

3GPP2 X.S0003-0 v1.0

Version Date: January, 2005



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

## *One-Way Roaming from X.S0004 to GSM*

**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 [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*

# Revision History

Revision	Date	Remarks
X.S0003-0 v1.0	January, 2005	Initial Publication

# One-Way Roaming from X.S0004 to GSM

## Contents

---

Revision History .....	ii
List of Tables .....	iv
List of Figures .....	v
<b>1 PURPOSE AND SCOPE .....</b>	<b>1</b>
1.1 References.....	1
1.1.1 Normative References .....	1
1.1.2 Informative References.....	1
1.2 Definitions .....	1
1.3 Assumptions.....	1
<b>2 Introduction .....</b>	<b>4</b>
<b>3 TIA/EIA-41 Chapter-3 .....</b>	<b>5</b>
3.Y TIA/EIA-41 Roaming to GSM Systems.....	5
3.Y.1 Successful Authentication on Initial Access in GSM System.....	6
3.Y.2 Authentication Failure on Initial Access in GSM System.....	8
3.Y.3 Authentication Failure on Initial Access in GSM System – Authentication Failure Message Not Supported .....	10
3.Y.4 GSM System Request for Additional Triplets .....	12
<b>4 TIA/EIA-41 Chapter-5 (Signaling Protocols) .....</b>	<b>13</b>
4.1 Operation Definitions .....	13
4.1.1 AuthenticationRequest.....	13
4.2 MAP Parameters .....	16
4.2.1 Parameter Definitions .....	16
4.2.1.1 SystemAccessType.....	16
<b>5 Signaling Procedures .....</b>	<b>18</b>
5.1 Authentication Request.....	18
5.1.1 HLR Receiving AuthenticationRequest INVOKE.....	18
5.1.2 AC Receiving AuthenticationRequest INVOKE .....	22

## List of Tables

---

Table 1:	HLR AuthenticationRequest Response.....	20
Table 2:	AC AuthenticationRequest Response.....	27

## List of Figures

---

Figure 1	Successful Authentication on Initial Access in GSM System .....	6
Figure 2	Authentication Failure on Initial Access in GSM System .....	8
Figure 3	Authentication Failure on Initial Access in GSM System – Authentication Failure Message Not Supported .....	10
Figure 4	GSM System Request for Additional Triplets .....	12

# 1 PURPOSE AND SCOPE

---

This document provides recommended *ANS/TIA/EIA-41-D* enhancements required to support *TIA/EIA-41* SIM (Subscription Identification Module) roaming one-way into *GSM* serving areas (without modification to the *GSM* serving network).

## 1.1 References

---

### 1.1.1 Normative References

---

[*ANSI-41*]      *ANSI/TIA/EIA-41-D* Cellular Radiotelecommunications Intersystem Operations 1998.

### 1.1.2 Informative References

---

[*TSB100*]      *TSB100-A* TR-45 Wireless Network Reference Model (NRM); April 2001.

## 1.2 Definitions

---

AC	Authentication Center
GSM	Global System for Mobile Communications
CAVE	Cellular Authentication and Voice Encryption
HLR	Home Location Register
IIF	Interoperability and Interworking Function
KC	Cipher key for voice encryption.
ME	Mobile Equipment
SIM	Subscription Identification Module
SSD	Shared Secret Data
UIM	User Identity Module
XRES	Expected Response.

## 1.3 Assumptions

---

The following assumptions are applicable to this document, they are:

1. General TIA/EIA-41 Authentication:
  - i. “A-key” shall be stored in both the UIM and in the *TIA/EIA-41* AC.
  - ii. “SSD” shall be retained in both the UIM and in the *TIA/EIA-41* HLR-AC.
  - iii. “SSD-A” and or “SSD-B” may be retained in the IIF.

- iv. “SSD” shall not be updated when the UIM is in the GSM roaming state:
    - » The AC cannot update SSD when the subscriber is served by a GSM system. From an TIA/EIA-41 perspective, the serving system can only perform authentication on a traffic channel.
    - » The AC cannot update COUNT when the subscriber is served by a GSM system.
  - v. “SSD” shall be available in the UIM when the UIM is in the GSM roaming state.
2. GSM Network:
- i. This document shall not impact the GSM infrastructure.
3. TIA/EIA-41 HLR-AC:
- i. This document shall not impact the TIA/EIA-41 HLR-AC security algorithms (i.e. CAVE).
  - ii. The TIA/EIA-41 Home System has enhanced authentication capabilities to support roaming of subscribers to GSM systems. Subscribers may be using multi-mode mobile stations capable of roaming into a GSM system or UIMs that are inserted into GSM terminal equipment.
  - iii. The TIA/EIA-41 home system should update SSD when the MS returns to an TIA/EIA-41 system:
4. IIF:
- i. Service Orders shall not apply to the IIF.
  - ii. A temporary IIF data base is required for each UIM in the GSM roaming state.
  - iii. Subscriber specific data is not provisioned or stored in the IIF.
  - iv. The IIF functions as a VLR in its interaction with the TIA/EIA-41 Home System:
    - » The TIA/EIA-41 AC shares SSD with the IIF for subscribers roaming in a GSM network. The IIF generates the triplets (RAND, XRES, KC) used by the GSM system.
    - » After the subscriber is registered in a GSM system, the IIF reports authentication failures to the TIA/EIA-41 system using the AuthenticationFailureReport operation.
    - » SSD is shared with the IIF until registration in the GSM system is canceled. The TIA/EIA-41 AC/HLR can cancel registration using the RegistrationCancellation operation.
    - » The IIF shall remove the subscriber’s SSD when registration in the GSM system is canceled.
  - v. The IIF functions as a GSM HLR/AC in its interactions with the GSM system:
    - » The IIF provides the GSM triplets needed for authentication and privacy in the GSM system.
    - » The IIF generates triplets using the SSD value stored in the UIM (or multi-mode MS).
  - vi. The IIF shall prevent disclosure of SSD values received from TIA/EIA-41 systems:
    - » The IIF shall provide a secure method of storing SSD values received from TIA/EIA-41 systems.

- 1                   » The SSD values shall not be disclosed nor transmitted to any other network entity.  
2  
3       vii. The IIF shall be able to request the MS's ESN in the AuthenticationRequest INVOKE  
4           sent to the home TIA/EIA-41 system:  
5  
6           » As an optimization, the AC can include the MS's ESN in the AuthenticationRequest  
7           RETURN RESULT sent to the IIF. This avoids two additional messages to request and  
8           provide the ESN. (Note, a similar mechanism could be used to retrieve the ESN if the  
9           MS roams into a GSM system that does not use authentication).  
10  
11       5. UIM:  
12  
13       i. The UIM shall retain independent dual profiles (i.e., *TIA/EIA-41* and *GSM*).  
14  
15       ii. The UIM may retain common *TIA/EIA-41* and *GSM* information required for  
16           operation.  
17  
18       iii. The UIM receiving a GSM specific authentication operation from the ME, while in the  
19           GSM roaming state, shall appropriately generate GSM security parameters.  
20  
21       iv. A valid SSD value must be generated in the UIM (or multi-mode MS) before the  
22           subscriber can roam into a GSM system.  
23  
24       v. When roaming in a GSM system, the UIM uses the "authentication" algorithm  
25           supported by the IIF:  
26  
27           » When roaming in a GSM system, the UIM (or multi-mode MS) must use an  
28           authentication algorithm supported by the IIF for the computation of the cipher key  
29           and the response to the random challenge.  
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 INTRODUCTION

---

This recommendation proposes that the Interoperability and Interworking Function (IIF) for one-way roaming from an *TIA/EIA-41* to *GSM* systems operate as a VLR (that can share SSD) in its interaction with an *TIA/EIA-41* home system. SSD is shared with the IIF. The IIF computes the random challenge for authentication and the expected MS response. From an *TIA/EIA-41* home system perspective, the IIF performs authentication and only reports authentication failures. The *TIA/EIA-41* AC will never generate RANDU and AUTHU. The IIF functions very much like a VLR that can share SSD and can only perform authentication on a traffic channel. However, the SSD stored in a UIM (or multi-mode MS) cannot be updated while the MS is roaming in a *GSM* system. Additionally, the *TIA/EIA-41* AC has limited control of serving system operation when an authentication failure is detected (e.g., registration cannot be canceled).

The IIF functions as a *GSM* AC/HLR in its interaction with the serving *GSM* system. The IIF uses the MS's SSD to compute the *GSM* triplets needed by the serving *GSM* system. The SSD enables the IIF and UIM to provide the required security. The authentication algorithm used by the UIM (or Multi-mode MS) to compute the *GSM* random challenge response (and the associated cipher key) must be an algorithm supported by the IIF.

This recommendation also proposes the use of existing authentication operations for one-way roaming from *TIA/EIA-41* to *GSM* systems. No new operations or sequence of operations is required. This simplifies intersystem operations and reduces the time needed to authenticate the MS on an initial access. (Note, there are optimizations possible that would reduce the number of intersystem operations used for authentication and registration, but they are not considered in this recommendation).

# 3 TIA/EIA-41 CHAPTER-3

---

This document provides recommended *ANS/TIA/EIA-41-D* enhancements required to support *TIA/EIA-41* SIM (Subscription Identification Module) roaming one-way into *GSM* serving areas (without modification to the *GSM* serving network).

## 3.Y TIA/EIA-41 Roaming to GSM Systems

---

(new Section for TIA/EIA-41.3-D)

This section depicts the interactions between network entities in the situations related to one way roaming from TIA/EIA-41 to GSM systems.

These scenarios are for illustrative purposes only.

### 3.Y.1 Successful Authentication on Initial Access in GSM System

This scenario illustrates the successful authentication of an MS on the initial MS access is a GSM system.

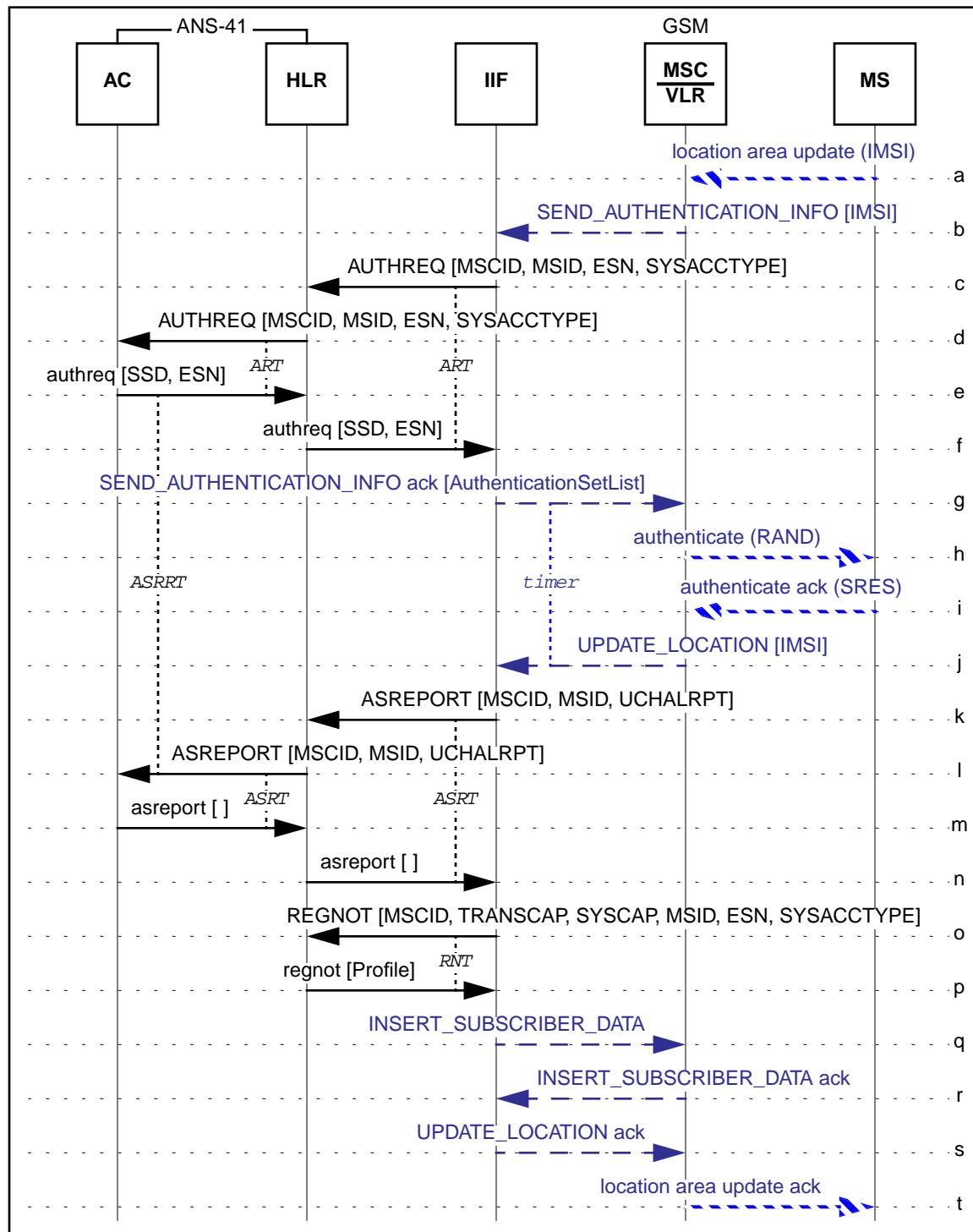


Figure 1 Successful Authentication on Initial Access in GSM System

The MS determines that a new serving system has been entered. The MS registers at the new GSM

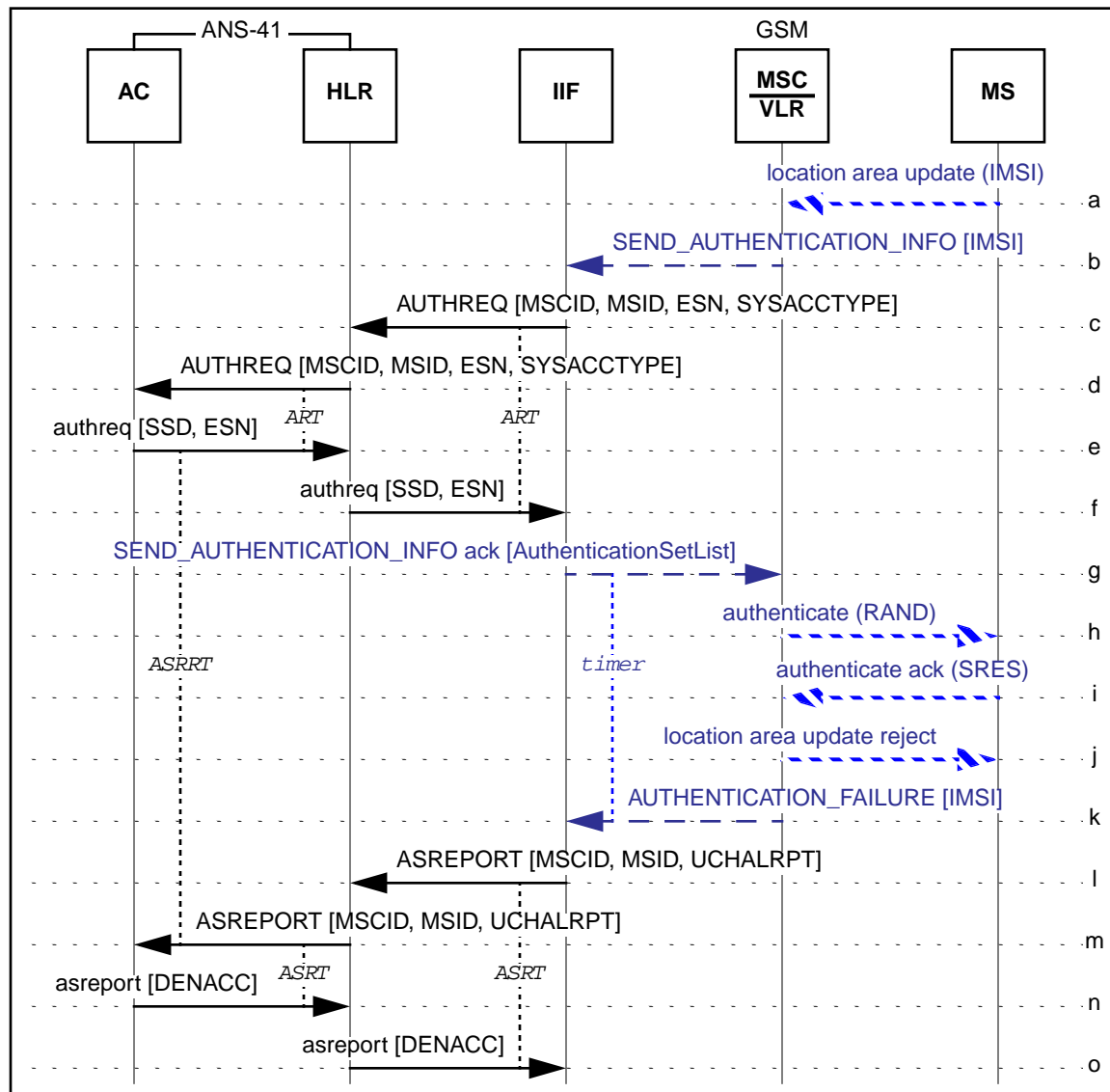
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 serving system and provides its IMSI.  
2

- 3 a. The MS determines that a new serving system has been entered. The MS registers at the new  
4 GSM serving system and provides its IMSI.
- 5 b. The GSM serving system sends a SEND\_AUTHENTICATION\_INFO to the IIF.  
6
- 7 c. The IIF sends an AUTHREQ to the HLR associated with the MS. The MSCID parameter  
8 identifies the IIF. The ESN parameter is set to a default value of all-zeroes. The  
9 SYSACCTYPE parameter is set to indicate *GSM system access*.  
10
- 11 d. The HLR forwards the AUTHREQ to the AC.  
12
- 13 e. The AC determines that the subscriber is roaming in a GSM system. The AC includes the SSD  
14 parameter in the authreq sent to the HLR. The ESN parameter is set to the indicated MS's  
15 ESN.
- 16 f. The HLR forwards the authreq to the IIF.  
17
- 18 g. The IIF stores the received SSD and ESN. The IIF computes one or more groups of GSM  
19 triplets using the subscriber's SSD. The IIF sends a SEND\_AUTHENTICATION\_INFO ack  
20 to the GSM system and includes the groups of triplets.  
21
- 22 h. The GSM system issues a random challenge to the MS.  
23
- 24 i. The MS responds to the challenge with the computed response.  
25
- 26 j. The GSM system compares the response received from the MS with the expected response. In  
27 this scenario, the response is equal to the expected response. The GSM system sends a  
28 UPDATE\_LOCATION to the IIF. The IMSI is used to identify the MS.
- 29 k. The IIF sends an ASREPORT to the HLR associated with the MS. The UCHALRPT  
30 parameter is set to indicate *Unique Challenge successful*.  
31
- 32 l. The HLR forwards the ASREPORT to the AC.  
33
- 34 m. The AC sends an asreport to the HLR.  
35
- 36 n. The HLR forwards the asreport to the IIF.  
37
- 38 o. The IIF sends a REGNOT to the HLR.  
39
- 40 p. The HLR sends a regnot to the IIF with the subscriber's service profile.  
41
- 42 q. The IIF sends an INSERT\_SUBSCRIBER\_DATA to the GSM system.  
43
- 44 r. The GSM system sends an INSERT\_SUBSCRIBER\_DATA ack to the IIF.  
45
- 46 s. The IIF sends an UPDATE\_LOCATION ack to the GSM system.  
47
- 48 t. The GSM system sends a location area update ack to the MS.  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

### 3.Y.2 Authentication Failure on Initial Access in GSM System

This scenario illustrates an authentication failure on the initial MS access in a GSM system. The GSM system reports the authentication failure to the IIF.



**Figure 2 Authentication Failure on Initial Access in GSM System**

- a-i. Same as Scenario 3.Y.1, Steps a-i.
- j. The GSM system compares the response received from the MS with the expected response. In this scenario, the response does not equal to the expected response. The GSM system sends a location area update reject to the MS.
- k. The GSM system sends an authentication failure indication to the IIF. The subscriber's IMSI is used to identify the MS.
- l. The IIF sends an ASREPORT to the HLR associated with the MS. The UCHALRPT parameter is set to indicate *Unique Challenge failed*.
- m. The HLR forwards the ASREPORT to the AC.

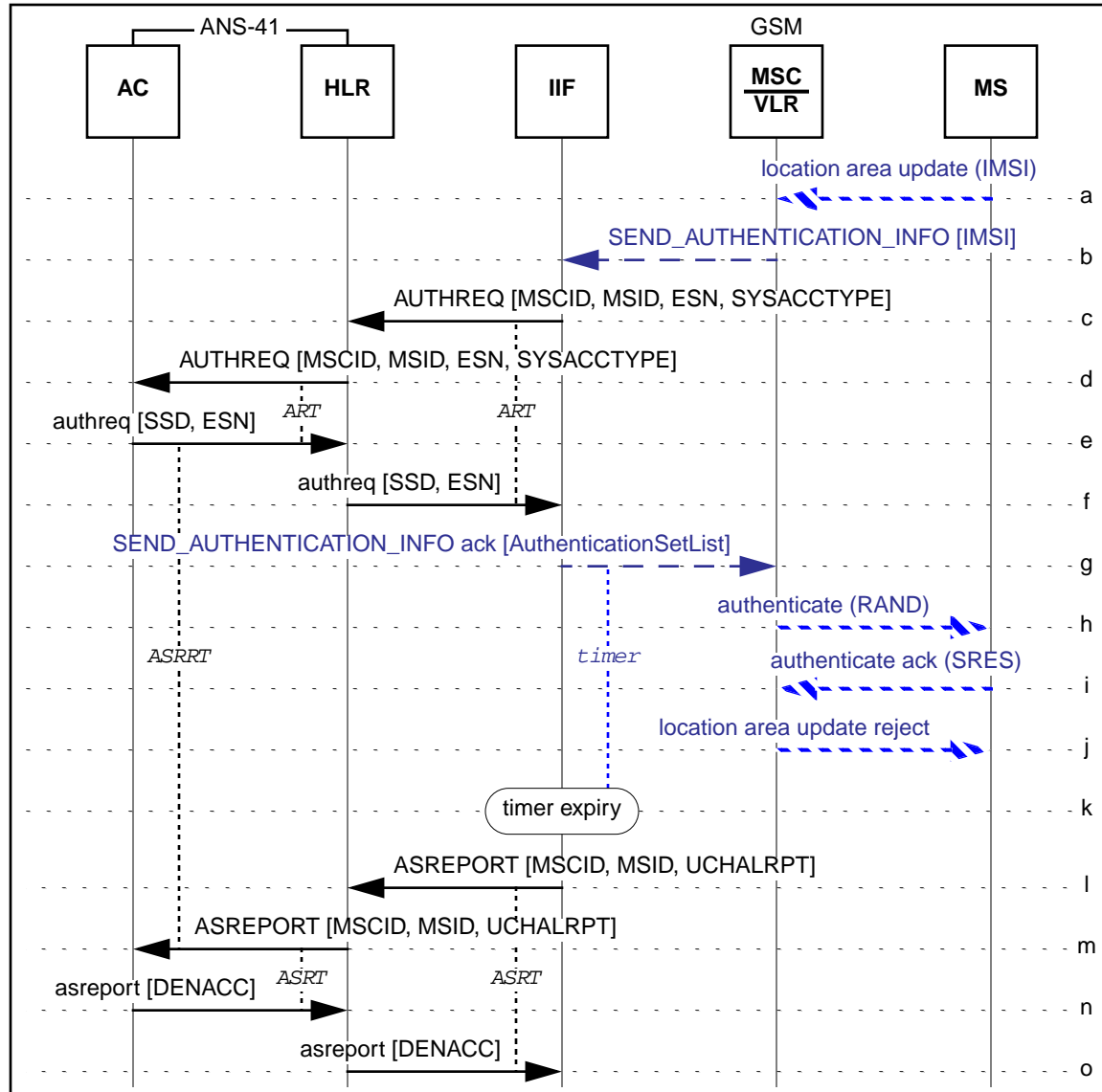
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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

- n. The AC includes the DENACC parameter and sends an asreport to the HLR.
- o. The HLR forwards the asreport to the IIF. The IIF removes the SSD, ESN and other information stored for the MS.

### 3.Y.3 Authentication Failure on Initial Access in GSM System — Authentication Failure Message Not Supported

This scenario illustrates an authentication failure on the initial MS access in a GSM system. The GSM system does not report the authentication failure to the IIF.



**Figure 3 Authentication Failure on Initial Access in GSM System – Authentication Failure**

- a-j. Same as Scenario 3.Y.2, Steps a-j.
- k. An IIF timer expires when no message for the MS is received from the GSM system.
- l. The IIF sends an ASREPORT to the HLR associated with the MS. The UCHALRPT parameter is set to indicate *Unique Challenge failed*.
- m. The HLR forwards the ASREPORT to the AC.
- n. The AC includes the DENACC parameter and sends an asreport to the HLR.

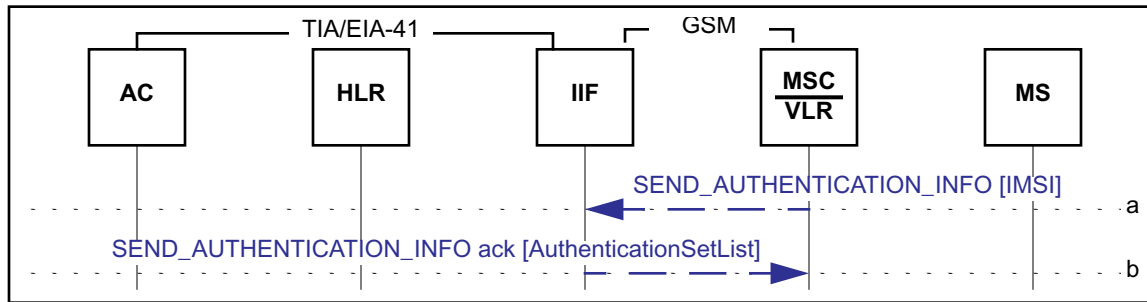
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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

- o. The HLR forwards the asreport to the IIF. The IIF removes the SSD, ESN and other information stored for the MS.

### 3.Y.4 GSM System Request for Additional Triplets

This scenario illustrates a GSM system requesting additional triplets after the MS is registered in the serving GSM system.



**Figure 4 GSM System Request for Additional Triplets**

- a. The GSM system determines that additional triplets are required and sends a SEND\_AUTHENTICATION\_INFO to the IIF. The IMSI identifies the subscriber.
- b. The IIF computes one or more groups of triplets and includes them in the response to the GSM system. (Note, the IIF may have pre-computed triplets for the MS that it sends to the GSM system).

# 4 TIA/EIA-41 CHAPTER-5 (SIGNALING PROTOCOLS)

## 4.1 Operation Definitions

(TIA/EIA-41-D, page 5-27)

### 4.1.1 AuthenticationRequest

(TIA/EIA-41-D, page 5-34)

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

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

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

Authentication may be initiated under the following circumstances:

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

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

No changes have been made to the AuthenticationRequest INVOKE parameters

Note 1

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

AuthenticationRequest RETURN RESULT Parameters				
Field	Value	Type	Reference	Notes
Identifier	SET [NATIONAL 18]	M	<a href="#">520-1.3.2.2</a>	
Length	variable octets	M	<a href="#">520-1.3.2.2</a>	
Contents				
AnalogRedirectRecord		O	<a href="#">3.8</a>	j
AuthenticationAlgorithmVersion		O	<a href="#">3.11</a>	a
AuthenticationResponseUniqueChallenge		O	<a href="#">3.17</a>	b
CallHistoryCount		O	<a href="#">3.26</a>	c
CaveKey		O	<a href="#">3.38</a>	q
CDMAPrivateLongCodeMask		O	<a href="#">3.63</a>	d
CDMARedirectRecord		O	<a href="#">3.64</a>	k
DenyAccess		O	<a href="#">3.102</a>	e
DestinationDigits		O	<a href="#">3.105</a>	p
<a href="#">ElectronicSerialNumber</a>		<u>O</u>	<a href="#">3.114</a>	<u>r</u>
MobileIdentificationNumber		O	<a href="#">3.141</a>	l
RoamingIndication		O	<a href="#">3.212</a>	m
ServiceRedirectionInfo		O	<a href="#">3.227</a>	j, k
RandomVariableSSD		O	<a href="#">3.195</a>	f
RandomVariableUniqueChallenge		O	<a href="#">3.196</a>	b
RoutingDigits		O	<a href="#">3.213</a>	o
SharedSecretData		O	<a href="#">3.231</a>	c
SignalingMessageEncryptionKey		O	<a href="#">3.233</a>	g
SSDNotShared		O	<a href="#">3.259</a>	h
UpdateCount		O	<a href="#">3.296</a>	i
VoicePrivacyMask		O	<a href="#">3.301</a>	d

Notes:

- a. May be included if the SharedSecretData parameter is included.
- b. Include if the MSC-V shall initiate a Unique Challenge to the MS.
- c. Include if the SystemCapabilities include *CAVE Execution* and AC administration policies allow distribution of the SSD.
- d. Include if appropriate and the SystemAccessType value is *Call Origination* or *Page Response*.
- e. Include if the MSC may initiate a release of system resources allocated for this access. This may include disconnection of any call in progress.

- 1 f. Include if the MSC-V shall initiate an SSD update and a Unique Challenge to the MS.  
2  
3 g. Include if the SystemAccessType value is *Autonomous Registration, Call Origination or*  
4 *Page Response*.  
5  
6 h. Include if the VLR shall discard the SSD.  
7  
8 i. Include if the MSC-V should initiate COUNT Update to the MS.  
9  
10 j. Include for NDSS if HLR is to redirect the MS to an analog system.  
11  
12 k. Include for NDSS if HLR is to redirect the MS to a CDMA system.  
13  
14 l. Include if:  
15     » SSD or pending SSD is shared,  
16     » MIN is needed for authentication calculations, and  
17     » MIN was not present as the MSID in the corresponding INVOKE.  
18  
19 m. Include for CDMA to support Enhanced Roaming Indicator.  
20  
21 n. Include if the SystemAccessType is set to *Autonomous Registration* and the MS Terminal  
22 Type requires this parameter (e.g., *PACS*).  
23  
24 o. Include if the MSC-V should initiate COUNT Update to the MS.  
25  
26 p. Include if authentication failed and the AC/HLR determines the call should be redirected.  
27 These parameters may be included if the DenyAccess parameter is present.  
28  
29 q. Include if appropriate and the received SystemAccessType parameter value is *Autonomous*  
30 *registration, Call Origination or Page response*.  
31  
32 r. Include if appropriate and the received SystemAccessType parameter value is *GSM system*  
33 *access*.  
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

## 4.2 MAP Parameters

(TIA/EIA-41-D, page 5-119)

### 4.2.1 Parameter Definitions

(TIA/EIA-41-D, page 5-128)

#### 4.2.1.1 SystemAccessType

(TIA/EIA-41-D, page 5-296)

The SystemAccessType (SYSACCTYPE) parameter defines the type of system access made by the MS.

Field	Value	Type	Reference	Notes					
Identifier	SystemAccessType IMPLICIT Unsigned Enumerated	M	1.2						
Length	1 octet	M	1.1						
Contents									
<b>H</b>	<b>G</b>	<b>F</b>	<b>E</b>	<b>D</b>	<b>C</b>	<b>B</b>	<b>A</b>	<b>Octet</b>	<b>Notes</b>
SystemAccessType								1	

<i>SystemAccessType(octet 1)</i>	
Decimal Value	Meaning
0	Not used.
1	Unspecified.
2	<b>Flash request.</b>
3	<b>Autonomous registration.</b>
4	<b>Call origination.</b>
5	<b>Page response.</b>
6	<b>No access.</b>
7	<b>Power down registration.</b>

<i>SystemAccessType(octet 1)</i>	
<b>Decimal Value</b>	<b>Meaning</b>
8	<b>SMS page response.</b>
9	<b>OTASP.</b>
10	<b>Packet Data Channel Access.</b>
<u>11</u>	<u><b>GSM system access.</b></u>
<u>12 14</u> through 223	Reserved. Treat the same as value 1, <i>Unspecified</i> .
224 through 255	Reserved for <i>TIA/EIA-41</i> protocol extension. If unknown, treat the same as value 1, <i>Unspecified</i> .

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

## 5 SIGNALING PROCEDURES

(TIA/EIA-41-D, Chapter-6)

### 5.1 Authentication Request

(see TIA/EIA-41.6-D, page 6-75)

#### 5.1.1 HLR Receiving AuthenticationRequest INVOKE

(see TIA/EIA-41.6-D, page 6-85)

(see TIA/EIA/IS-735, page 157)

(see TIA/EA/IS-737, page 10)

(see TIA/EIA/IS-751, page 46)

(see TIA/EIA/IS-778, page 74)

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

- 1 IF the received message can be processed:
  - 1-1 IF the MS identity is within the range of the HLR:
    - 1-1-1 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:
      - 1-1-1-1 IF the HLR determines there is a more preferable system for the MS and decides to select the system for NDSS redirection:
        - 1-1-1-1-1 IF the selected system is a CDMA system:
          - 1-1-1-1-1-1 Include the CDMARedirectRecord of the selected system.
        - 1-1-1-1-2 ELSEIF the selected system is an analog system:
          - 1-1-1-1-2-1 Include the AnalogRedirectRecord of the selected system.
        - 1-1-1-1-3 ENDIF.
        - 1-1-1-1-4 Include the ServiceRedirectionInfo of the selected system, if available.
        - 1-1-1-1-5 Include the SystemMyTypeCode parameter set to the HLR's manufacturer.
        - 1-1-1-1-6 Send a RETURN RESULT to the requesting VLR.
        - 1-1-1-1-7 Exit this task.
      - 1-1-1-2 ENDIF.
    - 1-1-2 ENDIF.
  - 1-2 ENDIF.
  - 1-3 IF the SystemAccessType is GSM system access:
    - 1-3-1 IF the access shall be denied to the MS:
      - 1-3-1-1 Include the DenyAccess parameter set to indicate Unspecified.
      - 1-3-1-2 Send an AuthenticationRequest RETURN RESULT to the VLR.
      - 1-3-1-3 Exit this task.
    - 1-3-2 ENDIF.

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

1-4    ENDIF.

1-5    IF the MS's AuthenticationCapability indicates *No authentication required*:

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

1-5-2        Exit this task.

1-6    ENDIF.

1-7    Include the MSID parameter set to identify the MS to the AC.

1-8    Include the SenderIdentificationNumber set to the identification number of the HLR.

1-9    Relay all other received parameters.

1-10   Send an AuthenticationRequest INVOKE to the AC associated with the MS.

1-11   Start the Authentication Request Timer (ART).

1-12   WAIT for an Authentication Request response:

1-13   WHEN a RETURN RESULT is received:

1-13-1       Stop timer (ART).

1-13-2       IF the message can be processed:

1-13-2-1       IF the SharedSecretData parameter is received:

1-13-2-1-1       IF the MIN may be needed for authentication calculations for the MS:

1-13-2-1-1-1       IF the MobileIdentificationNumber parameter was not present as the MSID parameter in the INVOKE ANDIF the MIN cannot be derived from the IMSI:

1-13-2-1-1-1-1       Include the MobileIdentificationNumber parameter set to identify the MS to the VLR.

1-13-2-1-1-2       ENDIF.

1-13-2-1-2       ENDIF.

1-13-2-2       ENDIF.

1-13-2-3       IF the MS's service profile indicates that the MS is not authorized for Voice Privacy:

1-13-2-3-1       Discard any received VoicePrivacyMask (VPMASK) or CDMAPrivateLongCodeMask (CDMAPLCM) parameters.

1-13-2-4       ENDIF.

1-13-2-5       IF the MS's service profile indicates that the MS is not authorized for Data Privacy:

1-13-2-5-1       Discard the DataKey (DKEY) parameter.

1-13-2-6       ENDIF.

1-13-2-7       Relay all other received parameters.

1-13-2-8       Send a RETURN RESULT to the requesting VLR.

1-13-2-9       Exit this task.

1-13-3       ELSE (the message cannot be processed):

1-13-3-1       Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.

1-13-3-2       Execute the "Local Recovery Procedures" task (see 3.5.1).

1-13-3-3       Exit this task.

1-13-4       ENDIF.

- 1-14 WHEN a RETURN ERROR is received:
  - 1-14-1 Stop timer (ART).
  - 1-14-2 Send a RETURN ERROR to the requesting VLR with the received Error Code.
  - 1-14-3 Execute the “Local Recovery Procedures” task (see 3.5.1).
  - 1-14-4 Exit this task.
- 1-15 WHEN a REJECT is received:
  - 1-15-1 Stop timer (ART).
  - 1-15-2 Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.
  - 1-15-3 Execute the “Local Recovery Procedures” task (see 3.5.1).
  - 1-15-4 Exit this task.
- 1-16 WHEN timer (ART) expires:
  - 1-16-1 Send a RETURN ERROR to the requesting VLR with the Error Code indicating *SystemFailure*.
  - 1-16-2 Execute the “Local Recovery Procedures” task (see 3.5.1).
  - 1-16-3 Exit this task.
- 1-17 ENDWAIT.
- 2 ELSE (the received message cannot be processed):
  - 2-1 Send a RETURN ERROR to the requesting VLR.
- 3 ENDIF.
- 4 Exit this task.

**Table 1: HLR AuthenticationRequest Response**

Problem Detection and Recommended Response from HLR to VLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
MSID/HLRMismatch	The supplied MSID parameter is not in the HLR’s range of MSIDs or Directory Numbers (suspect routing error). <b>Note: This response may have been originated by the AC.</b>
ResourceShortage	A required HLR resource (e.g., internal memory record, HLR is fully occupied) is temporarily not available (e.g., congestion). <b>Note: This response may have been originated by the AC.</b>

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 1: HLR AuthenticationRequest Response

Problem Detection and Recommended Response from HLR to VLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
OperationNotSupported	The requested MAP operation is recognized, but not supported, by the receiving HLR, or the requesting functional entity is not authorized. <b>Note:</b> <i>This response may have been originated by the AC.</i> <b>Note:</b> <i>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). <b>Note:</b> <i>This response may have been originated by the AC.</i> <b>Note:</b> <i>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. <b>Note:</b> <i>This response may have been originated by the AC.</i>
UnrecognizedParameter-Value	A supplied parameter value is unrecognized or has nonstandard values. <b>Note:</b> <i>This response may have been originated by the AC.</i> <b>Note:</b> <i>Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
MissingParameter	An optional parameter was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported (AUTH=1), AuthenticationResponse (AUTHR), CallHistoryCount (COUNT) and RandomVariable (RAND) parameters were received, SystemAccessType indicated Call origination, but Digits (Dialed) parameter was not received). <b>Note:</b> <i>This response may have been originated by the AC.</i> <b>Note:</b> <i>Include the Parameter Identifier in question as the FaultyParameter parameter.</i>
RETURN RESULT DenyAccess	The AC (HLR) responded that the MIN cannot be Authenticated because of the reason identified by the supplied DenyAccess parameter value. <b>Note:</b> <i>This response may have been originated by the AC.</i> <b>Note:</b> <i>Only RETURN RESULT operations needing clarification have been included.</i>

## 5.1.2 AC Receiving AuthenticationRequest INVOKE

(see TIA/EIA-41.6-D, page 6-87)

(see TIA/EA/IS-737, page 12)

(see TIA/EIA/IS-751, page 46)

(see TIA/EIA/IS-778, page 77)

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* authentication procedures):

1-2-1 IF the SystemAccessType is *GSM system access*:

1-2-1-1 Include the SharedSecretData (SSD) parameter.

1-2-1-2 Include the ElectronicSerialNumber parameter set for the indicated MS.

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

1-2-1-4 Send an AuthenticationRequest RETURN RESULT to the requesting HLR.

1-2-1-5 Execute the “AC Awaiting AuthenticationStatusReport INVOKE” task (see 4.5.4).

1-2-1-6 Exit this task.

1-2-2 ENDIF.

1-2-3 IF the MSID and ElectronicSerialNumber parameters reported by the MS cannot be validated:

1-2-3-1 Include the DenyAccess parameter set to indicate *MSID or ESN authorization failure*.

1-2-3-2 Send a RETURN RESULT to the requesting HLR.

1-2-3-3 Exit this task.

1-2-4 ENDIF.

1-2-5 IF the TerminalType (TERMTYP) reported for the MS is not valid:

1-2-5-1 IF access shall be denied to the MS:

1-2-5-1-1 Include the DenyAccess parameter set to indicate *TerminalType mismatch*.

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

1-2-5-1-3 Exit this task.

1-2-5-2 ENDIF.

1 1-2-6           ENDIF:

2 1-2-7           IF the SystemAccessType is *FlashRequest* AND IF the ConfidentialityModes

3                   (CMODES-Actual) parameter was received:

4

5 1-2-7-1           Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using

6                   the value of the MS's SharedSecretData (SSD) recorded in the AC's database to

7                   produce an AuthenticationResponseUniqueChallenge (AUTHU).

8

9 1-2-7-2           Include the RandomVariableUniqueChallenge (RANDU) and

10                   AuthenticationResponseUniqueChallenge (AUTHU) parameters.

11 1-2-7-3           Mark the MS *pending Unique Challenge*.

12

13 1-2-8           ENDIF.

14 1-2-9           IF the SystemAccessType is *Call origination, Page response, SMS page response,*

15                   *Power down registration, or Autonomous registration*:

16

17 1-2-9-1           IF the received SystemCapabilities (SYSCAP) parameter indicates that the

18                   Serving MSC requested authentication parameters for this system access

19                   (AUTH=1 in the Overhead Message Train):

20

21 1-2-9-1-1           IF authentication parameters were not received from the MS:

22

23 1-2-9-1-1-1           IF access shall be denied to the MS:

24

25 1-2-9-1-1-1-1           Include the DenyAccess parameter set to indicate *Missing*

26                   *authentication parameters*.

27 1-2-9-1-1-1-2           Send a RETURN RESULT to the requesting HLR.

28 1-2-9-1-1-1-3           Exit this task.

29 1-2-9-1-1-2           ENDIF.

30 1-2-9-1-2           ELSEIF the AuthenticationData parameter was received:

31

32 1-2-9-1-2-1           Execute CAVE using the value of the RandomVariable (RAND)

33                   parameter, the MS's SharedSecretData (SSD) recorded in the VLR's

34                   database, the ESN and the AuthenticationData parameter.

35 1-2-9-1-3           ELSE:

36

37 1-2-9-1-3-1           Convert values in the Digits (Dialed) parameter (if received) into TBCD

38                   encoding.

39 1-2-9-1-3-2           Execute CAVE using the value of the MS's SharedSecretData (SSD)

40                   recorded in the AC's database and the parameters requested by the

41                   received SystemAccessType parameter.

42

43 1-2-9-1-4           ENDIF.

44 1-2-9-1-5           IF the CAVE authentication result and the AuthenticationResponse

45                   (AUTHR) received from the MS (see Annex C "Authentication Response

46                   Verification") match:

47

48 1-2-9-1-5-1           IF SharedSecretData (SSD) is presently shared with another VLR:

49

50 1-2-9-1-5-1-1           Execute the "AC Initiating a COUNT Request" task (see 4.10.1).

51 1-2-9-1-5-2           ENDIF.

52 1-2-9-1-5-3           IF the stored count and the CallHistoryCount (COUNT) reported by the

53                   MS do not significantly match:

54

55 1-2-9-1-5-3-1           IF access shall be denied to the MS:

56

57 1-2-9-1-5-3-1-1           Include the DenyAccess parameter set to indicate *COUNT*

58                   *mismatch*.

59 1-2-9-1-5-3-1-2           Send a RETURN RESULT to the requesting HLR.

60

1-2-9-1-5-3-1-3	Exit this task.	1
1-2-9-1-5-3-2	ENDIF.	2
1-2-9-1-5-4	ENDIF.	3
1-2-9-1-5-5	IF the SystemAccessType is <i>Call origination</i> or <i>Page response</i> :	4
1-2-9-1-5-5-1	Generate the SignalingMessageEncryptionKey (SMEKEY).	5
1-2-9-1-5-5-2	Include the SignalingMessageEncryptionKey (SMEKEY) parameter.	6
1-2-9-1-5-5-3	IF the MS supports TDMA:	7
1-2-9-1-5-5-3-1	Generate the VoicePrivacyMask (VPMASK).	8
1-2-9-1-5-5-3-2	Include the VoicePrivacyMask (VPMASK) parameter.	9
1-2-9-1-5-5-4	ELSEIF the MS supports CDMA:	10
1-2-9-1-5-5-4-1	Generate the CDMAPrivateLongCodeMask (CDMAPLCM).	11
1-2-9-1-5-5-4-2	Include the CDMAPrivateLongCodeMask (CDMAPLCM) parameter.	12
1-2-9-1-5-5-5	ENDIF.	13
1-2-9-1-5-5-6	Generate the DataKey (DKEY).	14
1-2-9-1-5-5-7	Include the DataKey (DKEY) parameter.	15
1-2-9-1-5-6	ENDIF.	16
1-2-9-1-6	ELSE (AuthenticationResponse (AUTHR) reported by the MS is invalid):	17
1-2-9-1-6-1	IF access shall be denied to the MS:	18
1-2-9-1-6-1-1	Include the DenyAccess parameter set to indicate <i>AUTHR mismatch</i> .	19
1-2-9-1-6-1-2	Send a RETURN RESULT to the requesting HLR.	20
1-2-9-1-6-1-3	Exit this task.	21
1-2-9-1-6-2	ENDIF.	22
1-2-9-1-6-3	IF SharedSecretData (SSD) is presently shared with another VLR:	23
1-2-9-1-6-3-1	Execute the “AC Initiating a COUNT Request” task (see 4.10.1).	24
1-2-9-1-6-4	ENDIF.	25
1-2-9-1-6-5	Validate the CallHistoryCount (COUNT) reported by the MS.	26
1-2-9-1-6-6	IF the COUNT is not valid:	27
1-2-9-1-6-6-1	IF access shall be denied to the MS:	28
1-2-9-1-6-6-1-1	Include the DenyAccess parameter set to indicate <i>COUNT mismatch</i> .	29
1-2-9-1-6-6-1-2	Send a RETURN RESULT to the requesting HLR.	30
1-2-9-1-6-6-1-3	Exit this task.	31
1-2-9-1-6-6-2	ENDIF.	32
1-2-9-1-6-7	ENDIF.	33
1-2-9-1-7	ENDIF.	34
1-2-9-2	ENDIF.	35
1-2-10	ENDIF.	36
1-2-11	IF SharedSecretData (SSD) presently shared with the VLR shall be discarded:	37

1	1-2-11-1	Include the SSDNotShared (NOSSD) parameter.
2	1-2-12	ENDIF.
3	1-2-13	IF an SSD update shall be initiated:
4	1-2-13-1	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.
5	1-2-13-2	Include the RandomVariableSSD (RANDSSD) parameter.
6	1-2-13-3	Mark the MS <i>pending SSD update</i> .
7	1-2-13-4	IF AC administrative procedures indicate that the pending SSD shall be shared with the VLR for the SSD update operation AND IF the received SystemCapabilities (SYSCAP) parameter indicates that the VLR is able to execute the CAVE algorithm:
8	1-2-13-4-1	Include the SharedSecretData (SSD) parameter set to the pending SSD value.
9	1-2-13-4-2	IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different from the default value:
10	1-2-13-4-2-1	Include the AuthenticationAlgorithmVersion (AAV) parameter.
11	1-2-13-4-3	ENDIF.
12	1-2-13-5	ELSE (the pending SSD is not shared):
13	1-2-13-5-1	Select a RandomVariableUniqueChallenge (RANDU) and execute CAVE using the value of the pending SSD to produce an AuthenticationResponseUniqueChallenge (AUTHU).
14	1-2-13-5-2	Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.
15	1-2-13-5-3	Mark the MS <i>pending Unique Challenge</i> .
16	1-2-13-6	ENDIF.
17	1-2-14	ELSE (SSD update not initiated):
18	1-2-14-1	IF the SharedSecretData (SSD) shall be shared with the VLR:
19	1-2-14-1-1	IF the received SystemCapabilities (SYSCAP) indicates the VLR is capable of executing the CAVE algorithm:-
20	1-2-14-1-1-1	Include the SharedSecretData (SSD) and CallHistoryCount (COUNT) parameters.
21	1-2-14-1-1-2	IF the AuthenticationAlgorithmVersion (AAV) parameter for this MS is different than the default value:
22	1-2-14-1-1-2-1	Include the AuthenticationAlgorithmVersion (AAV) parameter.
23	1-2-14-1-1-3	ENDIF.
24	1-2-14-1-2	ENDIF.
25	1-2-14-2	ENDIF.
26	1-2-14-3	IF the SystemAccessType is <i>Unspecified</i> 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:
27	1-2-14-3-1	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).
28	1-2-14-3-2	Include the RandomVariableUniqueChallenge (RANDU) and AuthenticationResponseUniqueChallenge (AUTHU) parameters.
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		

1-2-14-3-3	Mark the MS <i>pending Unique Challenge</i> .	1
1-2-14-4	ENDIF.	2
1-2-15	ENDIF.	3
1-2-16	IF local administrative procedures request that a COUNT update shall be initiated:	4
1-2-16-1	Include the UpdateCount (UPDCOUNT) parameter.	5
1-2-16-2	Mark the MS <i>pending COUNT update</i> .	6
1-2-17	ENDIF.	7
1-2-18	Send an AuthenticationRequest RETURN RESULT to the requesting HLR.	8
1-2-19	IF the MS is marked <i>pending SSD update</i> , OR IF the MS is marked <i>pending Unique Challenge</i> , OR IF the MS is marked <i>pending COUNT update</i> :	9
1-2-19-1	Execute the “AC Awaiting AuthenticationStatusReport INVOKE” task (see 4.5.4).	10
1-2-20	ENDIF.	11
1-2-21	Exit this task.	12
1-3	ENDIF.	13
2	ELSE (the received message cannot be processed):	14
2-1	Send a RETURN ERROR to the requesting HLR.	15
3	ENDIF.	16
4	Exit this task.	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

**Table 2: AC AuthenticationRequest Response**

Problem Detection and Recommended Response from AC to HLR	
RETURN ERROR Error Code	PROBLEM DEFINITION
MSID/HLRMismatch	The supplied MSID parameter is not in the AC's range of 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. <b>Note: It is recommended that an AC supports AuthenticationRequest transactions.</b>
ParameterError	A supplied parameter has an encoding problem (e.g., the supplied MobileIdentificationNumber or IMSI parameter digit values do not meet the BCD specification). <b>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</b>
SystemFailure	A required resource (e.g., data base access, functional entity) is not presently accessible due to a failure. Human intervention may be required for resolution.
UnrecognizedParameter-Value	A supplied parameter value is unrecognized or has nonstandard values. <b>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</b>
MissingParameter	An optional parameter was expected, but not received (e.g., SystemCapabilities (SYSCAP) parameter indicated authentication is supported (AUTH=1), AuthenticationResponse (AUTHR), CallHistoryCount (COUNT) and RandomVariable (RAND) parameters were received, SystemAccessType indicated Call origination, but Digits (Dialed) parameter was not received). <b>Note: Include the Parameter Identifier in question as the FaultyParameter parameter.</b>