successful HandoffToThird2

a. The Serving MSC determines that a call should be handed off to a target system and that path minimization may be possible. It sends a HANDTHIRD2 to the MSC which had previously handed off the call to the Serving MSC (i.e., the Anchor MSC in this scenario), requesting that a handoff with path minimization be performed.

Parameters	Usage	Type
RequestedServiceInfo:	Set of parameters for Requested Service Information	
[CDMACallMode]	Indicates the acceptable mode of the current call = {AMPS | NAMPS | CDMA}.	O
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the serving channel, if CDMA.	O
[CDMAStationClass-Mark][1]	Identifies certain characteristics of a dual-mode CDMA MS.	O
[CDMAStationClass-Mark2][2]	Identifies certain characteristics of a CDMA MS (e.g., dual-band, dual-mode).	O
...		
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the serving channel, if TDMA.	O

...

b. If the receiving MSC accepts the request to perform a handoff with path minimization, and a voice channel on the target system is found available, the receiving MSC returns the parameters of the selected voice channel to the Serving MSC in a `handthird2`.

[1] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMAStationClassMark is used.

[2] For [*TSB76*] and later, CDMAStationClassMark2 is used.

Parameters	Usage	Type
GrantedServiceInfo:	Set of parameters for Granted Service Information.	
[CDMACodeChannel-List]	Identifies the code channels in a Forward CDMA Channel used for the call. Included if target channel is CDMA.	O
[CDMASearchPara-meters][1]	Specifies search information (SearchWindow, T_ADD, T_DROP, T_COMP, T_TDROP) that a CDMA MS should use to search for pilots. Included if target channel is CDMA.	O
[CDMASearchWindow][2]	Specifies the number of PN chips that a CDMA MS should use to search for usable multipath components of the pilots in the Active Set and the Candidate Set. Included if target channel is CDMA.	O
[ConfidentialityModes]	Identifies the status of Signaling Message Encryption and Voice Privacy features for the MS actually used for call. Included if the TerminalType value is '2' or greater.	O
[TDMABurstIndicator]	Indicates whether or not the MS is required to transmit shortened burst (as defined in *TDMA*) after handoff. Included if a TDMA channel is in use.	O
GrantedTargetInfo:	Set of parameters for Target Service Information.	
[CDMAChannelData]	Indicates the CDMA Channel Number field, the Frame Offset field, the ~~and a~~ Long Code Mask field, Nominal Power Extension field, Nominal Power field, and a Number Preamble field of the target channel, if CDMA.	O
[ChannelData]	Indicates the SAT Color Code, Voice Mobile Attenuation Code, and the channel number of the target channel, if analog.	O
[NAMPSChannelData]	Indicates the Digital SAT Color Code and the narrow voice channel assignment associated with the target analog channel, if NAMPS.	O
[TDMAChannelData]	Indicates the Rate, Digital Verification Color Code, Digital Mobile Attenuation Code, and the channel number of the target channel, if TDMA.	O
[TargetCellID]	Specifies the ID of the actual target cell site selected (AMPS, NAMPS, TDMA).	O

[1] For this Standard and later, CDMASearchParameters is used.

[2] For [*TSB64*], [*IS-41-C*], and [*ANSI-41*], CDMASearchWindow is used.

7. *N.S0005-0 v 1.0* Chapter 3 "Automatic Roaming" Modifications

7.1 *N.S0005-0 v 1.0* Chapter 3, Section 4 "Automatic Roaming Operations" Modifications

4.4 AuthenticationRequest (*N.S0005-0 v 1.0* Chapter 3, page 21)

The AuthenticationRequest (AUTHREQ) operation is used to request authentication of an authentication-capable MS.

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

Table 5 FE Combinations for AUTHREQ

	INVOKING FE	RESPONDING FE
Case 1	Serving MSC	Serving VLR
Case 2	Serving VLR	HLR
Case 3	HLR	AC

Authentication may be initiated under the following circumstances:

1. When the MS is informed that authentication is required on system accesses and:
   a. the MS attempts initial registration,
   b. the MS attempts call origination,
   c. the MS attempts call termination, or
   d. the MS issues an in-call flash request.
2. When the MS is informed that authentication is not required on system accesses and the MS attempts an initial system access (e.g., registration, origination, page response).

Also, the AuthenticationRequest operation may vary depending on whether SSD is shared or not. Note that the AuthenticationRequest (AUTHREQ) operation may result in a Network Directed System Selection (NDSS) procedure.

4.4.1 Successful Authentication on Initial Access

This operation scenario describes the successful use of the AuthenticationRequest operation to authenticate an MS which is attempting initial access. The MS is aware that authentication is required on all system accesses. The result of the operation is to allow access.

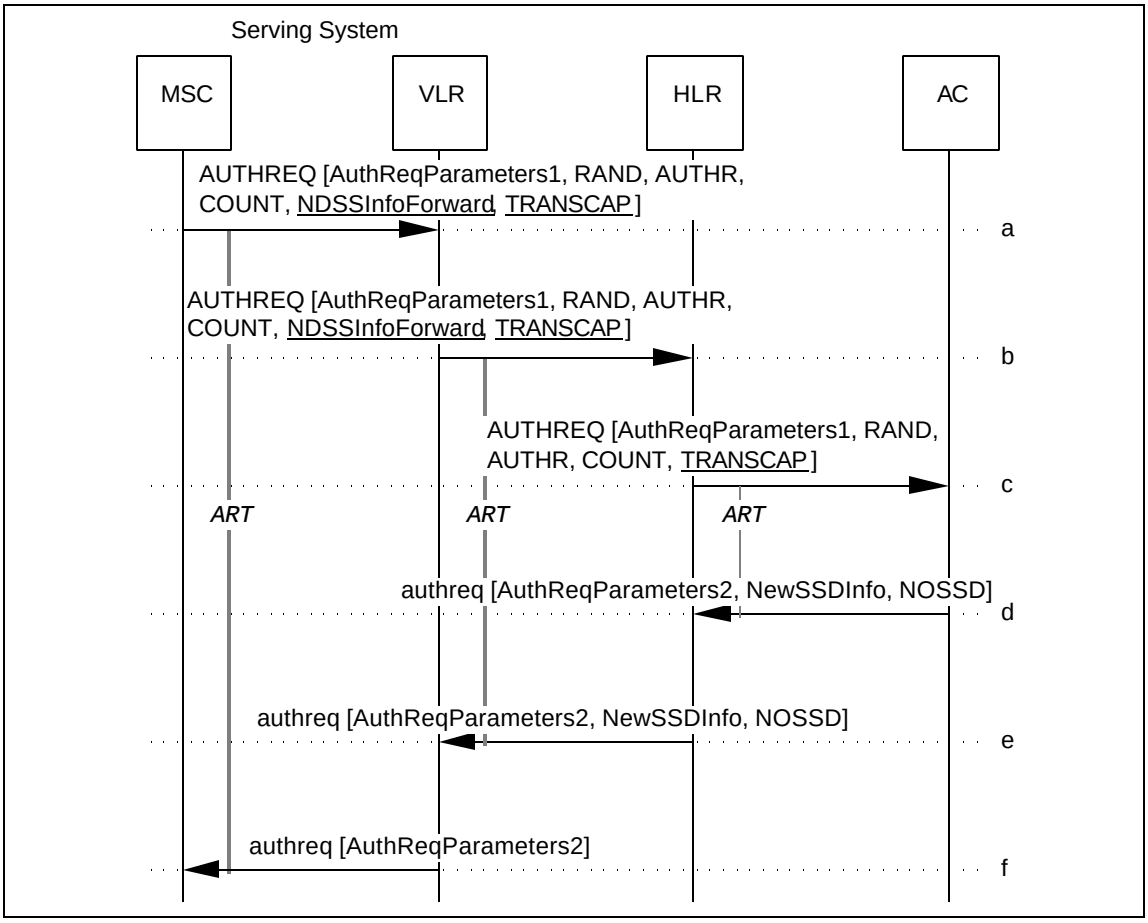

Figure 9 Successful Authentication on Initial Access

a. On an initial access attempt by an authentication-capable MS, the Serving MSC sends an AUTHREQ to the Serving VLR.

Parameters	Usage	Type
AuthReqParameters1:	Set of parameters in AUTHREQ:	
~~[MIN]~~	~~Served MS MIN.~~	~~R~~
[MSID]	Served MS MSID.	R
[ESN]	Served MS ESN.	R
[MSCID]	Serving MSC MSCID.	R
[PC_SSN]	Serving MSC PC_SSN. Include if SS7 carriage services are used.	O
[SystemCapabilities]	Authentication capabilities of Serving MSC.	R
[SystemAccessType]	Type of system access = registration.	R
[TerminalType]	Identifies the radio frequency interface standard supported by the associated MS.	R
RAND	Random number derived from MS-provided RANDC by Serving MSC.	R
AUTHR	Authentication result provided by MS.	R
COUNT	Value of CallHistoryCount provided by MS.	R
TRANSCAP	System's transaction capability	O
NDSSInfoForward:	Parameters included if NDSS was initiated by the Serving MSC:	
[CDMANID]	Serving MSC CDMA NID.	O
[ControlChannelMode]	MS mode of operation.	O
[SRCAUSE]	Indicates reason of MS registration or access.	O

b. The VLR sends an AUTHREQ to the HLR associated with the MS.

Parameters are as in Step-a, with the following modifications:		
Parameters	Usage	Type
[PC_SSN]	Serving VLR PC_SSN. Include if SS7 carriage services are used.	O
[SystemCapabilities]	Authentication capabilities of Serving VLR.	R

c. The HLR forwards the AUTHREQ to the AC. Parameters are as in Step-b, except NDSSInfoForward is not included.

d. The AC determines that the MS should be allowed access. The AC sends an `authreq` to the HLR.

Parameters	Usage	Type
AuthReqParameters2:	Set of parameters in authreq:	
[CallHistoryCount]	Event counter used for clone detection. Included if SSD is shared.	O
[RANDSSD]	Random number for SSD generation. Included if a SSD update and a Unique Challenge to the MS should be initiated by the serving system.	O
[RANDU]	Random number generated by AC to produce AUTHU. Included if a Unique Challenge to the MS should be initiated by the serving system.	O
[AUTHU]	Expected MS response to Unique Challenge Order as calculated by AC. Included if a Unique Challenge to the MS should be initiated by the serving system.	O
[UpdateCount]	Indicates that the COUNT update procedure should be initiated by the serving system.	O
NewSSDInfo:	New SSD information:	
[Authentication-AlgorithmVersion]	Include if SSD included to select authentication algorithm other than default.	O
[SSD]	New value of VLR and AC shared secret data. May be included if the SystemCapabilities of the VLR include “CAVE execution” and AC administration policies allow distribution of the SSD.	O
NOSSD	Indicates that previously provided SSD is no longer valid and should be discarded.	O

e. The HLR forwards the `authreq` to the Serving VLR. Parameters are as in Step-d.

f. The Serving VLR forwards the `authreq` to the Serving MSC. Parameters are as in Step-d, with the exception that the SSD, AAV and NOSSD parameters are not included.

4.4.A NDSS Procedure As a Result of AuthenticationRequest

This operation scenario describes the successful use of the AuthenticationRequest operation to redirect an MS which is attempting initial access to a serving system. The MS is aware that authentication is required on all system accesses. The result of the operation is a system redirection.

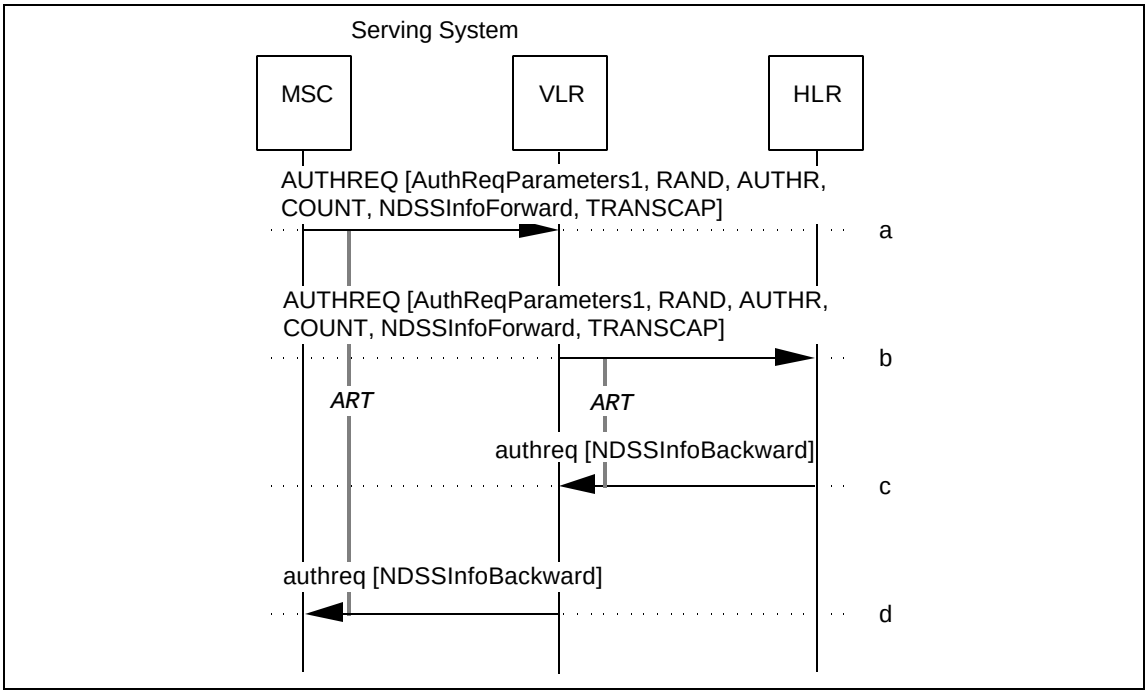

Figure 4.4.A-1 NDSS Procedure as a Result of AuthenticationRequest

a-b. Same as Section 4.4.1, Steps a-b.

c. The HLR determines the MS should be redirected to a preferred system. HLR sends an `authreq` to the VLR with the following redirection parameters.

Parameters	Usage	Type
NDSSInfoBackward:	Parameters included for NDSS operation.	
[SRINFO]	Instructs MS whether to return to the serving system if NDSS fails.	O
[ROAMIND]	Specifies roaming indication to the MS.	O
RedirectRecord:	Defines preferred system information:	
[ANALOGRR]	Defines preferred analog system information.	O
[CDMARR]	Defines preferred CDMA system information.	O

d. The Serving VLR forwards the `authreq` to the Serving MSC. Parameters are as in step-c.

4.14 InterSystemPage

(*N.S0005-0 v 1.0* Chapter 3, page 60)

The InterSystemPage (ISPAGE) operation is used by a Serving MSC to request a Border MSC to either (a) page an MS, or (b) listen for a page response from an MS, in the border system.

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

Table 15 FE Combinations for ISPAGE

	INVOKING FE	RESPONDING FE
Case 1	Serving MSC	Border MSC

One of several possible results is returned:

1. Routing information in the form of a TLDN on the Border MSC.
2. An indication that access to the identified MS is denied with reason for denial (e.g., due to an MS busy condition, no page response, or unavailable).
3. An error indicating the transaction cannot be completed.

4.14.1 Successful InterSystemPage: Border MSC Routing Information Returned

This operation scenario describes the InterSystemPage operation when the response provides routing information to the MS on the Border MSC.

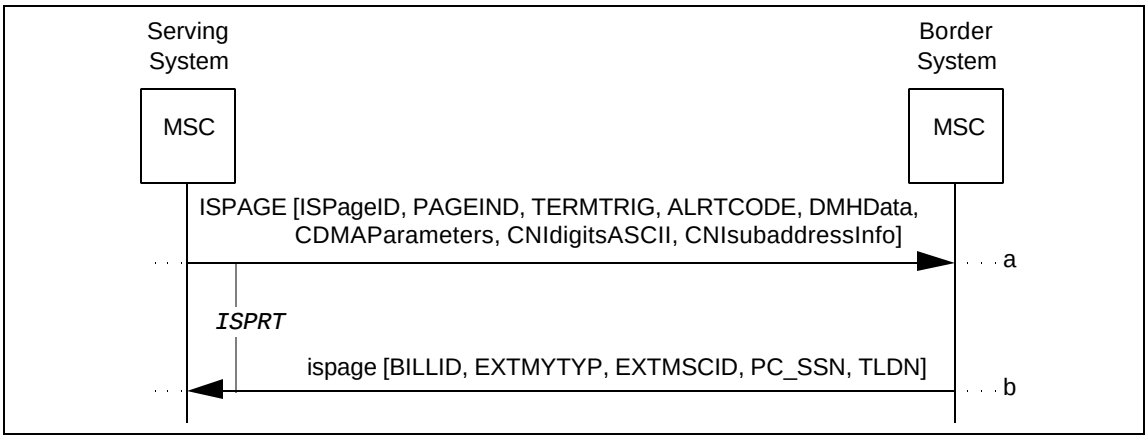

Figure 29 Successful InterSystemPage: Border MSC Routing Information Returned

a. The Serving MSC sends an ISPAGE to the Border MSC, including an indication of the area where the MS's presence was last detected, an indication of whether to page or just listen for an unsolicited page response, and other relevant parameters.

Parameters	Usage	Type
ISPageID:	Set of identification parameters in ISPAGE:	
[BillingID]	Originating Call ID. Used for billing and redirection purposes when ISPAGE results in call routing.	R
~~[MIN]~~	~~Served MS MIN.~~	~~R~~
[MIN, IMSI]	Served MS MIN and IMSI (include all known).	O
[ESN]	Served MS ESN.	R
[MSCID]	Originating MSC MSCID.	R
[LocationAreaID]	Served MS LocationAreaID for paging purposes. Included if available.	O
[ExtendedSystemMy-TypeCode]	Serving MSC vendor identification.	O
[ExtendedMSCID]	Serving MSC MSCID.	O
[SystemMyTypeCode]	Originating MSC vendor identification.	O
[MSCIN]	Identifies Originating MSC.	O
[NETMSI]	Served NetworkTMSI. Include if supported by the Border MSC.	O
[PC_SSN]	Originating MSC PC_SSN. Include if SS7 carriage services are used.	O
...		

…

4.15 InterSystemPage2 (*N.S0005-0 v 1.0* Chapter 3, Page 65)

The InterSystemPage2 (ISPAGE2) operation is used by a Serving MSC that has received a call via a TLDN to request a Border MSC to either (a) page an MS, or (b) listen for a page response from an MS, in the border system.

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

Table 16 FE Combinations for ISPAGE2

	INVOKING FE	RESPONDING FE
Case 1	Serving MSC	Border MSC

One of several possible results is returned:

1. An indication that identified MS's presence is confirmed in the Border MSC. Include indication if authentication should be performed for MS.
2. An indication that access to the identified MS is denied with reason for denial (e.g., due to an MS busy condition, no page response, or unavailable).
3. An error indicating the transaction cannot be completed.

4.15.1 Successful InterSystemPage2: MS Presence Confirmed in Border MSC

This operation scenario describes the InterSystemPage2 operation when the response indicates that the MS's presence has been successfully confirmed in the Border MSC.

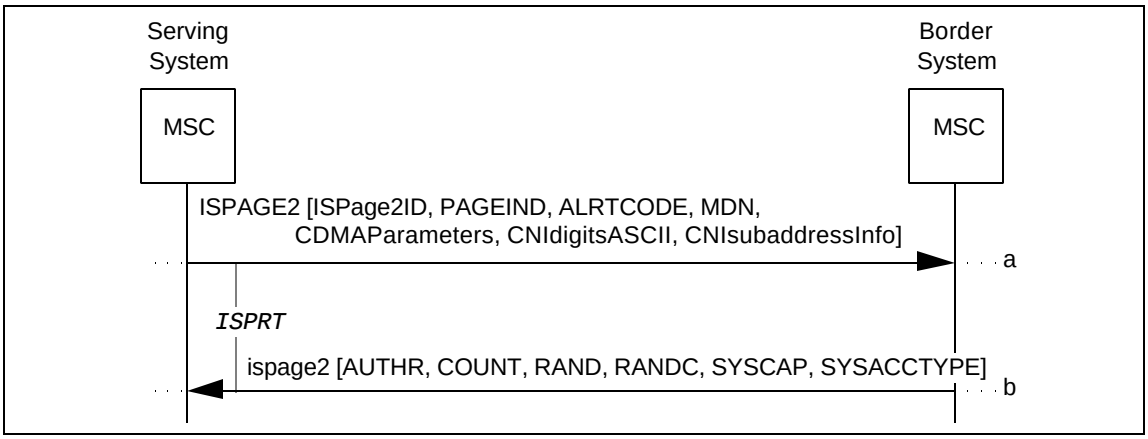

Figure 32 Successful InterSystemPage2: MS Presence Confirmed in Border MSC

a. The Serving MSC sends an `ISPAGE2` to the Border MSC, including an indication of the area where the MS's presence was last detected, an indication of whether to page or just listen for an unsolicited page response, and other relevant parameters. If the MS is a CDMA MS, appropriate parameters necessary for paging the MS are included.

Parameters	Usage	Type
ISPage2ID:	Set of identification parameters in ISPAGE2:	
[BillingID]	Originating Call ID. Used for billing and redirection purposes when ISPAGE2 results in call routing.	R
~~[MIN]~~	~~Served MS MIN.~~	~~R~~
[MIN, IMSI]	Served MS MIN and IMSI (include all known).	O
[ESN]	Served MS ESN.	R
[LocationAreaID]	Served MS LocationAreaID for paging purposes. Included if available.	O
[NETMSI]	Served NetworkTMSI. Include if supported by the Border MSC.	O
...		

…

4.A ParameterRequest

(*N.S0005-0 v 1.0* Chapter 3, page 86)

The ParameterRequest (PARMREQ) operation is used to obtain the required parameters associated with MS. The following table lists the valid combinations of invoking and responding FEs.

Table 4.A-1 FE Combinations for PARMREQ

	INVOKING FE	RESPONDING FE
Case 1	New Serving VLR	Old Serving VLR
Case 2	Serving MSC	Serving VLR

One of two possible results is returned:

1. The ParameterRequest operation is successful.
2. Notification that the ParameterRequest is unsuccessful with an appropriate denied reason.

4.A.1 Successful ParameterRequest between New Serving VLR and Old Serving VLR

This scenario describes the successful use of the ParameterRequest operation between New Serving VLR and Old Serving VLR.

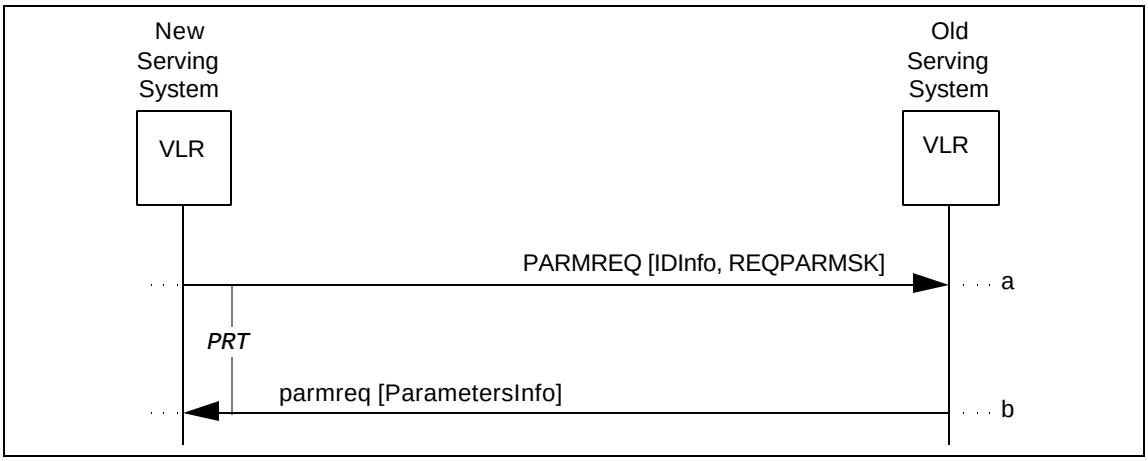

Figure 4.A.1-1 Successful ParameterRequest between New Serving VLR and Old Serving VLR

a. The New Serving VLR determines that MS's IMSI (or MIN) and ESN are unknown. According to the known ID information (i.e., NetworkTMSI) it sends a PARMREQ to the Old Serving VLR to get the required parameters of IMSI and ESN.

Parameters	Usage	Type
REQPARMSK	Mask of parameters required.	R
IDInfo:	Identifies the Subscriber:	
[NETMSI]	Served MS NetworkTMSI.	R
[MSID]	Served MS MIN, or IMSI.	O
[MSCID]	VLR's MSC address. Identifies the VLR requesting the parameter information.	O
[PC_SSN]	Serving VLR PC_SSN. Include if SS7 carriage services are used.	O
[SENDERIN]	SenderIdentificationNumber. Indicates the identification number of FE sending this message.	O
[SystemMyTypeCode]	Vendor identification of New Serving VLR.	O

b. The Old Serving VLR determines that it can provide the requested parameters and then returns a parmreq including the requested MSID (e.g., IMSI or MIN) and ESN to the New Serving VLR .

Parameters	Usage	Type
ParametersInfo:	Indicates the required parameters. Include if requested in REQPARMSK:	
[ESN]	Served MS ESN.	R
[IMSI]	Served MS IMSI.	O
[MIN]	Served MS MIN.	O

4.A.2 Successful ParameterRequest between Serving MSC and Serving VLR

This scenario describes the successful use of the ParameterRequest operation between Serving MSC and Serving VLR.

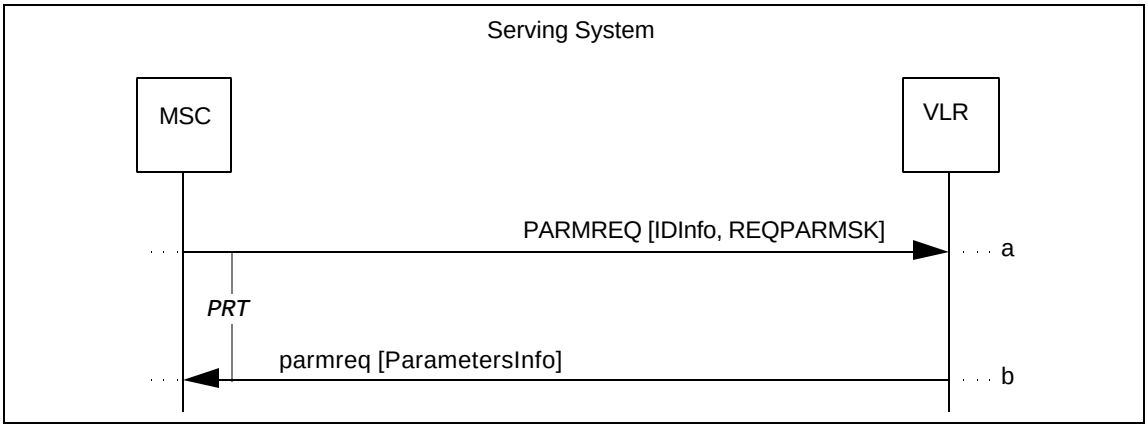

Figure 4.A.2-1 Successful ParameterRequest between Serving MSC and Serving VLR

a. The Serving MSC determines that additional parameters are required. According to the known ID information (e.g., NetworkTMSI) it sends a PARMREQ to the Serving VLR to get the required parameters (e.g., IMSI and ESN).

Parameters	Usage	Type
REQPARMSK	Mask of parameters required.	R
IDInfo:	Identifies the Subscriber. At least one of the following is required (IMSI, ESN, MIN, or NetworkTMSI):	
[NETMSI]	Served MS NetworkTMSI.	R
[ESN]	Served MS ESN.	O
[MSID]	Served MS MIN, or IMSI.	O
[PC_SSN]	Serving VLR PC_SSN. Include if SS7 carriage services are used.	O

b. The Serving VLR determines that it can provide the required parameters and then returns a `parmreq` including the requested information to the Serving MSC.

Parameters	Usage	Type
ParametersInfo:	Indicates the required parameters. Include if requested in REQPARMSK:	R
[IMSI]	Served MS IMSI.	O
[MIN]	Served MS MIN.	O
[ESN]	Served MS ESN.	O
[NETMSI]	Served MS NetworkTMSI.	O
[LOCID]	Location Area ID.	O

4.A.3 Unsuccessful ParameterRequest between New Serving VLR and Old Serving VLR

This scenario describes an unsuccessful invocation of the ParameterRequest operation between New Serving VLR and Old Serving VLR.

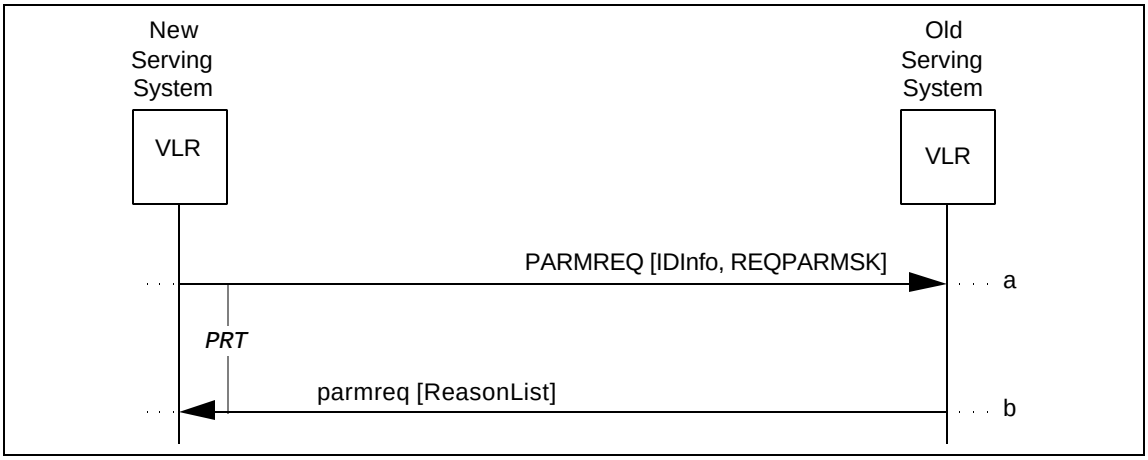

Figure 4.A.3-1 Unsuccessful ParameterRequest between New Serving VLR and Old Serving VLR

a. Same as Section 4.A.1, Step-a.

b. If the Old Serving VLR determines that the required parameters (e.g. IMSI or ESN) do not exist in its database, it returns a `parmreq` with the ReasonList set to 'Required parameters unavailable.'

4.A.4 Unsuccessful ParameterRequest between Serving MSC and Serving VLR

This scenario describes an unsuccessful invocation of the ParameterRequest operation between Serving MSC and Serving VLR.

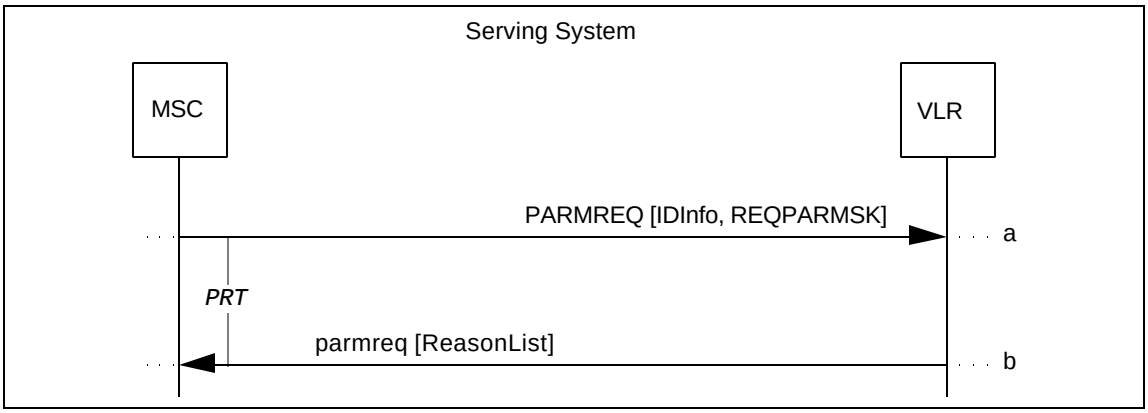

Figure 4.A.4-1 Unsuccessful ParameterRequest between Serving MSC and Serving VLR

a. Same as Section 4.A.2, Step-a.

b. The Serving VLR determines that the required parameters do not exist in its database and then returns a `parmreq` to the Serving MSC with the appropriate value of ReasonList.

4.20 QualificationDirective (*N.S0005-0 v 1.0* Chapter 3, page 89)

The QualificationDirective (QUALDIR) operation is used to update the authorization information, profile information, or both, previously obtained for an MS.

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

Table 21 FE Combinations for QUALDIR

	INVOKING FE	RESPONDING FE
Case 1	HLR	Serving VLR
Case 2	Serving VLR	Serving MSC

One of several possible results is achieved:

1. The MS is re-authorized with an indication of the authorization duration (e.g., per call, eight hours, one day).
2. Item 1 along with the delivery of the MS's updated calling capabilities (i.e., profile information) to the serving system.
3. An update of the MS's calling capabilities is delivered to the serving system.
4. The MS is de-authorized with reason (e.g., due to a delinquent account).
5. The MS is being redirected to a preferred system.

4.20.3 Successful QualificationDirective: Update Profile Only

This operation scenario describes the QualificationDirective operation when the request is to update the MS's profile only.

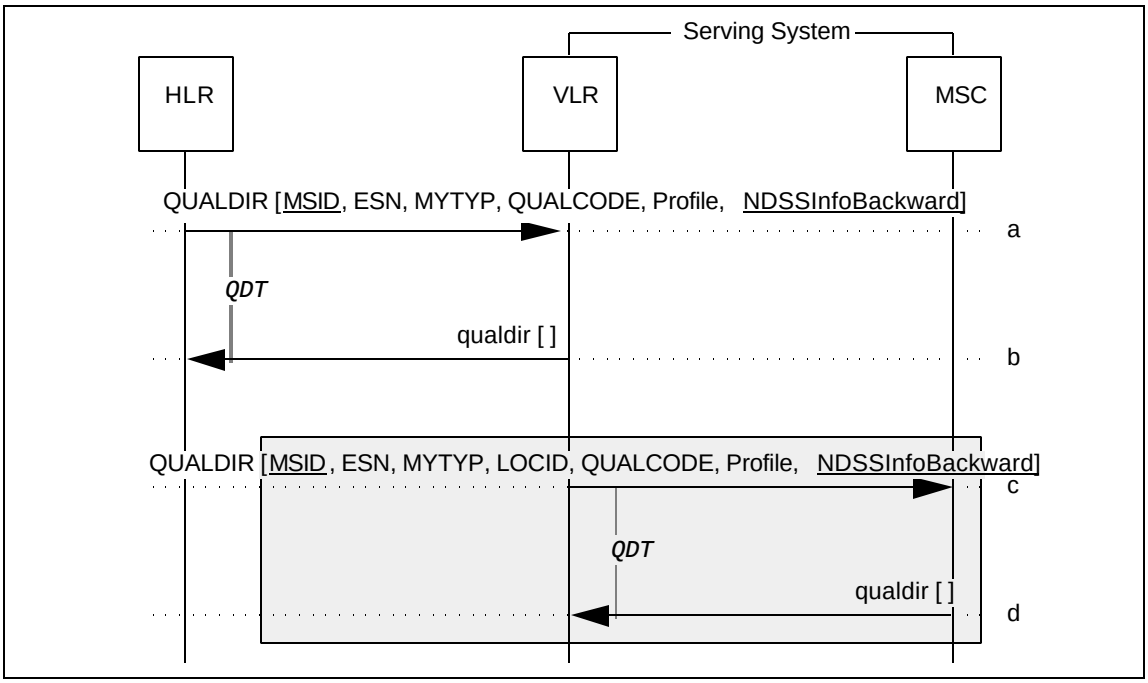

Figure 49 Successful QualificationDirective: Update Profile Only

a-d. Same as Section 4.21.2, Steps a-d.

Parameters are as in Section 4.21.2, Steps a-d, with the AUTHPER parameter omitted in Steps a and c, and with the following modification and additions to both Steps a and c:		
Parameters	Usage	Type
~~MIN~~	~~Served MS MIN.~~	~~R~~
MSID	Served MS MSID (last identifier used for registration at serving system).	R
QUALCODE	Type of qualification = profile only.	MBC
NDSSInfoBackward:	Parameters included for NDSS operation:	
[SRINFO]	Instructs MS whether to return to the serving system if NDSS fails.	O
[ROAMIND]	Specifies roaming indication to the MS.	O
RedirectRecord:	Defines preferred system information:	
[ANALOGRR]	Defines preferred analog system information.	O
[CDMARR]	Defines preferred CDMA system information.	O

Note: Steps c and d are optional and are executed only if the service or call in progress may be discontinued. It should be also noted that when NDSSInfoBackward is included, the Serving MSC may use this information to respond to the MS.

4.21 QualificationRequest (*N.S0005-0 v 1.0* Chapter 3, page 97)

The QualificationRequest (QUALREQ) operation is used (a) to request validation of an MS or (b) to request validation of an MS and obtain its profile information.

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

Table 22 FE Combinations for QUALREQ

	INVOKING FE	RESPONDING FE
Case 1	Serving MSC	Serving VLR
Case 2	Serving VLR	HLR

One of several possible results is returned:

1. An indication that authorization is confirmed with an indication of the authorization duration (e.g., per call, eight hours, one day).
2. Item 1 along with the MS's calling capabilities (i.e., profile information).
3. Only the MS's calling capabilities.
4. An indication that authorization is denied with reason for denial (e.g., due to an invalid serial number).
5. An indication that the MS is being redirected to a preferred system.

4.21.1 Successful QualificationRequest: Authorization Confirmed

This operation scenario describes the QualificationRequest operation when authorization is confirmed and no profile is requested.

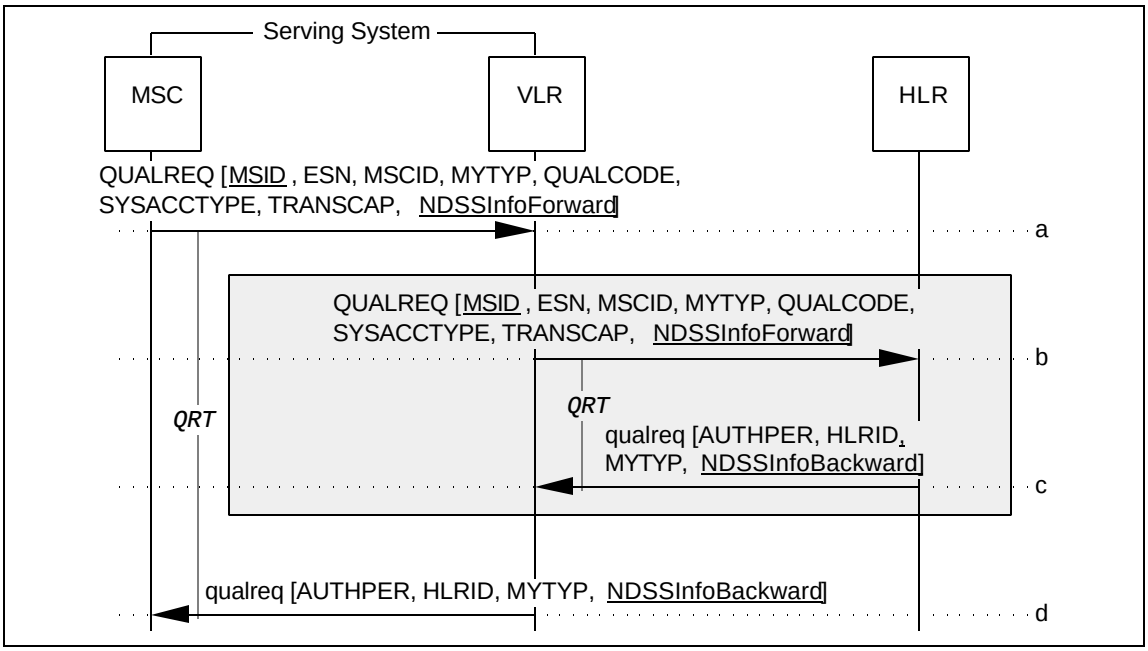

Figure 51 Successful QualificationRequest: Authorization Confirmed

a. After determining that a roaming MS is now within its service area, the Serving MSC sends a QUALREQ to its VLR; the Serving MSC may detect the MS's presence through autonomous registration, call origination, call termination (i.e. a page response following a call to the roamer port) or a service order.

Parameters	Usage	Type
~~MIN~~	~~Served MS MIN.~~	~~R~~
MSID	Served MS MIN or IMSI .	R
ESN	Served MS ESN.	R
MSCID	Serving MSC MSCID.	R
MYTYP	Serving MSC vendor identification.	MBC
QUALCODE	Type of request = validation only.	R
SYSACCTYPE	Indicates the type of system access.	R
TRANSCAP	Indicates the serving system's transaction capability at the current time.	R
NDSSInfoForward:	Parameters included if NDSS was initiated by the Serving MSC:	
[CDMANID]	Serving MSC CDMA NID.	O
[ControlChannelMode]	MS mode of operation.	O
[SRCAUSE]	Indicates reason of MS registration or access.	O
[TERMTYP]	Identifies the radio frequency interface standard supported by the associated MS.	O

b. If the MS had previously registered with an MSC within the domain of the VLR, the VLR may take no further action other than to record the identity of the MSC currently serving the MS and proceed to Step-d. If the MS is unknown to the VLR or if the information requested by the MSC is not available at the VLR, the VLR sends a QUALREQ to the HLR associated with the MS.

Parameters are as in Step-a, with the following modifications:		
Parameters	Usage	Type
MYTYP	VLR vendor identification.	MBC

c. The HLR determines that authorization can be granted to the MS and returns this indication to the Serving VLR in the qualreq.

Parameters	Usage	Type
AUTHPER	Authorization confirmed indication with period of authorization.	R
HLRID [MSCID]	HLR MSCID to key MS record against for a subsequent UnreliableRoamerDataDirective.	R
MYTYP	HLR vendor identification.	MBC
NDSSInfoBackward:	Parameters included for NDSS operation:	
[SRINFO]	Instructs MS whether to return to the serving system if NDSS fails.	O
[ROAMIND]	Specifies roaming indication to the MS.	O
RedirectRecord:	Defines preferred system information:	
[ANALOGRR]	Defines preferred analog system information.	O
[CDMARR]	Defines preferred CDMA system information.	O

d. The VLR sends a qualreq to the Serving MSC.

Parameters are as in Step-c, with the following modification:		
Parameters	Usage	Type
HLRID [MSCID]	HLR MSCID. Include if received in Step-c.	O
MYTYP	VLR vendor identification.	MBC

4.26 RegistrationNotification (*N.S0005-0 v 1.0* Chapter 3, page 118)

The RegistrationNotification (REGNOT) operation is used to report the location of a newly registered MS and, optionally, to (a) validate the MS or (b) validate the MS and obtain its profile information. The following table lists the valid combinations of invoking and responding FEs.

Table 27 FE Combinations for REGNOT

	INVOKING FE	RESPONDING FE
Case 1	Serving (or Bordering) MSC	Serving (or Bordering) VLR
Case 2	Serving (or Bordering) VLR	HLR

One of several possible results is returned:

1. An indication that authorization is confirmed with an indication of the authorization duration (e.g., per call, eight hours, one day).
2. Item 1 along with the MS's calling capabilities (i.e., profile information).
3. Only the MS's calling capabilities.
4. An indication that authorization is denied with reason for denial (e.g., due to an invalid serial number).
5. An indication that the MS is being redirected to a preferred system.

4.26.1 Successful RegistrationNotification: Confirmed at the VLR

This operation scenario describes the RegistrationNotification operation when confirmed at the VLR.

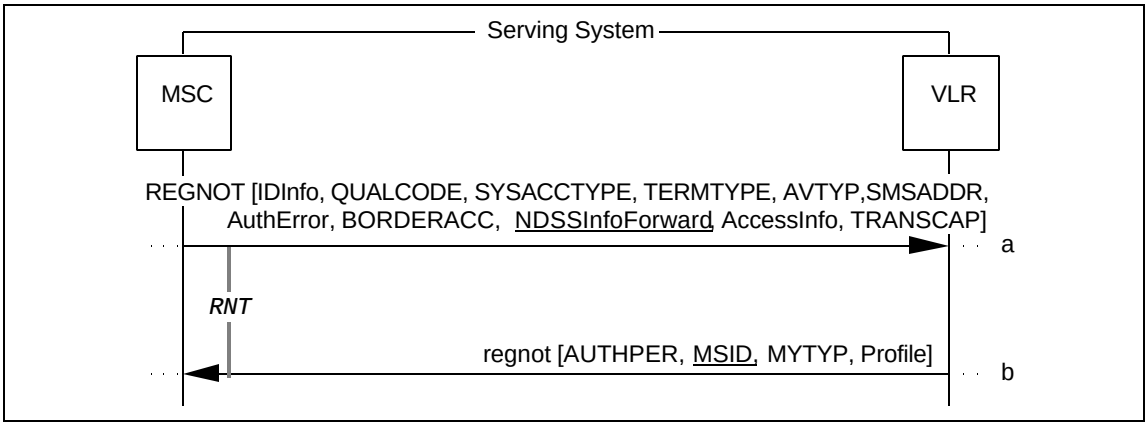

Figure 64 Successful RegistrationNotification: Confirmed at the VLR

a. The Serving MSC determines that a roaming MS is within its service area; the Serving MSC may detect the MS's presence through autonomous registration, call origination, call termination (i.e., a page response following a call to the roamer port) or a service order. The Serving MSC sends a REGNOT to its VLR.

Parameters	Usage	Type
IDInfo:	Set of identification parameters in REGNOT:	
~~[MIN]~~	~~Served MS MIN.~~	~~R~~
[MSID]	Served MS MSID. Include the identifier (MIN or IMSI) used by the MS to access this system.	R
[ESN]	Served MS ESN.	R
[MSCID]	Serving MSC MSCID.	R
[PC_SSN]	Serving MSC PC_SSN. Include if SS7 carriage services are used.	O
[LocationAreaID]	For paging served MS. Include if available.	O
[SystemMyTypeCode]	Serving MSC vendor identification.	MBC
QUALCODE	Type of qualification required.	R
SYSACCTYPE	Type of system access.	R
TRANSCAP	System's transaction capability.	R
TERMTYP	Identifies the radio frequency interface standard supported by the associated MS.	R
AVTYP	Indicates MS is unavailable for normal call delivery, if applicable.	O
SMSADDR	Temporary routing address of SMS subscriber, if applicable.	O
AuthError:	Parameters included if authentication parameters were requested by the Serving MSC but not received from the MS:	O
[SystemCapabilities]	Authentication capabilities of serving system.	
[ReportType]	Report of missing authentication parameters.	
BORDERACC	Indicates that system access is in a border cell, as determined by local procedures.	O

continued on next page...

...continued from previous page

Parameters	Usage	Type
NDSSInfoForward:	Parameters included if NDSS was initiated by the Serving MSC:	
[CDMANID]	Serving MSC CDMA NID.	O
[ControlChannelMode]	MS mode of operation.	O
[SRCAUSE]	Indicates reason of MS registration or access.	O
AccessInfo:	Subscriber's access information. Included if system access is in a border cell. Includes:	O
[ReceivedSignalQuality]	Raw received signal strength from MS for use in multiple access signal strength arbitration.	
[ControlChannelData]	Includes: DCC and CHNO of analog access channel for use in multiple access detection; CMAC for use in signal strength arbitration.	
[SystemAccessData]	Indicates the Serving MSC and cell site for use in multiple access detection.	

b. The Serving VLR determines that (a) the MS had previously registered with an MSC within the domain of the VLR, (b) the MS is in the 'active' state[3], (c) this is not a multiple access situation, and (d) the requested information is available for the indicated MS.

Under these conditions, the Serving VLR records the identity of the MSC currently serving the MS and the location area identity (if applicable) of the MS. It then sends a `regnot` to the Serving MSC.

Parameters	Usage	Type
AUTHPER	Authorization confirmed indication with period of authorization.	O
MSID	Served MS MSID (for MIN and IMSI capable MS, return the "other" MS identifier than the one used in the Invoke).	O
MYTYP	VLR vendor identification.	MBC
Profile:	Subscriber's profile information. Include if profile requested in QUALCODE:	O
[CallingFeatures-Indicator]	Authorization and activity states for features.	
...		
[TerminationTriggers]	Termination trigger points currently active for the subscriber. Include if applicable.	

[3] A MS is deemed to be in the 'active' state if its most recent registration activity at the Serving VLR was a successful RegistrationNotification operation.

4.26.2 Successful RegistrationNotification: Confirmed at the HLR

This operation scenario describes the RegistrationNotification operation when confirmed at the HLR.

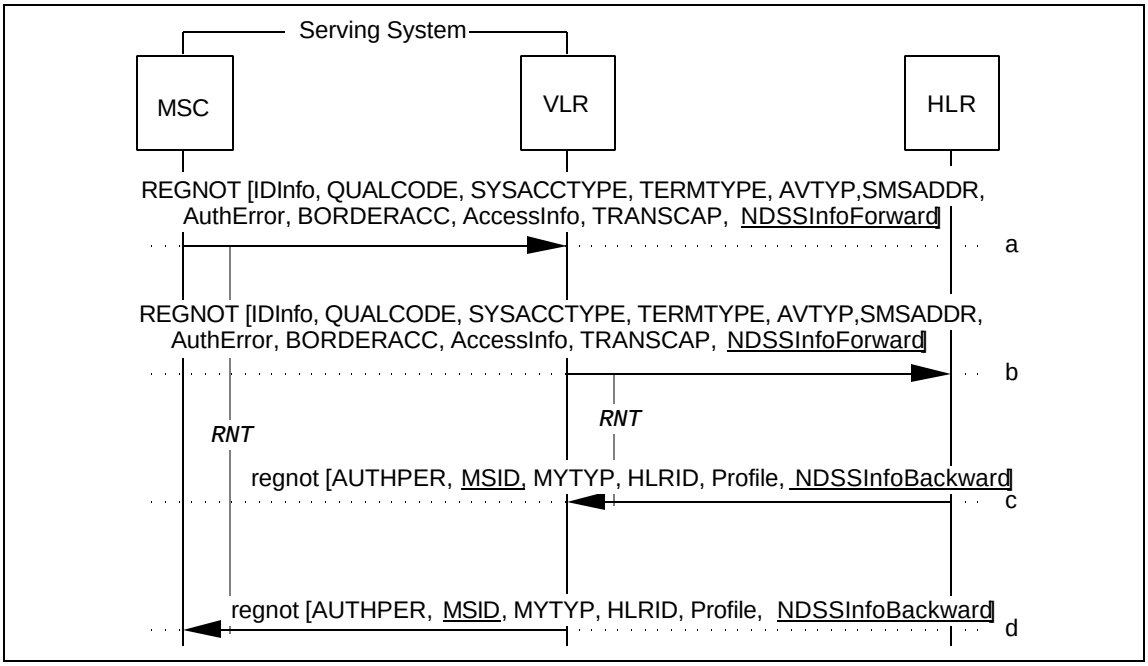

Figure 65 Successful RegistrationNotification: Confirmed at the HLR

a. Same as Section 4.27.1, Step-a.

b. The Serving VLR determines that either (a) the MS had previously registered with an MSC within the domain of the VLR but the MS has been reported inactive by the VLR, (b) the MS is not known to the VLR, or (c) the requested information cannot be made available for the indicated MS.

Under these conditions, the Serving VLR forwards the `REGNOT` to the HLR associated with the MS.

Parameters are as in Step-a, with the following modifications:		
Parameters	Usage	Type
IDInfo:	Set of identification parameters in REGNOT:	
[PC_SSN]	Serving VLR PC_SSN. Include if SS7 carriage services are used.	O
[MYTYP]	Serving VLR vendor identification.	MBC

c. The HLR determines that authorization can be granted to the MS. It returns the requested information to the Serving VLR in the `regnot`.

Parameters are as in Section 4.27.1, Step-b, with the following additions and modifications:		
Parameters	Usage	Type
HLRID [MSCID]	HLR MSCID to key MS record against for a subsequent UnreliableRoamerDataDirective.	R
MYTYP	HLR vendor identification.	MBC
NDSSInfoBackward:	Parameters included for NDSS operation:	
[SRINFO]	Instructs MS whether to return to the serving system if NDSS fails.	O
[ROAMIND]	Specifies roaming indication to the MS.	O
RedirectRecord:	Defines preferred system information:	
[ANALOGRR]	Defines preferred analog system information.	O
[CDMARR]	Defines preferred CDMA system information.	O

d. The VLR forwards the `regnot` to the Serving MSC.

Parameters are as in Step-c, with the exception that the HLRID parameter is not included and with the following modification:		
Parameters	Usage	Type
MYTYP	VLR vendor identification.	MBC

4.B TMSIDirective

(*N.S0005-0 v 1.0* page 153)

The TMSIDirective (TMSIDIR) operation is used to assign the MS's full TMSI within a TMSI Zone .

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

Table 4.B-1 FE Combinations for TMSIDIR

	INVOKING FE	RESPONDING FE
Case 1	Serving VLR	Serving MSC

One of two possible results is returned:

1. Notification that the TMSIDirective was successful.
2. Notification that the TMSIDirective was unsuccessful with an appropriate reason.

4.B.1 Successful TMSIDirective

This scenario describes the successful use of the TMSIDirective operation.

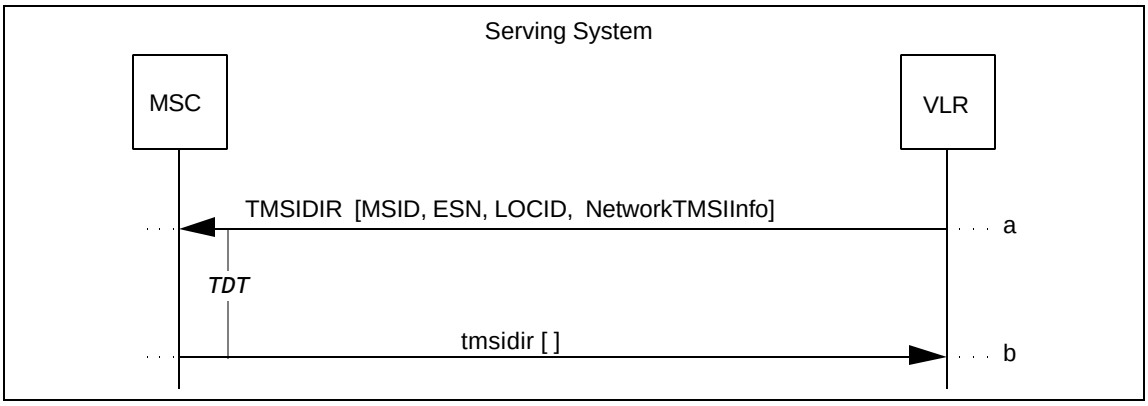

Figure 4.B.1-1 Successful TMSIDirective

a. The Serving VLR sends a `TMSIDIR` to the Serving MSC with NetworkTMSI included.

Parameters	Usage	Type
ESN	Served MS ESN.	R
MSID	Served MS MIN or IMSI.	R
NetworkTMSIInfo:	Set of NetworkTMSI parameters:	
[NewNetworkTMSI]	Indicates new assigned NetworkTMSI.	R
[NetworkTMSI-ExpirationTime]	TMSI expiration time.	R
[NetworkTMSI]	Served MS NetworkTMSI.	O
LOCID	Location Area ID. Include if available.	O

b. The Serving MSC returns an empty `tmsidir` to the Serving VLR to indicate that the newly assigned TMSI was accepted.

4.B.2 Unsuccessful TMSIDirective

This scenario describes an unsuccessful invocation of the TMSIDirective operation.

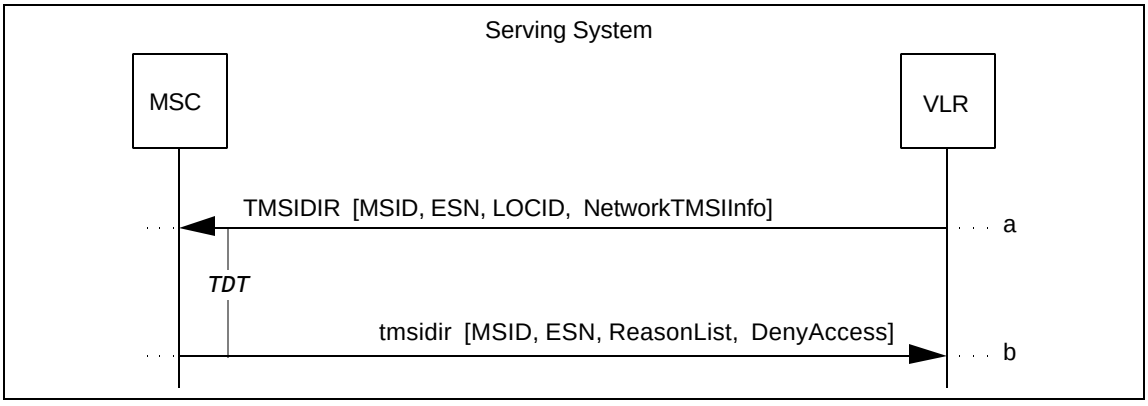

Figure 4.B.2-1 Unsuccessful TMSIDirective a. Same as Section 4.B.1, Step-a.

b. The Serving MSC determines that it is unable to perform TMSIDirective operation and returns a `tmsidir` to the Serving VLR which includes the ReasonList parameter for no response from MS or the DenyAccess parameter for unsuccessful authentication. If MS fails authentication, MS's IMSI and ESN may also be included.

Parameters	Usage	Type
MSID	Served MS MIN or IMSI. Include if MS fails to pass authentication.	O
ESN	Served MS ESN. Include if MS fails to pass authentication.	O
ReasonList	Indicates the reason for TMSI assignment failure. Include if no response from MS.	O
DenyAccess	Indication that MS is invalid. Include if authentication is required and MS fails to pass authentication.	O

7.2 *N.S0005-0 v 1.0* Chapter 3, Section 5 "Basic Automatic Roaming Scenarios" Modifications

5.A NDSS at Explicit Registration - Successful Scenarios

This section illustrates some typical explicit MS initial registration scenarios, i.e.,

- Initial Registration
- Initial Registration with Authentication

Normal *N.S0005-0 v 1.0* registration procedures shall be followed for subsequent registrations after MS's initial registration with the preferred system.

5.A.1 Initial Registration

This scenario describes the initial registration and validation process as an MS roams from one system to another, and while registering with the visited system, it is directed by its home service provider to a preferred roaming system.

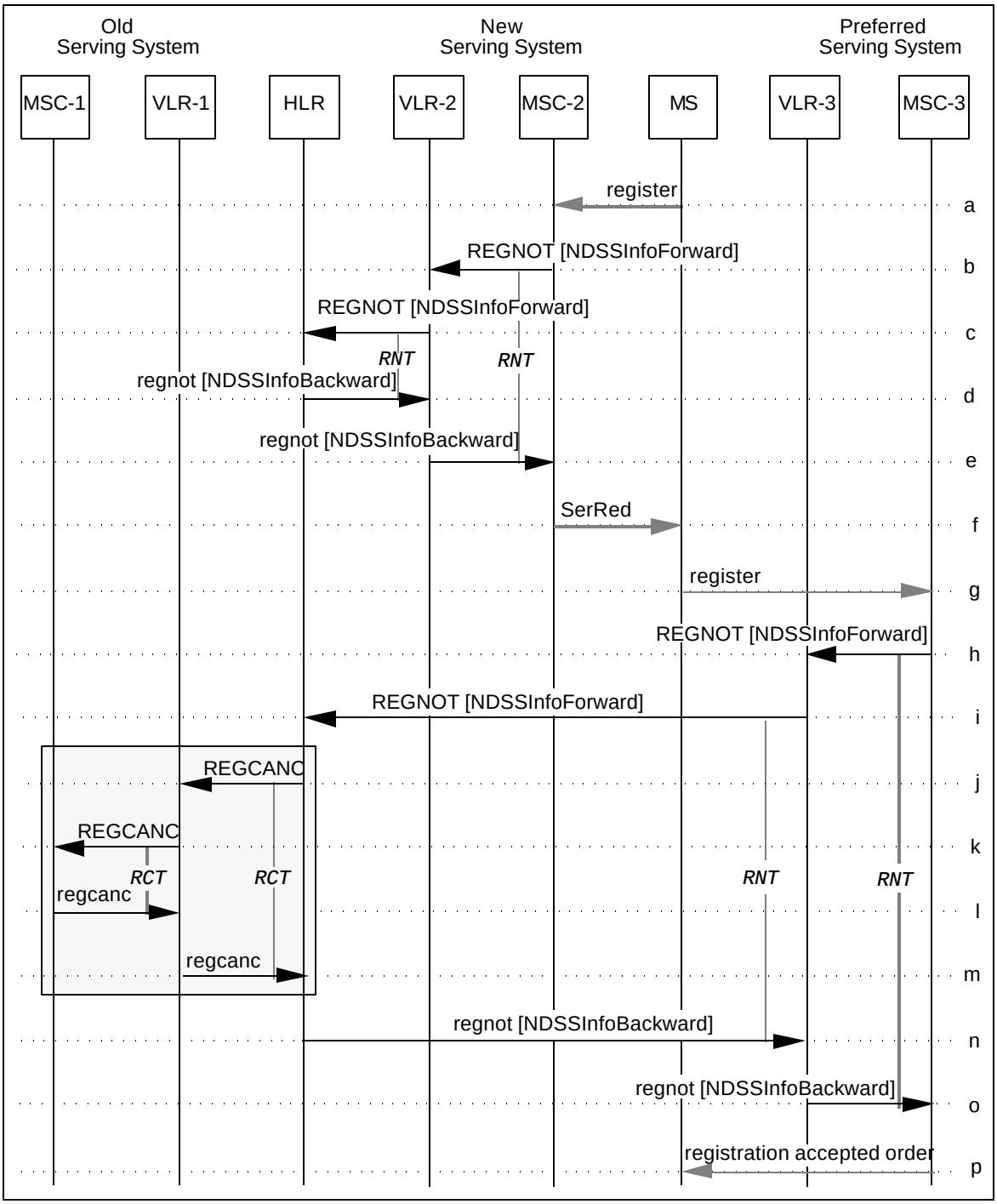

Figure 5.A.1-1 Initial Registration

a. The MS determines that a new serving system has been entered and a registration is needed. The MS registers with the new serving system (MSC-2).

b. The new Serving MSC (MSC-2) sends a REGNOT to its VLR (VLR-2).

c. VLR-2 sends a REGNOT to the HLR associated with the MS. Note that the RegistrationNotification response from the VLR to the MSC is contingent upon the response received from the HLR.

d. If the HLR determines that another system is preferable, MSC-2 is NDSS capable, and the subscriber has not suppressed the NDSS override of the MS's system selection procedure, the HLR sends a regnot message to the serving system (VLR-2) indicating an NDSS operation request and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter. The HLR may choose not to send MS's service profiles in regnot. The HLR may not perform location updating since the MSC is not authorized for service.

e. VLR-2, upon receipt of the regnot message specifying an NDSS operation, essentially removes all record of the MS from its memory if Return If Failed field of the ServiceRedirectionInfo parameter is disabled. VLR-2 sends a regnot message to MSC-2.

f. The MSC-2 sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system (MSC-3) and the RETURN_IF_FAIL specification.

g. Upon receipt of the *Service Redirection* message, the MS scans and finds the specified preferred system (MSC-3) and performs registration.

h. The preferred Serving MSC (MSC-3) sends a REGNOT to its VLR (VLR-3).

i. VLR-3 sends a REGNOT to the HLR associated with the MS. Note that the RegistrationNotification response from the VLR to the MSC is contingent upon the response received from the HLR.

j. If the MS was previously registered elsewhere, the HLR sends a REGCANC to the previously visited VLR (VLR-1). That VLR, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

k. VLR-1 sends a REGCANC to the previously visited MSC (MSC-1). That MSC, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

l. MSC-1 sends a regcanc to VLR-1.

m. VLR-1 sends a regcanc to the HLR.

n. The HLR sends a regnot to VLR-3.

o. VLR-3 forwards the regnot to MSC-3.

p. MSC-3 sends the *Registration Accepted Order* to the MS.

5.A.2 Initial Registration with Authentication

This scenario describes the intersystem message flow required to support authentication when an MS initially registers in a visited system, and while being authenticated, it is directed by its home service provider to a preferred roaming system. When the preferred system also requires authentication, the mobile registers again with the required authentication parameters.

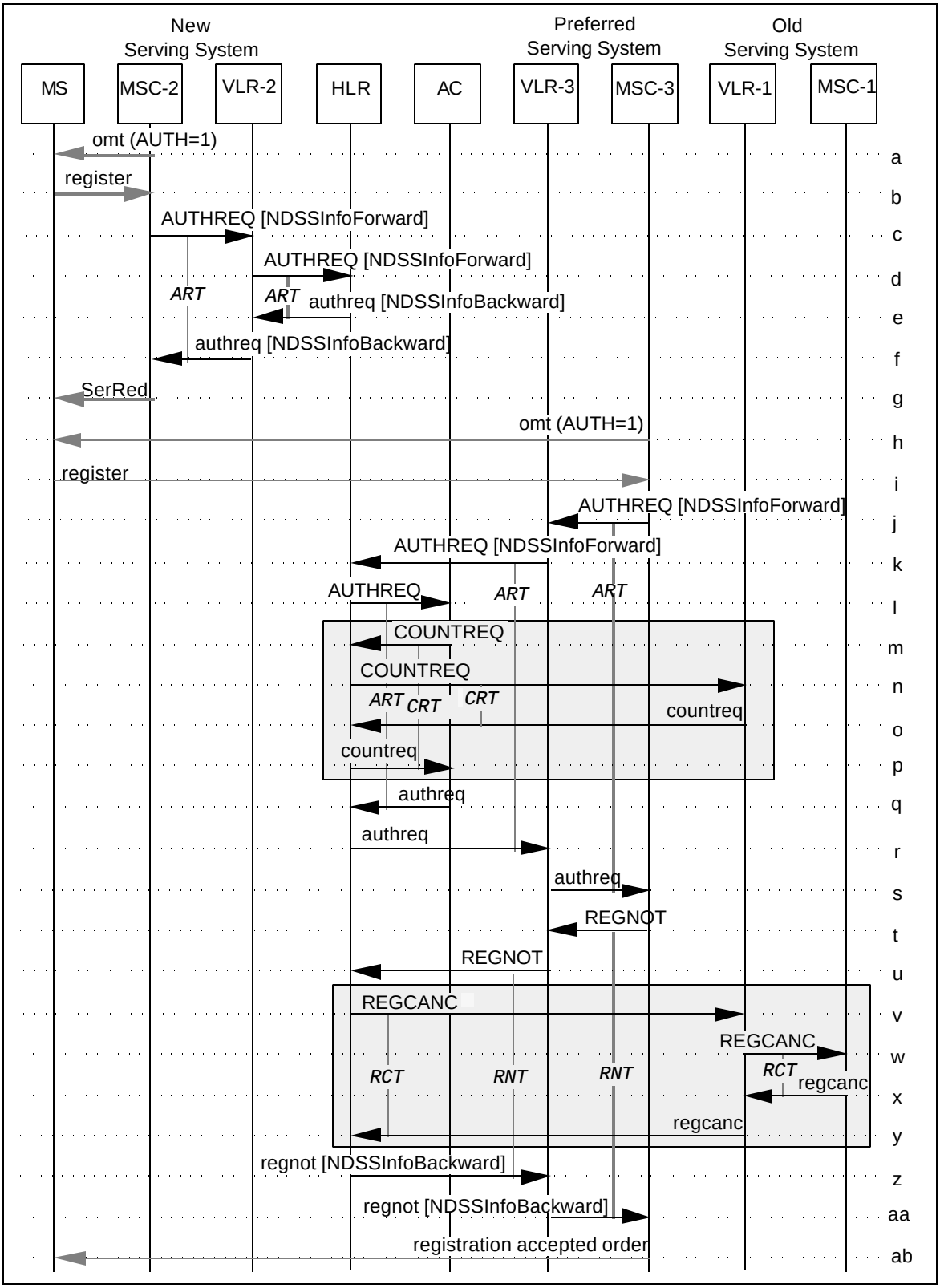

Figure 5.A.2-1 Initial Registration with Authentication

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. If it is not, a zero value is used by the MS as prescribed by TR-45 Authentication.

   The MS executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) and the RAND value to produce a registration Authentication Result (AUTHR).

b. The MS registers at the new Serving MSC (MSC-2), providing its MSID, ESN, AUTHR, CallHistoryCount (COUNT), and RANDC derived from the RAND used to compute AUTHR.

c. MSC-2 verifies RANDC supplied by the MS and sends the appropriate value of RAND in an AUTHREQ to the New Serving VLR (VLR-2).

d. VLR-2 forwards the AUTHREQ to the HLR associated with the MIN.

e. If the HLR determines that another system is preferable, MSC-2 is NDSS capable, and the subscriber has not suppressed the NDSS override of the MS's system selection procedure, the HLR sends an authreq message to the serving system (VLR-2) indicating an NDSS operation request and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter.

f. VLR-2, upon receipt of the authreq message specifying an NDSS operation, essentially removes all record of the MS from its memory if Return If Failed field of the ServiceRedirectionInfo parameter is disabled. VLR-2 sends an authreq message to MSC-2. If Return If Failed field of the ServiceRedirectionInfo parameter is enabled, VLR-2 may keep the authentication data related to this MS for a certain amount of time, in case the MS fails to find the re-directed system and registers again with authentication parameters within this period of time.

g. The MSC-2 sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system (MSC-3) and the RETURN_IF_FAIL field specification.

h. Upon receipt of the *Service Redirection* message, the MS scans and finds the specified preferred system (MSC-3) and performs registration.

   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 RandomVariable (RAND) to be used for authentication may also be obtained by the MS at this time. If it is not, a zero value is used by the MS as prescribed by TR-45 Authentication.

   The MS executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) and the RAND value to produce a registration Authentication Result (AUTHR).

i. The MS registers at the preferred Serving MSC (MSC-3), providing its MSID, ESN, AUTHR, CallHistoryCount (COUNT), and RANDC derived from the RAND used to compute AUTHR.

j. MSC-3 verifies RANDC supplied by the MS and sends the appropriate value of RAND in an AUTHREQ to the New Serving VLR (VLR-3).

k. VLR-3 forwards the AUTHREQ to the HLR associated with the MSID.

l. The HLR forwards the AUTHREQ to its AC.

m-p. If SSD is presently shared with another system, the AC shall perform validation of the MS as described in Section 5.4.8 (Authentication with sharing of SSD) of Chapter 3, *N.S0005-0 v 1.0* and go on to Step-q. below.

Otherwise, the AC verifies the MSID and ESN reported by the MS. The AC then executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) 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 then verifies that the COUNT received from the MS is consistent with the value currently stored at the AC.

q. The AC sends an `authreq` to the HLR. The `authreq` may include SSD and directives to issue a Unique Challenge, to update the MS SSD or to update the MS COUNT according to AC/HLR local administrative practices. These update procedures are described in Sections 5.4.6, 5.4.7, and 5.4.9 of Chapter 3, *TIA/EIA-41-D*. Alternatively, the `authreq` may include DenyAccess.

r. The HLR forwards the `authreq` to VLR-3.

s. VLR-3 forwards the `authreq` to the MSC-3.

t. Following successful authentication of the MS, MSC-3 sends a `REGNOT` to VLR-3.

u. VLR-3 forwards the `REGNOT` to the HLR.

v. If the MS was previously registered in another system, the HLR sends a `REGCANC` to the Old Serving VLR (VLR-1).

w. VLR-1 forwards the `REGCANC` to the Old Serving MSC (MSC-1).

x. MSC-1 returns a `regcanc` to VLR-1.

y. VLR-1 returns a `regcanc` to the HLR.

z. The HLR records the new location of the MS in its local memory and responds to the `REGNOT` with a `regnot` that includes the information requested by VLR-3.

aa. VLR-3 forwards the `regnot` to MSC-3.

ab. MSC-3 sends the *Registration Accepted Order* to the MS.

5.B NDSS at Call Origination - Successful Scenarios

This section illustrates some typical implicit MS registration scenarios at call origination which occurs prior to any registration process, i.e.,

- Call Origination without Authentication
- Call Origination with Authentication
- Call Origination without Profile

It is also understood that the following scenarios may also apply to the other implicit registration case (i.e., page response message) with appropriate modifications. Furthermore, subsequent call originations shall follow normal *N.S0005-0 v 1.0* call origination procedures.

5.B.1 Call Origination without Authentication

This scenario describes the case when the mobile originates in a visited system without prior registration with the system, and while accessing the visited system, it is directed by its home service provider to a preferred roaming system. Furthermore, in this case both the visited system and the preferred system do not require authentication.

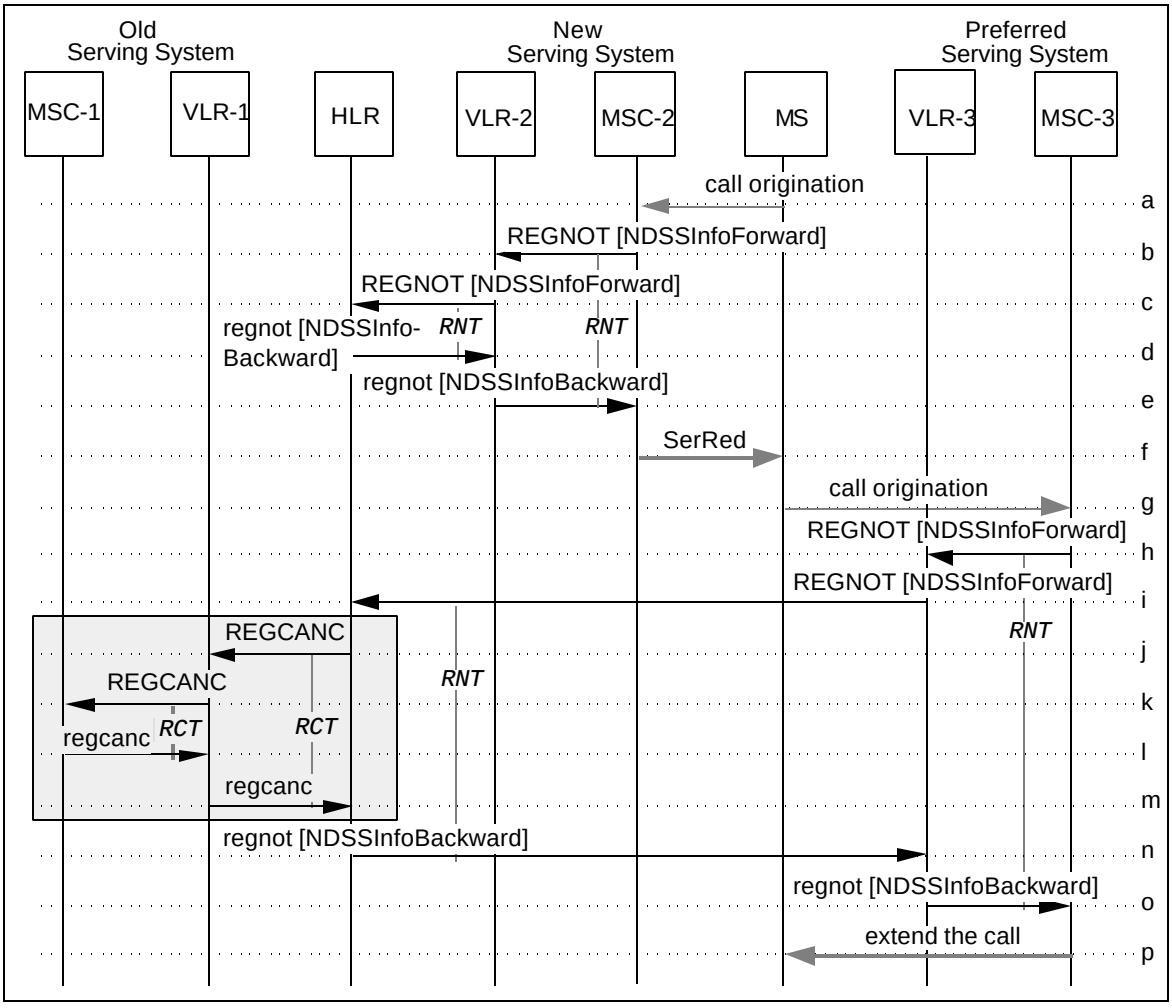

Figure 5.B.1-1 Call Origination without Authentication

a. The MS scans and finds a new serving system and sends an *Origination* message to the New Serving MSC (MSC-2).

b. The New Serving MSC (MSC-2) sends a `REGNOT` to its VLR (VLR-2).

c. VLR-2 sends a `REGNOT` to the HLR associated with the MS. Note that the RegistrationNotification response from the VLR to the MSC is contingent upon the response received from the HLR.

d. If the HLR determines that another system is preferable, MSC-2 is NDSS capable, and the subscriber has not suppressed the NDSS override of the MS's system selection procedure, the HLR sends a `regnot` message to the serving system (VLR-2) indicating an NDSS operation request and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter. The HLR may choose not to send MS service profiles in `regnot`. The HLR may not perform location updating since the MSC is not authorized for service.

e. VLR-2, upon receipt of the `regnot` message specifying an NDSS operation, essentially removes all record of the MS from its memory if Return If Failed field of the ServiceRedirectionInfo parameter is disabled. VLR-2 sends `regnot` message to MSC-2.

f. The MSC-2 sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system (MSC-3) and the RETURN_IF_FAIL field specification.

   Alternatively, if Return If Failed field of the ServiceRedirectionInfo parameter is enabled, MSC-2 may choose to extend the call instead of redirecting the MS, and thus skip the following steps.

g. Upon receipt of the *Service Redirection* message, the MS scans and finds the specified preferred system (MSC-3) and automatically sends an *Origination* message to the New Serving MSC (MSC-3).

h. The preferred Serving MSC (MSC-3) sends a `REGNOT` to its VLR (VLR-3).

i. VLR-3 sends a `REGNOT` to the HLR associated with the MS. Note that the RegistrationNotification response from the VLR to the MSC is contingent upon the response received from the HLR.

j. If the MS was previously registered elsewhere, the HLR sends a `REGCANC` to the previously visited VLR (VLR-1). That VLR, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

k. VLR-1 sends a `REGCANC` to the previously visited MSC (MSC-1). That MSC, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

l. MSC-1 sends a `regcanc` to VLR-1.

m. VLR-1 sends a `regcanc` to the HLR.

n. The HLR sends a `regnot` to VLR-3.

o. VLR-3 forwards the `regnot` to MSC-3.

p. The Serving MSC (MSC-3) then continues with call origination.

5.B.2 Call Origination with Authentication

This scenario describes the intersystem message flow required to support authentication when the initial access in the visited system is a call origination, and when the mobile is being directed to a preferred roaming system by the visited system.

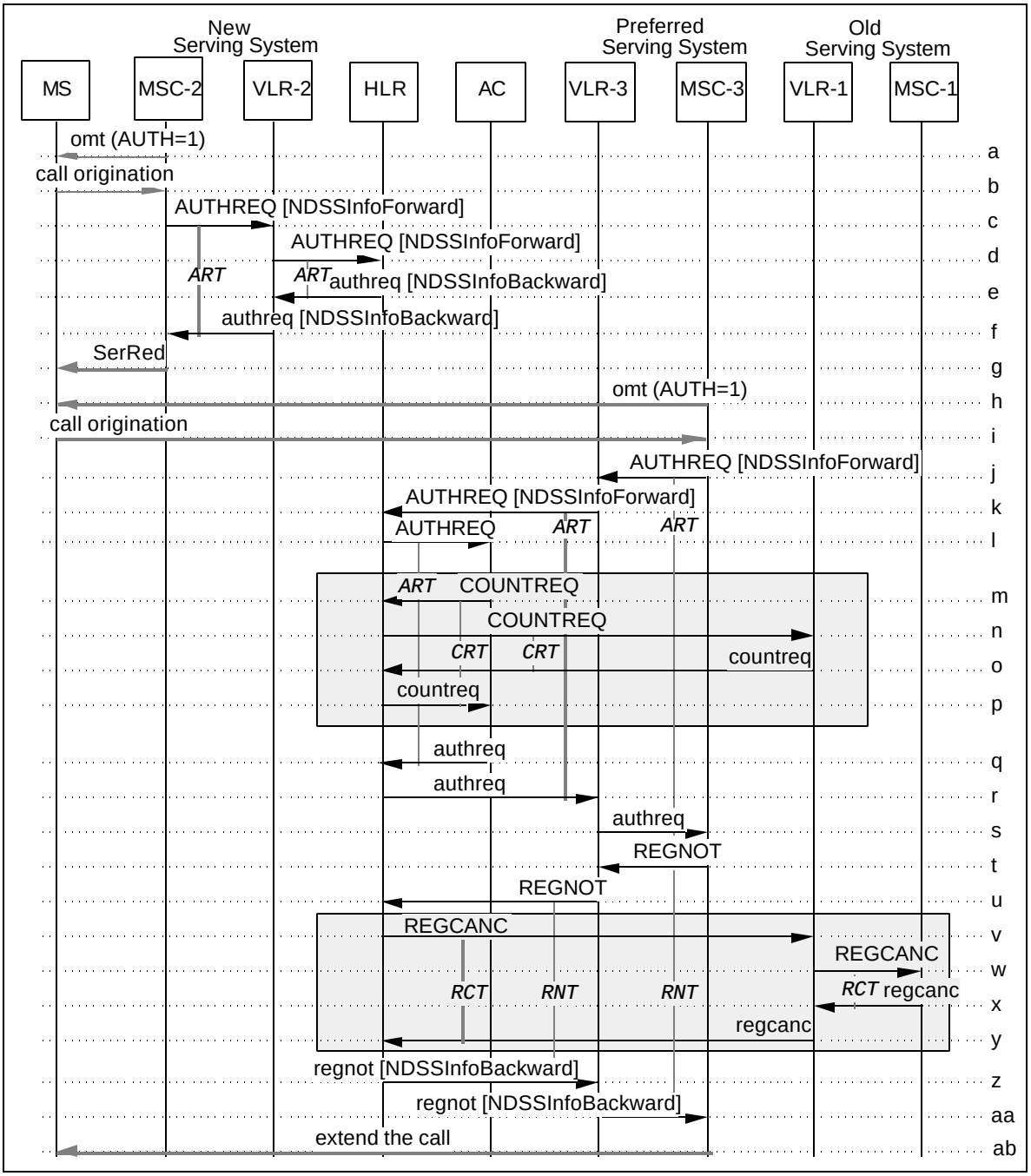

Figure 5.B.2-1 Call Origination with Authentication

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 RandomVariable (RAND) to be used for authentication may also be obtained by the MS at this time. If it is not, a zero value is used by the MS as prescribed by TR-45 Authentication.

   The MS executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) and the RAND value to produce a registration Authentication Result (AUTHR).

b. The MS sends an *Origination* message to the New Serving MSC (MSC-2), providing the dialed digits, its MSID, ESN, Authentication Result (AUTHR), CallHistoryCount (COUNT) and the RANDC from the RAND used to compute AUTHR.

c. MSC-2 verifies RANDC supplied by the MS and sends the appropriate value of RAND in an `AUTHREQ` to the New Serving VLR (VLR-2).

d. VLR-2 forwards the `AUTHREQ` to the HLR associated with the MSID.

e. If the HLR determines that another system is preferable, MSC-2 is NDSS capable, and the subscriber has not suppressed the NDSS override of the MS's system selection procedure, the HLR sends an `authreq` message to the serving system (VLR-2) indicating an NDSS operation request and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter.

f. VLR-2, upon receipt of the `authreq` message specifying an NDSS operation, essentially removes all record of the MS from its memory if Return If Failed field of the ServiceRedirectionInfo parameter is disabled. VLR-2 sends an `authreq` message to MSC-2. If Return If Failed field of the ServiceRedirectionInfo parameter is enabled, VLR-2 may keep the authentication data related to this MS for a certain amount of time, in case the MS fails to find the re-directed system and registers again with authentication parameters within this period of time.

g. The MSC-2 sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system (MSC-3) and the Return If Failed field specification.

   Alternatively, if Return If Failed field of the ServiceRedirectionInfo parameter is enabled, MSC-2 may choose to extend the call instead of redirecting the MS, and thus skip the following steps.

h. Upon receipt of the *Service Redirection* message, the MS scans and finds the specified preferred system (MSC-3) and performs registration.

   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 RandomVariable (RAND) to be used for authentication may also be obtained by the MS at this time. If it is not, a zero value is used by the MS as prescribed by TR-45 Authentication.

   The MS executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) and the RAND value to produce a registration Authentication Result (AUTHR).

i. The MS sends an *Origination* message to the New Serving MSC (MSC-3), providing the dialed digits, its MSID, ESN, Authentication Result (AUTHR), CallHistoryCount (COUNT) and the RANDC from the RAND used to compute AUTHR.

j. MSC-3 verifies RANDC supplied by the MS and sends the appropriate value of RAND in an `AUTHREQ` to the New Serving VLR (VLR-3).

k. VLR-3 forwards the AUTHREQ to the HLR associated with the MSID.

l. The HLR forwards the AUTHREQ to its AC.

m-p. If SSD is presently shared with another system, the AC shall perform validation of the MS as described in Section 5.4.8 (Authentication with sharing of SSD) of Chapter 3, *N.S0005-0 v 1.0* and go on to Step-q. below.

Otherwise, the AC verifies the MSID and ESN reported by the MS. The AC then executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) 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 then verifies that the COUNT received from the MS is consistent with the value currently stored at the AC.

q. The AC sends an authreq to the HLR. The authreq may include SSD and directives to issue a Unique Challenge, to update the MS SSD or to update the MS COUNT according to AC/HLR local administrative practices. These update procedures are described in Sections 5.4.6, 5.4.7, and 5.4.9 of Chapter 3, *TIA/EIA-41-D*. Alternatively, the authreq may include DenyAccess.

r. The HLR forwards the authreq to VLR-3.

s. VLR-3 forwards the authreq to the MSC-3.

t. Following successful authentication of the MS, MSC-3 sends a REGNOT to VLR-3.

u. VLR-3 forwards the REGNOT to the HLR.

v. If the MS was previously registered in another system, the HLR sends a REGCANC to the Old Serving VLR (VLR-1).

w. VLR-1 forwards the REGCANC to the Old Serving MSC (MSC-1).

x. MSC-1 returns a regcanc to VLR-1.

y. VLR-1 returns a regcanc to the HLR.

z. The HLR records the new location of the MS in its local memory and responds to the REGNOT with a regnot that includes the information requested by VLR-3.

aa. VLR-3 forwards the regnot to MSC-3.

ab. The Serving MSC (MSC-3) then continues with call origination.

5.B.3 NDSS Call Origination without Profile

This scenario describes the case when call origination is attempted by a registered MS without the profile being present in the Serving MSC. The request for the profile results in a service redirection from the HLR.

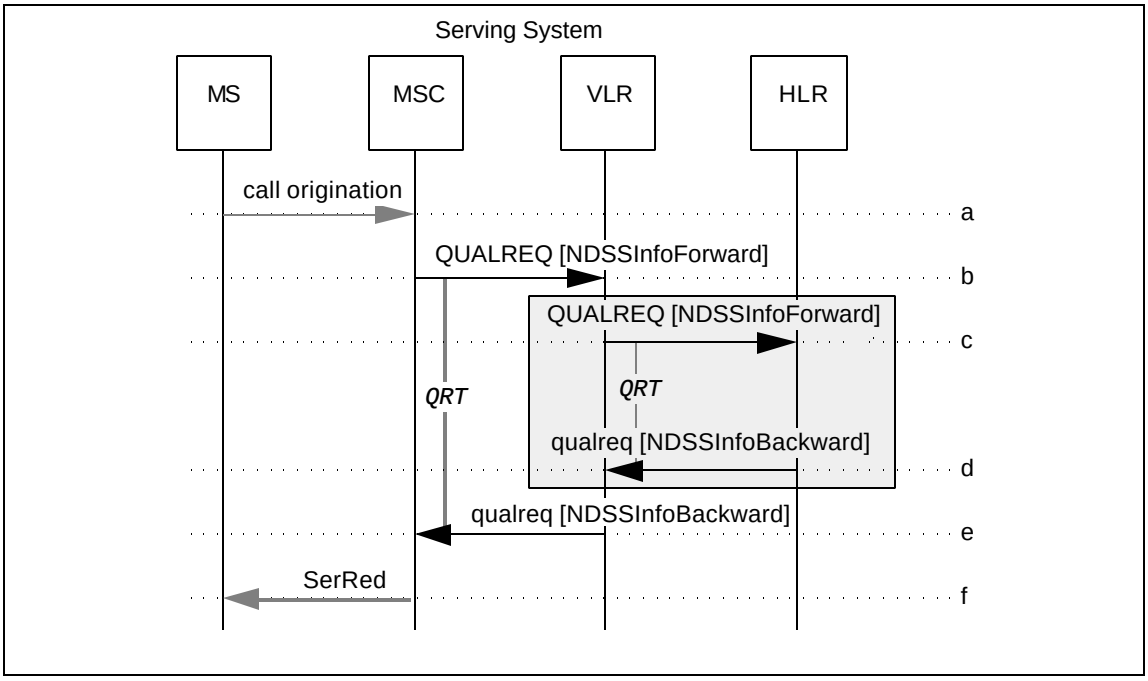

Figure 5.B.3-1 NDSS Call Origination without Profile

a. The Serving MSC receives a call origination from the served MS.

b. If the service profile of the MS is unknown to the MSC, it sends a `QUALREQ` to the VLR.

c. If the service profile of the MS is unknown to the VLR, it sends a `QUALREQ` to the HLR associated with the MS.

d. If the HLR determines that another system is preferable, the MSC is NDSS capable, and the subscriber has not suppressed the NDSS override of the MS's system selection procedure, the HLR sends a `qualreq` message to the Serving VLR indicating an NDSS operation request and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter. The HLR may choose not to send MS service profile information. The HLR may not perform location updating since the MSC is not authorized for service.

e. The VLR sends a `qualreq` to the Serving MSC, including the MS's service profile information if it is available.

f. The MSC sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system and the Return If Failed field specification.

5.B.4 NDSS Feature Suppression

This scenario describes the case when the user requests a suppression of the NDSS feature.

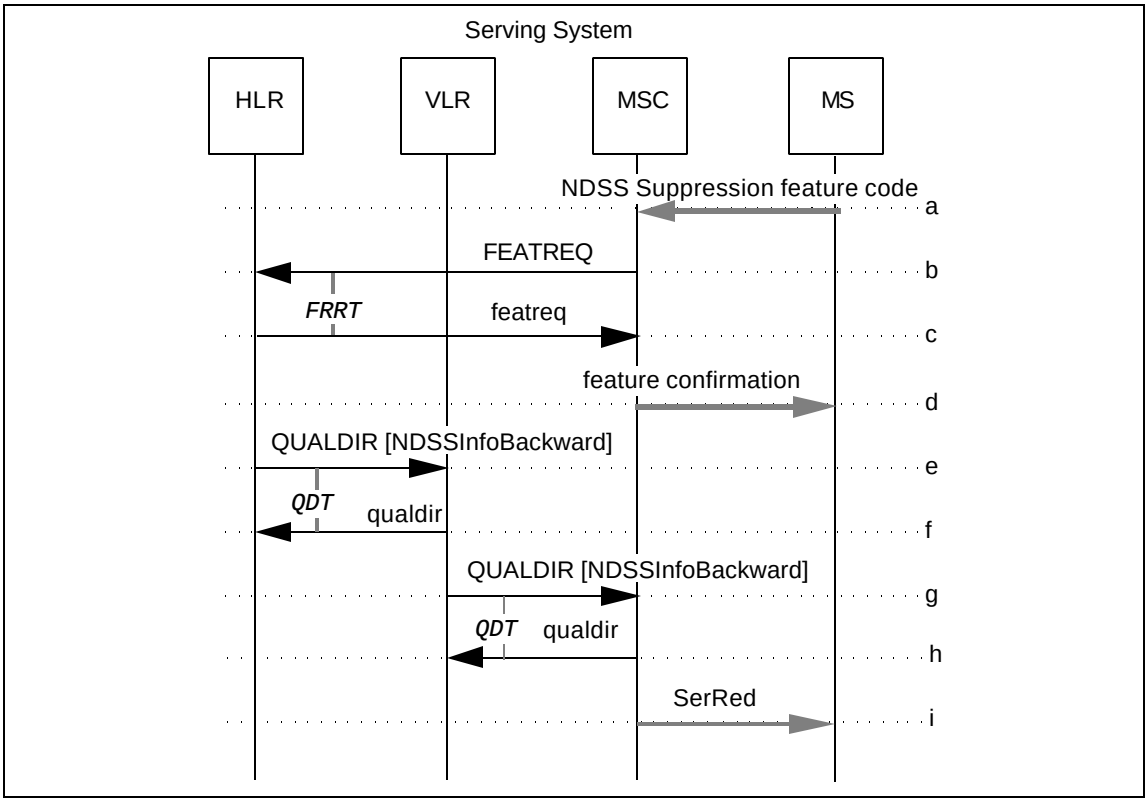

Figure 5.B.4-1 NDSS Feature Suppression

a-d. Normal FeatureRequest operation (FEATREQ, see Chapter 3, Section 4.9, *TIA/EIA-41-D*) applies when the user requests a suppression of the NDSS feature.

e. The HLR sends a `QUALDIR` to the Serving VLR indicating the suppression of NDSS.

f. The Serving VLR sends an empty `qualdir` to the HLR.

g. The Serving VLR forwards the `QUALDIR` message to the Serving MSC.

h. The Serving MSC sends an empty `qualdir` to the Serving VLR.

i. The Serving MSC sends a *Service Redirection* message to the MS, indicating the suppression of NDSS. The MS may perform initialization in accordance with its custom system selection procedure.

5.B.5 NDSS Feature Activation

This scenario describes the case when the user requests an Activation of the NDSS Feature Suppression requested earlier by the user.

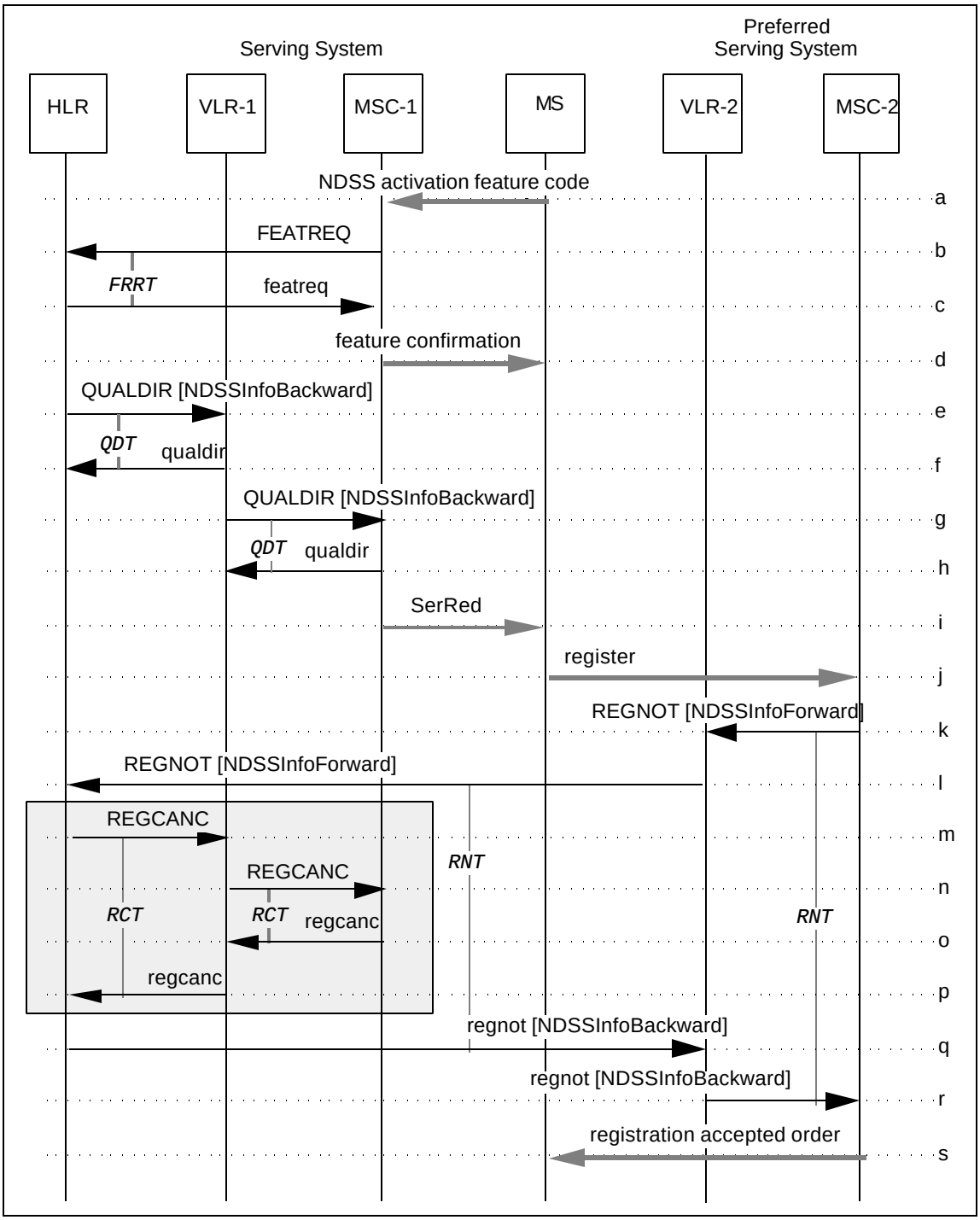

Figure 5.B.5-1 NDSS Feature Activation

a-d. Normal FeatureRequest operation (FEATREQ, see Chapter 3, Section 4.9,*TIA/EIA-41-D*) applies when the user requests an activation of the NDSS feature.

e. If the HLR determines that another system is preferable and MSC-1 is NDSS capable, the HLR sends a QUALDIR message to the serving system (VLR-1) indicating an NDSS operation request, and specifying the RedirectRecord and Return If Failed field of the ServiceRedirectionInfo parameter. The HLR may choose not to send MS service profiles in QUALDIR.

f. The VLR-1 sends an empty qualdir to the HLR.

g. The VLR-1 sends a QUALDIR message to the MSC-1.

h. The MSC-1 sends an empty qualdir to the VLR-1.

Once the NDSS feature is activated the MS shall be redirected following a subsequent registration. Redirection based on NDSS shall not impact calls in progress.

i. The MSC-1 sends a *Service Redirection* message to the MS, to provide the MS information about the preferred system (MSC-2) and the Return If Failed field specification.

j. Upon receipt of the *Service Redirection* message, the MS scans and finds the specified preferred system (MSC-2) and performs registration.

k. The preferred Serving MSC (MSC-2) sends a REGNOT to its VLR (VLR-2).

l. VLR-2 sends a REGNOT to the HLR associated with the MS. Note that the RegistrationNotification response from the VLR to the MSC is contingent upon the response received from the HLR.

m. Since the MS was previously registered elsewhere, the HLR sends a REGCANC to the previous Serving VLR (VLR-1). That VLR, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

n. VLR-1 sends a REGCANC to the previous Serving MSC (MSC-1). That MSC, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

o. MSC-1 sends a regcanc to VLR-1.

p. VLR-1 sends a regcanc to the HLR.

q. The HLR sends a regnot to VLR-2.

r. VLR-2 sends a regnot to MSC-2.

s. MSC-2 sends the *Registration Accepted Order* to the MS.

5.C NDSS - Failure Operations

In this section, NDSS failure cases are discussed.

5.C.1 No Preferred System Found

When the MS cannot find the new system to which it was directed, the MS should check the RETURN_IF_FAIL bit in the *Service Redirection* message. If the bit is enabled, the MS should attempt registration with the original serving system, and indicate this condition. If the bit is disabled, the MS may try to find another system, other than the originating system.

5.C.2 Registration Rejection from the Directed System

When the MS receives a registration rejection from the new system to which it was directed, the MS should check the RETURN_IF_FAILED bit in the *Service Redirection* message. If the bit is enabled, the MS should attempt registration with the original serving system, and indicate this condition. If the bit is disabled, the MS may try to find another system, other than the originating system.

5.C.3 Directed System with a Wrong SID/NID

When the MS finds, upon service redirection, a system whose SID or NID does not match the SID or NID in the *Service Redirection* message, the MS should check the RETURN_IF_FAIL bit in the *Service Redirection* message. If the bit is enabled, the MS should attempt registration with the original serving system, and indicate this condition. If the bit is disabled, the MS may try to find another system, other than the originating system.

5.D TMSI Registration

(*N.S0005-0 v 1.0* Chapter 3, Page 171)

This section illustrates examples of typical explicit MS initial registration scenarios, as:

- Initial Registration.
- Initial Registration with Authentication.

5.D.1 Normal Registration with TMSI_CODE

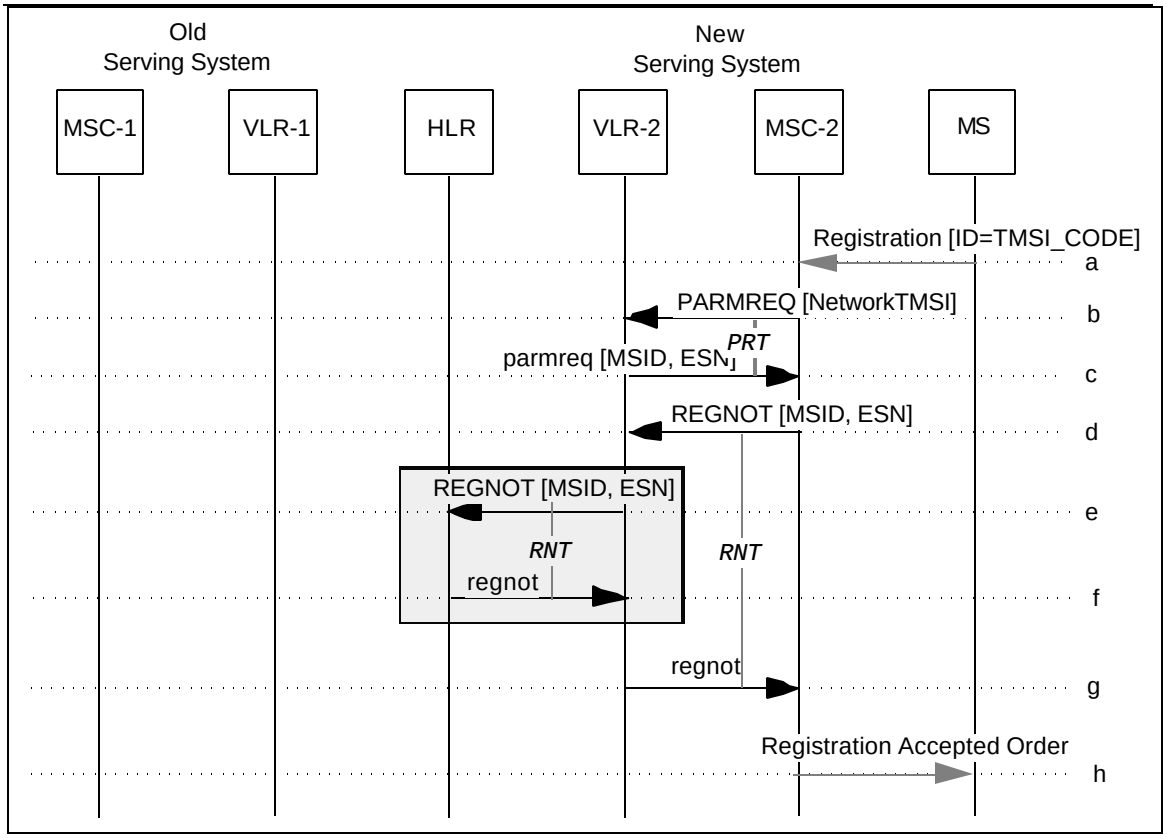

Figure 5.D.1-1 Normal Registration with TMSI_CODE

a. When the MS determines that the TMSI_ZONE broadcast by the BS is equal to the TMSI_ZONE stored in MS, the MS then sends *Registration* message to the Serving MSC (MSC-2), providing its TMSI_CODE only.

b. MSC-2 determines that additional parameters are required. According to the known ID information (e.g., TMSI_CODE) it sends a `PARMREQ` to the Serving VLR (VLR-2) to get the required parameters (e.g., IMSI or MIN and ESN).

c. VLR-2 determines that it can provide the required parameters and then returns a `parmreq` containing the requested information to the MSC-2.

d. Then MSC-2 sends a `REGNOT` to VLR-2.

e. In this case the NetworkTMSI is known to VLR-2. If the information requested by MSC-2 is not available at VLR-2, VLR-2 then sends a `REGNOT` to the HLR associated with the MS.

f. The HLR sends a `regnot` to VLR-2.

g. VLR-2 sends a `regnot` to MSC-2.

h. MSC-2 sends a *Registration Accept Order* to the MS.

5.D.2 Normal Registration with Full TMSI

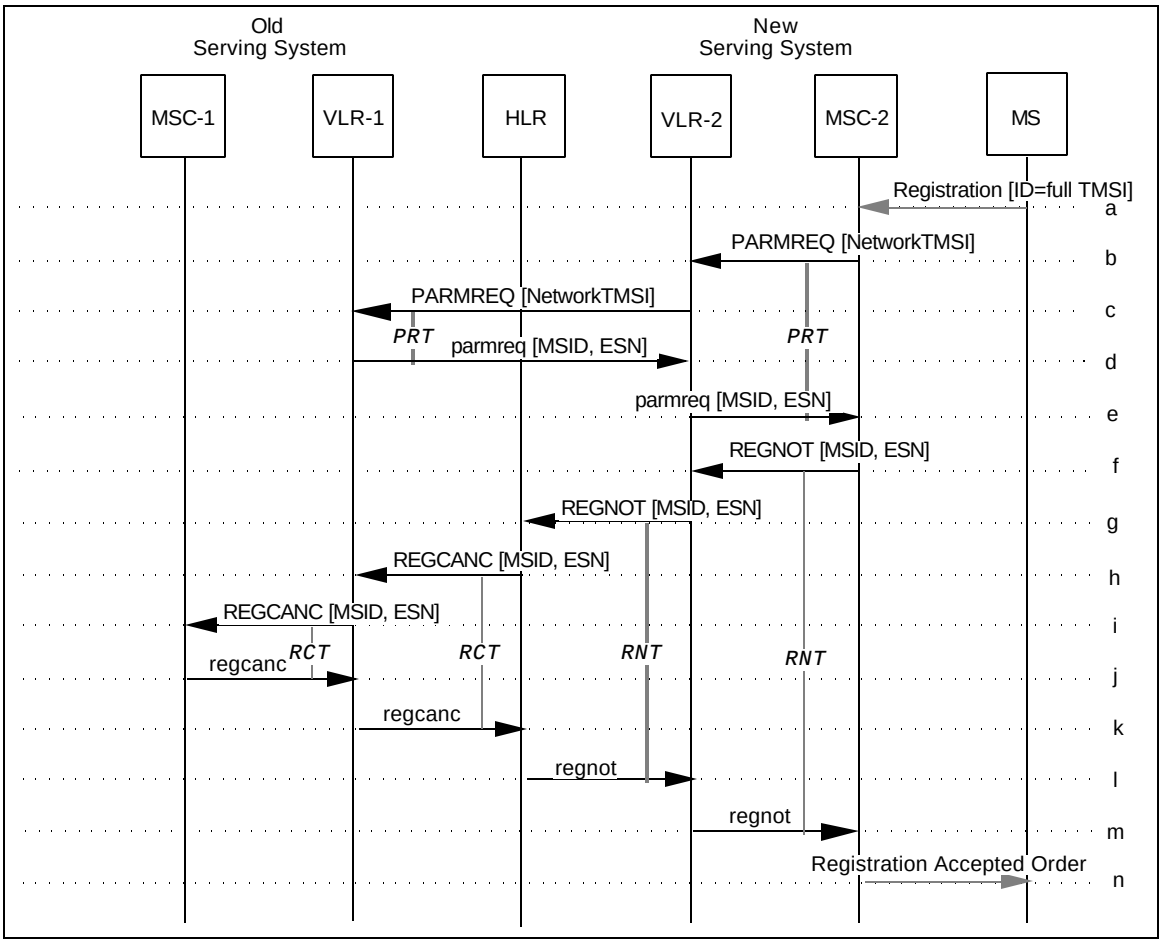

Figure 5.D.2-1 Normal Registration with Full TMSI

a. When the MS determines that the TMSI_ZONE broadcast by the BS is not equal to the TMSI_ZONE which is stored in MS, the MS then sends *Registration* message to the Serving MSC (MSC-2), providing its full TMSI.

b. MSC-2 determines that additional parameters are required. According to the known ID information (e.g., NetworkTMSI) it sends a `PARMREQ` to the Serving VLR (VLR-2) to get the required parameters (e.g., IMSI and ESN).

c. In this scenario the NetworkTMSI is unknown to VLR-2, therefore, VLR-2 then sends a `PARMREQ` to the Old Serving VLR (i.e., VLR-1, which previously assigned the NetworkTMSI) according to TMSI_ZONE field of the NetworkTMSI parameter.

d. VLR-1 sends a `parmreq` to VLR-2, including the MS's MSID (e.g., IMSI) and ESN.

e. VLR-2 sends a `parmreq` to MSC-2.

f. MSC-2 sends a REGNOT to VLR-2.

g. VLR-2 sends a REGNOT to the HLR associated with the MS.

h. HLR sends a REGCANC to the previously visited VLR (VLR-1). VLR-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

i. VLR-1 sends a REGCANC to the previously visited MSC (MSC-1). MSC-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

j. MSC-1 sends a regcanc to VLR-1.

k. VLR-1 sends a regcanc to the HLR.

l. The HLR sends a regnot to VLR-2.

m. VLR-2 sends a regnot to MSC-2.

n. MSC-2 sends a *Registration Accept Order* to the MS.

5.D.3 Normal Registration with Full TMSI (Unavailable at VLR)

This scenario describes a normal registration with the full TMSI which is inaccessible or unsuccessful at the prior Serving VLR.

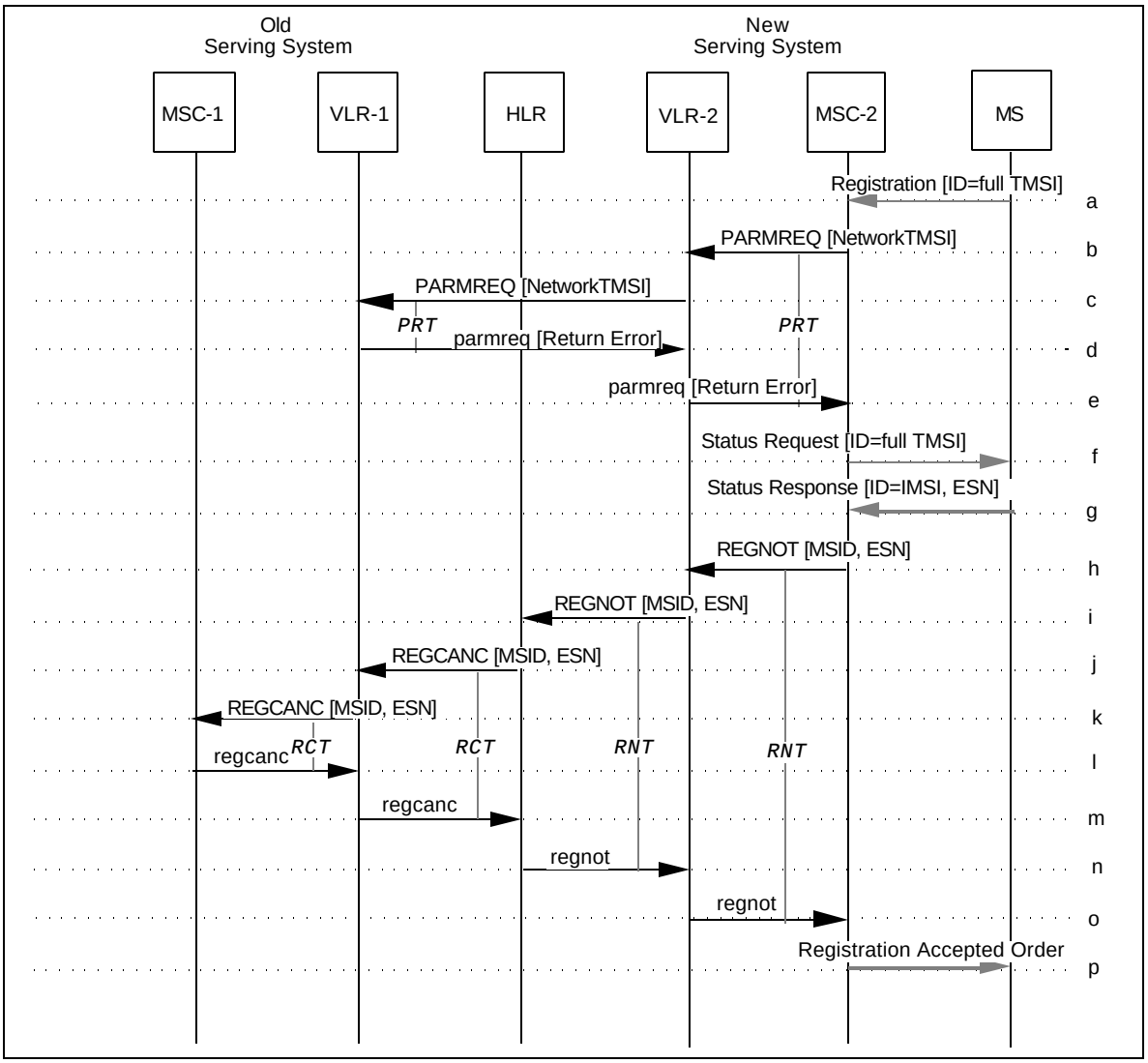

Figure 5.D.3-1 Normal Registration with Full TMSI (Unavailable at VLR)

a-c. Same as Section 5.D.2 Steps a-c.

If the Old Serving VLR is inaccessible by the serving system, skip Steps-c and d and go to Step-e.

d. VLR-1 sends a `parmreq` to VLR-2 with `RETURN ERROR`, indicating that the access to the Old Serving VLR is unsuccessful.

e. VLR-2 sends `parmreq` to MSC-2 with `RETURN ERROR`.

f. MSC-2 sends the *Status Request* message on the air interface to request the IMSI and ESN from MS.

g. MS sends the *Status Response* message to MSC-2, including MS's IMSI and ESN.

h. MSC-2 sends a REGNOT to VLR-2, including MS's IMSI and ESN.

i. VLR-2 sends a REGNOT to the HLR associated with the MS.

j. HLR sends a REGCANC to the previously visited VLR (VLR-1). VLR-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

k. VLR-1 sends a REGCANC to the previously visited MSC (MSC-1). MSC-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

l. MSC-1 sends a regcanc to VLR-1.

m. VLR-1 sends a regcanc to the HLR.

n. The HLR sends a regnot to VLR-2.

o. VLR-2 sends a regnot to MSC-2.

p. MSC-2 sends a *Registration Accept Order* to the MS.

5.D.4 Normal Registration with Full TMSI (Full-TMSI Timer expired)

This scenario describes a normal registration with the full TMSI following the expiration of the Full-TMSI Timer.

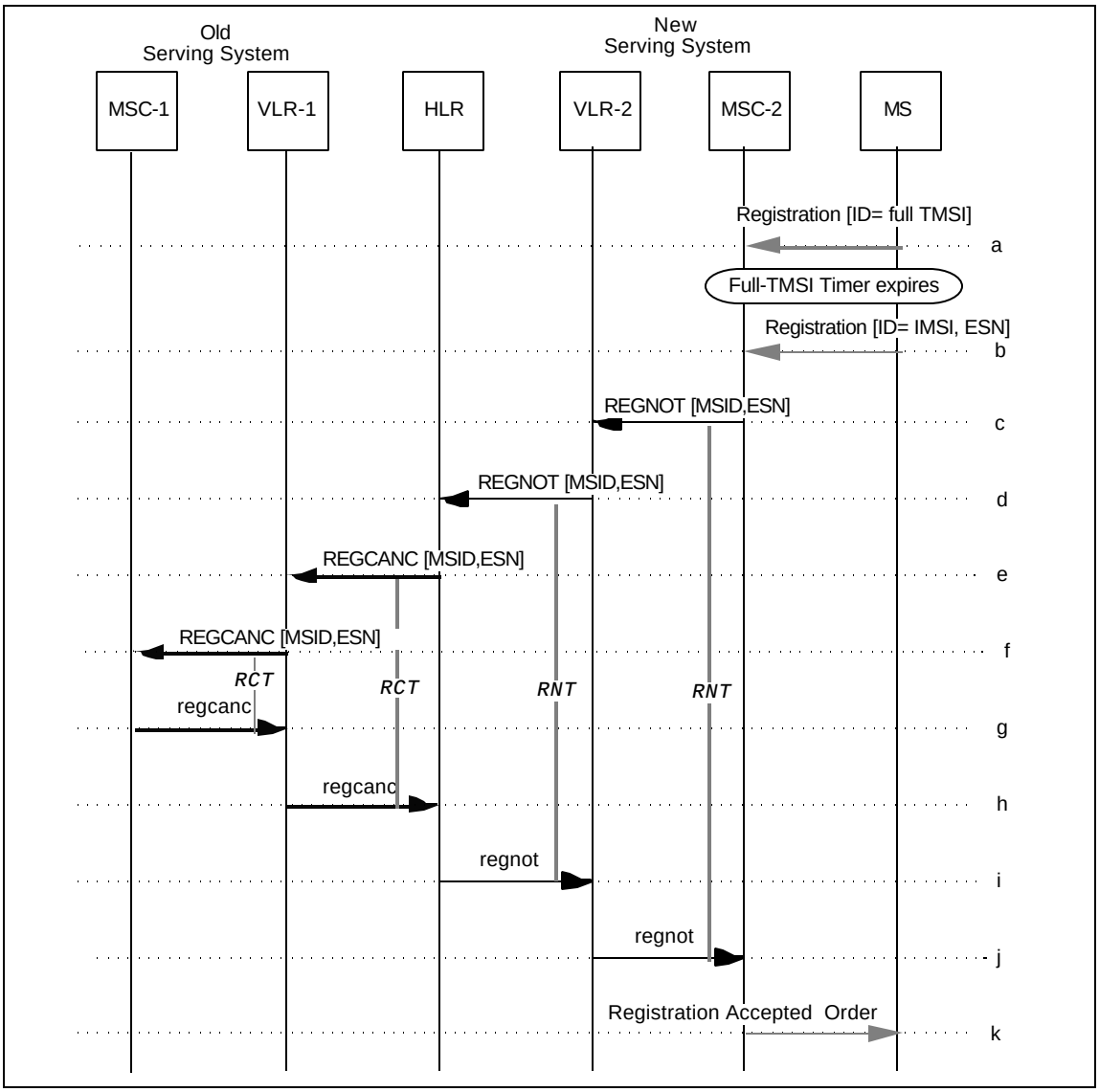

Figure 5.D.4-1 Normal Registration with Full TMSI (Full-TMSI Timer expired)

a. When the MS determines that the TMSI_ZONE broadcast by the BS is not equal to the TMSI_ZONE which is stored in MS, the MS then sends *Registration* message to the Serving MSC (MSC-2), providing its full TMSI. At the same time, the MS starts the Full-TMSI TIMER awaiting a new NetworkTMSI assignment by the New Serving VLR (VLR-2).

b. If the Full-TMSI TIMER expires before a new NetworkTMSI is assigned, the MS then deletes the TMSI and sends *Registration* message again to the Serving MSC using its IMSI and ESN.

Note: If the Full-TMSI TIMER expires and the MS registers with the only IMSI, the network can send the *Status Request* message to the MS to obtain ESN.

c-k. Same as Section 5.D.3, Steps h-p.

5.D.5 Normal Registration with Full TMSI (Service Redirection)

This scenario describes a normal registration with full TMSI, re-directed by MS's home service provider to a preferred serving system.

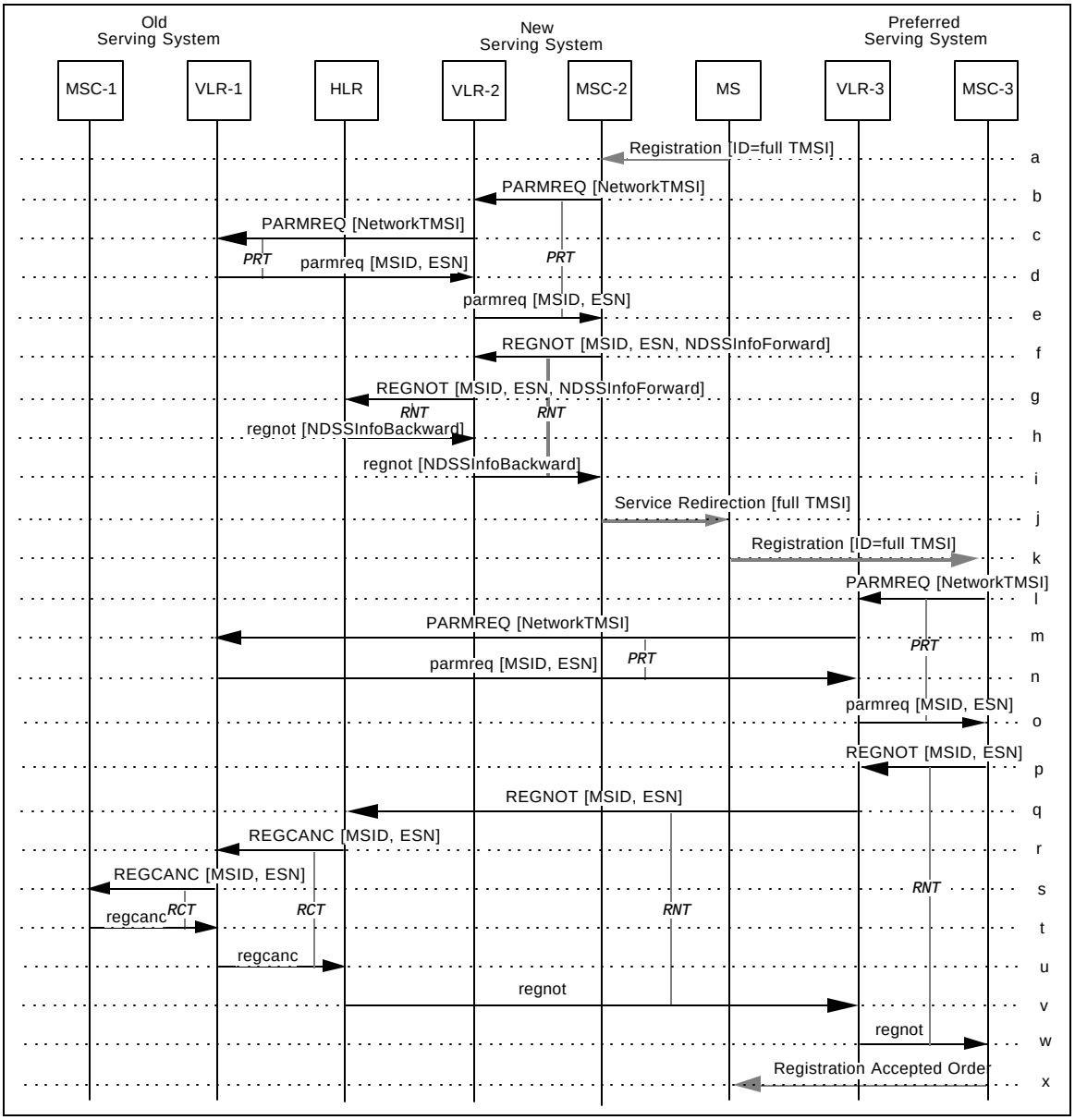

Figure 5.D.5-1 Normal Registration with Full TMSI (Service Redirection)

a-g. Same as Section 5.D.2, Steps a-g.

h. If the HLR determines that another system is preferable, HLR sends a `regnot` to VLR-2 indicating the preferred system.

i. VLR-2 sends `regnot` message to MSC-2. If Return If Failed field of the ServiceRedirectionInfo parameter is disabled, VLR-2 essentially removes all record of the MS.

j. MSC-2 sends *Service Redirection* message to the MS over the air interface.

k. The MS, upon receipt of the message, scans and accesses the specified system (MSC-3) and sends *Registration* message with the same full TMSI to the MSC-3.

l. MSC-3 determines that additional parameters are required. According to the known ID information (e.g., NetworkTMSI) it sends a PARMREQ to the Serving VLR (VLR-3) to get the required parameters (e.g., IMSI and ESN).

m. If the NetworkTMSI is unknown to VLR-3, it then sends a PARMREQ to the Old Serving VLR (i.e., VLR-1, which previously assigned the NetworkTMSI) according to TMSI_ZONE.

n. VLR-1 sends a parmreq to VLR-3 including the MS's MSID (e.g., IMSI) and ESN.

o. VLR-3 sends a parmreq to MSC-3.

p. MSC-3 sends a REGNOT to VLR-3.

q. VLR-3 sends a REGNOT to the HLR associated with the MS.

r. HLR sends a REGCANC to the previously visited VLR (VLR-1). VLR-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

s. VLR-1 sends a REGCANC to the previously visited MSC (MSC-1). MSC-1, upon receipt of the cancellation message, essentially removes all record of the MS from its memory.

t. MSC-1 sends a regcanc to VLR-1.

u. VLR-1 sends a regcanc to the HLR.

v. The HLR sends a regnot to VLR-3.

w. VLR-3 sends a regnot to MSC-3.

x. MSC-3 sends a *Registration Accept Order* to the MS.

5.E TMSIDirective

(*N.S0005-0 v 1.0* Chapter 3, page 171)

This scenario describes the assignment of a new NetworkTMSI.

5.E.1 Successful TMSIDirective

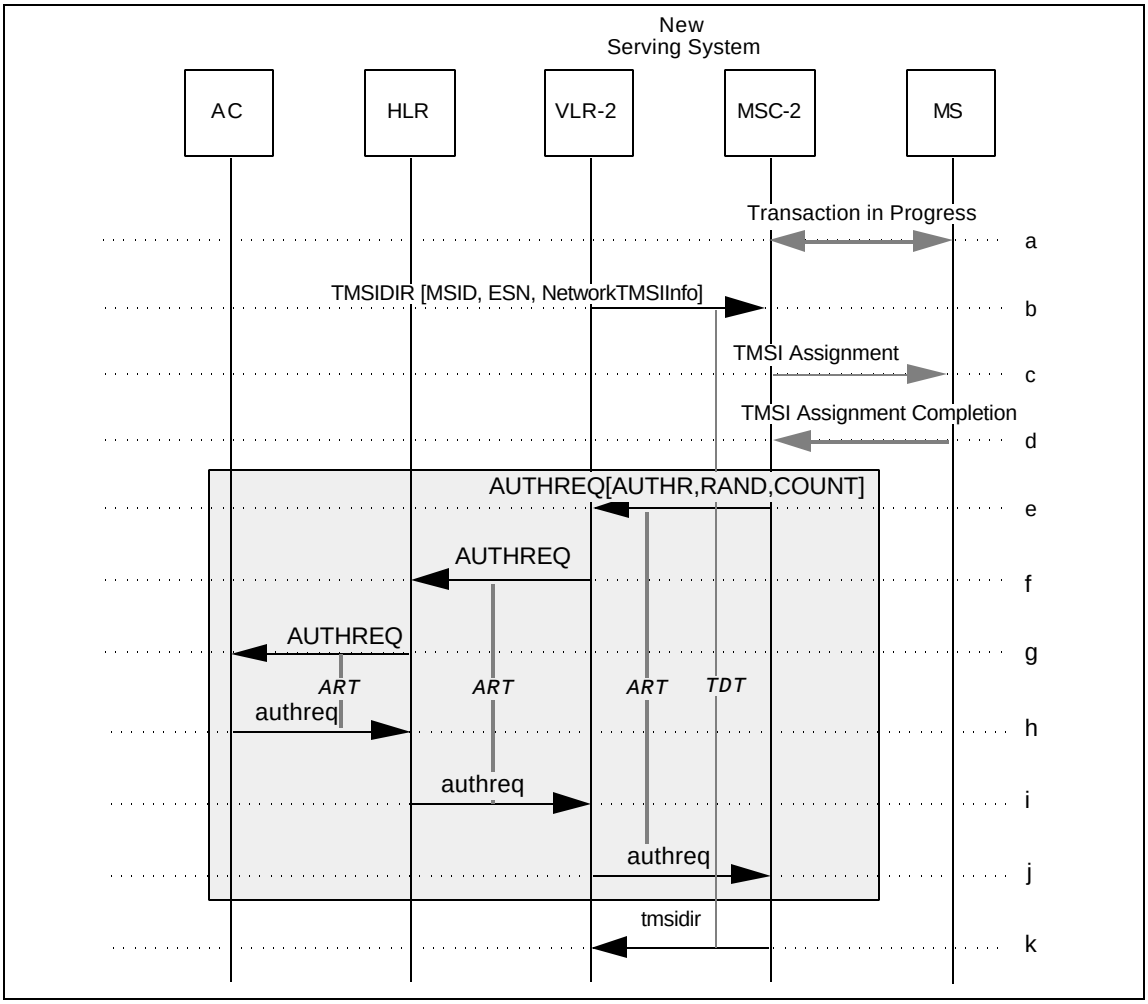

Figure 5.E.1-1 SuccessfulTMSIDirective

a. The MS is on either the paging channel or traffic channel (i.e., either idle or in a call).

b. Based on internal algorithms, VLR-2 sends a `TMSIDIR` to MSC-2. The serving system may start the TMSIDirective procedure at any time after MS's identification information has been obtained.

c. MSC-2 sends *TMSI Assignment* message to the MS over the air interface.

d. MS sends *TMSI Assignment Completion* message to the Serving MSC.

e-j. Authentication procedures may be executed only if the *TMSI Assignment Completion* message received from the access channel includes AUTHR, RANDC and COUNT. If MS is on the traffic channel, go to Step- k.

k. MSC-2 sends a `tmsidir` to VLR-2.

5.E.2 Unsuccessful TMSIDirective with MS failed authentication

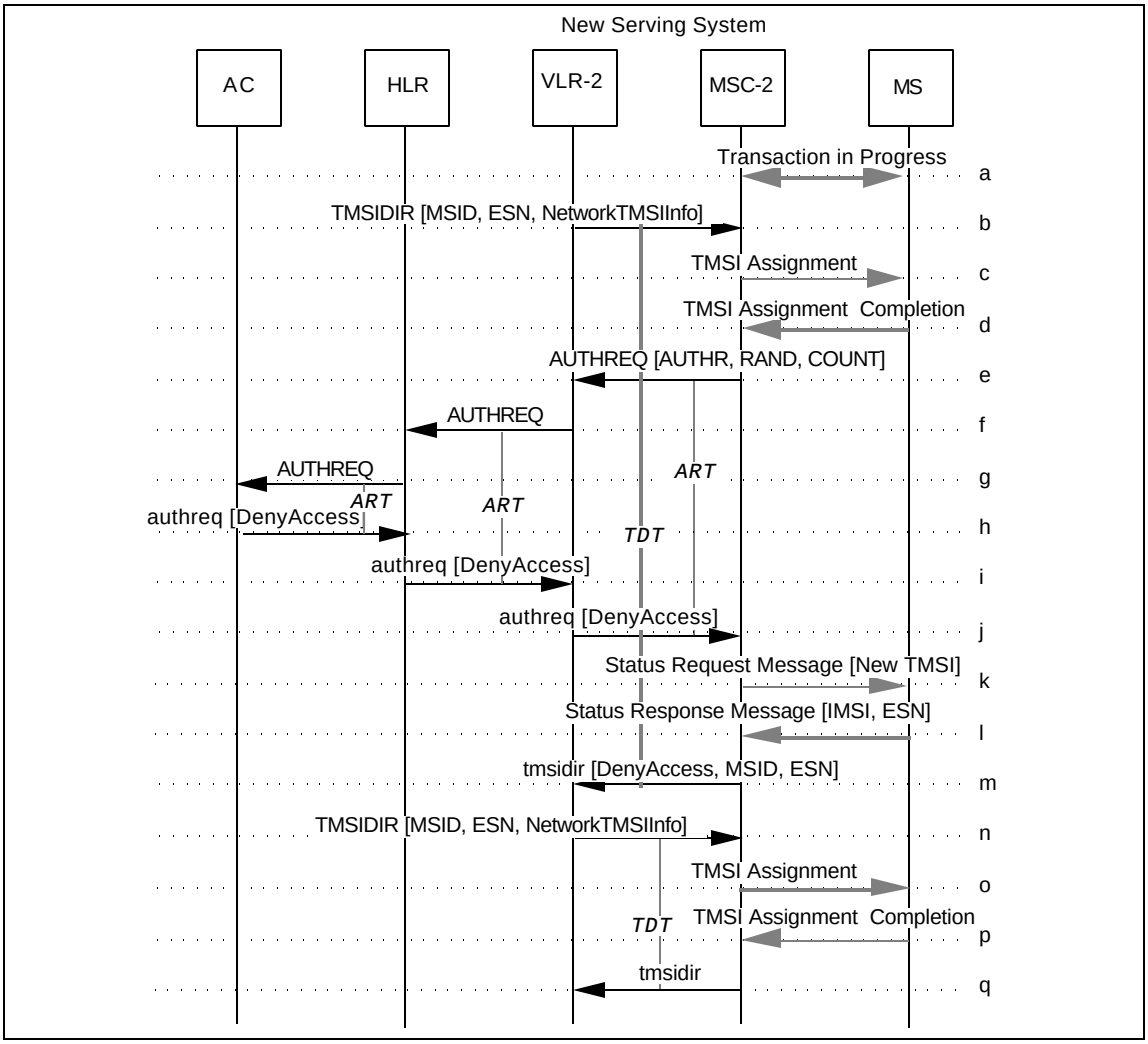

Figure 5.E.2-1 Unsuccessful TMSIDirective with MS failed authentication

a. The MS is on the paging channel and determines that authentication is required on all system accesses (AUTH=1). RAND to be used for authentication may also be obtained by the MS at that time.

b-g. Same as Section 5.E.1., Steps b-g.

h. The AC determines that the MS should be denied access. The AC sends an `authreq` to the HLR including the DenyAccess parameter.

i. The HLR forwards the `authreq` to the Serving VLR (VLR-2).

j. The VLR forwards the `authreq` to the MSC.

k The MSC sends the *Status Request* message to the MS with MSID set to Full TMSI.

l. The MS returns the *Status Response* message to the MSC, including MS's IMSI and ESN.

m. The MSC returns an `tmsidir` to the VLR, including MS's MSID (e.g., IMSI), ESN and DenyAccess parameters.

n. Same as Step- b, except NetworkTMSI is set to all 1s to delete MS's previously assigned Full TMSI.

o-p. Same as Steps c-d.

q. The MSC returns an empty `tmsidir`. Upon receiving `tmsidir`, the VLR shall delete MS's TMSI.

5.4 Authentication

5.4.A Normal Registration with Full TMSI (with Authentication) (*TIA/EIA-41-D* Chapter 3, page 183)

These scenarios describe the intersystem message flow required to support authentication when an MS registers using its full TMSI in a visited system.

5.4.A.1 Successful Scenario

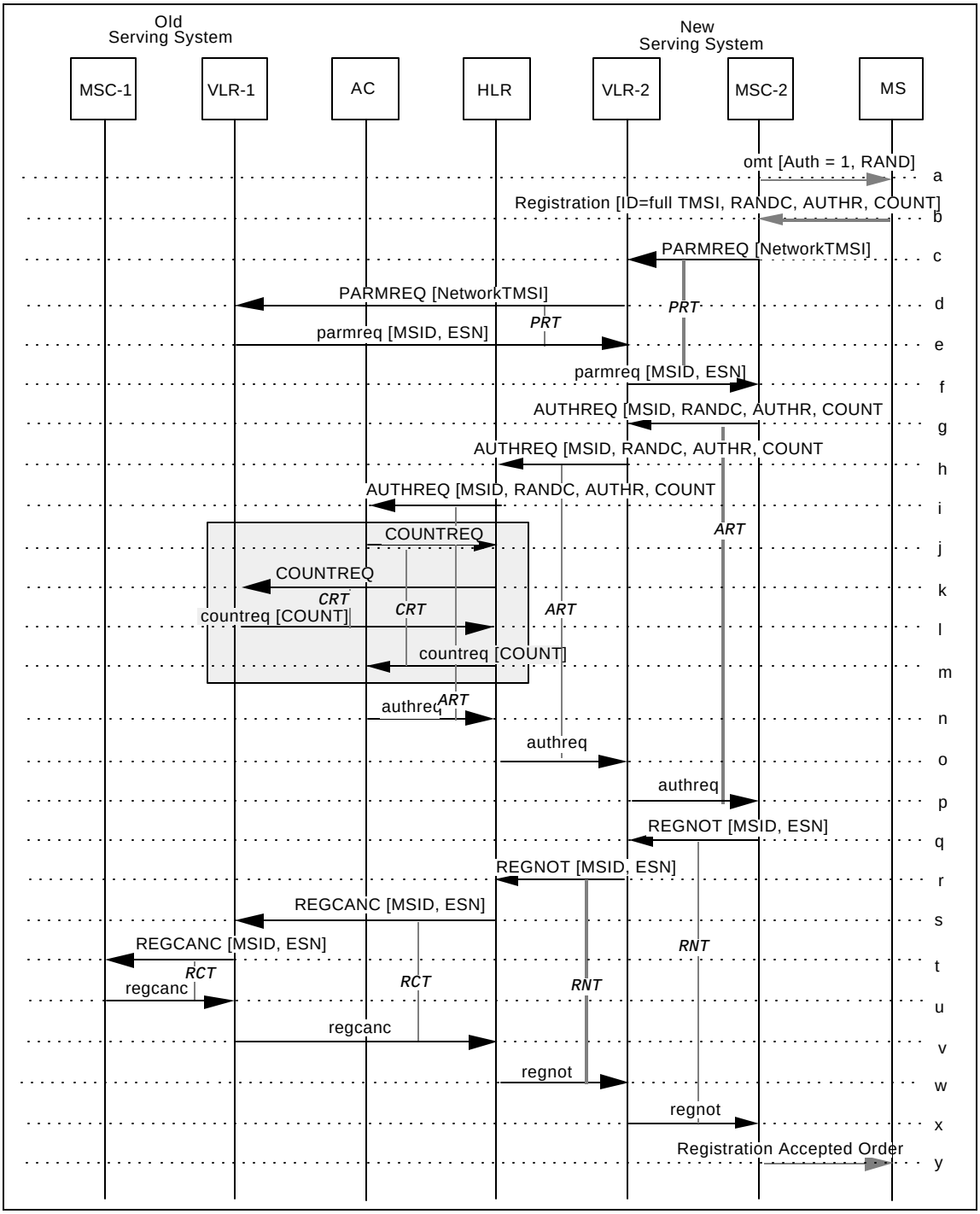

Figure 5.4.A.1-1 Successful Scenario

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 RandomVariable (RAND) to be used for authentication may also be obtained by the MS at this time. If it is not, a zero value is used by the MS as prescribed by TR-45 Authentication.

The MS executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) and the RAND value to produce a registration Authentication Result (AUTHR).

b. The MS registers at the New Serving MSC (MSC-2), including its full TMSI, AUTHR, CallHistoryCount (COUNT), and RANDC derived from the RAND used to compute AUTHR.

c. MSC-2 determines that additional parameters are required. According to the known ID information (e.g., full TMSI) it sends a `PARMREQ` to the Serving VLR (VLR-2) to get the required parameters (e.g., IMSI and ESN).

d. In this case NetworkTMSI is unknown to VLR-2, therefore, VLR-2 sends a `PARMREQ` to the Old Serving VLR (VLR-1).

e. VLR-1 sends a `parmreq` to VLR-2, including MS's MSID (e.g., IMSI) and ESN.

f. VLR-2 sends a `parmreq` to MSC-2.

g. MSC-2 verifies RANDC supplied by the MS and sends the appropriate value of RAND in an `AUTHREQ` to the New Serving VLR (VLR-2).

h. VLR-2 forwards the `AUTHREQ` to the HLR associated with the MSID (e.g., IMSI).

i. The HLR forwards the `AUTHREQ` to its AC.

j-m. If SSD is presently shared with another system, the AC shall perform validation of the MS as described in Section 5.4.8 of Chapter 3, *N.S0005-0 v 1.0* (Authentication with sharing of SSD) and go on to Step-n below.

Otherwise, the AC verifies the MSID and ESN reported by the MS. The AC then executes CAVE using the SSD-A currently stored, ESN, MIN1 (or IMSI_S1) 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 then verifies that the COUNT received from the MS is consistent with the value currently stored at the AC.

n. The AC sends an `authreq` to the HLR. The `authreq` may include SSD and directives to issue a Unique Challenge, to update the MS SSD or to update the MS COUNT according to AC/HLR local administrative practices. These update procedures are described in Sections 5.4.6, 5.4.7, and 5.4.9 of Chapter 3, *TIA/EIA-41-D*. Alternatively, the `authreq` may include DenyAccess.

o. The HLR forwards the `authreq` to VLR-2.

p. VLR-2 forwards the `authreq` to the MSC-2.

q. Following successful authentication of the MS, MSC-2 sends a `REGNOT` to VLR-2.

r. VLR-2 forwards the `REGNOT` to the HLR.

s. If the MS was previously registered in another system, the HLR sends a `REGCANC` to the Old Serving VLR (VLR-1).

t. VLR-1 forwards the `REGCANC` to the Old Serving MSC (MSC-1).

u. MSC-1 returns a `regcanc` to VLR-1.

v. VLR-1 returns a `regcanc` to the HLR.

w. The HLR records the new location of the MS in its local memory and responds to the `REGNOT` with a `regnot` that includes the information requested by VLR-2.

x. VLR-2 forwards the `regnot` to MSC-2.

y. MSC-2 sends *Registration Accepted Order* to the MS.

5.4.A.2 Unsuccessful Scenario: New Serving VLR obtains incorrect MSID and ESN from the Old Serving VLR

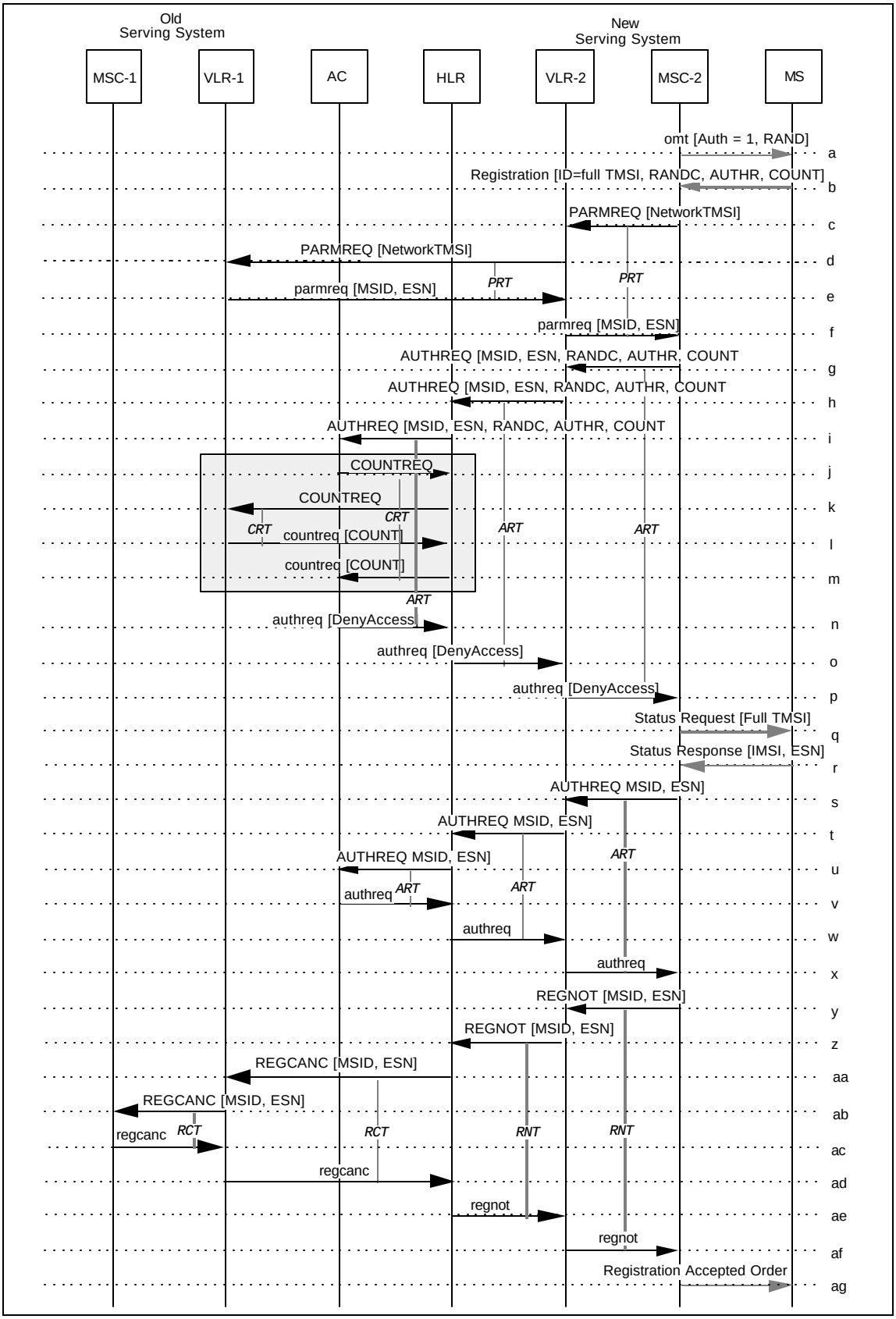

Figure 5.4.A.2-1 Unsuccessful Scenario

a-m. Same as Section 5.4.A.1, Steps a-m.

n-r. Same as Section 5.E.2, Steps h-l.

s-x. Authentication procedure is executed again by using IMSI and ESN obtained from the MS in Step-r.

y. The MSC-2 sends REGNOT to the MSC-2, using MS's IMSI and ESN.

z-ag. Same as Section 5.4.A.1, Steps r-y.

5.4.A.3 Full TMSI Origination with Authentication

This scenario describes the intersystem message flow required to support authentication when the access in the visited system is a call origination.

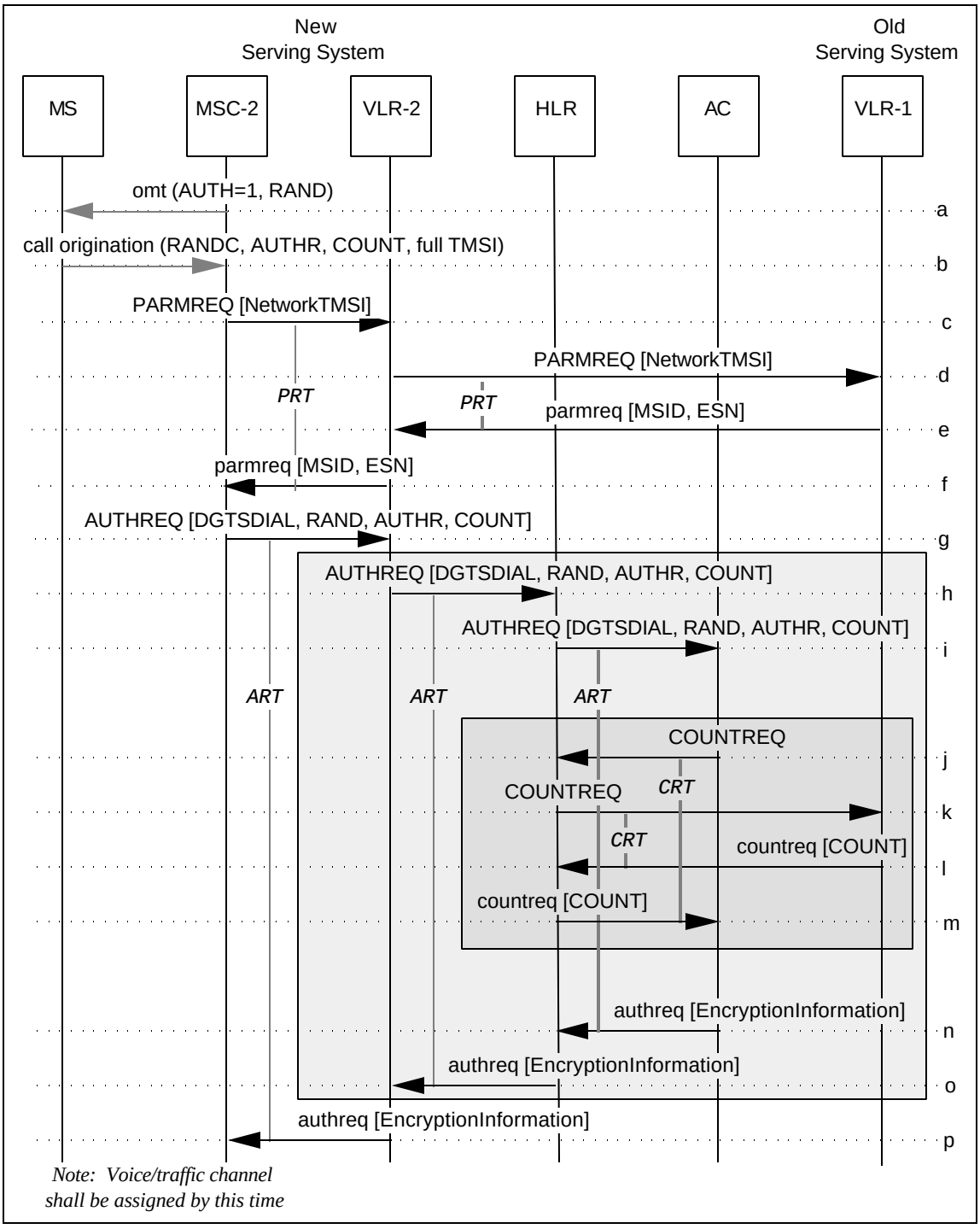

Figure 5.4.A.3-1 Full TMSI Origination with Authentication

a. The MS determines from the Overhead Message Train (OMT) that authentication is required on all system accesses (AUTH=1). The RandomVariable to be used for authentication (RAND) may also be obtained by the MS at this time. If it is not, a zero value is used by the MS, as prescribed by TR-45 authentication.

The MS executes CAVE using the dialed digits, RAND, ESN, and the SSD currently stored to produce an origination Authentication Result (AUTHR).

b. The MS sends an *Origination* message to the New Serving MSC (MSC-2), providing the dialed digits, its full TMSI Authentication Result (AUTHR), CallHistoryCount (COUNT) and the RANDC from the RAND used to compute AUTHR.

c-f. Same as Section 5.4.A.1, Steps c-f.

g-m. If SSD is presently shared with another system, the AC shall retrieve the current COUNT value and perform validation of the MS as described in Section 5.4.8 of Chapter 3, *N.S0005-0 v 1.0* (Authentication with Shared SSD) and go on to Step-n below.

Otherwise, the AC verifies the MSID and ESN reported by the MS and then executes CAVE using the SSD-A and ESN currently associated with the MS along with the value of RAND and the dialed digits provided by the serving system to produce an origination Authentication Response (AUTHR).

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

The AC then verifies that the COUNT received from the MS is consistent with the value currently stored at the AC.

n. The AC sends an `authreq` to the HLR. The `authreq` shall include the SMEKEY and VPMASK associated with this system access. Currently the AC has no way of determining whether the MS has subscribed to Voice Privacy. Therefore, the VPMASK is generated and passed by the AC on all system accesses which are origination or page response.

Note: The `authreq` may also include SSD and directives to issue a Unique Challenge, to update the MS SSD, or to update the MS COUNT according to AC local administrative practices. These update procedures are described in Sections 5.4.6, 5.4.7, and 5.4.9 of Chapter 3, *N.S0005-0 v 1.0* . Alternatively, the `authreq` may include DenyAccess.

o. The HLR forwards the `authreq` to VLR-2.

p. VLR-2 returns an `authreq` to MSC-2.

Following successful authentication of the MS, MSC-2 assigns the MS to an analog voice channel or a digital traffic channel or retains the existing assignment.

7.3 *N.S0005-0 v 1.0* Chapter 3, Section 6 "Voice Feature Scenarios" Modifications

6.1 Call Delivery

6.1.A CD Invocation with Unsolicited Page Response with a Full TMSI (*TIA/EIA-41-D* Chapt

This scenario describes procedures to resolve the unsolicited page response problem for MSs in border systems during call delivery.

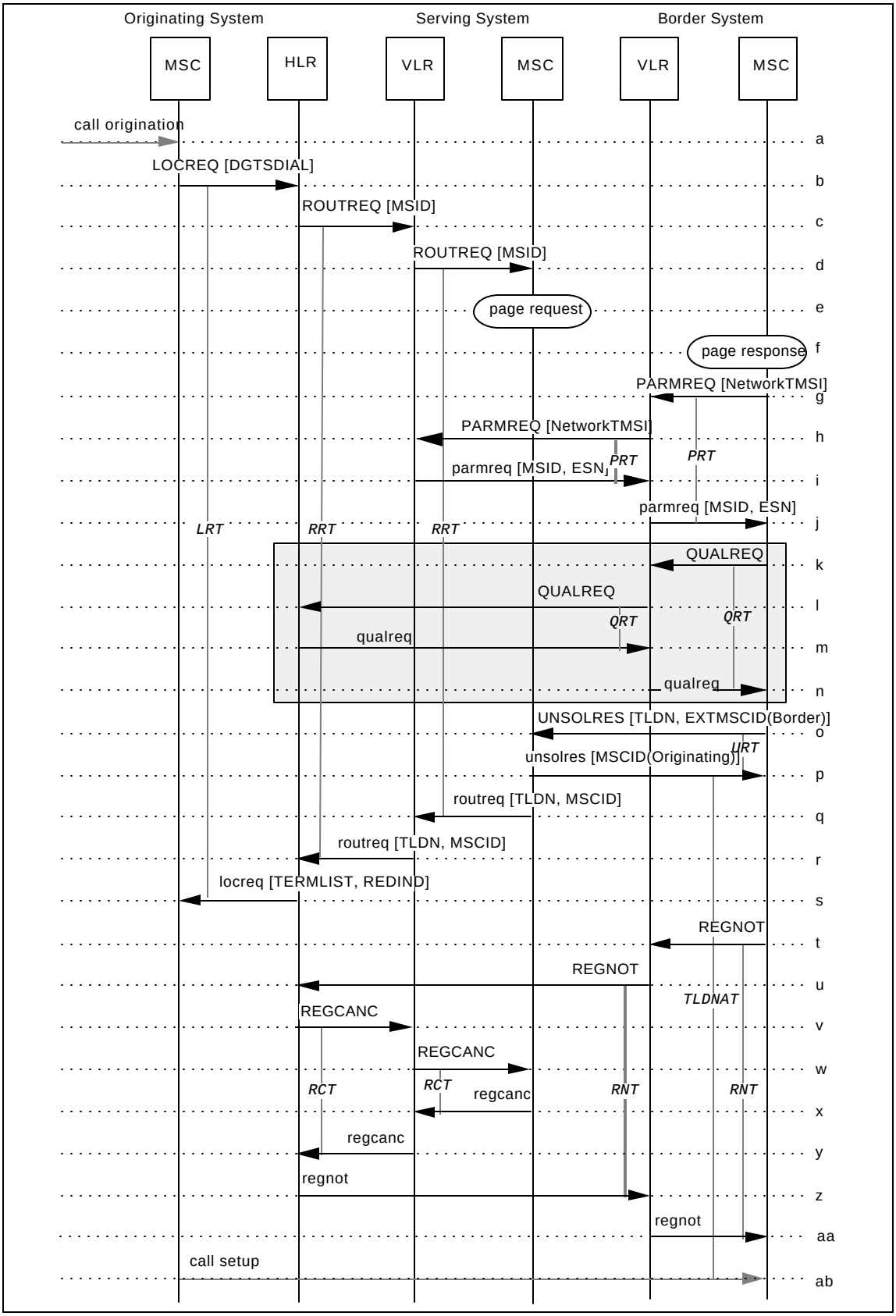

Figure 6.1.A-1 CD Invocation with Unsolicited Page Response with Full TMSI

a-d. Same as CD, Section 6.1.2 of Chapter 3, *N.S0005-0 v 1.0*, Steps a-d.

e. When the serving system receives a ROUTREQ, it initiates paging in its serving area.

f. The Border MSC receives an unsolicited page response.

After the Border MSC receives a page response it can assign the MS to a voice/traffic channel. The Border MSC verifies the presence of the MS in its serving area (e.g. via SAT detection, through a voice channel audit or both).

g. If the unsolicited page response in Step- f. includes an ID=full TMSI, the Border MSC determines that additional parameters are required. According to the known ID information (e.g., full TMSI or TMSI_CODE) it sends a PARMREQ to the Border VLR to get the required parameters (e.g., IMSI and ESN).

h. In this situation the NetworkTMSI is unknown to the Border VLR, therefore, it then sends a PARMREQ to the prior Serving VLR (i.e., which previously assigned the NetworkTMSI) according to TMSI_ZONE field of the NetworkTMSI parameter.

i. The Serving VLR determines that it can provide the required parameters and then returns a parmreq containing the requested information to the Border VLR.

j. The Border VLR sends a parmreq to the Border MSC.

k. Optionally the Border MSC sends a QUALREQ to the VLR indicating Border Access.

l. If the service profile of the MS is unknown to the VLR, it sends a QUALREQ to the HLR associated with the MS.

m. The HLR sends a qualreq to the Border MSC's VLR, including the MS's service profile information.

n. The VLR sends a qualreq to the Border MSC, including the MS's service profile information.

If the MS is authenticable, optionally authenticate it using a control channel (i.e., as in 5.4.3 of Chapter 3, *N.S0005-0 v 1.0*), or a voice channel (i.e., as in 5.4.4 of Chapter 3, *N.S0005-0 v 1.0*).

o. The Border MSC then allocates a routing alias (TLDN) and sends an UNSOLRES to one or more neighboring MSCs.

When the Serving MSC receives this UNSOLRES, it stops the paging process.

p. The Serving MSC then responds with the unsolres sent to the Border MSC.

q-ab. Same as CD, Section 6.1.8 of Chapter 3, *N.S0005-0 v 1.0*, Steps m-x.

8. *N.S0005-0 v 1.0* Chapter 5 "Signaling Protocols" Modifications

6.3.2.3.1. Error Definitions (*N.S0005-0 v 1.0* Chapter 5, page 20)

The detailed handling of operation errors is specified in *N.S0005-0 v 1.0* Chapter 5**.**

...

MissingParameter

a. Expected optional parameter is missing.

b. All profile parameters are expected, but some are missing.

c. All qualification parameters are expected, but some are missing.

MissingParameter errors should include exactly one FaultyParameter parameter in the parameter set (see 6.5.2.66).

Note that this Error Code is not used to indicate a missing mandatory parameter, a REJECT ~~message~~ component with a Problem Specifier of *Incorrect Parameter* is used in this case.

...

UnrecognizedTMSI

a. Supplied TMSI is not currently served by the Old Serving VLR. TMSI_ZONE may be matched, but TMSI_CODE is not matched.

b. Supplied TMSI is not currently served by the Serving VLR. TMSI_ZONE may be matched, but TMSI_CODE is not matched.

TMSI/VLRMismatch

a. Supplied TMSI is not resident on the Old Serving VLR.

b. Supplied TMSI is not resident on the Serving VLR.

For *IS-41* the Error Code Identifier is coded as Private TCAP. Error Codes are coded as follows:

Table 6 Error Codes

Error Code Name	Error Code H	G	F	E	D	C	B	A
UnrecognizedMIN	1	0	0	0	0	0	0	1
UnrecognizedESN	1	0	0	0	0	0	1	0
MSID ~~MIN~~/HLRMismatch	1	0	0	0	0	0	1	1
OperationSequenceProblem	1	0	0	0	0	1	0	0
ResourceShortage	1	0	0	0	0	1	0	1
OperationNotSupported	1	0	0	0	0	1	1	0
TrunkUnavailable	1	0	0	0	0	1	1	1
ParameterError	1	0	0	0	1	0	0	0
SystemFailure	1	0	0	0	1	0	0	1
UnrecognizedParameterValue	1	0	0	0	1	0	1	0
FeatureInactive	1	0	0	0	1	0	1	1
MissingParameter	1	0	0	0	1	1	0	0
UnrecognizedTMSI	1	0	0	0	1	1	0	1
TMSI/VLRMismatch	1	0	0	0	1	1	1	0
Other Error Codes are Reserved	Reserved (Note a)							
Reserved for Protocol Extension (Note b)	1	1	1	0	0	0	0	0 through 1 1 1 1 1 1 1 1

Notes:

a. Treat a reserved value the same as value 133 (decimal), *ResourceShortage*.

b. Error codes 224 to 255 (decimal) shall be reserved for protocol extension. If unknown, treat the same as value 133 (decimal), *Resource Shortage*.

6.4 MAP OPERATIONS

...

6.4.1.2 Operation Specifiers

(*N.S0005-0 v 1.0* Chapter 5, page 24)

The following table lists the *N.S0005-0 v 1.0* MAP Operation Codes.

Table 8 *N.S0005-0 v 1.0* MAP Operation Specifiers

Operation Name	Operation Code								
	H	G	F	E	D	C	B	A	Decimal
not used	0	0	0	0	0	0	0	0	0
	...								
SMSRequest	0	0	1	1	0	1	1	1	55
OTASPRequest	0	0	1	1	1	0	0	0	56
InformationBackward	0	0	1	1	1	0	0	1	57
ChangeFacilities	0	0	1	1	1	0	1	0	58
ChangeService	0	0	1	1	1	0	1	1	59
ParameterRequest	0	0	1	1	1	1	0	0	60
TMSIDirective	0	0	1	1	1	1	0	1	61
Other Values Reserved	X	X	X	X	X	X	X	X	• • •
Reserved for Protocol Extension	1	1	1	0	0	0	0	0	224
	through								• • •
	1	1	1	1	1	1	1	1	255

6.4.2 Operation Definitions

(*N.S0005-0 v 1.0* Chapter 5, page 26)

The following table summarizes the operations defined for the *N.S0005-0 v 1.0* MAP:

Table 10 Summary of MAP Operations

Operation	Reference
AuthenticationDirective	6.4.2.1
...	
OriginationRequest	6.4.2.31
ParameterRequest	6.4.2.e
...	
SMSRequest	6.4.2.48
TMSIDirective	6.4.2.f
TransferToNumberRequest	6.4.2.49
...	

6.4.2.4 AuthenticationRequest (*N.S0005-0 v 1.0* Chapter 5, page 34)

The AuthenticationRequest (AUTHREQ) operation is used to request authentication of an authentication-capable MS.

The AuthenticationRequest 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:

Table 17 AuthenticationRequest INVOKE Parameters

AuthenticationRequest INVOKE Parameters				Timer: ART
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
MSID		M	6.5.2.bu	h, i
MSCID (Serving MSC)		M	6.5.2.82	
SystemAccessType		M	6.5.2.145	
SystemCapabilities (Serving)		M	6.5.2.146	
AuthenticationData		O	6.5.2.9	a
AuthenticationResponse		O	6.5.2.10	b
CallHistoryCount		O	6.5.2.18	b
CDMANetworkIdentification (Serving MSC)		O	6.5.2.bk	j
ConfidentialityModes (Actual)		O	6.5.2.50	c
ControlChannelMode		O	6.5.2.ac	k
Digits (Dialed)		O	6.5.2.58	d
PC_SSN		O	6.5.2.93	e
RandomVariable		O	6.5.2.101	b
ServiceRedirectionCause		O	6.5.2.bp	l
SenderIdentificationNumber		O	6.5.2.116	f
TerminalType		O	6.5.2.154	g
TransactionCapability		O	6.5.2.160	m

Notes:

a. Include if the SystemAccessType value is and if the air interface encoding of dialed digits is not TBCD.

b. Include if the SystemAccessType value is , , or and the authentication parameters were requested (AUTH=1 in the Overhead Message Train) on the system access.

c. Include if the SystemAccessType value is and if the SignalingMessageEncryptionKey parameter was provided to the Serving MSC.

d. Include if the SystemAccessType value is or .

e. Include to override lower layer addressing

f. Include to identify the functional entity sending the message.

g. Should be included on *IS-41-C* or later.

h. Include the identifier with which the the MS last accessed the system, unless that identifier was a MIN-based IMSI, in which case the MobileIdentificationNumber (populated with the MIN derived from that IMSI) should be included.

i. The HLR may replace the IMSI parameter, if received, by the MobileIdentificationNumber parameter before forwarding this message the AC.

j. Include for NDSS to identify the serving network.

k. Include for NDSS to identify the operating mode of the MS.

l. Include for NDSS to indicate reason of MS registration or access.

m. Include if system is NDSS capable.

The AuthenticationRequest 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:

Table 18 AuthenticationRequest RETURN RESULT Parameters

AuthenticationRequest RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
AnalogRedirectRecord		O	6.5.2.bd	j
AuthenticationAlgorithmVersion		O	6.5.2.7	a
AuthenticationResponseUniqueChallenge		O	6.5.2.12	b
CallHistoryCount		O	6.5.2.18	c
CDMAPrivateLongCodeMask		O	6.5.2.36	d
CDMARedirectRecord		O	6.5.2.bh	k
DenyAccess		O	6.5.2.54	e
MobileIdentificationNumber		O	6.5.2.81	l
RoamingIndication		O	6.5.2.br	m
ServiceRedirectionInfo		O	6.5.2.bq	j, k
RandomVariableSSD		O	6.5.2.103	f
RandomVariableUniqueChallenge		O	6.5.2.104	b
SharedSecretData		O	6.5.2.119	c
SignalingMessageEncryptionKey		O	6.5.2.120	g, n
SSDNotShared		O	6.5.2.141	h
UpdateCount		O	6.5.2.163	i
VoicePrivacyMask		O	6.5.2.167	d,n

Notes:

a. May be included if the SharedSecretData parameter is included.

b. Include if the MSC-V shall initiate a Unique Challenge to the MS.

c. Include if the SystemCapabilities include and AC administration policies allow distribution of the SSD.

d. Include if appropriate and the SystemAccessType value is or .

e. Include if the MSC may initiate a release of system resources allocated for this access. This may include disconnection of any call in progress.

f. Include if the MSC-V shall initiate an SSD update and a Unique Challenge to the MS.

g. Include if the SystemAccessType value is or .

h. Include if the VLR shall discard the SSD.

i. Include if the MSC-V should initiate COUNT Update to the MS.

j. Include for NDSS if HLR is to redirect the MS to an analog system.

k. Include for NDSS if HLR is to redirect the MS to a CDMA system.

l. Include if:

- SSD or pending SSD is shared,
- MIN is needed for authentication calculations, and
- MIN was not present as the MSID in the corresponding INVOKE.

m. Include for CDMA to support Enhanced Roaming Indicator.

n. Include if the SystemAccessType is set to *Autonomous Registration* and the MS Terminal Type requires this parameter (e.g., *PACS).*

6.4.2.12 FacilitiesDirective2 (*N.S0005-0 v 1.0* Chapter 5, page 44)

The FacilitiesDirective2 (FACDIR2) operation is used to request that the Target MSC initiate the Handoff-Forward task. This operation differs from the FacilitiesDirective operation in its addition of support for CDMA, and NAMPs MSs.

...

The FacilitiesDirective2 operation success is reported with a TCAP RETURN RESULT (LAST). This is carried by a TCAP CONVERSATION WITH PERMISSION package. The Parameter Set is encoded as follows:

Table 34 FacilitiesDirective2 RETURN RESULT Parameters

FacilitiesDirective2 RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
CDMAChannelData (Target)		O	6.5.2.30	a
CDMACodeChannelList		O	6.5.2.33	a
CDMASearchParameters		O	6.5.2.bi	a, k
CDMASearchWindow		O	6.5.2.37	a, l
CDMAServiceConfigurationRecord		O	6.5.2.e	a, h
ChannelData (Target)		O	6.5.2.47	b, i
ConfidentialityModes (Actual)		O	6.5.2.50	c
NAMPSChannelData (Target)		O	6.5.2.86	d
TargetCellID		O	6.5.2.148	e
TDMABurstIndicator (Target)		O	6.5.2.151	f
TDMAChannelData (Target)		O	6.5.2.153	g
TDMAVoiceCoder (Target)		O	6.5.2.k	j

Notes:

a. Include if target is a CDMA channel.

b. Include if target is an AMPS or NAMPS channel.

c. Include to reflect actual assignment if ConfidentialityModes (Desired) parameter was present in the INVOKE.

d. Include if target is an NAMPS channel.

e. Include for an AMPS, NAMPS or a TDMA handoff.

f. May be included if target is a TDMA channel. See parameter definition.

g. Include if target is a TDMA channel.

h. Include to indicate a granted service configuration, other than agreed upon the default configuration.

i. For forced handoffs to an analog voice channel, include the VMAC value set to the target system's expected MS power level at handoff for the identified AMPS or NAMPS Channel Number.

j. Include to indicate the granted Voice Coder. If not included the MS shall continue using the current Voice Coder.

k. Include for this Standard and later.

l. Include for [*ANSI-41*] and earlier (Replaced by CDMASearchParameters).

6.4.2.17 HandoffBack2 (*N.S0005-0 v 1.0* Chapter 5, page 55)

The HandoffBack2 (HANDBACK2) operation is used by the Serving MSC to request that the Target MSC initiate the Handoff-Back task. This task is used to handoff a call to a Target MSC to which the Serving MSC is already connected, for the call in question, via an inter-MSC trunk. This operation differs from the HandoffBack operation in its addition of support for CDMA, and NAMPS MSs.

...

The HandoffBack2 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:

Table 44 HandoffBack2 RETURN RESULT Parameters

HandoffBack2 RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
CDMAChannelData (Target)		O	6.5.2.30	a
CDMACodeChannelList		O	6.5.2.33	a
CDMASearchParameters		O	6.5.2.bi	a, k
CDMASearchWindow		O	6.5.2.37	a, l
CDMAServiceConfigurationRecord		O	6.5.2.e	a, h
ChannelData (Target)		O	6.5.2.47	b, i
ConfidentialityModes (Actual)		O	6.5.2.50	c
NAMPSChannelData (Target)		O	6.5.2.86	d
TargetCellID		O	6.5.2.148	e
TDMABurstIndicator (Target)		O	6.5.2.151	f
TDMAChannelData (Target)		O	6.5.2.153	g
TDMAVoiceCoder (Target)		O	6.5.2.k	j

Notes:

a. Include if target is a CDMA channel.

b. Include if target is an AMPS or NAMPS channel.

c. Include to reflect actual assignment if ConfidentialityModes (Desired) parameter was present in the INVOKE.

d. Include if target is an NAMPS channel.

e. Include for an AMPS, NAMPS or a TDMA handoff.

f. May be included if target is a TDMA channel. See parameter definition.

g. Include if target is a TDMA channel.

h. Include to indicate a granted service configuration, other than the agreed upon default configuration.

i. For forced handoffs to an analog voice channel, include the VMAC value set to the target system's expected MS power level at handoff for the identified AMPS or NAMPS Channel Number.

j. Include to indicate the granted Voice Coder. If not included the MS shall continue using the current Voice Coder.

k. Include for this Standard and later.

l. Include for [*ANSI-41*] and earlier (Replaced by CDMASearchParameters).

6.4.2.21 HandoffToThird2 (*N.S0005-0 v 1.0* Chapter 5, page 63)

The HandoffToThird2 (HANDTHIRD2) operation is used by the Serving MSC (non-Anchor) to initiate a handoff with path minimization. This operation differs from the HandoffToThird operation in its support of dual-mode CDMA, and NAMPS MSs.

...

The HandoffToThird2 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:

Table 52 HandoffToThird2 RETURN RESULT Parameters

HandoffToThird2 RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
CDMAChannelData (Target)		O	6.5.2.30	a
CDMACodeChannelList		O	6.5.2.33	a
CDMASearchParameters		O	6.5.2.bi	a, k
CDMASearchWindow		O	6.5.2.37	a, l
CDMAServiceConfigurationRecord		O	6.5.2.e	a, h
ChannelData (Target)		O	6.5.2.47	b, i
ConfidentialityModes (Actual)		O	6.5.2.50	c
NAMPSChannelData (Target)		O	6.5.2.86	d
TargetCellID		O	6.5.2.148	e
TDMABurstIndicator (Target)		O	6.5.2.151	f
TDMAChannelData (Target)		O	6.5.2.153	g
TDMAVoiceCoder (Target)		O	6.5.2.k	j

Notes:

a. Include if target is a CDMA channel.

b. Include if target is an AMPS or NAMPS channel.

c. Include to reflect actual assignment if ConfidentialityModes (Desired) parameter was present in the INVOKE.

d. Include if target is an NAMPS channel.

e. Include for an AMPS, NAMPS or a TDMA handoff.

f. May be included if target is a TDMA channel. See parameter definition.

g. Include if target is a TDMA channel.

h. Include to indicate a granted service configuration, other than the agreed upon default configuration.

i. For forced handoffs to an analog voice channel, include the VMAC value set to the target system's expected MS power level at handoff for the identified AMPS or NAMPS Channel Number.

j. Include to indicate the granted Voice Coder. If not included the MS shall continue using the current Voice Coder.

k. Include for this Standard and later.

l. Include for [*ANSI-41*] and earlier (Replaced by CDMASearchParameters).

6.4.2.25 InterSystemPage (*N.S0005-0 v 1.0* Chapter 5, page 71)

The InterSystemPage (ISPAGE) operation is used by a Serving MSC to request a Border MSC to either (a) page an MS, or (b) listen for a page response from an MS, in the Border MSC prior to Call Delivery. If the MS's presence is confirmed on the Border MSC, the MS should be registered in the Border MSC and the call is delivered directly to the Border MSC.

The InterSystemPage 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:

Table 59 InterSystemPage INVOKE Parameters

InterSystemPage INVOKE Parameters				**Timer: ISPRT**
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
BillingID (Originating)		M	6.5.2.16	
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
AlertCode		O	6.5.2.3	a
CallingPartyNumberString1		O	6.5.2.23	a
CallingPartyNumberString2		O	6.5.2.24	a
CallingPartySubaddress		O	6.5.2.25	a
CDMABandClass		O	6.5.2.a	m
CDMAMobileProtocolRevision		O	6.5.2.34	c
CDMASlotCycleIndex		O	6.5.2.40	b
CDMAStationClassMark		O	6.5.2.41	n, ~~c~~
CDMAStationClassMark2		O	6.5.2.h	m
DMH_AccountCodeDigits		O	6.5.2.59	a
DMH_AlternateBillingDigits		O	6.5.2.60	a
DMH_BillingDigits		O	6.5.2.61	a
ExtendedMSCID (Serving MSC)		O	6.5.2.64	d
ExtendedSystemMyTypeCode (Serving MSC)		O	6.5.2.65	e
IMSI		O	6.5.2.bu	o
LegInformation		O	6.5.2.75	f
LocationAreaID		O	6.5.2.77	f
MobileIdentificationNumber		O	6.5.2.81	o
MobileDirectoryNumber		O	6.5.2.80	a
MSCID (Originating MSC)		O	6.5.2.82	g
MSCIdentificationNumber		O	6.5.2.83	f
NetworkTMSI		O	6.5.2.bl	o
OneTimeFeatureIndicator		O	6.5.2.88	f
PageIndicator		O	6.5.2.92	h
PC_SSN (Originating MSC)		O	6.5.2.93	i
PilotBillingID		O	6.5.2.94	j
PilotNumber		O	6.5.2.95	k
RedirectingNumberString		O	6.5.2.108	a
RedirectingSubaddress		O	6.5.2.109	a
SenderIdentificationNumber		O	6.5.2.116	f
SystemMyTypeCode (Originating MSC)		O	6.5.2.147	l

TerminalType	O	6.5.2.154	f
TerminationTreatment	O	6.5.2.158	f
TerminationTriggers	O	6.5.2.159	a

Notes:

a. Include if available (i.e., provided in the associated RoutingRequest INVOKE).

b. Included when the Serving MSC knows that the MS is operating in CDMA Slotted Mode.

c. Include if a CDMA channel is in use.

d. Include to identify serving system.

e. Include to identify serving system manufacturer.

f. Include if known.

g. Include to identify originating system.

h. Include if request is to listen only. May include if request is to page.

i. Include if available for subsequent call redirection.

j. Include if appropriate.

k. Include on a multileg call.

l. Include to identify originating system manufacturer.

m. Include on [*TSB76*] and later to indicate information of the current band in use.

n. Include if an 800 MHz CDMA channel is in use for a [*TSB64*], [*IS-41-C*], or [*ANSI-41*] system.

o. Include if supported in the border system. At least one should be present.

6.4.2.26 InterSystemPage2 (*N.S0005-0 v 1.0* Chapter 5, page 74)

The InterSystemPage2 (ISPAGE2) operation is used by a Serving MSC that has received a call via a TLDN to request a Border MSC to either (a) page an MS, or (b) listen for a page response from an MS, in the Border MSC. If an MS's presence is confirmed in the Border MSC, the call is terminated to the Border MSC via intersystem trunk facilities.

The InterSystemPage2 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:

Table 61 InterSystemPage2 INVOKE Parameters

InterSystemPage2 INVOKE Parameters				Timer: ISPRT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
BillingID (Originating)		M	6.5.2.16	
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
AlertCode		O	6.5.2.3	a
CallingPartyNumberString1		O	6.5.2.23	a
CallingPartyNumberString2		O	6.5.2.24	a
CallingPartySubaddress		O	6.5.2.25	a
CDMABandClass		O	6.5.2.a	f
CDMAMobileProtocolRevision		O	6.5.2.34	c
CDMASlotCycleIndex		O	6.5.2.40	b
CDMAStationClassMark		O	6.5.2.41	g, ~~e~~
CDMAStationClassMark2		O	6.5.2.h	f
IMSI		O	6.5.2.bu	h
LocationAreaID		O	6.5.2.77	d
MobileDirectoryNumber		O	6.5.2.80	a
MobileIdentificationNumber		O	6.5.2.81	h
NetworkTMSI		O	6.5.2.bl	h
PageIndicator		O	6.5.2.92	e
RedirectingNumberString		O	6.5.2.108	a
RedirectingSubaddress		O	6.5.2.109	a
TerminalType		O	6.5.2.154	d

Notes:

a. Include if available (i.e., provided in associated RoutingRequest INVOKE).

b. Included when the Serving MSC knows that the MS is operating in CDMA Slotted Mode.

c. Include if a CDMA channel is in use.

d. Include if known.

e. Include if request is to listen only. May include if request is to page.

f. Include on [*TSB76*] and later to indicate information of the current band in use.

g. Include if an 800 MHz CDMA channel is in use for a [*TSB64*], [*IS-41-C*], or [*ANSI-41*] system.

h. Include if supported in the border system. At least one should be presented.

6.4.2.e ParameterRequest (*N.S0005-0 v 1.0* Chapter 5, page 83)

The Parameter Request (PARMREQ) operation is used to obtain the required parameters associated with the MS.

The ParameterRequest 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:

Table 6.4.2.e-1 ParameterRequest INVOKE Parameters

ParameterRequest INVOKE Parameters				Timer: PRT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
RequiredParametersMask		M	6.5.2.j	
ElectronicSerialNumber		O	6.5.2.63	a
MSID		O	6.5.2.bu	b
MSCID		O	6.5.2.82	c
NetworkTMSI		O	6.5.2.bl	b
PC_SSN		O	6.5.2.93	d
SenderIdentificationNumber		O	6.5.2.116	e
SystemMyTypeCode		O	6.5.2.147	f

Notes:

a. Include if appropriate.

b. Include to identify the MS; at least one should be provided.

c. Include to identify initiating MSC.

d. Include if SS7 is used.

e. Include to identify the functional entity sending this message.

f. Include to identify the originating system manufacture.

The ParameterRequest 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:

Table 6.4.2.e-2 ParameterRequest RETURN RESULT Parameters

ParameterRequest RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		O	6.5.2.63	a
IMSI		O	6.5.2.bu	a
LocationAreaID		O	6.5.2.77	a
MobileIdentificationNumber		O	6.5.2.81	a
NetworkTMSI		O	6.5.2.bl	a
ReasonList		O	6.5.2.aw	b

Notes:

a. Include as indicated in RequiredParametersMask received in the ParameterRequest Invoke.

b. Include if the required parameters are unavailable.

6.4.2.32 QualificationDirective (*N.S0005-0 v 1.0* Chapter 5, page 84)

The QualificationDirective (QUALDIR) operation is used to update the authorization information, profile information, or both, previously obtained for an MS.

The QualificationDirective 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:

Table 72 QualificationDirective INVOKE Parameters

QualificationDirective INVOKE Parameters				Timer: QDT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
MSID		M	6.5.2.bu	j
QualificationInformationCode		M	6.5.2.99	
SystemMyTypeCode (HLR or VLR)		M	6.5.2.147	
AnalogRedirectRecord		O	6.5.2.bd	k
AuthorizationDenied		O	6.5.2.13	a
AuthorizationPeriod		O	6.5.2.14	b
CDMARedirectRecord		O	6.5.2.bh	l
DeniedAuthorizationPeriod		O	6.5.2.53	c
Digits (Carrier)		O	6.5.2.58	d, e
Digits (Destination)		O	6.5.2.58	d, f
LocationAreaID		O	6.5.2.77	g
Profile **Macro**		O	6.5.2.97	h
ServiceRedirectionInfo		O	6.5.2.bq	k, l, m
RoamingIndication		O	6.5.2.br	n
SenderIdentificationNumber		O	6.5.2.116	i

Notes:

a. If included, no other optional parameters shall be present.

b. Include if validation is being updated.

c May be included if the AuthorizationDenied parameter is present to indicate the interval before re-authorization may be attempted.

d. Use only on systems not capable of supporting the TransactionCapability parameter.

e. Include if profile is being updated and preferred carrier is applicable.

f. Include if profile is being updated and originations are restricted to NPA- or NPA-NXX-XXXX.

g. May be included from VLR to MSC-V. Usage from the HLR is not defined.

h. Include applicable parameter(s) (see 6.5.2.97).

i. Include to identify the functional entity sending the message.

j. The HLR includes the type of MSID last received from the Serving System. The VLR includes the type of MSID last received from the Serving MSC; this may not be the type of MSID received from the HLR.

k. Include for NDSS if HLR is to redirect the MS to an analog system.

l. Include for NDSS if HLR is to redirect the MS to a CDMA system.

m. Include if the MS NDSS feature is to be suppressed or activated.

n. Include for CDMA to support Enhanced Roaming Indicator.

6.4.2.33 QualificationRequest (*N.S0005-0 v 1.0* Chapter 5, page 86)

The QualificationRequest (QUALREQ) operation is used (a) to request validation of an MS or (b) to request validation of an MS and obtain its profile information.

The QualificationRequest 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:

Table 74 QualificationRequest INVOKE Parameters

QualificationRequest INVOKE Parameters				Timer: QRT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
MSID		M	6.5.2.bu	c
QualificationInformationCode		M	6.5.2.99	
SystemMyTypeCode (MSC or VLR)		M	6.5.2.147	
CDMANetworkIdentification (Serving)		O	6.5.2.bk	d
ControlChannelMode		O	6.5.2.ac	e
MSCID (Serving MSC or Originating MSC)		O	6.5.2.82	a
ReturnCause		O	6.5.2.bp	f
SenderIdentificationNumber		O	6.5.2.116	b
SystemAccessType		O	6.5.2.145	a
TerminalType		O	6.5.2.154	e
TransactionCapability		O	6.5.2.160	a, g

Notes:

a. Should be included on *IS-41-C* or later.

b. Include to identify the functional entity sending the message

c. Include the identifier with which the MS last accessed the system, unless that identifier was a MIN-based IMSI, in which case the MobileIdentificationNumber (populated with the MIN derived from that IMSI) should be included.

d. Include for NDSS to identify the serving network.

e. Include for NDSS to identify the operating mode of the MS.

f. Include for NDSS to indicate reason of MS registration or access.

g. Include if the system is NDSS capable.

The QualificationRequest 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:

Table 75 QualificationRequest RETURN RESULT Parameters

QualificationRequest RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
SystemMyTypeCode (VLR or HLR)		M	6.5.2.147	
AnalogRedirectRecord		O	6.5.2.bc	h
AuthorizationDenied		O	6.5.2.13	a
AuthorizationPeriod		O	6.5.2.14	b
CDMARedirectRecord		O	6.5.2.bh	i
DeniedAuthorizationPeriod		O	6.5.2.53	c
Digits (Carrier)		O	6.5.2.58	d
Digits (Destination)		O	6.5.2.58	e
MSCID (HLR)		O	6.5.2.82	f
Profile **Macro**		O	6.5.2.97	g
ServiceRedirectionInfo		O	6.5.2.bq	h, i
RoamingIndication		O	6.5.2.br	j

Notes:

a. If included, no other optional parameters shall be present.

b. Include if validation requested.

c. May be included if the AuthorizationDenied parameter is present to indicate the interval before re-authorization may be attempted.

d. Include if profile requested and preferred carrier is applicable and TransactionCapability parameter is not received.

e. Include if profile requested and originations are restricted to NPA-NXX or NPA-NXX-XXXX and TransactionCapability parameter is not received.

f. Include on *IS-41-C* and later and authorization is not denied.

g. Include applicable parameter(s) (see 6.5.2.97).

h. Include for NDSS if HLR is to redirect the MS to an analog system.

i. Include for NDSS if HLR is to redirect the MS to a CDMA system.

j. Include for CDMA to support Enhanced Roaming Indicator.

6.4.2.38 RegistrationNotification (*N.S0005-0 v 1.0* Chapter 5, page 94)

The RegistrationNotification (REGNOT) 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.

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:

Table 84 RegistrationNotification INVOKE Parameters

RegistrationNotification INVOKE Parameters				Timer: RNT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		M	6.5.2.63	
~~MobileIdentificationNumber~~		~~M~~	~~6.5.2.81~~	
MSID		M	6.5.2.bu	l
MSCID (Serving MSC)		M	6.5.2.82	
QualificationInformationCode		M	6.5.2.99	
SystemMyTypeCode (Serving MSC or VLR)		M	6.5.2.147	
AvailabilityType		O	6.5.2.15	a
BorderCellAccess		O	6.5.2.17	b
CDMANetworkIdentification (Serving)		O	6.5.2.bk	m
ControlChannelData		O	6.5.2.51	b
ControlChannelMode		O	6.5.2.ac	n
ExtendedMSCID (VLR)		O	6.5.2.64	c
LocationAreaID		O	6.5.2.77	d
PC_SSN (Serving MSC or VLR)		O	6.5.2.93	e
ReceivedSignalQuality		O	6.5.2.106	b
ReportType		O	6.5.2.111	f
ServiceRedirectionCause		O	6.5.2.bp	o
SenderIdentificationNumber		O	6.5.2.116	g
SMS_Address		O	6.5.2.123	h
SMS_MessageWaitingIndicator		O	6.5.2.129	i
SystemAccessData		O	6.5.2.144	b
SystemAccessType		O	6.5.2.145	j
SystemCapabilities		O	6.5.2.146	f, k
TerminalType		O	6.5.2.154	j
TransactionCapability		O	6.5.2.160	j

Notes:

a. Include when MS is predictably unavailable for Call Delivery (e.g., slotted mode or sleep mode).

b. Include if access occurred in a border cell (based on internal algorithms).

c. Included by VLR if its MSCID is different than the MSC's MSCID.

d. May be included from MSC to VLR.

e. Include to override lower layer addressing.

f. Include if authentication parameters were requested by the Serving MSC (AUTH=1 in the Overhead Message Train) but were not received from the MS for the system access.

g. Include to identify message sender.

h. Include to indicate that the Serving MSC supports Short Message Service.

i. Include if the MS was previously registered with this VLR, the MS is registering to a new serving MSC that does not support SMS, and an SMS message is pending delivery in the previous serving system. This is only used between a VLR and an HLR.

j. Include on *IS-41-C* and later.

k. Include if the system is authentication capable (including voice channel authentication only systems where all flags are zero).

l. Include the identifier with which the MS last accessed the system, unless that identifier was a MIN-based IMSI, in which case the MobileIdentificationNumber (populated with the MIN derived from that IMSI) should be included.

m. Include for NDSS to identify the serving network.

n. Include for NDSS to identify the operating mode of the MS.

o. Include for NDSS to indicate reason of MS registration or access.

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:

Table 85 RegistrationNotification RETURN RESULT Parameters

RegistrationNotification RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
SystemMyTypeCode (VLR or HLR)		M	6.5.2.147	
AnalogRedirectRecord		O	6.5.2.bd	k
AuthorizationDenied		O	6.5.2.13	a
AuthorizationPeriod		O	6.5.2.14	b
CDMARedirectRecord		O	6.5.2.bh	l
ControlChannelData		O	6.5.2.51	c
DeniedAuthorizationPeriod		O	6.5.2.53	d
Digits (Carrier)		O	6.5.2.58	e
Digits (Destination)		O	6.5.2.58	f
MSCID (HLR)		O	6.5.2.82	g
MSID		O	6.5.2.bu	m
Profile **Macro**		O	6.5.2.97	h
ReceivedSignalQuality		O	6.5.2.106	c
ServiceRedirectionInfo		O	6.5.2.bq	k, l
RoamingIndication		O	6.5.2.br	n
SenderIdentificationNumber		O	6.5.2.116	i
SMS_MessageWaitingIndicator		O	6.5.2.129	j
SystemAccessData		O	6.5.2.144	c

Notes:

a. If included, only the ControlChannelData, DeniedAuthorizationPeriod, ReceivedSignalQuality, and SystemAccessData optional parameters have significance.

b. Include if validation requested.

c. Include if AuthorizationDenied parameter is included with value of *Multiple Access*.

d. May be included if the AuthorizationDenied parameter is present to indicate the interval before re-authorization may be attempted.

e. Include if the profile is requested, the preferred carrier is applicable, and the CarrierDigits parameter is not included in the Profile macro.

f. Include if the profile is requested, originations are restricted to NPA-NXX or NPA-NXX-XXXX, and the RestrictionDigits parameter is not included in the Profile macro.

g. Include on *IS-41-C* and later and authorization is not denied.

h. Include applicable parameter(s) (see 6.5.2.97).

i. Include to identify the functional entity sending the message.

j. Include to indicate that an SMS message is pending delivery.

k. Include for NDSS if HLR is to redirect the MS to an analog system.

l. Include for NDSS if HLR is to redirect the MS to a CDMA system.

m. Include MIN if applicable and IMSI was included in the INVOKE. Include IMSI if applicable and MIN was included in the INVOKE.

n. Include for CDMA to support Enhanced Roaming Indicator.

6.4.2.f TMSIDirective (*N.S0005-0 v 1.0* Chapter 5, page 109)

The TMSIDirective (TMSIDIR) operation is used to assign the MS's full TMSI or TMSI Code within a TMSI Zone. The INVOKE comes from the serving system (e.g., VLR).

The TMSIDirective 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:

Table 6.4.2.f-1 TMSIDirective INVOKE Parameters

TMSIDirective INVOKE Parameters				Timer: TDT
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
ElectronicSerialNumber		M	6.5.2.63	
MSID		M	6.5.2.bu	
NetworkTMSIExpirationTime		M	6.5.2.bm	
NewNetworkTMSI		M	6.5.2.bn	
LocationAreaID		O	6.5.2.83	a
NetworkTMSI		O	6.5.2.bl	a

Notes:

a. Include if known.

The TMSIDirective 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:

Table 6.4.2.f-2 TMSIDirective RETURN RESULT Parameters

TMSI Directive RETURN RESULT Parameters				
Field	**Value**	**Type**	**Reference**	**Notes**
Identifier	SET [NATIONAL 18]	M	6.4.1.2	
Length	variable octets	M	6.4.1.1	
Contents				
DenyAccess		O	6.5.2.54	b
ElectronicSerialNumber		O	6.5.2.63	b
MSID		O	6.5.2.bu	b
ReasonList		O	6.5.2.aw	a

Notes:

a. Include if no response from the MS.

b. Include if MS fails authentication.

6.5 MAP PARAMETERS

6.5.1 General

6.5.1.1 Parameter Format

IS-41 MAP uses the TCAP parameter format defined in *ANSI T1.114*.

6.5.1.2 Parameter Identifiers

(N.S0005-0 *v 1.0* Chapter 5, page 121)

The following table lists the *N.S0005-0 v 1.0* MAP Parameter Identifiers.

Table 112 *N.S0005-0 v 1.0* MAP Parameter Identifiers

Parameter Identifier Name	Parameter Identifier Code H G F E D C B A	Reference
BillingID	1 0 0 0 0 0 0 1	6.5.2.16
ServingCellID	1 0 0 0 0 0 1 0	6.5.2.117
TargetCellID	1 0 0 0 0 0 1 1	6.5.2.148
• • •	• • •	• • •
CDMABandClass	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 0 1 0	6.5.2.a
CDMABandClassInformation	1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1	6.5.2.b
CDMABandClassList	1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 1 0 0	6.5.2.c
CDMAPilotPN	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 1 0 1	6.5.2.d
CDMAServiceConfiguration Record	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 1 1 0	6.5.2.e
CDMAServiceOption	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 0 1 1 1 1	6.5.2.f
CDMAServiceOptionList	1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0	6.5.2.g
CDMAStationClassMark2	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 0 0 1	6.5.2.h

Table 112 (continued)

Parameter Identifier Name	Parameter Identifier Code H G F E D C B A	Reference
TDMAServiceCode	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 0 1 0	6.5.2.i
TDMATerminalCapability	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 0 1 1	6.5.2.j
TDMAVoiceCoder	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 1 0 0	6.5.2.k
• • •	• • •	• • •
ControlChannelMode	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 1	6.5.2.ac

...	...	...
AnalogRedirectInfo	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 0	6.5.2.bc
AnalogRedirectRecord	1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1	6.5.2.bd
CDMAChannelNumber	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 1 0	6.5.2.be
CDMAChannelNumberList	1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 0 1 1	6.5.2.bf
CDMAPowerCombinedIndicator	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0	6.5.2.bg
CDMARedirectRecord	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 1	6.5.2.bh
CDMASearchParameters	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 1 1 0	6.5.2.bi
Reserved	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 0 1 1 1	6.5.2.bj
CDMANetworkIdentification	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 0 0 0	6.5.2.bk
NetworkTMSI	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 0 0 1	6.5.2.bl
NetworkTMSIExpirationTime	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 0 1 0	6.5.2.bm

Table 112 (concluded)

Parameter Identifier Name	Parameter Identifier Code H G F E D C B A	Reference
NewNetworkTMSI	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 0 1 1	6.5.2.bn
RequiredParametersMask	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 0 0	6.5.2.bo
ServiceRedirectionCause	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1	6.5.2.bp
ServiceRedirectionInfo	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 1 0	6.5.2.bq
RoamingIndication	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 0 1 1 1 1	6.5.2.br
• • •	• • •	• • •
MSID	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 1 0 0 0 0	6.5.2.bu
Other values are reserved	X X X X X X X X	
Reserved for Protocol Extension	1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 0 1 0 0 • • • 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1	

6.5.2 Parameter Definitions (*N.S0005-0 v 1.0* Chapter 5, page 128)

This Section provides the definitions of the parameters used in this specification.

6.5.2.30 CDMAChannelData (*N.S0005-0 v 1.0* Chapter 5, page 164)

The CDMAChannelData (CDMADATA) parameter contains the CDMA Channel Number field, the Frame Offset field and a Long Code Mask field associated with the CDMA Traffic channel in use. The CDMA Channel Number is an 11-bit number corresponding to the CDMA frequency assignment. This number specifies the channel number for the CDMA Channel center frequency (see *CDMA* for details).

The Frame Offset is a 4-bit binary number that contains the time skew of Traffic Channel frames in units of 1.25 ms. The maximum frame offset is 18.75 ms which is 15 times 1.25 ms. The valid values in the Frame Offset field are 0 through 15.

The Long Code Mask is a 42-bit binary number that contains the long code mask in use at the Serving MSC. The Long Code Mask creates a unique identity of the MS's long code which is a Pseudo Random Number sequence with period of 2^{42}-1 that is used for scrambling on the Forward CDMA Channel and spreading on the Reverse CDMA Channel.

The Band Class indicates the frequency band to which the MS is being redirected.

NP_EXT is a flag sent from the Base Station to the MS to indicate that the correction factor in Nominal Power is in the range of - 9 dB to - 24 dB inclusive.

Nominal Power is the nominal transmit power offset that the Base Station sends to the MS set to the correction factor to be used in the open loop power estimate. If the range of the correction factor is - 8 dB to 7 dB inclusive, the NP_EXT is set to 0 (or not included). If the range of the correction factor is - 9 dB to - 24 dB inclusive, the NP_EXT is set to 1.

Number Preamble is sent from the Base Station to the MS and is set to the number of Traffic Channel preamble frames the MS should send during handoff.

The minimum length of this parameter is 8 octets.

Field	Value	Type	Reference	Notes
Identifier	CDMAChannelData 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
Res'd	Frame Offset				MSB			1	
CDMA Channel Number							LSB	2	a, b
Res'd	Band Class					MSB		3	
Long Code Mask								• • •	
								7	a, b, c
							LSB	8	
NP_EXT	Nominal Power				Number Preamble			9	a
• • •								*n*	d

Figure 37 CDMAChannelData parameter

Notes:

a. See *CDMA* [*IS-95-A*] for definitions of ~~these~~ Nominal Power and Number Preamble fields. See *CDMA* [*J-STD-008*] for the definition of NP_EXT field.

b. Reserved (Res'd) bits shall be ignored on receipt and set to zero on sending.

c. The bit layout is the same as that of Band Class Value Assignments defined in *CDMA* [*TSB58*].

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

Table 37 CDMAChannelData value

octet 3, bits C-G)

Bits H G F E D C B A	Value	Meaning
0 0 0 0 0	0	**800 MHz Cellular System**.
0 0 0 0 1	1	~~Reserved.~~ See [*TSB58*] for defined values other than value 0. If unknown, treat the same as value 0, *800 MHz Cellular System*.
• • •	through	
1 1 1 1 1	31	

6.5.2.32 CDMACodeChannelInformation (*N.S0005-0 v 1.0*, pg. 166)

The CDMACodeChannelInformation (CDMACHINFO) parameter specifies CDMA code channel information which is used in the handoff process.

Field	Value	Type	Reference	Notes
Identifier	CDMACodeChannelInformation IMPLICIT SEQUENCE	M	6.5.1.2	
Length	variable	M	6.5.1.1	
Contents				
TargetCellID		M	6.5.2.148	
CDMACodeChannel		M	6.5.2.31	
CDMAPilotPN		O	6.5.2.d	a
CDMAPowerCombinedIndicator		O	6.5.2.bg	b
• • •				~~a~~ c

Figure 39 CDMACodeChannelInformation parameter

Notes:

a. Include for [*TSB76*] and later.

b. Include for this Standard and later.

c. Ignore unexpected parameters, if received.

6.5.2.37 CDMASearchWindow (*N.S0005-0 v 1.0* Chapter 5, page 170)

This parameter is replaced by CDMASearchParameters.

The CDMASearchWindow (CDMASWIN) parameter specifies the number of pseudonoise (PN) chips that a CDMA MS should use to search for usable multipath components (i.e., multipath components that the MS can use for demodulation of the associated Forward Traffic Channel) of the pilots in the Active Set and the Candidate Set. The valid values are 0 through 15.

Field	Value	Type	Reference	Notes
Identifier	CDMASearchWindow IMPLICIT OCTET STRING	M	6.5.1.2	a
Length	1 octet	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
Reserved				CDMA Search Window				1	b, c

Figure 44 CDMASearchWindow parameter

Notes:

a. Used for [*TSB64*], [*IS-41-C*] and [*ANSI-41*] .

b. See *CDMA* [*IS-95-A*] SRCH_WIN_A for the definition of this field.

c. Reserved bits shall be ignored on receipt and set to zero on sending.

6.5.2.160 TransactionCapability (*N.S0005-0 v 1.0* Chapter 5, page 315)

The TransactionCapability (TRANSCAP) parameter indicates a system's transaction capability at the current time (i.e., this capability may change over time).

Field	Value	Type	Reference	Notes
Identifier	TransactionCapability 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
Res'd	NDSS	UZCI	SPINI	RUI	ANN	BUSY	PROF	1	a
Reserved			TL	Multiple Terminations				2	a
• • •								*n*	a, b

Figure 177 TransactionCapability parameter

Notes:

a. Reserved (Res'd) bits shall be ignored on receipt and set to zero on sending.

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

Table 192 TransactionCapability value

Profile (PROF) (octet 1, bit A)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of supporting the *IS-41-C* profile parameters.
1	1	The system is capable of supporting the *IS-41-C* profile parameters.

Busy Detection (BUSY) (octet 1, bit B)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of detecting a busy condition at the current time.
1	1	The system is capable of detecting a busy condition at the current time.

Announcements (ANN) (octet 1, bit C)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of honoring the AnnouncementList parameter at the current time.
1	1	The system is capable of honoring the AnnouncementList parameter at the current time.

Table 192 (concluded)

Remote User Interaction (RUI) (octet 1, bit D)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of interacting with the user.
1	1	The system is capable of interacting with the user.

Subscriber PIN Intercept (SPINI) (octet 1, bit E)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of supporting local SPINI operation at the current time.
1	1	The system is capable of supporting local SPINI operation.

UZ Capability Indicator (UZCI) (octet 1, bit F)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not User Zone capable at the current time.
1	1	The system is User Zone capable at the current time.

NDSS Capability (NDSS) (octet 1, bit G)

Bits H G F E D C B A	Value	Meaning
0	0	Serving system is not NDSS capable.
1	1	Serving system is NDSS capable.

Multiple Terminations (octet 2, bits A-D)

Bits H G F E D C B A	Value	Meaning
0 0 0 0	0	The system cannot accept a termination at this time (i.e., cannot accept routing information).
0 0 0 1	1	The system supports the number of call legs indicated.
• • •	through	
1 1 1 1	15	

TerminationList (TL) (octet 2, bit E)

Bits H G F E D C B A	Value	Meaning
0	0	The system is not capable of supporting the TerminationList parameter at the current time.
1	1	The system is capable of supporting the TerminationList parameter at the current time.

6.5.2.bc AnalogRedirectInfo

(*N.S0005-0 v 1.0* Chapter 5, page 133)

The AnalogRedirectInfo (ANALOGRI) indicates whether the MS is to ignore the CDMA Capability Message on the analog system to which it is being redirected, and the order in which the MS is to attempt to obtain service on an analog system.

Field	Value	Type	Reference	Notes
Identifier	AnalogRedirectInfo 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
Reserved		IC	Sys Ordering					1	a
• • •								*n*	b

Figure 6.5.2.bc-1 AnalogRedirectInfo parameter

Notes:

a. Reserved bits shall be ignored on receipt and set to zero on sending.

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

Table 6.5.2.bc-1 AnalogRedirectInfo value

Sys Ordering (octet 1, bits A-E)

Bits H G F E D C B A	Value	Meaning
0 0 0 0 0	0	**Attempt to obtain service on either System A or B in accordance with the custom system selection process.**
0 0 0 0 1	1	**Attempt to obtain service on System A only**.
0 0 0 1 0	2	
0 0 0 1 1	3	**Attempt to obtain service on System A first. If unsuccessful, attempt to obtain service on System B**.
0 0 1 0 0	4	**Attempt to obtain service on System B first. If unsuccessful, attempt to obtain service on System A.**
0 0 1 0 1	5	**Attempt to obtain service on either System A or System B. If unsuccessful, attempt to obtain service on the alternate system (System A or System B)**.
0 0 1 1 0	6	Reserved for [*ANSI-41*] protocol extension.
1 1 1 1 1	31	

Ignore CDMA (IC) (octet 1, bit F)

Bits H G F E D C B A	Value	Meaning
0	0	
1	1	**Ignore the CDMA Capability Message on the analog system to which it is being redirected.**

6.5.2.bd AnalogRedirectRecord (*N.S0005-0 v 1.0* Chapter 5, page 132)

The AnalogRedirectRecord (ANALOGRR) indicates whether the MS is to ignore the CDMA Capability Message on the analog system to which it is being redirected, and the order in which the MS is to attempt to obtain service on an analog system.

Field	Value	Type	Reference	Notes
Identifier	AnalogRedirectRecord IMPLICIT SEQUENCE	M	6.5.1.2	
Length	variable	M	6.5.1.1	
Contents				
AnalogRedirectInfo		M	6.5.2.bc	
MSCID		M	6.5.2.82	
• • •				a

Figure 6.5.2.bd-1 AnalogRedirectRecord parameter

Notes:

a. Ignore extra unexpected parameters, if received.

6.5.2.be CDMAChannelNumber (*N.S0005-0 v 1.0* Chapter 5, page 166)

The CDMAChannelNumber (CDMACN) parameter is used to indicate the 11-bit number corresponding to a CDMA frequency assignment. The number specifies the channel number for the CDMA Channel center frequency (see *CDMA* [*IS-95-A*] for details).

The minimum length of this parameter is 2 octets.

Field	Value	Type	Reference	Notes
Identifier	CDMAChannelNumber 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
Reserved					MSB			1	a
CDMA Channel Number							LSB	2	b
• • •								*n*	c

Figure 6.5.2.be-1 CDMAChannelNumber parameter

Notes:

a. Reserved bits shall be ignored on receipt and set to zero on sending.

b. See *CDMA* [*IS-95-A*] for definitions of this field.

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

6.5.2.bf CDMAChannelNumberList (*N.S0005-0 v 1.0* Chapter 5, page 166)

The CDMAChannelNumberList (CDMACNL) parameter specifies a list of CDMA channel numbers.

Field	Value	Type	Reference	Notes
Identifier	CDMAChannelNumberList IMPLICIT SEQUENCE OF	M	6.5.1.2	
Length	variable	M	6.5.1.1	
Contents				
CDMAChannelNumber		M	6.5.2.be	
CDMAChannelNumber		O	6.5.2.be	a
• • •				

Figure 6.5.2.bf-1 CDMAChannelNumberList parameter

Notes:

a. Optionally include additional CDMAChannelNumber parameters.

6.5.2.bg CDMAPowerCombinedIndicator (*N.S0005-0 v 1.0* Chapter 5, page 169)

The CDMAPowerCombinedIndicator (CDMAPCI) parameter indicates whether the Forward Traffic Channel associated with this pilot carries the same closed-loop power control sub-channel bits as that of the previous pilot in the list.

Field	Value	Type	Reference	Notes
Identifier	CDMAPowerCombinedIndicator IMPLICIT OCTET STRING	M	6.5.1.2	
Length	1 octet	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
Reserved							PCI	1	a, b

Figure 6.5.2.bg-1 CDMAPowerCombinedIndicator parameter

Notes:

a. See *CDMA* [*IS-95-A*] PWR_COMB_IND for the definition of the PCI field.

b. Reserved bits shall be ignored on receipt and set to zero on sending.

6.5.2.bh CDMARedirectRecord (*N.S0005-0 v 1.0* Chapter 5, page 170)

The CDMARedirectRecord (CDMARR) contains the redirect record for redirecting a MS to a CDMA system.

Field	Value	Type	Reference	Notes
Identifier	CDMARedirectRecord IMPLICIT SEQUENCE	M	6.5.1.2	
Length	variable octets	M	6.5.1.1	
Contents				
CDMABandClass		M	6.5.2.a	a
CDMAChannelNumberList		M	6.5.2.bf	
MSCID		M	6.5.2.82	
CDMANetworkIdentification		M	6.5.2.bk	
• • •				b

Figure 6.5.2.bh-1 CDMARedirectRecord parameter

Notes:

a. See *CDMA* [*TSB76*] for the definition of this parameter.

b. Ignore unexpected parameters, if received. Send only defined (or significant) parameters.

6.5.2.bi CDMASearchParameters (*N.S0005-0 v 1.0* Chapter 5, page 170)

The CDMASearchParameters parameter (CDMASP) contains the CDMASearchWindow field, the T_ADD field, the T_DROP field, T_COMP field, and the T_TDROP field used to establish handoff criteria and initiate the handoff process.

CDMASearchWindow specifies the number of pseudonoise (PN) chips that a CDMA MS should use to search for usable multipath components (i.e., multipath components that the MS can use for demodulation of the associated Forward Traffic Channel) of the pilots in the Active Set and the Candidate Set. The valid values are 0 through 15.

T_ADD is a pilot threshold for adding a pilot to the Candidate Set. It is used by the MS to trigger the sending of the *Pilot Strength Measurement Message* to initiate the handoff process.

T_DROP is a pilot drop threshold. It is used by the MS to trigger the sending of the *Pilot Strength Measurement Message* to terminate the handoff process.

T_COMP is the comparison threshold for pilots in the Active Set vs. the Candidate Set. The MS sends a *Pilot Strength Measurement Message* when the strength of a pilot in the Candidate Set exceeds that of a pilot in the Active Set by this margin.

T_TDROP is the drop timer value after which an action is taken by the MS for a pilot that is a member of the Active Set or the Candidate Set, and whose strength has not become greater than T_DROP. If the pilot is a member of the Active Set, a *Pilot Strength Measurement Message* is issued. If the pilot is a member of the Candidate Set, it will be moved to the Neighbor Set.
The minimum length of this parameter is 4 octets.

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

H	G	F	E	D	C	B	A	octet	Notes
Reserved				CDMA Search Window				1	b, c
Reserved		T_ADD						2	b, d
Reserved		T_DROP						3	b, e
T_TDROP				T_COMP				4	f
• • •								*n*	g

Figure 6.5.2.bi-1 CDMASearchParameters parameter

Notes:

a. Used for this Standard and later.

b. Reserved bits shall be ignored on receipt and set to zero on sending.

c. See *CDMA* [*IS-95-A*] SRCH_WIN_A for the definition of this field.

d. See *CDMA* [*IS-95-A*] T_ADD for the definition of this field.

e. See *CDMA* [*IS-95-A*] T_DROP for the definition of this field.

f. See *CDMA* [*IS-95-A*] T_COMP and T_TDROP for the definition of these fields.

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

6.5.2.bk CDMANetworkIdentification (*N.S0005-0 v 1.0* Chapter 5, page 169)

The CDMANetworkIdentification (CDMANID) parameter is used to indicate the 16-bit identification number of a network.

The minimum length of this parameter is 2 octets.

Field	Value	Type	Reference	Notes
Identifier	CDMANetworkIdentification 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	a
CDMA Network ID									
							LSB	2	
• • •								*n*	b

Figure 6.5.2.bk-1 CDMANetworkIdentification parameter

Notes:

a. See *CDMA* [*J-STD-008*] for encoding of this field.

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

6.5.2.ac ControlChannelMode

The ControlChannelMode (CCM) parameter indicates the current (or last known) Control Channel operating mode used by the MS to access the system.

Field	Value	Type	Reference	Notes
Identifier	ControlChannelMode 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
Control Channel Mode								1	
• • •								*n*	a

Figure 6.5.2.ac-1 ControlChannelMode parameter

Notes:

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

Table 6.5.2.ac-1 ControlChannelMode value

Control Channel Mode (octet 1)

Bits	H	G	F	E	D	C	B	A	Value	Meaning
	0	0	0	0	0	0	0	0	0	Unknown.
	0	0	0	0	0	0	0	1	1	**MS is in Analog CC Mode**
	0	0	0	0	0	0	1	0	2	**MS is in Digital CC Mode**
	0	0	0	0	0	0	1	1	3	**MS is in NAMPS CC Mode**
	0	0	0	0	0	1	0	0	4	
				• • •					through	Reserved. Treat the same as value 0, *Unknown*.
	1	1	0	1	1	1	1	1	223	
	1	1	1	0	0	0	0	0	224	
				• • •					through	Reserved for [*ANSI-41*] protocol extension. If
	1	1	1	1	1	1	1	1	255	unknown, treat the same as value 0, *Unknown*.

6.5.2.bl NetworkTMSI

(*N.S0005-0 v 1.0* Chapter 5, page 219)

The NetworkTMSI (NETMSI) consists of the TMSI_CODE and the TMSI_ZONE fields. TMSI_CODE defines a 32-bit MS temporary identification in one TMSI Zone. The TMSI_ZONE is associated with a group of cell sites (e.g., cell sites associated with a single MSC) such that all TMSI_CODEs assigned to mobiles within the TMSI_ZONE are unique. TMSI_CODEs may be re-used in different TMSI zones.

The minimum length of this parameter is 4 octets.

Field	Value	Type	Reference	Notes
Identifier	NetworkTMSI IMPLICIT DigitsType	M	6.5.1.2	
Length	variable octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
TMSI_CODE								1 2 3 4	a
1st Digit of TMSI_ZONE				Type of Addressing				5	b
3rd Digit of TMSI_ZONE				2nd Digit of TMSI_ZONE				6	b
5th Digit of TMSI_ZONE				4th Digit of TMSI_ZONE				7	b
• • •				• • •				• • •	b
nth Digit of TMSI_ZONE				nth-1 Digit of TMSI_ZONE				*n*	b, c

Figure 6.5.2.bl-3 NetworkTMSI parameter

Notes:

a. See *CDMA* [*J-STD-008*] for the encoding details of this field.

b. The encoding scheme of the address digits is BCD encoding.

c. Where there is an odd number of digits, the nth digit is set to *filler*.

Table 6.5.2.bl-1 NetworkTMSI value

Type of Addressing (octet 5, bits A-D)										
Bits	H	G	F	E	D	C	B	A	Value	Meaning
					0	0	0	0	0	Not Used
					0	0	0	1	1	
					0	0	1	0	2 through 15	Reserved for [*ANSI-41*] protocol extension. If unknown, treat the same as value 0, *Not Used*.
					• • •					
					1	1	1	1		

6.5.2.bm NetworkTMSIExpirationTime

(*N.S0005-0 v 1.0* Chapter 5, page 219)

NetworkTMSIExpirationTime (NETMSIT) parameter defines the NetworkTMSI Expiration Time which is used to automatically de-assign the assigned TMSI.

Field	Value	Type	Reference	Notes
Identifier	NetworkTMSIExpirationTime 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	
TMSI Expiration Time								2	a
								3	
							LSB	4	
• • •								*n*	b

Figure 6.5.2.bm-1 NetworkTMSIExpirationTime parameter

Notes:

a. See *CDMA* [*J-STD-008*] for the definition of this field. It is the System Time in the units of 80ms $\times 2^{12}$ when the TMSI is to expire.

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

6.5.2.bn NewNetworkTMSI (*N.S0005-0 v 1.0* Chapter 5, page 219)

The NewNetworkTMSI (NNETMSI) parameter consists of the TMSI_CODE and the TMSI_ZONE fields. The NewNetworkTMSI is used in the TMSI Assignment operation to update an MS's TMSI. See Section 6.5.2.bl NetworkTMSI for encoding details.

The minimum length of this parameter is 4 octets.

Field	Value	Type	Reference	Notes
Identifier	NewNetworkTMSI IMPLICIT DigitsType	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	
				TMSI_CODE				2	a
								3	
							LSB	4	
MSB								5	
				TMSI_ZONE				6	b
								...	
				• • •			LSB	*n*	

Figure 6.5.2.bn-1 NewNetworkTMSI parameter

Notes:

a. See *CDMA* [*J-STD-008*] for the encoding details of this field.

b. See section 6.5.2.bl for the encoding details of this field.

6.5.2.aw ReasonList

(*N.S0005-0 v 1.0* Chapter 5, page 241)

The ReasonList (RSNLST) parameter is used to indicate the reason for operation failure (e.g., rejecting a ChangeService, ChangeFacilities or TMSIAssignment failure).

Field	Value	Type	Reference	Notes
Identifier	ReasonList IMPLICIT ENUMERATED	M	6.5.1.2	
Length	2 octets	M	6.5.1.1	
Contents				

H	G	F	E	D	C	B	A	octet	Notes
Reason List								1	a
• • •								n	b

Figure 6.5.2.aw-1 ReasonList parameter

Notes:

a. Include one or more occurrences of this field.

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

Table 6.5.2.aw-1 Reason List value

Reason List (octet 1)

Bits	H	G	F	E	D	C	B	A	Value	Meaning
	0	0	0	0	0	0	0	0	0	**Unknown.**
	0	0	0	0	0	0	0	1	1	**Unable to configure ISLP.**
	0	0	0	0	0	0	1	0	2	**ISLP failure.**
	0	0	0	0	0	0	1	1	3	**Service allowed but facilities not available.**
	0	0	0	0	0	1	0	0	4	**Service not allowed.**
	0	0	0	0	0	1	0	1	5	**No Response to TMSI assignment.**
	0	0	0	0	0	1	1	0	6	**Required parameters unavailable.** (e.g., as indicated by the RequiredParametersMask parameter).
	0	0	0	0	0	1	1	1	7	Reserved for common CDMA and TDMA
				....					through	network error causes. If unknown, treat the same
	0	1	1	1	1	1	1	0	110	as value 0.
	0	1	1	0	1	1	1	1	111	Reserved for common CDMA and TDMA
				....					through	network error causes for [*ANSI-41*] protocol
	0	1	1	1	1	1	1	1	127	extension. If unknown, treat the same as value 0.
	1	0	0	0	0	0	0	0	128	CDMA Specific error causes. If unknown, treat
				...					through	the same as value 0.
	1	0	1	0	1	1	1	0	174	
	1	0	1	0	1	1	1	1	175	CDMA Specific error causes for [*ANSI-41*]
				...					through	protocol extension. If unknown treat the same as
	1	0	1	1	1	1	1	1	191	value 0.
	1	1	0	0	0	0	0	0	192	TDMA Specific error causes as defined in by the
				....					through	TDMACause parameter. If unknown treat the
	1	1	1	0	1	1	0	1	237	same as value 0.
	1	1	1	0	1	1	1	0	238	TDMA Specific error causes for [*ANSI-41*]
				....					through	protocol extension. If unknown, treat the same
	1	1	1	1	1	1	1	1	255	as value 0.

6.5.2.bo RequiredParametersMask (*N.S0005-0 v 1.0* Chapter 5, page 248)

RequiredParametersMask (RPM) parameter identifies the parameters which are required by the serving system.

Field	Value	Type	Reference	Notes
Identifier	RequiredParametersMask 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
Reserved			LOCID	TMSI	ESN	MIN	IMSI	1	a
• • •								*n*	b

Figure 6.5.2.bo-1 RequiredParametersMask parameter

Notes:

a. Reserved bits shall be ignored on receipt and set to zero on sending.

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

Table 6.5.2.bo-1 RequiredParametersMask value

IMSI (octet 1, bit A)

Bits H G F E D C B A	Value	Meaning
0	0	Not Required.
1	1	Required.

MIN (octet 1, bit B)

Bits H G F E D C B A	Value	Meaning
0	0	Not Required.
1	1	Required.

ESN (octet 1, bit C)

Bits H G F E D C B A	Value	Meaning
0	0	Not Required.
1	1	Required.

TMSI (octet 1, bit D)

Bits H G F E D C B A	Value	Meaning
0	0	Not Required.
1	1	Required.

LocationAreaID (LOCID) (octet 1, bit E)

Bits H G F E D C B A	Value	Meaning
0	0	Not Required.
1	1	Required.

6.5.2.bp ServiceRedirectionCause (*N.S0005-0 v 1.0* Chapter 5, page 252)

The ServiceRedirectionCause (SRCAUSE) parameter is used to indicate the reason for MS registration or access is a return from a redirection failure.

Field	Value	Type	Reference	Notes
Identifier	ServiceRedirectionCause 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
Service Redirection Cause								1	
• • •								*n*	a

Figure 6.5.2.bp-1 ServiceRedirectionCause parameter

Notes:

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

Table 6.5.2.bp-1 ServiceRedirectionCause value

ServiceRedirectionCause (octet 1)

Bits H	G	F	E	D	C	B	A	Value	Meaning
0	0	0	0	0	0	0	0	0	**Not used**.
0	0	0	0	0	0	0	1	1	**NormalRegistration**
0	0	0	0	0	0	1	0	2	**SystemNotFound**.
0	0	0	0	0	0	1	1	3	**ProtocolMismatch**.
0	0	0	0	0	1	0	0	4	**RegistrationRejection**.
0	0	0	0	0	1	0	1	5	**WrongSID**.
0	0	0	0	0	1	1	0	6	**WrongNID**.
0	0	0	0	0	1	1	1	7 through 223	Reserved. Treat the same as value 1, *NormalRegistration.*
1	1	1	0	0	0	0	0	224 through 255	Reserved for [*ANSI-41*] protocol extension. If unknown, treat the same as value 1 *NormalRegistration.*

6.5.2.bq ServiceRedirectionInfo (*N.S0005-0 v 1.0* Chapter 5, page 252)

The ServiceRedirectionInfo (SRINFO) parameter identifies whether the MS should return to the system from which it is being redirected upon failure to obtain service (Return If Fail). The NDSS Status field identifies whether the NDSS feature is suppressed.

Field	Value	Type	Reference	Notes
Identifier	ServiceRedirectionInfo 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
Reserved						NDS	RIF	1	a
• • •								*n*	b

Figure 6.5.2.bq-1 ServiceRedirectionInfo parameter

Notes:

a. Reserved bits shall be ignored on receipt and set to zero on sending.

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

Table 6.5.2.bq-1 ServiceRedirectionInfo value

Return If Fail (RIF) (octet 1, bit A)

Bits H G F E D C B A	Value	Meaning
0	0	**If MS fails to access the redirected system, MS shall not return to the serving system.**
1	1	**If MS fails to access the redirected system, MS shall return to the serving system.**

NDSS Status (NDS) (octet 1, bit B)

Bits H G F E D C B A	Value	Meaning
0	0	**NDSS is not suppressed.**
1	1	**NDSS is suppressed.**

6.5.2.br RoamingIndication (N.S0005-0 v 1.0 Chapter 5, page 249)

The RoamingIndication (ROAMIND) parameter is used to support the Enhanced Roaming Indicator feature.

Field	Value	Type	Reference	Notes
Identifier	RoamingIndication 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
Roaming Indication								1	a
• • •								*n*	b

Figure 6.5.2.br-1 RoamingIndication parameter

Notes:

a. See *CDMA* [*TSB58*] for the definition of this field.

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

9. *N.S0005-0 v 1.0* Chapter 6 "Signaling procedures" Modifications

3.1 Registration Call Task (N.S0005-0 v 1.0 Chapter 6, Page 9)

3.1.1 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:

1-1 IF the MS has authentication capabilities:

1-1-1 Include the SystemAccessType parameter set to .

1-1-2 Execute the “MSC Initiating an Authentication Request” task (see 4.4.1).

1-1-3 IF the 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 3.5.1).

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 4.38.1).

3-2 IF the 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 3.5.1).

3-5 ENDIF.

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

4 ENDIF.

5 Exit this task.

Remainder unchanged

3.2 Origination Call Tasks

(*N.S0005-0 v 1.0* Chapter 6, Page 12)

3.2.1 Idle MS Origination

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

1 IF an appropriate 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 authenticated and authentication is active (AUTH=1 in the Overhead Message Train):

3-1 IF the MS has authentication capabilities:

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

3-1-2 Execute the "MSC Initiating an Authentication Request" task (see 4.4.1).

3-1-3 IF the MS is being redirected:

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

3-1-3-2 Exit this task.

3-1-4 ENDIF.

3-1-5 IF authentication fails:

3-1-5-1 Execute "Local Recovery Procedures" task (see 3.5.1).

3-1-5-2 Exit this task.

3-1-6 ENDIF.

3-2 ENDIF.

4 ENDIF.

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

5-1 Execute the "MSC Initiating MS Registration" task (see 4.38.1).

5-1-1 IF the MS is being redirected:

5-1-1-1 Send the MS the AnalogRedirectRecord or the CDMARedirectRecord, and the ServiceRedirectionInfo parameter if received.

5-1-1-2 Exit this task.

5-1-2 ENDIF.

5-2 Send the MS the RoamingIndication parameter if received, in addition to other messages.

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

6-1 Execute the "MSC Initiating Qualification Request" task (see 4.33.1).

6-1-1 IF the MS is being redirected:

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

6-1-1-2 Exit this task.

6-1-2 ENDIF.

6-2 Send the MS the RoamingIndication parameter if received, in addition to other messages.

7 ENDIF.

8 Execute "Initialize the OneTimeFeatureIndicator Parameter" task (see 3.2.8).

9 Execute "MSC Analyze MS Dialed Number" task (see 3.2.3).

10 IF the PointOfReturn is *ToneTermination*:

10-1 Execute "Apply Access Denial Treatment" task (see 3.4.5).

10-2 Exit this task.

11 ENDIF.

12 IF the MS is not authorized:

12-1 Execute "Apply Access Denial Treatment" task (see 3.4.5).

12-2 Exit this task.

13 ENDIF.

14 Execute the "MSC PACA Call Origination Invocation" task (see 5.17.2).

15 IF unsuccessful:

15-1 Execute "Apply Access Denial Treatment" task (see 3.4.5).

16 ELSE (seize the channel by):

16-1 Reserve the available voice or traffic channel.

16-2 Order the MS to acquire the reserved voice or traffic channel.

16-3 Verify the MS has properly tuned to this voice or traffic channel.

16-4 IF unsuccessful:

16-4-1 Execute "Apply Access Denial Treatment" task (see 3.4.5).

16-5 ENDIF.

17 ENDIF.

18 Execute the “MSC MWN Call Origination Invocation” task (see 5.13.7).

19 ENDIF.

20 IF the AnnouncementList parameter is received:

20-1 Execute the “Play All Announcements in the AnnouncementList” task (see 3.2.5).

21 ENDIF.

22 Execute the “MSC Routing Points Of Return” task (see 3.2.6).

23 Exit this task.

Remainder unchanged

4.4 Authentication Request (*N.S0005-0 v 1.0* Chapter 6, Page 75)

4.4.1 MSC Initiating an Authentication Request INVOKE

The MSC shall start the authentication request process:

a. when an authentication capable MS accesses the system and the AuthenticationCapability for the MS is not available, and

b. when an authentication capable MS accesses the system and the MS's AuthenticationCapability status information indicates that authentication is required.

System accesses include autonomous registration, call origination, call termination, flash requests, power down (de-)registrations, and SMS page responses. On the assumption that the Anchor MSC is responsible for authenticating an MS before providing service, handoff into an MSC should not trigger the authentication request process in the new Serving MSC.

The Serving MSC shall perform the following:

1 IF authentication parameters were received:

1-1 Determine the value of the RandomVariable (RAND) used by the MS to compute its AuthenticationResponse (AUTHR) (see Annex A "Procedures for RANDC Verification").

1-2 IF the value of RandomVariable (RAND) cannot be determined:

1-2-1 IF the value of RANDC received from the MS corresponds to a RandomVariable (RAND) value that may have been transmitted by a neighboring MSC:

1-2-1-1 Execute the "MSC Initiation of Random Variable Request" task (Section 4.34.1).

1-2-1-2 IF the random variable request is unsuccessful:

1-2-1-2-1 Execute the "MSC Initiation of a Authentication Failure Report" task (Section 4.3.1) with a ReportType parameter value of .

1-2-1-2-2 Exit this task with an *authentication failed* indication.

1-2-1-3 ELSE (random variable request is successful):

1-2-1-3-1 The RandomVariable (RAND) value received from the neighboring MSC shall be treated as the RandomVariable (RAND) used by the MS for this system access.

1-2-1-3-2 Continue this task.

1-2-1-4 ENDIF.

1-2-2 ELSE:

1-2-2-1 Execute the "MSC Initiation of a Authentication Failure Report" task (Section 4.3.1) with a ReportType parameter value of .

1-2-2-2 Exit this task with an *authentication failed* indication.

1-2-3 ENDIF.

1-3 ENDIF.

2 ENDIF.

3 Include the SystemAccessType parameter set to indicate the type of access triggering the request (e.g., , , , ,).

4 Include the SystemCapabilities (SYSCAP) parameter indicating whether authentication parameters were requested for this system access.

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

~~6 Include the TransactionCapability parameter set to the current capabilities of the system.~~

6 IF the MSC is NDSS capable:

6-1 Include the TransactionCapability parameter set to the current capabilities of the system.

6-2 Include the ControlChannelMode (CCM) parameter set to indicate the operating mode of the MS.

6-3 Include the CDMANetworkIdentification (CDMANID) parameter set to identify the serving network.

6-4 Include the ServiceRedirectionCause parameter set to the reason of MS registration or access.

7 ENDIF.

8 IF authentication parameters were received:

8-1 Include the CallHistoryCount (COUNT) and AuthenticationResponse (AUTHR) parameters provided by the MS.

8-2 Include the RandomVariable (RAND) parameter used by the MS to compute the AuthenticationResponse (AUTHR) parameter.

8-3 Include the TerminalType (TERMTYP) parameter as declared by the MS.

8-4 IF the SystemAccessType parameter indicates a or with digits:

8-4-1 Include the Digits (Dialed) parameter set to the decrypted digits received from the MS.

8-4-2 IF the SystemAccessType parameter indicates a and air interface encoding of the dialed digits was not TBCD:

8-4-2-1 Include the AuthenticationData parameter set to the value used by the MS to compute the AuthenticationResponse (AUTHR).

8-4-3 ENDIF.

8-5 ENDIF.

8-6 IF the SystemAccessType parameter indicates a and the SignalingMessageEncryptionKey parameter was provided to the Serving MSC:

8-6-1 Include the ConfidentialityModes (CMODES-actual) parameter indicating the current status of Signaling Message Encryption.

8-7 ENDIF.

9 ENDIF.

10 Send an AuthenticationRequest INVOKE to the MSC's associated VLR.

11 Start the Authentication Request Timer (ART).

12 WAIT for an Authentication Request response:

13 WHEN a RETURN RESULT is received:

13-1 Stop timer (ART).

13-2 IF the message can be processed:

13-2-1 IF the AnalogRedirectRecord or the CDMARedirectRecord parameter is received (i.e., the MS is being redirected):

13-2-1-1 Return to the invoking process.

13-2-2 ENDIF.

13-2-3 IF the TerminalType (TERMTYP) parameter is received (i.e., the AC is using *TSB51* authentication procedures):

13-2-3-1 IF *TSB51* operation is supported:

13-2-3-1-1 Execute *TSB51* procedures for AuthenticationRequest (refer to *TIA/EIA TSB51*).

13-2-3-1-2 Return to the invoking process.

13-2-3-2 ELSE (*TSB51* operation is not supported):

13-2-3-2-1 Execute the "Local Recovery Procedures" task (see 3.5.1).

13-2-3-2-2 Return to the invoking process.

13-2-3-3 ENDIF.

13-2-4 ELSE (the TerminalType (TERMTYP) parameter is not received, i.e., the AC is using *IS-41-C* authentication procedures):

13-2-4-1 Execute the "MSC Receiving Authentication Parameters" task (see 4.1.6) using the parameters received.

13-2-4-2 Return to the invoking process.

13-2-5 ENDIF.

13-3 ELSE (the message cannot be processed):

13-3-1 Execute the "Local Recovery Procedures" task (see 3.5.1).

13-3-2 Return to the invoking process with an *authentication failed* indication.

13-4 ENDIF.

14 WHEN a RETURN ERROR or REJECT is received:

14-1 Stop timer (ART).

14-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

14-3 Return to the invoking process with an *authentication failed* indication.

15 WHEN timer (ART) expires:

15-1 Execute the "Local Recovery Procedures" task (see 3.5.1).

15-2 Return to the invoking process with an *authentication failed* indication.

16 ENDWAIT.

4.4.2 VLR Receiving AuthenticationRequest INVOKE

When a VLR receives an AuthenticationRequest INVOKE, it shall perform the following:

1 IF the received message can be processed:

1-1 IF the indicated MS's AuthenticationCapability status information indicates that authentication is not required:

1-1-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-1-2 Exit this task.

1-2 ENDIF.

1-3 IF the MS is not allowed to register (e.g., the MS is on a negative list or registration attempts for the MS from same MSCID and LocationAreaID have failed in the recent past or the request is within a previously received DeniedAuthorizationPeriod):

1-3-1 Include the DenyAccess parameter set to .

1-3-2 Send a RETURN RESULT to the requesting MSC.

1-3-3 Exit this task.

1-4 ENDIF.

1-5 IF the SharedSecretData (SSD) was provided to the VLR:

1-5-1 IF the ~~MobileIdentificationNumber~~ MSID and ElectronicSerialNumber parameters reported by the MS cannot be validated:

1-5-1-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-1-2 Include the ReportType parameter set to .

1-5-1-3 Execute the "VLR Initiating an Authentication Failure Report" task (see 4.3.5).

1-5-1-4 Exit this task.

1-5-2 ENDIF.

1-5-3 IF the TerminalType (TERMTYP) reported for the MS is invalid:

1-5-3-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-3-2 Execute the "VLR Initiating an Authentication Failure Report" task (see 4.3.5) with the ReportType parameter set to indicate .

1-5-3-3 Exit this task.

1-5-4 ENDIF.

1-5-5 IF the SystemAccessType is , , , or :1-5-5-1 IF the received SystemCapabilities (SYSCAP) parameter indicates that the Serving MSC requested authentication parameters for this system access (in the Overhead Message Train):

1-5-5-1-1 IF authentication parameters were not received from the MS:

1-5-5-1-1-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-5-1-1-2 Execute the "VLR Initiating an Authentication Failure Report" task (see 4.3.5) with the ReportType parameter set to indicate .

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

1-5-5-1-2 ELSE (authentication parameters were received from the MS):

1-5-5-1-2-1 Convert values in the Digits (Dialed) parameter into TBCD encoding.

1-5-5-1-2-2 Execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the VLR's database and the parameters requested by the SystemAccessType.

1-5-5-1-2-3 IF the CAVE authentication result and the AuthenticationResponse (AUTHR) received from the MS (see Annex C "Authentication Response Verification") do not match:

1-5-5-1-2-3-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-5-1-2-3-2 Execute the "VLR Initiating an Authentication Failure Report" task (see 4.3.5) with the ReportType parameter set to indicate .

1-5-5-1-2-3-3 Exit this task.

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

1-5-5-1-2-5 IF the stored count and the CallHistoryCount (COUNT) reported by the MS do not match:

1-5-5-1-2-5-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-5-1-2-5-2 Include the CallHistoryCount (COUNT) parameter set to the COUNT reported by the MS.

1-5-5-1-2-5-3 Include the CallHistoryCountExpected parameter set to the COUNT expected by the VLR.

1-5-5-1-2-5-4 Execute the "VLR Initiating an Authentication Failure Report" task (see 4.3.5) with the ReportType parameter set to indicate .

1-5-5-1-2-5-5 Exit this task.

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

1-5-5-1-2-7 IF the SystemAccessType is or :

1-5-5-1-2-7-1 Generate the SignalingMessageEncryptionKey (SMEKEY) parameter.

1-5-5-1-2-7-2 Include the SignalingMessageEncryptionKey (SMEKEY) parameter.

1-5-5-1-2-7-3 IF the MS's Service Profile indicates that the MS subscribes to Voice Privacy:

1-5-5-1-2-7-3-1 IF the MS supports :

1-5-5-1-2-7-3-1-1 Generate the VoicePrivacyMask (VPMASK).

1-5-5-1-2-7-3-1-2 Include the VoicePrivacyMask (VPMASK) parameter.

1-5-5-1-2-7-3-2 ELSEIF the MS supports :

1-5-5-1-2-7-3-2-1 Generate the CDMAPrivateLongCodeMask (CDMAPLCM).

1-5-5-1-2-7-3-2-2 Include the CDMAPrivateLongCodeMask (CDMAPLCM) parameter.

1-5-5-1-2-7-3-3 ENDIF.

1-5-5-1-2-7-4 ENDIF.

1-5-5-1-2-8 ENDIF.

1-5-5-1-3 ENDIF.

1-5-5-2 ENDIF.

1-5-6 ELSEIF the SystemAccessType is and the ConfidentialityModes (CMODES-Actual) parameter is received and the ConfidentialityModes (CMODES-Actual) indicates that Signaling Message Encryption is inactive:

1-5-6-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the VLR's database to produce an AuthenticationResponseUnique (AUTHU).

1-5-6-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.

1-5-6-3 Mark the MS *pending Unique Challenge*.

1-5-7 ENDIF.

1-5-8 IF local administrative procedures request that a Unique Challenge shall be initiated:

1-5-8-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the VLR's database to produce an AuthenticationResponseUnique (AUTHU).

1-5-8-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.

1-5-8-3 Mark the MS *pending Unique Challenge*

1-5-9 ENDIF.

1-5-10 IF local administrative procedures request that a COUNT update shall be initiated:

1-5-10-1 Include the UpdateCount (UPDCOUNT) parameter.

1-5-10-2 Mark the MS *pending COUNT update*.

1-5-11 ENDIF.

1-5-12 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-13 IF the MS is marked *pending Unique Challenge*, OR IF the MS is marked *pending COUNT update*:

1-5-13-1 Execute the "VLR Awaiting AuthenticationStatusReport INVOKE" task (see 4.5.2).

1-5-14 ENDIF.

1-5-15 Exit this task.

1-6 ELSE (the SharedSecretData (SSD) was not provided to the VLR):

1-6-1 Relay the SystemCapabilities (SYSCAP) parameter modified to indicate whether the VLR is able to perform .

1-6-2 Include the SenderIdentificationNumber set to the identification number of the sending functional entity.

1-6-3 Relay all other received parameters.

1-6-4 IF the VLR is sending the message to an SS7 network.

1-6-4-1 Include the PC_SSN parameter with the Type field set to *VLR* and the PC and SSN fields set to the VLR's point code and subsystem number.

1-6-5 ENDIF.

1-6-6 Send an AuthenticationRequest INVOKE to the HLR associated with the MS.

1-6-7 Start the Authentication Request Timer (ART).

1-6-8 WAIT for an Authentication Request response:

1-6-9 WHEN a RETURN RESULT is received:

1-6-9-1 Stop timer (ART).

1-6-9-2 IF the message can be processed:

1-6-9-2-1 IF the TerminalType (TERMTYP) parameter is received (i.e., the AC is using *TSB51* authentication procedures):

1-6-9-2-1-1 IF *TSB51* operation is supported:

1-6-9-2-1-1-1 Execute *TSB51* procedures for AuthenticationRequest (refer to *TIA/EIA TSB51*).

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

1-4-9-2-1-2 ELSE (*TSB51* operation is not supported):

1-6-9-2-1-2-1 Execute the "Local Recovery Procedures" task (see 3.5.1).

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

1-6-9-2-1-3 ENDIF.

1-6-9-2-2 ELSE (the TerminalType (TERMTYP) parameter is not received, i.e., the AC is using *IS-41-C* authentication procedures):

1-6-9-2-2-1 IF the DenyAccess parameter is received:

1-6-9-2-2-1-1 Relay the received DenyAccess parameter.

1-6-9-2-2-2 ENDIF.

1-6-9-2-2-3 IF the SSDNotShared (NOSSD) parameter is received:

1-6-9-2-2-3-1 Remove the MS's current SharedSecretData (SSD) and AuthenticationAlgorithmVersion (AAV) from the VLR's database.

1-6-9-2-2-4 ENDIF.

1-6-9-2-2-5 IF the RandomVariableSSD (RANDSSD) is received:

1-6-9-2-2-5-1 IF SharedSecretData (SSD) is shared:

1-6-9-2-2-5-1-1 Remove the MS's current SharedSecretData (SSD) and AuthenticationAlgorithmVersion (AAV) from the VLR's database.

1-6-9-2-2-5-2 ENDIF.

1-6-9-2-2-5-3 Relay the received RandomVariableSSD (RANDSSD) parameter.

1-6-9-2-2-5-4 Mark the MS *pending SSD update*.

1-6-9-2-2-5-5 IF the SharedSecretData (SSD) parameter is received:

1-6-9-2-2-5-5-1 Store the pending SharedSecretData (SSD) value.

1-6-9-2-2-5-5-2 IF the AuthenticationAlgorithmVersion (AAV) parameter is received:

1-6-9-2-2-5-5-2-1 Store the AuthenticationAlgorithmVersion (AAV) value.

1-6-9-2-2-5-5-3 ENDIF.

1-6-9-2-2-5-5-4 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the pending

SharedSecretData (SSD) to produce an AuthenticationResponseUnique (AUTHU).

1-6-9-2-2-5-5-5 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.

1-6-9-2-2-5-5-6 Mark the MS *pending Unique Challenge*.

1-6-9-2-2-5-6 ELSE (SharedSecretData (SSD) parameter not received):

1-6-9-2-2-5-6-1 Relay the RandomVariableUniqueChallenge (RANDU) parameter.

1-6-9-2-2-5-6-2 Relay the AuthenticationResponseUnique (AUTHU) parameter.

1-6-9-2-2-5-6-3 Mark the MS *pending Unique Challenge*.

1-6-9-2-2-5-7 ENDIF.

1-6-9-2-2-6 ELSE (RandomVariableSSD (RANDSSD) not received):

1-6-9-2-2-6-1 IF the SharedSecretData (SSD) parameter is received:

1-6-9-2-2-6-1-1 Store the SharedSecretData (SSD).

1-6-9-2-2-6-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter is received:

1-6-9-2-2-6-1-2-1 Store the AuthenticationAlgorithmVersion (AAV) value.

1-6-9-2-2-6-1-3 ENDIF.

1-6-9-2-2-6-1-4 IF the CallHistoryCount (COUNT) parameter is received:

1-6-9-2-2-6-1-4-1 Store the received CallHistoryCount (COUNT) value.

1-6-9-2-2-6-1-5 ENDIF.

1-6-9-2-2-6-2 ENDIF.

1-6-9-2-2-6-3 IF the RandomVariableUniqueChallenge (RANDU) is received:

1-6-9-2-2-6-3-1 Relay the received RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.

1-6-9-2-2-6-3-2 Mark the MS *pending Unique Challenge*.

1-6-9-2-2-6-4 ENDIF.

1-6-9-2-2-7 ENDIF.

1-6-9-2-2-8 IF UpdateCount (UPDCOUNT) is received:

1-6-9-2-2-8-1 Relay the received UpdateCount (UPDCOUNT) parameter.

1-6-9-2-2-8-2 Mark the MS *pending COUNT update*.

1-6-9-2-2-9 ENDIF.

1-6-9-2-2-10 IF the SignalingMessageEncryptionKey (SMEKEY) is available:

1-6-9-2-2-10-1 Relay the SignalingMessageEncryptionKey (SMEKEY) parameter.

1-6-9-2-2-11 ENDIF.

1-6-9-2-2-12 IF the VoicePrivacyMask (VPMASK) is received:

1-6-9-2-2-12-1 Relay the VoicePrivacyMask (VPMASK) parameter.

1-6-9-2-2-13 ENDIF.

1-6-9-2-2-14 IF the CDMAPrivateLongCodeMask (CDMAPLCM) is received:

1-6-9-2-2-14-1 Relay the CDMAPrivateLongCodeMask (CDMAPLCM) parameter.

1-6-9-2-2-15 ENDIF.

1-6-9-2-2-16 IF the AnalogRedirectRecord is received:

1-6-9-2-2-16-1 Relay the AnalogRedirectRecord.

1-6-9-2-2-17 ENDIF.

1-6-9-2-2-18 IF the CDMARedirectRecord is received:

1-6-9-2-2-18-1 Relay the CDMARedirectRecord.

1-6-9-2-2-19 ENDIF.

1-6-9-2-2-20 IF the ServiceRedirectionInfo is received:

1-6-9-2-2-20-1 Relay the ServiceRedirectionInfo parameter.

1-6-9-2-2-21 ENDIF.

1-6-9-2-2-22 IF the RoamingIndication is received:

1-6-9-2-2-22-1 Relay the RoamingIndication parameter.

1-6-9-2-2-23 ENDIF.

1-6-9-2-2-24 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-6-9-2-2-25 IF the MS is marked *pending SSD update*, OR IF the MS is marked *pending Unique Challenge*, OR IF the MS is marked *pending COUNT update*:

1-6-9-2-2-25-1 Execute the "VLR Awaiting AuthenticationStatusReport INVOKE" task (see 4.5.2).

1-6-9-2-2-26 ENDIF.

1-6-9-2-2-27 Exit this task.

1-6-9-2-3 ENDIF.

1-6-9-3 ELSE (the message cannot be processed):

1-6-9-3-1 Send a RETURN ERROR to the MSC with the Error Code indicating .

1-6-9-3-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

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

1-6-9-4 ENDIF.

1-6-10 WHEN a RETURN ERROR or REJECT is received:

1-6-10-1 Stop timer (ART).

1-6-10-2 CASE Error Code OF:

1-6-10-3 :

1-6-10-3-1 IF the parameter was originated from the initiating functional entity:

1-6-10-3-1-1 Send a RETURN ERROR with the Error Code indicating .

1-6-10-3-2 ELSE:

1-6-10-3-2-1 Send a RETURN ERROR with the Error Code indicating .

1-6-10-3-3 ENDIF.

1-6-10-4 *DEFAULT*:

1-6-10-4-1 Send a RETURN ERROR with the Error Code indicating .

1-6-10-5 ENDCASE.

1-6-10-6 Execute the “Local Recovery Procedures” task (see 3.5.1).

1-6-10-7 Exit this task.

1-6-11 WHEN timer (ART) expires:

1-6-11-1 Send a RETURN ERROR to the MSC with the Error Code indicating .

1-6-11-2 Execute the “Local Recovery Procedures” task (see 3.5.1).

1-6-11-3 Exit this task.

1-6-12 ENDWAIT.

1-7 ENDIF.

2 ELSE (the received message cannot be processed):

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

3 ENDIF.

4 Exit this task.

Table 8 VLR AuthenticationRequest Response

Problem Detection and Recommended Response from VLR to MSC									
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Notes**
RETURN ERROR Error Code									
									a
									a
						X			e
									a
		X							e
	X								b, e
									a
				X					d, e
			X						e
					X				d, e
									a
							X		d, e
									a
									a
									a
RETURN RESULT DenyAccess								X	c, e

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving VLR, or the requesting functional entity is not authorized.
2. A required VLR resource (e.g., internal memory record, VLR is fully occupied) is temporarily not available (e.g., congestion).
3. 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.

4. A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter digit values do not meet the BCD specification); or, two or more mutually exclusive parameters have been supplied (e.g., Digits (Dialed) parameter received, but SystemAccessType is not).
5. A supplied parameter value is unrecognized or has nonstandard values (e.g., *Not used*).
6. The supplied ~~MobileIdentificationNumber~~ MSID's ~~parameter's~~ AC (HLR) responded that the ~~MIN~~ MSID is not in the AC (HLR)'s range of ~~MINs~~ MSIDs or Directory Numbers (suspect routing error).
7. An optional parameter required by the AC (HLR) was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported () but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not received; or SystemAccessType indicated , but Digits (Dialed) parameter was not received).
8. The supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter's AC (HLR) responded that the ~~MIN~~ MS cannot be Authenticated because of the reason identified by the supplied DenyAccess parameter value.

Notes:

a. This Error Code is not an appropriate VLR response to an AuthenticationRequest transaction.
b. It is recommended that a VLR supports AuthenticationRequest transactions.
c. Only RETURN RESULT operations needing clarification have been included.
d. Include the in question as the FaultyParameter parameter.
e. This response may have been originated by the AC (HLR).

4.4.3 HLR Receiving AuthenticationRequest INVOKE

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

1 IF the received message can be processed:

1-2 IF the MS identity is within the range of the HLR:

1-2-1 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:

1-2-1-1 IF the HLR determines there is a more preferable system for the MS and decides to select the system for NDSS redirection:

1-2-1-1-1 IF the selected system is a CDMA system:

1-2-1-1-1-1 Include the CDMARedirectRecord of the selected system.

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

1-2-1-1-2-1 Include the AnalogRedirectRecord of the selected system.

1-2-1-1-3 ENDIF.

1-2-1-1-4 Include the ServiceRedirectionInfo of the selected system if available.

1-2-1-1-5 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-2-1-1-6 Send a RETURN RESULT to the requesting VLR.

1-2-1-1-7 Exit this task.

1-2-1-2 ENDIF.

1-2-2 ENDIF.

1-3 ENDIF.

1-4 Include the MSID parameter set to identify the MS to the AC.

1-5 Include the SenderIdentificationNumber set to the identification number of the HLR.

1-6 Relay all other received parameters.

1-7 Send an AuthenticationRequest INVOKE to the AC associated with the MS.

1-8 Start the Authentication Request Timer (ART).

1-9 WAIT for an Authentication Request response:

1-10 WHEN a RETURN RESULT is received:

1-10-1 Stop timer (ART).

1-10-2 IF the message can be processed:

1-10-2-1 IF the SharedSecretData parameter is received:

1-10-2-1-1 IF the MIN may be needed for authentication calculations for the MS:

1-10-2-1-1-1 IF the MobileIdentificationNumber parameter was not present as the MSID parameter in the INVOKE ANDIF the MIN cannot be derived from the IMSI:

1-10-2-1-1-1-1 Include theMSID parameter set to identify the MS to the VLR.

1-10-2-1-1-2 ENDIF.

1-10-2-1-2 ENDIF.

1-10-2-2 ENDIF.

1-10-2-3 IF the MS's service profile indicates that the MS did not subscriber to Voice Privacy:

1-10-2-3-1 Discard any received VoicePrivacyMask (VPMASK) or CDMAPrivateLongCodeMask (CDMAPLCM) parameters.

1-10-2-4 ENDIF.

1-10-2-5 Relay all other received parameters.

1-10-2-6 Send a RETURN RESULT to the requesting VLR.

1-10-2-7 Exit this task.

1-10-3 ELSE (the message cannot be processed):

1-10-3-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating .

1-10-3-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-10-3-3 Exit this task.

1-10-4 ENDIF.

1-11 WHEN a RETURN ERROR or REJECT is received:

1-11-1 Stop timer (ART).

1-11-2 CASE Error Code OF:

1-11-3 :

1-11-3-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating .

1-11-4 *DEFAULT*:

1-11-4-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating .

1-11-5 ENDCASE.

1-11-6 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-11-7 Exit this task.

1-12 WHEN timer (ART) expires:

1-12-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating .

1-12-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-12-3 Exit this task.

1-13 ENDWAIT.

2 ELSE (the received message cannot be processed):

2-1 Send a RETURN ERROR to the requesting VLR.

3 ENDIF.

4 Exit this task

Table 9 HLR AuthenticationRequest Response

Problem Detection and Recommended Response from HLR to VLR									
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Notes**
RETURN ERROR Error Code									
									a
									a
						X			e
									a
		X							e
	X								b, e
									a
				X					d, e
			X						e
					X				d, e
									a
							X		d, e
									a
									a
									a
RETURN RESULT DenyAccess								X	c, e

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized.
2. A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion).
3. 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.
4. A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter digit values do not meet the BCD specification); or,

two or more mutually exclusive parameters have been supplied (e.g., Digits (Dialed) parameter received, but SystemAccessType is not).

5. A supplied parameter value is unrecognized or has nonstandard values (e.g., *Not used*).
6. The supplied ~~MobileIdentificationNumber~~ MSID ~~parameter~~ is not in the HLR's range of ~~MINs~~ MSIDs or Directory Numbers (suspect routing error).
7. An optional parameter required by the HLR (AC) was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported () but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not received; or SystemAccessType indicated , but Digits (Dialed) parameter was not received).
8. The supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter's AC (HLR) responded that the ~~MIN~~ MS cannot be Authenticated because of the reason identified by the supplied DenyAccess parameter value.

Notes:

a. This Error Code is not an appropriate HLR response to an AuthenticationRequest transaction.
b. It is recommended that a HLR supports AuthenticationRequest transactions.
c. Only RETURN RESULT operations needing clarification have been included.
d. Include the in question as the FaultyParameter parameter.
e. This response may have been originated by the AC.

4.32 Qualification Directive

(*N.S0005-0 v 1.0* Chapter 6, Page 205)

4.32.1 HLR Initiating a Qualification Directive INVOKE

When an HLR detects that an MS's profile or qualification information is changed, or if HLR receives a request to suppress or activate the NDSS feature, it shall perform the following:

1 IF the MS's current serving VLR is known:

1-1 IF the NDSS feature is activated and the HLR decides to redirect the MS:

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

1-1-1-1 Include the CDMARedirectRecord of the selected system.

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

1-1-2-1 Include the AnalogRedirectRecord of the selected system.

1-1-3 ENDIF.

1-1-4 Include the ServiceRedirectionInfo parameter if available.

1-2 ELSEIF the NDSS is suppressed:

1-2-1 Include the ServiceRedirectionInfo parameter.

1-3 ENDIF.

1-4 Include the ElectronicSerialNumber parameter set to the MS's ESN.

1-5 Include the ~~MobileIdentificationNumber~~ MSID parameter set to identify the MS to the MSC ~~the MS's MIN~~.

1-6 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-7 IF the MS is not authorized:

1-7-1 Include the AuthorizationDenied parameter.

1-7-2 Include the DeniedAuthorizationPeriod parameter set appropriately.

1-7-3 Set the QualificationInformationCode to .

1-8 ELSEIF only profile is to be updated:

1-9-1 Execute the "Loading of Profile Parameters" task (see 3.1.3).

1-10-2 Set the QualificationInformationCode to .

1-11 ELSEIF only validation parameters are to be updated:

1-11-1 Include the AuthorizationPeriod parameter set appropriately.

1-11-2 Set the QualificationInformationCode to .

1-12 ELSEIF profile and validation parameters are to be updated:

1-12-1 Execute the "Loading of Profile Parameters" task (see 3.1.3).

1-12-2 Include the AuthorizationPeriod parameter set appropriately.

1-12-3 Set the QualificationInformationCode to .

1-13 ENDIF.

1-14 Send a QualificationDirective INVOKE to the MS's current serving VLR.

1-15 Start the Qualification Directive Timer (QDT).

1-16 WAIT for a Qualification Directive response:

1-17 WHEN a RETURN RESULT is received:

1-17-1 Stop timer (QDT).
1-17-2 IF the message cannot be processed:
1-17-2-1 Execute "Local Recovery Procedures" task (see 3.5.1).
1-17-3 ENDIF.
1-18 WHEN a RETURN ERROR or REJECT is received:
1-18-1 Stop timer (QDT).
1-18-2 Execute "Local Recovery Procedures" task (see 3.5.1).
1-19 WHEN timer (QDT) expires:
1-19-1 Execute "Local Recovery Procedures" task (see 3.5.1).
1-20 ENDWAIT.

2 ENDIF.

3 Exit this task.

4.32.3 VLR Initiating a Qualification Directive INVOKE

When a VLR detects that an MS's profile or qualification information is changed, it shall perform the following:

1 Include the ElectronicSerialNumber parameter set to the MS's ESN.

2 Include the ~~MobileIdentificationNumber~~ MSID parameter set to the MSID that the mobile last registered with ~~MS's MIN.~~

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

4 Relay the CDMARedirectRecord if received.
5 Relay the AnalogRedirectRecord if received.
6 Relay the ServiceRedirectionInfo parameter if received.

7 IF the MS is not authorized:

7-1 Include the AuthorizationDenied parameter.
7-2 Include the QualificationInformationCode parameter set to .

8 ELSEIF only profile is to be updated:

8-1 Execute the "Loading of Profile Parameters" task (see 3.1.3).
8-2 Include the QualificationInformationCode parameter set to .

9 ELSEIF only validation parameters are to be updated:

9-1 Include the AuthorizationPeriod parameter set appropriately.
9-2 Include the QualificationInformationCode parameter set to .

10 ELSEIF profile and validation parameters are to be updated:

10-1 Execute the "Loading of Profile Parameters" task (see 3.1.3).
10-2 Include the AuthorizationPeriod parameter set appropriately.

10-3 Include the QualificationInformationCode parameter set to .

11 ENDIF.

12 Start the Qualification Directive Timer (QDT).

13 Send a QualificationDirective INVOKE to the MS's current Serving MSC.

14 WAIT for a Qualification Directive response:

15 WHEN a RETURN RESULT is received:

15-1 Stop timer (QDT).

15-2 IF the message cannot be processed:

15-2-1 Execute "Local Recovery Procedures" task (see 3.5.1).

15-3 ENDIF.

16 WHEN a RETURN ERROR or REJECT is received:

16-1 Stop timer (QDT).

16-2 Execute "Local Recovery Procedures" task (see 3.5.1).

17 WHEN timer (QDT) expires:

17-1 Execute "Local Recovery Procedures" task (see 3.5.1).

18 ENDWAIT.

19 Return to the calling task.

4.32.4 MSC Receiving QualificationDirective INVOKE

When an MSC receives a QualificationDirective INVOKE:

1 IF the received message can be processed:

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

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

1-2-2 Exit this task.

1-3 ELSEIF the ServiceRedirectionInfo parameter is received:

1-3-1 Send the MS the ServiceRedirectionInfo parameter.

1-3-2 Exit this task.

1-4 ENDIF.

1-5 IF AuthorizationDenied parameter is received:

1-5-1 IF the indicated MS is involved in a call or service operation anchored by this MSC:

1-5-1-1 The MSC may optionally discontinue the call or service operation currently in progress.

1-5-2 ENDIF.

1-5-3 Clear the subscriber's profile.

1-6 ELSEIF the indicated MS's profile information is received:

1-6-1 Overwrite any existing profile parameter(s) with the received value(s).

1-6-2 Add any new profile parameter(s) received to the MS's profile information.

1-6-3 Execute the "MSC MWN Status Change Invocation" task (see 5.13.9).

1-7 ENDIF.

1-8 Send a RETURN RESULT to the requesting VLR.

1-9 IF the indicated MS is involved in a call or service operation anchored by this MSC:

1-9-1 IF the MS is not authorized for the current call or service operation:

1-9-1-1 The Serving System may optionally discontinue the call or service operation currently in progress.

1-9-2 ENDIF.

1-10 ENDIF.

2 ELSE (the received message cannot be processed):

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 43 MSC QualificationDirective Response

Problem Detection and Recommended Response from MSC to VLR										
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Notes**
RETURN ERROR **Error Code**										
						X				
								X		
										a
										a
		X								
	X									b
										a
				X						d
			X							
					X					d
										a
									X	d
							X			
										a
										a
RETURN RESULT										c

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving MSC, or the requesting functional entity is not authorized.
2. A required MSC resource (e.g., internal memory record, MSC is fully occupied) is temporarily not available (e.g., congestion).
3. 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.
4. A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter digit values do not meet the BCD specification), a Digits parameter has an inconsistent length, digits in a Digits parameter do not meet the BCD specification, or two or more mutually exclusive optional parameters have been supplied (e.g., both AuthorizationDenied and AuthorizationPeriod).
5. A supplied parameter value is unrecognized or has nonstandard values (e.g., *Not used*, a supplied Digits parameter does not have an expected number of digits, a Digits parameter contains a Code 11, a Code 12, or an ST digit, a Digits parameter is using an unrecognized value for numbering plan, encoding, or type of digit), the OriginationIndicator is set to and an agreement does not exist).
6. An MSC record does not presently exist for the supplied MobileIdentificationNumber parameter.
7. An MSC record does not presently exist for the supplied InternationalMobileStationIdentity parameter.
8. An MSC record exists for the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter, but the supplied ElectronicSerialNumber parameter does not match the ESN in the MSC record.
9. An expected, or required, optional parameter (e.g., AuthorizationDenied, AuthorizationPeriod, OriginationIndicator, TerminationRestrictionCode, CallingFeaturesIndicator, Digits (Carrier)) was not received. A received optional parameter required the MSC to expect an additional optional parameter that was not received (e.g., OriginationIndicator value set to but the expected Digits (Destination) parameter was not received).

Notes:

a. This Error Code is not an appropriate MSC response to a QualificationDirective transaction.
b. It is recommended that an MSC supports QualificationDirective transactions.
c. Only RETURN RESULT operations needing clarification have been included.
d. Include the in question as the FaultyParameter parameter.

4.33 Qualification Request

(*N.S0005-0 v 1.0* Chapter 6, Page 210)

The Qualification Request Task is executed to retrieve the MS's qualification information or profile information or both. The HLR does not update the MS's current location pointer when the Qualification Request Task is executed.

4.33.1 MSC Initiating a QualificationRequest INVOKE

When an MSC determines that it needs to retrieve an MS's qualification information, profile information, or both; it shall perform the following:

1 Include the MSCID parameter set to the identity of the requesting MSC.

2 Include the SenderIdentificationNumber parameter of the sending functional entity.

3 Include the SystemAccessType parameter set to the type of access triggering the request.

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

5 Include the ~~MobileIdentificationNumber~~ MSID parameter set to identify the requesting MS.

6 Include the ElectronicSerialNumber parameter set to identify the requesting MS.

7 Include the QualificationInformationCode parameter set to indicate the required qualification information, profile information, or both.

8 IF the MSC is NDSS capable:

8-1 Include the ControlChannelMode (CCM) parameter set to indicate the operating mode of the MS.

8-2 Include the TerminalType parameter as declared by the MS.

8-3 Include the CDMANetworkIdentification (CDMANID) parameter set to identify the serving network.

8-4 Include the ServiceRedirectionCause parameter set to the reason of MS registration or access.

9 ENDIF.

10 Include the SystemMyTypeCode parameter set to indicate the manufacturer of the MSC.

11 Send a QualificationRequest INVOKE to its associated VLR.

12 Start the Qualification Request Timer (QRT).

13 WAIT for a Qualification Request response:

14 WHEN a RETURN RESULT is received:

14-1 Stop timer (QRT).

14-2 IF the message can be processed:

14-2-1 IF the AnalogRedirectRecord or the CDMARedirectRecord parameter is received (i.e., the MS is being redirected):

14-2-1-1 Return to the invoking process.

14-2-2 ENDIF.

14-2-1 IF an AuthorizationDenied parameter is received:

14-2-1-1 IF the indicated MS is involved in a call or service operation anchored by this MSC:

14-2-1-1-1 The Serving MSC may optionally discontinue the call or service operation currently in progress.

14-2-1-2 ENDIF.

14-2-1-3 Clear the subscriber's profile.

14-2-2 ELSEIF profile information for the indicated MS is received:

14-2-2-1 Overwrite any existing profile parameter(s) with the received value(s).

14-2-2-2 Add any new profile parameter(s) received to the MS's profile information.

14-2-2-3 Execute the "MSC MWN Status Change Invocation" task (see 5.13.9).

14-2-3 ENDIF.

14-3 ELSE (the message cannot be processed):

14-3-1 Execute "Local Recovery Procedures" task (see 3.5.1).

14-4 ENDIF.

15 WHEN a RETURN ERROR or REJECT is received:

15-1 Stop timer (QRT).

15-2 Execute "Local Recovery Procedures" task (see 3.5.1).

16 WHEN timer (QRT) expires:

16-1 Execute "Local Recovery Procedures" task (see 3.5.1).

17 ENDWAIT.

18 IF the indicated MS is involved in a call or service operation anchored by this MSC:

18-1 IF the service profile information does not authorize the current call or service operation:

18-1-1 The Serving System may optionally discontinue the call or service operation currently in progress.

18-2 ENDIF.

19 ENDIF.

20 Exit this task.

4.33.4 HLR Receiving QualificationRequest INVOKE

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

1 IF the received message can be processed:

1-2 IF the MS identity within the range of the HLR:

1-2-1 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:

1-2-1-1 IF the HLR determines there is a more preferable system for the MS and decides to select the system for NDSS redirection:

1-2-1-1-1 IF the selected system is a CDMA system:

1-2-1-1-1-1 Include the CDMARedirectRecord of the selected system.

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

1-2-1-1-2-1 Include the AnalogRedirectRecord of the selected system.

1-2-1-1-3 ENDIF.

1-2-1-1-4 Include the ServiceRedirectionInfo of the selected system if available.

1-2-1-1-5 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.

1-2-1-1-6 Send a RETURN RESULT to the requesting VLR.

1-2-1-1-7 Exit this task.

1-2-1-2 ENDIF.

1-2-2 ENDIF.

1-3 ENDIF.

1-4 IF the MS is authorized for the service:

1-4-1 IF the received QualificationInformationCode parameter is or :

1-4-1-1 Execute the “Loading of Profile Parameters” task (see 3.1.3).

1-4-2 ENDIF.

1-4-3 IF the received QualificationInformationCode parameter is or :

1-4-3-1 Include the AuthorizationPeriod parameter set appropriately.

1-4-4 ENDIF.

1-5 ELSE:

1-5-1 Include the AuthorizationDenied parameter set appropriately.

1-5-2 Include the DeniedAuthorizationPeriod parameter set appropriately.

1-6 ENDIF.

1-7 Send a RETURN RESULT to the requesting VLR.

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 45 HLR QualificationRequest Response

Problem Detection and Recommended Response from HLR to VLR											
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Notes**
RETURN ERROR Error Code											
											a
											a
						X					
											a
		X									
	X										b
											a
				X							d
			X								
					X						d
											a
							X				d
											a
											a
											a
RETURN RESULT AuthorizationDenied											c
										X	
									X		
										X	
										X	
								X			
										X	
										X	
										X	
										X	
										X	

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized.
2. A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion).

3. 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.
4. A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter digit values do not meet the BCD specification).
5. A supplied parameter value is unrecognized or has nonstandard values (e.g., *Not used*).
6. The supplied ~~MobileIdentificationNumber~~ MSID ~~parameter~~ is not in the HLR's range of ~~MINs~~ MSIDs or Directory Numbers (suspect routing error).
7. An expected, or required, optional parameter (e.g., AuthorizationDenied, AuthorizationPeriod, OriginationIndicator, TerminationRestrictionCode, CallingFeaturesIndicator, or a Digits (Carrier)) was not received. A received optional parameter required the VLR to expect an additional optional parameter that was not received (e.g., OriginationIndicator value set to , but the expected Digits (Destination) parameter was not received).
8. The supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter is within the range of the HLR, but the ~~MIN~~ MSID is not presently assigned to a subscriber.
9. The supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter is within the range of the HLR, but the supplied ElectronicSerialNumber parameter is not valid for the MIN or IMSI record.
10. The supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter is within the range of the HLR, but the MIN or IMSI is either a , , , , , , , or .

Notes:

a. This Error Code is not an appropriate HLR response to a QualificationRequest transaction.
b. It is recommended that an HLR supports QualificationRequest transactions.
c. Only RETURN RESULT operations needing clarification have been included.
d. Include the in question as the FaultyParameter parameter.

4.38 Registration Notification (N.S0005-0 v 1.0 Chapter 6, Page 233)

4.38.1 MSC Initiating MS Registration INVOKE

When an MSC determines that a roaming Mobile Station (MS) is now within its service area (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), 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.

3 IF the access occurred in a border cell:

3-1 Include the BorderCellAccess parameter with a value of .

3-2 The MSC should include the ReceivedSignalQuality parameter set to the signal strength of the received access.

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

3-4 The MSC should include the SystemAccessData parameter set to the cell site information.

4 ENDIF.

5 IF the MSC is authentication capable:

5-1 Include the SystemCapabilities (SYSCAP) parameter set to indicate the authentication-related capabilities of this system.

6 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:

6-1 Include the ReportType (RPTTYP) parameter indicating .

7 ENDIF.

8 Include the ElectronicSerialNumber parameter set to identify the MS.

9 Include the ~~MobileIdentificationNumber~~ MSID parameter set to identify the MS.

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

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

12 IF the MSC is NDSS capable:

12-1 Include the ControlChannelMode (CCM) parameter set to indicate the operating mode of the MS.

12-2 Include the CDMANetworkIdentification (CDMANID) parameter set to identify the serving network.

12-4 Include the ServiceRedirectionCause parameter set to the reason of MS registration or access.

13 ENDIF.

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

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

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

16-1 Include the PC_SSN parameter with the Type set to and the PC and SSN fields set to the MSC's point code and subsystem number.

17 ENDIF.

18 IF the MS and MSC are SMS capable:

18-1 Include the SMS_Address parameter set to be used to route SMS messages to the MS.

19 ENDIF.

~~19 IF the MSC supports local SPINI operation:~~

~~19-1 Include the TransactionCapability parameter indicating local SPINI operation supported.~~

~~20 ENDIF.~~

20 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):

20-1 Include the AvailabilityType parameter set to AvailabilityType: *Unspecified mobile inactivity type*.

21 ENDIF.

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

23 Start the Registration Notification Timer (RNT).

24 WAIT for a Registration Notification response:

25 WHEN a RETURN RESULT is received:

25-1 Stop timer (RNT).

25-2 IF the message can be processed:

25-2-1 IF the AnalogRedirectRecord or the CDMARedirectRecord parameter is received (i.e., the MS is being redirected):

25-2-1-1 Return to the invoking process.

25-2-2 ENDIF.

25-2-1 IF the message contained an AuthorizationDenied parameter:

25-2-1-2 IF the indicated MS is involved in a call or service operation anchored by this MSC:

25-2-1-2-1 The Serving System may optionally discontinue the call or service operation currently in progress.

25-2-1-3 ENDIF.

25-2-1-4 IF a record exists for the indicated MS:

25-2-1-4-1 Clear the subscriber's profile.

25-2-1-5 ENDIF.

25-2-2 ELSE:

25-2-2-1 Update the MS's service profile and qualification information with the received parameters.

25-2-2-2 IF the SMS_MessageWaitingIndicator parameter was received:

25-2-2-2-1 Set the *SMS Delivery Pending Flag* for this MS.

25-2-2-3 ENDIF.

25-2-2-4 Execute the "MSC MWN Status Change Invocation" task (see 5.13.9).

25-2-2-5 IF the indicated MS is involved in a call or service operation anchored by this MSC:

25-2-2-5-1 IF the service profile parameters do not authorize the current call or service operation:

25-2-2-5-1-1 The Serving System may optionally discontinue the call or service operation currently in progress.

25-2-2-5-2 ENDIF.

25-2-2-6 ENDIF.

25-2-3 ENDIF.

25-3 ELSE (the message cannot be processed):

25-3-1 Execute “Local Recovery Procedures” task (see 3.5.1).

25-4 ENDIF.

26 WHEN a RETURN ERROR OR REJECT is received:

26-1 Stop timer (RNT).

26-2 Execute “Local Recovery Procedures” task (see 3.5.1).

27 WHEN timer (RNT) expires:

27-1 Execute “Local Recovery Procedures” task (see 3.5.1).

28 ENDWAIT.

29 Exit this task.

4.38.3 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 :[4]

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 .

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:

[4]The HLR may record the time at which the message was received as described in informative Annex F.

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:

1-5-1 Update the current VLR location of the MS.

1-5-2 IF the MS is registered with a different VLR:

1-5-2-1 IF the received SystemAccessType parameter indicates :

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

1-5-2-1-1-1 Include the ReceivedSignalQuality, ControlChannelData and SystemAccessData parameters according to the values received with the best RegistrationNotification INVOKE received for this access.

1-5-2-1-2 ENDIF.

1-5-2-2 ENDIF.

1-5-2-3 Execute the “HLR Initiating Registration Cancellation” task (see 4.37.1).

1-5-2-4 IF the CancellationDenied parameter is received:

1-5-2-4-1 Include the AuthorizationDenied parameter set to .

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

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

1-5-2-4-3 ENDIF.

1-5-2-4-4 Restore the current VLR location of the MS.

1-5-2-4-5 Include the SystemMyTypeCode parameter set to the HLR’s manufacturer.

1-5-2-4-6 Send a RETURN RESULT to the requesting VLR.

1-5-2-4-7 Exit this task.

1-5-2-5 ELSE (no CancellationDenied parameter received):

1-5-2-5-1 Relay any received parameters, except the SMS_MessageWaitingIndicator parameter, from the RegistrationCancellation RETURN RESULT.

1-5-2-6 ENDIF.
1-5-3 ELSE (the MS is registered with the same VLR):
1-5-3-1 IF an SMS_MessageWaitingIndicator parameter was received:
1-5-3-1-1 Set the *SMS Delivery Pending Flag* for this MS.
1-5-3-2 ENDIF.
1-5-4 ENDIF.
1-5-5 IF the QualificationInformationCode indicates or *:*
1-5-5-1 Execute the "Loading of Profile Parameters" task (see 3.1.3).
1-5-6 ENDIF.
1-5-7 IF the QualificationInformationCode indicates or *:*
1-5-7-1 Include the AuthorizationPeriod parameter set appropriately.
1-5-8 ENDIF.
1-5-9 IF an SMS_Address parameter is received with the RegistrationNotification INVOKE:
1-5-9-1 IF an AvailabilityType parameter is NOT received with the RegistrationNotification INVOKE:
1-5-9-1-1 IF SMS service is authorized for the MS on the current serving system:
1-5-9-1-1-1 IF the *SMS Delivery Pending Flag* is set for this MS:
1-5-9-1-1-1-1 Include the SMS_MessageWaitingIndicator parameter.
1-5-9-1-1-2 ENDIF.
1-5-9-1-2 ENDIF.
1-5-9-2 ENDIF.
1-5-10 ENDIF.
1-5-11 Include the RoamingIndication parameter of the serving MSC if available.
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 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):
1-10-1 IF an AvailabilityType parameter was NOT received with the RegistrationNotification INVOKE:
1-10-1-1 IF SMS service is authorized for the MS on the current serving system:
1-10-1-1-1 Optionally set the temporary SMS routing address to the received SMS_Address.
1-10-1-1-2 IF the *SMS Delivery Pending Flag* is set for this MS:
1-10-1-1-2-1 Clear the *SMS Delivery Pending Flag*.

1-10-1-1-2-2 Execute the "HLR Initiating SMSNotification INVOKE" task (see 4.47.1).

1-10-1-1-3 ENDIF.

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

1-10-1-2-1 GOTO SMS Not Available.

1-10-1-3 ENDIF.

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

1-10-2-1 GOTO SMS Not Available.

1-10-3 ENDIF.

1-11 ELSE (no SMS_Address parameter was received):

SMS Not Available:

1-11-2 Set the SMS status to *unavailable*.

1-11-3 Clear the temporary SMS routing address.

1-11-4 Optionally, IF the MC is to be informed of MS unavailability:

1-11-4-1 Include the SMS_AccessDeniedReason parameter set to .

1-11-4-2 Execute the "HLR Initiating SMSNotification INVOKE" task (see 4.47.1).

1-11-5 ENDIF.

1-12 ENDIF.

1-13 IF an AvailabilityType parameter was received in the RegistrationNotification INVOKE:

1-13-1 Set the MS's state to *inactive*.

1-14 ELSE:

1-14-1 Set the MS's state to *active*.

1-15 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 52 HLR RegistrationNotification Response

Problem Detection and Recommended Response from HLR to VLR											
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Notes**
RETURN ERROR **Error Code**											
											a
											a
						X					
											a
		X									
	X										b
											a
				X							d
			X								
					X						d
											a
							X				d
											a
											a
											a
RETURN RESULT **AuthorizationDenied**											c
										X	
									X		
										X	
										X	
								X			
										X	
										X	
										X	
										X	

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized.
2. A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion).
3. 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.
4. A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or InternationalMobileStationIdentity parameter digit values do not meet the BCD specification).
5. A supplied parameter value is unrecognized or has nonstandard values (e.g., *Not used*).
6. The supplied ~~MobileIdentificationNumber~~ MSID is not in the HLR's range of ~~MIN~~ MSIDs or directory numbers (suspect routing error).
7. An expected, or required, optional parameter (e.g., PC_SSN) was not received.
8. The supplied ~~MobileIdentificationNumber~~ MSID ~~parameter~~ is within the range of the HLR, but the ~~MIN~~ MSID is not presently assigned to a subscriber.
9. The supplied ~~MobileIdentificationNumber~~ MSID ~~parameter~~ is within the range of the HLR, but the supplied ElectronicSerialNumber parameter is not valid for the ~~MIN~~ MSID's record.

10. The supplied ~~MobileIdentificationNumber~~ MSID ~~parameter~~ is within the range of the HLR, but the ~~MIN~~ MSID is either a , , , , , , or .

Notes:

a. This Error Code is not an appropriate HLR response to a RegistrationNotification transaction.
b. It is recommended that an HLR supports RegistrationNotification transactions.
c. Only RETURN RESULT operations needing clarification have been included.
d. Include the in question as the FaultyParameter parameter.

4.E Parameter Request

(*N.S0005-0 v 1.0* Chapter 6, page 204)

4.E.1 Serving MSC Initiation of a ParameterRequest INVOKE

When a Serving MSC determines that it needs to retrieve the parameters associated with a MS (e.g., MS registration or page response contains a TMSI), it shall perform the following:

1 Include the appropriate MSID parameter set to identify the MS.

2 Include the RequiredParametersMask parameter.

3 Send a ParametersRequest INVOKE to the serving VLR.

4 Start the Parameter Request Timer (PRT).

5 WAIT for a Parameters Request response:

6 WHEN a RETURN RESULT is received:

6-1 Stop the Parameter Request Timer (PRT).
6-2 IF the message can be processed:
6-2-1 IF ReasonList is received:
6-2-1-1 Provide the treatment indicated in the ReasonList parameter.
6-2-2 ELSE (ReasonList was not received):
6-2-2-1 Store the MS's paging information (MSID, ESN, etc.) and the associated TMSI for future use.
6-2-3 ENDIF.
6-3 ELSE (the message can not be processed):
6-3-1 Execute "Local Recovery Procedures" task (see 3.5.1).
6-3-2 Exit this task.
6-4 ENDIF.

7 WHEN a RETURN ERROR or REJECT is received:

7-1 Stop timer (PRT).
7-2 Execute "Local Recovery Procedures" task (see 3.5.1).

8 WHEN timer (PRT) expires:

8-1 Execute "Local Recovery Procedures" task (see 3.5.1).

9 ENDWAIT.

10 Exit this task.

4.E.2 Serving VLR Receiving ParameterRequest INVOKE

When an Serving VLR receives a ParametersRequest INVOKE, it shall perform the following:

1 IF the received message can be processed:

1-1 Include the required parameters.

1-2 Send a RETURN RESULT to the requesting MSC.

2 ELSE (the message can not be processed):

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

3 ENDIF.

4 Exit this task.

Table 4.E.2-1 Serving VLR ParametersRequest Response

Problem Detection and Recommended Response from serving VLR to the serving MSC												
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Notes**
RETURN ERROR **Error Code**												
									X			
											X	
												a
												a
		X										
	X											
												a
				X								**b**
			X									
					X							**b**
												a
						X						**b**
										X		
Unrecognized TMSI							**X**					
TMSI/VLRMismatch								**X**				
RETURN RESULT												**c**

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving VLR, or the requesting network node is not authorized.

2. A required VLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion).

3. A required resource (e.g., data base access, network element) is not presently accessible due to a failure. Human intervention may be required for resolution.

4. A supplied parameter value has an encoding problem (e.g., The supplied MSID parameter digit values do not meet the BCD specification).

5. A supplied parameter value is unrecognized or has non-standard values (e.g., *Not used*).

6. An optional parameter required by the new serving VLR was expected but not received (e.g., only MSID and ElectronicSerialNumber parameters received).

7. The supplied TMSI_ZONE parameter is within the range of the VLR, but the supplied TMSI_CODE parameter is not valid for the TMSI_ZONE stored in receiving VLR.

8. The supplied TMSI_ZONE parameter is not in the VLR's range of TMSI zone number (suspect routing error).

9. An VLR record doesn't presently exist for the supplied MobileIdentificationNumber.

10. An VLR record doesn't presently exist for the supplied InternationalMobileStationIdentity.

11. An VLR record exists for MSID but the supplied ESN parameter doesn't match the ESN in the VLR record.

Notes:

a. This Error Code is not an appropriate VLR response to an Parameter Request transaction.

b. Only RETURN RESULT operations needing clarification have been included.

c. Include the in question as the FaultyParameter parameter.

4.E.3 New Serving VLR Initiation of a ParametersRequest

When an new serving VLR determines that it needs to retrieve the MS's MSID and ESN, it shall perform the following:

1 Include the NetworkTMSI parameter set to identify the MS.

2 Include the RequiredParametersMask parameter.

3 Include the MSCID parameter set to the identity of the new serving VLR.

4 Include the SystemMyTypeCode parameter set to the VLR's manufacturer.

5 Include the SenderIN parameter set to the identification number of the sending functional entity.

6 IF the message is launched on an SS7 network:

6-1 Include the PC_SSN parameter for the VLR.

7 ENDIF.

8 Send a ParametersRequest INVOKE to the old serving VLR.

9 Start the Parameter Request Timer (PRT).

10 WAIT for a Parameter Request response:

11 WHEN a RETURN RESULT is received:

11-1 Stop the Parameter Request Timer (PRT).

11-2 IF the message can be processed:

11-2-1 IF ReasonList is received:

11-2-1-1 Provide the treatment indicated in the ReasonList parameter.

11-2-2 ENDIF.

11-3 ELSE (the message can not be processed):

11-3-1 Execute "Local Recovery Procedures" task (see 3.5.1)

11-3-2 Exit this task.

11-4 ENDIF.

12 WHEN a RETURN ERROR or REJECT is received:

12-1 Stop timer (PRT).

12-2 Execute "Local Recovery Procedures" task (see 3.5.1)

13 WHEN timer (PRT) expires:

13-1 Execute "Local Recovery Procedures" task (see 3.5.1)

14 ENDWAIT.

15 Exit this task.

4.E.4 Old Serving VLR Receiving ParameterRequest INVOKE

When an old Serving VLR receives a ParametersRequest INVOKE, it shall perform the following:

1 IF the received message can be processed:

1-1 Include the required parameters.

1-2 Send a RETURN RESULT to the requesting VLR.

2 ELSE (the message can not be processed):

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

3 ENDIF.

4 Exit this task.

Table 4.E.4-1 Old Serving VLR ParametersRequest Response

Problem Detection and Recommended Response from old serving VLR to the new serving VLR									
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Notes**
RETURN ERROR **Error Code**									
									a
									a
									a
									a
		X							
	X								**a**
									a
				X					**b**
			X						
					X				**b**
									a
						X			**b**
									a
Unrecognized TMSI							**X**		
TMSI/VLRMismatch								**X**	
RETURN RESULT									**c**

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving VLR, or the requesting network node is not authorized.

2. A required VLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (congestion).

3. A required resource (e.g., data base access, network element) is not presently accessible due to a failure. Human intervention may be required for resolution.

4. A supplied parameter value has an encoding problem (e.g., The supplied MSID parameter digit values do not meet the BCD specification).

5. A supplied parameter value is unrecognized or has non-standard values (e.g., *Not used*).

6. An optional parameter required by the new serving VLR was expected but not received (e.g., only MSID and ElectronicSerialNumber parameters received).

7. The supplied TMSI_ZONE is within the range of the VLR, but the supplied TMSI_CODE is not valid for the TMSI_ZONE stored in receiving VLR.

8. The supplied TMSI_ZONE is not in the VLR's range of TMSI zone number (suspect routing error).

Notes:

a. This Error Code is not an appropriate VLR response to an Parameter Request transaction.

b. Only RETURN RESULT operations needing clarification have been included.

c. Include the in question as the FaultyParameter parameter.

4.F TMSI DIRECTIVE

(*N.S0005-0 v 1.0* Chapter 6, page 295)

4.F.1 Serving VLR Initiation of a TMSIDirective INVOKE

When a Serving VLR determines that the NetworkTMSI associated with an MS must be assigned or reassigned, it shall start the TMSI directive process. For example, a new NetworkTMSI is assigned following initial registration, and may be assigned or reassigned during MS registration, origination, termination or periodically.

The VLR shall perform the following:

1 Include the ElectronicSerialNumber parameter set to identify the MS.

2 Include the MSID parameter set to identify the MS.

3 Include the NewNetworkTMSI parameter.

4 Include the NetworkTMSIExpirationTime (NETMSIT) parameter.5 IF there exists TMSI_ZONE and TMSI_CODE in the VLR:

5-1 Include the NetworkTMSI (NETMSI) parameter.

6 ENDIF.

7 Send a TMSIDirective INVOKE to the serving MSC .

8 Start the TMSIDirective Timer (TDT).

9 WAIT for a TMSIDirective response:

10 WHEN a RETURN RESULT is received:

10-1 Stop timer (TDT).
10-2 IF the message cannot be processed:
10-2-1 Execute the "Local Recovery Procedures" task (see 3.5.1).
10-2-2 Return to the invoking process with an indication of unsuccessful.
10-3 ELSE (the message can be processed):
10-3-1 IF ReasonList is received:
10-3-1-1 Provide the treatment indicated in the ReasonList parameter.
10-3-2 ENDIF.

10-3-3 IF DenyAccess and MS's ESN and IMSI are received:
10-3-3-1 Compare ESN and IMSI with stored ones.
10-3-3-2 IF they are not equal:
10-3-3-2-1 Re-initiate TMSI Directive.
10-3-2-3 ELSE:
10-3-2-3-1 Clear the profile of the MS.
10-3-2-4 ENDIF.
10-3-4 ENDIF.
10-3-5 Return to the invoking process with a successful indication.
10-4 ENDIF.

11 WHEN a RETURN ERROR or REJECT is received:

11-1 Stop Timer (TDT).
11-2 Execute the " Local Recovery Procedures" task (see 3.5.1).
11-3 Return to the invoking process with a unsuccessful indication.

12 WHEN timer (TDT) expires:

12-1 Execute the " Local Recovery Procedures" task (see 3.5.1).
12-2 Return to the invoking process with a unsuccessful indication.

13 ENDWAIT.

14 Exit this task.

4.F.2 MSC Receiving TMSIDirective INVOKE

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

1 IF the received message can be processed:

1-1 Send a TMSI Assignment message to the MS.
1-2 Start a TMSI Assignment timer.
1-3 WAIT for an MS response of TMSI assignment completion:
1-5 WHEN the response is received:
1-5-1 Stop the TMSI Assignment timer.
1-5-2 IF authentication parameters are included in the response from the MS:
1-5-2-1 Execute "MSC Initiating an Authentication Request" task (see 4.4.1) to authenticate the MS.
1-5-2-2 IF the MS is authentic:
1-5-2-2-1 Send an empty RETURN RESULT to the VLR.
1-5-2-2-2 Exit this task.
1-5-2-3 ELSE:
1-5-2-3-1 Send a Status Request message to the MS.
1-5-2-3-2 Start a Status Request timer.

1-5-2-3-2 WAIT for an MS response:
1-5-2-3-3 WHEN the response is received:
1-5-2-3-3-1 Stop the Status Request timer.
1-5-2-3-3-2 Include MS's IMSI and ESN received from the MS.
1-5-2-3-3-2 Include DenyAccess parameter.
1-5-2-3-3-2 Send a RETURN RESULT to the VLR.
1-5-2-3-3-3 Exit this task.
1-5-2-3-4 WHEN the Status Request timer expires:
1-5-2-3-4-1 Include ReasonList set to *No Response to TMSI assignment* .
1-5-2-3-4-2 Include DenyAccess.
1-5-2-3-4-3 Send a RETURN RESULT.
1-5-2-3-4-4 Exit this task.
1-5-2-4 ENDIF.
1-5-3 ELSE:
1-5-3-1 Send an empty RETURN RESULT to the VLR.
1-5-4 ENDIF.
1-6 WHEN the TMSI Assignment timer expires,
1-6-1 Include ReasonList set to *No Response to TMSI assignment*.
1-6-2 Send a RETURN RESULT.
1-7 ENDWAIT.

2 ELSE (the message cannot be processed):

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

3 ENDIF.

4 Exit this task.

Table 4.F.2-1 MSC TMSI Directive Response

Problem Detection and Recommended Response from MSC to VLR														
PROBLEM DEFINITION	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**Notes**
RETURN ERROR **Error Code**														
						X								
									X					
														a
											X			
		X												
	X													**b**
														a
				X										**d**
			X											
					X									**d**
														a
								X						**d**
							X							
Unrecognized TMSI										**X**				
TMSI/VLRMismatch														**a**
RETURN RESULT **DenyAccess** **ReasonList**												**X**	**X**	**c**

Problem Detections:

1. The requested MAP operation is recognized, but not supported, by the receiving MSC, or the requesting network node is not authorized.

2. A required MSC resource (e.g., internal memory record, MSC is fully occupied) is temporarily not available (congestion).

3. A required resource (e.g., data base access, network element) is not presently accessible due to a failure. Human intervention may be required for resolution.

4. A supplied parameter value has an encoding problem (e.g., The supplied MSID parameter digit values do not meet the BCD specification).

5. A supplied parameter value is unrecognized or has non-standard values (e.g., *Not used*).

6. An MSC record doesn't presently exit for the supplied MobileIdentificationNumber.

7. An MSC record doesn't presently exit for the supplied InternationalMobileStationIdentity.

8. An optional parameter required by the MSC was expected but not received (e.g., only MSID and ElectronicSerialNumber parameters received).

9. An MSC record exists for MSID, but the supplied ESN parameter doesn't match the ESN in the MSC record.

10. The supplied old TMSI doesn't match the MSID and ESN in the MSC record.

11. The receiving MSC has another TMSIDirective process in-progress for the supplied MSID.

12. TMSI assignment is unsuccessful because of the reason identified by the supplied DenyAccess parameter value.

13. TMSIAssignment operation is unsuccessful because of the reason identified by supplied ReasonList parameter value.

Notes:

a. This Error Code is not an appropriate MSC response to an TMSIDirective transaction.

b. It is recommended that an MSC support TMSIDirective transactions.

c. Only RETURN RESULT operations needing clarification have been included.

d. Include the in question as the FaultyParameter parameter.

7 Operation Timer values

(N.S0005-0 v 1.0 Chapter 6, page 400)

Table 63 Operation Timer Values

Timer	Default (sec.)	Started when	Normally stopped when	Action when timer expires
PRT Parameter Request Timer	6	Parameter Request INVOKE is sent	Parameter Request RETURN RESULT or RETURN ERROR is received	Execute recovery procedures.
TDT TMSI Directive Timer	24	TMSI Directive INVOKE is sent	TMSI Directive RETURN RESULT or RETURN ERROR is received	Execute recovery procedures.

ANNEX A Information Stored in Databases

This Annex is informative and is not consider part of this Standard.

1. Basic assumption

N.S0005-0 v 1.0 Functional Entities (e.g., MSC, VLR, HLR, AC) store information pertinent to registration, authentication, subscription and call processing. Each FE contains information relevant to the functions it performs and the processes it supports. The following assumptions state in general terms what information is contained in the FEs:

1. The HLR should contain permanent subscriber profile information for the home system.
2. The VLR should contain subscriber information required for roaming subscribers currently registered in the visited system controlled by the VLR. If SSD is shared, the VLR should contain authentication information.
3. The MSC should maintain a subset of information related to the registered subscriber while the MS is actively registered. This should include MSID information, other paging information and optionally profile information.
4. The AC should contain authentication information of the MSs.

Table A-1 provides a summary of information in *N.S0005-0 v 1.0* FEs and under what conditions it should be stored in the FE's database.

Table A-1: Overview of information stored in *IS-41* Functional Entities

Parameter	MSC	VLR	HLR	AC
MSID (i.e., IMSI or MIN)	Required for visiting MS	Required for visiting MS	Required	Required
ESN	Required for call in progress	Required for visiting MS	Required	Required
DN	_	Required for visiting MS	Required	_
TMSI	Required for visiting MS, if available	Required for visiting MS, if available	_	_
TLDN	_	Temporary for setting up the call	_	_
Mobile Station Class Mark	Required for visiting MS, if available	Required for visiting MS, if available	Required	_
A Key	_	_	_	Required
SSD	_	Required for visiting MS, if shared	_	Required
COUNT	_	Required for visiting MS, if shared	_	Required
SMEKEY	_	Required for visiting MS, if shared	_	Required
VPMASK	_	Required for visiting MS, if shared	_	Required
Slot cycle Index	Required for visiting MS, if MS in slotted mode	Required for visiting MS, if MS in slotted mode	_	_
Location Area ID	Required for call in progress, if available	Required for visiting MS, if available	_	_
Cell_ID	Required for call in progress	Required for visiting MS	_	_
Profile	Partly required for call in progress	Partly required for visiting MS	Required	_
Authorization Period	_	Required for visiting MS	Required	_
Mobile Protocol Revision	Required for visiting MS, Include if available	Required for visiting MS, Include if available	Required	_