INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.246
Annex E2
(11/2000)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Interworking of H-Series multimedia terminals with H-Series multimedia terminals and voice/voiceband terminals on GSTN and ISDN

Annex E2: ANSI-41 (Americas) Mobile Application Part and H.225.0 interworking

ITU-T Recommendation H.246 – Annex E2

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
SYSTEMS AND TERMINAL EQUIPMENT FOR AUDIOVISUAL SERVICES	H.300–H.399
SUPPLEMENTARY SERVICES FOR MULTIMEDIA	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation H.246

Interworking of H-Series multimedia terminals with H-Series multimedia terminals and voice/voiceband terminals on GSTN and ISDN

Annex E2

ANSI-41 (Americas) Mobile Application Part and H.225.0 interworking

Summary

This annex describes the interworking between ANSI-41 (Americas) Mobile Application Part (MAP) of North American Signalling System No. 7 and H.225.0 Multimedia protocols. It specifies the User Mobility Services using User Identification Module (H323_UIM) and the necessary mapping an Inter-working Function would utilize to achieve connectivity and functionality between H.323 networks and the Americas' Public Land Mobile Networks.

The detailed specifications of User Mobility Services between H.323 and ANSI-41 Public Land Mobile Networks are covered in the following functions:

– AnnexE2_GK: Specifications for interworking function between ANSI-41 Mobile Application Part (MAP) and H.225.0;

– H323_UIM: Specifications for ANSI-41 PLMN User Identification Module capability in an H.323 Terminal.

This annex requires ITU-T Recs. H.323 and H.225.0 versions 4 or later. Version 4 products can be identified by H.225.0 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 4}.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation H.246

Interworking of H-Series multimedia terminals with H-Series multimedia terminals and voice/voiceband terminals on GSTN and ISDN

Annex E2

ANSI-41 (Americas) Mobile Application Part and H.225.0 interworking

E2.1 Scope

This annex specifies the interworking function (IWF) between 2nd Generation ANSI-41 PLMNs and H.323 networks. The IWF includes the mapping of ANSI-41 PLMN Mobile Application Part (MAP) with H.323 messages, some new messages, parameters and procedures within H.323 networks. This annex does not require any changes in the mobile networks.

This annex also specifies how the ANSI-41 mobile User Identification Module (UIM) or User Identification Information may be used in an H.323 terminal. UIM support enables H.323 terminals to appear as ANSI-41 PLMN terminals on the H.323 network. The PLMN interworking function between H.323 and ANSI-41 PLMNs networks allows the mobile user to pursue functions such as sending and receiving voice calls, voice mail notification, sending short messages and receiving short messages. The scope is limited to:

−   G.711 IMT/ISDN_PRI/CAS trunks between ANSI-41 PLMN and H.323 networks. End-to-end mobile phone codecs use (i.e. EIA/TIA-136-Rev.A, etc.) is for further study (FFS).

−   operations where the H.323 terminal has either UIM or User Identification Information. If the H.323 terminal does not have UIM or User Identification Information, the following principles will apply:

  •   The H.323 terminal without UIM is a regular H.323 terminal. Calls from a regular H.323 terminal to phone numbers on PLMN or PSTN through an associated H.323 Gateway will be regarded as regular H.323 calls in the packet data network.

  •   Calls from the PLMN cannot be delivered to a regular H.323 terminal unless an association of the mobile phone number with the regular H.323 terminal exists.

The key areas of mobile networks are Mobility Management and Communications Management.

Mobility Management enables the mobile network to maintain the location and mobile subscriber status in order to provide mobile telecommunication to the end user.

Communication Management enables the mobile network to provide call control, supplementary services, short message services and data services. ANSI-41 provides seamless network capabilities between network equipment manufactured by different manufacturers. Without the ANSI-41 Rev.D standardization, it will be difficult for a cellular/PCS Wireless service provider to provide mobility between systems. ANSI-41 Rev.D covers standard interface and procedures to achieve:

−   call origination, call termination, supplementary services, short message services and data services anywhere in the wireless network;

−   subscription transparency across networks;

−   ease of use;

−   secure service access:

  •   fraud prevention,

  •   authentication and privacy;

−   billing capability, operation administration and management capability.

E2.2   Definitions

E2.2.1 H323_UIM: An H.323 terminal with User Identification Module or User Identification Information of a current ANSI-41 Public Land Mobile Network.

E2.2.2 AnnexE2_GK: An H.323 gatekeeper with ANSI-41 PLMN Interworking function.

E2.3   Normative references

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

All the normative references of ITU-T Rec. H.323, version 3 (1999), ITU-T Rec. H.225.0 version 2 (1998) and ITU-T Rec. H.245 apply:

–   ITU-T Recommendation H.225.0, version 2 (1998), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*

–   ITU-T Recommendation H.235 (1998), *Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals.*

–   ITU-T Recommendation H.323, version 2 (1998), *Packet-based multimedia communications systems.*

–   ITU-T Recommendation H.323, Annex K (2000), *HTTP-based service control transport channel.*

–   ITU-T Recommendation X.680 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

–   ITU-T Recommendation X.691 (1997), *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

–   ANSI/TIA/EIA-664-1996, *Cellular Features Description.*

–   ETSI GSM 09.02 (1990-1991), *Mobile Application Part (MAP) specifications.*

–   ANSI/TIA/EIA-41D-97, *Cellular Radiotelecommunications Intersystem Operations.*

–   TTC JJ.70.10, *Mobile Application Part (MAP) signalling system of Digital Mobile Communications Network Inter-node Interface (DMNI) for PDC.*

–   ANSI T1.707-1998, *Requirements for a User Identity Module.*

–   GSM 11.11 (1995), *Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface.*

–   TSB50 (1993), *User Interface for Authentication Key Entry.*

–   ANSI TIA/EIA-136-A (currently out for ballot), *TDMA/Cellular/PCS – Radio Interface – Mobile Station – Base Station Compatibility Standard.*

–   TIA/EIA-136-510-A (currently out for ballot), *Authentication, Encryption of Signalling Information/User Data and Privacy.*

–   TIA/EIA-136-511, *Messages Subject to Encryption.*

E2.3.1 Informative references

–   EIA/TIA/553-A (currently out for ballot), *Mobile Station – Land Station Compatibility Specification.*

–   *Common Cryptographic Algorithms*, Revision C (1998), An EAR-controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Arlington, VA.

–   *Interface Specification for Common Cryptographic Algorithms*, Revision C (1998), An EAR-controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Arlington, VA.

E2.4   Abbreviations

This annex uses the following abbreviations:

ADN	Abbreviated Dialling Number
ANSI-41	American National Standards Institute Mobile Networks specifications – 41
AuC/AC	Authentication Centre
BSC	Base Station Controller
BTS	Base Trans-receiver Station
CAVE	Cellular Authentication and Voice Encryption
CDMA-2000	Code-Division Multiple Access – 2000
CHV1	Card Holder Verification 1
CHV2	Card Holder Verification 2
EDGE	Enhanced Data Rates for GSM Evolution
EF	Elementary Files
EIR	Equipment Identification Register
ESN	Electronic Serial Number
GMSC	Gateway Mobile Switching Centre
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
H.323_UIM	H.323 User Identification Module
HLPI	Higher Layer Protocol Indicator
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IK	Integrity Key
IMEI	International Mobile Equipment Identify
IMSI	International Mobile Subscriber Identity
IMT-2000	International Mobile Telecommunications – 2000 (known as 3rd Generation Wireless standards group under ITU)
IRDB	Intelligent Roaming Database
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
MAP	Mobile Application Part

MC	ANSI-136 Message Centre (for SMS)
MDN	Mobile Directory Number
ME	Mobile Equipment
MGC	Media Gateway Controller
MGW	Media Gateway
MIN	Mobile Identification Number
MO	Mobile Originated
MS	Mobile Station
MSC	Mobile Switching Centre
MSCIN	MSC Identification Number
MSID	Mobile Station Identity
MSISDN	Mobile Subscriber ISDN Number
MSRN	Mobile Station Routing Number
MT	Mobile Terminated
MWN	Message Waiting Notification
NAM	Numeric Assignment Module
NNI	Network-to-Network Interface
NSDB	Network Selection Database
ODB	Operator Determined Barring
OTA	Over-the-Air Activation
PCS	Personal Communication Service
PDC	Personal Digital Cellular – the digital network used primarily in Japan
PDU	Packet Data Unit
PHS	Personal Handy phone systems – the digital network used primarily in Japan
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PRI	Primary Rate Interface
PRN	Provide Roaming Number
PSAP	Public Safety Access Point
PSDN	Packet Switched Data Network
PSTN	Public Switched Telephone Network
SESN	SIM Electronic Serial Number
SGW	Signalling Gateway
SID	System Identity
SIM	Subscriber Identity Module
SMDPP	Short Message Delivery Point-to-Point
SMS	Short Message Service

SMSC	Short Message Service Centre
SOC	System Operator Code
SS7	Signalling System No. 7
STP	Signalling Transfer Point
TCAP	Transaction Capabilities Application Part
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TLDN	Temporary Location Directory Number
TMSI	Temporary Mobile Station Identity
TP-FCS	TP Failure Cause
TS	Teleservice Server
TSAR	Teleservice Segmentation and Reassembly
UDH	Universal Data Header
UIM	User Identity Module
USIM	Universal Subscriber Identity Module
UWCC	Universal Wireless Communications Consortium
VLR	Visited Location Register
VMS	Voice Mail System
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol
W-CDMA	Wideband Code-Division Multiple Access

E2.5   H.323 and PLMN interworking network architecture

This annex specifies only those services, procedures, protocol messages, etc., that are mandatory for the implementation of an H.323 Mobile Gateway (AnnexE2_GK) and H.323 Mobile Endpoints (H323_UIM Terminal) – which is a subset of the optional functionality of an H.323 version 4 (2000) system.

All other (optional) mobile features defined in ITU-T Rec. H.323 version 4 – by definition – optional, and their implementation in an H.323 mobile device is entirely at the discretion of the manufacturer.
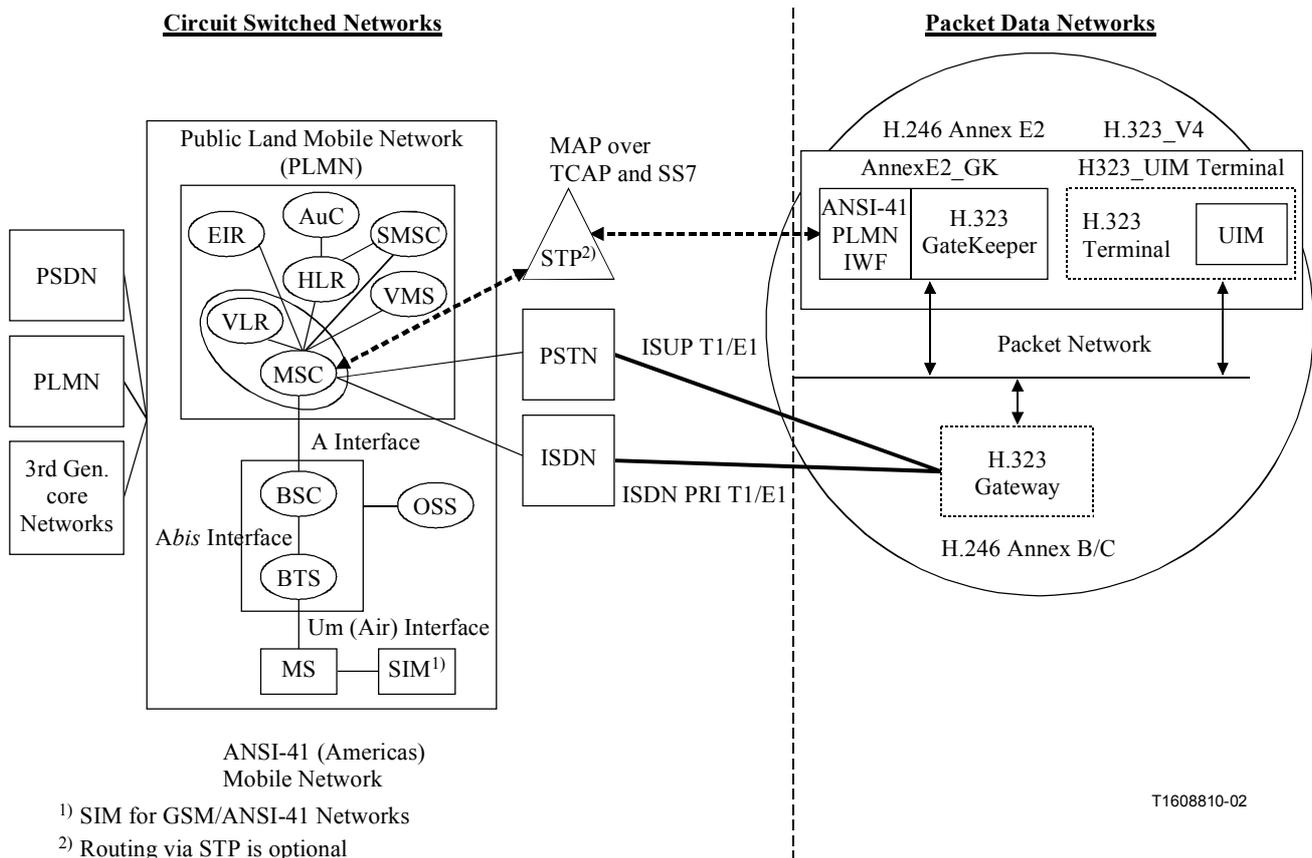
Figure E2.1/H.246 – ANSI-41 PLMN and H.323 interworking network architecture

E2.5.1 New functions of H.323 and PLMN interworking network architecture

The following sections shown in Figure E2.1 describe the functions of the H.246 Annex E2 Network components.

- H323_UIM Terminal contains an ANSI-41 User Identification Module (UIM) or User Identification Information provisioned in ANSI-41 Mobile Network.

- AnnexE2_GK is a new Interworking function between H.323 networks and ANSI-41 Public Land Mobile Networks (PLMN).

E2.6 H323_UIM Terminal contains an ANSI-41 User Identification Module

An H.323 terminal shall share and present the subscriber identity used in the ANSI-41 PLMN with which interworking is desired. This allows the H.323 terminal to provide the required subscriber identity to register with the ANSI-41 PLMN and gain access to User Mobility Services.

Note that in the future these identities should be harmonized with the proposed Universal subscriber Identity Module (USIM) in 3rd Generation wireless standards groups.

E2.6.1 A-Key

A-Key is accessible only to the algorithm used for Key generation. The A-Key may be programmed into the UIM directly by the service provider, or it may be programmed into the UIM through a specific over-the-air procedure. The A-Key is not accessible by the mobile equipment; therefore, the method of storage on the UIM is not specified in this annex.

A procedure for manual entry of the A-Key shall be provided, using the mobile equipment keypad and display. This procedure shall use the standard series of keystrokes and otherwise be consistent with the procedures defined in TIA/EIA Telecommunications Systems Bulletin TSB-50 User Interface for Authentication Key Entry. The UIM command A-KEY_VALIDATION is used to store the A-Key on the UIM.

Once an authentication key is entered, it shall not, under any circumstances or in any mode of operation, be viewed through a mobile station's display or through any device attached to the mobile station.

E2.6.2   Shared Secret Data (SSD)

The Shared Secret Data is accessible only to the Authentication and the Key Generation functions. SSD is not accessible by the mobile equipment; therefore the method of storage on the UIM is not specified in this annex.

E2.6.3   Authentication

The authentication CAVE algorithm, as per references below, shall be implemented on the UIM and has the following interface to the H.323 Terminal. All of these functions apply only to the EIA/TIA-553 directory 5F40. This DF (Data File) is expanded to include EFs (Elementary Files) and procedures for ANSI-41 H323_UIM operation.

E2.6.4   Assumptions

– The following data structures, all inputs to the CAVE algorithm, are located on the H323_UIM Terminal:

- A-Key – Accessible only to CAVE Algorithm. May be programmed via H323_UIM Terminal keypad or over the air;
- Shared Secret Data (SSD_A, SSD_B) – Accessible only to the CAVE Algorithm;
- COUNTsp – Accessible by the H323_UIM Terminal;
- Mobile Identification Number (MIN) – Accessible by the H323_UIM Terminal;
- RANDBS – Calculated on the UIM, then passed to the H323_UIM Terminal for transfer to the system;
- SIM Electronic Serial Number (S-ESN).

– The following data structures, all inputs to the CAVE algorithm, are located in H323_UIM Terminal memory:

- Electronic Serial Number (ESN);
- RANDs (combined Random Challenge A and B values, received in Global Action messages);
- Last Dialled Digits;
- RANDU;
- AUTHBSs (received from the system);
- RANDSeed.

– Encryption of Signalling data on the RAS Signalling is supported on the UIM. This function may also be performed in the H323_UIM Terminal.

– The UIM initiates the generation of keys for all ANSI-41 H323_UIM ciphering procedures. Traffic to be ciphered may include digitized voice, short messages, and Signalling data.

– The H323_UIM Terminal will perform some processing of keys that may be needed for Enhanced Privacy and Encryption (EPE) procedures.

–   The H323_UIM Terminal will support manual entry of the A-Key into the H.323 Terminal, as done in ANSI-136 mobiles.

–   Will use T = 0 transmission protocol.

–   UIM task execution is context specific to first selecting the EIA/TIA-553 (5F40) directory.

E2.6.5   Description

It is necessary to provide six interfaces to the CAVE Algorithm and Secret Data areas, as listed below:

•   Generation of Authentication Signature data, and generation of ciphering keys;

•   Validation and storage of entered A-Keys;

•   Ask Random task (generates RANDBS);

•   Update Shared Secret Data (Generates SSD_A_NEW, SSD_B_NEW and AUTHBS values);

•   Confirm Shared Secret Data (Updates SSD values);

•   CMEA Encryption of voice channel data digits.

In addition, some commands are defined for manipulating the COUNTsp value.

NOTE 1 – For each task, the expected normal (i.e. success) status code is listed in the status word description. A list of possible error codes that apply to all tasks can be found in the UIM Status Codes.

NOTE 2 – The phrase "Use H323_UIM Terminal ESN (= "00")" in the tasks below is obsolete, and is preserved for backwards compatibility with legacy equipment. This byte is set to "00" in this annex. The four-byte parameter that is used by the UIM for the calculations shall be set to the value of the H323_UIM Terminal's ESN field if the "usage indicator" directs the UIM to use the H323_UIM Terminal's ESN. If the "usage indicator" directs the UIM to use its S_ESN, the internally stored S_ESN shall be used. In the latter instance, the four-byte parameter passed by the H323_UIM Terminal shall not be used as an input to the calculations in these sections.

E2.6.6   Generation of Authentication Signature Data and Ciphering Keys

This task produces an Authentication response, and shall be used during H323_UIM Terminal Registrations, Originations, and Terminations and for the Unique Challenge-Response Procedure. If Byte 0, Bit 1 is set, the UIM should also generate key bits after completing the Authentication function. Some of those ciphering octets may be passed back to the H323_UIM Terminal for use with supplementary crypto mechanisms, which reside in the H323_UIM Terminal. This task requires the following input parameters:

Task name: Internal_Authenticate

Class = "A0", INS = "88", P1 = "00", P2 = "00", Lc = "0F"

Data Bytes coding:

Byte 0   *Process Control Byte*

• bit 0   0 = RANDs, 1 = RANDU

• bit 1   Generate Key Bits flag (0 = No, 1 = Yes)

• bit 2   Load Internal key flag

                   0 = pass all generated key bytes to handset

                   1 = load first 8 bytes of generated keys internally to UIM, pass all remaining key bytes to H323_UIM Terminal)

• bits 3-7   Unused, future expansion

Bytes 1-4   *Bytes 1-4:* RANDs (for Registrations, Originations, and Terminations)

                        or

Bytes 1-3: RANDU (for Unique Challenge-Response Procedures)

Byte 4: = 0 (MIN2 will be filled in by UIM)

Byte 5   Digits Length

(in bits, = 0, 4, 8, 12, 16, 20 or 24, = 4 x number of digits in bytes 6-8)

Bytes 6-8   = 0,0,0 (for Registrations, Terminations, Unique Challenge Response Procedures)

= Last Dialled Digits, unused bits filled with 0's (for Originations). If more than 6 digits are dialled, these are the last 6 digits in the origination string. If less than 6 digits are dialled, MIN1 will be filled in by the UIM for the unused bits.

Byte 9   Use H323_UIM Terminal ESN (="00")

Bytes 10-13   ESN (Electronic Serial Number)

Byte 14   Key_size

= 0 if Byte 0, bit 1 = 0

= "08"hex or "49"hex if Byte 0, Bit 1 = 1

Where:

"00"hex = no key generation

"08"hex = generate the CMEA Key

"49"hex = generate the CMEA Key + a 520 bit VPMASK Key

The output of this task shall be:

Status Bytes   SW1 (="9F" if success)

SW2 (="nn" if success)

"nn" is 03+Key_size if Byte 0, Bit 2 above = 0
"nn" is 03+Key_size-08 if Byte 0, Bit 2 above = 1

Task name: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "nn"

"nn" is 03+Key_size if Byte 0, bit 2 above = 0
"nn" is 03+Key_size-08 if Byte 0, bit 2 above = 1

The output of this task shall be:

Bytes 0-2   the 18-bit Authentication Signature (AUTHR/AUTHU) value.

Bytes 3-(n+2)   Cipher octets for crypto mechanisms (n = Key_size or Key_size-8).

Status Bytes   SW1 (= "90" if success)

SW2 (= "00" if success)

The following values represent examples of this function:

To generate Authentication values only:

Byte 0

• bit 1   = 0 (No cipher keys need to be generated)

• bit 2   = 0 (No keys generated, not applicable)

Byte 14   = 0 (No cipher keys passed to H323_UIM Terminal, means bytes 3-(n+2) in Get_Response task do not exist).

To generate Authentication values and ciphering key for use with CMEA on UIM:

Byte 0

- bit 1   = 1 (ciphering keys need to be generated)
- bit 2   = 1 (Use first 8 bytes of generated ciphering keys in the UIM)

Byte 14   = 8 (8 bytes of ciphering keys should be generated, means bytes 3-(n+2) in Get_Response task do not exist as all generated ciphering key bytes are used in the UIM).

To generate Authentication values and ciphering keys for H323_UIM Terminal-based algorithms:

Byte 0

- bit 1   = 1 (ciphering keys need to be generated)
- bit 2   = 0 (pass all generated ciphering keys to the H323_UIM Terminal)

Byte 14   = n (n bytes of ciphering keys should be generated, means bytes 3-(n+2) in Get_Response task will be passed to the H323_UIM Terminal).

NOTE – Additional processing of ciphering keys may need to be performed by H323_UIM Terminal, for use with some H323_UIM Terminal-based ciphering methods.

E2.6.7 Validation and Storage of Entered A-Keys

With manual entry of the A-Key, the input A-Key must be validated prior to its storage in the UIM. If successful, the A-Key is saved in the UIM and the COUNTsp and Shared Secret Data (SSD) are reset to zero. This task requires the following input parameters:

Task name: AKEY_validation

Class = "A0", INS = "86", P1 = "00", P2 = "00", Lc = "12"

Data Bytes coding:

Bytes 0-12   Authentication digits string (first digit in Most-Significant nibble of byte 0, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)

Byte 13   Use H323_UIM Terminal ESN (= "00")

Bytes 14-17   ESN

The output of this task shall be:

Status Bytes   SW1 (= "90" if success)

                        SW2 (= "00" if success)

E2.6.8 Ask Random Task

This task is used to generate the RANDBS random value. This task must be executed prior to updating the Shared Secret Data (SSD). The value RANDSeed must be generated by the H323_UIM Terminal prior to calling this task. This task requires the following input parameters:

Task name: Ask_Random

Class = "A0", INS = "8A", P1 = "00", P2 = "00", Lc = "04"

Data Bytes coding:

Bytes 0-3   RANDSeed

The output of this task shall be:

Status Bytes   SW1 (= "9F" if success)

                        SW2 (= "04" if success)

Task name: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "04"

The output of this task shall be:

Bytes 0-3   RANDBS

Status Bytes   SW1 (= "90" if success)

SW2 (= "00" if success)

E2.6.9 Update Shared Secret Data

This task is used to generate the preliminary new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) and the AUTHBS value. The Ask Random Task (see above) must be executed prior to this routine. The task requires the following input parameters:

Task name: Update_SSD

Class = "A0", INS = "84", P1 = "00", P2 = "00", Lc = "0C"

Data Bytes coding:

Bytes 0-6   RANDSSD

Byte 7   Use H323_UIM Terminal ESN (= "00")

Bytes 8-11   ESN

The output of this task shall be:

Status Bytes   SW1 (= "90" if success, = "98" if failure)

SW2 (= "00" if success, = "04" if failure)

E2.6.10 Confirm Shared Secret Data

This task is used to validate the new Shared Secret Data (SSD_A_NEW, SSD_B_NEW) by comparing the internally computed AUTHBS with the AUTHBSs received from the system. If successful, the SSD_A and SSD_B values will be updated to match the SSD_A_NEW and SSD_B_NEW values, respectively The task requires the following input parameters:

Task name: Confirm_SSD

Class = "A0", INS = "82", P1 = "00", P2 = "00", Lc = "03"

Data Bytes coding:

Bytes 0-2   AUTHBSs

The output of this task shall be:

Status Bytes   SW1 (= "90" if success)

SW2 (= "00" if success)

E2.6.11 CMEA Encryption of Voice Channel Data Digits

This task is used when the H323_UIM Terminal is on a Voice Channel, to encrypt and decrypt some portions of digital messages transmitted to the AnnexE1_GK. These will occur for the following message:

–   Called Address Message (in response to a hookflash, up to 4 bytes per word, 4 words, total of 16 bytes)

This task requires the following input parameters:

Task name: CMEA_encrypt

Class = "A0", INS = "8C", P1 = "00", P2 = "00", Lc = "nn"

("nn" is hex value of data length n)

Data Bytes coding:

Bytes 0-(n-1)   The n-byte data to be encoded, max. size = 32 bytes.

The output of this task shall be:

Status Bytes   SW1 (= "9F" if success)

                        SW2 (= "nn" if success) ("nn" is hex value of data length n)

Task name: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "nn" ("nn" is hex value of data length n)

The output of this task shall be:

Bytes 0-(n-1)   n-byte value, containing the encrypted bits, max. size = 32 bytes.

Status Bytes   SW1 (= "90" if success)

                        SW2 (= "00" if success)

For example, encrypting a 16-byte hookflash string would result in the following sequence of data to/from the UIM:

TO UIM:

Class = "A0", INS = "8C", P1 = "00", P2 = "00", Lc = "10", Data: d0, d1, d2, ..., d14, d15

FROM UIM:

SW1 = "9F", SW2 = "10"

TO UIM:

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "10"

FROM UIM:

e0, e1, e2, ..., e14, e15, SW1 = "90", SW2 = "00"

E2.6.12   Updating of the COUNTsp Value

COUNTsp is a synchronization data unit that is passed back to the system in coordination with the ANSI-41 H323_UIM Terminal Authentication process. It may be updated by the ANSI-41 and AMPS system at any time while the H323_UIM Terminal is active. The H323_UIM Terminal must be able to fetch and increment COUNTsp.

Get Call Count

Task name: Read_Record (Get Call Count)

Class = "A0", INS = "B2", P1 = "00", P2 = "04", Le = "03"

The output of this task shall be:

Byte 0-2   Returned COUNTsp value

Status Bytes   SW1 (= "90" if success)

                        SW2 (= "00" if success)

Set Call Count

Task name: Update Record (Set Call Count)

Class = "A0", INS = "DC", P1 = "00", P2 = "03", Lc = "03"

Data Bytes coding:

Byte 0-2   COUNTsp value

The output of this task shall be:

Status Bytes   SW1 (= "90" if success)

                        SW2 (= "00" if success)

Update Call Count

Task name: Increase (Increment Call Count)

Class = "A0", INS = "32", P1 = "00", P2 = "00", Lc = "03"

Data Bytes coding:

Bytes 0-2   00, 00, 01 (increment amount)

The output of this task shall be:

Status Bytes   SW1 (= "9F" if success)

                      SW2 (= "06" if success)

Task name: Get_Response

Class = "A0", INS = "C0", P1 = "00", P2 = "00", Le = "06"

The output of this task shall be:

Byte 0-2   COUNTsp

Bytes 3-5   Value that was added

Status Bytes   SW1 (= "90" if success)

                      SW2 (= "00" if success)

E2.6.13   H323_UIM status codes

The following status codes, returned by the UIM in response to the execution of any of the tasks specified in this annex, are valid. The first hex value is returned in SW1 (status word 1), the second hex value in SW2 (status word 2).

Success codes

90, 00   Generic success code

9F, xx   Success, xx bytes of data available to be read via "Get_Response" task.

Error codes

92, 40   Error, memory problem

94, 08   Error, file is inconsistent with the command

98, 04   Error, no CHV1 (cardholder verification 1) has been presented successfully

98, 34   Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence)

67, xx   Error, incorrect parameter P3 (ISO code)

6B, xx   Error, incorrect parameter P1 or P2 (ISO code)

6D, xx   Error, unknown instruction code given in the command (ISO code)

6E, xx   Error, wrong instruction class given in the command (ISO code)

6F, xx   Error, technical problem with no diagnostic given (ISO code)

6A, 80   Error, incorrect parameters in the data field

E2.7   H323_UIM management procedures

After H323_UIM activation (see GSM 11.11, subclause 4.3.2) the H323_UIM Terminal follows the ANSI-41 initialization procedures up to and including the IMSI Request. The H323_UIM Terminal then attempts to select the Dedicated File DF$_{TIA/EIA-41}$. If DF$_{TIA/EIA-41}$ is present, then the UIM is an H.323/ANSI-136 UIM. If the DF$_{TIA/EIA-136}$ is not present, then UIM is not associated with the H323_UIM Terminal.

For an H323/ANSI-41 UIM, the H323_UIM Terminal shall perform the H.323-ANSI-41 Phase ID Request. An H.323/ANSI-41 UIM is required to support the elementary files and procedures defined for the H.246 Annex E2 phase defined in the H.323-ANSI-41 UIM Phase ID EF, and any previous H.246 Annex E2 phases. The H323_UIM Terminal must operate at the level defined by the lower of its own H.323-ANSI-41 Phase ID or the H.323-ANSI-41 Phase ID of the UIM.

Also as part of the management phase, the H323_UIM Terminal shall retrieve the Protocol Priority Indicator value by performing an ANSI-Usage Indicator Request. The H323_UIM Terminal shall then perform the Home System Operator Code and Mobile Country Code Request, which shall be required to perform any personalization checks, if required, in order to determine if the current UIM will be allowed to operate or not.

If the personalization check fails, the H323_UIM Terminal enters the "limited service state" based on the Protocol Priority Indicator value in which only emergency calls can be attempted (see GSM 02.22 Annex A.2 and TIA/EIA-136-123). If the check is successful, then the H323_UIM Terminal continues with the session initialization based on the type of UIM.

Upon completion of this, the H323_UIM Terminal is free to request any user data information it may require, see GSM 11.11, subclause 11.5. Note however, that the reading of this information may occur prior to this point i.e. after reading the initial initialization data (ANSI-41).

Figures E2.2 and E2.3 below describe the process and are to be used for information only.
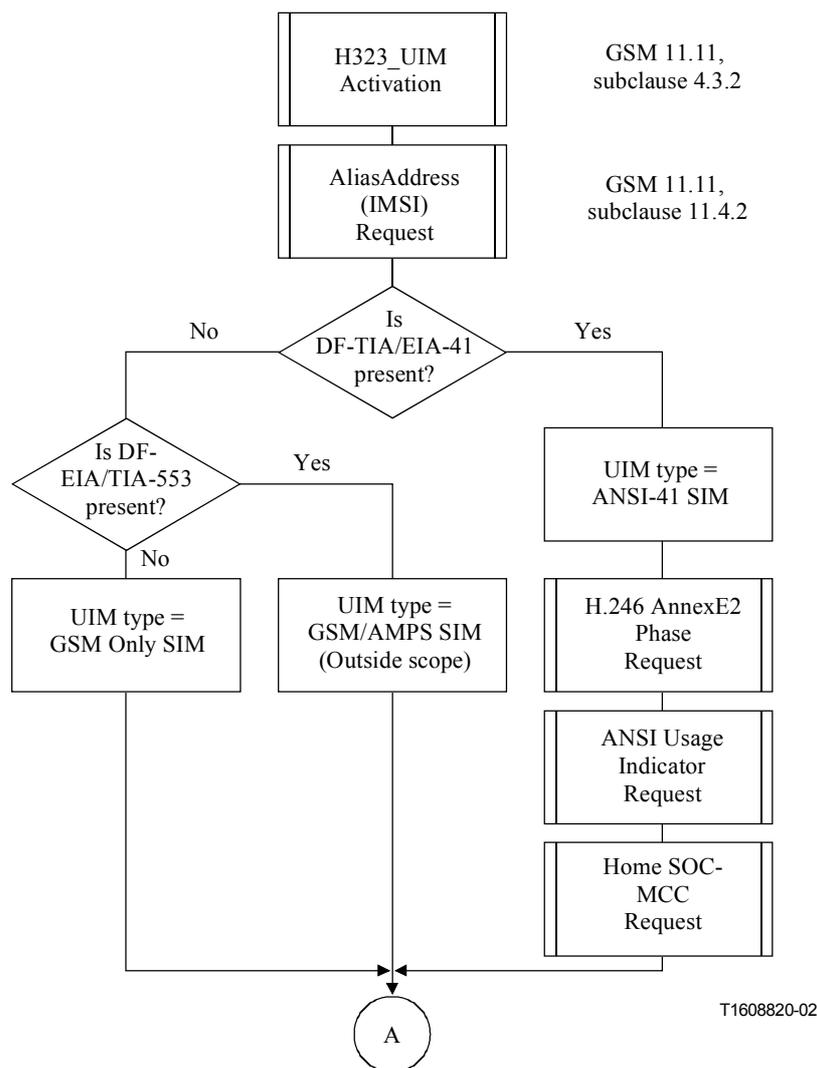
Figure E2.2/H.246 – UIM management procedures – 1 (informative)
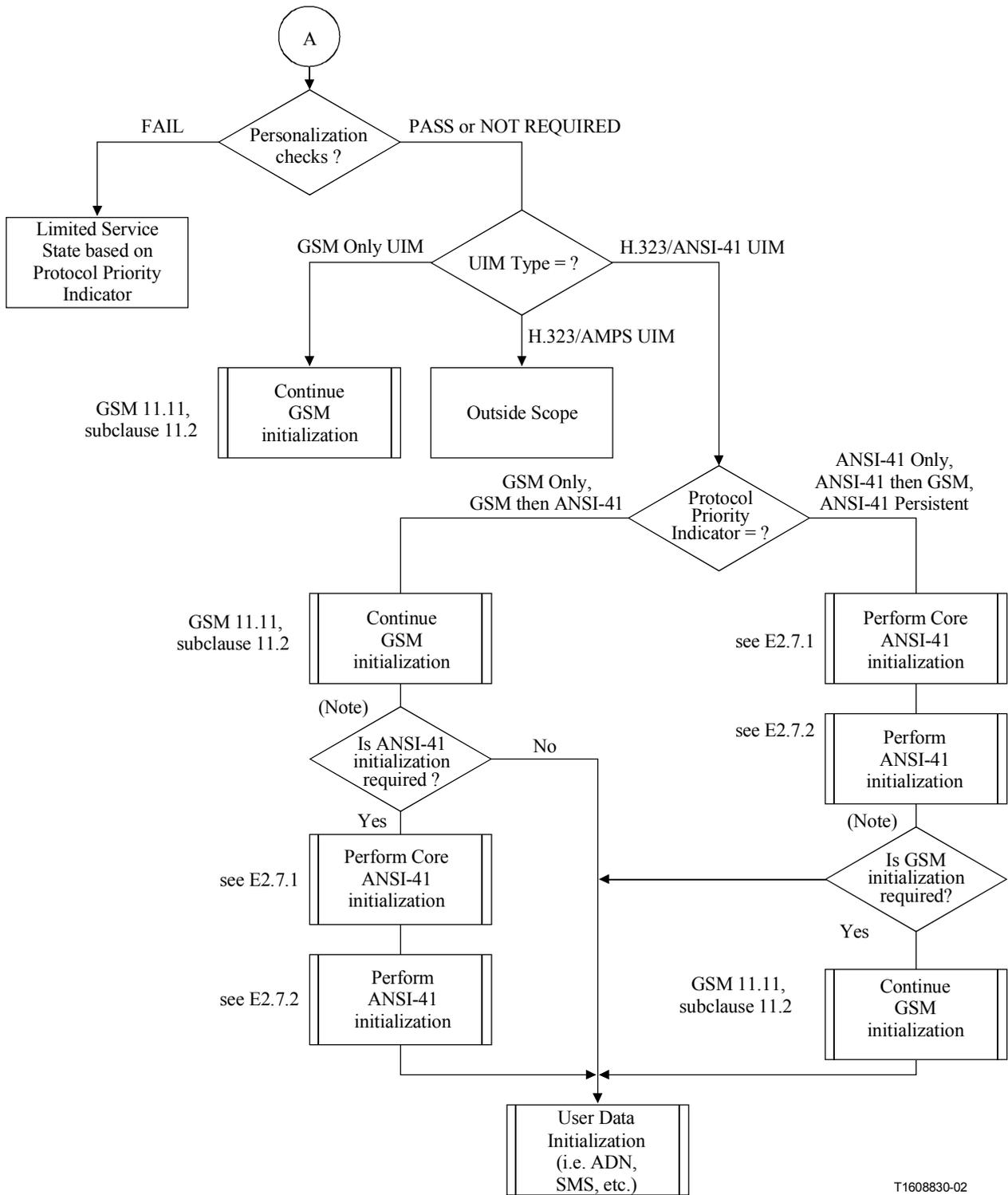
NOTE – User Data initialization may also occur at this point.

Figure E2.3/H.246 – UIM management procedures – 2 (informative)

E2.7.1 Core ANSI-41 initialization

The H323_UIM Terminal runs the following procedures:

* MIN Request;

* ACCOLC Request;

* SID request;

* Group ID request;

* S-ESN request;

* COUNTsp request;

* Positive/Favoured SID List request;

* Negative/Forbidden SID List request;

Registration Threshold request. There are other files in the $DF_{PCS1900}$ which are required for the GSM/AMPS mobile station; however,the reading of these files is not required for a GSM/ANSI-136 mobile and as such is outside the scope of this annex.

E2.7.2 ANSI-41 H323_UIM initialization

The H323_UIM Terminal runs the following procedures:

* IRDB Parameters request;

* Additional User Registration Parameters request;

* Partner SID List request;

* Partner SOC List request;

* Favoured SOC List request;

* Forbidden SOC List request;

* Alpha Tag request;

* Triggered Scan Timers request;

* TeleService Server Address request;

* SS Feature Code Table request;

* IRDB Version Table request;

* User Group ID request;

* Cooperative SOC List request.

E2.7.3 UIM session termination

The H323_UIM Terminal shall perform the session termination procedures defined in GSM 11.11, subclause 11.2.2 in the following cases:

* ANSI-41 H323_UIM with the Protocol Priority Indicator set to ANSI-41, then to GSM.

The H323_UIM Terminal shall perform the following updates:

* Additional User Registration Parameters update.

For the following cases:

* ANSI-41 H323_UIM with the Protocol Priority Indicator set to ANSI-41 only.

As soon as the UIM indicates that these procedures are completed, the H323_UIM Terminal/UIM link may be terminated. Upon termination of the link, the H323_UIM Terminal shall delete all subscriber-related information from its memory. If the H323_UIM Terminal has already updated any of the subscriber related information during the UIM session and the value has not changed until UIM session termination, the H323_UIM Terminal may omit the respective update procedure.

E2.7.4 H323_UIM NAM information procedures

E2.7.4.1 Mobile Identification Number

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{MIN}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{MIN}

E2.7.4.2 Access Overload Class

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{ACCOLC}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{ACCOLC}

E2.7.4.3 System Identification of Home System

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{SID}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{SID}

E2.7.4.4 Home System Operator Code and Mobile Country Code

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{HSOC-MCC}$

Update: The H323_UIM Terminal performs the updating procedure with the $EF_{HSOC-MCC}$

E2.7.4.5 Initial Paging Channel

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{IPC}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{IPC}

E2.7.4.6 Group ID

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{GPI}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{GPI}

E2.7.4.7 SIM Electronic Serial Number

Request   The H323_UIM Terminal performs the reading procedure with the EF_{SESN}

E2.7.4.8 AMPS Usage Indicators

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{AMPS-UI}$

E2.7.4.9 ANSI-41 Usage Indicators

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{ANSI-UI}$

E2.7.4.10 Alpha Tags

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{A-TAG}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{A-TAG}

E2.7.5 H323_UIM authentication related procedures

E2.7.5.1 Call Count

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{COUNT-SP}$

Update: The H323_UIM Terminal performs the updating procedure with the $EF_{COUNT-SP}$

E2.7.6 UIM network selection related procedures

E2.7.6.1 Positive/Favoured SID List

Request: The H323_UIM Terminal performs the reading procedure with the EF_{PSID}

E2.7.6.2 Negative/Forbidden SID List

Request: The H323_UIM Terminal performs the reading procedure with the EF_{NSID}

E2.7.6.3 Cooperative SOC List

Requirement: The EF_{CNL} is marked "allocated" and "activated"

Request: The H323_UIM Terminal performs the reading procedure with the EF_{CSL}

E2.7.6.4 IRDB Version Table

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{IRDB-VER}$

E2.7.6.5 Partner SID List

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{PART-SID}$

E2.7.6.6 Partner SOC List

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{PART-SOC}$

E2.7.6.7 Favoured SOC List

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{FAV-SOC}$

E2.7.6.8 Forbidden SOC List

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{FORB-SOC}$

E2.7.6.9 IRDB Parameter

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{IRDB-PARAM}$

E2.7.7 H323_UIM user interface related procedures

E2.7.7.1 SS (Supplementary Services) Feature Code Table

Request: The H323_UIM Terminal performs the reading procedure with the EF_{SSFC}

E2.7.8 H323_UIM timing related procedures

E2.7.8.1 Triggered Scan Timers

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{TS-TIMER}$

E2.7.9 H323_UIM registration related procedures

E2.7.9.1 Registration Threshold

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{REG\text{-}THRESH}$

Update: The H323_UIM Terminal performs the updating procedure with the $EF_{REG\text{-}THRESH}$

E2.7.10 H323_UIM additional procedures

E2.7.10.1 H.246 Annex E2 UIM Phase ID

Request: The H323_UIM Terminal performs the reading procedure with the $EF_{GA\text{-}PHASE}$

E2.7.10.2 TeleService Server Address Info

Request: The H323_UIM Terminal performs the reading procedure with the EF_{TSAI}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{TSAI}

E2.7.10.3 Additional User Registration Parameters

Request: The H323_UIM Terminal performs the reading procedure with the EF_{AURP}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{AURP}

E2.7.10.4 User Group ID

Requirement: As per UIM specification

Request: The H323_UIM Terminal performs the reading procedure with the EF_{UGIDI}

Update: The H323_UIM Terminal performs the updating procedure with the EF_{UGIDI}

E2.7.10.5 SOC De-personalization control Key

Request: The H323_UIM TERMINAL performs the reading procedure with the EF_{SDCK}

E2.7.11 H323_UIM update management procedures

Under some circumstances it may be necessary for the H323_UIM to notify the Terminal of a change in its configuration i.e. an ANSI-41 Host SMS Teleservice update to the UIM's IRDB and/or NAM information. As such, the H323_UIM Terminal may be required to update any images of elementary files it may contain and/or perform some other procedures (i.e. power up scan after updating of the NAM). For these situations, the H323_UIM shall use the UIM Tool Kit Command REFRESH to notify the H.323 mobile terminal of such changes to its configuration. Refer to GSM 11.14 for further details.

Table E2.1 defines the guidelines to be used when UIM modifications have taken place. Upon receiving a REFRESH command, the H.323 mobile terminal shall take the actions defined in Table E2.1 if the appropriate file has been changed.

Table E2.1/H.246 – H323_UIM Terminal guidelines for UIM modifications

File Updated	H323_UIM Terminal Updates Image	H323_UIM Terminal performs Power Up Scan
MIN		✓ if in ANSI-41 H323_UIM
ACCOLC		NA
SID		✓
Group ID		NA
S-ESN	NA	NA
COUNTsp		NA
Positive/Favoured SID List		✓
Negative/Forbidden SID List		✓
Registration Threshold		NA
IRDB Parameters		✓
Additional User Registration Pars.	✓ if in GSM	NA
Partner SID List		✓
Partner SOC List		✓
Favoured SOC List		✓
Forbidden SOC List		✓
Alpha Tag		NA
Triggered Scan Timers		NA
TeleService Server Address		NA
SS Feature Code Table		NA
IRDB Version Table		NA
User Group ID		NA
SOC De-personalization Control Key	✓	

If a REFRESH command is received by the H.323 mobile terminal and as a result some files in the list above are changed, the H.323 mobile terminal shall update any images it may contain of that information regardless of whether it is in ANSI-41 or GSM mode and, as the table dictates, a power up scan may be required.

E2.8   AnnexE2_GK with PLMN Interworking Function (IWF) and H.323 Gatekeeper

The current ANSI-41 digital wireless networks mainly comprises of:

•   ANSI-41 networks with TDMA and CDMA air-interfaces throughout North and South America, most parts of Asia, Russia, Australia and some parts of Europe.

The ANSI-41 Public Land Mobile Network's main role is to manage the communications between the mobile users and other users, such as mobile users, H323_UIM users, ISDN users, fixed telephony users, etc. It also includes databases needed in order to store information about the subscribers and to manage their mobility. The ANSI-41 PLMN IWF provides interworking between the PLMN and an H.323 network.

The basic model of an AnnexE2_GK solution is a logical interworking function that performs the appropriate protocol conversion, database mapping and transaction management to support the Mobility Management, Call Origination, and Call Delivery functions.

An H.246 Annex E2 Gatekeeper between an H.323 network and a PLMN network maps the operations and messages between Gateway, Gatekeeper and serving Mobile Switching Centre (MSC), Visitor Location Register (VLR). The interworking functions are as follows:

Mobility Management areas

• Registration of H323_UIM Terminal and/or user.

• Authentication of the H323_UIM Terminal and user.

Communication Management area

• Call Termination to H323_UIM Terminal from PLMN.

• Message Waiting Notification delivery to H323_UIM Terminal.

• Short Message Origination from Short Message Entity in H323_UIM Terminal.

• Short Message Termination to Short Message Entity in H323_UIM Terminal.

This AnnexE_GK looks like a Gatekeeper from the H.323 Endpoint and like a Visitor Location Register (VLR) and a serving Mobile Switching Centre (MSC) from the PLMN.

E2.8.1 Mapping of ANSI-41 PLMN MAP messages to H.225.0 messages

Table E2.2/H.246 – ANSI-41 PLMN MAP ↔ H.225.0 messages mapping

Functions	ANSI-41 MAP messages	H.225.0 messages
Registration		GRQ, GCF, GRJ, RRQ, RCF, RRJ operations are used for Registration and Authentication of the H323_UIM Terminal
	RegistrationNotification (REGNOT)	
Authentication	AuthenticationRequest (AUTHREQ)	
	AuthenticationDirective (AUTHDIR)	
	AuthenticationStatusReport (ASREPORT)	
	CountRequest (COUNTREQ)	
	AuthenticationFailureReport (AFREPORT)	
	RandomVariableRequest (RANDREQ)	
Subscriber Profile Update	QualificationRequest (QUALREQ)	ARQ, ACF, ARJ
	FeatureRequest (FEATREQ)	
	QualificationDirective (QUALDIR)	
Call Delivery	LocationRequest (LOCREQ)	
	RoutingRequest (ROUTREQ)	
	RemoteUserInteractionDirective (RUIDIR)	Setup, Connect, Info
Mapping of ISUP ↔ Q.931	Call Setup and Call Release messages	Refer to H.248 contributions
MessageWaiting Notification	(QUALDIR), InformationDirective (INFODIR), MWN Indication	H.450.7 MWI SS
Short Message Service	SMSRequest (SMSREQ), SMS Delivery Point to Point (SMD PP), SMS Notification (SMSNOT), SMS Backward (SMS BACK), SMS Forward (SMS FWD)	H.323 Annex K (HTTP-based service control transport channel in H.323)
Wireless Application Protocol (WAP) services	WML Scripts and Web Browser	H.323 Annex K (HTTP-based service control transport channel in H.323)
Deregistration	RegistrationCancellation (REGCANC)	URQ, UCF, URJ,
	MSInactive (MSINACT)	URQ, UCF, URJ
	BulkDeregistration (BULKDEREG)	URQ, UCF, URJ

E2.9 Mobility Management and Communication Management AnnexE2_GK procedures

E2.9.1 Additions of Mobility parameters and procedure to H.225 RAS messages

Extending the aliasAddress type with a new type MobileUIM that supports all the various mobile identification formats provides the H.323 mobile user identification information.

E2.9.2 Security aspects of mobile H.323 User Identity Module (UIM)

Follow procedures of H.235 to ensure privacy of the H323_UIM and ANSI-41 Authentication of H323_UIM.

E2.9.3 H.323 foreign mode

When an ANSI-41 native subscriber operates in H.323 foreign mode, the mobile station shall use the H.323 interface. The H.246 Annex E2 Interworking function (AnnexE2_GK) shall provide both H.323 HLR and ANSI-41 VLR emulation to allow the subscriber to automatically register and obtain service. To the visited H.323 network, the subscriber appears to register with the AnnexE2_GK, emulating an H.323 HLR. This emulated H.323 HLR acts as a limited proxy for the actual ANSI-41 HLR, with the true ANSI-41 HLR retaining ultimate control. At the same time, to the home ANSI-41 network, the subscriber appears to register from the AnnexE2_GK, emulating an ANSI-41 VLR. The AnnexE2_GK links H.225.0 operations and data to the equivalent ANSI-41 MAP operations and data, and vice versa, in order to support interoperability.

To support H.323 foreign mode operation, an H.323 Authentication Centre (AuC) can be integrated into the AnnexE2_GK gateway.

For SMS interoperability, the AnnexE2_GK shall also provide SMSC emulation using H.323 Annex K (Service Control protocol), acting as a limited proxy for the subscriber's ANSI-41 MC. In some cases, the AnnexE2_GK will need to originate short messages in order to support interoperability. In order to support late call forwarding, the AnnexE2_GK and H.246 Annex B/C also provides gateway MSC emulation.

E2.9.4 Subscriber data

The AnnexE2_GK does not duplicate the subscriber's existing HLR, but provides a gateway to any visited network that uses a foreign MAP protocol. The original source of subscription data remains in the home network's HLR. Most of this data shall not reside in the AnnexE2_GK, but shall be dynamically converted and translated between H.323 and ANSI-41 MAP messages as needed.

Nevertheless, some basic subscriber identity information shall need to be provisioned in the AnnexE2_GK to support this mapping process, such as:

• International Mobile Subscriber Identity (IMSI);

• Mobile Identification Number (MIN);

• Electronic Serial Number (ESN);

• Terminal type.

Authentication and encryption services are critical functions that shall be supported with network interoperability. These capabilities are managed in both H.323 and ANSI-41 networks by the Authentication Centre (AuC or AC), which can be physically separated from the associated HLR or integrated with it. Different authentication processes and algorithms are defined for H.323 and ANSI-41. Therefore, for phase 1 implementation, subscriber-specific authentication data shall be provisioned and maintained on both an H.323 AuC and ANSI-41 AC, in order to support service on either network. Subscriber data that needs to be maintained includes:

• Ki (H.323 subscriber authentication key);

• Triplets or groups of Kc (cipher key), CKSN (cipher key sequence number), and SRES (signed response) for H.323-based authentication and ciphering;

- A-key (ANSI-41 authentication key);
- SSD-A (ANSI-41 shared secret data for authentication);
- SSD-B (ANSI-41 shared secret data used for generated signalling message encryption (SME) and voice privacy (VP) masks).

The foreign mode Authentication Centre can be integrated into the AnnexE2_GK gateway or implemented as a separate network element.

E2.10 Automatic registration and authentication

The H.246 AnnexE2 mobile station shall use network selection to automatically obtain the best possible service in any geographic area. Upon automatic selection of a service provider in a particular area, the network shall support automatic registration from that serving area back to the home location register (HLR).

E2.10.1 Addressing

In H.323 foreign mode, the AnnexE2_GK shall support registration using the Mobile Identification Number (MIN) as the Mobile Station Identity (MSID). When MIN is used as identification for registration, the AnnexE2_GK shall correlate this MIN to the associated IP address for the H.323 native subscriber.

E2.10.2 Authentication, encryption, voice privacy

Authentication, encryption, and voice privacy in H323_UIM ANSI-41 modes shall be supported as defined in "Common Cryptographic Algorithms, Revision C", ANSI TIA/EIA-136-510, and ANSI TIA/EIA-136-511, with the exception that the ESN input to the CAVE algorithm shall be governed by the status of the ESN Usage Indicator in H323_UIM.

E2.11 UIM-based roaming

H323_UIM-based roaming identifies the capability of a UIM-based subscriber to place his UIM in any supporting H.323 terminal or mobile equipment to obtain service without operator or carrier intervention. Supporting H323 Terminal/mobile equipment refers to H323_UIM Terminal/mobile terminals that can read the required subscription identification and associated information on the H323_UIM.

UIM-based roaming allow subscribers to change H.323 terminal/mobile equipment for purpose of accessing specific bands or features which may not be available from existing H.323 terminal/mobile equipment. It also allows subscribers to easily change out H.323 terminal/mobile equipment for upgrade or repair, without operator or carrier intervention.

E2.11.1 Use of mobile equipment identifiers

ANSI-41 uses the Electronic Serial Number (ESN) to uniquely identify the mobile station; the IMEI is not currently transmitted from the mobile station to the ANSI-41 network. The ESN is currently used in ANSI-41 subscriber authorization, authentication, signalling message encryption, and voice privacy, and in AMPS subscriber authorization, authentication, and signalling message encryption. Some ANSI-41 service providers also use the ESN to track in-service mobile stations. Permanently attaching the ESN to the mobile transmitter is currently required by some federal regulatory bodies in order to reduce the potential for fraud by changing the ESN.

When all the subscriber data for authorization and authentication is stored on the H323_UIM, UIM-based roaming can be easily supported without additional network requirements. However, storing the mobile station identity (MSID) on the H323_UIM and the ESN on the mobile equipment makes it difficult to support UIM-based roaming in ANSI-41 networks because the MSID and ESN used for authentication, encryption, and voice privacy may not match the MSID and ESN combination

stored in the HLR/AC for the subscriber. Options may exist in the future to modify the current ESN usage in ANSI-41 networks. These options include:

1)   changing the role of the ESN in authentication, encryption, and voice privacy;

2)   allowing the ESN to be resident on the UIM with the mobile station identification; and

3)   adding the IMEI to ANSI-41.

There are benefits and drawbacks to each option.

In order to allow for flexibility in implementing a solution to allow UIM-based roaming in ANSI-41, the H.246 AnnexE2 H323_UIM Terminal shall support the following method of using the ESN:

1)   The H323_UIM Terminal shall contain an ESN.

2)   The H323_UIM shall contain a SIM Electronic Serial Number (SESN) of the same length as the ESN. ***The SESN shall be permanently loaded by the H323_UIM Terminal manufacturer and shall not be alterable by any means***. This SESN will not necessarily be related to any manufacturer or assigned by the ITU/TIA.

3)   The SIM shall contain an ESN Usage Indicator (EUI) that determines how the ESN and SESN are used for security and identification. Security refers to the methods used to authenticate a mobile station and provide encrypted data (user and signalling) and voice communications. Identification refers to the method of reporting the H323_UIM mobile equipment to the network. The EUI field shall be protected from unauthorized programming. It shall identify to the mobile station which of the following modes of operation to use:

Mode 1   Use the ESN on the mobile equipment for security and identification.

Mode 2   Use the SESN on H323_UIM for security and the ESN on the mobile equipment for identification.

Mode 3   Use the SESN on the H323_UIM for security and identification.

Due to fraud prevention in existing legacy systems and pending regulatory issues, initial H.246 AnnexE2 mobile equipment shall not support Mode 3 operation. In the event that the EUI on the H.323_UIM is programmed to Mode 3, the mobile station shall default to Mode 1 operation.

E2.11.2 ANSI-41 mode support

With respect to IS-751, the mobile station identity (MSID) is tied to a specific ESN. This fixed MSID-ESN combination is used to validate the subscriber when the subscriber accesses the network. For AnnexE2_GK H323_UIM Terminals, the mobile station identity for ANSI-41 mode shall reside on the UIM. To support UIM-based roaming for an H.246 AnnexE2 subscriber operating in ANSI-41 mode when:

•   the ESN remains solely with the mobile equipment (ME);

•   the ESN Usage Indicator (EUI) indicates Mode 1 operation; and

•   the SIM Electronic Serial Number (SESN) is not used.

The ANSI-41 HLR/AC and H.246 AnnexE2_GK for ANSI-41 operation shall support the following capabilities:

1)   UIM-based roaming support for ANSI-41 operation is a service provisionable option in the HLR/AC and AnnexE2_GK for the ANSI-41 subscriber.

2)   Both the home network and AnnexE2_GK authentication centre (AC) for ANSI-41 operation shall disable the initial validation of the MSID-ESN combination when the subscriber first accesses the network for registration. Instead, the AC shall use the reported, dynamic ESN when performing CAVE processing upon registration. If CAVE authentication upon registration is successful based on the reported, dynamic ESN, the AC

shall store this ESN as the current, validated ESN. MSID-ESN validation during subsequent network access attempts shall be performed based on the current, validated ESN.

3) When an ANSI-41 native subscriber registers in H.323 foreign mode, an initially provisioned, fixed ESN for this subscriber shall always be passed from the AnnexE2_GK to the subscriber's HLR. The HLR shall always authorize subscriber registration using this fixed ESN.

4) Both the home network HLR and AnnexE2_GK HLR emulation for ANSI-41 operation shall perform MSID-ESN validation based on the results of subscriber authentication upon registration. If authentication upon registration is successful based on any reported, dynamic ESN, that ESN shall then be stored as the current, validated, dynamic ESN. Subsequent MSID-ESN validation at the AnnexE2_GK HLR shall be performed based on the current, validated, dynamic ESN. Subsequent MSID-ESN validation at the home network HLR shall be performed based on either the initial provisioned, fixed ESN or the current, validated dynamic ESN. Any validated, dynamic ESN shall remain indefinitely as an authorized ESN for this subscriber until a newly reported ESN has been successfully used for authentication upon registration.

E2.11.3 Automatic call delivery

After successful registration in either ANSI-41 or H.323 foreign mode, incoming calls to the subscriber will be automatically delivered from the home network. The AnnexE2_GK shall query the serving network to obtain a Temporary Local Directory Number (TLDN) or Mobile Station Routing Number (MSRN) to provide back to the gateway or originating MSC in order to route the call to the serving network. In cases where the TLDN is not provided in international E.164 format, the AnnexE2_GK shall provide the necessary numbering plan conversion when mapping to and from the MSRN.

E2.11.4 Supplementary Service Feature Control

Subscribers shall transparently activate and use supplementary services without any regard or knowledge of the type of network which is being accessed, whether it be ANSI-41 or H.323 network.

E2.11.5 H.323 foreign mode support

When the subscriber invokes a supplementary service control in an H.323 network, the mobile station shall relay the requested action by issuing a REGISTER operation to the serving MSC, indicating the supplementary service action that is requested. The serving MSC shall initiate the appropriate H.225.0 operation or request to the subscriber's HLR.

In the case of an ANSI-41 native subscriber roaming in H.323 foreign mode, this H.225.0 operation or request shall be directed to the AnnexE2_GK. The AnnexE2_GK shall translate this request to an ANSI-41 FeatureRequest operation, populated with the appropriate *FC dialled digit string, and send this query to the HLR for the ANSI-136 subscriber. Once a return result or acknowledgement is received from the HLR, the AnnexE2_GK shall provide the appropriate acknowledgement back to the AnnexE2_GK serving MSC.

Typical call flows for supplementary service control in H.323 foreign mode are provided with the call forwarding description in ITU-T Rec. H.450.

E2.11.6 Feature code mapping

In order to support supplementary service feature control in foreign mode, the AnnexE2_GK shall map feature control requests to specific feature codes, and vice versa. A common set of supplementary service feature codes has not been implemented across all ANSI-41-based networks.

In some cases, A-side cellular networks, B-side cellular networks, and CDMA/ANSI-136 networks in the 1900 MHz hyperband (PCS) may use different feature code sets.

To best enable interoperability, the use of standard ANSI TIA/EIA-660 feature codes is recommended. The feature codes defined in Table E2.3 shall be recognized and used by the network for feature control interoperability.

Table E2.3/H.246 – Feature codes for Supplementary Service Feature Control

Supplementary Service Feature Control	Associated ANSI-660 Feature Code (FC)
Call Waiting Deactivation (per Call)	700
Call Forwarding Unconditional Activation	72
Call Forwarding Unconditional Deactivation	720
Call Forwarding Busy Activation	90
Call Forwarding Busy Deactivation	900
Call Forwarding No Answer Activation	92
Call Forwarding No Answer Deactivation	920

In most cases, these standard feature codes should not conflict with other existing feature code sets. Therefore, operators should be able to support these feature codes in addition to existing feature code sets.

Supplementary services shall be controlled and activated within ANSI-41-based networks using ANSI-660 feature codes and dialled digit strings as indicated in Table E2.4. When an ANSI-41 subscriber requests these feature controls in H.323 foreign mode, the AnnexE2_GK shall transmit these dialled digit strings to the HLR.

Table E2.4/H.246 – Dialled digit string for Supplementary Service Feature Control

Supplementary Service Control Request	Dialled Digit String in FeatureRequest
Call Forwarding Unconditional Activation – activate and register	*72 + forwarded-to number
Call Forwarding Unconditional Activation – activate only	*72
Call Forwarding Unconditional Deactivation	*720
Call Forwarding Busy Activation – activate and register	*90 + forwarded-to number
Call Forwarding Busy Activation – activate only	*90
Call Forwarding Busy Deactivation	*900
Call Forwarding No Answer Activation – activate and register	*92 + forwarded-to number
Call Forwarding No Answer Activation	*92
Call Forwarding No Answer Deactivation	*920

In order to allow different feature code implementations, the AnnexE2_GK shall allow for the storage of a Supplementary Service Feature Code Table consisting of one set of feature codes to be populated by the home service provider. The Supplementary Service Feature Code Table shall consist of entries supported in the H.323/ANSI-41 Common H.323 and Mobile Terminal Specification. If the Supplementary Service Feature Code Table is not populated, the AnnexE2_GK shall default to the use of standard ANSI TIA/EIA-660 feature codes.

E2.11.7 Call Barring and Operator Determined Barring

For an ANSI-41 native subscriber, operator control of incoming or outgoing calls, as well as roaming authorization, can also be provided by the subscriber's HLR.

E2.11.8 Outgoing Call Barring (Supplementary Service and ODB)

The following outgoing call barring capabilities shall be mapped in H.323 foreign mode:

• Barring of all outgoing calls (BAOC);

• Barring of outgoing international calls (BOIC);

• Barring of outgoing international calls except those directed to the Home Public Land Mobile Network (HPLMN) country (BOIC-exHC).

The mapping of ANSI-41 outgoing barring conditions in H.323 foreign mode (see Table E2.5) shall be performed according to the ANSI-41 OriginationIndicator is a parameter provided from the HLR to the VLR in the subscriber profile to designate which types of outgoing calls are authorized.

Table E2.5/H.246 – H.323 foreign mode mapping for Outgoing Call Barring

H.323 Call Barring Feature	Corresponding ANSI-41 OriginationIndicator
Bar all outgoing calls (BAOC)	Origination denied
Bar all international calls (BOIC)	National long distance (which includes local calls)
Bar all international calls except to HPLMN country (BOIC-exHC)	National long distance (which includes local calls)

E2.11.9 Incoming Call Barring (Supplementary Service and ODB)

Barring of incoming calls is controlled and invoked by the subscriber's HLR. The invocation of barring all incoming calls (BAIC) shall be supported in H.323 foreign mode. To support the invocation of barring all incoming calls when roaming outside the HPLMN country (BIC-Roam), the AnnexE2_GK shall provide a specific serving system or Visited Public Land Mobile Network (VPLMN) identifier to the ANSI-41 HLR when the subscriber registers in H.323 foreign mode. Each H.246 AnnexE2 serving system shall be uniquely identified with an appropriate E.164 address to the ANSI-41 HLR.

E2.11.10 Operator Determined Barring of Roaming

Operator determined barring of roaming is controlled by the ANSI-41 HLR. To support this feature, the AnnexE2_GK shall provide a specific serving system or VPLMN identifier to the ANSI-41 HLR when the subscriber attempts to register in H.323 foreign mode. Upon invocation of this feature, the GSM HLR shall deny registration. The degree of granularity to which roaming can be denied (e.g. roaming outside home PLMN country) will be determined by the HLR capabilities.

E2.11.11 Registration and Activation

ANSI-41 native subscribers can only register or activate call forwarding no reply (CFNR) in native mode, rather than CFNRy and CFNRc individually. Therefore, the registration or activation of either CFNRc or CFNRy in H.323 foreign mode shall result in registration or activation of CFNR. If either CFNRc or CFNRy is registered or activated in H.323 foreign mode, the other feature shall be registered or activated as well.

In H.323 foreign mode, the AnnexE2_GK shall query the HLR of the ANSI-41 subscriber with the Transfer to Number Request if either call forwarding busy (CFB) or CFNR is registered. The resulting forwarded-to numbers shall be provided to the AnnexE2_GK VLR to support early invocation of CFNRc and non-optimal routing for late call forwarding.

E2.11.12   Optimal routing for Late Call Forwarding

The AnnexE2_GK shall support the invocation of optimal routing for late call forwarding in H.323 foreign mode. With this capability, the AnnexE2_GK will receive a Resume Call Handling message from the H.246 AnnexE2 serving MSC and generate a Redirection Request to the ANSI-41 serving MSC. If a return error is received as a result of the Redirection Request INVOKE, the AnnexE2_GK will reject the Resume Call Handling request from the H.246 AnnexE2 serving MSC, causing the H.246 AnnexE2 serving MSC to forward the call using non-optimal routing.

E2.11.13   SMS Teleservice Support

The AnnexE2_GK with H.323 Annex K capabilities shall provide interworking between ANSI-41 SMS and H323_UIM Terminal for mobile originated and mobile terminated short messaging. When an ANSI-41 Forward Short Message (FSM) is delivered to the AnnexE2_GK, the AnnexE2_GK will convert it to an H.323 Annex K Service Control message carrying ANSI-41 Short Message data and deliver it through the H.323 network. Similarly, when a Short Message is originated from H323_UIM Terminal, an H.323 Annex K service control message is delivered to the AnnexE2_GK, the AnnexE2_GK will convert it to an ANSI-41 FSM and deliver it through the ANSI-41 network.

E2.11.14   Message Waiting Notification

The H323_UIM Terminal and AnnexE2_GK shall support delivery of Message Waiting Notification (MWN) from ANSI-41 network by converting the ANSI-41 MWN information into H.450.7 MWN information.

E2.11.15   Emergency Service

The AnnexE2_GK does not perform any direct role in the routing or completion of emergency calls from H323_UIM mobile stations. However, the ANSI-41 and H.323 serving networks provide "pass through" capability to ensure that the call will be routed and offered to a Public Safety Answering Point (PSAP).

Emergency service permits a subscriber to dial an emergency number and be connected to a Public Safety Answering Point (PSAP) to request an emergency response from the appropriate agency (e.g. fire, police, ambulance, poison control centre, or suicide prevention centre).

An emergency call shall bypass any authorization restrictions or call origination restrictions features.

Once the call is answered, the subscriber shall be able to communicate the type of emergency over a normal voice connection with the PSAP. (Encryption shall be removed on the connection to the PSAP.)

An emergency call does impact a subscriber's ability to originate or receive calls while the emergency call is in progress. Supplementary services and features controlled by activating the SEND key (such as Call Waiting, Three-Way Calling, Conference Calling, and Call Transfer) are suspended during the emergency call, except to reconnect a call placed on hold to place the emergency call. When the emergency call is released, the subscriber's normal calling capabilities are restored. Release occurs when either the subscriber or PSAP disconnects.

In ANSI-41 mode, the mobile station shall support the emergency call procedure as described in TIA/EIA-136-123-A. When an emergency call is dialled by the subscriber in ANSI-41 mode, the mobile station shall set the Emergency Call flag in the Origination message. If this flag is set, it indicates an emergency call, and the Called Party Number is ignored by the network.

Emergency calling shall meet all the regulatory requirements imposed by government agencies.

E2.11.16 Location services

It is not required that the H323_UIM Terminal include GPS functionality. Location services can be provided in H.323 and ANSI-41 modes via network solutions.

E2.11.17 WAP services

H323_UIM Terminals that support the Wireless Application Protocol (WAP) shall conform to the following requirements via H.323 Annex K Service Control transport channel. The H323_UIM Terminal shall support WAP as specified by the WAP Forum in the WAP Wireless Datagram Protocol Specification. It is desired that the H323_UIM Terminal support at least WAP 1.2. The bearers for WAP shall be, at a minimum, ANSI-41 SMS, GPRS Packet Data and Over-the-Air or Remote activation and programming. The H323_UIM Terminal shall support WAP Over-the-Air Provisioning (WAP 1.3) when this standard is finalized. The H323_UIM Terminal is not precluded from supporting WAP via the General UDP Transport Service (GUTS) while in ANSI-41 mode.

E2.12 Stage 2 descriptions of ANSI-41 PLMN Interworking and H323_UIM Terminal features

E2.12.1 Operational model and message flows

This clause describes some typical message flows for ANSI-41 PLMN interworking function (AnnexE2_GK) and H323_UIM Terminal function in an H.323 network. The following conventions are used in the figures of this clause.

1)   The following notation is used:

      —————▶   H.323 and ANSI-41 MAP protocol message.
      - - - - ▶   HTTP message.
      ············▶   Informative example primitive (implementation matter).

ANSI-41 MAP, HTTP and RAS messages are capitalized (ANSI-41: REGNOT(invoke), REGNOT(response), HTTP:GET, RAS:ARQ), while H.225.0 call signalling messages are written with the first letters capitalized (Setup). ASN.1 codepoints in H.225.0 are written in bold (**ServiceControlAddress**).

The message parameters shown in the message flow tables, which are shown required (R), mandatory backward compatible (MBC) and optional (O) shall be given the same treatment in including the equivalent H.225.0 MobileUIM parameters in AnnexE2_GK related H.225.0 messages.

The following message flows shown in this annex are not limited, but are shown as example message flows.

Mobility Management areas message flows

•   Registration of H323_UIM Terminal and/or user;

•   Authentication of the H323_UIM Terminal and user.

Communication Management area message flows

•   Call Termination to H323_UIM Terminal from PLMN;

•   Message Waiting Notification delivery to H323_UIM Terminal;

•   Short Message Origination from Short Message Entity in H323_UIM Terminal;

•   Short Message Termination to Short Message Entity in H323_UIM Terminal.

E2.12.2 Registration and Authentication of H323_UIM Terminal messages flow
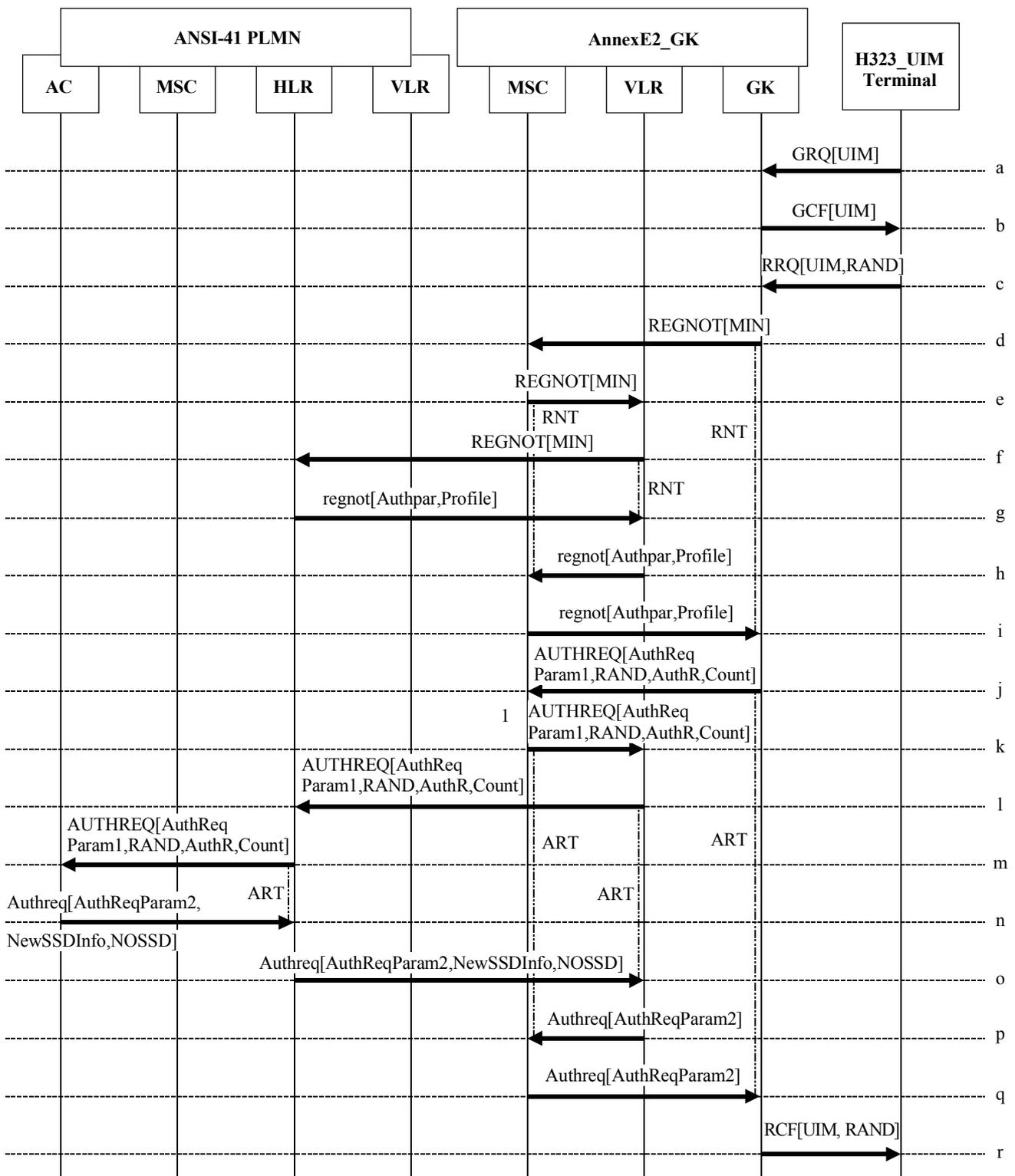
Figure E2.4/H.246 – H323_UIM Terminal Registration and Authentication messages flow

This operation scenario (Figure E2.4) describes the successful use of the GRQ, GCF, RRQ, and RCF interworking with the ANSI-41 PLMN RegistrationNotification, AuthenticationRequest operations to authenticate an H323_UIM Terminal (HUT) which is attempting initial access. The HUT is aware that Registration and Authentication is required on all PLMN system accesses. The result of these operations is to allow access.

a)   The H323_UIM Terminal with Encrypted Mobile User Identity and System Identity multicasts (or uses other methods as described in Appendix IV/H.225.0) a Gatekeeper Request (GRQ) message, asking, "Who is my AnnexE_GK?". This is sent to the AnnexE_GKs well-known Discovery Multicast Address within the PLMN IWF Networks Serving area.

b)   One or more AnnexE_GK may respond with the Gatekeeper Confirmation (GCF) message indicating "I can be your AnnexE_GK.", and returns the Transport Address of the AnnexE_GK Gatekeeper's RAS Channel.

c)   H323_UIM Terminal (HUT) shall send a Registration Request (RRQ) with UIM to an AnnexE_GK. This is sent to the AnnexE_GK's RAS Channel Transport Address. The HUT has the Network Address of the AnnexE_GK from the Gatekeeper discovery process and uses the well-known RAS Channel TSAP Identifier or the TSAP identifier returned in the GCF. The AnnexE_GK converts all the H323_UIM Terminal information to appropriate PLMN information in order to start transactions to PLMN as the serving MSC and servingVLR.

d)   The Gateway/Gatekeeper interworking function sends REGNOT (RegistrationNotification) message to serving MSC within the AnnexE_GK.

e)   The serving MSC determines that a roaming H323_UIM Terminal is within its service area; the serving MSC may detect the HUT's presence through autonomous registration, call origination, call termination or a service order. The serving MSC sends a REGNOT to its VLR the information in Table E2.6 as defined in the ANSI-41 PLMN specifications (refer to ITU-T Rec. X.691).

Table E2.6/H.246 – RRQ (UIM) and REGNOT message parameters

Parameters	Usage	Type
IDInfo:	Set of identification parameters in REGNOT:	
[MIN]	Served MS MIN.	R
[ESN]	Served MS ESN.	R
[MSCID]	Serving MSC MSCID.	R
[PC_SSN]	Serving MSC PC_SSN. Include if SS7 carriage services are used.	O
[LocationAreaID]	For paging served MS. Include if available.	O
[SystemMyTypeCode]	Serving MSC vendor identification.	MBC
QUALCODE	Type of qualification required	R
SYSACCTYPE	Type of system access	R
	System's transaction capability	R
TERMTYP	Identifies the radio frequency interface standard supported by the associated MS	R
AVTYP	Indicates MS is unavailable for normal call delivery, if applicable	O
SMSADDR	Temporary routing address of SMS subscriber, if applicable	O
AuthError:	Parameters included if authentication parameters were requested by the serving MSC but not received from the MTH:	O
[SystemCapabilities]	Authentication capabilities of serving system.	
[ReportType]	Report of missing authentication parameters.	
AccessInfo:	Subscriber's access information. Included if system access is in a border cell. Includes:	O
[ReceivedSignalQuality]	Raw received signal strength from MS for use in multiple access signal strength arbitration.	
[ControlChannelData]	Includes: DCC and CHNO of analog access channel for use in multiple access detection; CMAC for use in signal strength arbitration.	
[SystemAccessData]	Indicates the serving MSC and cell site for use in multiple access detection.	
BORDACC	Indicates that system access is in a border cell, as determined by local procedures.	O

f)   The serving VLR determines that:

i)   either the HUT had previously registered with an MSC within the domain of the VLR but the HUT has been reported inactive by the VLR;

ii)   or the HUT is not known to the VLR;

iii) or the requested information cannot be made available for the indicated HUT.

Under these conditions, the serving VLR forwards the REGNOT to the HLR associated with the HUT.

Table E2.7/H.246 – VLR → HLR REGNOT message parameters

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

g) The HLR determines that authorization can be granted to the HUT. It returns the requested information to the serving VLR in the REGNOT.

Table E2.8/H.246 – HLR → VLR regnot message parameters

Parameters	Usage	Type
AUTHPER	Authorization confirmed indication with period of authorization.	O
MYTYP	VLR vendor identification.	MBC
Profile:	Subscriber's profile information. Include if profile requested in QUALCODE:	O
[CallingFeatures-Indicator]	Authorization and activity states for features.	
[OriginationIndicator]	Type of calls MS is allowed to originate.	
[Digits(Restriction)]	Selected leading digits or full Directory Number allowed for call origination as indicated in OriginationIndicator. Include if applicable.	
[Termination-RestrictionCode]	Type of calls MS is allowed to terminate.	
HLRID [MSCID]	HLR MSCID to key MS record against a subsequent UnreliableRoamerDataDirective.	R
[Digits(Carrier)]	Indicates MS's preferred IC, if applicable.	
[RoutingDigits]	Special routing instructions, if applicable.	
[Geographic-Authorization]	Include if applicable.	
[Authentication-Capability]	Include if authentication of the HUT is required.	
[DMH_AccountCode-Digits]	Include if applicable.	
[DMH_AlternateBillingDigits]	Include if applicable.	
[DMH_BillingDigits]	Include if applicable.	
[MobileDirectory-Number]	Include if applicable.	
[MessageWaiting-NotificationCount]	Include if MessageWaitingNotificationType is *Count Indication*.	
[MessageWaiting-NotificationType]	Include if Message Waiting Notification feature is active and an action is required.	
[OriginationTriggers]	Origination trigger points currently active for the subscriber. Include if applicable.	
[PACAIndicator]	Indicates the PACA permanent activation status and priority level assigned to the subscriber, if applicable.	
[PreferredLanguage-Indicator]	Indicates the preferred language associated with the subscriber, if applicable.	
[SMS_Origination-Restrictions]	Defines the type of messages the MS is allowed to originate, if applicable.	
[SPINIPIN]	Indicates Subscriber's PIN, if applicable.	
[SPINITriggers]	SPINI trigger points currently active for the subscriber. Include if applicable.	
[SMS_Termination-Restrictions]	Defines the type of messages the MS is allowed to terminate, if applicable.	
[TerminationTriggers]	Termination trigger points currently active for the subscriber. Include if applicable.	

h)   The VLR forwards the regnot to the serving MSC.

Table E2.9/H.246 – AnnexE2_GK (VLR → MSC) regnot message parameters

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

i)   The serving MSC inturn forwards the regnot with subscriber profile information into the interworking function of Gateway/Gatekeeper.

j)   On this initial access attempt by an authentication-capable HUT, the interworking function of Gateway/Gatekeeper sends an AUTHREQ to the serving MSC.

Table E2.10/H.246 – AnnexE2_GK (GK→MSC) AUTHREQ message parameters

Parameters	Usage	Type
AuthReqParameters1:	Set of parameters in AUTHREQ:	
[MIN]	Served MS MIN.	R
[ESN]	Served MS ESN.	R
[MSCID]	Serving MSC MSCID.	R
[PC_SSN]	Serving MSC PC_SSN. Include if SS7 carriage services are used.	O
[SystemCapabilities]	Authentication capabilities of the serving MSC.	R
[SystemAccessType]	Type of system access = registration.	R
[TerminalType]	Identifies the radio frequency interface standard supported by the associated MS	R
RAND	Random number derived from the HUT-provided RANDC by the serving MSC.	R
AUTHR	Authentication result provided by the HUT.	R
COUNT	Value of CallHistoryCount provided by the HUT.	R

k)   The serving MSC sends an AUTHREQ to the serving VLR with all parameters shown in Step j).

l)   The VLR sends an AUTHREQ to the HLR associated with the HUT.

Table E2.11/H.246 – AnnexE2_GK (VLR) → HLR AUTHREQ message parameters

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

m)   The HLR forwards the AUTHREQ to the AC. Parameters are as in Step k).

n)   The AC determines that the HUT should be allowed access. The AC sends an authreq to the HLR.

Table E2.12/H.246 – AuC→ HLR authreq message parameters

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

o)   The HLR forwards the authreq to the serving VLR. Parameters are as in Step n).

p)   The serving VLR forwards the authreq to the serving MSC. Parameters are as in Step n), with the exception that the SSD, AAV and NOSSD parameters are not included.

q)   The serving MSC sends the authreq to interworking function Gateway/Gatekeeper to allow complete the authentication of the H323_UIM Terminal.

r)   The AnnexE_GK's Gatekeeper shall send Registration Confirmation (RCF) with AuthReqParam2 set of parameters to the H323_UIM Terminal indicating the successful registration and Authentication of H323_UIM Terminal in the AnnexE_GK PLMN area. After this step the HUT is ready to access Mobile Services from all preferred Service Providers PLMN and H.323 networks.

E2.12.3 Authentication of subscriber using PIN to invoke services message flow
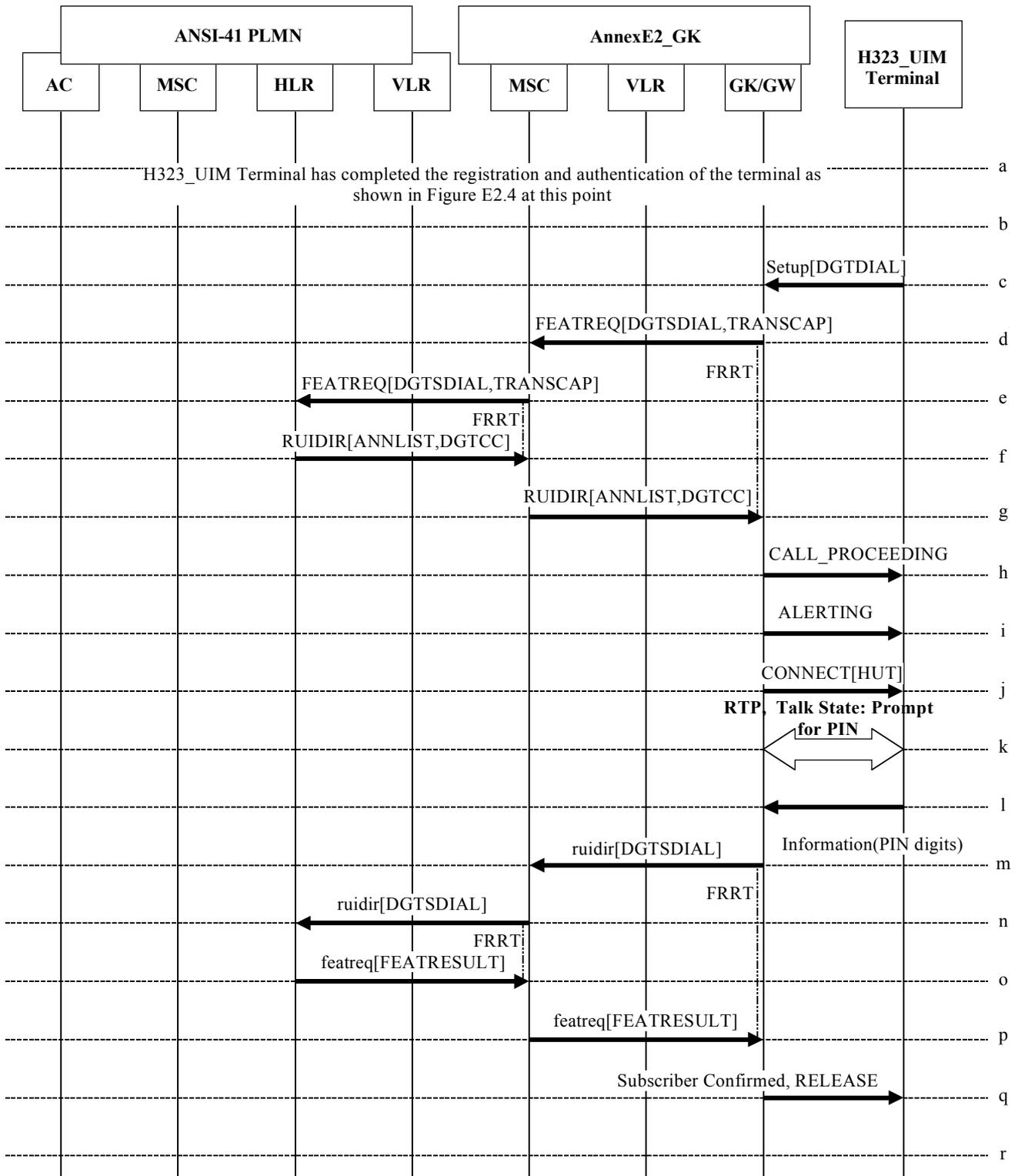
Figure E2.5/H.246 – Authentication of Subscriber using PIN messages flow

This operation messages flow in Figure E2.5 describes the successful use of the Q.931 messages (Setup, Call_proceed, Alerting, Connect, Release Complete and Information) interworking with ANSI-41 PLMN FeatureRequest (FEATREQ), RemoteUserInteractionDirective (RUIDIR) operation to authenticate a H323_UIM Subscriber, who is attempting initial mobile service access.

The Mobile subscriber is aware that authentication using PIN is required on all PLMN Service accesses. The result of these operations is to provide access to subscribed and active mobile users.

a)   Discover the Mobile Gateway using GRQ, GCF operations.

b)   Registration and Authentication of the H323_UIM Terminal using RRQ, RCF operations. Steps a) to b) functions, which are shown in Figure E2.1 are successfully completed at this point of the scenario.

c)   The H323_UIM Terminal with Encrypted Mobile User Identity and System Identity dials feature code digits (e.g. *1234), a Setup Message with Digits Dialled is sent from the HUT to AnnexE_GK (Mobile Gatekeeper).

d)   Mobile Gateway/Gatekeeper interworking function in AnnexE_GK detects the feature code in the SETUP message from the H323_UIM and sends a PLMN operation FeatureRequest with Dialled Digits to initiate subscriber authentication on PLMN.

e)   The serving MSC sends the FEATREQ to the HLR associated with the H323_UIM Subscriber. The TransactionCapability parameter is also included in the FEATREQ, indicating that the serving MSC supports receiving RUIDIRs.

f)   The HLR recognizes the dialled digits as a feature registration with a forward-to or diversion termination address that matches a SPINI Trigger. The HLR send a RUIDIR to the serving MSC.

g)   On receipt of the RUIDIR, the serving MSC turns off the FEATREQ timer (FRRT) and forwards the FEATREQ message to the IWF of H.323 Gateway/Gatekeeper in order to provide call treatment as indicated in the received message. In this case, the treatment is to answer the call (i.e. connect the calling party to the subsystem capable of user interaction), and prompt the user based on the information in the received RUIDIR (in the DigitCollectionControl parameter) and wait for digits.

h)   The AnnexE_GK sends the CallProceeding message to the H323_UIM Terminal (HUT).

i)   The AnnexE_GK sends the Alerting message to the HUT.

j)   The AnnexE_GK also sends the Connect message to the HUT.

k)   The HUT and AnnexE_GK are in Talk State with RTP media, The AnnexE_GK-IVR prompts the user for PIN.

l)   The user responds with the authentication PIN, which is sent in **Information (collected digits)** from HUT to AnnexE_GK.

m)   The IWF H.323 Gateway/Gatekeeper takes the collected digits and sends it to the serving MSC function in ruidir operation.

n)   The serving MSC sends a ruidir to the HLR and includes the digits dialled by the user. The serving MSC restarts the FRRT Timer.

o)   The HLR updates the served MS's feature registration information and sends a featreq including the FeatureResult parameter indicating successful feature operation to the Serving MSC.

p)   The Serving MSC turns off the FEATREQ timer (FRRT) and provides treatment to the served HUT as indicated in the received featreq. In this case, the treatment is to provide feature confirmation and release the call.

q)   The AnnexE_GK updates the subscriber confirmed profile and sends the Release Complete message to the HUT to teardown the call.

r)   The HUT subscriber is now ready to use Mobile Services until Deregistration of the Terminal and user.

E2.12.4 H323_UIM Terminal powers off

If a H323_UIM Terminal powers off while operating in ANSI-41 foreign mode (H.323 network), the AnnexE2_GK receives an MS INACTIVE message from the serving VLR. This results in the AnnexE2_GK setting the "IMSI Detached" Flag. If the H323_UIM Terminal remains inactive for an extended period of time (determined by operator), the AnnexE2_GK may delete the subscriber record associated with that H323_UIM Terminal and send an MS Purge (mobile station purge) to the HLR.

E2.12.5 H323_UIM Powers On

If a H323_UIM Terminal powers on and registers on an AnnexE2_GK (serving MSC/VLR), while operating in ANSI-41 foreign mode, normal registration procedures apply.

E2.13 Automatic call delivery

Automatic call delivery is invoked when an incoming call attempt arrives for a subscriber who is roaming. Call delivery scenarios for the case in which an ANSI-41 subscriber is roaming in an H.323 network is provided.

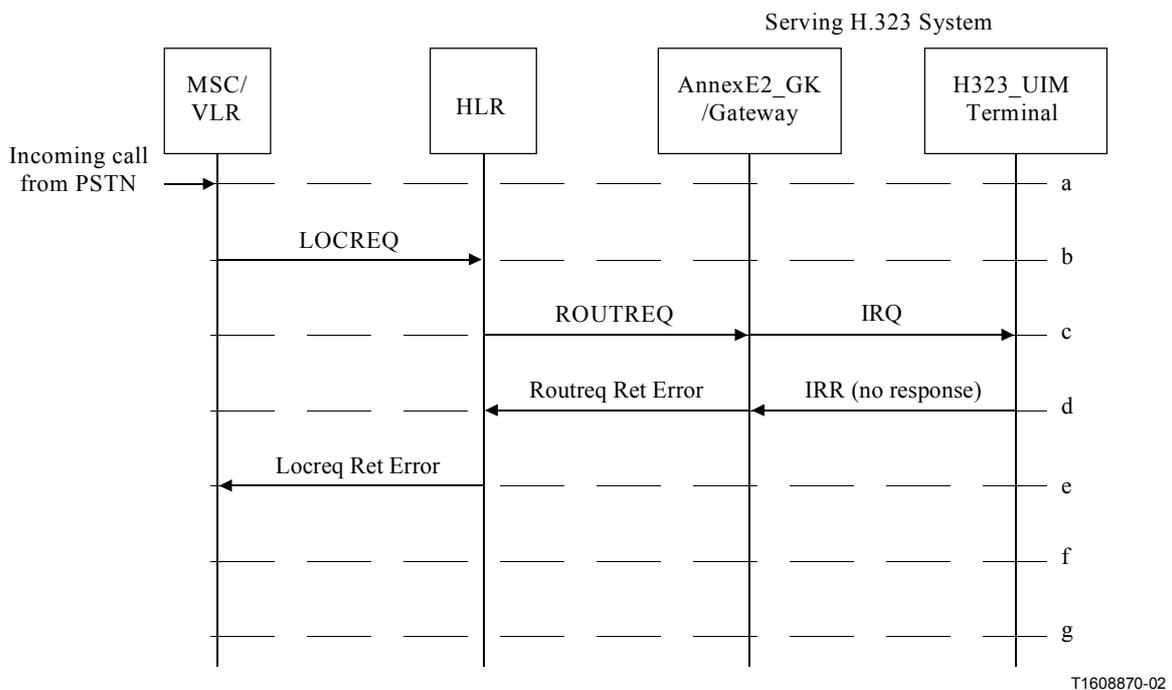### E2.13.1 Call delivery to ANSI-41 subscriber roaming in H.323 network
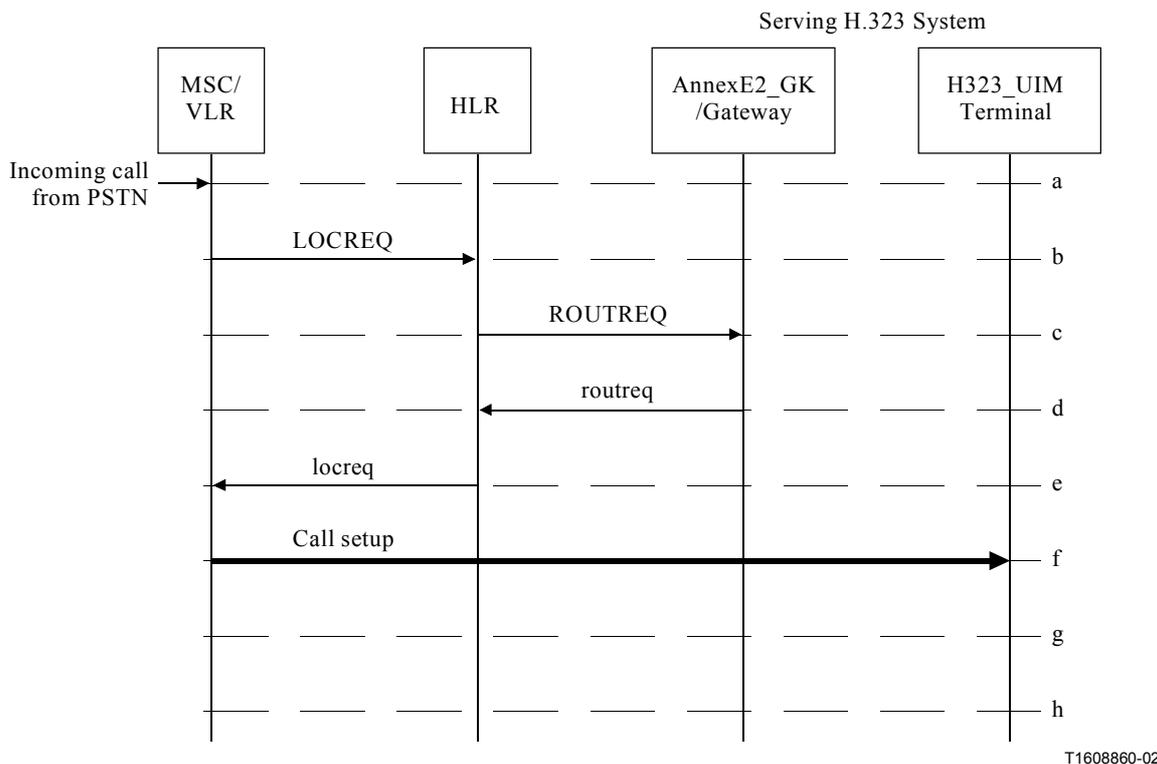
Figure E2.6/H.246 – Call delivery to ANSI-41 subscriber roaming in an H.323 network

a)   A call origination and the dialled MS address digits (i.e. directory number) are received by the Originating MSC from the PSTN destined to a subscriber to the ANSI-41 network.

b)   The Originating MSC sends a LOCREQ to the HLR associated with the called subscriber; this association is made through the dialled MS address digits.

c)   The HLR sends a ROUTREQ to the AnnexE2_GK emulating the VLR where the H323_UIM associated with MS is registered.

d)   The AnnexE2_GK returns a routreq message to the HLR that includes a TLDN (Temporary Local Directory Number), set to the received MSRN, in the Digits (Destination) parameter. Note that the MSRN is always in international format. It is assumed that the gateway MSC on the ANSI-41 side is capable of supporting internationally formatted TLDNs.

e)   When the routreq is received by the HLR, it returns a locreq to the Originating MSC. The locreq includes routing information in the form of the TerminationList parameter, along with an indication of the reason for extending the incoming call (i.e. for Call Delivery, in this case) in the DMH_RedirectionIndicator parameter.

f)   Upon receiving the locreq, the Originating MSC sets up a voice path to the Serving H.323 Network's AnnexE2_GK (using a protocol such as SS7 ISUP and H.225.0 Call Control messages).

E2.13.2   Delivery to an ANSI-41 subscriber roaming in an H.323 Network – Unsuccessful case

In the following scenario in Figure E2.7, call delivery to an ANSI-41 subscriber roaming in an H.323 network fails because the user does not answer a page sent by the serving system during the processing of the Provide Roaming Number message, and call forwarding is not active for the subscriber.

Figure E2.7/H.246 – Unsuccessful call delivery to an ANSI-41 subscriber roaming in an H.323 network

a)   A call origination and the dialled MS address digits (i.e. directory number) are received by the Originating ANSI-41 MSC from the PSTN destined to a subscriber to the ANSI-41 network.

b)   The Originating ANSI-41 MSC sends a LOCREQ message to the ANSI-41 HLR associated with the called subscriber; this association is made through the dialled MS address digits.

c)   The ANSI-41 HLR sends a ROUTREQ message to the AnnexE2_GK emulating the VLR where the H323_UIM associated MS is registered. If necessary, mapping from IMSI to MIN is done beforehand by the AnnexE2_GK. Also, AnnexE2_GK sends an IRQ (Information Request) message to the H323_UIM Terminal to get the status of the terminal for call delivery.

d)   The AnnexE2_GK sends a RoutingRequest RETURN ERROR message with the error code set to *ResourceShortage* to the subscriber's ANSI-41 HLR after getting IRR (no response) from the H323_UIM Terminal.

e)   The ANSI-136 HLR sends a LocationRequest RETURN ERROR message to the Originating ANSI-136 MSC with the *SystemFailure* error code.

With respect to other call delivery failure cases, Table E2.13 describes the following preferred mapping between H.323 and ANSI-41. Note that the response the AnnexE2_GK sends to the ANSI-41 HLR may differ based on the error code received from the H.323 AnnexE2_GK (VLR/MSC).

Table E2.13/H.246 – ANSI-41 PLMN and H.323 networks call delivery Roaming User error handling

H.246 AnnexE2_GK Return Error User Error	AnnexE2_GK response to ANSI-41 HLR's ROUTREQ
Absent Subscriber	routreq with AccessDeniedReason set to *Unavailable*
No Routing Number Available	RETURN ERROR with Error Code set to *ResourceShortage*
OR Not Allowed	*(Outside of the scope of the Call Delivery capability for GAIT Phase 1.)*
Facility Not Supported	RETURN ERROR with Error Code set to *SystemFailure*
System Failure	RETURN ERROR with Error Code set to *SystemFailure*
Data Missing	RETURN ERROR with Error Code set to *System Failure*
Unexpected Data Value	RETURN ERROR with Error Code set to *System Failure*

E2.14   Successful Mobile Terminating ANSI-136 Short Message Service (CMT) mapped to H.323 Annex K Service Control message
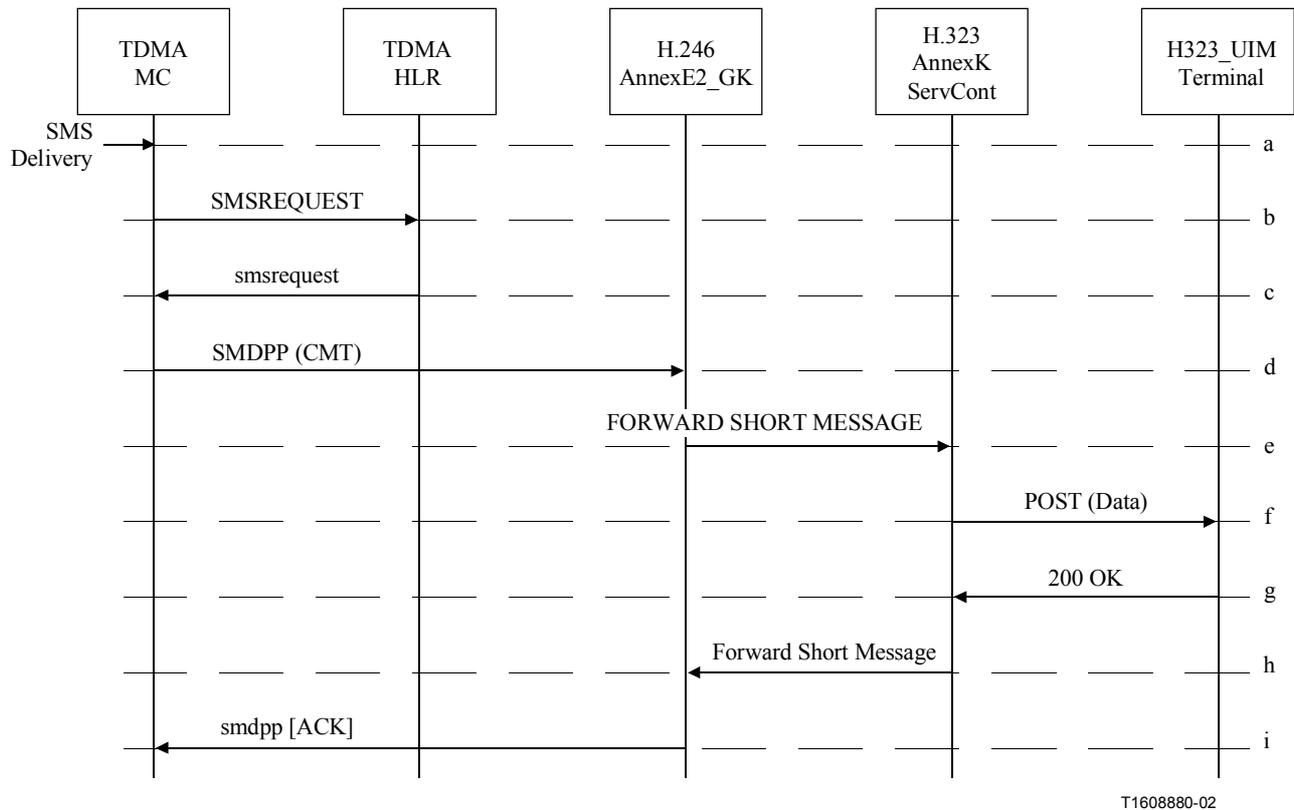
Figure E2.8/H.246 – Short Message Delivery to Subscriber's H323_UIM Terminal while roaming in H.323 network

a)   The ANSI-41 Message Centre (MC) receives a short message for a specific subscriber.

NOTE – This step is shown for completeness only and is not repeated in subsequent call flows.

b)   The Message Centre sends an SMS Request message to the ANSI-41 HLR of the short message recipient to request a routing address for delivering the short message to that subscriber.

c)   Since the subscriber has a current valid location stored in the HLR, the HLR returns it to the MC in the SMS Request Return Result message.

d)   The Message Centre then sends a Short Message Delivery Point to Point message to the H.246 AnnexE2_GK, which is seen as the current serving ANSI-41 MSC/VLR for that subscriber. Note that in this case, the format used by the MC is the CMT format (Cellular Messaging Transport).

e)   Upon reception of the Short Message Delivery Point-to-Point message from the ANSI-41 MC, the AnnexE2_GK originates a FORWARD SHORT MESSAGE to the Service Centre Server after having translated the short message into H.323 Annex K Service Control format.

f)   The Service Control Server sends the POST (Data) message to the H323_UIM Terminal.

g)   The H323_UIM Terminal acknowledges the delivery of the short message with response 200 OK message.

h) The Service Centre Server sends the result of the Forward Short Message to the AnnexE2_GK.

i) The AnnexE2_GK sends the result of the Short Message Delivery Point to Point to the ANSI-41 Message Centre.

E2.14.1 Error handling at the reception of a Forward Short Message in the H.246 AnnexE2_GK

1) If a mandatory parameter is missing (MAP V2), a **Forward Short Message Return Error** with the indication "Data Missing" is sent back to the SMS-GMSC.

2) If a mandatory parameter is missing (MAP V1), a **Forward Short Message Return Reject** with the indication "Mistyped Parameter" is sent back to the SMS-GMSC.

3) A **Forward Short Message Return Reject** with the problem code "Mistyped Parameter" is sent in the following cases:

   a) A parameter tag is not one of those associated with the operation.

   b) The received value is not a value of the type associated with the operation.

   c) Erroneous tag and length information.

   d) Exceeding of the defined size of an ASN.1 module.

4) If the *SM-RP-DA* parameter does not have an IMSI number, a **Forward Short Message Return Error** with the indication "Unexpected Data Value" is sent back to the SMS-GMSC.

5) If the *SM-RP-OA* parameter does not have an SC, a **Forward Short Message Return Error** with the indication "Unexpected Data Value" is sent back to the SMS-GMSC.

6) If the subscriber is not connected in the IIF or if the profile is not available, a **Forward Short Message Return Error** with the indication "Unidentified Subscriber" is sent back to the SMS-GMSC.

7) If location is unknown or inactive, send back to the SMS-GMSC a **Forward Short Message Return Error** message with the indication "Absent Subscriber".

8) If the subscriber has an ANSI SMS termination restriction, a **Forward Short Message Return Error** message with indication "Facility Not Supported" is sent back to the SMS-GMSC.

9) If the short message contents could not be extracted from the SM-RP-UI parameter, send back to the SMS-GMSC a **Forward Short Message Return Error** message with the indication "System Failure".

E2.14.2 Mapping of H.323 Annex K Service Control message into ANSI-136 SMDPP Message

The ANSI-41CMT, forwarded to the ANSI-41 VLR/MSC as a **SMS Delivery Point-to-Point** message, will contain the following parameters:

1) *MIN*;

2) *ESN*;

3) *SMS Bearer Data* (see below for details);

4) *SMS Teleservice Identifier* (with value CMT or GSM Hosted SMS Teleservice);

5) *SMS Original Originating Address* (with the value received in parameter *Originating Address of* the GSM SMS-DELIVER message).

The *SMS Bearer Data* parameter sent in the message **SMS Delivery Point to Point** is structured as an ANSI-136 SMS-DELIVER message and has the following parameters:

1) *Message Type Indicator* (mandatory): Set to value "SMS-DELIVER";

2)   *Message Reference* (mandatory): Number created by the IIF and increased with each message sent;

3)   *Privacy Indicator* (mandatory): Set to value "Not restricted";

4)   *Urgency Indicator* (mandatory): Set to value "Very Urgent" if parameter *Data Coding Scheme* indicates "class 0 message", otherwise set to value "Normal";

5)   *Delivery Acknowledgement Request* (mandatory): Set to provided value;

6)   *Manual Acknowledgement Request* (mandatory): Set to provided value;

7)   *Message Updating* (mandatory): Set to value "New (do not overwrite)";

8)   *Validity* (mandatory): Set to value "Indefinite";

9)   *Display Time* (mandatory): Set to value "Default";

10)   *User Data Unit* (mandatory): It contains the message itself and it is structured in the following way:

   10.1)   Least Significant Byte of Length: Length of message.

   10.2)   Encoding Identifier: Set to value "IRA" if received message is in GSM default alphabet; otherwise, set to value "User Specific".

   10.3)   Length Modifier: Set to value "0".

   10.4)   User Data Structure Type: Set to value "00".

   10.5)   User Data: The ANSI-41 SMS message (parameter User Data). If encoding Identifier has value "IRA" translate short message to the ANSI-136 IRA alphabet.

E2.15   Message Waiting Notification

E2.15.1   H323_UIM Terminal in ANSI-41 Mode

For a native ANSI-41 subscriber roaming in an H.323 environment, there can be two events that trigger the H.246 AnnexE2_GK to send the Message Waiting Notification (MWN) using the H.450.7 Message Waiting Notification (MWN) to the H323_UIM Terminal. The first one is at registration (location update): if there is an indication in the ANSI-41 HLR that messages have been delivered to the subscriber's voice mail box, the ANSI-41 HLR will indicate that in the Registration Notification Return Result message. This will trigger the H.246 AnnexE2_GK to send an H.450.7 MWN information. The second event is when the HLR receives a Message Waiting Notification for a subscriber that is already registered. In this case, the ANSI-41 HLR will send a Qualification Directive message to the H.246 AnnexE2_GK which will translate it into a H.450.7 with MWN indication.

E2.15.2 MWN via ANSI-41 Qualification Directive message mapped to H.450.7 MWN
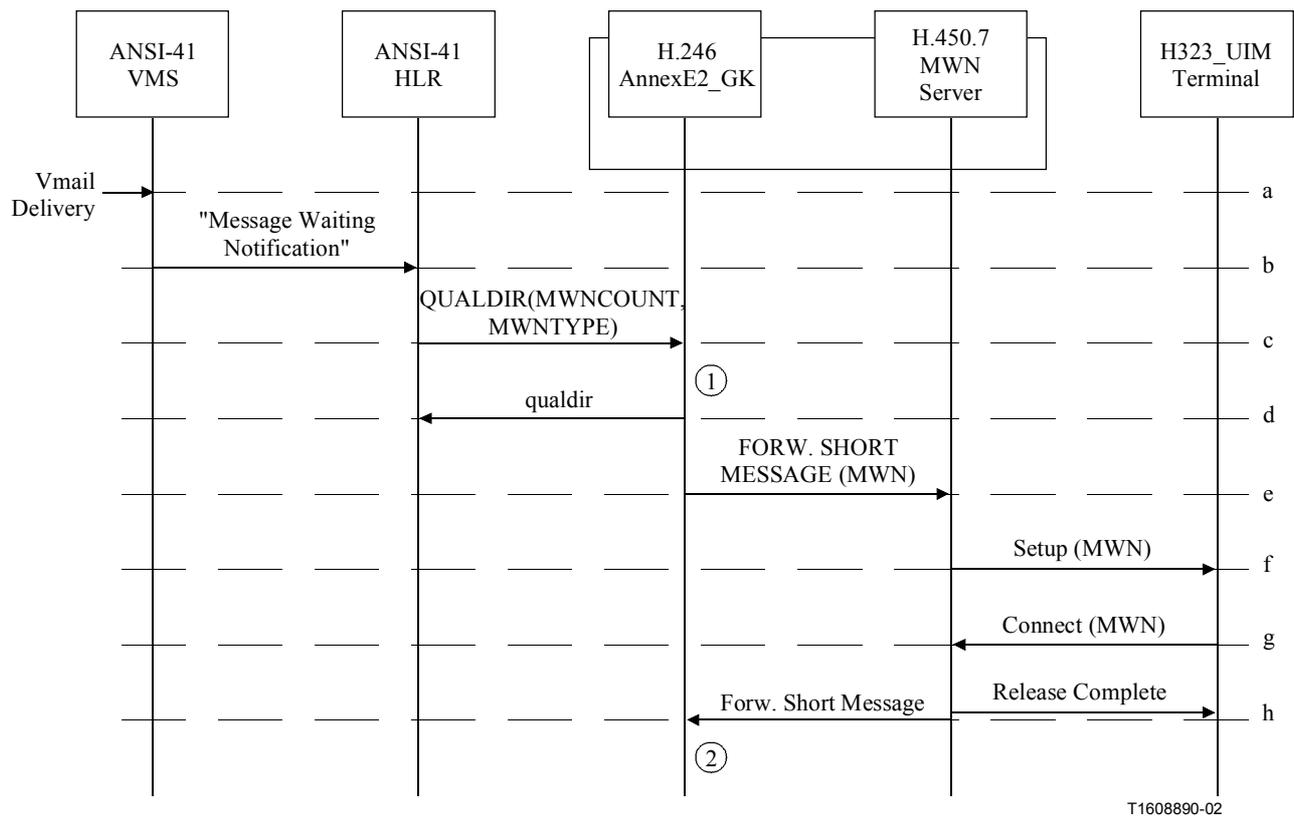
Figure E2.9/H.246 – Message Wait Notification for the ANSI-41 Subscriber roaming in H.323 Networks messages flow

a) The ANSI-41 Voice Mail System (VMS) receives a voice mail for a specific subscriber.

b) The ANSI-41 VMS sends the "Message Waiting Notification" (MWN) to the ANSI-41 HLR of the voice mail recipient. Note that the interface between the ANSI-41 VMS and the ANSI-41 HLR is not standardized in ANSI-41-D.

c) Since the subscriber has a current valid location stored in the HLR, the HLR initiates a Qualification Directive message with the MWN information to the AnnexE2_GK/H.450.7 Server acting as the serving ANSI-41 MSC/VLR. The MWN information consists of two parameters: MessageWaitingNotificationCount (MWNCOUNT) and MessageWaitingNotificationType (MWNTYPE). For a description of these parameters, refer to the ANSI-41-D specifications (EIA/TIA-41-5-D), Chapter 5 (Signalling Protocols), Sections 6.5.2.78 and 6.5.2.79.

① At this point, the AnnexE2_GK/H.450.7 Server sets the MWN flag. This is an indication that Message Waiting Notification is to be delivered to the H323_UIM Terminal.

d) The AnnexE2_GK/H.450.7 Server sends the result of the Qualification Directive message to the ANSI-41 HLR.

e) The AnnexE2_GK/H.450.7 Server converts the ANSI-41 MWN information into H.450.7 MWN format

f) The serving AnnexE2_GK/H.450.7 Server sends the Setup message with the MWN information to the H323_UIM Terminal.

g) The H323_UIM Terminal acknowledges the delivery of the MWN information and removes the MWN flag and replies with Connected (MWN) message.

h)   The serving AnnexE2_GK/H.450.7 Server clears the MWN flag in the H323_UIM Terminal subscriber's profile. Also, Sends a Release Complete message to the H323_UIM Terminal.

The reception of the Connected Message Result without error and sending Release complete message to the terminal indicates that the MWN information was delivered successfully to the H323_UIM Terminal.

E2.15.3 Encoding of Qualification Directive with MWN Information

The MWN information is encoded in the Qualification Directive (QUALDIR) operation using the MessageWaitingNotificationCount (MWNCOUNT) and the MessageWaitingNotificationType (MWNTYPE) parameters.

The Qualification Directive (ANSI-41) with MWN information sent from the H.246 AnnexE2_GK to the ANSI-41 MSC/VLR will contain the following parameters:

1)   *SystemMyTypeCode* (mandatory) (use the value for the IIF vendor).

2)   *QualificationInformationCode* (mandatory) (set to value "Profile only").

3)   *ElectronicSerialNumber* (mandatory) (use the ESN of the MS).

4)   *MobileIdentificationNumber* (mandatory) (use the MIN of the MS).

Profile (include the list of message waiting information below).

5)   *MessageWaitingNotificationCount*

- Octet 1: Type of message (set to 0 "Voice Messages").

- Octet 2: Number of messages waiting. Set to the number of voice mail messages waiting (set from 1 to 253). If the number of voice mail messages is 254 or greater, set to value 254. If the number of voice mail messages is zero, the parameter shall be set with the value "no message waiting" (value 0). If the number of voice mail messages is not received but the Data Coding Scheme has value "disable indication" (i.e. bit number 3 has value 0) or the Originating Address has value "clear indicator" (i.e. Octet 3 – bit 0 has value 0) then set the number of pending messages to "no message waiting" (value 0). If the number of messages is not available, the parameter shall be set with value "Unknown" (value 255).

6)   *MessageWaitingNotificationType*

- Bit 0 (A) set value to "Pip Tone notification not required" (value 0).

- Bit 1 (B) set value to "Alert Pip Tone notification not required" (value 0).

- Bit 32 (DC) Set value to "MWI on" (value 2) if the number of messages is > 0 and if the number of messages has changed. Set value to "MWI off" (value 3) if the number of messages is 0 and if the number of messages has changed. If the number of messages has not changed set value to "No MWI" (value 0).

NOTE – For details, see EIA/TIA-41-5-D section 6.4.2.31.

SERIES OF ITU-T RECOMMENDATIONS

Series A   Organization of the work of ITU-T

Series B   Means of expression: definitions, symbols, classification

Series C   General telecommunication statistics

Series D   General tariff principles

Series E   Overall network operation, telephone service, service operation and human factors

Series F   Non-telephone telecommunication services

Series G   Transmission systems and media, digital systems and networks

Series H   Audiovisual and multimedia systems

Series I   Integrated services digital network

Series J   Cable networks and transmission of television, sound programme and other multimedia signals

Series K   Protection against interference

Series L   Construction, installation and protection of cables and other elements of outside plant

Series M   TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits

Series N   Maintenance: international sound programme and television transmission circuits

Series O   Specifications of measuring equipment

Series P   Telephone transmission quality, telephone installations, local line networks

Series Q   Switching and signalling

Series R   Telegraph transmission

Series S   Telegraph services terminal equipment

Series T   Terminals for telematic services

Series U   Telegraph switching

Series V   Data communication over the telephone network

Series X   Data networks and open system communications

Series Y   Global information infrastructure and Internet protocol aspects

Series Z   Languages and general software aspects for telecommunication systems