



User Identity Module

COPYRIGHT

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

CONTENTS

8	CONTENTS	i
9	REVISION HISTORY	ii
10	DOCUMENT SOURCES	iii
11	FOREWORD	iv
12	ASSUMPTIONS	v
13	1 INTRODUCTION	1
14	1.1 OBJECTIVE	1
15	1.2 SCOPE	1
16	1.3 ORGANIZATION	1
17	2 REFERENCES	2
18	2.1 Normative References	2
19	2.2 Informative References	2
20	3 Abbreviations	3
21	4 Definitions	3
22	5 General Background	4
23	5.1 Users' Key Capabilities	4
24	5.2 ME Key Capability	4
25	6 Incorporating UIM in Telecommunication wireless networks operations	5
26	6.1 Normal Procedures With Successful Outcome	5
27	6.1.1 Authorization	5
28	6.1.2 De-authorization	5
29	6.1.3 Registration	5
30	6.1.4 De-registration	5
31	6.1.5 Activation	5
32	6.1.6 De-Activation	5
33	6.1.7 Invocation	5
34	6.1.8 Normal Operation with Successful Outcome	5
35	6.1.9 Potential UIM Capabilities which may be supported	Error! Bookmark not defined.
36	6.1.10 Exception Procedures for Unsuccessful Outcome	6
37	7 TIA/EIA-41-D Chapter 3 Modification "Automatic Roaming Information Flows"	7
38	1 UIM Authentication and Registration	7
39	1.1 Initial UIM Authentication and Registration	7
40	1.2 UIM Authentication and Registration When a VLR Record Exists and SSD is Not Shared	9
41	1.3 UIM Authentication and Registration When a VLR Record Exists and SSD is Shared	12
42	1.4 UIM Global Challenge Authentication Failure	15
43	X.Y.A Successful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch17	
44	Unsuccessful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch - ESN Swapping by the VLR	21
45	8 TIA/EIA-41-D Chapter 5 Modification "Signalling Protocols"	24
46	9 TIA/EIA-41-D Chapter 6 Modification "Signalling Procedures"	26
47	4.1.2 HLR Receiving AuthenticationDirective INVOKE	26
48	4.3.3 HLR Receiving AuthenticationFailureReport INVOKE	32
49	4.3.4 AC Receiving AuthenticationFailureReport INVOKE	38
50	4.4.2 VLR Receiving AuthenticationRequest INVOKE	45
51	4.4.3 HLR Receiving AuthenticationRequest INVOKE	55
52	4.4.4 AC Receiving AuthenticationRequest INVOKE	61
53	4.5.3 HLR Receiving AuthenticationStatusReport INVOKE	70
54	4.5.4 AC Awaiting AuthenticationStatusReport INVOKE	75

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

REVISION HISTORY

Revision	Committee	Remarks
Rev 0.0	4/7/99 Conf Call Results	Editor - Ben Levitan
Rev 0.1	4/13/99 TR45.2.1 Results	Editor - Ben Levitan
Rev 0.2	5/6/99 Conf Call Results	Editor - Ben Levitan
Rev 1.0	5/17/99 TR45.2.1 Results	Approved as Baseline Text
Rev 2.0	6/15/99 TR45.2.1 Results	Editor - Ben Levitan
Rev 3.0	8/18/99 TR45.2.1 Results	Editor – Ben Levitan
Rev 4.0	9/14/99 TR45.2.1 Results	Editor – Ben Levitan
Rev 5.0	10/15/99 TR45.2.1 Results	Editor – Ben Levitan
Rev 6.0	11/11/99 TR45.2.3 Results	Editor – Ben Levitan
Rev 7.0	12/17/99 TR45.2 Results & Sections rearranged by editor to conform to TIA style guide	Editor – Ben Levitan
Rev 7.1	1/5/00 Editor’s Results	Some agreed text from referenced 12/17/99 TR45.2 meeting was omitted by Editor. Added in.
Rev 8.0	1/21/00 TR45.2 Results	Approved for 60 day ballot

UIM Rev. 8.0 (Ballot Version)

DOCUMENT SOURCES

Source	Date	Title
Gemplus	TR45.2.1/99.03.29	UIM Functional Characteristics and Requirements
GTE	4/7/99 Conf. Call	Proposed General Section for UIM project
GTE	5/6/99 Conf. Call	Proposed Assumption for UIM
Gemplus	TR45.2.1/99.06.15.22	UIM Functional Characteristics and Requirements
CDG	TR45.2.1/99.08.18.03	UIM Functional Characteristics and Requirements
GTE	TR45.2.1/99.09.14.04	Proposed General Changes for PN-4282 – UIM
3GPP2 TSG	TR45.2/99.09.13.36	Removeable UIM Stage 1 – Notes on Conf Call
3GPP2 TSG	TR45.2.2/99.10.12.11	Removeable UIM Stage 2
GTE	TR45.2.3/99.11.10.04	Integration of dynamic ESN binding alternative for UIM
GTE	TR45.2.2/99.12.16.07	Stage 2 flows for R-UIM transfer when SSD is shared
Lucent	TR45.2/99.12.13.22	UIM Authentication and Registration Stage 2 and 3
Lucent	TR45.2/99.12.13.22a	UIM Authentication and Registration
GTE	TR45.2/00.01.10.08	PN-4371 Personal Mobility integration to PN-4582
GTE	TR45.2/00.01.10.09	PN-4582 UIM Pre-V&V comments & recommendations

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

FOREWORD

This Interim Standard contains recommendations for supporting the wireless subscriber feature “User Identity Modules (UIM)”.

The *ANSI/TIA/EIA-41-D* recommendation upon which this Interim Standard builds is:

- *TIA/EIA-41-D Cellular Radiotelecommunications Intersystem Operations; Telecommunications Industry Association; 1997.*

UIM Rev. 8.0 (Ballot Version)

ASSUMPTIONS

The following items are basic understandings used during the development of this document:

- a. In mobile stations supporting an R-UIM, the ESN remains Mobile Equipment based.
- b. No upgrades are needed to Serving System functionality to provide support for UIM-capable roamers. In particular, no air interface, A- interface, or serving system intersystem signaling enhancements are to be needed.
- c. Each unique set of user identity and security information may be active in only one terminal simultaneously.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

1 INTRODUCTION

1.1 OBJECTIVE

This Interim Standard (IS) presents Stage-1 (new chapter *TIA/EIA-664-A*) Enhancements, Stage-2 (*TIA/EIA-41.3-D* enhancements), and Stage-3 (*TIA/EIA-41.5-D* and *TIA/EIA-41.6-D* enhancements) recommendations for supporting the mobile stations equipped with User Identity Modules (UIM) in the Wireless Radiotelephone Service.

1.2 SCOPE

This standard defines the enhancements required for the support of mobile stations equipped with User Identification Modules (UIM.) The UIM provides functionality to certain types of mobile stations to enable them to operate in the wireless network.

This document defines requirements for the wireless network to support operation of UIM equipped mobile stations. A UIM provides compatible mobile stations with the parameters required of mobile stations operating in the TIA/EIA-41 environment and specific additional functionality unique to UIM-equipped mobile stations.

The UIM can be in one of two forms, as either integrated within the mobile or removable that can be inserted or removed from the mobile equipment. This document addresses Removable UIM (R-UIM) only.

1.3 ORGANIZATION

This document is organized as per *TIA/EIA-41-D* and *TIA/EIA-664-A*.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

2 REFERENCES

2.1 Normative References

TIA/EIA:

- ANSI/TIA/EIA-41-D *Cellular Radiotelecommunications Intersystem Operations*; Telecommunications Industry Association; December 1997.
- TIA/EIA-664-A *Cellular Features Description* Telecommunications Industry Association; February 2000.
- TIA/EIA/IS-725-A *TIA/EIA-41 Revision D Enhancements to Support Over-The-Air Service Provisioning (OTASP) and Parameter Administration (OTAPA)*
- TIA/EIA/IS-735 *Support for IS-95-A (CDMA).*
- TIA/EIA/IS-737 *Circuit Mode Services – Data (TDMA/CDMA).*
- TIA/EIA/IS-751 *TIA/EIA-41-D Modifications to support IMSI.*
- TIA/EIA/IS-778 *Wireless Authentication Authentication Enhancements Descriptions*

2.2 Informative References

None Identified

UIM Rev. 8.0 (Ballot Version)

3 TIA/EIA-664-A “Cellular Feature Descriptions” Modifications

The section provides the Stage 1 feature descriptions for User Identity Module (UIM) according to the structure of TIA/EIA-664.

3.1 Abbreviations

(TIA/EIA-664-A)

For the purpose of this document, the following abbreviations apply:

AMPS	Advance Mobile Phones System
CDMA	Code Division Multiple Access
EIA	Electronic Industry Association
ME	Mobile Equipment
OTAPA	Over-The-Air Parameter Administrations
OTASP	Over-The-Air Service Provisioning
R-UIM	Removable User Identity Module
TDMA	Time Division Multiple Access
TIA	Telephone Industry Association
UIM	User Identity Module
GSM	Global System for Mobile Communications

3.2 Definitions

Mobile Equipment (ME)

An R-UIM capable mobile station without an R-UIM inserted.

Mobile Station (MS)

Together, the R-UIM and the ME, is referred to as the R-UIM capable MS which is used to register and gain access to wireless networks.

Personal Mobility

The capability of a user to move their subscription from one mobile device to another without the need for the service provider to re-provision services. The mobile must support Personal Mobility in order to allow this service and the current user must configure their mobile station to allow replacement of their subscription. UIM is one method of implementing Personal Mobility. A terminal may not be available for wireless personal mobility unless authorized by the terminal owner.

Rebinding

The process by which the network updates the ESN associated to an MSID when an R-UIM is transferred from one ME to another.

Removable User Identity Module (R-UIM)

The R-UIM can be physically removed from one ME and inserted into another as long as both have compatible ME-UIM interfaces. UIM is the entity that stores and manages the identity of the subscriber and subscription related data.

Subscription Data

UIM Rev. 8.0 (Ballot Version)

Data that is unique for each subscriber relating to the subscribed services (e.g. MDN, language preference) and can be updated using provisioning procedures.

7.X User Identity Module

(new Section for TIA/EIA-664-A Chapter 7)

The R-UIM is an entity that stores and manages the identity of the subscriber and their personal network and subscription related data.

The network service provider can update the data stored in the R-UIM. This data may be updated via Over-the-Air Service Provisioning (OTASP) and Parameter Administration (OTAPA) techniques or via external programming devices.

UIMs may be supported on non-TIA/EIA-41 mobile stations and thus permit a TIA/EIA-41 subscriber to access service on a non-TIA/EIA-41 network if compatible interfaces exist.

7.X.1 Users' Key Capabilities

An R-UIM equipped mobile has the same capabilities as other mobiles phone. Additionally, a R-UIM must support the following key capabilities. Subscribers using Mobile Equipment with an R-UIM may be offered all or some of the following services and capabilities based on the service offerings of the network service provider:

- a) Store number assignment module (NAM) and other needed parameters for the operation of AMPS, CDMA, TDMA and/or GSM air-interfaces.
- b) An R-UIM's Subscription Data may be activated or updateable via Over-the-Air Service Provisioning (OTASP) and Over the Air Parameters Administration (OTAPA). Subscription data for the R-UIM may also be updated via MS keypad.
- c) Storage and execution of authentication algorithm(s) for execution of authentication or generation of privacy keys as instructed by the MS.
- d) Offer to the user a mechanism of protecting unauthorized usage of the R-UIM via verification PIN
- e) Service access using one R-UIM with multiple MEs if compatible ME-UIM interfaces exist
- f) A list of DN's will be built on the R-UIM; the list shall be accessible with all ME which the R-UIM is used. This permits, origination of calls using speed dialing from the stored DN's on the R-UIM.
- g) Selection of optional languages and character sets from the handset keypad, if the ME supports multiple languages and character sets.

7.X.2 ME Key Capability

The User shall have access to emergency services from the ME when a R-UIM is not inserted.

8.X Incorporating UIM in Telecommunication wireless networks operations

(new Section for TIA/EIA-664-A Chapter 8)

The UIM provides functionality to certain types of mobile stations to enable them to operate in the wireless network.

8.X.1 Normal Procedures With Successful Outcome

A wireless subscriber with an R-UIM should be able to use any compatible mobile equipment to register, authenticate and access network services.

Authorization

The subscriber's home network service provider or network operator is responsible for providing the subscriber with a R-UIM and a compatible ME.

De-authorization

The network service provider may withdraw at the subscriber's request or for administrative reasons this service.

Registration

Registration occurs upon authorization.

De-registration

De-registration occurs upon de-authorization.

Activation

The R-UIM shall be activated upon authorization.

De-Activation

The R-UIM shall be de-activated upon de-authorization.

Invocation

The R-UIM service is invoked when the R-UIM is inserted into compatible mobile equipment and the mobile equipment is activated in a compatible system.

8.X.2 Normal Operation with Successful Outcome

The R-UIM must first be inserted into the ME. On power-up, the UIM should be activated after initialization with the ME. If the MS is in a compatible network, the MS can then proceed with the normal registration and authentication processes required by the serving network.

If the R-UIM and ME were not associated together for the last network access, rebinding shall be necessary.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Roaming Capability:

- Within the same air-interface (e.g., roam to another network with same air-interface but different frequency than the user’s home network.)
- Cross different air interface in the same network - e.g. CDMA to AMPS
- Cross different air-interfaces and networks -e.g. roam into a GSM network

Use one mobile station for different R-UIMs - Allow R-UIM’s having different subscriptions to use the same mobile equipment.

Use multiple mobile equipment with one R-UIM Allow subscribers to change mobile equipment as desired with one R-UIM.

8.X.3 Exception Procedures for Unsuccessful Outcome

None Identified.

UIM Rev. 8.0 (Ballot Version)

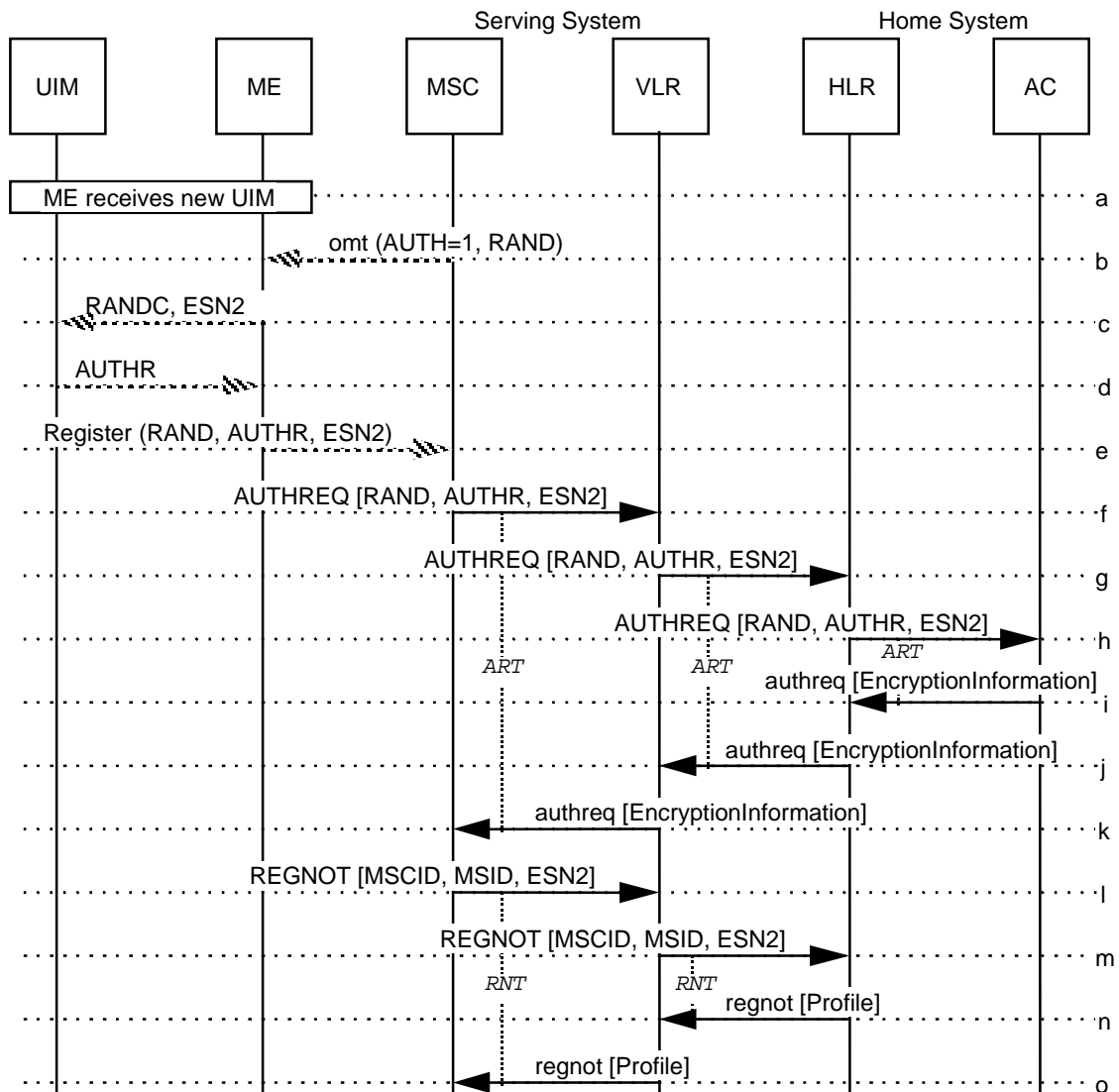
4 TIA/EIA-41-D Chapter 3 Modification “Automatic Roaming Information Flows”

6.X UIM Authentication and Registration

This section provides call flows describing various conditions for UIM authentication and registration. These flows apply to both removable and integrated UIMs when the UIM is ported between MEs.

6.X.1 Initial UIM Authentication and Registration

This scenario describes authentication and registration upon first radio contact in a new system after an ME receives a new UIM. There is no existing VLR record in the current serving system.



UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Figure 1 Initial UIM Authentication and Registration

- a. The subscriber populates the ME with an UIM.
- b. The ME determines that registration and authentication are required. The RAND to be used for authentication may be obtained at this time. Otherwise, a zero value may be used.
- c. The ME sends the RAND and its ESN to the UIM. The UIM executes CAVE using the currently stored SSD, MSID, and ESN2 (the ESN of the mobile equipment to which the R-UIM is transferred) and RAND from the ME to produce AUTHR.
- d. The UIM sends AUTHR to the ME.
- e. The MS request registration at the Serving MSC, providing MSID, ESN2, AUTHR, and RANDC.
- f. The Serving MSC verifies RANDC and sends ESN2 and the appropriate value of RAND in an AUTHREQ to the VLR.
- g. The VLR has no record for the subscriber so it sends an AUTHREQ to the HLR including all received parameters.
- h. The HLR forwards the AUTHREQ to the AC. The AC executes CAVE using the currently stored SSD, the received MSID, ESN2, and RAND to produce AUTHR. The AC verifies the AUTHR received from the MS matches its CAVE result.
- i. The AC sends an authreq to the HLR including encryption information.
- j. Since the authentication process succeeded, the HLR binds the new ESN2 for the subscriber. The HLR forwards the authreq to the VLR.
- k. The VLR forwards the authreq to the Serving MSC.
- l. The Serving MSC sends a REGNOT to the VLR to register the MS.
- m. The VLR forwards the REGNOT to the HLR.
- n. The HLR sends a regnot to the VLR including the subscriber profile.
- o. The VLR forwards the regnot to the Serving MSC.

UIM Rev. 8.0 (Ballot Version)

3
4
5 **6.X.2 UIM Authentication and Registration When a VLR**
6 **Record Exists and SSD is Not Shared**
7

8
9 This scenario describes authentication and registration upon first radio contact after an ME
10 receives a new UIM. In this scenario a VLR record exists with the ESN of a prior ME. SSD has
11 not been shared at the VLR.
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

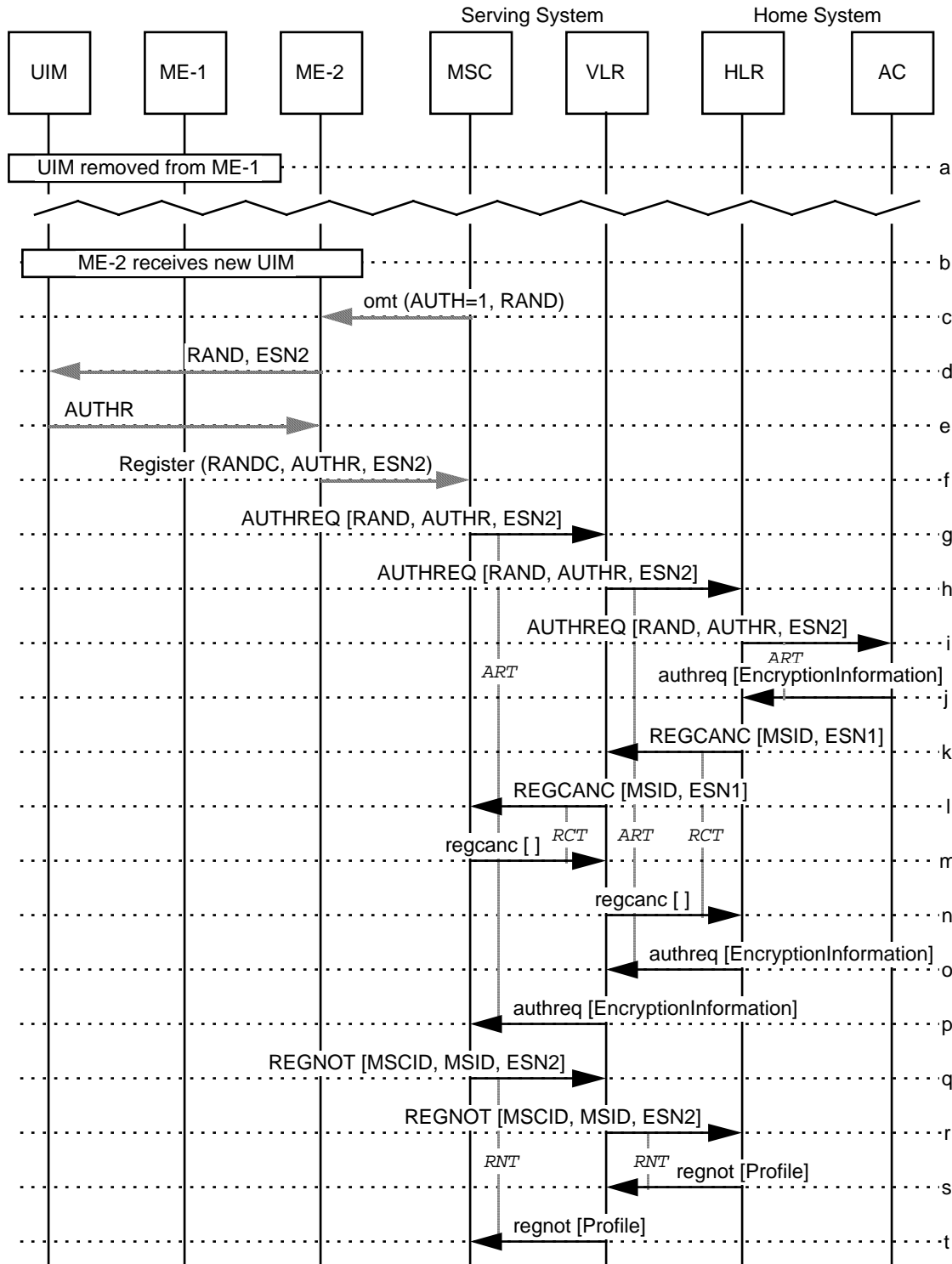


Figure 2 R-UIM Authentication and Registration with VLR and no SSD

- a. A subscriber removes the UIM from ME-1.
- b. The subscriber populates ME-2 with an UIM.

- c. ME-2 determines that registration and authentication are required. The RAND to be used for authentication may be obtained at this time. Otherwise, a zero value may be used.
- d. ME-2 sends the RAND and ESN2 (the ESN of the mobile equipment to which the R-UIM is transferred) to the R-UIM. The R-UIM executes CAVE using the currently stored SSD, MSID, and ESN2 and RAND from ME-2 to produce AUTHR.
- e. The UIM sends AUTHR to ME-2.
- f. The MS requests registration at the Serving MSC, providing MSID, ESN2, AUTHR, and RANDC.
- g. The Serving MSC verifies RANDC and sends ESN2 and the appropriate value of RAND in an AUTHREQ to the VLR.
- h. Since SSD is not shared, the VLR forwards the AUTHREQ to the HLR.
- i. The HLR forwards the AUTHREQ to the AC. The AC executes CAVE using the currently stored SSD, the received MSID, ESN2, and RAND to produce AUTHR. The AC verifies the AUTHR received from the MS matches its CAVE result.
- j. The AC sends an authreq to the HLR including encryption information.
- k. The HLR determines that the subscriber is registered in the serving system with a different ESN. It sends a REGCANC to the VLR to remove the current registration record. The previous ESN1 (the ESN of the mobile equipment from which the R-UIM is transferred) is included.
- l. The VLR forwards the REGCANC to the Serving MSC.
- m. The Serving MSC acknowledges the REGCANC by returning a regcanc to the VLR.
- n. The VLR acknowledges the registration cancellation by returning a regcanc to the HLR.
- o. Since both authentication and registration cancellation were successful, the HLR binds the new ESN for the subscriber. The HLR forwards the authreq to the VLR.
- p. The VLR forwards the authreq to the Serving MSC.
- q. The Serving MSC sends a REGNOT to the VLR to register the MS.
- r. The VLR forwards the REGNOT to the HLR.
- s. The HLR sends a regnot to the VLR including the subscriber profile.
- t. The VLR forwards the regnot to the Serving MSC.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

6.X.3 UIM Authentication and Registration When a VLR Record Exists and SSD is Shared

This scenario describes authentication and registration upon first radio contact after an ME receives a new UIM. In this scenario a VLR record exists with the ESN of a prior ME. SSD has been shared at the VLR. The subscriber profile indicates UIM capability is supported.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

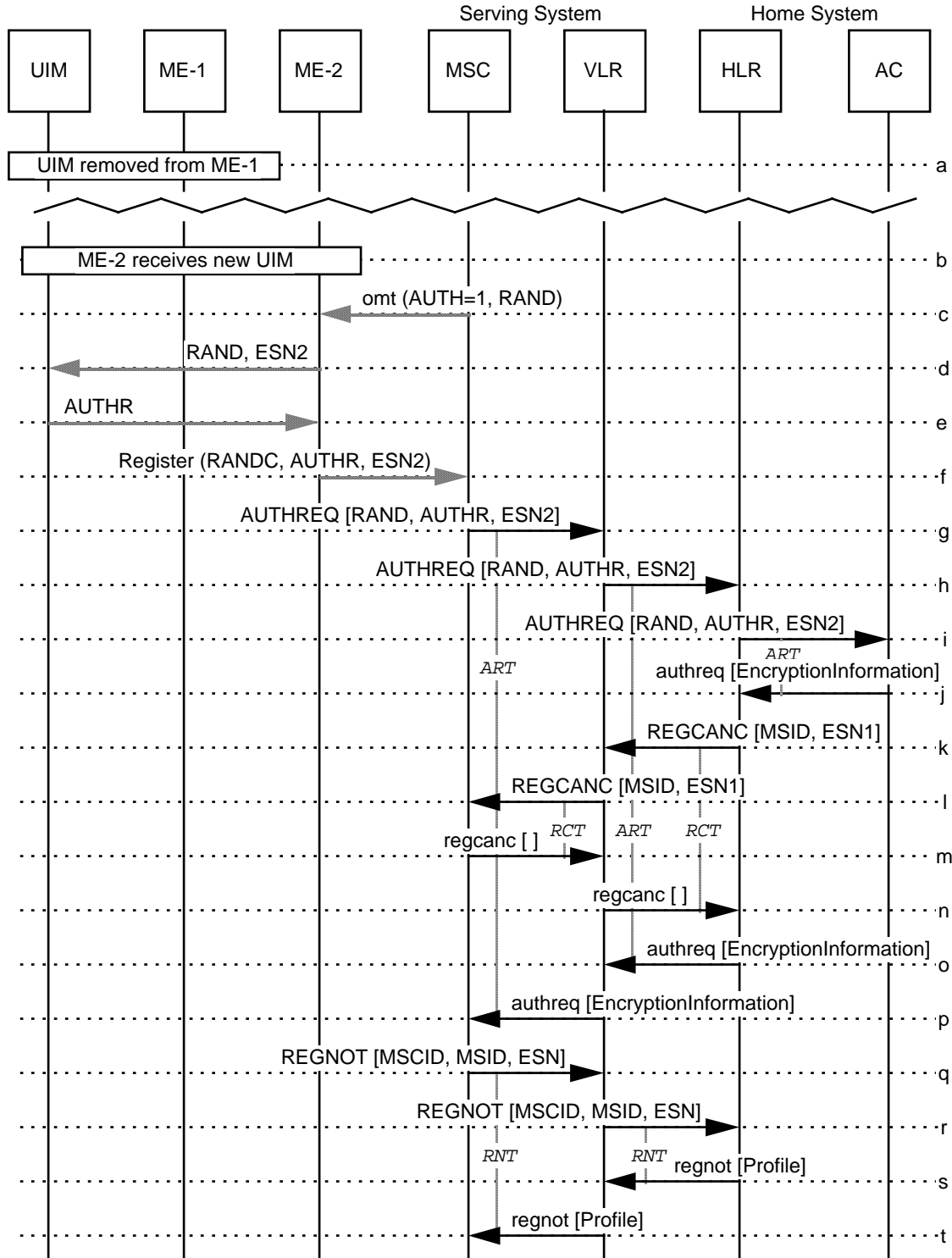


Figure 3 UIM Authentication and Registration with VLR, SSD, and UIM Capability

- a. A subscriber removes the UIM from ME-1.
- b. The subscriber populates ME-2 with an UIM.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- c. ME-2 determines that registration and authentication are required. The RAND to be used for authentication may be obtained at this time. Otherwise, a zero value may be used.
- d. ME-2 sends the RAND and ESN2 (the ESN of the mobile equipment to which the R-UIM is transferred) to the UIM. The UIM executes CAVE using the currently stored SSD, MSID, and ESN2 and RAND from ME-2 to produce AUTHR.
- e. The UIM sends AUTHR to ME-2.
- f. The MS requests registration at the Serving MSC, providing MSID, ESN2, AUTHR, and RANDC.
- g. The Serving MSC verifies RANDC and sends ESN2 and the appropriate value of RAND in an AUTHREQ to the VLR.
- h. The VLR checks if the subscriber is authorized for UIM. Since it is an UIM subscriber, the VLR forwards the AUTHREQ to the HLR.
- i. The HLR forwards the AUTHREQ to the AC. The AC executes CAVE using the currently stored SSD, the received MSID, ESN2, and RAND to produce AUTHR. The AC verifies the AUTHR received from the MS matches its CAVE result.
- j. The AC sends an authreq to the HLR including encryption information.
- k. The HLR determines that the subscriber is registered in the serving system with a different ESN. It sends a REGCANC to the VLR to remove the current registration record. The previous ESN1 (the ESN of the mobile equipment from which the R-UIM is transferred) is included.
- l. The VLR forwards the REGCANC to the Serving MSC.
- m. The Serving MSC acknowledges the REGCANC by returning a regcanc to the VLR.
- n. The VLR acknowledges the registration cancellation by returning a regcanc to the HLR. The CallHistoryCount parameter is included since SSD is shared.
- o. Since both authentication and registration cancellation were successful, the HLR binds the new ESN for the subscriber. The HLR forwards the authreq to the VLR.
- p. The VLR forwards the authreq to the Serving MSC.
- q. The Serving MSC sends a REGNOT to the VLR to register the MS.
- r. The VLR forwards the REGNOT to the HLR.
- s. The HLR sends a regnot to the VLR including the subscriber profile.
- t. The VLR forwards the regnot to the Serving MSC.

UIM Rev. 8.0 (Ballot Version)

6.X.4 UIM Global Challenge Authentication Failure

This scenario describes a global challenge authentication failure upon first radio contact in a new system after an ME receives a new UIM. In this scenario, the HLR does not rebind to the new, and possibly fraudulent ESN.

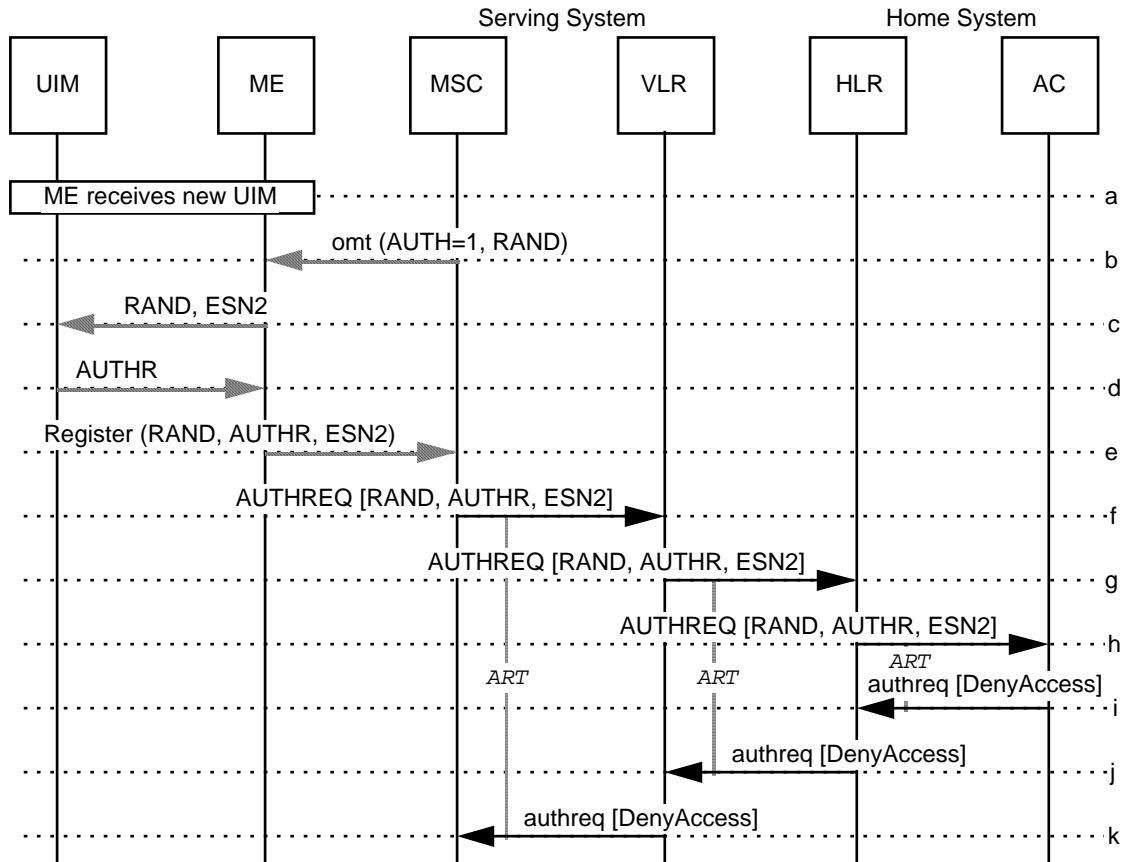


Figure 4 UIM Global Challenge Authentication Failure

- a. The subscriber populates the ME with an UIM.
- b. The ME determines that registration and authentication are required. The RAND to be used for authentication may be obtained at this time. Otherwise, a zero value may be used.
- c. The ME sends the RAND and its ESN2 (the ESN of the mobile equipment to which the R-UIM is transferred) to the UIM. The UIM executes CAVE using the currently stored SSD, MSID, and ESN2 and RAND from the ME to produce AUTHR.
- d. The UIM sends AUTHR to the ME.
- e. The MS request registration at the Serving MSC, providing MSID, ESN2, AUTHR, and RANDC.
- f. The Serving MSC verifies RANDC and sends ESN2 and the appropriate value of RAND in an AUTHREQ to the VLR.

UIM Rev. 8.0 (Ballot Version)

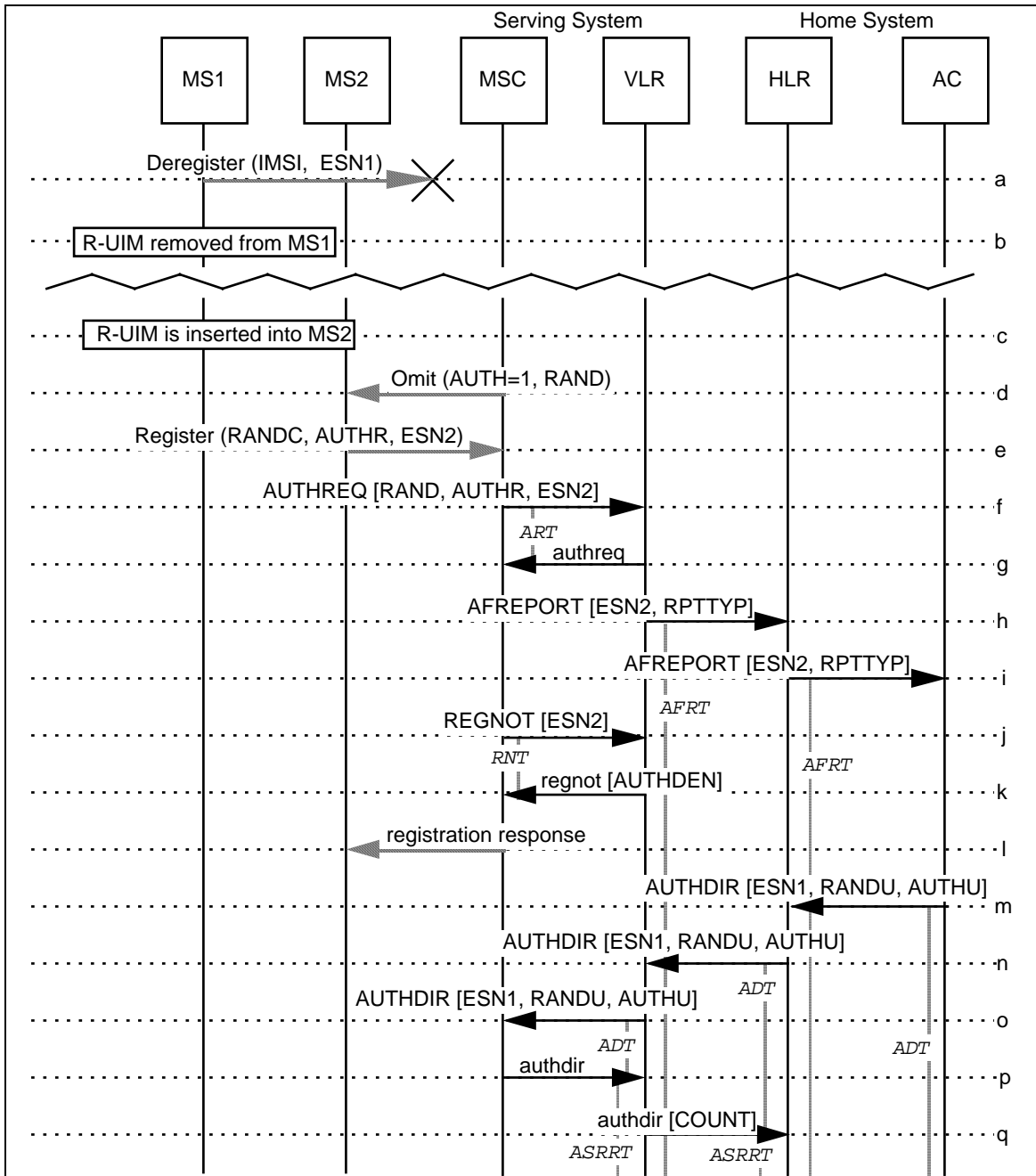
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- g. The VLR sends an AUTHREQ to the HLR including all received parameters.
- h. The HLR forwards the AUTHREQ to the AC. The AC executes CAVE using the currently stored SSD, the received MSID, ESN2, and RAND to produce AUTHR. The AC determines the AUTHR received from the MS does not match its CAVE result.
- i. The AC sends an authreq to the HLR indicating access is denied. The AC retains the old ESN (ESN1, the ESN of the mobile equipment from which the R-UIM is transferred) for the subscriber.
- j. Since the authentication process did not succeed, the HLR retains the old ESN1 for the subscriber. The HLR forwards the authreq to the VLR.
- k. The VLR forwards the authreq to the Serving MSC.

UIM Rev. 8.0 (Ballot Version)

6.X.5 Successful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch

This scenario describes ESN rebinding following an R-UIM transfer that takes place within one authenticating network when the Serving MSC does not receive an air interface indication that the old registration should be canceled. In this scenario SSD had been shared for MS1, the MS shell used by the subscriber prior to the transfer.



UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Figure 4 Successful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch

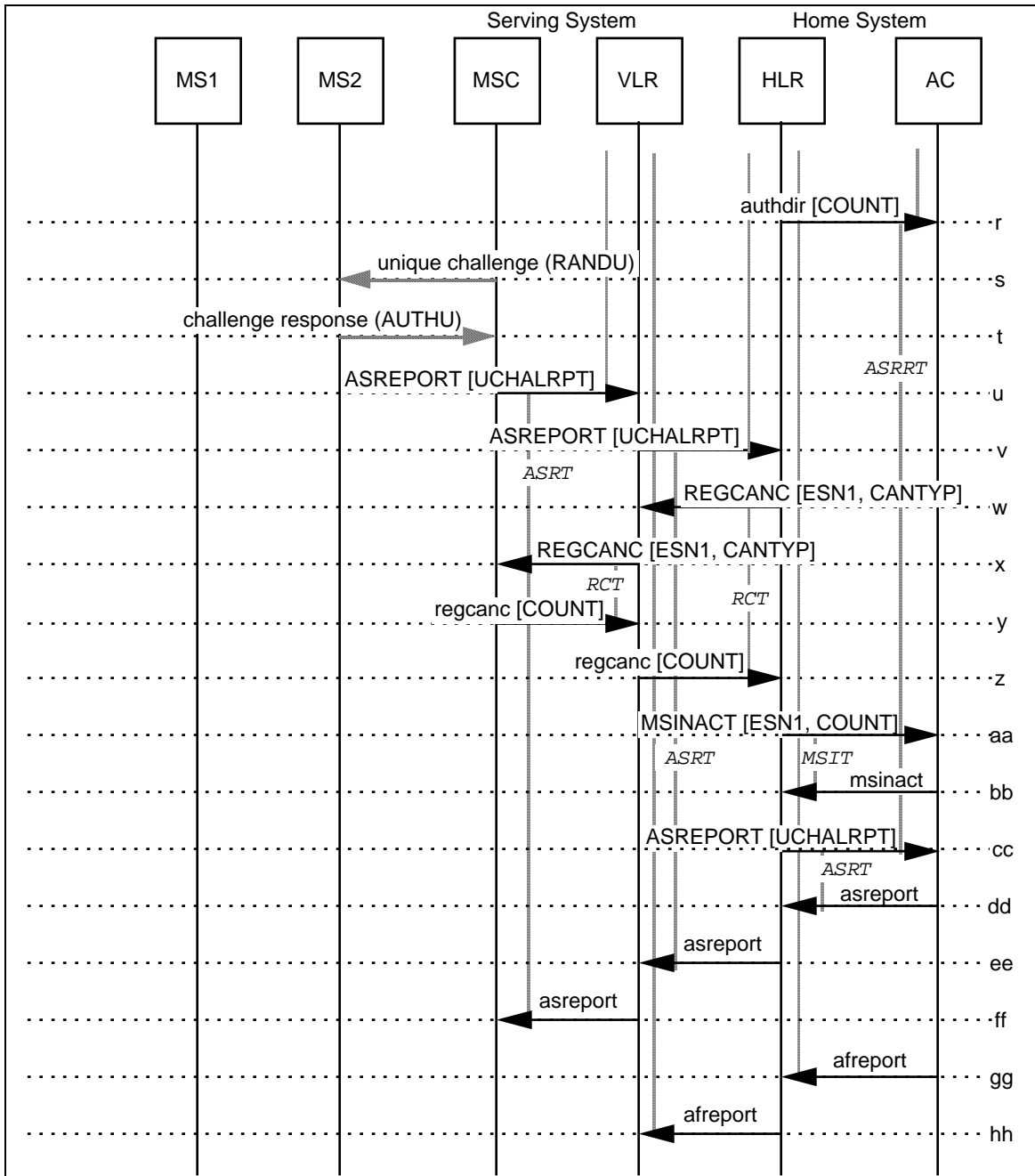


Figure 5 Successful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch (continued)

- a. MS1 is powered down in preparation for R-UIM transfer. However, in the illustrated scenario any air interface indication of that event is lost.
- b. The R-UIM is removed from MS1.
- c. The subscriber inserts the R-UIM into MS2 and powers up MS2.

UIM Rev. 8.0 (Ballot Version)

- 1
2
3
4
5
6
7
8
- d MS2 determines from the Overhead Message Train (OMT) that authentication is required on all system accesses (AUTH=1). The Random Number (RAND) to be used for authentication may also be obtained by MS2 at this time. If it is not, a zero value is used by MS2 as prescribed by TR-45 Authentication.

9 MS2 executes CAVE using the SSD-A currently stored, ESN2 (the ESN of the mobile equipment to which the R-UIM is transferred), the MIN1 and the RAND value to produce a registration Authentication Result (AUTHR).

- 10
11
12
13
14
15
16
17
18
19
20
21
22
23
- e. MS2 registers at the MSC, providing its MIN, ESN2, AUTHR, CallHistoryCount (COUNT), and RANDC derived from the RAND used to compute AUTHR.
- f. The MSC verifies RANDC supplied by MS2 and sends the appropriate value of RAND in an AUTHREQ to the VLR.
- g. The VLR detects the MIN/ESN mismatch and returns an empty authreq to the Serving MSC.
- h. The VLR sends an AFREPORT to the HLR with the ReportType parameter set to *MIN/ESN Mismatch*. In the illustrated scenario, the ESN included in this message by the VLR is ESN2, the ESN received in the AUTHREQ.

24 The HLR recognizes the subscriber as being R_UIM capable; it marks the subscriber as *pending ESN rebinding* and stores ESN2 as pending ESN.

- 25
26
27
- i. The HLR forwards the AFREPORT to the AC.

28 The AC recognizes the subscriber as being R_UIM capable; it marks the subscriber as *pending ESN rebinding* and stores ESN2 as pending ESN.

- 29
30
31
32
- j. When the MSC receives the authreq, it sends a REGNOT to the VLR to register MS2.

- 33
34
- k. The VLR detects the MIN/ESN mismatch and returns an regnot containing the AuthorizationDenied parameter set to *Invalid Serial Number* to the MSC.

- 35
36
- l. The MSC responds to the registration message received from MS2 at Step e.

- 37
38
39
40
- m. The AC chooses a Unique Random Variable (RANDU) and executes CAVE using RANDU, ESN2 (the pending ESN for the subscriber), MIN1 and MIN2 associated to the subscriber, and SSD-A currently stored for the subscriber to produce a Unique Authentication Response (AUTHU).

41 The AC sends an AUTHDIR to the HLR including RANDU and the expected AUTHU result. The ElectronicSerialNumber parameter in this message is populated with ESN1 (the ESN of the mobile equipment from which the R-UIM is transferred), the current ESN for the subscriber.

- 42
43
44
45
46
47
48
- n. Since the subscriber is already marked as *pending ESN rebinding*, and since the AUTHDIR carries a request for a Unique Challenge but it does not carry a request for an SSD update, the HLR marks the subscriber as *pending Unique Challenge*.

49 The HLR forwards the AUTHDIR to the VLR.

50
51
52
53
54
55

Note: From this point on (the point at which the subscriber is marked as *pending Unique Challenge*), the expiry of timer AFRT will not prevent the ESN rebinding process from succeeding. However, the expiry of timer AFRT prior to this point results in the HLR clearing the *pending ESN rebinding* status of the subscriber, which would cause ESN rebinding to fail.

- 56
57
58
59
60
- o. The VLR forwards the AUTHDIR to the MSC.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

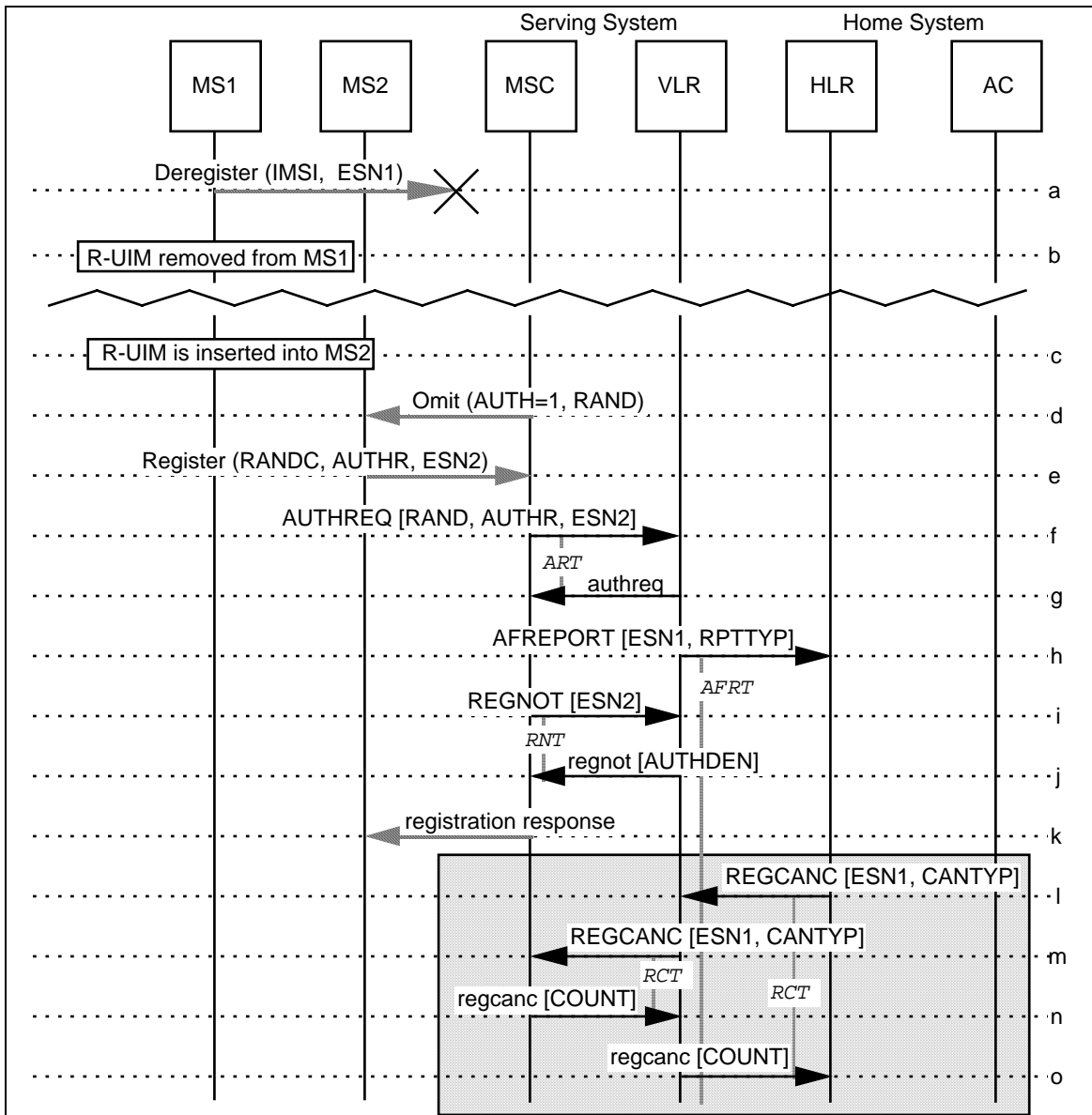
- p. The MSC returns an `authdir` to the VLR.
- q. The VLR includes the `CallHistoryCount` parameter set to the stored value of `COUNT` for MS1, and sends an `authdir` to the HLR.
- r. The HLR forwards the `authdir` to the AC.
- s. The MSC sends a Unique Challenge order to MS2 using the `RANDU` provided in the `AUTHDIR` (Step o).
- t. MS2 executes `CAVE` using `RANDU`, the `SSD-A` currently stored, the `MIN1` and `MIN2`, and `ESN2` to produce an Authentication Response for Unique Challenge (`AUTHU`) which is then sent to the Serving MSC.
- u. The MSC determines that the value of `AUTHU` provided in the `AUTHDIR` (Step o) is the same as that received from MS2.

The Serving MSC sends an `ASREPORT` to the VLR indicating the success of the Unique Challenge.
- v. The VLR forwards the `ASREPORT` to the HLR.
- w. Since the subscriber is marked as *pending ESN rebinding*, and since the `UniqueChallengeReport` parameter indicates that the unique challenge was successful, the HLR sends a `REGCANC` to the VLR with the `CancellationType` parameter set to a value of *Discontinue* to cancel the registration of MS1.
- x. The VLR forwards the `REGCANC` to the MSC.
- y. The MSC removes its records for MS1 from its memory and sends an empty `regcanc` to the VLR.
- z. The VLR includes the `CallHistoryCount` parameter set to the stored value of `COUNT` for MS1, sends a `regcanc` to the HLR, and removes its records for MS1 from its memory.
- aa. The HLR erases its registration pointer for the subscriber, relays the received `CallHistoryCount` parameter, and sends an `MSINACT` for MS1 to the AC.
- bb. The AC returns an `msinact` to the HLR.
- cc. The HLR updates its records for the subscriber to indicate that `ESN2` is now the current ESN for the subscriber; it clears the subscriber's *pending ESN rebinding* flag; and it forwards the `ASREPORT` to the AC.
- dd. The AC updates its records for the subscriber to indicate that `ESN2` is now the current ESN for the MS; it clears the subscriber's *pending ESN rebinding* flag; and it returns an `asreport` to the HLR.
- ee. The HLR clears the subscriber's *pending Unique Challenge* flag, and it relays the `asreport` to the VLR.
- ee. The VLR relays the `asreport` to the MSC.
- ff. The AC returns an `afreport` to the HLR.
- gg. The HLR relays the `afreport` to the VLR.

UIM Rev. 8.0 (Ballot Version)

6.X.6 Unsuccessful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch - ESN Swapping by the VLR

This scenario describes an unsuccessful attempt at ESN rebinding following an R-UIM transfer that takes place within one authenticating network when the Serving MSC does not receive an air interface indication that the old registration should be canceled. In this scenario SSD had been shared for MS1, the MS shell used by the subscriber prior to the transfer, and the VLR uses MS1's ESN when notifying the Home System that it has detected an authentication failure due to MIN/ESN mismatch causing ESN rebinding to fail.



UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Figure 6 Unsuccessful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch - ESN Swapping by the VLR

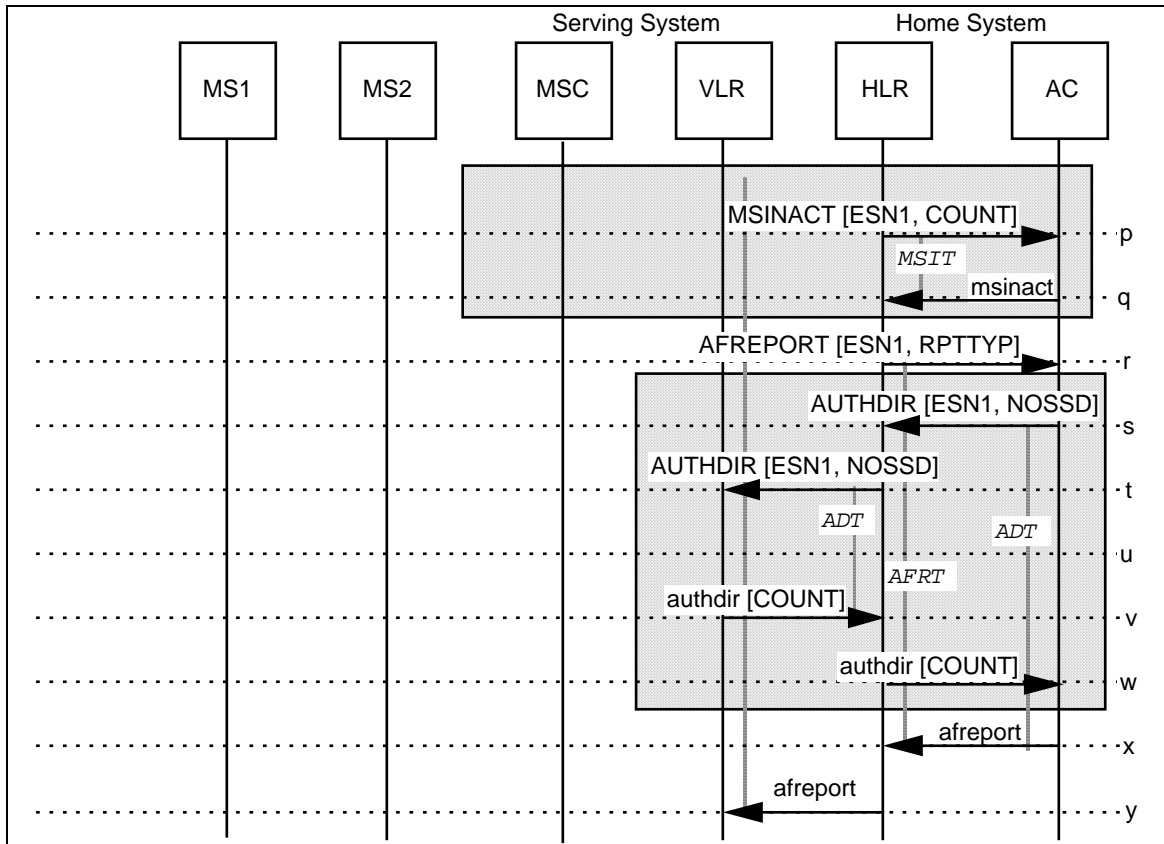


Figure 7 Unsuccessful R_UIM Transfer When SSD Had Been Shared and the VLR Detects MIN/ESN Mismatch - ESN Swapping by the VLR (continued)

- a-g. Same as Section X.Y.A, Steps a-g.
- h. The VLR sends an AFREPORT to the HLR with the ReportType parameter set to *MIN/ESN Mismatch*. In the illustrated scenario, the ESN included in this message by the VLR is ESN1 (the ESN of the mobile equipment from which the R-UIM is transferred), the ESN associated to the MIN in the VLR record for MS1.
- i. When the MSC receives the authreq, it sends a REGNOT to the VLR to register MS2.
- j. The VLR detects the MIN/ESN mismatch and returns an regnot containing the AuthorizationDenied parameter set to *Invalid Serial Number* to the MSC.
- k. The MSC responds to the registration message received from MS2 at Step e.
- l. Optionally, the HLR sends a REGCANC to the VLR with the CancellationType parameter set to a value of *ReportInCall* to cancel the registration of MS1.
- m. The VLR forwards the REGCANC to the MSC. Since MS1 is not engaged in a call, the MSC removes its records for MS1 from its memory.
- n. The MSC returns an empty regcanc to the VLR.

UIM Rev. 8.0 (Ballot Version)

- 2
- 3
- 4
- 5 o. The VLR includes the CallHistoryCount parameter set to the stored value of
- 6 COUNT for MS1, sends a regcanc to the HLR, and removes its records for MS1
- 7 from its memory.
- 8
- 9 p. The HLR erases its registration pointer for the subscriber, relays the received
- 10 CallHistoryCount parameter, and sends an MSINACT for MS1 to the AC.
- 11
- 12 q. The AC returns an msinact to the HLR.
- 13
- 14 r. The HLR forwards the AFREPORT to the AC.
- 15
- 16 s. Optionally, the AC sends an AUTHDIR to the HLR including the SSDNotShared
- 17 parameter to remove SSD from the VLR's record for MS1.
- 18
- 19 t. If the HLR has not erased its registration pointer for the subscriber (in particular the
- 20 optional Steps l-q were not performed), the HLR forwards the AUTHDIR to the
- 21 VLR.
- 22
- 23 u. If the VLR still has a record for MS1 (in particular the optional Steps l-q were not
- 24 performed), the VLR includes the CallHistoryCount parameter set to the stored
- 25 value of COUNT for MS1, sends an authdir to the HLR, and discards the current
- 26 value of SSD for MS1.
- 27
- 28 v. The HLR forwards the authdir to the AC.
- 29
- 30 w. The AC returns an afreport to the HLR.
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- x. The HLR relays the afreport to the VLR.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

5 TIA/EIA-41-D Chapter 5 Modification “Signalling Protocols”

6.5.2.8 AuthenticationCapability

The AuthenticationCapability (AUTHCAP) parameter indicates whether an MS shall or shall not be authenticated. For authentication capable mobiles, the parameter also indicates UIM capability.

Field	Value	Type	Reference	Notes					
Identifier	AuthenticationCapability 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
Authentication Capability								1	
...								<i>n</i>	<i>a</i>

Figure 15 AuthenticationCapability parameter

Notes:

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

Table 119 AuthenticationCapability value

<i>Authentication Capability (octet 1)</i>										
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	No authentication required.
	0	0	0	0	0	0	1	0	2	Authentication required.
	0	0	0	0	0	0	3	3	3	} Reserved. Treat the same as value 1, <i>No authentication required.</i>
			...						through 95	
	0	1	0	1	1	1	1	1	96	} Reserved for <i>TIA/EIA-41</i> protocol extension. If unknown, treat the same as value 1, <i>No authentication required.</i>
			...						through 127	
	1	0	0	0	0	0	0	0	128	Authentication required and UIM capable.
	1	0	0	0	0	0	0	1	129	} Reserved. Treat the same as value 2, <i>Authentication required.</i>
			...						through 223	
	1	1	0	1	1	1	1	1	224	} Reserved for <i>TIA/EIA-41</i> protocol extension. If unknown, treat the same as value 2, <i>Authentication required.</i>
			...						through 255	

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

6 TIA/EIA-41-D Chapter 6 Modification “Signalling Procedures”

4.1.2 HLR Receiving AuthenticationDirective INVOKE

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

1 IF the received message can be processed:

1-1 Include the SenderIdentificationNumber set to the identification number of the HLR.

Note: Modified by IS-751.

1-x Include the MSID parameter set to identify the MS to the VLR.

Steps 1-a through 1-b are proposed for R-UIM.

1-a IF the MS is marked as *pending ESN rebinding*:

1-a-1 IF the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters are received AND IF the RandomVariableSSD (RANDSSD) parameter is not received:

1-a-1-1 Mark the MS *pending Unique Challenge*.

1-a-2 ENDIF.

1-b ENDIF.

1-2 Relay all other received parameters.

1-3 Send an AuthenticationDirective INVOKE to the VLR currently serving the MS.

1-4 Start the Authentication Directive Timer (ADT).

1-5 WAIT for an Authentication Directive response:

1-6 WHEN a RETURN RESULT is received:

1-6-1 Stop timer (ADT).

1-6-2 IF the message can be processed:

1-6-2-1 Relay all received parameters.

1-6-2-2 Send a RETURN RESULT to the requesting AC.

Steps 1-6-2-c through 1-6-2-d are proposed for R-UIM.

1-6-2-c IF the MS is marked as *pending Unique Challenge*:

1-6-2-c-1 Start the Authentication Status Report Response Timer (ASRRT).

1-6-2-c-2 WAIT for an AuthenticationStatusReport INVOKE:

1-6-2-c-3 WHEN an AuthenticationStatusReport INVOKE is received:

1-6-2-c-3-1 Execute the “HLR Receiving AuthenticationStatusReport” task (see 4.5.3).

1-6-2-c-4 WHEN timer (ASRRT) expires:

1-6-2-c-4-1 Continue processing.

1-6-2-c-5 ENDWAIT.

1-6-2-c-6 IF the MS is marked as *pending ESN rebinding*:

1-6-2-c-6-1 Delete pending ESN for the MS.

1-6-2-c-6-2 Clear the MS's *pending ESN rebinding* flag.

1-6-2-c-6-3 IF the MS is currently registered:

1-6-2-c-6-3-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.

1-6-2-c-6-4 ENDIF.

1-6-3-c-7 ENDIF.

1-6-3-c-8 Clear the MS's *pending Unique Challenge* flag.

1-6-3-d ENDIF.

1-6-2-3 Exit this task.

1-6-3 ELSE (the message cannot be processed):

Steps 1-6-3-e through 1-6-3-f are proposed for R-UIM

1-6-3-e IF the MS is marked as *pending Unique Challenge*:

1-6-3-e-1 Delete pending ESN for the MS.

1-6-3-e-2 Clear the MS's *pending ESN rebinding* flag.

1-6-3-e-3 Clear the MS's *pending Unique Challenge* flag.

1-6-3-e-4 IF the MS is currently registered:

1-6-3-e-4-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.

1-6-3-e-5 ENDIF.

1-6-3-f ENDIF.

1-6-3-1 Send a RETURN ERROR to the requesting AC.

1-6-3-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-6-3-3 Exit this task.

1-6-4 ENDIF.

1-7 WHEN a RETURN ERROR or REJECT is received:

Steps 1-7-g through 1-7-h are proposed for R-UIM.

1-7-g IF the MS is marked as *pending Unique Challenge*:

1-7-g-1 Delete pending ESN for the MS.

1-7-g-2 Clear the MS's *pending ESN rebinding* flag.

1-7-g-3 Clear the MS's *pending Unique Challenge* flag.

1-7-g-4 IF the MS is currently registered:

1-7-g-4-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.

1-7-g-5 ENDIF.

- 1-7-h ENDIF.
- 1-7-1 Stop timer (ADT).
- 1-7-2 CASE Error Code OF:

Note: Modified by IS-778.

- 1-7-3 *ParameterError OR UnrecognizedParameterValue:*
- 1-7-3-1 IF the parameter was originated from the initiating functional entity:
- 1-7-3-1-1 Send a RETURN ERROR with Error Code set to the received Error Code. ~~indicate ParameterError.~~
- 1-7-3-2 ELSE:
- 1-7-3-2-1 Send a RETURN ERROR with Error Code set to indicate *SystemFailure.*
- 1-7-3-3 ENDIF.
- 1-7-a *MissingParameter:*
- 1-7-a-1 Send a RETURN ERROR with Error Code set to indicate MissingParameter.
- 1-7-4 *OperationSequenceProblem:*
- 1-7-4-1 Send a RETURN ERROR with Error Code set to indicate *OperationSequenceProblem.*
- 1-7-5 *DEFAULT:*
- 1-7-5-1 Send a RETURN ERROR with Error Code set to indicate *SystemFailure.*
- 1-7-6 ENDCASE.
- 1-7-7 Execute the “Local Recovery Procedures” task (see 3.5.1).
- 1-7-8 Exit this task.
- 1-8 WHEN timer (ADT) expires:

Steps 1-8-i through 1-8-j are proposed for R-UIM.

- 1-8-i IF the MS is marked as *pending Unique Challenge:*
- 1-8-i-1 Delete pending ESN for the MS.
- 1-8-i-2 Clear the MS’s *pending ESN rebinding flag.*
- 1-8-i-3 Clear the MS’s *pending Unique Challenge flag.*
- 1-8-i-4 IF the MS is currently registered:
- 1-8-i-4-1 Optionally, execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the *ElectronicSerialNumber* parameter set to the current ESN and with the *CancellationType* parameter set to *ReportInCall.*
- 1-8-i-5 ENDIF.
- 1-8-j ENDIF.
- 1-8-1 Send a RETURN ERROR with Error Code set to indicate *SystemFailure.*
- 1-8-2 Execute the “Local Recovery Procedures” task (see 3.5.1).
- 1-8-3 Exit this task.
- 1-9 ENDWAIT.
- 2 ELSE (the received message cannot be processed):

3
4 2-1 Send a RETURN ERROR with the proper Error Code value (see the following
5 table) to the requesting AC.

6
7 3 ENDIF.

8 4 Exit this task.
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Note: Modified by IS-778 and IS-751.

Table 1 HLR AuthenticationDirective Response

Problem Detection and Recommended Response from HLR to AC	
RETURN ERROR Error Code	PROBLEM DEFINITION
UnrecognizedMIN	The supplied MobileIdentificationNumber_or IMSI parameter is within the range of the HLR, but the MIN MS is not Authentication capable or authorized. <i>Note: This response may have been originated by the VLR (MSC).</i>
UnrecognizedESN	The supplied MobileIdentificationNumber_or IMSI parameter is within the range of the HLR, but the supplied ElectronicSerialNumber parameter is not valid for the MIN's authentication record. <i>Note: This response may have been originated by the VLR (MSC).</i>
MINMSID/HLRMismatch	The supplied MobileIdentificationNumber_MSID parameter is not in the HLR's range of MINs MSIDs or directory numbers (suspect routing error).
OperationSequenceProblem	The HLR has another Authentication process in progress for the supplied MobileIdentificationNumber parameter. <i>Note: This response may have been originated by the VLR (MSC).</i>
ResourceShortage	A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the VLR (MSC).</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized. <i>Note: It is recommended that an HLR supports AuthenticationDirective transactions. This response may have been originated by the VLR (MSC).</i>
TrunkUnavailable	<i>Note: This Error Code is not an appropriate HLR response to an AuthenticationDirective transaction.</i>
ParameterError	A supplied parameter value has an encoding problem (e.g., The supplied MobileIdentificationNumber parameter digit values do not meet the BCD specification). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter. This response may have been originated by the VLR (MSC).</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the VLR (MSC).</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter. This response may have been originated by the VLR (MSC).</i>
FeatureInactive	<i>Note: This Error Code is not an appropriate HLR response to an AuthenticationDirective transaction.</i>

UIM Rev. 8.0 (Ballot Version)

<p>MissingParameter</p>	<p>An optional parameter required by the HLR was expected, but not received (e.g., only MobileIdentificationNumber and ElectronicSerialNumber parameters received). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i> <i>This response may have been originated by the VLR (MSC).</i></p>
<p>Unrecognized IMSI</p>	<p>The supplied MobileIdentificationNumber or IMSI parameter is within the range of the HLR, but the MIN MS is not Authentication capable or authorized. <i>Note: This response may have been originated by the VLR (MSC).</i></p>
<p>RETURN RESULT DenyAccess</p>	<p>The HLR supports Authentication, but it does not support the requested Authentication feature (e.g., Count updates, Sharing secret data), initiate an AuthenticationStatusReport INVOKE. <i>Note: Only RETURN RESULT operations needing clarification have been included.</i> <i>This response may have been originated by the VLR (MSC).</i></p>

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.3.3 HLR Receiving AuthenticationFailureReport INVOKE

Note: Modified by IS-751.

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

1 IF the received message can be processed:

Steps 1-g through 1-h are proposed for R-UIM.

1-g IF dynamic ESN binding is supported for the MS identified by the received MSID:

1-g-1 IF the received ReportType is *MIN/ESN mismatch*:

1-g-1-1 IF the received ESN is not the current ESN for the MS AND IF the SystemAccessType is *Call origination, Page response, SMS page response, Power down registration, Autonomous registration, or Unspecified*:

1-g-1-1-1 Store the received ESN as pending ESN.

1-g-1-1-2 Mark the MS as *pending ESN rebinding*.

1-g-1-2 ELSE:

1-g-1-2-1 IF the MS is currently registered:

1-g-1-2-1-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to *ReportInCall*.

1-g-1-2-2 ENDIF.

1-g-1-3 ENDIF.

1-g-2 ENDIF.

1-h ENDIF.

1-x Include the MSID parameter set to identify the MS to the AC.

1-1 Relay all other received parameters.

1-2 Start the Authentication Failure Report Timer (AFRT).

1-3 Send an AuthenticationFailureReport INVOKE to the AC associated with the MS.

1-4 WAIT for an Authentication Failure Report response:

1-5 WHEN a RETURN RESULT is received:

1-5-1 Stop timer (AFRT).

1-5-2 IF the message can be processed:

Steps 1-5-2-m through 1-5-2-n are proposed for R-UIM.

1-5-2-m IF the MS is marked as *pending ESN rebinding*:

1-5-2-m-1 IF the DenyAccess parameter is received:

1-5-2-m-1-1 Delete pending ESN for the MS.

1-5-2-m-1-2 Clear the MS's *pending ESN rebinding* flag.

1-5-2-m-1-3 IF the MS is currently registered:

1-5-2-m-1-3-1 Optionally, execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.

1-5-2-m-1-4 ENDIF.

1-5-2-m-2 ELSEIF the RandomVariableUniqueChallenge is received AND IF the RandomVariableSSD is not received:

1-5-2-m-2-1 Start the Authentication Status Report Response Timer (ASRRT).

1-5-2-m-3 ELSE:

1-5-2-m-3-1 IF the MS is currently registered:

1-5-2-m-3-1-1 Execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to Discontinue.

1-5-2-m-3-2 ENDIF.

1-5-2-m-3-3 Update the HLR record for the MS to indicate that the pending ESN is now the current ESN for the MS.

1-5-2-m-3-4 Clear the MS’s pending ESN rebinding flag.

1-5-2-m-4 ENDIF.

1-5-2-n ENDIF.

1-5-2-x IF the SharedSecretData parameter is received:

1-5-2-x-1 IF the MIN may be needed for authentication calculations for the MS:

1-5-2-x-1-1 IF the MobileIdentificationNumber parameter was not present as theMSID parameter in the INVOKE ANDIF the MIN cannot be derived from the IMSI:

1-5-2-x-1-1-1 Include the MobileIdentificationNumber parameter set to identify the MS to the VLR.

1-5-2-x-1-2 ENDIF.

1-5-2-x-2 ENDIF.

1-5-2-y ENDIF.

1-5-2-1 Relay all received parameters.

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

Steps 1-5-2-3 through 1-5-2-4 are proposed for R-UIM.

1-5-2-3 IF the MS is marked as pending ESN rebinding:

1-5-2-3-1 WAIT for an AuthenticationStatusReport INVOKE:

1-5-2-3-2 WHEN an AuthenticationStatusReport INVOKE is received:

1-5-2-3-2-1 Execute the “HLR Receiving AuthenticationStatusReport” task (see 4.5.3).

1-5-2-3-3 WHEN timer (ASSRT) expires:

1-5-2-3-3-1 Continue processing.

1-5-2-3-4 ENDWAIT.

1-5-2-3-5 IF the MS is marked as pending ESN rebinding:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- 1-5-2-3-5-1 Delete pending ESN for the MS.
- 1-5-2-3-5-2 Clear the MS's *pending ESN rebinding* flag.
- 1-5-2-3-5-3 IF the MS is currently registered:
 - 1-5-2-3-5-3-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.
- 1-5-2-3-5-4 ENDIF.
- 1-5-2-3-6 ENDIF.
- 1-5-2-3 ENDIF.
- 1-5-3 ELSE:
 - 1-5-3-1 Send a RETURN ERROR with the Error Code set to indicate *SystemFailure* to the requesting VLR.

Steps 1-5-3-2 through 1-5-3-3 are proposed for R-UIM.

- 1-5-3-2 IF the MS is marked as *pending ESN rebinding*:
 - 1-5-3-2-1 Delete pending ESN for the MS.
 - 1-5-3-2-2 Clear the MS's *pending ESN rebinding* flag.
 - 1-5-3-2-3 IF the MS is currently registered:
 - 1-5-3-2-3-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.
 - 1-5-3-2-4 ENDIF.
- 1-5-3-3 ENDIF.
- 1-5-4 ENDIF.
- 1-6 WHEN a RETURN ERROR or REJECT is received:
 - 1-6-1 Stop timer (AFRT).

Steps 1-6-a through 1-6-b are proposed for R-UIM.

- 1-6-a IF the MS is marked as *pending ESN rebinding*:
 - 1-6-a-1 Delete pending ESN for the MS.
 - 1-6-a-2 Clear the MS's *pending ESN rebinding* flag.
 - 1-6-a-3 IF the MS is currently registered:
 - 1-6-a-3-1 Optionally, execute the "HLR Initiating Registration Cancellation" task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to ReportInCall.
 - 1-6-a-4 ENDIF.
- 1-6-b ENDIF.
- 1-6-2 CASE Error Code OF:
 - 1-6-3 *ParameterError*:
 - 1-6-3-1 IF the parameter was originated from the initiating functional entity:
 - 1-6-3-1-1 Send a RETURN ERROR with Error Code set to indicate *ParameterError*.

UIM Rev. 8.0 (Ballot Version)

1-6-3-2 ELSE:
 1-6-3-2-1 Send a RETURN ERROR with Error Code set to indicate *SystemFailure*.
 1-6-3-3 ENDIF.
 1-6-4 DEFAULT:
 1-6-4-1 Send a RETURN ERROR with Error Code set to indicate *SystemFailure*.
 1-6-5 ENDCASE.
 1-6-6 Execute “Local Recovery Procedures” task (see 3.5.1).
 1-6-7 Exit this task.
 1-7 WHEN timer (AFRT) expires:

Steps 1-7-c through 1-7-d are proposed for R-UIM.

1-7-c IF the MS is marked as *pending ESN rebinding* and the MS is not marked as *pending Unique Challenge*:
1-7-c-1 Delete pending ESN for the MS.
1-7-c-2 Clear the MS’s *pending ESN rebinding* flag.
1-7-c-3 IF the MS is currently registered:
1-7-c-3-1 Optionally, execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the *ElectronicSerialNumber* parameter set to the current ESN and with the *CancellationType* parameter set to *ReportInCall*.
1-7-c-4 ENDIF.
1-7-d ENDIF.
 1-7-1 Send a RETURN ERROR with the Error Code set to indicate *SystemFailure*.
 1-7-2 Execute “Local Recovery Procedures” task (see 3.5.1).
 1-7-3 Exit this task.
 1-8 ENDWAIT.
 2 ELSE (the received message cannot be processed):
 2-1 Send a RETURN ERROR with the proper Error Code value (see the following table) to the requesting VLR.
 3 ENDIF.
 4 Exit this task.

One change is proposed to the error table for R-UIM.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Table 6 HLR AuthenticationFailureReport Response

Problem Detection and Recommended Response from HLR to VLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
UnrecognizedMIN	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
UnrecognizedESN	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
MINMSID/HLRMismatch	The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MIN MSID is not in the AC (HLR)'s range of MIN's MSID's or directory numbers (suspect routing error). <i>Note: This response may have been originated by the AC (HLR).</i>
OperationSequenceProblem	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
ResourceShortage	A required AC (HLR) resource (internal memory record, AC (HLR/VLR) is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the AC (HLR).</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported by the receiving AC (HLR/VLR) or the requesting functional entity is not authorized. <i>Note: It is recommended that an AC (HLR) supports AuthenticationFailureReport transactions. This response may have been originated by the AC (HLR).</i>
TrunkUnavailable	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
ParameterError	A supplied parameter value has an encoding problem (e.g., the supplied MobileIdentificationNumber parameter or Digits (Dialed) parameter digit values do not meet the expected BCD specification)). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the AC (HLR).</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used, SystemCapabilities (SYSCAP) parameter indicated authentication is not supported (AUTH is 0) but this AuthenticationFailureReport was received). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter. This response may have been originated by the AC (HLR).</i>
FeatureInactive	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>

UIM Rev. 8.0 (Ballot Version)

<p>MissingParameter</p>	<p>An optional parameter required by the AC (HLR) was expected, but not received (e.g., a SSD update process was in-progress and a ReportType set to <i>SSD update successful</i> was received, but the expected second ReportType parameter indicating the CallHistoryCount's (COUNT's) incrementing status (e.g., COUNT update successful, COUNT mismatch, Count update no response etc.) was not received).</p> <p><i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p> <p><i>This response may have been originated by the AC (HLR).</i></p>
<p>RETURN RESULT DenyAccess</p>	<p>The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MINMSID is within the range of the AC (HLR), but the MIN MSID is not presently assigned to a subscriber. DenyAccess parameter value is <i>Unspecified</i>.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the supplied ElectronicSerialNumber parameter does not match the ESN in the MIN'SMSID's record <u>and the MS is not marked <i>pending ESN rebinding</i></u>. DenyAccess parameter value is <i>Unspecified</i>.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the MIN MSID is either a DelinquentAccount, StolenUnit, DuplicateUnit or Unspecified. DenyAccess parameter value is <i>Unspecified</i>.</p> <p><i>Note: Only RETURN RESULT operations needing clarification have been included.</i></p>

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.3.4 AC Receiving AuthenticationFailureReport INVOKE

Note: Modified by IS-778.

When an AC receives an AuthenticationFailureReport INVOKE, it shall perform the following:

- 1 IF the received message can be processed:
 - 1-1 IF the MSCID parameter is not received (the VLR is *TSB51* compliant):
 - 1-1-1 IF *TSB51* operation is supported:
 - 1-1-1-1 Execute *TSB51* procedures for the SecurityStatusReport (refer to *TIA/EIA TSB51*).
 - 1-1-2 ELSE (*TSB51* operation is not supported):
 - 1-1-2-1 Send a RETURN ERROR with the error code set to *OperationNotSupported*.
 - 1-1-3 ENDIF.
 - 1-1-4 Exit this task.
 - 1-2 ELSE (the MSCID parameter is received (the VLR is not *TSB51* compliant):

Steps 1-2-a through 1-2-e are proposed for R-UIM.

- 1-2-a IF dynamic ESN binding is supported for the MS identified by the received MSID:
 - 1-2-a-1 IF the received ReportType is *MIN/ESN mismatch*:
 - 1-2-a-1-1 IF the received ESN is not the current ESN for the MS AND IF the SystemAccessType is *Call origination, Page response, SMS page response, Power down registration, Autonomous registration, or Unspecified*:
 - 1-2-a-1-1-1 Store the received ESN as *pending ESN*.
 - 1-2-a-1-1-2 Mark the MS as *pending ESN rebinding*.
 - 1-2-a-1-1-3 IF an authentication directive is to be used to initiate a Unique Challenge of the MS:
 - 1-2-a-1-1-3-1 Select a *RandomVariableUniqueChallenge (RANDU)* and execute *CAVE* using the value of the *pending ESN* to produce an *AuthenticationResponseUniqueChallenge (AUTHU)*.
 - 1-2-a-1-1-3-2 Include the *RandomVariableUniqueChallenge (RANDU)* and *AuthenticationResponseUniqueChallenge (AUTHU)* parameters.
 - 1-2-a-1-1-3-3 Execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the *ElectronicSerialNumber* parameter set to the current ESN.
 - 1-2-a-1-1-3-4 IF the MS is marked as *pending ESN rebinding*:
 - 1-2-a-1-1-3-4-1 Delete *pending ESN* for the MS.
 - 1-2-a-1-1-3-4-2 Clear the MS’s *pending ESN rebinding* flag.
 - 1-2-a-1-1-3-4-3 Include the *DenyAccess* parameter.
 - 1-2-a-1-1-3-4-4 Send a RETURN RESULT.

UIM Rev. 8.0 (Ballot Version)

1-2-a-1-1-3-4-5 IF the SSD is currently shared for the MS:

1-2-a-1-1-3-4-5-1 Optionally, include the SSDNotShared parameter and execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.

1-2-a-1-1-3-4-6 ENDIF.

1-2-a-1-1-3-4-7 Exit this task.

1-2-a-1-1-3-5 ENDIF.

1-2-a-1-1-4 ENDIF.

1-2-a-1-2 ELSE:

1-2-a-1-2-1 IF the SSD is currently shared for the MS:

1-2-a-1-2-1-1 Optionally, include the SSDNotShared parameter and execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.

1-2-a-1-2-2 ENDIF.

1-2-a-1-3 ENDIF.

1-2-a-2 ENDIF.

1-2-b ENDIF.

1-2-c IF the MS is marked as *pending ESN rebinding*:

1-2-c-1 Select the pending ESN as the ESN to be used as input to all authentication calculations requiring ESN input during this invocation of the “AC Receiving AuthenticationFailureReport INVOKE” task.

1-2-d ELSE:

1-2-d-1 Select the current ESN as the ESN to be used as input to all authentication calculations requiring ESN input during this invocation of the “AC Receiving AuthenticationFailureReport INVOKE” task.

1-2-e ENDIF.

1-2-1 IF the ReportType parameter indicates that an authentication failure has been detected:

1-2-1-1 Execute recovery procedures according to the AC’s internal algorithm.

1-2-2 ENDIF.

1-2-3 IF service shall be denied:

1-2-3-1 Include the DenyAccess parameter.

1-2-3-2 Send a RETURN RESULT.

Steps 1-2-3-g through 1-2-3-h are proposed for R-UIM.

1-2-3-g IF the MS is marked as *pending ESN rebinding*:

1-2-3-g-1 Delete pending ESN for the MS.

1-2-3-g-2 Clear the MS’s *pending ESN rebinding* flag.

1-2-3-g-3 IF the SSD is currently shared for the MS:

1-2-3-g-3-1 Optionally, include the SSDNotShared parameter and execute the “AC Initiation of an Authentication Directive” task (see

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.

- 1-2-3-g-4 ENDIF.
- 1-2-3-h ENDIF.
- 1-2-3-3 Exit this task.
- 1-2-4 ENDIF.
- 1-2-5 IF SharedSecretData (SSD) presently shared with the VLR shall be discarded:
- 1-2-5-1 Include the SSDNotShared (NOSSD) parameter.
- 1-2-6 ENDIF.
- 1-2-7 IF an SSD update shall be initiated:
- 1-2-7-1 Select a RandomVariableSSD (RANDSSD) value and execute CAVE using the value of the MS's A-key recorded in the AC's database to produce a pending SSD.
- 1-2-7-2 Include the RandomVariableSSD (RANDSSD) parameter.
- 1-2-7-3 Mark the MS *pending SSD update*.
- 1-2-7-4 IF AC administrative procedures indicate that the pending SSD shall be shared with the VLR for the SSD update operation AND IF the VLR's SystemCapabilities (SYSCAP) indicates that the VLR is able to execute the CAVE algorithm:
- 1-2-7-4-1 Include the SharedSecretData (SSD) parameter set to the pending SSD value.
- 1-2-7-4-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different from the default value:
- 1-2-7-4-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.
- 1-2-7-4-3 ENDIF.
- ~~1-2-7-4~~ ~~IF AC administrative procedures indicate that the pending SSD shall be shared with the VLR for the SSD update operation:~~
- ~~1-2-7-4-1~~ ~~IF the VLR's SystemCapabilities (SYSCAP) indicates that the VLR is able to execute the CAVE algorithm:~~
- ~~1-2-7-4-1-1~~ ~~Include the SharedSecretData (SSD) parameter set to the pending SSD value.~~
- ~~1-2-7-4-1-2~~ ~~IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:~~
- ~~1-2-7-4-1-2-1~~ ~~Include the AuthenticationAlgorithmVersion (AAV) parameter.~~
- ~~1-2-7-4-1-3~~ ~~ENDIF.~~
- ~~1-2-7-4-2~~ ~~ENDIF.~~
- 1-2-7-5 ELSE (the pending SSD is not shared):
- 1-2-7-5-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the pending SSD to produce an AuthenticationResponseUnique (AUTHU).
- 1-2-7-5-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.
- 1-2-7-5-3 Mark the MS *pending Unique Challenge*.
- 1-2-7-6 ENDIF.
- 1-2-8 ELSE (SSD update not initiated):

UIM Rev. 8.0 (Ballot Version)

- 1-2-8-1 IF the SharedSecretData (SSD) shall be shared with the VLR:
- 1-2-8-1-1 IF the VLR's SystemCapabilities (SYSCAP) indicates the VLR is capable of executing the CAVE algorithm:
- 1-2-8-1-1-1 Include the SharedSecretData (SSD) and CallHistoryCount (COUNT) parameters.
- 1-2-8-1-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:
- 1-2-8-1-1-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.
- 1-2-8-1-1-3 ENDIF.
- 1-2-8-1-2 ENDIF.
- 1-2-8-2 ENDIF.
- 1-2-8-3 IF a Unique Challenge shall be initiated:
- 1-2-8-3-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the AC's database to produce an AuthenticationResponseUnique (AUTHU).
- 1-2-8-3-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique (AUTHU) parameters.
- 1-2-8-3-3 Mark the MS *pending Unique Challenge*.
- 1-2-8-4 ENDIF.
- 1-2-9 ENDIF.
- 1-2-10 IF a COUNT update shall be initiated:
- 1-2-10-1 Include the UpdateCount (UPDCOUNT) parameter.
- 1-2-10-2 Mark the MS *pending COUNT update*.
- 1-2-11 ENDIF.

Steps 1-2-q through 1-2-r are proposed for R-UIM.
--

- 1-2-q IF the MS is marked as *pending ESN rebinding*:
- 1-2-q-1 IF the MS is not marked *pending Unique Challenge* OR IF the MS is marked *pending SSD update*:
- 1-2-q-1-1 IF the SSD is currently shared for the MS:
- 1-2-q-1-1-1 Include the SSDNotShared parameter and execute the "AC Initiation of an Authentication Directive" task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.
- 1-2-q-1-2 ENDIF.
- 1-2-q-1-2-1 Update the AC record for the MS to indicate that the pending ESN is now the current ESN for the MS.
- 1-2-q-1-2-2 Clear the MS's *pending ESN rebinding* flag.
- 1-2-q-1-3 ENDIF.
- 1-2-q-2 ENDIF.
- 1-2-r ENDIF.
- 1-2-12 Send a RETURN RESULT to the requesting HLR.
- 1-2-13 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*:

1-2-13-1 Execute the “AC Awaiting AuthenticationStatusReport INVOKE” task (see 4.5.4).

Steps 1-2-13-2 through 1-2-13-3 are proposed for R-UIM.

- 1-2-13-2 IF the MS is marked as *pending ESN rebinding*:
- 1-2-13-2-1 Delete pending ESN for the MS.
- 1-2-13-2-2 Clear the MS’s *pending ESN rebinding* flag.
- 1-2-13-2-3 IF the SSD is currently shared for the MS:
- 1-2-13-2-3-1 Optionally, include the *SSDNotShared* parameter and execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the *ElectronicSerialNumber* parameter set to the current ESN, to end SSD sharing.
- 1-2-13-2-4 ENDIF.
- 1-2-13-3 ENDIF.
- 1-2-14 ENDIF.
- 1-2-15 Exit this task.
- 1-3 ENDIF.
- 2 ELSE (the message cannot be processed):
- 2-1 Send a RETURN ERROR to the requesting HLR.
- 3 ENDIF.
- 4 Exit this task.

One change is proposed to the error table for R-UIM.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Table 7 AC AuthenticationFailureReport Response

Problem Detection and Recommended Response from AC to HLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
UnrecognizedMIN	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
UnrecognizedESN	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
MINMSID/HLRMismatch	The supplied MIN's MSID's AC (HLR) responded that the MobileIdentificationNumber or IMSI parameter is not in the AC (HLR)'s range of MIN's MSID's or directory numbers (suspect routing error). <i>Note: This response may have been originated by the AC (HLR).</i>
OperationSequenceProblem	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
ResourceShortage	A required AC (HLR) resource (e.g., internal memory record, AC (HLR/VLR) is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the AC (HLR).</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported by the receiving AC (HLR/VLR) or the requesting functional entity is not authorized. <i>Note: It is recommended that an AC (HLR) supports AuthenticationFailureReport transactions. This response may have been originated by the AC (HLR).</i>
TrunkUnavailable	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>
ParameterError	A supplied parameter value has an encoding problem (e.g., the supplied MobileIdentificationNumber parameter or Digits (Dialed) parameter digit values do not meet the expected BCD specification)). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the AC (HLR).</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., <i>Not used</i> , SystemCapabilities (SYSCAP) parameter indicated authentication is not supported (AUTH is 0) but this AuthenticationFailureReport was received). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter. This response may have been originated by the AC (HLR).</i>
FeatureInactive	<i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationFailureReport transaction.</i>

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

<p>MissingParameter</p>	<p>An optional parameter required by the AC (HLR) was expected, but not received (e.g., a SSD update process was in-progress and a ReportType set to <i>SSD update successful</i> was received, but the expected second ReportType parameter indicating the CallHistoryCount's (COUNT's) incrementing status (e.g., <i>COUNT update successful</i>, <i>COUNT mismatch</i>, <i>Count update no response</i> etc.) was not received).</p> <p><i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p> <p><i>This response may have been originated by the AC (HLR).</i></p>
<p>RETURN RESULT DenyAccess</p>	<p>The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MIN MSID is within the range of the AC (HLR), but the MIN MSID is not presently assigned to a subscriber. DenyAccess parameter value is <i>Unspecified</i>.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the supplied ElectronicSerialNumber parameter does not match the ESN in the MIN's MSID's record <u>and the MS is not marked <i>pending ESN rebinding</i></u>. DenyAccess parameter value is <i>Unspecified</i>.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the MIN MSID is either a DelinquentAccount, StolenUnit, DuplicateUnit or Unspecified. DenyAccess parameter value is <i>Unspecified</i>.</p> <p><i>Note: Only RETURN RESULT operations needing clarification have been included.</i></p>

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 OR IF a REJECT or an *OperationNotSupported* RETURN ERROR has been received in the recent past in response to an attempt to authenticate the MS OR IF the VLR is aware that the HLR does not support authentication:
 - 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 *Unspecified*.
 - 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:

Note: Steps 1-5-1 through 1-5-2 added for UIM support.

- ~~1-5-1 IF the AuthenticationCapability parameter indicates *Authentication required and UIM capable*:~~
 - ~~1-5-1-1 GOTO Initiate Global Challenge.~~
 - ~~1-5-2 ENDIF.~~
- ~~1-5-1 IF the MobileIdentificationNumber 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 *MIN/ESN Mismatch*.~~
 - ~~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 *TERMTYP mismatch*.
 - 1-5-3-3 Exit this task.

UIM Rev. 8.0 (Ballot Version)

1-5-4 ENDIF.

1-5-5 IF the SystemAccessType is *Autonomous registration, Power down registration, Call origination, Page response, or SMS page response*:

1 IF the received SystemCapabilities (SYSCAP) parameter indicates that the Serving MSC requested authentication parameters for this system access (AUTH=1 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 *Missing authentication parameters*.

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

1-5-5-1-2 ELSEIF the AuthenticationData parameter was received:

1-5-5-1-2-1 Execute CAVE using the value of the RandomVariable (RAND) parameter, the MS’s SharedSecretData (SSD) recorded in the VLR’s database, the ESN and the AuthenticationData parameter.

1-5-5-1-3 ELSE:

~~1-5-5-1-2 ELSE (authentication parameters were received from the MS):~~

1-5-5-1-3-1 Convert values in the Digits (Dialed) parameter (if received) into TBCD encoding.

1-5-5-1-3-2 Execute CAVE using the value of the MS’s SharedSecretData (SSD) recorded in the VLR’s database and the parameters requested by the SystemAccessType.

1-5-5-1-4 ENDIF.

1-5-5-1-5 IF the CAVE authentication result and the AuthenticationResponse (AUTHR) received from the MS (see Annex C “Authentication Response Verification”) do not match:

1-5-5-1-5-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-5-1-5-2 Execute the “VLR Initiating an Authentication Failure Report” task (see 4.3.5) with the ReportType parameter set to indicate *AUTHR mismatch*.

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

1-5-5-1-6 ENDIF.

1-5-5-1-7 IF the stored count and the CallHistoryCount (COUNT) reported by the MS do not match:

1-5-5-1-7-1 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-5-5-1-7-2 Include the CallHistoryCount (COUNT) parameter set to the COUNT reported by the MS.

1-5-5-1-7-3 Include the CallHistoryCountExpected parameter set to the COUNT expected by the VLR.

1-5-5-1-7-4 Execute the “VLR Initiating an Authentication Failure Report” task (see 4.3.5) with the ReportType parameter set to indicate *COUNT mismatch*.

1-5-5-1-7-5 Exit this task.

- 1-5-5-1-8 ENDIF.
- 1-5-5-1-9 IF the SystemAccessType is *Call origination* or *Page response*:
- 1-5-5-1-9-1 Generate the SignalingMessageEncryptionKey (SMEKEY) parameter.
- 1-5-5-1-9-2 Include the SignalingMessageEncryptionKey (SMEKEY) parameter.
- 1-5-5-1-9-3 IF the MS's Service Profile indicates that the MS subscribes to Voice Privacy:
- 1-5-5-1-9-3-1 IF the MS supports TDMA:
- 1-5-5-1-9-3-1-1 Generate the VoicePrivacyMask (VPMASK).
- 1-5-5-1-9-3-1-2 Include the VoicePrivacyMask (VPMASK) parameter.
- 1-5-5-1-9-3-2 ELSEIF the MS supports CDMA:
- 1-5-5-1-9-3-2-1 Generate the CDMAPrivateLongCodeMask (CDMAPLCM).
- 1-5-5-1-9-3-2-2 Include the CDMAPrivateLongCodeMask (CDMAPLCM) parameter.
- 1-5-5-1-9-3-3 ENDIF.
- 1-5-5-1-9-4 ENDIF.

The next four steps are for IS-737 (with minor editorial enhancements).

- 1-5-5-1-9-5 IF the MS's Service Profile indicates that the MS subscribes to Data Privacy.
- 1-5-5-1-9-5-1 Generate the DataKey (DKEY).
- 1-5-5-1-9-5-2 Include the DataKey (DKEY) parameter.
- 1-5-5-1-9-6 ENDIF.
- 1-5-5-1-10 ENDIF.

Other than the additions for IS-737, the block of steps above is a block whose indentation level was reduced (with consequent step renumbering) by IS-778.

- ~~1-5-5-1-3 ENDIF.~~
- 1-5-5-2 ENDIF.
- 1-5-6 ELSEIF the SystemAccessType is *Flash request* ~~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 AuthenticationResponseUniqueChallenge (AUTHU).
- 1-5-6-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.
- 1-5-6-3 Mark the MS *pending Unique Challenge*.
- 1-5-7 ENDIF.
- 1-5-8 IF the SystemAccessType is *Unspecified* OR IF the SuspiciousAccess parameter was included in the received AuthenticationRequest INVOKE OR IF local administrative procedures request that a Unique Challenge shall be initiated:

UIM Rev. 8.0 (Ballot Version)

- 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 AuthenticationResponseUniqueChallenge (AUTHU).
- 1-5-8-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (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):

Note: label added for UIM support.

Initiate Global Challenge

- 1-6-1 Relay the SystemCapabilities (SYSCAP) parameter modified to indicate whether the VLR is able to perform CAVE.
- 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
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

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

1-6-9-2-1-2 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 AuthenticationResponseUniqueChallenge (AUTHU).

1-6-9-2-2-5-5-5 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (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 AuthenticationResponseUniqueChallenge (AUTHU) parameter.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

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 AuthenticationResponseUniqueChallenge (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.

The next three steps are for IS-737 (with minor editorial enhancements).

1-6-9-2-2-15a IF the DataKey (DKEY) is received:

1-6-9-2-2-15a-1 Relay the the DataKey (DKEY) parameter.

1-6-9-2-2-15b ENDIF.

The next twelve steps are for IS-735 (with minor editorial enhancements).

1-6-9-2-2-15b IF the AnalogRedirectRecord (ANALOGRR) is received:

1-6-9-2-2-15b-1 Relay the AnalogRedirectRecord (ANALOGRR) parameter.

1-6-9-2-2-15c ENDIF.

1-6-9-2-2-15d IF the CDMARedirectRecord (CDMARR) is received:

1-6-9-2-2-15d-1 Relay the CDMARedirectRecord (CDMARR) parameter.

1-6-9-2-2-15e ENDIF.

1-6-9-2-2-15f IF the ServiceRedirectionInfo (SRINFO) is received:

1-6-9-2-2-15f-1 Relay the ServiceRedirectionInfo (SRINFO) parameter.

1-6-9-2-2-15g ENDIF.

1-6-9-2-2-15h IF the RoamingIndication (ROAMIND) is received:

1-6-9-2-2-15h-1 Relay the RoamingIndication (ROAMIND) parameter.

1-6-9-2-2-15i ENDIF.

1-6-9-2-2-16 Send an AuthenticationRequest RETURN RESULT to the requesting MSC.

1-6-9-2-2-17 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*:

1-6-9-2-2-17-1 Execute the "VLR Awaiting AuthenticationStatusReport INVOKE" task (see 4.5.2).

1-6-9-2-2-18 ENDIF.

1-6-9-2-2-19 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 *SystemFailure*.

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-a *OperationNotSupported*:

1-6-10-a-1 Send a RETURN RESULT to the requesting MSC.

1-6-10-a-2 Exit this task.

1-6-10-3 *ParameterError*:

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 *ParameterError to the MSC*.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1-6-10-3-2 ELSE:
 1-6-10-3-2-1 Send a RETURN ERROR with the Error Code indicating *SystemFailure* to the MSC.
 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 *SystemFailure* to the MSC.
 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-a WHEN a REJECT is received:
1-6-a-1 Stop timer (ART).
1-6-a-2 Send a RETURN RESULT to the requesting MSC.
1-6-a-3 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 *SystemFailure*.
 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.

While the dieted table is all new, it has not been underlined since that would make it harder to focus on the substantive changes, which are the changes shown to the contents of the cells.

Changes to the error table are for IS-735, IS-751, IS-778, Miscellaneous 10, the error table diet, and the correction of errors agreed during the integration process.

The sources for technical changes are:

- Changes to problem detection 4 are for IS-735, IS-751, and IS-778.
- Changes to problem detection 5 are for Miscellaneous 10.
- Problem detection 6 was deleted by IS-778.
- Changes to problem detection 7 are for IS-778.
- Note e was removed from all errors except *ParameterError* and *SystemFailure* (and in particular, it was aged that *MSID/HLRMismatch* was not an appropriate response) during the integration process.
- Problem detection 8 was deleted during the integration process.

Table 8 VLR AuthenticationRequest Response

UIM Rev. 8.0 (Ballot Version)

Problem Detection and Recommended Response from VLR to MSC	
RETURN ERROR Error Code	PROBLEM DEFINITION
ResourceShortage	A required VLR resource (e.g., internal memory record, VLR is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the AC (HLR) or HLR.</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving VLR, or the requesting functional entity is not authorized. <i>Note: This response may have been originated by the AC (HLR) or HLR.</i> <i>Note: It is recommended that a VLR supports AuthenticationRequest transactions.</i>
ParameterError	A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or IMSI 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 Call origination). <i>Note: This response may have been originated by the AC (HLR) or HLR.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the AC (HLR) or HLR.</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used). <i>Note: This response may have been originated by the AC (HLR) or HLR.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
MissingParameter	An optional parameter required by the AC (HLR) was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported (AUTH=1), but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not were received; or SystemAccessType indicated Call origination, but Digits (Dialed) parameter was not received). <i>Note: This response may have been originated by the AC (HLR) or HLR.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
RETURN RESULT DenyAccess	The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MIN-MS cannot be Authenticated because of the reason identified by the supplied DenyAccess parameter value. <i>Note: This response may have been originated by the AC (HLR) or HLR.</i> <i>Note: Only RETURN RESULT operations needing clarification have been included.</i>

Table 8 – VLR AuthenticationRequest Response

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Problem Detection and Recommended Response from VLR to MSC									
PROBLEM DEFINITION	1	2	3	4	5	6	7	8	Notes
RETURN ERROR Error Code									
<i>UnrecognizedMIN</i>									a
<i>UnrecognizedESN</i>									a
<i>MIN/HLRMismatch</i>						x			e
<i>OperationSequenceProblem</i>									a
<i>ResourceShortage</i>		x							e
<i>OperationNotSupported</i>	x								b, e
<i>TrunkUnavailable</i>									a
<i>ParameterError</i>				x					d, e
<i>SystemFailure</i>			x						e
<i>UnrecognizedParameterValue</i>					x				d, e
<i>FeatureInactive</i>									a
<i>MissingParameter</i>							x		d, e
RETURN RESULT DenyAccess								x	e, 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 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 Call origination).~~
5. ~~A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used).~~
6. ~~The supplied MobileIdentificationNumber parameter's AC (HLR) responded that the MIN is not in the AC (HLR)'s range of MINs 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 (AUTH=1) but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not received; or SystemAccessType indicated Call origination, but Digits (Dialed) parameter was not received).~~
8. ~~The supplied MobileIdentificationNumber parameter's AC (HLR) responded that the MIN 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.~~
- e. ~~Only RETURN RESULT operations needing clarification have been included.~~
- d. ~~Include the Parameter Identifier in question as the FaultyParameter parameter.~~
- e. ~~This response may have been originated by the AC (HLR).~~

UIM Rev. 8.0 (Ballot Version)

All changes not otherwise identified are from IS-778.

4.4.3 HLR Receiving AuthenticationRequest INVOKE

Changes not otherwise identified are for IS-778.

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

1 IF the received message can be processed:

Steps 1-X through 1-Y are for IS-735 (with minor editorial enhancements).

1-X IF the MS identity is within the range of the HLR:

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

1-X-1-1-1-1 Include the CDMARedirectRecord of the selected system.

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

1-X-1-1-2-1 Include the AnalogRedirectRecord of the selected system.

1-X-1-1-3 ENDIF.

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

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

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

1-X-1-1-7 Exit this task.

1-X-1-2 ENDIF.

1-X-2 ENDIF.

1-Y ENDIF.

1-a IF the MS's AuthenticationCapability indicates *No authentication required*:

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

1-a-2 Exit this task.

1-b ENDIF.

Steps 1-g through 1-h are proposed for R-UIM.

1-g IF dynamic ESN binding is supported for the MS identified by the received MSID:

1-g-1 IF the received ESN is not the current ESN for the MS AND IF the SystemAccessType is *Call origination, Page response, SMS page response, Power down registration, Autonomous registration, or Unspecified*:

1-g-1-1 Store the received ESN as pending ESN.

1-g-1-2 Mark the MS as *pending ESN rebinding*.

1-g-2 ENDIF.

1-h ENDIF.

Steps 1-Z is for IS-735 and IS-751 (with minor editorial enhancements).

- 1-Z Include the MSID parameter set to identify the MS to the AC.
- 1-1 Include the SenderIdentificationNumber set to the identification number of the HLR.
- 1-2 Relay all other received parameters.
- 1-3 Send an AuthenticationRequest INVOKE to the AC associated with the MS.
- 1-4 Start the Authentication Request Timer (ART).
- 1-5 WAIT for an Authentication Request response:
- 1-6 WHEN a RETURN RESULT is received:
- 1-6-1 Stop timer (ART).
- 1-6-2 IF the message can be processed:

Steps 1-6-2-a through 1-6-2-b are for IS-735 and IS-751.

- 1-6-2-a IF the SharedSecretData parameter is received:
- 1-6-2-a-1 IF the MIN may be needed for authentication calculations for the MS:
- 1-6-2-a-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:
- 1-6-2-a-1-1-1 Include theMobileIdentificationNumber parameter set to identify the MS to the VLR.
- 1-6-2-a-1-2 ENDIF.
- 1-6-2-a-2 ENDIF.
- 1-6-2-b ENDIF.
- 1-6-2-1 IF the MS's service profile indicates that the MS is not authorized for Voice Privacy:
- 1-6-2-1-1 Discard any received VoicePrivacyMask (VPMASK) or CDMAPrivateLongCodeMask (CDMAPLCM) parameters.
- 1-6-2-2 ENDIF.

The next three steps are for IS-737.

- 1-6-2-2a IF the MS's service profile indicates that the MS is not authorized for Data Privacy:
- 1-6-2-2a-1 Discard the DataKey (DKEY) parameter.
- 1-6-2-2b ENDIF.

Steps 1-6-2-m through 1-6-2-n are proposed for R-UIM.

- 1-6-2-m IF the MS is marked as *pending ESN rebinding*:
- 1-6-2-m-1 IF the DenyAccess parameter is received:
- 1-6-2-m-1-1 Delete pending ESN for the MS.
- 1-6-2-m-1-2 Clear the MS's *pending ESN rebinding* flag.
- 1-6-2-m-2 ELSEIF the RandomVariableUniqueChallenge is received AND IF the RandomVariableSSD is not received:
- 1-6-2-m-2-1 Start the Authentication Status Report Response Timer (ASRRT).

1-6-2-m-3 ELSE:
 1-6-2-m-3-1 IF the MS is currently registered:
 1-6-2-m-3-1-1 Execute the “HLR Initiating Registration Cancellation”
 task (see 4.37.1) with the ElectronicSerialNumber
 parameter set to the current ESN and with the
 CancellationType parameter set to *Discontinue*.
 1-6-2-m-3-2 ENDIF.
 1-6-2-m-3-3 Update the HLR record for the MS to indicate that the pending
 ESN is now the current ESN for the MS.
 1-6-2-m-3-4 Clear the MS’s *pending ESN rebinding* flag.
 1-6-2-m-4 ENDIF.
 1-6-2-n ENDIF.
 1-6-2-3 Relay all other received parameters.
 1-6-2-4 Send a RETURN RESULT to the requesting VLR.

Steps 1-6-2-p through 1-6-2-q are proposed for R-UIM.

1-6-2-p IF the MS is marked as *pending ESN rebinding*:
 1-6-2-p-1 WAIT for an AuthenticationStatusReport INVOKE:
 1-6-2-p-2 WHEN an AuthenticationStatusReport INVOKE is received:
 1-6-2-p-2-1 Execute the “HLR Receiving AuthenticationStatusReport”
 task (see 4.5.3).
 1-6-2-p-3 WHEN timer (ASSRT) expires:
 1-6-2-p-3-1 Continue processing.
 1-6-2-p-4 ENDWAIT.
 1-6-2-p-5 IF the MS is marked as *pending ESN rebinding*:
 1-6-2-p-5-1 Delete pending ESN for the MS.
 1-6-2-p-5-2 Clear the MS’s *pending ESN rebinding* flag.
 1-6-2-p-6 ENDIF.
 1-6-2-q ENDIF.
 1-6-2-5 Exit this task.
 1-6-3 ELSE (the message cannot be processed):

Steps 1-6-2-i through 1-6-2-j are proposed for R-UIM.

1-6-2-i IF the MS is marked as *pending ESN rebinding*:
 1-6-2-i-1 Delete pending ESN for the MS.
 1-6-2-i-2 Clear the MS’s *pending ESN rebinding* flag.
 1-6-2-j ENDIF.
 1-6-3-1 Send a RETURN ERROR to the requesting VLR with the Error Code
 indicating *SystemFailure*.
 1-6-3-2 Execute the “Local Recovery Procedures” task (see 3.5.1).
 1-6-3-3 Exit this task.
 1-6-4 ENDIF.
 1-7 WHEN a RETURN ERROR or REJECT is received:
 1-7-1 Stop timer (ART).

Steps 1-7-c through 1-7-d are proposed for R-UIM.

- 1-7-c IF the MS is marked as *pending ESN rebinding*:
- 1-7-c-1 Delete pending ESN for the MS.
- 1-7-c-2 Clear the MS's *pending ESN rebinding* flag.
- 1-7-d ENDIF.
- 1-7-2 Send a RETURN ERROR to the requesting VLR with the received Error Code.
- ~~1-7-2~~ CASE Error Code OF:
- ~~1-7-3~~ *ParameterError*:
- ~~1-7-3-1~~ Send a RETURN ERROR to the requesting VLR with the Error Code indicating *ParameterError*.
- ~~1-7-4~~ *DEFAULT*:
- ~~1-7-4-1~~ Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.
- ~~1-7-5~~ ENDCASE.

This gap in step numbers is present in IS-778.

- 1-7-6 Execute the "Local Recovery Procedures" task (see 3.5.1).
- 1-7-7 Exit this task.
- 1-b WHEN a REJECT is received:
- 1-b-1 Stop timer (ART).

Steps 1-b-e through 1-b-f are proposed for R-UIM.

- 1-b-e IF the MS is marked as *pending ESN rebinding*:
- 1-b-e-1 Delete pending ESN for the MS.
- 1-b-e-2 Clear the MS's *pending ESN rebinding* flag.
- 1-b-f ENDIF.
- 1-b-2 Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.
- 1-b-3 Execute the "Local Recovery Procedures" task (see 3.5.1).
- 1-b-4 Exit this task.
- 1-8 WHEN timer (ART) expires:

Steps 1-8-s through 1-8-t are proposed for R-UIM.

- 1-8-s IF the MS is marked as *pending ESN rebinding*:
- 1-8-s-1 Delete pending ESN for the MS.
- 1-8-s-2 Clear the MS's *pending ESN rebinding* flag.
- 1-8-t ENDIF.
- 1-8-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.
- 1-8-2 Execute the "Local Recovery Procedures" task (see 3.5.1).
- 1-8-3 Exit this task.
- 1-9 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_

```

Changes to the error table are for IS-735, IS-751, IS-778, Miscellaneous 10, the error table diet, and changes accepted during the integration process. While the dieted table is all new, it has not been underlined since that would make it harder to focus on the substantive changes:

- Changes to problem detection 5 are for Miscellaneous 10.
- Changes to problem detection 6 are for IS-735 and IS-751.
- Changes to problem detection 4 are for IS-735, IS-751, and IS-778.
- Changes to problem detection 7 are for IS-778.
- Changes to problem detection 8 are for IS-735 and IS-751.
- During the integration process, Note e was added for any error codes from which it was missing.
- Problem detection 8 was deleted during the integration process.

Table 9 HLR AuthenticationRequest Response

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

Problem Detection and Recommended Response from from HLR to VLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
MIN MSID/HLRMismatch	The supplied MobileIdentificationNumber MSID parameter is not in the HLR's range of MINs MSIDs or Directory Numbers (suspect routing error). <i>Note: This response may have been originated by the AC.</i>
ResourceShortage	A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the AC.</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized. <i>Note: This response may have been originated by the AC.</i> <i>Note: It is recommended that a HLR supports AuthenticationRequest transactions.</i>
ParameterError	A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or IMSI 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 Call origination). <i>Note: This response may have been originated by the AC.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the AC.</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., <i>Not used</i>). <i>Note: This response may have been originated by the AC.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
MissingParameter	An optional parameter required by the HLR (AC) was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported (AUTH=1), but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not <u>were</u> received, or SystemAccessType indicated <i>Call origination</i> , but Digits (Dialed) parameter was not received). <i>Note: This response may have been originated by the AC.</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
RETURN RESULT DenyAccess	The supplied MobileIdentificationNumber parameter's AC (HLR) responded that the MIN cannot be Authenticated because of the reason identified by the supplied DenyAccess parameter value. <i>Note: This response may have been originated by the AC.</i> <i>Note: Only RETURN RESULT operations needing clarification have been included.</i>

4.4.4 AC Receiving AuthenticationRequest INVOKE

When an AC receives an AuthenticationRequest INVOKE, it shall perform the following:

- 1 IF the received message can be processed:
 - 1-1 IF the TerminalType (TERMTYP) parameter is not received (i.e., the VLR is using *TSB51* authentication procedures):
 - 1-1-1 IF *TSB51* operation is supported:
 - 1-1-1-1 Execute *TSB51* procedures for AuthenticationRequest (refer to *TIA/EIA TSB51*).
 - 1-1-1-2 Exit this task.
 - 1-1-2 ELSE (*TSB51* operation is not supported):
 - 1-1-2-1 Send a RETURN ERROR with the error code set to *OperationNotSupported*.
 - 1-1-2-2 Exit this task.
 - 1-1-3 ENDIF.
 - 1-2 ELSE (the TerminalType (TERMTYP) parameter is received, i.e., the VLR is using *TIA/EIA-41 IS-41-C* authentication procedures):

Steps 1-2-a through 1-2-a-2 are proposed for R-UIM. So is the change to 1-2-1.

- 1-2-a IF dynamic ESN binding is supported for the MS identified by the received MSID:
 - 1-2-a-1 IF the received ESN is not the current ESN for the MS
 - 1-2-a-1-1 IF the SystemAccessType is *Call origination, Page response, SMS page response, Power down registration, Autonomous registration, or Unspecified*:
 - 1-2-a-1-1-1 Store the received ESN as pending ESN.
 - 1-2-a-1-1-2 Mark the MS as *pending ESN rebinding*.
 - 1-2-a-1-2 ELSE:
 - 1-2-a-1-2-1 Include the DenyAccess parameter set to indicate *MIN or ESN authorization failure*.
 - 1-2-a-1-2-2 Send a RETURN RESULT to the requesting HLR.
 - 1-2-a-1-2-3 Exit this task.
 - 1-2-a-1-3 ENDIF.
 - 1-2-a-2 ENDIF.
- 1-2-1 ELSEIF the MobileIdentificationNumber and ElectronicSerialNumber parameters reported by the MS cannot be validated:
 - 1-2-1-1 Include the DenyAccess parameter set to indicate *MIN or ESN authorization failure*.
 - 1-2-1-2 Send a RETURN RESULT to the requesting HLR.
 - 1-2-1-3 Exit this task.
- 1-2-2 ENDIF.
- 1-2-3 IF the TerminalType (TERMTYP) reported for the MS is not valid:
 - 1-2-3-1 IF access shall be denied to the MS:

UIM Rev. 8.0 (Ballot Version)

- 1-2-3-1-1 Include the DenyAccess parameter set to indicate *TerminalType mismatch*.
- 1-2-3-1-2 Send a RETURN RESULT to the requesting HLR.

Steps 1-2-3-1-b through 1-2-3-1-c are proposed for R-UIM.

- 1-2-3-1-b IF the MS is marked as *pending ESN rebinding*:
- 1-2-3-1-b-1 Delete pending ESN for the MS.
- 1-2-3-1-b-2 Clear the MS's *pending ESN rebinding flag*.
- 1-2-3-1-c ENDIF.
- 1-2-3-1-3 Exit this task.
- 1-2-3-2 ENDIF.
- 1-2-4 ENDIF:

Steps 1-2-d through 1-2-f are proposed for R-UIM.

- 1-2-d IF the MS is marked as *pending ESN rebinding*:
- 1-2-d-1 Select the pending ESN as the ESN to be used as input to all authentication calculations requiring ESN input during this invocation of the "AC Receiving AuthenticationRequest INVOKE" task.
- 1-2-e ELSE:
- 1-2-e-1 Select the current ESN as the ESN to be used as input to all authentication calculations requiring ESN input during this invocation of the "AC Receiving AuthenticationRequest INVOKE" task.
- 1-2-f ENDIF.
- 1-2-5 IF the SystemAccessType is *FlashRequest* AND IF the ConfidentialityModes (CMODES-Actual) parameter was received ~~AND IF the ConfidentialityModes (CMODES Actual) parameter indicates that Signaling Message Encryption is inactive:~~
- 1-2-5-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the AC's database to produce an AuthenticationResponseUniqueChallenge (AUTHU).
- 1-2-5-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.
- 1-2-5-3 Mark the MS *pending Unique Challenge*.
- 1-2-6 ENDIF.
- 1-2-7 IF the SystemAccessType is *Call origination, Page response, SMS page response, Power down registration, or Autonomous registration*:
- 1-2-7-1 IF the received SystemCapabilities (SYSCAP) parameter indicates that the Serving MSC requested authentication parameters for this system access (AUTH=1 in the Overhead Message Train):
- 1-2-7-1-1 IF authentication parameters were not received from the MS:
- 1-2-7-1-1-1 IF access shall be denied to the MS:
- 1-2-7-1-1-1-1 Include the DenyAccess parameter set to indicate *Missing authentication parameters*.
- 1-2-7-1-1-1-2 Send a RETURN RESULT to the requesting HLR.

Steps 1-2-7-1-1-1-g through 1-2-7-1-1-1-h are proposed for R-UIM.

- 1-2-7-1-1-1-g IF the MS is marked as *pending ESN rebinding*:

1-2-7-1-1-1-g-1 Delete pending ESN for the MS.
1-2-7-1-1-1-g-2 Clear the MS's *pending ESN rebinding* flag.
1-2-7-1-1-1-h ENDIF.
 1-2-7-1-1-1-3 Exit this task.
 1-2-7-1-1-2 ENDIF.
1-2-7-1-2 ELSEIF the AuthenticationData parameter was received:
1-2-7-1-2-1 Execute CAVE using the value of the RandomVariable (RAND) parameter, the MS's SharedSecretData (SSD) recorded in the VLR's database, the ESN and the AuthenticationData parameter.
1-2-7-1-3 ELSE:
~~1-2-7-1-2~~ ELSE (authentication parameters were received from the MS):
 1-2-7-1-3-1 Convert values in the Digits (Dialed) parameter (if received) into TBCD encoding.
 1-2-7-1-3-2 Execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the AC's database and the parameters requested by the received SystemAccessType parameter.
1-2-7-1-4 ENDIF.
 1-2-7-1-5 IF the CAVE authentication result and the AuthenticationResponse (AUTHR) received from the MS (see Annex C "Authentication Response Verification") match:

Steps 1-2-7-1-5-i through 1-2-7-1-5-j are proposed for R-UIM.

1-2-7-1-5-i IF the MS is marked as *pending ESN rebinding*:
1-2-7-1-5-i-1 IF the SSD is currently shared for the MS:
1-2-7-1-5-i-1-1 Optionally, include the SSDNotShared parameter and execute the "AC Initiation of an Authentication Directive" task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.
1-2-7-1-5-i-2 ENDIF.
1-2-7-1-5-j ENDIF.
 1-2-7-1-5-1 IF SharedSecretData (SSD) is presently shared with another VLR:

The change to the next step is proposed for R-UIM.

1-2-7-1-5-1-1 Execute the "AC Initiating a COUNT Request" task (see 4.10.1) with the ElectronicSerialNumber parameter set to the current ESN.
 1-2-7-1-5-2 ENDIF.
 1-2-7-1-5-3 IF the stored count and the CallHistoryCount (COUNT) reported by the MS do not significantly match:
 1-2-7-1-5-3-1 IF access shall be denied to the MS:
 1-2-7-1-5-3-1-1 Include the DenyAccess parameter set to indicate *COUNT mismatch*.
 1-2-7-1-5-3-1-2 Send a RETURN RESULT to the requesting HLR.

Steps 1-2-7-1-5-3-1-k through 1-2-7-1-5-3-1-l are proposed for R-UIM.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

1-2-7-1-5-3-1-k IF the MS is marked as *pending ESN rebinding*:
1-2-7-1-5-3-1-k-1 Delete pending ESN for the MS.
1-2-7-1-5-3-1-k-2 Clear the MS's *pending ESN rebinding* flag.
1-2-7-1-5-3-1-l ENDIF.
 1-2-7-1-5-3-1-3 Exit this task.
 1-2-7-1-5-3-2 ENDIF.
 1-2-7-1-5-4 ENDIF.
 1-2-7-1-5-5 IF the SystemAccessType is *Call origination* or *Page response*:
 1-2-7-1-5-5-1 Generate the SignalingMessageEncryptionKey (SMEKEY).
 1-2-7-1-5-5-2 Include the SignalingMessageEncryptionKey (SMEKEY) parameter.
 1-2-7-1-5-5-3 IF the MS supports TDMA:
 1-2-7-1-5-5-3-1 Generate the VoicePrivacyMask (VPMASK).
 1-2-7-1-5-5-3-2 Include the VoicePrivacyMask (VPMASK) parameter.
 1-2-7-1-5-5-4 ELSEIF the MS supports CDMA:
 1-2-7-1-5-5-4-1 Generate the CDMAPrivateLongCodeMask (CDMAPLCM).
 1-2-7-1-5-5-4-2 Include the CDMAPrivateLongCodeMask (CDMAPLCM) parameter.
 1-2-7-1-5-5-5 ENDIF.

The next two steps are for IS-737 (with minor editorial enhancements).

1-2-7-1-5-5-6 Generate the DataKey (DKEY).
1-2-7-1-5-5-7 Include the DataKey (DKEY) parameter.
 1-2-7-1-5-6 ENDIF.
 1-2-7-1-6 ELSE (AuthenticationResponse (AUTHR) reported by the MS is invalid):
 1-2-7-1-6-1 IF access shall be denied to the MS:
 1-2-7-1-6-1-1 Include the DenyAccess parameter set to indicate *AUTHR mismatch*.
 1-2-7-1-6-1-2 Send a RETURN RESULT to the requesting HLR.

Steps 1-2-7-1-6-1-m through 1-2-7-1-6-1-n are proposed for R-UIM.

1-2-7-1-6-1-m IF the MS is marked as *pending ESN rebinding*:
1-2-7-1-6-1-m-1 Delete pending ESN for the MS.
1-2-7-1-6-1-m-2 Clear the MS's *pending ESN rebinding* flag.
1-2-7-1-6-1-n ENDIF.
 1-2-7-1-6-1-3 Exit this task.
 1-2-7-1-6-2 ENDIF.

Steps 1-2-7-1-6-s through 1-2-7-1-6-t are proposed for R-UIM.

1-2-7-1-6-s IF the MS is marked as *pending ESN rebinding*:
1-2-7-1-6-s1 IF the SSD is currently shared for the MS:

1-2-7-1-6-s-1 Optionally, include the SSDNotShared parameter and execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.

1-2-7-1-6-s-2 ENDIF.

1-2-7-1-6-t ENDIF.

1-2-7-1-6-3 IF SharedSecretData (SSD) is presently shared with another VLR:

The change to the next step is proposed for R-UIM.

1-2-7-1-6-3-1 Execute the “AC Initiating a COUNT Request” task (see 4.10.1) with the ElectronicSerialNumber parameter set to the current ESN.

1-2-7-1-6-4 ENDIF.

1-2-7-1-6-5 Validate the CallHistoryCount (COUNT) reported by the MS.

1-2-7-1-6-6 IF the COUNT is not valid:

1-2-7-1-6-6-1 IF access shall be denied to the MS:

1-2-7-1-6-6-1-1 Include the DenyAccess parameter set to indicate COUNT mismatch.

1-2-7-1-6-6-1-2 Send a RETURN RESULT to the requesting HLR.

Steps 1-2-7-1-6-6-1-o through 1-2-7-1-6-6-1-p are proposed for R-UIM.

1-2-7-1-6-6-1-o IF the MS is marked as pending ESN rebinding:

1-2-7-1-6-6-1-o-1 Delete pending ESN for the MS.

1-2-7-1-6-6-1-o-2 Clear the MS’s pending ESN rebinding flag.

1-2-7-1-6-6-1-p ENDIF.

1-2-7-1-6-6-1-3 Exit this task.

1-2-7-1-6-6-2 ENDIF.

1-2-7-1-6-7 ENDIF.

1-2-7-1-7 ENDIF.

~~1-2-7-1-3~~ ~~ENDIF.~~

1-2-7-2 ENDIF.

1-2-8 ENDIF.

1-2-9 IF SharedSecretData (SSD) presently shared with the VLR shall be discarded:

1-2-9-1 Include the SSDNotShared (NOSSD) parameter.

1-2-10 ENDIF.

1-2-11 IF an SSD update shall be initiated:

1-2-11-1 Select a RandomVariableSSD (RANDSSD) and execute CAVE using the value of the MS’s A-key recorded in the AC’s database to produce a pending SSD.

1-2-11-2 Include the RandomVariableSSD (RANDSSD) parameter.

1-2-11-3 Mark the MS pending SSD update.

1-2-11-4 IF AC administrative procedures indicate that the pending SSD shall be shared with the VLR for the SSD update operation AND IF the

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

received SystemCapabilities (SYSCAP) parameter indicates that the VLR is able to execute the CAVE algorithm:

1-2-11-4-1 Include the SharedSecretData (SSD) parameter set to the pending SSD value.

1-2-11-4-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different from the default value:

1-2-11-4-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.

1-2-11-4-3 ENDIF.

~~1-2-11-4 IF AC administrative procedures indicate that the pending SSD shall be shared with the VLR for the SSD update operation:~~

~~1-2-11-4-1 IF the received SystemCapabilities (SYSCAP) parameter indicates that the VLR is able to execute the CAVE algorithm:~~

~~1-2-11-4-1-1 Include the SharedSecretData (SSD) parameter set to the pending SSD value.~~

~~1-2-11-4-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:~~

~~1-2-11-4-1-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.~~

~~1-2-11-4-1-3 ENDIF.~~

~~1-2-11-4-2 ENDIF.~~

1-2-11-5 ELSE (the pending SSD is not shared):

1-2-11-5-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the pending SSD to produce an AuthenticationResponseUniqueChallenge (AUTHU).

1-2-11-5-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.

1-2-11-5-3 Mark the MS *pending Unique Challenge*.

1-2-11-6 ENDIF.

1-2-12 ELSE (SSD update not initiated):

1-2-12-1 IF the SharedSecretData (SSD) shall be shared with the VLR:

1-2-12-1-1 IF the received SystemCapabilities (SYSCAP) indicates the VLR is capable of executing the CAVE algorithm:-

1-2-12-1-1-1 Include the SharedSecretData (SSD) and CallHistoryCount (COUNT) parameters.

1-2-12-1-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:

1-2-12-1-1-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.

1-2-12-1-1-3 ENDIF.

1-2-12-1-2 ENDIF.

1-2-12-2 ENDIF.

1-2-12-3 IF the SystemAccessType is *Unspecified* OR IF the SuspiciousAccess parameter was included in the received AuthenticationRequest INVOKE OR IF local administrative procedures request that a Unique Challenge shall be initiated:

UIM Rev. 8.0 (Ballot Version)

- 1-2-12-3-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the AC's database to produce an AuthenticationResponseUniqueChallenge (AUTHU).
- 1-2-12-3-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.
- 1-2-12-3-3 Mark the MS *pending Unique Challenge*.
- 1-2-12-4 ENDIF.
- 1-2-13 ENDIF.
- 1-2-14 IF local administrative procedures request that a COUNT update shall be initiated:
- 1-2-14-1 Include the UpdateCount (UPDCOUNT) parameter.
- 1-2-14-2 Mark the MS *pending COUNT update*.
- 1-2-15 ENDIF.

Steps 1-2-q through 1-2-r are proposed for R-UIM.

- 1-2-q IF the MS is marked as *pending ESN rebinding*:
- 1-2-q-1 IF the MS is not marked *pending Unique Challenge* OR IF the MS is marked *pending SSD update*:
- 1-2-q-1-1 IF the SSD is currently shared for the MS:
- 1-2-q-1-1-1 Optionally, include the SSDNotShared parameter and execute the "AC Initiation of an Authentication Directive" task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.
- 1-2-q-1-2 ENDIF.
- 1-2-q-1-3 Update the AC record for the MS to indicate that the pending ESN is now the current ESN for the MS.
- 1-2-q-1-4 Clear the MS's *pending ESN rebinding* flag.
- 1-2-q-2 ENDIF.
- 1-2-r ENDIF.
- 1-2-16 Send an AuthenticationRequest RETURN RESULT to the requesting HLR.
- 1-2-17 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*:
- 1-2-17-1 Execute the "AC Awaiting AuthenticationStatusReport INVOKE" task (see 4.5.4).

Steps 1-2-17-2 through 1-2-17-3 are proposed for R-UIM.

- 1-2-17-2 IF the MS is marked as *pending ESN rebinding*:
- 1-2-17-2-1 Delete pending ESN for the MS.
- 1-2-17-2-2 Clear the MS's *pending ESN rebinding* flag.
- 1-2-17-3 ENDIF.
- 1-2-18 ENDIF.
- 1-2-19 Exit this task.
- 1-3 ENDIF.
- 2 ELSE (the received message cannot be processed):
- 2-1 Send a RETURN ERROR to the requesting HLR.

3 ENDIF.
4 Exit this task.

While the dieted table is all new, it has not been underlined since that would make it harder to focus on the substantive changes, which are the changes shown to the contents of the cells.

Changes to the error table are for IS-735, IS-751, IS-778, Miscellaneous 10, the error table diet, and the correction of errors agreed during the integration process.

The sources for technical changes are:

- Changes to problem detection 4 are for IS-735, IS-751, and IS-778.
- Changes to problem detection 5 are for Miscellaneous 10.
- Changes to problem detection 6 are for IS-735 and IS-751.
- Changes to problem detection 7 are for IS-778.
- Note e was deleted during the integration process.
- Problem detection 8 and Note c was deleted during the integration process, so the row associated to the RETURN RESULT was not included.

Table 10 AC AuthenticationRequest Response

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Problem Detection and Recommended Response from AC to HLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
MINMSID/HLRMismatch	The supplied MobileIdentificationNumber MSID parameter is not in the AC's range of MINs MSIDs or Directory Numbers (suspect routing error).
ResourceShortage	A required AC resource (e.g., internal memory record, AC is fully occupied) is temporarily not available (e.g., congestion).
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving AC, or the requesting functional entity is not authorized. <i>Note: It is recommended that an AC supports AuthenticationRequest transactions.</i>
ParameterError	A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or IMSI 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 Call origination). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution.
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used). <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
MissingParameter	An optional parameter required by the AC was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported (AUTH=1), but AuthenticationResponse (AUTHR), ConfidentialityModes (CMODES), CallHistoryCount (COUNT) and/or RandomVariable (RAND) parameters was not were received; or SystemAccessType indicated <i>Call origination</i> , but Digits (Dialed) parameter was not received). <i>Note: Include the .i.FaultyParameter: Parameter Identifier: AuthenticationRequest; in question as the FaultyParameter parameter.</i>

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.5.3 HLR Receiving AuthenticationStatusReport INVOKE

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

- 1 IF the received message can be processed:

Steps 1-m through 1-n are proposed for R-UIM.

1-m IF the MS identified by the received MSID is marked as *pending ESN rebinding*.

1-m-1 Stop timer (ASRRT).

1-m-2 IF the UniqueChallengeReport parameter set to *Unique Challenge successful* was received:

1-m-2-1 IF the MS is currently registered:

1-m-2-1-1 Execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to *Discontinue*.

1-m-2-2 ENDIF.

1-m-2-3 Update the HLR record for the MS to indicate that the pending ESN is now the current ESN for the MS.

1-m-2-4 Clear the MS’s *pending ESN rebinding* flag.

1-m-3 ELSE:

1-m-3-1 Delete pending ESN for the MS.

1-m-3-2 Clear the MS’s *pending ESN rebinding* flag.

1-m-3-3 IF the MS is currently registered:

1-m-3-3-1 Optionally, execute the “HLR Initiating Registration Cancellation” task (see 4.37.1) with the ElectronicSerialNumber parameter set to the current ESN and with the CancellationType parameter set to *ReportInCall*.

1-m-3-4 ENDIF.

1-m-4 ENDIF.

1-n ENDIF.

The following steps are added for the CDMA portion of IS-725-A.

1-a IF the ServiceIndicator parameter set to CDMA OTASP Service value is received:

1-a-1 IF OTASPCallEntry is not found:

1-a-1-1 Send a RETURN ERROR with the Error Code indicating *UnrecognizedMIN*.

1-a-1-2 Exit this task.

1-a-2 ENDIF.

1-b ENDIF.

1-c Include the MSID parameter set to identify the MS to the AC.

1-1 Include the SenderIdentificationNumber set to the identification number of the HLR.

1-2 Relay all other received parameters.

1-3 Start the Authentication Status Report Timer (ASRT).

The following addition is for the CDMA portion of IS-725-A.

- 1-4 Send an AuthenticationStatusReport INVOKE to the AC associated with the MS. (For CDMA OTASP, the AC address is stored in the OTASPCallEntry).
- 1-5 WAIT for an Authentication Status Report response:
- 1-6 WHEN a RETURN RESULT is received:
 - 1-6-1 Stop timer (ASRT).
 - 1-6-2 IF the message can be processed:

The following steps are added for the CDMA portion of IS-725-A.

- 1-6-2-x IF the SharedSecretData parameter is received:
 - 1-6-2-x-1 IF the MIN may be needed for authentication calculations for the MS:
 - 1-6-2-x-1-1 IF the MobileIdentificationNumber parameter was not present as the MSID parameter in the INVOKE AND IF the MIN cannot be derived from the IMSI:
 - 1-6-2-x-1-1-1 Include the MobileIdentificationNumber parameter set to identify the MS to the VLR.
 - 1-6-2-x-1-2 ENDIF.
 - 1-6-2-x-2 ENDIF.
- 1-6-2-y ENDIF.
- 1-6-2-1 Relay all received parameters.
- 1-6-2-2 Send a RETURN RESULT to the requesting VLR.
- 1-6-3 ELSE:
 - 1-6-3-1 Send a RETURN ERROR with the Error Code indicating SystemFailure to the requesting VLR.
- 1-6-4 ENDIF.

The following changes are the result of a WG 3 decision made during the integration process that inconsistencies between the procedures and the error table be resolved by having the HLR relay unchanged any RETURN ERROR received in response to an ASREPORT.

- 1-7-X WHEN a REJECT is received:
 - 1-7-X-1 Stop timer (ASRT).
 - 1-7-X-2 Send a RETURN ERROR to the requesting VLR with the Error Code indicating SystemFailure.
 - 1-7-X-3 Execute the "Local Recovery Procedures" task (see 3.5.1).
 - 1-7-X-4 Exit this task.
- 1-7 WHEN a RETURN ERROR or REJECT is received:
 - 1-7-1 Stop timer (ASRT).
 - 1-7-2 Send a RETURN ERROR to the requesting VLR with the received Error Code (and FaultyParameter parameter, if one has been received).
 - ~~1-7-2~~ CASE Error Code OF:
 - ~~1-7-3~~ ParameterError:
 - ~~1-7-3-1~~ IF the parameter was originated from the initiating functional entity:
 - ~~1-7-3-1-1~~ Send a RETURN ERROR with Error Code set to indicate ParameterError.
 - ~~1-7-3-2~~ ELSE:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

~~1-7-3-2-1 Send a RETURN ERROR with Error Code set to indicate SystemFailure.~~

~~1-7-3-3 ENDIF.~~

~~1-7-4 OperationSequenceProblem:~~

~~1-7-4-1 Send a RETURN ERROR with Error Code set to indicate OperationSequenceProblem.~~

~~1-7-5 DEFAULT:~~

~~1-7-5-1 Send a RETURN ERROR with Error Code set to indicate SystemFailure.~~

~~1-7-6 ENDCASE.~~

1-7-7 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-7-8 Exit this task.

1-8 WHEN timer (ASRT) expires:

1-8-1 Send a RETURN ERROR with the Error Code indicating SystemFailure.

1-8-2 Execute the "Local Recovery Procedures" task (see 3.5.1).

1-8-3 Exit this task.

1-9 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.

Changes to the error table are for IS-751, IS-735, the error table diet, and changes accepted during the integration process. While the dieted table is all new, it has not been underlined since that would make it harder to focus on the substantive changes, which are the changes shown to the contents of the cells.

- A new problem detection has been added for *UnrecognizedMIN* for the CDMA portion of IS-725-A , but during the integration process it was agreed no to add one for *UnrecognizedIMSI*.
- Changes were made to problem detection 4 for IS-735, and IS-751.
- Problem detection 5 was changed for Miscellaneous 10.
- During the integration process, Note e was added for any error codes from which it was missing. It was also added for RETURN RESULT.
- Obvious errors in problem detections 4, 5, and 7 were corrected during the integration process.
- Problem detections 1, 2, and 6 were reworded editorially during the integration process to make the wording specific to problem detections at the HLR. Notes b and e were reworded for the analogous reason.
- Problem detections 8, 9, and 10 were deleted during the integration process.

Table 12 HLR AuthenticationStatusReport Response

UIM Rev. 8.0 (Ballot Version)

Problem Detection and Recommended Response from HLR to VLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
UnrecognizedMIN	<p>The HLR does not have an OTASPCallEntry for the CDMA OTASP transaction.</p> <p><i>Note: This response may have been originated by the AC.</i></p> <p><i>Note: This Error Code is not an appropriate AC (HLR) response to a AuthenticationStatusReport transaction.</i></p>
MINMSID/HLRMismatch	<p>The supplied MobileIdentificationNumber MSID parameter's AC (HLR) responded that the MIN-MSID is not in the HLR's AC (HLR)'s range of MINs MSIDs or directory numbers (suspect routing error).</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p>
ResourceShortage	<p>A required HLR-AC (HLR) resource (e.g., internal memory record, HLR AC (HLR/VLR) is fully occupied) is temporarily not available (e.g., congestion).</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p>
OperationNotSupported	<p>The requested MAP operation is recognized, but not supported by the receiving HLR-AC (HLR/VLR) or the requesting functional entity is not authorized.</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p> <p><i>Note: It is recommended that an HLR-AC (HLR) supports AuthenticationStatusReport transactions.</i></p>
ParameterError	<p>A supplied parameter value has an encoding problem (e.g., the supplied MobileIdentificationNumber or IMSI parameter or Digits (Dialed) parameter digit values do not meet the expected BCD specification).</p> <p><i>Note: This response may have been originated by the AC.</i></p> <p><i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p>
SystemFailure	<p>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.</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p>
UnrecognizedParameterValue	<p>A supplied parameter value is unrecognized or has nonstandard values (e.g., Not used, the SystemCapabilities (SYSCAP) parameter indicated authentication is not supported (AUTH is 0), but this AuthenticationStatusReport was received).</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p> <p><i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p>
MissingParameter	<p>An optional parameter required by the AC (HLR) was expected, but not received (e.g., a SSD update process was in-progress and a SSDUpdateReport-ReportType set to SSD update successful-SSD update successful was received, but the expected UniqueChallengeReport-second ReportType parameter indicating the CallHistoryCount's (COUNT's) incrementing status (e.g., COUNT update successful, COUNT mismatch, Count update no response etc.) was not received).</p> <p><i>Note: This response may have been originated by the AC (HLR).</i></p> <p><i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p>

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

<p>RETURN RESULT DenyAccess</p>	<p>The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MIN MSID is within the range of the AC (HLR), but the MIN MSID is not presently assigned to a subscriber. DenyAccess parameter value is Unspecified.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the supplied ElectronicSerialNumber parameter does not match the ESN in the MIN's MS's record. DenyAccess parameter value is Unspecified.</p> <p>An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the MIN MS is either a DelinquentAccount, StolenUnit, DuplicateUnit or Unspecified. DenyAccess parameter value is Unspecified.</p> <p><u>Note: This response may have been originated by the AC.</u></p> <p><i>Note: Only RETURN RESULT operations needing clarification have been included.</i></p>
--	---

UIM Rev. 8.0 (Ballot Version)

4.5.4 AC Awaiting AuthenticationStatusReport INVOKE

When an AC requests the VLR to perform authentication operations that require the VLR to report the outcome, the AC shall perform the following:

- 1 Start the Authentication Status Report Response Timer (ASRRT).
- 2 WAIT for an AuthenticationStatusReport INVOKE:
- 3 WHEN an AuthenticationStatusReport INVOKE is received:
 - 3-1 Stop timer (ASRRT).
 - 3-2 IF the received message can be processed:

Steps 3-2-m through 3-2-n are proposed for R-UIM.

- 3-2-m IF the MS identified by the received MSID is marked as *pending ESN rebinding*.
- 3-2-m-1 IF the UniqueChallengeReport parameter set to *Unique Challenge successful* was received:
 - 3-2-m-1-1 IF the SSD is currently shared for the MS:
 - 3-2-m-1-1-1 Include the SSDNotShared parameter and execute the “AC Initiation of an Authentication Directive” task (see 4.1.1) with the ElectronicSerialNumber parameter set to the current ESN, to end SSD sharing.
 - 3-2-m-1-2 ENDIF.
 - 3-2-m-1-3 Update the HLR record for the MS to indicate that the pending ESN is now the current ESN for the MS.
 - 3-2-m-1-4 Clear the MS’s *pending ESN rebinding* flag.
 - 3-2-m-2 ENDIF.
 - 3-2-n ENDIF.
 - 3-2-1 Clear all the MS’s pending operation flags.

The following steps are added for the CDMA portion of IS-725-A.

- 3-2-a IF the ServiceIndicator parameter, set to either the CDMA OTASP Service or the CDMA OTAPA Service value, is received:
 - 3-2-a-1 Indicate *success* and relay received parameters to the calling task.
 - 3-2-b ENDIF.
 - 3-2-2 IF the INVOKE reports that SSD updating has been successful:

The following deletion and additions are for the CDMA portion of IS-725-A.

- ~~3-2-2-1 Update the AC’s database to indicate that the pending SharedSecretData (SSD) value is now the value used by the MS.~~
- 3-2-2-1 IF the ServiceIndicator parameter set to either the CDMA OTASP Service value or the CDMA OTAPA Service value is received:
 - 3-2-2-1-1 IF an OTASPCallEntry exists AND IF the OTASPCallEntry contains an A-key:
 - 3-2-2-1-1-1 Mark the pending SSD in the OTASPCallEntry as valid SSD.

3-2-2-1-2 ELSE (OTASPCallEntry does not exist¹ OR OTASPCallEntry does not contain an A-key):

3-2-2-1-2-1 Update the AC's database to indicate that the pending SharedSecretData (SSD) value is now the value used by the MS.

3-2-2-1-3 ENDIF.

3-2-2-2 ELSE:

3-2-2-2-1 Update the AC's database to indicate that the pending SharedSecretData (SSD) value is now the value used by the MS.

3-2-2-3 ENDIF.

3-2-3 ENDIF.

3-2-4 IF the INVOKE reports that COUNT updating has been successful:

3-2-4-1 Increment the value of COUNT in the AC's database.

3-2-5 ENDIF.

The following addition is for the TDMA portion of IS-725-A.

Integrators comment:

This addition is made, without the word "TDMA," in a portion of IS-725-A that was TDMA specific, implicitly limiting its scope to TDMA. That limitation must be made explicit in the integrated text. The word "TDMA" was added to step 3-2-6 as part of the integration process to accomplish this.

3-2-6 IF an authentication or TDMA re-authentication failure has been detected:

3-2-6-1 Execute recovery procedures according to the AC's internal algorithm.

3-2-7 ENDIF.

3-2-8 IF local administrative procedures request that service shall be denied:

3-2-8-1 Include the DenyAccess parameter:

3-2-9 ENDIF.

3-2-10 IF SharedSecretData (SSD) presently shared with the VLR shall be discarded:

3-2-10-1 Include the SSDNotShared (NOSSD) parameter.

3-2-11 ENDIF.

3-2-12 IF an SSD update shall be initiated:

3-2-12-1 Select a RandomVariableSSD (RANDSSD) and execute CAVE using the value of the MS's A-key recorded in the AC's database to produce a pending SharedSecretData (SSD).

3-2-12-2 Include the RandomVariableSSD (RANDSSD) parameter.

3-2-12-3 Mark the MS pending SSD update.

The changes to the block of steps beginning with 3-2-12-4 are for IS-778, except that the last condition added to step 3-2-12-4 is added for the CDMA portion of IS-725-A and that steps 3-2-12-4-2 through 3-2-12-4-3 have be replaced based on an accepted LG Sansys contribution

3-2-12-4 IF AC administrative procedures indicate that the pending SharedSecretData (SSD) shall be shared with the VLR for the SSD update operation AND IF the VLR's SystemCapabilities indicates that

¹ At this point of processing an OTASPCallEntry will always exist for OTASP but it might not exist for OTAPA.

the VLR is able to execute the CAVE algorithm AND IF the ServiceIndicator parameter, set to either the CDMA OTASP Service or the CDMA OTAPA Service value, is not received:

3-2-12-4-1 Include the SharedSecretData (SSD) parameter set to the pending SSD value.

~~3-2-12-4-2 IF the AuthenticationAlgorithmVersion (AAV) parameter is received:~~

~~3-2-12-4-2-1 Store the AuthenticationAlgorithmVersion (AAV) value.~~

~~3-2-12-4-3 ENDIF.~~

3-2-12-4-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:

3-2-12-4-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.

3-2-12-4-3 ENDIF.

~~3-2-12-4 IF AC administrative procedures indicate that the pending SharedSecretData (SSD) shall be shared with the VLR for the SSD update operation:~~

~~3-2-12-4-1 IF the VLR's SystemCapabilities indicates that the VLR is able to execute the CAVE algorithm:~~

~~3-2-12-4-1-1 Include the SharedSecretData (SSD) parameter set to the pending SSD value.~~

~~3-2-12-4-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter is received:~~

~~3-2-12-4-1-2-1 Store the AuthenticationAlgorithmVersion (AAV) value.~~

~~3-2-12-4-1-3 ENDIF.~~

~~3-2-12-4-2 ENDIF.~~

3-2-12-5 ELSE (pending SharedSecretData (SSD) is not to be shared:

3-2-12-5-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the pending SSD to produce an AuthenticationResponseUniqueChallenge (AUTHU).

3-2-12-5-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.

3-2-12-5-3 Mark the MS *pending Unique Challenge*.

3-2-12-6 ENDIF.

3-2-13 ELSE (SSD update not initiated):

3-2-13-1 IF the SharedSecretData (SSD) shall be shared with the VLR:

3-2-13-1-1 IF the VLR's SystemCapabilities indicates the VLR is capable of executing the CAVE algorithm:

3-2-13-1-1-1 Include the SharedSecretData (SSD) and CallHistoryCount (COUNT) parameters.

The replacement of steps 3-2-13-1-1-2 through 3-2-13-1-1-3 is based on an accepted LG Sansys comment.

~~3-2-13-1-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter is received:~~

~~3-2-13-1-1-2-1 Store the AuthenticationAlgorithmVersion (AAV) value.~~

~~3-2-13-1-1-3 ENDIF.~~

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

- 3-2-13-1-1-2 IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:
- 3-2-13-1-1-2-1 Include the AuthenticationAlgorithmVersion (AAV) parameter.
- 3-2-13-1-1-3 ENDIF.
- 3-2-13-1-2 ENDIF.
- 3-2-13-2 ENDIF.
- 3-2-13-3 IF a Unique Challenge shall be initiated:
- 3-2-13-3-1 Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the MS's SharedSecretData (SSD) recorded in the AC's database to produce an AuthenticationResponseUniqueChallenge (AUTHU).
- 3-2-13-3-2 Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUnique Challenge(AUTHU) parameters.
- 3-2-13-3-3 Mark the MS *pending Unique Challenge*.
- 3-2-13-4 ENDIF.
- 3-2-14 ENDIF.
- 3-2-15 IF a COUNT update shall be initiated:
- 3-2-15-1 Include the UpdateCount (UPDCOUNT) parameter.
- 3-2-15-2 Mark the MS *pending COUNT update*.
- 3-2-16 ENDIF.
- 3-2-17 Send an AuthenticationStatusReport RETURN RESULT to the requesting HLR.
- 3-2-18 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*:
- 3-2-18-1 Execute the "AC Awaiting AuthenticationStatusReport INVOKE" task (see 4.5.4).
- 3-2-19 ENDIF.
- 3-2-20 Exit this task.
- 3-3 ELSE (the message cannot be processed):
- 3-3-1 Send a RETURN ERROR to the requesting HLR.

The following steps are added for the CDMA portion of IS-725-A.

- 3-3-a IF the invoking task is related to CDMA OTASP or CDMA OTAPA:
- 3-3-a-1 Indicate *failure* to the calling task.
- 3-3-b ENDIF.
- 3-3-2 IF the MS is marked *pending SSD update*:
- 3-3-2-1 Remove the pending SharedSecretData (SSD) from the AC's database.
- 3-3-3 ENDIF.
- 3-3-4 Clear all the MS's pending operation flags.
- 3-3-5 Execute the "Local Recovery Procedures" task (see 3.5.1).
- 3-3-6 Exit this task.
- 3-4 ENDIF.
- 4 WHEN timer (ASRRT) expires:
- 4-1 IF the MS is marked *pending SSD update*:

UIM Rev. 8.0 (Ballot Version)

- 4-1-1 Remove the pending SharedSecretData (SSD) from the AC's database.
- 4-2 ENDIF.
- 4-3 Clear all the MS's pending operation flags.
- 4-4 Execute the "Local Recovery Procedures" task (see 3.5.1).

The following steps are added for the CDMA portion of IS-725-A.

- 4-5 IF the invoking task is related to CDMA OTASP or CDMA OTAPA:
- 4-5-1 Indicate *failure* to the calling task.
- 4-6 ENDIF.
- 5 ENDWAIT.
- 6 Exit this task.

Changes to the error table are for IS-751, IS-735, the error table diet, and changes accepted during the integration process. While the dieted table is all new, it has not been underlined since that would make it harder to focus on the substantive changes, which are the changes shown to the contents of the cells.

- A new problem detection has been added for *UnrecognizedMIN* for the CDMA portion of IS-725-A , but during the integration process it was agreed no to add one for *UnrecognizedIMSI*.
- Changes were made to problem detection 4 for IS-735, and IS-751.
- Problem detection 5 was changed for Miscellaneous 10.
- Note e was deleted during the integration process.
- Obvious errors in problem detections 4, 5, and 7 were corrected during the integration process.
- Problem detections 1, 2, 6, 8, 9, and 10 were reworded editorially during the integration process to make the wording specific to problem detections at the AC. Note b was reworded for the analogous reason.
- Problem detections 8, 9, and 10 were footnoted during the integration process to indicate that their use during CDMA OTASP is inappropriate (since in that case the MobileIdentificationNumber parameter carries an Activation_MIN unrelated to the MS's identity).

One change is proposed to the error table for R-UIM.

Table 13 AC AuthenticationStatusReport Response

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

UIM Rev. 8.0 (Ballot Version)

Problem Detection and Recommended Response from AC to HLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
UnrecognizedMIN	The <u>ServiceIndicator</u> parameter is received and the AC does not have an <u>OTASPCallEntry</u> for the CDMA OTASP transaction. <i>Note: This Error Code is not an appropriate AC (HLR) response to a <u>AuthenticationStatusReport</u> transaction.</i>
MINMSID/HLRMismatch	The supplied <u>MobileIdentificationNumber</u> <u>MSID</u> parameter's AC (HLR) responded that the <u>MIN MSID</u> is not in the AC's (HLR)'s range of <u>MINs MSIDs</u> or directory numbers (suspect routing error). <i>Note: This response may have been originated by the AC (HLR).</i>
ResourceShortage	A required AC (HLR) resource (e.g., internal memory record, AC (HLR/VLR) is fully occupied) is temporarily not available (e.g., congestion). <i>Note: This response may have been originated by the AC (HLR).</i>
OperationNotSupported	The requested MAP operation is recognized, but not supported by the receiving AC (HLR/VLR) or the requesting functional entity is not authorized. <i>Note: This response may have been originated by the AC (HLR).</i> <i>Note: It is recommended that an AC (HLR) supports <u>AuthenticationStatusReport</u> transactions.</i>
ParameterError	A supplied parameter value an encoding problem (e.g., the supplied <u>MobileIdentificationNumber</u> or <u>IMSI</u> parameter or <u>Digits (Dialed)</u> parameter-digit values do not meet the expected BCD specification). <i>Note: Include the Parameter Identifier in question as the <u>FaultyParameter</u> parameter.</i>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution. <i>Note: This response may have been originated by the AC (HLR).</i>
UnrecognizedParameterValue	A supplied parameter value is unrecognized or has nonstandard values (e.g., <i>Not used</i> , the <u>SystemCapabilities (SYSCAP)</u> parameter indicated authentication is not supported (AUTH is 0), but this <u>AuthenticationStatusReport</u> was received). <i>Note: This response may have been originated by the AC (HLR).</i> <i>Note: Include the Parameter Identifier in question as the <u>FaultyParameter</u> parameter.</i>

<p>MissingParameter</p>	<p>An optional parameter required by the AC (HLR) was expected, but not received (e.g., a SSD update process was in-progress and a SSDUpdateReport-ReportType set to SSD update successful-SSD update successful was received, but the expected UniqueChallengeReport-second ReportType parameter indicating the CallHistoryCount's (COUNT's) incrementing status (e.g., COUNT update successful, COUNT mismatch, Count update no response) was not received). <i>Note: This response may have been originated by the AC (HLR).</i> <i>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</i></p>
<p>RETURN RESULT DenyAccess</p>	<p>The supplied MobileIdentificationNumber or IMSI parameter's AC (HLR) responded that the MIN MSID is within the range of the AC (HLR), but the MIN MSID is not presently assigned to a subscriber. DenyAccess parameter value is <i>Unspecified</i>.¹ An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the supplied ElectronicSerialNumber parameter does not match the ESN in the MIN's MS's record <u>and the MS is not marked pending ESN rebinding</u>. DenyAccess parameter value is <i>Unspecified</i>.² An AC (HLR) record exists for the supplied MobileIdentificationNumber or IMSI parameter, but the MIN MS is either a DelinquentAccount, StolenUnit, DuplicateUnit or Unspecified. DenyAccess parameter value is <i>Unspecified</i>.³ <i>Note: Only RETURN RESULT operations needing clarification have been included.</i></p>

¹This problem detection is not appropriate for use during a CDMA OTASP session.

²This problem detection is not appropriate for use during a CDMA OTASP session.

³This problem detection is not appropriate for use during a CDMA OTASP session.

UIM Rev. 8.0 (Ballot Version)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60