ANSI

ANSI/TIA/EIA-553-A-1999
Approved: October 14, 1999

TIA/EIA STANDARD

TIA/EIA-553-A

Mobile Station – Base Station Compatibility Standard

TIA/EIA-553-A

(Revision of EIA/TIA-553)

NOVEMBER 1999

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Representing the telecommunications industry in association with the Electronic Industries Alliance

EIA Electronic Industries Alliance

NOTICE

TIA/EIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards and Publications shall not in any respect preclude any member or nonmember of TIA/EIA from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than TIA/EIA members, whether the standard is to be used either domestically or internationally.

Standards and Publications are adopted by TIA/EIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA/EIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(From Standards Proposal No. 3598-B, formulated under the cognizance of the TIA TR-45.1 Subcommittee on Analog Technology.)

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 1999
Standards and Technology Department
2500 Wilson Boulevard
Arlington, VA 22201

PRICE: Please refer to current Catalog of
EIA ELECTRONIC INDUSTRIES ALLIANCE STANDARDS and ENGINEERING
PUBLICATIONS or call Global Engineering Documents, USA and Canada
(1-800-854-7179) International (303-397-7956)

Preface

These technical requirements form a compatibility standard for 800 MHz analog cellular mobile telecommunications systems. Their purpose is to ensure that a mobile station can obtain service in any cellular system manufactured according to this standard. These requirements do not address the quality or reliability of that service, nor do they cover equipment performance or measurement procedures.

To ensure compatibility (see Note 1), it is essential that both radio-system parameters and call-processing procedures be specified. The speech-filtering, modulation, and RF-emission parameters commonly encountered in two-way radio systems have been updated and expanded to reflect the unique radio plan upon which cellular systems are based. The sequence of call processing steps that the mobile stations and base stations execute to establish calls has been specified along with the digital control messages and analog signals that are exchanged between the two stations.

The base station is subject to fewer compatibility requirements than the mobile station. Radiated power levels, both desired and undesired, are fully specified for mobile stations to control the RF interference that one mobile station can cause another. Base stations are fixed in location and their interference is controlled by proper layout and operation of the system in which the station operates. Detailed call-processing procedures are specified for mobile stations to ensure a uniform response to all base stations. Base station call procedures, like power levels, are not specified in detail because they are a part of the overall design of the individual base system. This approach to writing the compatibility specification provides the base system designer with sufficient flexibility to respond to local service needs and to account for local topography and propagation conditions.

The basic radio-system parameters and call-processing procedures embodied in the compatibility specification were originally derived from the Chicago and Baltimore-Washington developmental cellular systems and include certain additions and modifications gained by experience with the operation of commercial systems.

As commercial systems evolve there may be a need for additional capabilities primarily in the area of call-processing procedures and new system features. It is important that evolutionary changes be readily accommodated. To that end, these technical requirements have been organized into six general sections. Alterations to §2 and §3 can affect fundamental mobile station - base station compatibility. All other sections may be altered without affecting basic compatibility.

The following is a summary of each section:

1. General. This section comprises a list of brief explanations of terms, processes, and functions used in these requirements. Since it is the intention of these requirements to permit great latitude of system configurations and the implementation of system features, only those items required for compatibility have strict definitions. Other items may be interpreted to fit the needs of manufacturers and system operators. For example, control channels may be implemented with either combined paging/access functions or as separate paging and access channels.

2. Mobile Station Compatibility Requirements. This section comprises the fundamental signaling compatibility requirements of mobile stations. If strictly adhered to, a mobile station technically will be able to signal a base station. This section assures communications only if service is not otherwise restricted by operational or RF signal level constraints. For example, service may be denied for reasons of subscriber credit or because the mobile station is out of the effective range of a base station. In general, changes or alterations to this section will affect fundamental mobile station - base station compatibility and the ability of mobile stations to signal base stations irrespective of operational or RF signal level conditions.

3. Base Station Compatibility Requirements. This section comprises the fundamental signaling compatibility requirements of base stations and is organized in a manner similar to §2. (In fact, §2 and §3 should be read together for a clearer understanding of the bi-directional signaling protocol.) If strictly adhered to, a base station technically will be able to signal a mobile station. As in §2, communications are assured only if not otherwise restricted by factors such as RF signal limitations or operational limitations. In general, changes or alterations to this section will affect fundamental mobile station - base station compatibility and the ability of mobile stations to signal base stations irrespective of operational or RF signal level conditions.

4. Mobile Station Options. This section is reserved for requirements for use of optional functions and features by mobile stations.

5. Base Station Options. This section is reserved for requirements for use of optional functions and features by base stations.

6. Change History. This section traces all changes to these technical requirements beginning with the initial release of this standard. A brief description of each change as well as a reference to the affected section(s) is provided.

Notes

1. Compatibility, as used in connection with these standards, is understood to mean: Any mobile is able to place and receive calls in any cellular system. Conversely all systems are able to place and receive calls for any mobile station. In a subscriber's home system, all call placement shall be automatic. It is preferable that call placement be automatic when a mobile station is in roam status.

2. The term "mobile station" is defined as one "... intended to be used while in motion or during halts at unspecified points." It is assumed that mobile stations include portable units (e.g., hand-held 'personal' units) as well as units installed in vehicles.

3. This compatibility specification is based upon the specific US spectrum allocation for cellular systems.

4. Technical details are included for the operation of two systems in a geographic area, System A and System B, each with a separate set of control channels.

5. ANSI TIA/EIA 690, *Recommended Minimum Standards for 800 MHz Cellular Subscriber Units*, and ANSI TIA/EIA 712, *Recommended Minimum Standards for 800 MHz Cellular Base Stations* provide specifications and measurement methods for cellular equipment.

6. Each cellular system is identified by a unique 15 bit digital code, the SID code (see §2.3.8). The Federal Communications Commission assigns SID codes when cellular system construction permits are issued.

7. Each mobile station is assigned a unique 32 bit binary serial number that cannot be changed by the subscriber without rendering the mobile station inoperative (see §2.3.2).

8. In the message formats used between the mobile stations and base stations, some bits are marked as reserved (RSVD). Some or all of these reserved bits may be used in the future for additional messages. Therefore, all mobile stations and base stations shall set all bits that they are programmed to treat as reserved bits to "0" (zero) in all messages that they transmit. All mobile stations and base stations shall ignore the state of all bits that they are programmed to treat as reserved bits in all messages that they receive.

   In the specific case of overhead messages on the Forward Control Channel, if the mobile station receives a BCH-code-correct but unrecognizable overhead message (including Global Action Message types), the mobile station shall count that message as part of the train for NAWC-counting purposes, but shall not attempt to execute the message. All other messages and fields of an overhead message train that carries a message type herein indicated as 'Reserved' shall be decoded and used as appropriate.

   Implementors of mobile stations are cautioned that many other functions and features are deployed on the FOCC than those described in this standard. These functions frequently employ bits indicated herein as 'Reserved.' Reference may be made to the current version of TSB-70 for details.

9. RF Emissions. Minimum advisory standards of ANSI and the processing guidelines of the FCC are contained in ANSI C95.1-1991 Advisory Standards and FCC Rules and Regulations, respectively.

10. It is required that autonomous registration be supported by all mobile stations conforming to this standard.

11. The allocation of SID numbers is under review by EIA/TIA TR45 for potential revision to accommodate international requirements. Utilization of SID numbers shall be coordinated.

12. The Authentication processes (AUTH=1) incorporated in this standard are identical with those of IS-54-B and TIA/EIA-95. The following backward compatible timer changes have been made: The mobile station timer has been reduced to prevent fraudulent mobile stations from determining the authentication signature as well as to minimize the time that the mobile station is in a state where no actions can occur (handoff, etc.) The base station time has been increased to allow for network delays that may be encountered when a remote Authentication Center is used.

13. Forward control channel mobile station control messages of greater than five words in length have been shown to yield compatibility problems in some mobile stations. Implementers of systems are advised that the functions performed by these optional messages may be achieved on assigned voice channels without causing compatibility issues. Mobile Station manufacturers are advised that the length of forward control channel messages defined in future standards may be different from that defined in this standard.

14. Those wishing to deploy systems compliant with this standard should also take notice of the requirement to be compliant with FCC Part 22, and the referenced version of FCC Office of Engineering and Technology Bulletin 53.

15. The use of the global action messages Random Challenge A and Random Challenge B, which were added in Revision A of this standard, have been shown to yield compatibility problems in some mobile stations. Implementors of systems are advised that these problems may be reduced if these messages are not transmitted in all overhead message trains.

16. New registration functions have been added as part of this revision. A mobile station is able to register under the following conditions: power up, power down, and movement into a cell/sector that is broadcasting a location area identity (LOCAID) on the analog control channel that is different from the mobile station's stored location area identity.

References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

—American National Standards:

1. ANSI X3.4-1986, *Coded Character Set - 7-bit American National Standard Code for Information Interchange*, 1992.
2. ANSI TIA/EIA 553-A, Appendix A, Message Encryption. An ITAR controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Washington, D.C., July 1999.
3. ANSI TIA/EIA 712-97, *Recommended Minimum Standards for 800 MHz Cellular Base Stations*, July, 1997.
4. ANSI TIA/EIA 690-99, *Recommended Minimum Standards for 800 MHz Cellular Subscriber Units*, July, 1999.

—Other Standards:

1. *Common Cryptographic Algorithms*. An ITAR controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Washington, D.C., October, 1998.
2. ITU-T Recommendation G.162, *Characteristics of Compandors for Telephony*. 1989.
3. *Interface Specification for Common Cryptographic Algorithms, Rev C*. Contact the Telecommunications Industry Association, Washington, D.C., October, 1998.
4. TSB 16, *Assignment of Access Overload Classes in the Cellular Telecommunications Services*, March 1985.
5. TSB 29-B-2, *International Implementation of Wireless Telecommunication Systems Compliant with TIA/EIA-41*, June, 1998.
6. TSB 50, *User Interface for Authentication Key Entry*, March 1993.
7. TSB 70-A, *Mobile Station – Land Station Compatibility Specifications Common Message Protocol Cross-Reference*, July, 1999.

Table of Contents

Figures

Tables

Foreword

(This foreword is not part of this Standard)

These technical requirements form a compatibility standard for a cellular radio telecommunications system. Their purpose is to ensure that a mobile station can obtain service in any cellular system manufactured according to this standard. These requirements do not cover equipment performance or measurement procedures. These issues are addressed for the mobile and base station, respectively, in ANSI TIA/EIA 690, *Recommended Minimum Standard for 800 MHz Cellular Subscriber Units* and ANSI TIA/EIA 712, *Recommended Minimum Standard for 800 MHz Cellular Base Stations.*

There is one normative annex that is considered part of this Standard.

1 Introduction

1.1 Scope

These technical requirements form a compatibility standard for a cellular radio telecommunications system. Their purpose is to ensure that a mobile station can obtain service in any cellular system manufactured according to this standard. These requirements do not cover equipment performance or measurement procedures. These issues are addressed for the mobile and base station, respectively, in ANSI TIA/EIA 690, *Recommended Minimum Standard for 800 MHz Cellular Subscriber Units* and ANSI TIA/EIA 712, *Recommended Minimum Standard for 800 MHz Cellular Base Stations*.

1.2 Definitions

For the purposes of this Standard, the following definitions apply.

A-key. A secret, 64 bit pattern stored in the mobile station. It is used to generate/update the mobile station's Shared Secret Data. The A-key is used in the mobile station authentication process.

Access Channel. A control channel used by a mobile station to access a system to obtain service

Analog Color Code. An analog signal (see SAT) transmitted by a base station on a voice channel and used to detect capture of a mobile station by an interfering base station or the capture of a base station by an interfering mobile station.

AUTH. A 1 bit field in the System Parameter Overhead Message. When set to 1, it signifies that the system supports the authentication procedures.

Authentication. A procedure used by base stations to validate a mobile station's identity or by mobile stations to validate a base station's identity.

Authentication Response (AUTHR). An 18 bit output of the authentication algorithm. It is used to validate mobile station registrations, originations and terminations.

Average Peak Deviation. Half the sum of the maximum positive and negative peaks of the modulated radio frequency signal, i.e. ((Peak dev+)+(Peak dev-))/2.

Base Station. A station in the Cellular Radiotelephone Service, other than a mobile station, used for radio communications with mobile stations.

Base Station Authentication Response (AUTHBS). An 18 bit pattern generated by the authentication algorithm. AUTHBS is used to confirm the validity of base station orders to update the Shared Secret Data.

Base Station Random Variable (RANDBS). A 32 bit random number generated by the mobile station for use in authenticating base station orders to update the Shared Secret Data.

BCH Code. Bose-Chaudhuri-Hocquenghem Code.

Busy-Idle Bits. The portion of the data stream transmitted by a base station on a forward control channel that is used to indicate the current busy-idle status of the corresponding reverse control channel.

Continuous Transmission. A mode of operation in which Discontinuous Transmission is not permitted.

Control Channel. A channel used for the transmission of digital control information from a base station to a mobile station or from a mobile station to a base station.

Digital Color Code (DCC). A digital signal transmitted by a base station on a forward control channel that is used to detect capture of a base station by an interfering mobile station.

Discontinuous Transmission. A mode of operation in which a mobile station transmitter autonomously switches between two transmitter power levels while the mobile station is in the conversation state on a voice channel.

Flash Request. A message sent on a voice channel from a mobile station to a base station indicating that a user desires to invoke special processing.

Forward. The forward communication path is for transmission from a base station to a mobile station.

Forward Control Channel (FOCC). A control channel used from a base station to a mobile station.

Forward Voice Channel (FVC). A voice channel used from a base station to a mobile station.

Group Identification. A subset of the most significant bits of the system identification (SID) that is used to identify a group of cellular systems.

Handoff. The act of transferring a mobile station from one voice channel to another.

Home Mobile Station. A mobile station that operates in the cellular system from which service is subscribed.

Land Station. See Base Station.

Manchester. Manchester encoding is a method of data encoding where each zero is represented as a one to zero transition and each one is represented as a zero to one transition.

Message. A message consists of one or more words of data.

Mobile Identification Number (MIN). The 34 bit number that is a digital representation of the 10-digit number that uniquely identifies the mobile station. The MIN may be identical to the directory number associated with the mobile station.

Mobile Station. A station in the Cellular Radiotelephone Service intended to be used while in motion or during halts at unspecified points. It is assumed that mobile stations include portable units (e.g., hand-held 'personal' units) as well as units installed in vehicles.

Mobile Station Class. The following mobile station classes are defined (see §2.1.2.2):

- Class I. High power station
- Class II. Mid-range power station
- Class III. Low power station.

NRZ. Data is transmitted in a non-return-to-zero (NRZ) waveform if each data bit is represented by a discrete level.

Numeric Information. Numeric information is used to describe the operation of the mobile station. The following subscripts are used to clarify the use of the numeric information:

- "s" to indicate a value stored in a mobile stations temporary memory,
- "sv" to indicate a stored value that varies as a mobile station processes various tasks,
- "sl" to indicate the stored limits on values that vary,
- "r" to indicate a value received by a mobile station over a forward control channel,
- "p" to indicate a value set in a mobile station's permanent security and identification memory, and
- "s-p" to indicate a value stored in a mobile station's semi-permanent security and identification memory.

The numeric indicators are:

- $ACCOLC_p$ A four bit number used to identify which overload class field controls access attempts.
- BIS_s Identifies whether a mobile station shall check for an idle-to-busy transition on a reverse control channel when accessing a system.
- $BSCAP_s$ Base station core analog protocol received in the access type parameters global action overhead message. BSCAP indicates the version of the core analog air-interface standard supported by the system.
- $BSPC_s$ Base station protocol capability received in the access type parameters global action overhead message. BSPC indicates the version of the advanced air-interface standard supported by the system.
- $CCLIST_s$ The list of control channels to be scanned by a mobile station processing the Directed-Retry Task (see §2.6.3.14).
- $CMAX_s$ The maximum number of channels to be scanned by a mobile station when accessing a system.
- $COUNT_{s\text{-}p}$ A modulo-64 count held in the mobile station. $COUNT_{s\text{-}p}$ is maintained during power off.
- CPA_s Identifies whether the access functions are combined with the paging functions on the same set of control channels.
- DTX_s Identifies in what way the mobile station is permitted to use the discontinuous transmission mode on the voice channel.
- E_s The stored value of the E field sent on the forward control channel. E_s identifies whether a home mobile station shall send only $MIN1_p$ or both $MIN1_p$ and $MIN2_p$ when accessing the system.
- EX_p Identifies whether home mobile stations shall send $MIN1_p$ or both $MIN1_p$ and $MIN2_p$ when accessing the system. EX_p differs from E_s in that the information is stored in the mobile station's security and identification memory.
- $FIRSTCHA_s$ The number of the first control channel used for accessing a system.

- $FIRSTCHP_S$ The number of the first control channel used for paging mobile stations.
- $LASTCHA_S$ The number of the last control channel used for accessing a system.
- $LASTCHP_S$ The number of the last control channel used for paging mobile stations.
- $LOCAID_S$ The received location area identity.
- $LOCAID_{S\text{-}P}$ Identifies the current location area.
- $LRCC_S$ The last registration control channel used by a mobile station.
- $LREG_S$ The stored value of the LREG field received in the most recent Location Area Global Action Message.
- LT_S Identifies whether the next access attempt is required to be the last try.
- $MIN1_P$ The 24 bit number that corresponds to the 7-digit directory telephone number assigned to a mobile station.
- $MIN2_P$ The 10 bit number that corresponds to the 3-digit area code assigned to a mobile station.
- $MAXBUSY_{SI}$ The maximum number of busy occurrences allowed on a reverse control channel.
- $MAXSZTR_{SI}$ The maximum number of seizure attempts allowed on a reverse control channel.
- $MSCAP_P$ Mobile station core analog protocol indicates the version of the core analog air-interface standard supported by the mobile station.
- $MSPC_P$ Mobile station protocol capability indicates the version of the advanced air-interface standard supported by the mobile station.
- N_S The number of paging channels that a mobile station shall scan.
- $NBUSY_{SV}$ The number of times a mobile station attempts to seize a reverse control channel and finds the reverse control channel busy.
- $NSZTR_{SV}$ The number of times a mobile station attempts to seize a reverse control channel and fails.
- $NXTREG_{S\text{-}P}$ Identifies when a mobile station shall make its next registration to a system.
- O/E_S. The odd/even data field sent in orders and used for adjacent channel protection.
- PCI_HOME_S Protocol capability indicator (home) indicates whether a home mobile station reports its protocol capability.
- PCI_ROAM_S Protocol capability indicator (roam) indicates whether a roaming mobile station reports its protocol capability.

- $PCSID_S$ The stored value of the latest SID to which the mobile station sent a protocol capability registration message.
- $PDREG_S$ The stored value of the PDREG field received in the most recent Location Area Global Action message and indicating status of power down registration.
- PL_S The mobile station RF power level.
- $PUREG_S$ The stored value of the PUREG field received in the most recent Location Area Global Action message and indicating status of power up registration.
- $PUREG_{S\text{-}P}$ The semi-permanent value of $PUREG_S$.
- R_S Indicates whether registration is enabled or not.
- $RAND_S$ The stored value of the random variable used in authentication.
- RCF_S Identifies whether the mobile station shall read a control-filler message before accessing a system on a reverse control channel.
- $REGID_S$ The stored value of the last registration number ($REGID_R$) received on a forward control channel.
- $REGINCR_S$ Identifies increments between registrations by a mobile station.
- S_S Identifies whether the mobile station shall send its serial number when accessing a system.
- SCC_S A digital number that is stored and used to identify which SAT frequency a mobile station should be receiving.
- $SDCC1_S$ The SDCC1 value stored in a mobile station's temporary memory.
- $SDCC2_S$ The SDCC2 value stored in a mobile station's temporary memory.
- SID_P The home system identification stored in the mobile station's permanent security and identification memory.
- $SID_{S\text{-}P}$ Identifies the system of current (last successful) registration.
- SID_R The system identification received on a paging or access control channel.
- SID_S The system identification received on a dedicated control channel.
- $UPDATE\_NEXTREG_S$ Indicates whether the mobile station shall update NXTREGs after it successfully registers on a new paging channel.
- $WFOM_S$ Identifies whether a mobile station shall wait for an overhead message train before accessing a system on a reverse control channel.

Orders. The following orders can be sent to a mobile station from a base station:

- Abbreviated Alert. The abbreviated alert order is used by a base station to remind the user that previously selected alternative routing features are still active.

- Alert. The alert order is used to inform the user that a call is being received.
- Alert With Info. The alert with info order is used to inform the user that a call is being delivered and additionally provide character information to the mobile station.
- Audit. The audit order is used by a base station to determine whether the mobile station is active in the system.
- Change Power. The change power order is used by a base station to change the RF power level of a mobile station.
- Disable DTMF. The disable DTMF order is used by a base station to indicate to the mobile station that it shall disable its DTMF tone generator.
- Flash With Info. The flash with info order is used by a base station to indicate to the mobile station that special processing is required and additionally provide character information to the mobile station.
- Handoff. The handoff order is used by a base station to cause a mobile station to transfer from one channel to another.
- Intercept. The intercept order is used to inform the user of a procedural error made in placing the call.
- Local Control. The local control order is used by a base station to initiate local control action in the mobile station.
- Maintenance. The maintenance order is used by a base station to check the operation of a mobile station. All functions are similar to alert but the alerting device is not activated.
- Message Encryption Mode. The message encryption mode order is used by the base station to activate and deactivate signaling message encryption in the mobile station.
- Message Waiting. The message waiting order is used by the base station to indicate to the mobile station the presence of messages waiting.
- Parameter Update. The parameter update order is used by the base station to update the mobile station's call history parameter ($COUNT_{S\text{-}P}$).
- Protocol Capability Indicator. The protocol capability indicator order is used by the base station to inform the mobile station of a protocol capability report requirement.
- Release. The release order is used to disconnect a call that is being established or is already established.
- Reorder. The reorder order is used to inform the user that all facilities are in use and the call should be placed again.
- Send Called-Address. The send called-address order is used to inform the mobile station that it shall send a message to the base station with dialed-digit information.
- Serial Number Request. The serial number request order is used by a base station to request the ESN from a mobile station.

- SSD Update. The SSD update order is used by a base station to initiate the generation of new shared secret data in the mobile station.
- Stop Alert. The stop alert order is used to inform a mobile station that it shall discontinue alerting the user.
- Unique Challenge. The unique challenge order is used by a base station to initiate the confirmation of a mobile station's identity and uses a challenge specific random number (RANDU) instead of the random variable broadcast globally (RAND).

Paging. The act of seeking a mobile station when an incoming call has been placed to it.

Paging Channel. A forward control channel that is used to page mobile stations and send orders.

Power Down Registration. Autonomous registration performed just before a mobile station powers down.

Power Up Registration. Autonomous registration performed immediately after a mobile station powers up.

Random Variable (RAND). A 32 bit random number issued periodically by the base station in two, 16 bit pieces: RAND1_A and RAND1_B. The mobile station stores and uses the most recent version of RAND in the authentication process.

Random Variable Confirmation (RANDC). A 8 bit number used to confirm the last RAND received by the mobile station.

Registration. The steps by which a mobile station identifies itself to a base station as being active in the system at the time the message is sent to the base station.

Release Request. A message sent from a mobile station to a base station indicating that the user desires to disconnect the call.

Reverse. The communication path for transmission of data from the mobile station to the base station.

Reverse Control Channel (RECC). The control channel used from a mobile station to a base station.

Reverse Voice Channel (RVC). The voice channel used from a mobile station to a base station.

Roamer. A mobile station that operates in a cellular system other than the one from which service is subscribed.

Scan of Channels. The procedure by which a mobile station examines the signal strength of each forward control channel.

Seizure Precursor. The initial digital sequence transmitted by a mobile station to a base station on a reverse control channel.

Shared Secret Data (SSD). A 128 bit pattern stored in the mobile station (in semi-permanent memory) and known by the base station. SSD is a concatenation of two 64 bit subsets: SSD_A, which is used to support the authentication procedures, and SSD_B, which is utilized in the message encryption process. Shared Secret Data is maintained during power off.

Shared Secret Data Random Variable (RANDSSD). A 56 bit random number generated by the mobile station's home system. RANDSSD is used in conjunction with the mobile station's A-key and ESN to generate its Shared Secret Data.

Signaling Tone. A 10-kilohertz tone transmitted by a mobile station on a voice channel to: 1) confirm orders, 2) signal flash requests, and 3) signal release requests.

Status Information. The following status information is used in this section to describe mobile station operation:

- Fade Timing Status. Indicates whether the mobile station's fade timer has expired.
- First-Idle ID Status. A status variable used by the mobile station in association with its processing of the Idle Task.
- First-Location-Area ID Status. A status variable used by the mobile station in association with its processing of received Location Area ID messages.
- First-Registration ID Status. Indicates whether a mobile station has received a registration ID message since initialization.
- Local Control Status. Indicates whether the mobile station shall respond to local control messages.
- Location-Registration ID Status. Status variable used by the mobile station in association with its processing of Power Up Registrations and location-based registrations.
- Roam Status. Indicates whether a mobile station is in its home system or not.
- Serving-System Status. Indicates whether a mobile station is tuned to channels associated with System A or System B.
- Termination Status. Indicates whether a mobile station shall terminate the call when it is on a voice channel.
- Update Protocol Capability ID Status. Indicates whether a mobile station should report its protocol capability to the serving system.

Supervisory Audio Tone (SAT). One of three tones in the 6 kHz region that are transmitted by a base station and transponded by a mobile station.

Supplementary Digital Color Code. Additional optional bits, transmitted on the forward analog control channel, assigned to increase the number of color codes from four to sixty-four. The DCC, SDCC1, and SDCC2 are assigned to and transmitted from base stations. The mobile station then retransmits the received DCC, SDCC1, and SDCC2 to the base station to indicate which base station transmitter the mobile station is receiving.

System Identification (SID). A 15 bit identification associated with a cellular system; each system is assigned a unique number.

Unique Challenge Authentication Response (AUTHU). An 18 bit pattern generated by the authentication algorithm. AUTHU is used to support the Unique Challenge-Response procedure.

Unique Challenge-Response Procedure. An exchange of information between a mobile station and a base station for the purpose of confirming the mobile station's identity. The procedure is initiated by the base station and is characterized by the use of a challenge-specific random number (i.e., RANDU) instead of the random variable broadcast globally (RAND).

Unique Random Variable (RANDU). A 24 bit random number generated by the base station in support of the Unique Challenge-Response procedure.

Voice Channel. A channel on which a voice conversation occurs and on which brief digital messages may be sent from a base station to a mobile station or from a mobile station to a base station.

1.3 Tolerances

Unless otherwise specified, all time and timing values have a tolerance of ±10% of the nominal value.

2 Mobile Station

2.1 Transmitter

2.1.1 Frequency parameters

2.1.1.1 Channel spacing and designation

Spectrum used in the cellular service is allocated to systems A and B according to Table 2.1.1-1. Channel spacing shall be 30 kHz and the mobile station transmit channel at 825.030 MHz (and the corresponding base station transmit channel at 870.030 MHz) shall be termed channel number 1. The mobile station shall support the 20 MHz range of channels 1 through 666 as shown in Table 2.1.1-1 for System A and System B and the additional 5 MHz of channels 667 through 799 and (wrap-around) 991 through 1023 for extending System A (A', A") and B (B'). In either case, the station class mark (SCM, see §2.3.3) shall be set appropriately.

Table 2.1.1-1 Channel numbers and frequencies

System	Bandwidth MHz	Number of channels	Boundary channel number	Transmitter center frequency MHz	
				Mobile	Base Station
(Not used)		1	(990)	(824.010)	(869.010)
			991	824.040	869.040
A"	1	33	1023	825.000	870.000
			1	825.030	870.030
A	10	333	333	834.990	879.990
			334	835.020	880.020
B	10	333	666	844.980	889.980
			667	845.010	890.010
A'	1.5	50	716	846.480	891.480
			717	846.510	891.510
B'	2.5	83	799	848.970	893.970

In the above, the center frequency in MHz corresponding to the channel number (expressed as N) is calculated as follows:

Transmitter	Channel Number	Center Frequency MHz
Mobile	$1 \le N \le 799$	0.030 N + 825.000
	$990 \le N \le 1023$	0.030 (N-1023) + 825.000
Base Station	$1 \le N \le 799$	0.030 N + 870.000
	$990 \le N \le 1023$	0.030 (N-1023) + 870.000

2.1.1.2 Frequency tolerance

The mobile station carrier frequency shall be maintained within ±2.5 parts per million (ppm) of any assigned channel frequency, except during channel switching (see §2.1.2.1). This tolerance shall be maintained over the ambient temperature range of -30°C to +60°C, and over the supply voltage range of ±15% from the nominal value, accumulative.

2.1.2 Power output characteristics

2.1.2.1 Carrier on/off conditions

The carrier-off condition is defined as a power output at the transmitting antenna connector not exceeding -60 dBm. When commanded to the carrier-on condition on a reverse control channel, a mobile station transmitter shall come to within 3 dB of the specified output power (see §2.1.2.2) and to within the required stability (see §2.1.1.2) within 2 ms. Conversely, when commanded to the carrier-off condition, the transmit power shall fall to a level not exceeding -60 dBm within 2 ms. Whenever a transmitter is more than 1 kHz from its initial or final value during channel switching, the transmitter carrier shall be inhibited to a power output level not greater than -60 dBm.

2.1.2.2 Power output and power control

The maximum effective radiated power with respect to a half-wave dipole (ERP) for any class mobile station transmitter is 8 dBW (6.3 Watts). An inoperative antenna assembly shall not degrade the spurious emission levels as defined in §2.1.4.2. The nominal ERP for each class of mobile station transmitter is:

- Class I 6 dBW (4.0 Watts)
- Class II 2 dBW (1.6 Watts)
- Class III -2 dBW (0.6 Watts).

A mobile station transmitter shall be capable of reducing power in steps of 4 dB on command from a base station (see §§2.6.3.3, 2.6.3.5, 3.7.1.1, 3.7.1.2.4, and 3.7.2). The nominal levels are given in Table 2.1.2-1. Each power level shall be maintained within the range of +2 dB and -4 dB of its nominal level over the ambient temperature range of -30°C to +60°C, and over the supply voltage range of ±10% from the nominal value, accumulative.

Table 2.1.2-1 Mobile station nominal power levels

Mobile Station Power Level	Mobile Attenuation	Nominal ERP for Mobile Station Power Class (dBW)		
(PL)	Code (MAC)	I	II	III
0	000	6	2	- 2
1	001	2	2	-2
2	010	- 2	- 2	- 2
3	011	- 6	- 6	- 6
4	100	-10	-10	-10
5	101	-14	-14	-14
6	110	-18	-18	-18
7	111	-22	-22	-22

2.1.3 Modulation characteristics

2.1.3.1 Voice signals

The (FM) modulator is preceded by the following four voice-processing stages (in the order listed):

- Compressor
- Pre-Emphasis
- Deviation Limiter
- Post Deviation-Limiter Filter.

2.1.3.1.1 Compressor

This stage is the compressor portion of a 2:1 syllabic compandor. For every 2 dB change in input level to a 2:1 compressor within its operating range, the change in output level is a nominal 1 dB. The compressor shall have a nominal attack time of 3 ms and a nominal recovery time of 13.5 ms as defined by the ITU-T (Reference: Recommendation G.162, 1989). The nominal reference input level to the compressor is that corresponding to a 1000 Hz acoustic tone at the expected nominal speech volume level. This level shall produce a nominal ±2.9 kHz peak frequency deviation of the transmitted carrier.

2.1.3.1.2 Pre-emphasis

The pre-emphasis characteristic shall have a nominal +6 dB/octave response between 300 and 3000 Hz.

2.1.3.1.3 Deviation limiter

For audio (voice) inputs applied to the transmitter voice-signal processing stages, the mobile station shall limit the instantaneous frequency deviation to ±12 kHz. This requirement excludes supervision signals (see §2.4) and wideband data signals (see §2.1.3.2).

2.1.3.1.4 Post deviation-limiter filter

The deviation limiter shall be followed by a low-pass filter whose attenuation characteristics shall exceed:

Frequency Band	Attenuation Relative to 1000 Hz
3000 - 5900 Hz	40 log (f/3000) dB
5900 - 6100 Hz	35 dB
6100 - 15000 Hz	40 log (f/3000) dB
above 15000 Hz	28 dB

2.1.3.2 Wideband data signals

2.1.3.2.1 Encoding

The reverse control channel (RECC) and reverse voice channel (RVC) wideband data streams (see §2.7) shall be further encoded such that each nonreturn-to-zero binary one is transformed to a zero-to-one transition, and each nonreturn-to-zero binary zero is transformed to a one-to-zero transition.

2.1.3.2.2 Modulation and polarity

The filtered wideband data stream shall then be used to modulate the transmitter carrier using direct binary frequency shift keying. A one (i.e., high state) into the modulator shall correspond to a nominal peak frequency deviation 8 kHz above the carrier frequency, and a zero into the modulator shall correspond to a nominal peak frequency deviation 8 kHz below the carrier frequency.

2.1.4 Limitations on emissions

2.1.4.1 Bandwidth occupied

Modulation products outside the region ±20 kHz from the carrier shall not exceed a level of 26 dB below the unmodulated carrier. Modulation products outside the region of ±45 kHz from the carrier shall not exceed a level of 45 dB below the unmodulated carrier. Modulation products outside the region of ±90 kHz from the carrier shall not exceed a level of

a. 60 dB below the unmodulated carrier, or

b. $43 + 10 \log_{10}$(mean output power in Watts) dB below the unmodulated carrier.

Measurement techniques are defined in the current edition of ANSI TIA/EIA 690, *Recommended Minimum Standard for 800 MHz Cellular Subscriber Units.*

2.1.4.2 Conducted spurious emissions

2.1.4.2.1 Suppression inside cellular band

When transmitting on any channel, the total emissions in each 30 kHz band located in the mobile station transmit band, centered 60 kHz or more from the transmitted carrier shall be at least 45 dB below the level of the unmodulated carrier. In addition, the transmitter emissions in each 30 kHz band located anywhere in the mobile station receive band shall not exceed -80 dBm at the transmit antenna connector.

2.1.4.2.2 Suppression outside cellular band

Current FCC rules shall apply.

2.1.4.3 Radiated spurious emissions

Radiated spurious emissions (from sources other than via the antenna connector) shall meet levels corresponding to the conducted spurious requirements listed in §2.1.4.2.

2.2 Receiver

2.2.1 Frequency parameters

2.2.1.1 Channel spacing and designation

Channel spacing shall be 30 kHz and the mobile station receive channel at 870.030 MHz (and the corresponding base station receive channel at 825.030 MHz) shall be termed channel number 1. The mobile station shall support the 20 MHz range of channels 1 through 666 as shown in Table 2.1.1-1 for System A and System B and the additional 5 MHz of channels 667 through 799 and (wrap-around) 991 through 1023 for extending Systems A (A', A") and B (B'). In either case, the station class mark (SCM, see §2.3.3) shall be set appropriately.

2.2.2 Demodulation characteristics

2.2.2.1 Voice signals

The demodulator is followed by the following two voice-signal processing stages:

- De-emphasis

- Expandor.

2.2.2.1.1 De-emphasis

The de-emphasis characteristic shall have a nominal -6 dB per octave response between 300 and 3000 Hz.

2.2.2.1.2 Expandor

This stage is the expandor portion of a 2:1 syllabic compandor. For every 1 dB change in input level to a 1:2 expandor, the change in output level is a nominal 2 dB. The signal expansion shall follow all other demodulation signal processing (including the 6 dB/octave de-emphasis and filtering). The expandor shall have a nominal attack time of 3 ms and a nominal recovery time of 13.5 ms as defined by the ITU-T (Reference: Recommendation G.162, 1989). The nominal reference input level to the expandor is that corresponding to a 1000 Hz tone from a carrier with a ±2.9 kHz peak frequency deviation.

2.2.3 Limitations on emissions

2.2.3.1 Conducted spurious emissions

2.2.3.1.1 Suppression inside cellular band

Any RF signals emitted by the receiver and falling within the mobile station receive band shall not exceed -80 dBm, as measured at the antenna connector. Additionally, signals falling within the mobile station transmit band shall not exceed -60 dBm, as measured at the antenna connector.

2.2.3.1.2 Suppression outside cellular band

Current FCC rules shall apply.

2.2.3.2 Radiated spurious emissions

Current FCC rules shall apply.

2.2.4 Other receiver parameters

System performance is predicated upon receivers meeting ANSI TIA/EIA 690, *Recommended Minimum Standard for 800 MHz Cellular Subscriber Units.*

2.3 Security and identification

2.3.1 Mobile identification number

A 34 bit binary mobile identification number (MIN) required for use in several control messages associated with call origination and call termination is derived from a 10 digit decimal mobile station number.

The MIN is derived according to the algorithm described in §2.3.1.1. If the MIN is derived from a ten digit national significant number, commonly referred to as the telephone's "directory number", the format of this number is NPA-NXX-XXXX, where

NPA — represents the three digit Numbering Plan Area,

NXX — represents the three digit mobile exchange code, and

XXXX — represents the four digit telephone number within the exchange.

2.3.1.1 Encoding procedure

A 34 bit binary mobile identification number (MIN) is derived according to the following procedure (see also §2.7.1).

(1) The first three digits are mapped into 10 bits (corresponding to $MIN2_p$) by the following coding algorithm:

(a) Represent the 3-digit field as D_1 D_2 D_3 with the digit 0 having the value 10.

(b) Compute $100D_1 + 10D_2 + D_3 - 111$

(c) Convert the result in step (b) to binary by a standard decimal-to-binary conversion (see Table 2.3.1-1).

(2) The second three digits are mapped into the 10 most significant bits of $MIN1_p$ by the coding algorithm described in (1).

(3) The last four digits are mapped into the 14 least significant bits of $MIN1_p$ as follows:

(a) The thousands digit should be mapped into four bits by a Binary-Coded-Decimal (BCD) conversion, as specified in Table 2.3.1-1.

(b) The last three digits are mapped into 10 bits by the coding algorithm described in (1).

Table 2.3.1-1 Bit encoding headings for MIN

Decimal-to-Binary Conversion		Thousands-Digit BCD Mapping Procedure	
Decimal number	**Binary number**	**Thousands digit**	**Binary sequence**
1	0000000001	1	0001
2	0000000010	2	0010
3	0000000011	3	0011
4	0000000100	4	0100
		5	0101
		6	0110
		7	0111
998	1111100110	8	1000
999	1111100111	9	1001
		0	1010

2.3.1.2 Encoding Example

In the following example, the 10-digit mobile station number is 321-456-7890. This reflects a mobile station whose national significant number (i.e. "directory number") is 321-456-7890 (Numbering Plan Area = "321", mobile exchange = "456"). This number is encoded into the MIN2 and MIN1 components of the MIN using the procedures described in §2.3.1.1 as follows:

- $MIN2_p$. The 10 bit $MIN2_p$ is derived from the first three digits of the telephone number (i.e., 321):

  (a) $D_1 = 3$; $D_2 = 2$; $D_3 = 1$.

  (b) $100D_1 + 10D_2 + D_3 - 111 = 100(3) + 10(2) + (1) - 111 = 210$.

  (c) 210 in binary is '00 1101 0010'.

  Therefore $MIN2_p$ is '00 1101 0010'.

- $MIN1_p$. The 10 most significant bits of $MIN1_p$ are derived from the second three digits of the telephone number (i.e., 456):

  (a) $D_1 = 4$; $D_2 = 5$; $D_3 = 6$.

  (b)$100D_1 + 10D_2 + D_3 - 111 = 100(4) + 10(5) + (6) - 111 = 345$.

  (c) 345 in binary is '0101 0110 01'.

  The next four most significant bits of $MIN1_p$ are derived from the thousands digit of the telephone number (i.e.,7) by BCD conversion:

  7 in BCD is '01 11'.

The 10 least significant bits of MIN1 are derived from the last three digits of the telephone number (i.e., 890):

(a) $D_1 = 8$; $D_2 = 9$; $D_3 = 10$.

(b) $100D_1 + 10D_2 + D_3 - 111 = 100(8) + 10(9) + (10) - 111 = 789$.

(c) 789 in binary is '11 0001 0101'.

Therefore, $MIN1_p$ is '0101 0110 0101 1111 0001 0101'.

2.3.2 Electronic Serial Number

The electronic serial number (ESN) is a unique 32-bit binary number that identifies a mobile station to any cellular system. The primary storage component that holds the ESN shall be factory-set and not alterable in the field. Any circuitry that stores or manipulates the ESN shall be isolated from fraudulent contact and tampering. Mobile stations shall contain mechanisms such that fraudulent attempts to modify them so that they transmit a serial number (see §2.7.1.1) other than the original factory-set ESN shall render them inoperative. These mechanisms shall include methods to prevent fraudulent disabling of or tampering with the strong authentication procedures described in §2.3.12 and elsewhere in this standard.

The bit allocation of the serial number (SN) shall be as follows:

31 24	23 0
MFR CODE	SERIAL NUMBER

The FCC ensures that an eight bit Manufacturer's (MFR) Code is assigned to all grantees of type acceptance in the Part 22 band. The manufacturer shall set this code into the eight most significant bits (bit 31 through bit 24) of the 32-bit serial number. Bits 23 through 0 shall be uniquely assigned by the manufacturer in accordance with the FCC guidelines.

2.3.3 Station class mark

Class-of-station information referred to as the station class mark (SCM_p) shall be stored in a mobile station. The digital representation of this class mark is specified below.

Table 2.3.3-1 Station Class Mark

Power Class SCM_p (see §2.1.2.2)		Transmission SCM_p (see §2.3.11)		Bandwidth SCM_p (see §§2.1.1.1 and 2.2.1.1)	
Class I	0XX00	Continuous	XX0XX	20 MHz	X0XXX
Class II	0XX01	Discontinuous	XX1XX	25 MHz	X1XXX
Class III	0XX10				
Reserved	XXX11				

2.3.4 Registration memory

2.3.4.1 Autonomous Registration memory

A single 21 bit (20 data bits plus an overflow bit) next registration ($NXTREG_{s-p}$) and corresponding 15 bit system identification (SID_{s-p}) pair shall be retained when the mobile station power is turned off. The data retention time under power-off condition shall be longer than 48 hours. If the integrity of the stored data can not be guaranteed after the mobile station is disconnected from the vehicle battery, then the memory shall be set to zero when power is re-applied to the mobile station.

2.3.4.2 Location Area memory

A 12-bit Location Area identifier ($LOCAID_{s-p}$) shall be stored in the mobile station and used to identify changes in location area (see §2.6.2.1). The $LOCAID_{s-p}$ value shall be retained when the mobile station power is turned off. The data retention time under power-off condition shall be longer than 48 hours. If the integrity of the stored data cannot be guaranteed after the mobile station is disconnected from the vehicle battery, then the memory shall be set to zero when power is re-applied to the mobile station.

A 1-bit Power Up Registration identifier ($PUREG_{s-p}$) shall be stored in the mobile station and used to identify changes in the Power Up Registration flag (see §2.6.2.1). The $PUREG_{s-p}$ value shall be retained when the mobile station power is turned off. The data retention time under power-off condition shall be longer than 48 hours. If the integrity of the stored data cannot be guaranteed after the mobile station is disconnected from the vehicle battery, then the memory shall be set to zero when power is re-applied to the mobile station.

2.3.5 Access overload class

A 4 bit number ($ACCOLC_p$) shall be stored in the mobile station and used to identify which overload class field controls access attempts by the mobile station (see §2.6.3.4). [1]

2.3.6 Access method

A 1 bit access method (EX_p) shall be stored in the mobile station and used to determine if the extended address word shall be included in all access attempts (see §2.6.3.7).

---

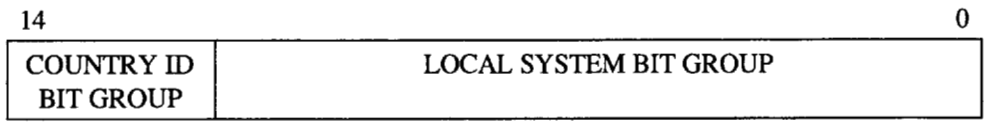
[1] For more information, refer to EIA Telecommunications Systems Bulletin No. 16 (March 1985), "Assignment of Access Overload Classes in the Cellular Telecommunications Services."

2.3.7 First paging channel

An 11 bit first paging channel ($FIRSTCHP_p$) shall be stored in the mobile station and used to identify the channel number of the first paging channel when the mobile station is "home" (see §2.6.1.1.2).

2.3.8 Home system identification

A 15 bit system identification (SID_p) shall be stored in the mobile station and used to identify the mobile station's home system (see §2.6.1.1.2). The bit allocation of the system identification (SID) shall be as follows:



The division of the SID into these segments, and the population of the segments shall be prescribed in the current edition of EIA/TIA Telecommunications Systems Bulletin 29 (TSB 29), entitled *International Implementation of Wireless Telecommuniations Systems Compliant with TIA/EIA-41*.

2.3.9 Local control option

A means shall be equipped within the mobile station to enable or disable the local control option (see §§2.6.1.2.2 and 2.6.2.1).

2.3.10 Preferred system selection

A means shall be provided within the mobile station to identify the preferred system as either System A or System B.

2.3.11 Discontinuous transmission

Discontinuous transmission refers to the ability of certain mobile stations to switch autonomously between two transmitter power-level states ("DTX-high" and "DTX-low") while the mobile station is in the conversation state on a voice channel. Discontinuous transmission is not permitted in any other state than the conversation state.

In the DTX-high state (see Table 2.3.11-1), the transmitter radiates at the power level indicated by the most recent power-controlling order (initial-voice-channel-designation, handoff, or power-change order) received by the mobile station. In this state the mobile station shall transpond SAT at all times, except for the normal suspensions of SAT covered in §2.4.1.

In the DTX-low state (see Table 2.3.11-1), the transmitter radiates at a power level determined by the DTX-high state power level ("DTX-high level") and the DTX_S indicator

that is copied from the DTX field in Word 2 of the System Parameter Overhead Message (see §3.7.1.2.1). If the DTX_S indicator is set to '10', the DTX-low level shall equal or exceed a level that is 8 dB below the DTX-high level[1]. If the DTX_S indicator is set to '11', no minimum applies to the DTX-low level; that is, the transmitter may be turned off or it may be turned on at any level up to the DTX-high level. In the DTX-low state, the mobile station shall not transpond SAT. If the DTX_S indicator is set to '00', only the DTX-high state (that is "continuous transmission") is permitted. The DTX_S indicator setting of '01' is reserved.

Table 2.3.11-1 Discontinuous transmission state values

DTX	Discontinuous transmission
00	disabled
01	reserved
10	enabled power=-2 steps
11	enabled power=no minimum

When a mobile station switches from the DTX-high state to the DTX-low state, it shall pass through a transition state in which the transmitted power is at the DTX-high level but SAT is not transponded. The sequence shall be as follows: starting in the DTX-high state, enter the transition state; remain in the transition state 300 ms; enter the DTX-low state.

When a mobile station switches from the DTX-low state to the DTX-high state, it shall begin transponding SAT immediately after changing the power level, except for the normal suspensions of SAT covered in §2.4.1. Each time that the mobile station enters the DTX-high state, it shall remain in that state for at least 1.5 seconds, unless it enters the DTX-high state in response to an audit order in which case it shall remain in that state for at least 5 seconds. (Note that any requirement for the mobile station to remain in the DTX-high state for a certain minimum time interval does not prohibit the mobile station from leaving the conversation state before the interval ends.)

2.3.12 Authentication and Encryption of Signaling Information/User Data

Messages received during the authentication procedures that are unrelated to the authentication process shall also be processed.

---

[1] Mobile stations manufactured prior to the formal addition of this option in IS-3-C may switch to any power between DTX-high level and completely off when in DTX-low state.

2.3.12.1 Authentication

Authentication is the process during which information is exchanged between a mobile station and the base station for the purpose of enabling the base station to confirm the identity of the mobile station. A successful outcome of the authentication process occurs only when it can be demonstrated that the mobile station and base station possess identical sets of Shared Secret Data (SSD).

The authentication algorithms are described in *Common Cryptographic Algorithms*. The interface (input and output parameters) for the algorithms are described in *Interface Specification for Common Cryptographic Algorithms)*. See §2.3.12.1.9 of this document for more information. Table 2.3.12-1 summarizes the setting of the input parameters of the Auth_Signature procedure for each of its uses in this standard.

Table 2.3.12-1 Auth_Signature Input Parameters

Procedure	RAND_CHALLENGE	ESN	AUTH_-DATA	SSD_-AUTH	SAVE_-REGISTERS
Registration (§2.3.12.1.4)	$RAND_S$	ESN_P	MIN1	SSD_A	FALSE
Unique Challenge (§2.3.12.1.5)	256 × RANDU + (8 LSBs of MIN2)	ESN_P	MIN1	SSD_A	FALSE
Originations (§2.3.12.1.6)	$RAND_S$	ESN_P	Digits	SSD_A	TRUE
Terminations (§2.3.12.1.7)	$RAND_S$	ESN_P	MIN1	SSD_A	TRUE
Base Station Challenge (§2.3.12.1.8)	RANDBS	ESN_P	MIN1	SSD_A_-NEW	FALSE

2.3.12.1.1 Shared Secret Data (SSD)

SSD is a 128 bit pattern stored in the mobile station (in semi-permanent memory) and readily available to the base station. As depicted in Figure 2.3.12-1, SSD is partitioned into two distinct subsets. Each subset is used to support a different process.

Figure 2.3.12-1 Partitioning of SSD

Contents	SSD_A	SSD_B
Length (bits)	64	64

Specifically,

- SSD_A is used to support the authentication procedures; and
- SSD_B is used to support message encryption services.

SSD is generated according to the procedure specified in §2.3.12.1.8.

2.3.12.1.2 Random Challenge Memory ($RAND_S$)

$RAND_S$ is a 32 bit value held in the mobile station. When received on the forward analog control channel, it is the concatenation of the last RAND1_A and RAND1_B values received in Random Challenge A and Random Challenge B Global Action Messages appended to the overhead message train. Both RAND1_A and RAND1_B shall be received on the same control channel and in the same Overhead Message Train in order for a valid $RAND_S$ to exist.

$RAND_S$ is used in conjunction with SSD_A and other parameters, as appropriate, to authenticate mobile station originations, terminations and registrations.

2.3.12.1.3 Call History Parameter ($COUNT_{s-p}$)

$COUNT_{s-p}$ is a modulo-64 count held in the mobile station. $COUNT_{s-p}$ is updated at the mobile upon receipt of a Parameter Update Order (see Table 3.7.1-1) on the FVC.

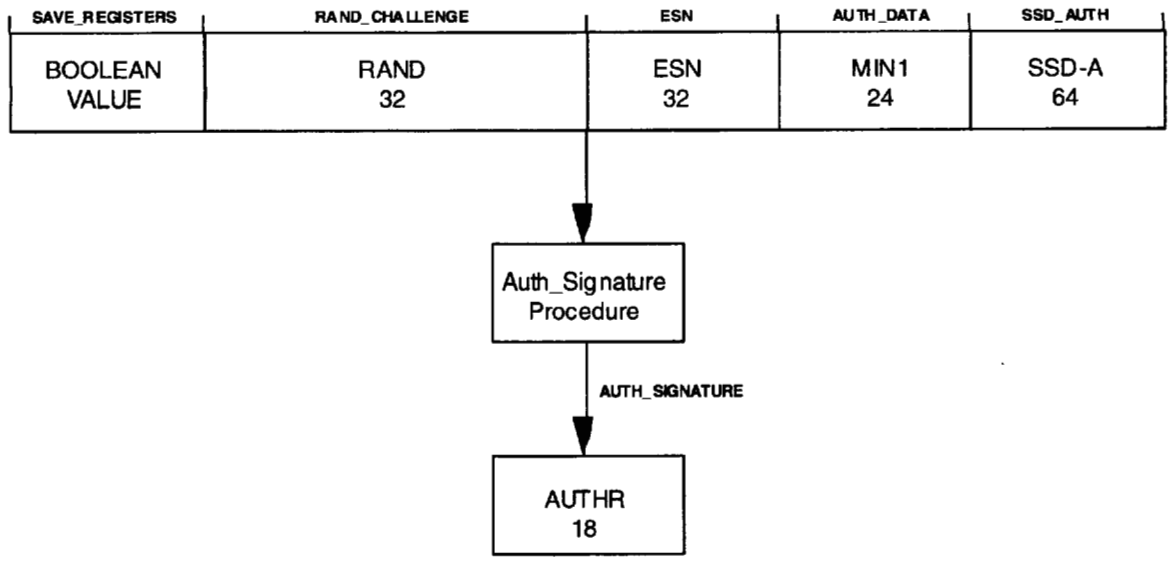
2.3.12.1.4 Authentication of Mobile Station Registrations

When the information element AUTH in the System Parameter Overhead Message is set to 1, and the mobile station attempts to register, the following authentication-related procedures shall be performed:

- In the mobile station,
  - set the input parameters of the Authentication procedure as illustrated in Figure 2.3.12-2;
  - set the SAVE_REGISTERS input parameter to FALSE;
  - execute the Auth_Signature procedure;
  - set AUTHR to the 18 bit output AUTH_SIGNATURE;
  - send AUTHR together with RANDC (eight most significant bits of RAND) and $COUNT_{s-p}$ to the base station (Authentication Word C of RECC Autonomous Registration Order Message).
- At the base station,
  - compare the received values for RANDC, and optionally COUNT, with the internally stored values associated with the received MIN/ESN;
  - compute AUTHR as described above, except use the internally stored value of SSD_A; and
  - compare the value for AUTHR computed internally with the value of AUTHR received from the mobile station.

If any of the comparisons by the base station fail, the base station may deem the registration attempt unsuccessful, initiate the Unique Challenge-Response procedure (see §2.3.12.1.5), or commence the process of updating the SSD (see §2.3.12.1.8).

Figure 2.3.12-2 Computation of AUTHR for MS Registrations



2.3.12.1.5 Unique Challenge-Response Procedure

The Unique Challenge-Response procedure is initiated by the base station and can be carried out over any combination of control and voice channels.

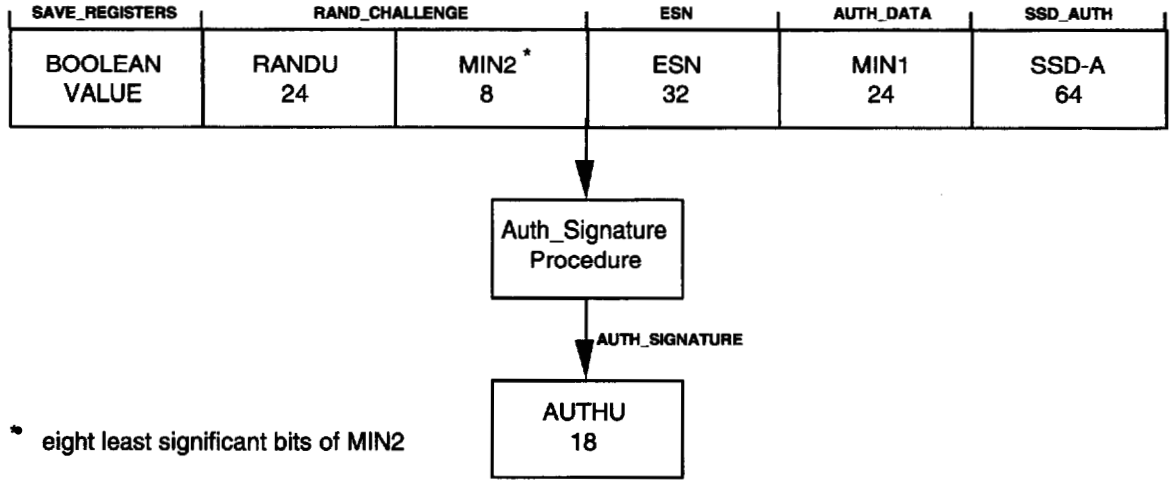
More specifically:

- In the base station,
  - a 24 bit, random pattern referred to as RANDU is generated and sent to the mobile station via:
    + the FOCC in Word 3 - Unique Challenge Order Word of a mobile station control message if the procedure is to be initiated on a forward control channel (see §§3.6.2.3 and 3.7.1.1); or
    + the FVC in Word 2 - Unique Challenge Order Word of a mobile station control message if the mobile station has been assigned to a voice channel (see §§3.6.4 and 3.7.2.1).
  - set the input parameters of the Authentication procedure as illustrated in Figure 2.3.12-3. The 24 most significant bits of the RAND_CHALLENGE input parameter shall be filled with RANDU, and the 8 least significant bits of RAND_CHALLENGE shall be filled with the 8 least significant bits of MIN2;
  - set the SAVE_REGISTERS input parameter to FALSE;
  - execute the Auth_Signature procedure;
  - set AUTHU to the 18 bit output AUTH_SIGNATURE;
- At the mobile station,

- compute AUTHU as described above using the received RANDU and its internally stored values for the remaining input parameters;
- send AUTHU to the base station via:
  - + the RECC in Word C - Unique Challenge Order Confirmation Word of an order confirmation message if the mobile station is not tuned to an analog voice channel (see §§2.6.2.3 and 2.7.1.1); or
  - + the RVC in a Unique Challenge Order Confirmation message if the mobile station is tuned to an analog voice channel (see §§2.6.4 and 2.7.2.1).

Upon receipt of the Unique Challenge Order Confirmation from the mobile station, the base station compares the received value for AUTHU to that generated/stored internally. If the comparison fails, the base station may deny further access attempts by the mobile station, drop the call in progress, or initiate the process of updating the SSD (see §2.3.12.1.8).

Figure 2.3.12-3 Computation of AUTHU



2.3.12.1.6 Authentication of Mobile Station Originations

When the information element AUTH in the System Parameter Overhead Message is set to 1, and the mobile station attempts to originate a call, the following authentication-related procedures shall be performed:

- In the mobile station,
  - set the input parameters of the Auth_Signature procedure as illustrated in Figure 2.3.12-4. If there were at least six digits dialed, then the last six digits dialed shall comprise the DIGITS input parameter. If there were less than six digits dialed, then the DIGITS input parameter shall be populated as follows:
    - + MIN1 shall be used to initially fill the DIGITS input parameter.
    - + the least significant 4 bits of the DIGITS input parameter are replaced by the last dialed digit.
    - + The next least significant 4 bits of the DIGITS input parameter are replaced by the second last dialed digit.

+ continue replacing 4-bit segments of the DIGITS input parameter in this manner until all dialed digits have been included.

– set the SAVE_REGISTERS input parameter to TRUE;

– execute the Auth_Signature procedure;

– set AUTHR to the 18 bit output AUTH_SIGNATURE;

– send AUTHR together with RANDC (eight most significant bits of RAND) and $COUNT_{S-P}$ to the base station (Authentication Word C of the RECC Origination Message);

• At the base station,

– compare the received values for RANDC, and optionally COUNT, with the internally stored values associated with the received MIN/ESN;

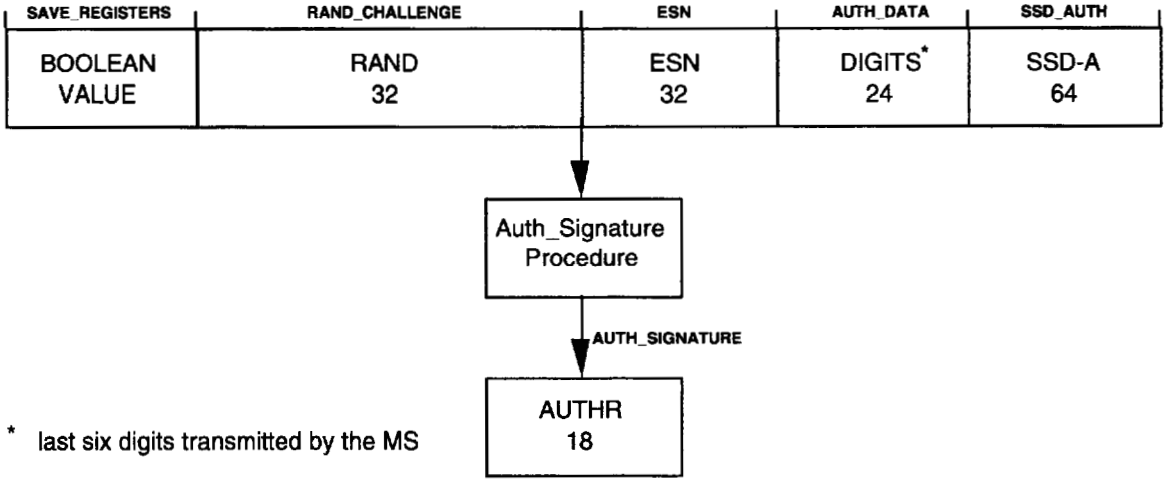
– compute AUTHR as described above, except use the internally stored value of SSD_A; and

– compare the value for AUTHR computed internally with the value of AUTHR received from the mobile station.

If the comparisons at the base station are successful, the appropriate channel assignment procedures are commenced. Once assigned to an analog voice channel, the base station may, at the discretion of the system operator, issue a Parameter Update Order (see Table 3.7.1-1) to the mobile station on the FVC. Mobile stations confirm the receipt of Parameter Update Orders by sending Parameter Update Confirmations on the RVC.

If any of the comparisons by the base station fail, the base station may deny service, initiate the Unique Challenge-Response procedure (see §2.3.12.1.5), or commence the process of updating the SSD (see §2.3.12.1.8).

Figure 2.3.12-4 Computation of AUTHR for MS Originations



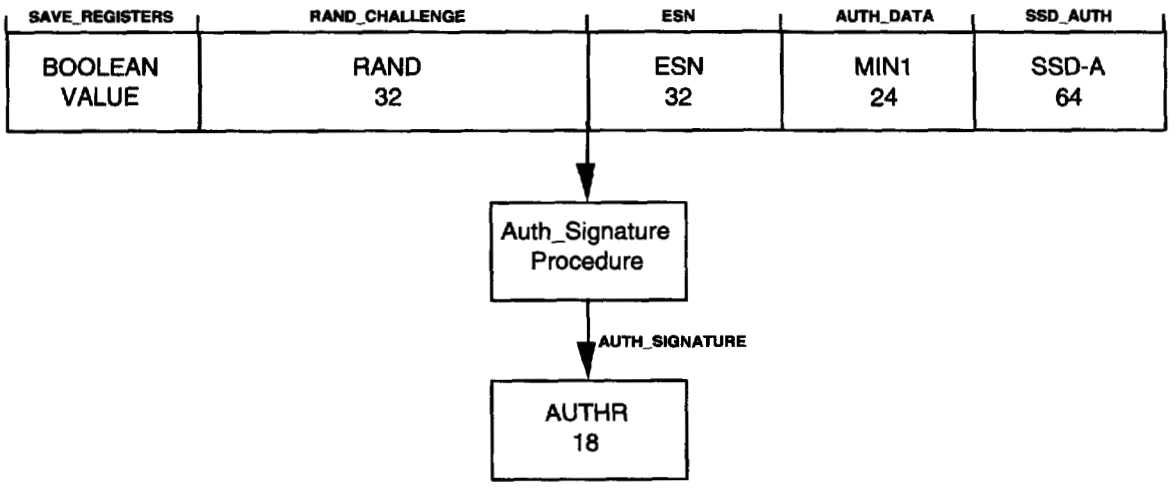
2.3.12.1.7 Authentication of Mobile Station Terminations

When the information element AUTH in the System Parameter Overhead Message is set to 1, and a "Page Match" occurs, the following authentication-related procedures shall be performed:

- In the mobile station,
  - set the input parameters of the Authentication procedure as illustrated in Figure 2.3.12-5;
  - set the SAVE_REGISTERS input parameter to TRUE;
  - execute the Auth_Signature procedure;
  - set AUTHR to the 18 bit output AUTH_SIGNATURE;
  - send AUTHR together with RANDC (eight most significant bits of RAND) and $COUNT_{S-P}$ to the base station (Authentication Word C of the RECC Page Response Message);
- At the base station,
  - compare the received values for RANDC, and optionally COUNT, with the internally stored values associated with the received MIN/ESN;
  - compute AUTHR as described above, except use the internally stored value of SSD_A; and
  - compare the value for AUTHR computed internally with the value of AUTHR received from the mobile station.

If the comparisons at the base station are successful, the appropriate channel assignment procedure is commenced. Once assigned to an analog voice channel, the base station may, at the discretion of the system operator, issue a Parameter Update Order (see Table 3.7.1-1) to the mobile station on the FVC. Mobile stations confirm the receipt of Parameter Update Orders by sending Parameter Update Confirmations on the RVC.

Figure 2.3.12-5 Computation of AUTHR for MS Terminations



If any of the comparisons by the base station fail, the base station may deny service, initiate the Unique Challenge procedure (see §2.3.12.1.5), or commence the process of updating the SSD (see §2.3.12.1.8).

2.3.12.1.8 Updating the Shared Secret Data (SSD)

SSD is updated using the SSD_Generation and SSD_Update procedures, initialized with mobile specific information, random data and the mobile station's A-key.

The A-key is:

- 64 bits long;
- assigned to the mobile station;
- stored in the mobile station's permanent security and identification memory; and
- is known only to the mobile station and its associated Home Location Register/Authentication Center (HLR/AC).

Notes:

1. Shared secret data is intended to enhance the security of the mobile station's secret data by eliminating the need to pass the A-key itself from system to system as the subscriber roams. As a consequence, SSD updates are carried out only in the mobile station and its associated HLR/AC, not in the serving system. For any instances in §2.3.12, where it is implied that base stations update SSD, in fact, this function is carried out in the HLR/AC. The serving system obtains a copy of the SSD computed by the HLR/AC via intersystem communication (see EIA/TIA IS-41) with the mobile station's HLR/AC.
2. Since the SSD Update procedure involves multiple transactions and can be started on one channel and completed on another channel, call processing and signaling text above and beyond that normally included in this portion of the document has been included here for the sake of added clarity.

An A-key shall be entered into the mobile station. See TSB-50 *User Interface for Authentication Key Entry* for details.

More specifically, updating the SSD in the mobile station proceeds as follows (See Figure 2.3.12-6):

- At the base station,
  - send an SSD Update Order, with the RANDSSD field set to the same 56 bit random number used in the HLR/AC computations, to the mobile station on the:
    + FOCC in Word 3 - First SSD Update Order Word, Word 4 - Second SSD Update Order Word and Word 5 - Third SSD Update Order Word of a mobile station control message if the mobile station has not been assigned to an analog voice channel (see §§3.6.2.3 and 3.7.1.1); or
    + FVC in Word 2 - First SSD Update Order Word, Word 3-Second SSD Update Order Word and Word 4-Third SSD Update Order Word of a mobile

station control message if the mobile station has been assigned to an analog voice channel (see §§3.6.4 and 3.7.2.1).

- In the mobile station,
  - upon receipt of the SSD Update Order, set the input parameters of the SSD_Generation procedure as illustrated in Figure 2.3.12-7;
  - execute the SSD_Generation procedure (this may also be performed after the generation and transmission of RANDBS);
  - set SSD_A_NEW and SSD_B_NEW to the outputs of the SSD_Generation procedure;
  - select a 32 bit random number, RANDBS and send it to the base station in a Base Station Challenge Order on the:
    + RECC in Word C - Base Station Challenge Word if the mobile station is not tuned to an analog voice channel (see §§2.6.2.3 and 2.7.1.1); or
    + RVC in Words 1 and 2 of a Base Station Challenge Order message if the mobile station is tuned to an analog voice channel (see §§2.6.4 and 2.7.2.1).
  - set the input parameters of the Auth_Signature procedure as illustrated in Figure 2.3.12-8;
  - set the SAVE_REGISTERS input parameter to FALSE;
  - execute the Auth_Signature procedure;
  - set AUTHBS to the 18 bit output AUTH_SIGNATURE.

Figure 2.3.12-6 SSD Update Message Flow

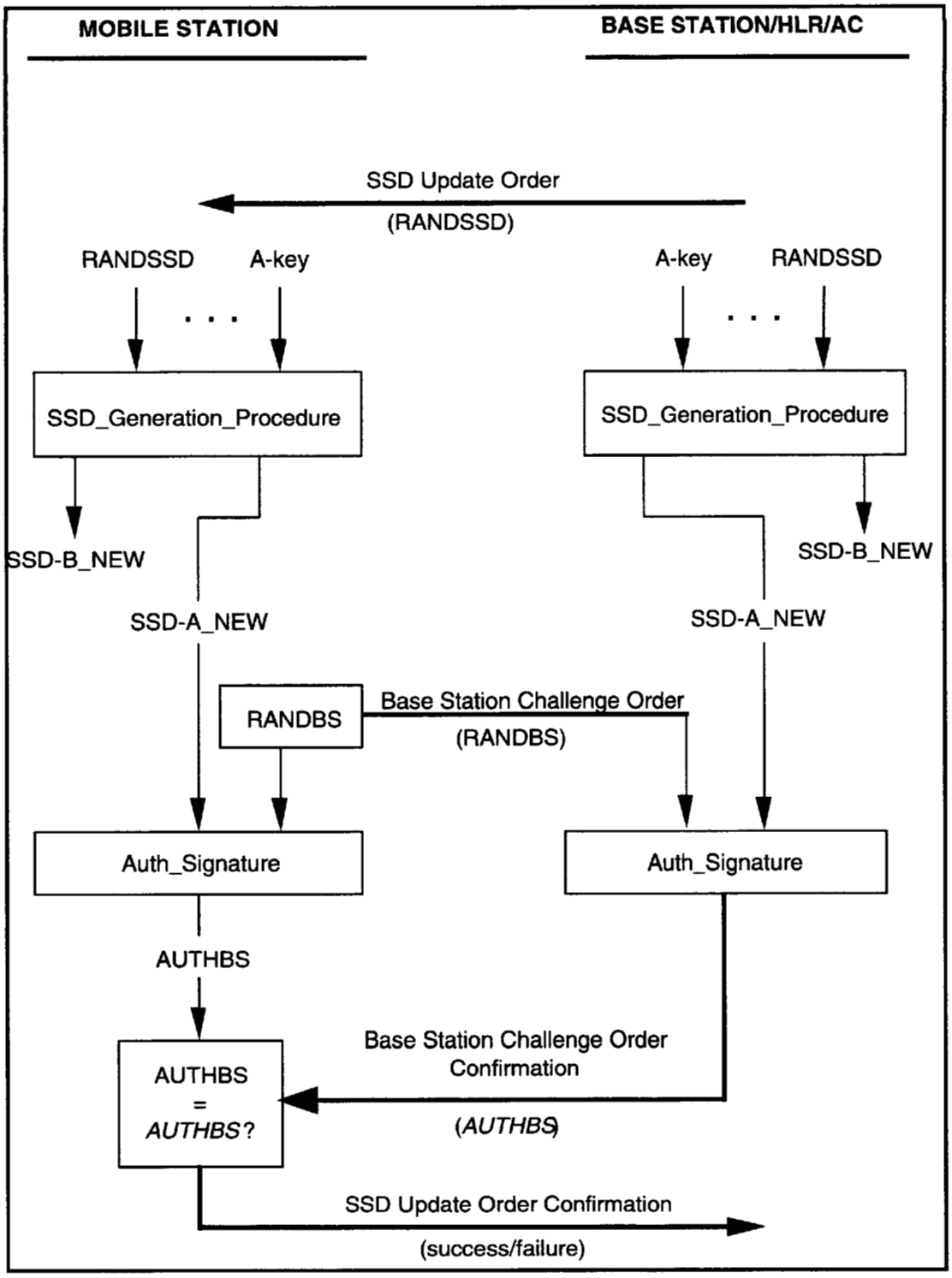
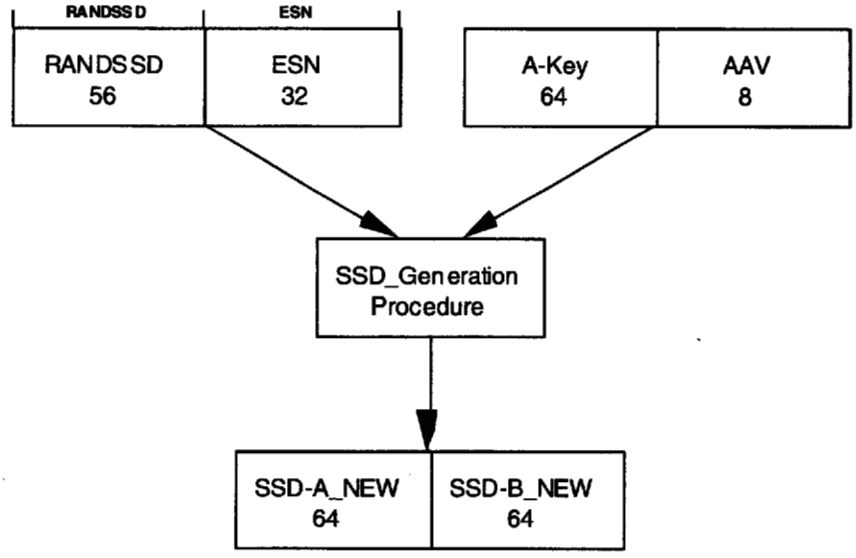
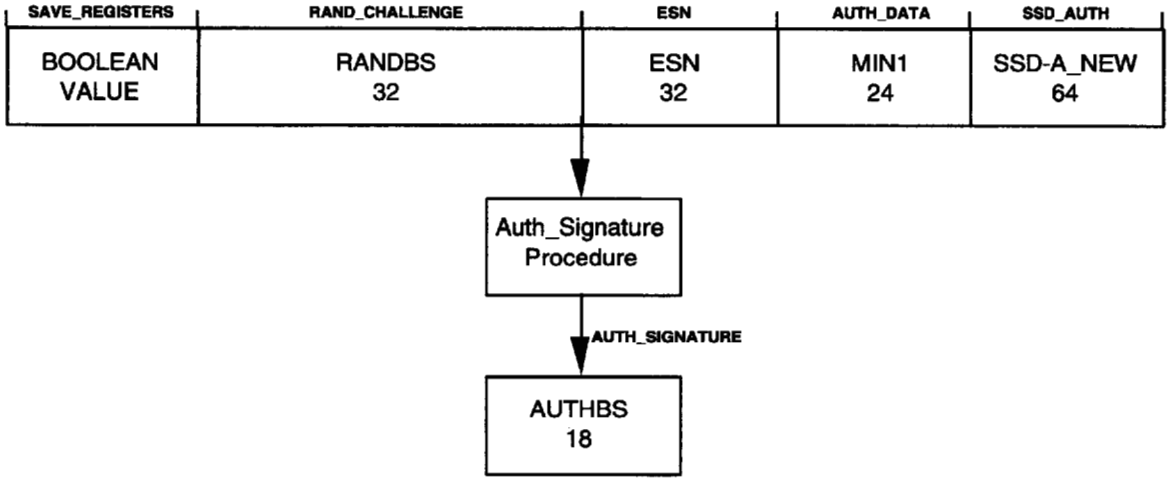


Figure 2.3.12-7 Computation of Shared Secret Data



AAV (Authentication Algorithm Version)

Figure 2.3.12-8 Computation of AUTHBS



- In the base station,
  - upon receipt of the Base Station Challenge Order, set the input parameters of the Auth_Signature procedure as illustrated in Figure 2.3.12-8, where RANDBS is set to the value received in the Base Station Challenge Order;
  - set the SAVE_REGISTERS input parameter to FALSE;
  - execute the Auth_Signature procedure;
  - set AUTHBS to the 18 bit output AUTH_SIGNATURE;
  - acknowledge receipt of the Base Station Challenge Order by including AUTHBS in the Base Station Challenge Order Confirmation message, which is sent on the:

+ FOCC in Word 3-Base Station Challenge Order Confirmation Word of a mobile station control message if the mobile station has not yet been assigned to an analog voice channel (see §§3.6.2.3, 3.6.3.3 and 3.7.1.1); or
+ FVC in Word 2-Base station Challenge Order Confirmation of a mobile station control message if the mobile station has been assigned to an analog voice channel (see §§3.6.4 and 3.7.2.1).

- In the mobile station,
  - upon receipt of the Base Station Challenge Order Confirmation, compare the AUTHBS received to that generated internally;
  - acknowledge receipt of the SSD Update Order as follows:
  - if the comparison at the mobile station is successful, execute the SSD_Update procedure to set SSD_A and SSD_B to SSD_A_NEW and SSD_B_NEW, respectively, and:
    + if the mobile station is not tuned to an analog voice channel send an order confirmation message to the base station on the RECC with:
      * the "T" field in Word A-Abbreviated Address Word set to '0' to identify the message as an Order Confirmation;
      * the "ORDER" field in Word B-Extended Address Word set to '10101' to signify confirmation of the SSD Update Order;
      * the "ORDQ" field in Word B-Extended Address Word set to '001' to denote the successful completion of the SSD Update process; and
      * all other fields set as described in §2.7.1.1 and in the references cited therein.
    + if the mobile station is tuned to an analog voice channel, send an Order Confirmation message to the base station on the RVC with:
      * the "T" field set to '1' to identify the message as an order confirmation;
      * the "ORDER" field set to '10101' to signify confirmation of the SSD Update order;
      * the "ORDQ" field set to '001' to denote the successful completion of the SSD Update process; and
      * all other fields set as described in §2.7.2.1 and in references cited therein.
  - if the comparison at the mobile station fails, discard SSD_A_NEW and SSD_B_NEW, and:
    + if the mobile station is not tuned to an analog voice channel send an order confirmation message to the base station on the RECC with:
      * the "T" field in Word A-Abbreviated Address Word set to '0' to identify the message as an Order Confirmation;
      * the "ORDER" field in Word B-Extended Address Word set to '10101' to signify confirmation of the SSD Update Order;
      * the "ORDQ" field in Word B-Extended Address Word set to '000' to denote the unsuccessful completion of the SSD Update process; and
      * all other fields set as described in §2.7.1.1 and in the references cited therein.
    + if the mobile station is tuned to an analog voice channel, send an Order Confirmation message to the base station on the RVC with:
      * the "T" field set to '1' to identify the message as an order confirmation;

* the "ORDER" field set to '10101' to signify confirmation of the SSD Update order;
* the "ORDQ" field set to '000' to denote the unsuccessful completion of the SSD Update process; and
* all other fields set as described in §2.7.2.1 and in references cited therein.

In the base station, if the SSD Update Confirmation received from the mobile station indicates a success, set SSD_A and SSD_B to the values received from the HLR/AC (see EIA/TIA IS-41).

2.3.12.1.9 Authentication Procedures

The availability of authentication algorithm information is governed under the U.S. International Traffic and Arms Regulations (ITAR) and the Export Administration Regulations. TIA will act as the focal point and facilitator for making such information available. Procedures for distribution of this information are contained in the Technology Transfer Control Plan which applies to *Common Cryptographic Algorithms*. The Technology Transfer Control Plan is available from TIA.

The *Interface Specification for Common Cryptographic Algorithms* and Appendix A of this standard also contain authentication information. Procedures for distribution of this information are contained in the Technology Transfer Control Plan which is administered by the TIA.

2.3.12.2 Signaling Message Encryption

In an effort to enhance the authentication process, and to protect sensitive subscriber information, provisions have been made to allow for the encryption of a select subset of FVC and RVC signaling messages. See Appendix A for the list of messages and fields to be encrypted.

2.3.12.2.1 Signaling Message Encryption Control

Signaling message encryption is controlled on a per-call basis. Signaling message encryption is deactivated at the beginning of each call. To activate signaling message encryption for a mobile station assigned to an analog voice channel, the base station shall send a Message Encryption Mode Order with the Order Qualifier field set to '001'.

The data used to initialize the algorithm is computed based on parameters in effect at the time the AUTHR appended to the origination/page response message was computed (see §§2.3.12.1.6 and 2.3.12.1.7).

Once activated, signaling message encryption can be deactivated by the base station by sending a Message Encryption Mode Order with the Order Qualifier field set to '000'.

In all cases both the base station and mobile station shall continue to operate in their present mode until the message sent to the mobile station has been properly acknowledged.

2.4 Supervision

2.4.1 Supervisory Audio Tone (SAT)

The Supervisory Audio Tone (SAT) will be one of three frequencies: 5970, 6000, or 6030 Hz. The SAT is added to the voice transmission by a base station (see §3.4.1). A mobile station shall detect, filter, and modulate the transmitted voice channel carrier with this tone. Transmission of the SAT by a mobile station shall be suspended during transmission of wideband data on the reverse voice channel (see §2.7.2), but shall not be suspended when Signaling Tone is sent (see §2.4.2).

While a valid SAT is detected and the measured SAT determination does not agree with the SAT color code (SCC_T) received in the mobile station control message (see §§3.7.1.1 and 3.7.2), the receiver audio shall be muted.

2.4.1.1 SAT detection

A mobile station shall make the following decisions to determine which SAT, or none, is present:

Measured frequency of incoming signal	Measured SAT determination	where
$f < f_1$	No valid SAT	f_1 = 5955 ±5 Hz
$f_1 \leq f < f_2$	SAT = 5970	f_2 = 5985 ±5 Hz
$f_2 \leq f < f_3$	SAT = 6000	f_3 = 6015 ±5 Hz
$f_3 \leq f < f_4$	SAT = 6030	f_4 = 6045 ±5 Hz
$f_4 \leq f$	No valid SAT	
No SAT Received	No valid SAT	

The determination of SAT is not required to be made continuously but shall be performed at least every 250 ms.

2.4.1.2 SAT transmission

The transmission requirements for the SAT signal, including time delays in the transmitter, receiver, and any equalization circuits, are summarized as follows:

• Steady-state phase difference between received and transmitted SAT at 5970, 6000, and 6030 Hz	May have any average phase but shall remain within a ±10 degree band
• Phase Step Response	Settle to within 10 degrees of final steady state phase difference in ≤250 ms
• Tone Modulation Index	1/3 radian ±10% ($\Delta f \sim \pm 2$ kHz)

2.4.1.3 Fade timing status

When an SAT determination is made a mobile station shall perform the following:

- If no valid SAT is detected or the measured SAT determination does not agree with the SAT color code (SCC_r) received in the mobile station control message (see §§3.7.1.1 and 3.7.2), the fade timing status shall be enabled (see §2.6.4.1).
- Otherwise, the fade timing status shall be disabled (see §2.6.4.1).

2.4.2 Signaling Tone

Signaling tone (ST) shall be 10 kHz±1 Hz and produce a nominal frequency deviation of ±8 kHz±10%.

2.5 Malfunction detection

2.5.1 Malfunction timer

A timer separate from and independent of all other functions shall be running continuously whenever power is applied to the transmitter of a mobile station. If the mobile station is software-controlled, sufficient reset commands shall be interspersed throughout the mobile station logic program to ensure that the timer never expires as long as the proper sequence of operations is taking place; similar means shall be provided, as appropriate, in hardware-controlled designs. If the timer expires, a malfunction shall be assumed and the mobile station shall be inhibited from transmitting. The maximum time allowed for expiration of the timer is 60 seconds.

This supersedes the requirement for a transmitter carrier-on indicator.

2.5.2 False transmission

A protection circuit shall be provided to minimize the possibility of false transmitter operation caused by component failure within the mobile station.

2.6 Call processing

The following sections describe mobile station operation as controlled by a base station. Frequent references are made to the corresponding sections in the base station section and to the messages that flow between a base station and a mobile station. It is helpful to read §§2.6 and 3.6 in parallel and examine the message formats in §§2.7 and 3.7 at the same time.

When power is applied to a mobile station, it should enter the Retrieve System Parameters Task (see §2.6.1.1). Each task from §§2.6.1.1 to 2.6.5.7 contains information describing which tasks shall be entered when a given task is completed.

2.6.1 Initialization

2.6.1.1 Retrieve system parameters

If this task has been entered as a result of a power up condition the mobile station shall:

- Set $PUREG_S = 0$, $PDREG_S = 0$, $LREG_S = 0$, $LRCC_S = 0$, $RAND_S = 0$, $PCSID_S = 0$, $BSPC_S = 0$, $BSCAP_S = 0$, $PCI\_HOME_S = 0$, $PCI\_ROAM_S = 0$, $SID_S = 0$, and $SID_r = 0$.
- Set the first-registration ID status to enabled.
- Set the first-idle ID status to enabled.
- Set the first-location-area ID status to enabled.
- Set the location-registration ID status to enabled.
- Set the Update Protocol Capability ID status to disabled.

If the preferred system (see §2.3.10) is System A, set the serving-system status to enabled; if the preferred system is System B, set the serving-system status to disabled.

The mobile station shall then enter the Scan Dedicated Control Channels Task (see §2.6.1.1.1).

2.6.1.1.1 Scan dedicated control channels

If $SID_r \neq SID_S$, the mobile station shall set registration increment ($REGINCR_S$) to its default value of 450, set the first-location-area ID status to enabled, set $LRCC_S = 0$ and set $RAND_S = 0$.

If the serving-system status is enabled, a mobile station shall examine the signal strength on each of the dedicated control channels assigned nationwide to System A. If the serving-system status is disabled, a mobile station shall examine the signal strength on each of the dedicated control channels assigned nationwide to System B.

The mobile station shall then enter the Update Overhead Information Task (see §2.6.1.1.2).

2.6.1.1.2 Update overhead information

Overhead messages are sent in a group called an overhead message train (see §3.7.1.2). The mobile station shall use the value given in the NAWC (number of additional words coming) field of the system parameter overhead message in the train to determine that all messages of the train have been received. The END field shall be used as a cross-check. For NAWC-counting purposes, inserted control-filler messages (see §3.7.1) shall not be counted as part of the overhead message train.

If the mobile station receives a BCH-code-correct but unrecognizable overhead message in the train, the mobile station shall count that message as part of the train for NAWC-counting purposes, but shall not attempt to execute the message.

The mobile station shall tune to the strongest dedicated control channel and, within 3 seconds, receive a system parameter message (see §3.7.1.2) and update the following numeric information:

- System identification (SID_S) Set the 14 most significant bits of SID_S to the value of the SID1 field. Set the least significant bit of SID_S to '1' if the serving-system status is enabled; otherwise, set the bit to '0'.
- Number of paging channels (N_S). Set N_S to 1 plus the value of the N-1 field.
- First paging channel ($FIRSTCHP_S$). Set $FIRSTCHP_S$ according to the following algorithm:
  - If $SID_S = SID_P$, $FIRSTCHP_S = FIRSTCHP_P$ (see §2.3.7).
  - If $SID_S \neq SID_P$ and the serving-system status is enabled, set $FIRSTCHP_S$ to the first dedicated control channel for System A (834.990 MHz mobile transmit, 879.990 MHz base transmit).
  - If $SID_S \neq SID_P$ and the serving-system status is disabled, set $FIRSTCHP_S$ to the first dedicated control channel for System B (835.020 MHz mobile transmit, 880.020 MHz base transmit).
- Last paging channel ($LASTCHP_S$). Set $LASTCHP_S$ according to the following algorithm:
  - If the serving-system status is enabled, $LASTCHP_S = FIRSTCHP_S - N_S + 1$
  - If the serving-system status is disabled, $LASTCHP_S = FIRSTCHP_S + N_S - 1$
- If $SID_T \neq SID_S$, the mobile station shall set registration increment ($REGINCR_S$) to its default value of 450, set the first-registration ID status to enabled, set the first-location-area ID status to enabled, set $LRCC_S = 0$ and set $RAND_S = 0$.

The mobile station shall then enter the Paging Channel Selection Task (see §2.6.1.2).

If the mobile station cannot complete this task on the strongest dedicated control channel, it may tune to the second strongest dedicated control channel and attempt to complete this task within a second 3 second interval. If it cannot complete this task on either of the two strongest control channels, the mobile station may check the serving-system status: If the serving-system status is enabled, it may be disabled; if the serving-system status is disabled, it may be enabled. The mobile station shall then enter the Scan Dedicated Control Channels Task (see §2.6.1.1.1).

2.6.1.2 Paging channel selection

2.6.1.2.1 Scan paging channels

Set $UPDATE\_NEXTREG_S = 0$.

The mobile station shall examine the signal strength on each of channels $FIRSTCHP_S$ to $LASTCHP_S$ (see §2.6.1.1.2).

The mobile station shall then enter the Verify Overhead Information Task (see §2.6.1.2.2).

2.6.1.2.2 Verify overhead information

The mobile station shall set the Wait-for-Overhead-Message bit ($WFOM_s$) to '0'; the mobile station shall then tune to the strongest paging channel and, within 3 seconds, receive an overhead message train (see §3.7.1.2) and update the following:

- System identification: Set the 14 most significant bits of SID_r to the value of the SID1 field. Set the least significant bit of SID_r to '1' if the serving-system status is enabled; otherwise, set the bit to '0'.
- ROAM status: The mobile station shall compare the received system identification (SID_r) with the stored system identification (SID_s). If $SID_r = SID_s$ the mobile station shall compare SID_s with SID_p. If $SID_p = SID_s$, the mobile station shall set the ROAM status to disabled. If $SID_p \neq SID_s$, the mobile station shall set the ROAM status to enabled. If $SID_r \neq SID_s$, the mobile station shall enter the Retrieve System Parameters Task (see §2.6.1.1).
- Local control status: If the local control option is enabled within the mobile station (see §2.3.9) and the bits of the home system identification (SID_p) that comprise the group identification match the corresponding bits of SID_s, then the local control status shall be enabled. Otherwise, the local control status shall be disabled.
- Power-Up Registration: If $SID_r \neq SID_{s\text{-}p}$ the mobile station shall set $PUREG_{s\text{-}p}$ to '0'.

If the mobile station cannot complete this task on the strongest paging channel, it may tune to the second strongest paging channel and attempt to complete this task within a second 3 second interval. If it cannot complete this task on either of the two strongest paging channels, the mobile station may check the serving-system status: If the serving-system status is enabled, it may be disabled; if the serving-system status is disabled, it may be enabled. The mobile station shall then enter the Scan Dedicated Control Channels Task (see §2.6.1.1.1).

The mobile station shall then enter Idle at the Response to Overhead Information Task (see §2.6.2.1).

2.6.2 Idle

During the Idle Task, a mobile station shall execute each of the following four (sub)tasks (see §§2.6.2.1, 2.6.2.2, 2.6.2.3, and 2.6.2.4) at least every 46.3 ms, the periodicity of word blocks on the forward control channel. If the mobile station is not listening to a control channel of the preferred system, it may exit the Idle task and enter the Retrieve System Parameters Task (see §2.6.1.1).

2.6.2.1 Response to overhead information

Whenever a mobile station receives an overhead message train (see §3.7.1.2), the mobile station shall update SID_r (see §2.6.1.2.2) and then compare SID_s with SID_r. If $SID_s \neq SID_r$,

the mobile station shall exit the Idle Task and enter the Retrieve System Parameters Task (see §2.6.1.1).

If $SID_S = SID_r$, the mobile station shall update the following numeric values using information contained in the system parameter overhead message:

- Serial number bit (S_S): Set S_S to the value in the S field.
- Registration bit (R_S): If the roam status is disabled, set R_S to the value of the REGH field; if the roam status is enabled, set R_S to the value of the REGR field.
- Extended address bit (E_S): Set E_S to the value in the E field.
- Authentication bit ($AUTH_S$): Set $AUTH_S$ to the value in the AUTH field.
- Discontinuous transmission bit (DTX_S): Set DTX_S to the value of the DTX field.
- Number of paging channels (N_S): Set N_S to 1 plus the value of the N-1 field.
- Read-control-filler bit (RCF_S): Set RCF_S to the value of the RCF field.
- Combined paging/access bit (CPA_S): Set CPA_S to the value of the CPA field.
- Number of access channels ($CMAX_S$): Set $CMAX_S$ to 1 plus the value of the CMAX-1 field.
- Determine control channel boundaries for accessing the system ($FIRSTCHA_S$ and $LASTCHA_S$) by using the following algorithm:
  - If the serving-system status is enabled,
    + If $CPA_S = 1$, set $FIRSTCHA_S$ to the first dedicated control channel for System A (834.990 MHz mobile transmit, 879.990 MHz base station transmit).
    + If $CPA_S = 0$, set $FIRSTCHA_S$ to the value of the first dedicated control channel for System A minus N_S.
    + $LASTCHA_S = FIRSTCHA_S - CMAX_S + 1$.
  - If the serving-system status is disabled,
    + If $CPA_S = 1$, set $FIRSTCHA_S$ to the first dedicated control channel for System B (835.020 MHz mobile transmit, 880.020 MHz base station transmit).
    + If $CPA_S = 0$, set $FIRSTCHA_S$ to the value of the first dedicated control channel for System B plus N_S.
    + $LASTCHA_S = FIRSTCHA_S + CMAX_S - 1$.

If $SID_S = SID_{S\text{-}p}$, $PUREG_{S\text{-}p} = 1$ and the first-idle ID status is enabled, the mobile station shall initiate an autonomous registration by entering the System Access Task (see 2.6.3) with a "registration" indication.

If Update Protocol Capability ID status is enabled and $PCSID_s = SID_s$, the mobile station shall initiate protocol capability registration by entering the System Access Task (see 2.6.3) with a "capability registration" indication.

The mobile station shall then respond as indicated to each of the following messages, if received in the overhead message train. The order in which the mobile station shall respond to the messages, if two or more are received, is given by their order in the following list:

1. Local Control Messages: If the local control status is enabled (see §2.6.1.2.2) the mobile station shall respond to the local control messages.

2. Access Type Parameters Message: The mobile station shall perform the following:

   - The mobile station shall set the busy-idle status bit (BIS_s) to the value of the BIS field of the received message.
   - The mobile station shall set PCI_HOME_s to the value of the PCI HOME field of the received message.
   - The mobile station shall set PCI_ROAM_s to the value of the PCI ROAM field of the received message.
   - The mobile station shall set $BSPC_s$ to the value of the BSPC field of the received message.
   - The mobile station shall set $BSCAP_s$ to the value of the BSCAP field of the received message.

   If $BSCAP_s$ indicates that the system supports TIA/EIA 553-A or later revisions of the core analog air interface standard, then

   – If $PCSID_s \neq SID_s$, then

   + If Roam status is enabled and $PCI\_ROAM_s = 1$ or

   + If Roam status is disabled and $PCI\_HOME_s = 1$

   Then, the mobile station shall initiate Protocol Capability registration by entering the System Access Task (§ 2.6.3) with a "capability registration" indication, set Update Protocol Capability ID status to enabled and set $PCSID_s = SID_s$.

3. New Access Channel Set Message:

   - The mobile station shall set $FIRSTCHA_S$ to the value of the NEWACC field of the message.
   - The mobile station shall set $LASTCHA_S$ according to the following algorithm:

   - If the serving-system status is enabled, $LASTCHA_S = NEWACC_T - CMAX_S + 1$.
   - If the serving-system status is disabled, $LASTCHA_S = NEWACC_T + CMAX_S - 1$.

4. Registration Increment Message: The mobile station shall set $REGINCR_S$ to the value of the REGINCR field in the message.

5. Location Area Message: The mobile station shall set $PUREG_S$, $PDREG_S$, $LREG_S$ and $LOCAID_S$ to the values contained in the corresponding fields of the received message and then set $PUREG_{S-p}$ equal to $PUREG_S$.

   - If this message is received while first-idle ID status is disabled, location-registration ID status is disabled, first-registration ID status is enabled, first-location-area ID

status is enabled, and the mobile station is tuned to a control channel different from $LRCC_S$, then the mobile station shall set first-location-area ID status to disabled.

- If $PUREG_S = 1$ and the location-registration ID status is enabled the mobile station shall set the first-registration ID status to enabled (see §2.6.1.1.2) and set first-location-area ID status to disabled (see §2.6.1.1.2). The mobile station shall then initiate an autonomous registration by entering the System Access Task (see §2.6.3) with a "registration" indication.

- If $LOCAID_{S-p} \neq LOCAID_S$ and $LREG_S = 1$ the mobile station shall do the following:

  – if the first-location-area ID status is disabled the mobile station shall set the first-registration ID status to enabled (see §2.6.1.1.2) and then initiate an autonomous registration by entering the System Access Task (§2.6.3) with a "registration" indication.

  – if the first-location-area ID status is enabled and $PUREG_{S-p} = 1$, the mobile station shall set the first-location-area ID status to disabled (see §2.6.1.1.2) and then enter the Autonomous Registration Update Task (see §2.6.3.11), supplying a "success" indication.

  – if the first-location-area ID status is enabled and $PUREG_{S-p} = 0$, the mobile station shall set the first-location-area ID status to disabled (see §2.6.1.1.2) and then initiate an autonomous registration by entering the System Access Task (see §2.6.3) with a "registration" indication.

  Otherwise, the mobile station shall set the first-location-area ID status to disabled (see §2.6.1.1.2).

- The mobile station shall continue to process messages in the overhead message train.

6. Random Challenge A Message: The mobile station shall set the corresponding portion of its internal $RAND1_S$ to the value of the RAND1_A field in the Global Action Message (see §2.3.12.1.2 for updating of RAND)

7. Random Challenge B Message: The mobile station shall set the corresponding portion of its internal $RAND1_S$ to the value of the RAND1_B field in the Global Action Message (see §2.3.12.1.2 for updating of RAND).

8. Registration ID Message: If $R_S = 1$, the mobile station shall perform the following:

   - If this message is received while first-idle ID status is disabled, location-registration ID status is disabled, first-registration ID status is enabled, first-location-area ID status is enabled, and the mobile station is tuned to a control channel different from $LRCC_S$, then the mobile station shall set first-registration ID status to disabled.

   - The mobile station shall set $REGID_S$ to the value of the REGID field of the received message. If the first-registration ID status is enabled, the location-registration ID status is disabled, and $SID_S = SID_{S-p}$, the mobile station shall do the following:

     – set the first-registration ID status to disabled (see §2.6.1.1.2).

– if autonomous registration is enabled, the mobile station shall enter the Autonomous Registration Update Task (see §2.6.3.11), supplying a "success" indication.

– the mobile station shall continue to process information in the overhead message stream.

Otherwise, the mobile station shall set the first-registration ID status to disabled (see §2.6.1.1.2) and proceed as follows.

- If SID_S equals the SID_{S-P} value stored in the registration memory, the mobile station shall perform the following:
  + The mobile station shall use the following (or an equivalent) algorithm to review the $NXTREG_{S-P}$ associated with the SID_{S-P} to determine if $REGID_S$ has cycled through zero:
    > If $UPDATE\_NEXTREG_S = 1$, set $NXTREG_{S-P}$ to $REGID_S + REGINCR_S$, and reset $UPDATE\_NEXTREG_S$ to 0.
    > If $NXTREG_{S-P}$ is greater than or equal to $REGID_S + REGINCR_S + 5$, then $NXTREG_{S-P}$ shall be replaced by the greater of 0 and the value $NXTREG_{S-P} - 2^{20}$
    > Otherwise do not change $NXTREG_{S-P}$.

  + The mobile station shall then compare $REGID_S$ with the $NXTREG_{S-P}$ associated with the SID_{S-P}.
    > If $REGID_S$ is greater than or equal to $NXTREG_{S-P}$, and autonomous registration is enabled, the mobile station shall set the first-registration ID status to disabled (see 2.6.1.1) and then enter the System Access Task with a "registration" indication (see §2.6.3).
    > If $REGID_S$ is greater than or equal to $NXTREG_{S-P}$, and autonomous registration is not enabled, then set $NXTREG_{S-P}$, equal to $REGID_S$.
    > If $REGID_S$ is less than $NXTREG_{S-P}$, the mobile station shall ignore the message and continue to process messages in the overhead message train.

- If SID_S is not equal to the SID_{S-P} value stored in the registration memory, the mobile station shall perform the following:
    > If autonomous registration is enabled, the mobile station shall set the first-registration ID status to disabled (see §2.6.1.1.2). The mobile station shall then enter the System Access Task with a "registration" indication supplied (see §2.6.3).

    > Otherwise, the mobile station shall ignore the message and continue to process messages in the overhead message train.

9. Rescan Message: The mobile station shall immediately exit this task and enter the Initialization Task (see §2.6.1).

10. Any Other Message (including messages and global action types herein defined as 'Reserved'): Use the message for NAWC-counting, but do not attempt to execute the message.

2.6.2.2 Page match

The mobile station shall monitor mobile station control messages for page messages (see §3.7.1.1).

- If the ROAM status is disabled, the mobile station shall attempt to match $MIN1_p$ to $MIN1_r$ for one-word messages and both $MIN1_p$ and $MIN2_p$ to $MIN1_r$ and $MIN2_r$, respectively, for two-word messages. All decoded MIN bits shall match to cause the mobile station to respond to the message.
- If the ROAM Status is enabled, the mobile station shall attempt to match both $MIN1_p$ and $MIN2_p$ to $MIN1_r$ and $MIN2_r$, respectively. All decoded MIN bits shall match to cause the mobile station to respond to the order.

When a match occurs, the mobile station shall enter the System Access Task with a "page response" indication (see §2.6.3).

2.6.2.3 Order

The mobile station shall monitor mobile station control messages for orders and shall attempt to match both $MIN1_p$ and $MIN2_p$ to $MIN1_r$ and $MIN2_r$, respectively. All decoded MIN bits shall match to cause the mobile station to respond to the order. The responses to the following orders are:

- Abbreviated Alert: The mobile station shall enter the System Access Task (see §2.6.3) with an "order confirmation" indication.
- Audit order: The mobile station shall enter the System Access Task (see §2.6.3) with an "order confirmation" indication.
- Local control order: The action to be taken depends on the local control field.
- Protocol capabiltiy indicator order: The mobile station shall enter the System Access Task (see §2.6.3) with a "Protocol Capability Indicator order confirmation" indication.
- SSD update order: The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. The mobile station shall then enter the System Access Task (see §2.6.3) with a "base station challenge" indication.
- Unique challenge order: The mobile station executes the Unique Challenge procedure as in §2.3.12.1.5. The mobile station shall then enter the System Access Task (see §2.6.3) with an "order confirmation" indication.
- Message Waiting Order: If the mobile station is capable of performing message waiting notification, the mobile station shall indicate the presence of messages waiting based on the information contained in the message type field of the Message Waiting order (i.e., 0 for clear or no messages, other non-zero values indicate the number of messages waiting). The mobile station then enters the System Access Task (see §2.6.3) with an "order confirmation" indication.
- Any other order: Ignore order.

2.6.2.4 Call initiation

When the user desires to initiate a call, the System Access Task (see §2.6.3) shall be entered with an "origination" indication.

2.6.2.5 Power Down

If the mobile station is intentionally removed from the air interface while in the Idle Task and $PDREG_S = 1$ the mobile station shall initiate an autonomous registration by entering the System Access Task (see §2.6.3) with a "power down registration" indication.

2.6.3 System access

2.6.3.1 Set access parameters

If a mobile station power down occurs during a system access and $PDREG_S = 1$, the mobile station shall initiate an autonomous registration by continuing this task with a Power Down Registration indication.

When the System Access Task is started, a timer, called the access timer, shall be set as follows:

- If this is an origination, to a maximum of 12 seconds.
- If this is a page response, to a maximum of 6 seconds.
- If this is an order confirmation, to a maximum of 6 seconds.
- If this is a registration other than power down registration, to a maximum of 6 seconds.
- If this is a power down registration, to a maximum of 3 seconds.
- If this is a Base Station Challenge, to a maximum of 12 seconds.

The mobile station shall set the last-try code (LT_S) to 0, set $UPDATE\_NEXTREG_S = 0$, and then enter the Scan Access Channels Task (see §2.6.3.2).

2.6.3.2 Scan access channels

The mobile station shall examine the signal strength on each of the channels $FIRSTCHA_S$ to $LASTCHA_S$ and choose up to two channels with the strongest signals. See §2.6.2.1 Response to Overhead Information Task for access channel set determination.

The mobile station shall then tune to the strongest access channel and enter the Retrieve Access Attempts Parameters Task (see §2.6.3.3).

2.6.3.3 Retrieve access attempt parameters

The mobile station shall set the maximum-number-of-seizure-attempts allowed ($MAXSZTR_{sl}$) to a maximum of 10, and the maximum-number-of-busy-occurrences ($MAXBUSY_{sl}$) to a maximum of 10.

The mobile station shall then initialize the following to zero:

- Number of busy occurrences ($NBUSY_{sv}$)
- Number of unsuccessful seizure attempts ($NSZTR_{sv}$)

The mobile station shall then examine the read control-filler bit (RCF_s).

- If $RCF_s = 0$, the mobile station shall then within 400 ms (+100 ms, -0 ms) set DCC_s to the value in the DCC field of a received message, set $SDCC1_s$ and $SDCC2_s$ to 0, set the power level (PL_s) to 0, and set $WFOM_s = 0$.
- If $RCF_s = 1$, the mobile station shall then within 1000 ms (+100 ms, -0 ms) read a control-filler message, set DCC_s and $WFOM_s$, set $SDCC1_s$ and $SDCC2_s$ to the values in the DCC, WFOM, SDCC1 and SDCC2 fields of the message, respectively, and set PL_s to the power level given by Table 2.1.2-1 for the value of the CMAC field of the message and the mobile station power class (see §§2.1.2.2, 2.3.3, and 3.7.1.2.4).

If the DCC field or the control-filler message is not received within the time allowed, then the mobile station shall examine the access timer. If the access timer has expired, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12). If the access timer has not expired, the mobile station shall enter the Alternate Access Channel Task (see §2.6.3.13).

The mobile station shall then set BIS_s to '1' and examine the $WFOM_s$ bit.

- If $WFOM_s = 1$, the mobile station shall enter the Update Overhead Information Task (see §2.6.3.4).
- If $WFOM_s = 0$, the mobile station shall wait a random delay. Each time it waits a random delay, a different random delay shall be generated with the time uniformly distributed in the interval 0 to 92±1 ms and, if quantized, with granularity no more than 1 ms. The mobile station shall then enter the Seize Reverse Control Channel Task (see §2.6.3.5).

2.6.3.4 Update overhead information

If this task is not completed within 1.5 seconds, the mobile station shall exit this task and enter the Serving-System Determination Task (see §2.6.3.12). If the Update Overhead Information Task is completed, the mobile station shall enter the Seize Reverse Control Channel Task (see §2.6.3.5)

The mobile station shall receive an overhead message train (see §3.7.1.2).

- Authentication bit ($AUTH_s$): Set $AUTH_s$ to the value in the AUTH field.

If the access is a registration, an origination or a page response, the mobile station shall perform the following:

- Update System Identification (SID_r). Set the 14 most significant bits of SID_r to the value of the SID1 field. Set the least significant bit of SID_r to '1' if the serving-system status is enabled; otherwise, set the bit to '0'.
- If the access is a registration, the mobile station shall then compare SID_r with SID_s. If $SID_r \neq SID_s$, then the mobile station shall exit the Update Overhead Information Task and enter the Serving System Determination Task (see §2.6.3.12). Otherwise, the mobile station shall continue to process this task.
- If this access is an origination or a page response, the mobile station shall compare SID_r with $SID_{s\text{-}p}$. IF $SID_r \neq SID_{s\text{-}p}$, the mobile station shall set $RAND_s$ equal to zero.

The mobile station shall act as indicated below in response to the following global action messages, if received in the overhead message train:

• Overload Control Message.

- If this access is an origination, the mobile station shall examine the value of the overload class field (OLC) identified by $ACCOLC_p$. If the identified OLC field is set to '0', the mobile station shall exit this task and enter the Serving-System Determination Task (see §2.6.3.12); if the identified OLC field is set to '1', the mobile station shall continue to respond to messages in the overhead message train.

- Otherwise, the mobile station shall continue to respond to messages in the overhead message train.

• Access Type Parameters Message:

– The mobile station shall set the busy-idle status bit (BIS_s) to the value of the BIS field of the received message.

– The mobile station shall set PCI_HOME_s to the value of the PCI HOME field of the received message.

– The mobile station shall set PCI_ROAM_s to the value of the PCI ROAM field of the received message.

– The mobile station shall set $BSPC_s$ to the value of the BSPC field of the received message.

– The mobile station shall set $BSCAP_s$ to the value of the BSCAP field of the received message.

If $BSCAP_s$ indicates that the system supports TIA/EIA 553-A or later revisions of the core analog air interface standard, then

+ If $PCSID_s \neq SID_s$, , then

  • If Roam status is enabled and $PCI\_ROAM_s = 1$ or

  • If Roam status is disabled and $PCI\_HOME_s = 1$

Then, the mobile station shall set Update Protocol Capability ID status to enabled and set $PCSID_s = SID_s$.

- Random Challenge A Message: The mobile station shall set the corresponding portion of its internal $RAND1_S$ to the value of the RAND1_A field in the Global Action Message (see §2.3.12.1.2 for updating of RAND).

- Random Challenge B Message: The mobile station shall set the corresponding portion of its internal $RAND1_S$ to the value of the RAND1_B field in the Global Action Message (see §2.3.12.1.2 for updating of RAND).

- Access Attempt Parameters Message: The mobile station shall update the following parameters:

  - If this access is a page response,

    + Maximum number of seizure tries allowed ($MAXSZTR_{sl}$) shall be set to the value of the MAXSZTR-PGR field of the received message.
    + Maximum number of busy occurrences allowed ($MAXBUSY_{sl}$) shall be set to the value of the MAXBUSY-PGR field of the received message.

  - Otherwise,

    + Maximum number of seizure tries allowed ($MAXSZTR_{sl}$) shall be set to the value of the MAXSZTR-OTHER field of the received message.
    + Maximum number of busy occurrences allowed ($MAXBUSY_{sl}$) shall be set to the value of the MAXBUSY-OTHER field of the received message.

If the access is a registration access, the mobile station shall respond as indicated to the registration identification message, if received in the overhead message train:

- The mobile station shall set $REGID_S$ to the value of the REGID field in the message.

After the overhead message train is received and processed as required above, the mobile station shall wait a random time. Each time this task is executed, a different random delay shall be generated, distributed uniformly in the interval 0 to 750 ms, and if quantized, with granularity no greater than 1 ms. At the end of the delay, the mobile station shall enter the Seize Reverse Control Channel Task (see §2.6.3.5).

2.6.3.5 Seize reverse control channel

The mobile station shall read the busy-idle status of the channel.

- If the channel is busy, the mobile station shall increment $NBUSY_{sv}$ by 1.

  - If $NBUSY_{sv}$ exceeds $MAXBUSY_{sl}$, then the mobile station shall exit this task and enter the Serving-System Determination Task (see §2.6.3.12).

  - If $NBUSY_{sv}$ does not exceed $MAXBUSY_{sl}$, then the mobile station shall exit this task and the Delay After Failure Task shall be executed (see §2.6.3.6).

- If the channel is idle, then the mobile station shall set $NBUSY_{sv}$ to zero, turn on the transmitter at the power level indicated by PL_S (see §§2.6.3.3 and 2.1.2.2), wait the proper delay (see §2.1.2.1) until the transmitter is within 3 dB of the required power level, and then start to send the message to the base station (see §2.7.1).

If BIS_S = 0, then the mobile station shall enter the Service Request Task (see §2.6.3.7); if BIS_S = 1, then upon starting to send the message, the mobile station shall continuously monitor the busy-idle status of the channel.

- If the channel becomes busy before the first 56 bits of the message are sent, the mobile station shall immediately stop sending the message and turn off the transmitter.
- If the channel fails to change to busy by the time the mobile station has sent 104 bits, then the mobile station shall immediately stop sending the message and turn off the transmitter.

In either of these cases, the mobile station shall then increment the count of seizure failures ($NSZTR_{SV}$) by 1 and compare the result with the maximum number of seizure attempts allowed ($MAXSZTR_{SI}$).

  - If $NSZTR_{SV}$ exceeds $MAXSZTR_{SI}$, the mobile station shall exit this task and enter the Serving-System Determination Task (see §2.6.3.12).
  - If $NSZTR_{SV}$ does not exceed $MAXSZTR_{SI}$, the mobile station shall exit this task and enter the Delay After Failure Task (see §2.6.3.6).

- If the busy-idle status changes to busy after 56 bits and before 104 bits are sent, then the mobile station shall enter the Service Request Task (see §2.6.3.7).

2.6.3.6 Delay after failure

The mobile station shall examine the access timer. If the access timer has expired, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12). If the access timer has not expired, the mobile station shall wait a random time. Each time it enters this task, it shall generate a different time, uniformly distributed in the interval 0 to 200 ms, and if quantized, with granularity no greater than 1 ms. The mobile station shall then enter the Seize Reverse Control Channel Task (see §2.6.3.5).

2.6.3.7 Service request

The mobile station shall continue to send its message to the base station. The information that shall be sent is as follows (with the formats given in §2.7.1):

Word A shall always be sent.

If:

- E_S = 1, or
- LT_S = 1, or
- $AUTH_S$ = 1, or
- the ROAM status is enabled, or
- the ROAM status is disabled and EX_P = 1, or
- the access is an "order confirmation", or
- the access is a "power down registration", or
- the access is a "registration", or
- the access is a "capability registration", or
- the access is a "base station challenge", or
- the mobile station was paged with a two-word mobile station control message, or
- RCF = 1,

THEN word B shall be sent.

Words C shall be sent per the following Table:

S_S Bit	Type of System Access			
	Registration Origination Order Confirmation* Page Response where $AUTH_S = 0$	**Registration Origination Page Response where $AUTH_S = 1$**	**Unique Challenge Order Confirmation**	**Base Station Challenge**
0	Send no Word C	Send Authentication Word C	Send Unique Challenge Order Confirmation Word C	Send Base Station Challenge Word C
1	Send Serial Number Word C	Send Serial Number Word C and Authentication Word C	Send Serial Number Word C and Unique Challenge Order Confirmation Word C	Send Serial Number Word C and Base Station Challenge Word C

* Order Confirmation other than Unique Challenge

Then

- If the access is a "capability registration" and Update Protocol Capability ID status is enabled, then Protocol Capability Indicator Word C shall be sent.
- If the access is a "registration" and Update Protocol Capability ID status is enabled, then Protocol Capability Indicator Word C shall be sent.
- If the access is a "protocol capability indicator order confirmation", then Protocol Capability Indicator Word C shall be sent.
- If the access is an "origination", word D shall be sent.
- If the access is an "origination" and 9 or more were dialed, word E shall be sent.
- If the access is an "origination" and 17 or more digits were dialed, then word F shall be sent.
- If the access is an "origination" and 25 to 32 digits were dialed, then word G shall be sent..

When the mobile station has sent its complete message, it shall continue to send unmodulated carrier for a nominal duration of 25 ms and then turn off the transmitter.

The next task to be entered depends on the type of access by the mobile station:

- If the access is an order confirmation, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).
- If the access is an origination, the mobile station shall enter the Await Message Task (see §2.6.3.8).
- If the access is a page response, the mobile station shall enter the Await Message Task (see §2.6.3.8).
- If the access is a registration request (including capability registration) other than a power down registration, the mobile station shall enter the Await Registration Confirmation Task (see §2.6.3.9). If the registration is a power down registration the mobile station shall power down.
- If the access is a base station challenge the mobile station shall enter the Await Message Task (see §2.6.3.8).
- If the access is a protocol capability indicator order confirmation, the mobile station shall enter the Await Message Task (see §2.6.3.8).

2.6.3.8 Await message

If this task is not completed within 10 seconds for a Base Station Challenge or within 5 seconds for other access types, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

The mobile station shall monitor mobile station control messages (see §3.7.1.1). If the mobile station sent Word B as part of the Service Request (see §2.6.3.7), then the mobile station shall attempt to match $MIN1_p$ and $MIN2_p$ to $MIN1_r$ and $MIN2_r$, respectively; otherwise, the mobile station shall attempt to match only $MIN1_p$ to $MIN1_r$.

The mobile station shall respond as indicated to any of the following messages if all decoded MIN bits match.

If the access is an origination or page response:

- Initial Voice Channel Designation Message (see §3.7.1.1): The mobile station shall update the parameters as set in the message. If R_S = 1, the mobile station shall enter the Autonomous Registration Update Task (see §2.6.3.11), supplying a "success" indication. Then enter the Confirm Initial Voice Channel Task (see §2.6.4.2).
- Directed-retry message (see §3.7.1.1): If the mobile station is equipped for directed retry, it shall respond to the directed-retry message as follows:

  If the mobile station encounters the start of a new message before it receives all four words of the directed-retry message, it shall exit this task and enter the Serving-System Determination Task (see §2.6.3.12).

  The mobile station shall set the last-try code (LT_S) according to the ORDQ field of the message:

  - If ORDQ = '000', set LT_S to '0'.
  - If ORDQ = '001', set LT_S to '1'.

The mobile station shall then clear $CCLIST_S$ and examine each CHANPOS field in Words 3 and 4 of the message. For each nonzero CHANPOS field, the mobile station shall calculate a corresponding channel number according to the following algorithm:

- If the serving-system status is enabled, subtract CHANPOS from $FIRSTCHA_S + 1$.
- If the serving-system status is disabled, add CHANPOS to $FIRSTCHA_S - 1$.

The mobile station shall then determine whether each channel number is within the set allocated to cellular systems, and if so, list the channel number in $CCLIST_S$.

After completing its response to the directed-retry message, the mobile station shall examine the access timer. If the access timer has expired, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12). If the access timer has not expired, the mobile station shall enter the Directed-Retry Task (see §2.6.3.14).

If the access is an origination:

- Intercept: The mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).
- Reorder: The mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

If the access is a page response:

- Release: The mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

If the access is a Protocol Capability Indicator order confirmation:

- Release: The mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).
- Message Waiting Order: If the mobile station is capable of performing Message Waiting Notification, the mobile station shall indicate the presence of messages waiting based on the information contained in the messages type field of the Message Waiting order (that is, 0 for no messages, non-zero values indicate the number of messages waiting). The mobile station then enters the System Access Task (see §2.6.3) with an "order confirmation" indication.

If the access is a Base Station Challenge:

- Base Station Challenge Order Confirmation: The mobile station compares the AUTHBS received in the Base Station Challenge Order Confirmation message to that computed internally. The mobile station shall then acknowledge receipt of the SSD Update Order with a success or failure indication as described in §2.3.12.1.8 by entering the System Access task (see §2.6.3) with an "order confirmation" indication (see §2.6.3.1). If the mobile station fails to receive the Base Station Challenge Order Confirmation within 10 seconds of when the Base Station Challenge Order was transmitted, terminate the SSD update process.

If the access is an origination and the user terminates a call during this task, the termination status shall be enabled so that the call can be released on a voice channel (see §2.6.4.4) instead of on a control channel.

2.6.3.9 Await registration confirmation

If this task is not completed within 5 seconds, the mobile station shall exit this task and enter the Action on Registration Failure Task (see §2.6.3.10).

The mobile station shall monitor mobile station control messages (see §3.7.1.1). If the mobile station sent Word B as part of the Service Request (see §2.6.3.7), then the mobile station shall attempt to match $MIN1_p$ and $MIN2_p$ to $MIN1_r$ and $MIN2_r$, respectively; otherwise, the mobile station shall attempt to match only $MIN1_p$ to $MIN1_r$.

The mobile station shall respond as indicated to any of the following messages if all decoded MIN bits match:

- Release order (see §3.7.1.1): The mobile station shall exit this task and enter the Action on Registration Failure Task (see §2.6.3.10).
- Order confirmation (see §3.7.1.1) [1]: If $R_S = 1$ or $PUREG_{S-p} = 1$ or $LREG_S = 1$ or Update Protocol Capability ID status is enabled, the mobile station shall enter the Autonomous Registration Update Task (see §2.6.3.11), supplying a "success" indication; the mobile station shall then compare the Paging Channel set to the access channel set.

  - If ($FIRSTCHP_S \neq FIRSTCHA_S$) OR ($LASTCHP_S \neq LASTCHA_S$), the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12),
  - Otherwise, the mobile station shall set $UPDATE\_NEXTREG_S = 1$, set the Wait-for-Overhead-Message bit (WFOMs) = 0, and within 3 seconds, receive an overhead message train (see §3.7.1.2) and update the following:
    + System identification: Set the 14 most significant bits of SID_r to the value of the SID1 field. Set the least significant bit of SID_r to '1' if the serving-system status is enabled; otherwise, set this bit to '0'.
    + ROAM status: The mobile station shall compare the received system identification (SID_r) with the stored system identification (SID_s). If $SID_r = SID_s$, the mobile station shall compare SID_s with SID_p. If $SID_p = SID_s$, the mobile station shall set the ROAM status to disabled. If $SID_p \neq SID_s$, the mobile station shall set the ROAM status to enabled. If $SID_r \neq SID_s$, the mobile station shall enter the Retrieve System Parameters Task (see §2.6.1.1.)
    + Local control status: If the local control option is enabled within the mobile station (see §2.3.9) and the bits of the home system identification (SID_p) that

---

[1] The MS will wait for an order confirmation message that has the same ORDER/ORDERQ codes as the message that is awaiting confirmation. If the mobile station sent a capability registration or a registration with PCI word C, the mobile station will wait for a confirmation with the order code set to the PCI order code. If the mobile station sent a registration without PCI word C then it will wait for a confirmation with the order code set to the registration order code.

comprise the group identification match the corresponding bits of SID_S, then local control status shall be enabled. Otherwise, local control status shall be disabled.

The mobile station shall then enter the Response to Overhead Information Task (see §2.6.2.1.)

If the mobile station cannot complete this task, it may check the serving-system status: If serving-system status is enabled, it may be disabled; if serving-system status is disabled, it may be enabled. The mobile station shall then enter the Scan Dedicated Control Channels Task (see §2.6.1.1.1.)

2.6.3.10 Action on registration failure

If Rs = 1 or $PUREG_{S-P}$ = 1 or $LREG_S$ = 1, the mobile station shall enter the Autonomous Registration Update Task (see §2.6.3.11), supplying a "failure" indication; the mobile station shall then enter the Serving-System Determination Task (see §2.6.3.12). Otherwise, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

2.6.3.11 Autonomous registration update

If the first-location area ID status is enabled, the first-registration ID status is enabled, the first-idle ID status is enabled and if a "success" indication was supplied to this task, the mobile station shall set the location-registration ID status to disabled.

If the first-location-area ID status is disabled and a "success" indication was supplied to this task, the mobile station shall set $LOCAID_{S-P}$ equal to $LOCAID_S$ and shall set location-registration ID status to disabled.

If the first-registration ID status is disabled and a "success" indication was supplied to this task, the mobile station shall set SID_{S-P} equal to SID_S, set $NXTREG_{S-P}$ equal to $REGID_S$ + $REGINCR_S$ and set location-registration ID status to disabled.

If the first-registration ID status is disabled and a "failure" indication was supplied to this task, the mobile station shall do the following:

- generate a random number ($NRANDOM_{SV}$). Each time this step is executed, a random number shall be generated, uniformly distributed in the interval 0 to 10, and with granularity no more than 1.
- set $NXTREG_{S-P}$ equal to $REGID_S$ + $NRANDOM_{SV}$.

If the Update Protocol Capability ID status is enabled and a "success" indication was supplied to this task, the mobile station shall set Update Protocol Capability ID status to disabled.

If a "success" indication was supplied to this task, the mobile station shall set $LRCC_S$ equal to the current control channel.

The mobile station shall set the first-idle ID status to disabled and then return to the invoking task.

2.6.3.12 Serving-system determination

If this task is entered as a result of a power down registration attempt the mobile station shall immediately power down. If this task is entered for any other reason, and if the serving-system status does not correspond to the preferred system, the mobile station may enter the Retrieve System Parameters Task (see §2.6.1.1); otherwise, it shall enter the Paging Channel Selection Task (see §2.6.1.2).

2.6.3.13 Alternate access channel

If the mobile station is tuned to the strongest access channel, it may tune to the second strongest channel and then enter the Retrieve Access Attempt Parameters Task (see §2.6.3.3). Otherwise, it shall enter the Serving-System Determination Task (see §2.6.3.12).

2.6.3.14 Directed retry

The mobile station shall examine the signal strength on each of the channels listed in $CCLIST_S$ and choose up to two channels with the strongest signals. The mobile station shall then tune to the strongest access channel and enter the Retrieve Access Attempt Parameters Task (see §2.6.3.3).

2.6.4 Mobile station control

2.6.4.1 Loss of radio link continuity

While the mobile station is tuned to a voice channel, it shall monitor the fade timing status (see §2.4.1.3). If the fade timing status is enabled, a fade timer shall be started; each time the fade timing status is disabled, the timer shall be reset. If the timer counts to 5 seconds, the mobile station shall turn off its transmitter; and enter the Serving-System Determination Task (see §2.6.3.12).

2.6.4.2 Confirm initial voice channel

Within 100 ms of the receipt of the initial voice channel designation (see §3.7.1.1), the mobile station shall determine whether the channel number is within the set allocated to cellular systems, and

- If it is within the allocated set, the mobile station shall tune to the designated voice channel, turn on the transmitter at the power level indicated by the VMAC field of the initial voice channel message (see §§2.1.2.2 and 3.7.1.1), turn on the SAT transponder (see §2.4.1), and set the stored SAT Color Code (SCC_S) to the value of the SCC field of the initial voice channel message (see §3.7.1.1). Discontinuous transmission (see §2.3.11) is prohibited while the mobile station is in this task. That is, a mobile station capable of discontinuous-transmission operation shall remain in the DTX-high state.

- If this is an origination access, the mobile station then shall enter the Conversation Task (see §2.6.4.4).
- If this is a page response access, the mobile station then shall enter the Waiting for Order Task (see §2.6.4.3.1).

• Otherwise, the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

2.6.4.3 Alerting

2.6.4.3.1 Waiting for order

Discontinuous transmission (see §2.3.11) is prohibited while the mobile station is in this task. That is, a mobile station capable of discontinuous-transmission operation shall remain in the DTX-high state. When this task is entered, an order timer shall be set to 5 seconds. The following may occur:

• If the order timer expires the mobile station shall turn off the transmitter; then the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).

• The mobile station may receive a Base Station Challenge Order Confirmation as part of the SSD Update process (see §2.3.12.1.8). The mobile station shall compare the AUTHBS received in the Base Station Challenge Order Confirmation message with that computed internally. Then, within 750 ms, the mobile station shall begin transmitting an acknowledge of the SSD Update Order with a success or failure indication as described in §2.3.12.1.8. Remain in the Waiting for Order task. If the mobile station fails to receive the Base Station Challenge Order Confirmation within 10 seconds of when the Base Station Challenge Order was transmitted, terminate the SSD update process. Reset the order timer to 5 seconds and remain in the Waiting for Order task.

• Within 100 ms of the receipt of any of the orders listed below (see §3.7.2), the mobile station shall compare SCC_S to the present SAT color code (PSCC) field in the received message. If $SCC_S \neq PSCC$, the order shall be ignored. If $SCC_S = PSCC$, the order timer shall be ignored for the duration of the processing of the order and the action to be taken for each order is as follows:

  - Handoff: Turn on signaling tone for 50 ms, turn off signaling tone, turn off transmitter, adjust power level, tune to new channel, adjust to new SAT, set SCC_S to the value of the SCC field of the message (see §2.4.1), turn on transmitter, reset fade timer, remain in the Waiting for Order Task (§2.6.4.3.1), and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.
  - Alert or Alert With Info: Turn on signaling tone, wait 500 ms, and enter the Waiting for Answer Task (see §2.6.4.3.2).
  - Release: Enter Release Task (see §2.6.4.5).
  - Audit: Send order confirmation message to base station (see §2.7.2), remain in the Waiting for Order Task, and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- Message Waiting Order: If the mobile station is capable of performing message waiting notification, the mobile station shall indicate the presence of messages waiting based on the information contained in the message type field of the Message Waiting order (i.e., 0 for clear or no messages, other non-zero values indicate the number of messages waiting). The mobile station shall send an order confirmation to the base station (see 2.7.2), reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response and remain in the Waiting for Order Task.

- Maintenance: Turn on signaling tone, wait 500 ms, and enter the Waiting for Answer Task (see §2.6.4.3.2).

- Change Power: Adjust the transmitter to the power level indicated by the order qualification code (see §§3.7.1.1 and 2.1.2.2) and send order confirmation message to base station (see §2.7.2). Remain in the Waiting for Order Task, and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- Local Control: If the local control status is enabled (see §2.6.1.2.2) and a local control order is received, the local control field shall be examined to determine the action and confirmation to take.

- Protocol Capability Indicator: Send the Protocol Capability Indicator report message (see §2.7.2). Remain in the Waiting for Order Task, and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- Serial Number Request: Reply with Serial Number Response Message. The mobile station shall remain in the Waiting for Order Task, and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- SSD Update Order: The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, the mobile station shall begin transmitting a Base Station Challenge Order. Remain in the Waiting for Order task and reset the order timer to 10 seconds.

- Unique Challenge Order: The mobile station executes the Unique Challenge procedure as described in §2.3.12.1.5. Within 750 ms, the mobile station shall begin transmitting an "unique challenge order confirmation" message to the base station (see §2.7.2). Remain in the current task and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- Message Encryption Mode Order; The base station is activating/deactivating signaling message encryption. If the order qualifier field in the received message is set to '001', activate signaling message encryption. If the order qualifier field in the received message is set to '000', deactivate signaling message encryption. In either case, send an "order confirmation" message to the base station (see §2.7.2), remain in the Waiting for Order Task and reset the order timer to 10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response.

- Parameter Update Order: Increment $COUNT_{s\text{-}p}$ (see §2.3.12.1.3), send an order confirmation message to the base station (see §2.7.2) and reset the order timer to

10 seconds if the mobile station is waiting for a response to a Base Station Challenge order, or to 5 seconds if waiting for any other response. Remain in the Waiting for Order task.

- Any other order: Ignore order.

2.6.4.3.2 Waiting for answer

Discontinuous transmission (see §2.3.11) is prohibited while the mobile station is in this task. That is, a mobile station capable of discontinuous-transmission operation shall remain in the DTX-high state. When this task is entered, an alert timer shall be set to 65 seconds (-0, +20%). The following may occur:

- If the alert timer expires the mobile station shall turn off the transmitter; then the mobile station shall enter the Serving-System Determination Task (see §2.6.3.12).
- If the user answers, signaling tone shall be turned off and the Conversation Task (see §2.6.4.4) shall be entered.
- The mobile station may receive a Base Station Challenge Order Confirmation as part of the SSD Update process (see §2.3.12.1.8). The mobile station shall compare the AUTHBS received in the Base Station Challenge Order Confirmation message with that computed internally. Then, within 750 ms, the mobile station shall begin transmitting an acknowledge of the SSD Update Order with a success or failure indication as described in §2.3.12.1.8. Remain in the Waiting for Answer task. If the mobile station fails to receive the Base Station Challenge Order Confirmation within 10 seconds of when the Base Station Challenge Order was transmitted, terminate the SSD update process. The mobile station shall remain in the Waiting for Answer task.
- Within 100 ms of the receipt of any of the orders listed below, the mobile station shall compare SCC_S to the PSCC field in the received message. If $SCC_S \neq$ PSCC, the order shall be ignored. If SCC_S = PSCC, the action to be taken for each order is as follows:
  - Handoff: Turn off signaling tone for 500 ms, turn on signaling tone for 50 ms, turn off signaling tone, turn off transmitter, adjust power level, tune to new channel, adjust to new SAT, set SCC_S to the value of the SCC field of the message (see §2.4.1), turn on transmitter, reset fade timer, and turn on signaling tone. Then remain in the Waiting for Answer task (§2.6.4.3.2).
  - Alert or Alert With Info: Remain in the Waiting for Answer Task, and reset the alert timer to 65 seconds.
  - Stop Alert: Turn off signaling tone, and enter the Waiting for Order Task (see §2.6.4.3.1).
  - Release: Turn off signaling tone, wait 500 ms, and then enter the Release Task (see §2.6.4.5).
  - Audit: Send order confirmation message to base station (see §2.7.2) and remain in the Waiting for Answer Task.
  - Flash With Info: Send order confirmation message to the base station (see 2.7.2) and remain in the Waiting for Answer Task.
  - Message Waiting Order: If the mobile station is capable of performing message waiting notification, the mobile station shall indicate the presence of messages waiting based on the information contained in the message type field of the

Message Waiting order (i.e., 0 for clear or no messages, other non-zero values indicate the number of messages waiting). The mobile station shall send an order confirmation to the base station (see 2.7.2) and remain in the Waiting for Answer Task.

- Maintenance: Remain in the Waiting for Answer Task, and reset the alert timer to 65 seconds.
- Change power: Adjust the transmitter to the power level indicated by the order qualification code (see §§3.7.1.1 and 2.1.2.2) and send order confirmation message to base station (see §2.7.2). Remain in the Waiting for Answer Task.
- Local Control: If the local control status is enabled (see §2.6.1.2.2) and a local control order is received, the local control field shall be examined to determine the action and confirmation to take.
- Protocol Capability Indicator: Send the Protocol Capability Indicator report message (see §2.7.2) and remain in the Waiting for Answer Task.
- Serial Number Request: Reply with the Serial Number Response message. The mobile station shall remain in the Waiting for Answer Task.
- SSD Update Order: The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, the mobile station shall begin transmitting a Base Station Challenge Order. Remain in the Waiting for Answer task .
- Unique Challenge Order: The mobile station executes the Unique Challenge procedure as described in §2.3.12.1.5. Within 750 ms, the mobile station shall begin transmitting an "unique challenge order confirmation" message to the base station (see §2.7.2). Remain in the current task.
- Message Encryption Mode Order; The base station is activating/deactivating signaling message encryption. If the order qualifier field in the received message is set to '001', activate signaling message encryption. If the order qualifier field in the received message is set to '000', deactivate signaling message encryption. In either case, send an "order confirmation" message to the base station (see §2.7.2) and remain in the Waiting for Answer Task.
- Parameter Update Order: Increment $COUNT_{s\text{-}p}$ (see §2.3.12.1.3) and send an order confirmation message to the base station (see §2.7.2). Remain in the Waiting for Answer task.
- Any other order: Ignore order.

2.6.4.4 Conversation

When this task is entered, a release-delay timer shall be set to 500 ms. If the termination status is enabled (see §2.6.3.8), the mobile station shall set the termination status to disabled, wait 500 ms and then enter the Release Task (see §2.6.4.5).

Discontinuous transmission (see §2.3.11) shall be inhibited for 1.5 seconds after the mobile station enters this task. That is, for at least 1.5 seconds after entering this task, a mobile station capable of discontinuous-transmission operation shall remain in the DTX-high state.

In the conversation state; the following may occur:

- If the user terminates the call, the release-delay timer shall be examined. If the timer has expired, the Release Task shall be entered (see §2.6.4.5). If the timer has not expired, the mobile station shall wait until the timer expires and then enter the Release Task.

- On power down or when possible low battery turn off, the release-delay timer shall be examined. If the timer has expired, the Power Down Task shall be entered (see §2.6.4.6). If the timer has not expired, the mobile station shall wait until the timer expires and then enter the Release Task.

- If the user requests a flash, the mobile station shall take the following steps. Mobile stations capable of discontinuous-transmission operation (see §2.3.11) shall inhibit discontinuous transmission for 1.5 seconds; that is, for at least 1.5 seconds the mobile station shall remain in the DTX-high state. Immediately following the flash, a mobile station not capable of discontinuous transmission or a mobile station capable of discontinuous transmission but in the DTX-high state shall turn on signaling tone for 400 ms.

  If the mobile station is capable of discontinuous transmission and is in the DTX-low state or the transition state when the flash occurs, the mobile station shall enter the DTX-high state and wait 200 ms. Then it shall turn on signaling tone for 400 ms. If a valid order (one that is not ignored) is received while processing a flash, the flash shall be terminated immediately and the order shall be processed. Flashes so terminated are not considered valid.

- The mobile station may receive a Base Station Challenge Order Confirmation as part of the SSD Update process (see §2.3.12.1.8). The mobile station shall compare the AUTHBS received in the Base Station Challenge Order Confirmation message with that computed internally. Then, within 750 ms, the mobile station shall begin transmitting an acknowledge of the SSD Update Order with a success or failure indication as described in §2.3.12.1.8. Remain in the Conversation task. If the mobile station fails to receive the Base Station Challenge Order Confirmation within 10 seconds of when the Base Station Challenge Order was transmitted, terminate the SSD update process. The mobile station shall remain in the Conversation task.

- Within 100 ms of the receipt of any of the orders listed below, the mobile station shall compare SCC_S to the PSCC field in the received message. If $SCC_S \neq$ PSCC, the order shall be ignored. If SCC_S = PSCC, the mobile station shall take the following steps. Except for the audit order, mobile stations capable of discontinuous-transmission operation (see §2.3.11) shall inhibit discontinuous transmission for 1.5 seconds; that is, for at least 1.5 seconds the mobile station shall remain in the DTX-high state. Upon receipt of the audit order, mobile stations capable of discontinuous transmission shall inhibit discontinuous transmission for at least 5 seconds. Immediately after determining that SCC_S = PSCC a mobile station not capable of discontinuous transmission or a mobile station capable of discontinuous transmission but in the DTX-high state shall take the actions specified below for each order.

  If the mobile station is capable of discontinuous transmission and is in the DTX-low state or the transition state when the order arrives, the mobile station shall enter the DTX-high state and wait 200 ms. Then it shall take the actions specified below for each order.

  - Handoff: Turn on signaling tone for 50 ms, turn off signaling tone, turn off transmitter, adjust power level, tune to new channel, adjust to new SAT, set SCC_S

to the value of the SCC field of the message (see §2.4.1), turn on transmitter, reset fade timer, and remain in the Conversation Task.

- Send Called-Address:
  + If received within 10 seconds of the completion of the last valid flash, send the called-address to the base station (see §2.7.2) and remain in the Conversation Task.
  + Otherwise, ignore the order and remain in the Conversation Task.

- Disable DTMF Order: Send an order confirmation message to the base station (see §2.7.2). The mobile station shall then disable its DTMF tone generator until the Called Address Message sent to the base station in response to the next Send Called-Address message received by the mobile station has been completely transmitted. The mobile station shall remain in the Conversation Task.

- Alert or Alert With Info: Turn on signaling tone, wait 500 ms, and then enter the Waiting for Answer Task (see §2.6.4.3.2).

- Release: Examine the release-delay timer. If the timer has expired, the mobile station shall enter the Release Task (see §2.6.4.5). If the timer has not expired, the mobile station shall wait until the timer expires and then enter the Release Task.

- Audit: Send order confirmation message to base station (see §2.7.2) and remain in the Conversation Task.

- Flash With Info: Send order confirmation message to the base station (see 2.7.2) and remain in the Conversation Task.

- Message Waiting Order: If the mobile station is capable of performing message waiting notification, the mobile station shall indicate the presence of messages waiting based on the information contained in the message type field of the Message Waiting order (i.e., 0 for clear or no messages, other non-zero values indicate the number of messages waiting). The mobile station shall send an order confirmation to the base station (see 2.7.2) and remain in the Conversation Task.

- Maintenance: Turn on signaling tone, wait 500 ms, and then enter the Waiting for Answer Task (see §2.6.4.3.2).

- Change power: Adjust the transmitter to the power level indicated by the order qualification code (see §§3.7.1.1 and 2.1.2.2) and send order confirmation message to base station (see §2.7.2). Remain in the Conversation Task. If the mobile station is capable of discontinuous transmission and is in the DTX-low state or the transition state when this order arrives, the mobile station shall immediately enter the DTX-high state at the power level indicated in the order.

- Local Control: If the local control status is enabled (see §2.6.1.2.2) and a local control order is received, the local control field shall be examined to determine the action and confirmation to take.

- Protocol Capability Indicator: Send the Protocol Capability Indicator report message (see §2.7.2) and remain in the Conversation Task.

- Serial Number Request: Reply with Serial Number Response message. The mobile station shall remain in the Conversation Task.

- SSD Update Order: The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, the mobile station

shall begin transmitting a Base Station Challenge Order. Remain in the Conversation task .

- Unique Challenge Order: The mobile station executes the Unique Challenge procedure as described in §2.3.12.1.5. Within 750 ms, the mobile station shall begin transmitting an "unique challenge order confirmation" message to the base station (see §2.7.2). Remain in the Conversation task.
- Message Encryption Mode Order; The base station is activating/deactivating signaling message encryption. If the order qualifier field in the received message is set to '001', activate signaling message encryption. If the order qualifier field in the received message is set to '000', deactivate signaling message encryption. In either case, send an "order confirmation" message to the base station (see §2.7.2) and remain in the Conversation Task.
- Parameter Update Order: Increment $COUNT_{s-p}$ (see §2.3.12.1.3) and send an order confirmation message to the base station (see §2.7.2). Remain in the Conversation task.
- Any other order: Ignore order.

2.6.4.5 Release

Discontinuous transmission (see §2.3.11) is prohibited while the mobile station is in this task. That is, a mobile station capable of discontinuous-transmission operation shall remain in the DTX-high state. Any mobile station in the DTX-low state shall immediately enter the DTX-high state, wait 200 ms, and take the following action:

- Send signaling tone for 1.8 seconds. If a flash (see §2.6.4.4) was being sent when this task was entered, signaling tone shall continue to be sent and the timing bridged so that no more than 1.8 seconds of signaling tone is sent.
- Stop sending signaling tone.
- Turn off the transmitter.

The mobile station shall then enter the Serving-System Determination Task (see §2.6.3.12).

2.6.4.6 Power down

If the mobile station is intentionally removed from the air interface while it is tuned to analog voice channel, the mobile shall immediately prohibit discontinuous transmission (see §2.3.11). That is, a mobile station capable of discontinuous transmission operation shall remain in the DTX-high state. Any mobile station in the DTX-low state shall immediately enter the DTX-high state, wait 200 ms. While in the DTX-high state, the mobile station shall do the following:

- If $PDREG_s$ = 1 the mobile station shall send an autonomous registration message with a power down indication on the reverse voice channel.
- Send signaling tone for 1.8 seconds. If a flash (§2.6.4.4) was being sent when this task was entered, signaling tone shall continue to be sent for no more than 1.8 seconds.
- Stop sending signaling tone, turn off the transmitter and then power down.

2.7 Signaling formats

In the message formats used between the mobile stations and base stations, some bits are marked as reserved (RSVD). Some or all of these reserved bits may be used in the future for additional messages. Therefore, all mobile stations and base stations shall set all bits that they are programmed to treat as reserved bits to "0" (zero) in all messages that they transmit unless specified otherwise. All mobile stations and base stations shall ignore the state of all bits that they are programmed to treat as reserved bits in all messages that they receive.

In the specific case of overhead messages on the Forward Control Channel, if the mobile station receives a BCH-code-correct but unrecognizable overhead message (including Global Action Message types), the mobile station shall count that message as part of the train for NAWC-counting purposes, but shall not attempt to execute the message. All other messages and fields of an overhead message train that carries a message type herein indicated as 'Reserved' shall be decoded and used as appropriate.

Implementors of mobile stations are cautioned that many other functions and features are deployed on the FOCC than those described in this standard. These functions frequently employ bits indicated herein as 'Reserved.' Reference may be made to the current version of TSB-70 for details.

2.7.1 Reverse control channel

The reverse control channel (RECC) is a wideband data stream sent from the mobile station to the base station. This data stream shall be generated at a 10 kbit/s±1 bit/s rate. Figure 2.7.1-1 depicts the format of the RECC data stream.

Figure 2.7.1-1 Reverse control channel message stream

DOTTING	WORD SYNC	CODED DCC*	FIRST WORD REPEATED 5 TIMES	SECOND WORD REPEATED 5 TIMES	THIRD WORD REPEATED 5 TIMES	...
30	11	7	240	240	240	
Seizure Precursor						

DOTTING = 1010...010

WORD SYNC = 11100010010

* DIGITAL COLOR CODE - Coded per Table 2.7.1-1.

All messages begin with the RECC seizure precursor that is composed of a 30 bit dotting sequence (1010...010), an 11 bit word sync sequence (11100010010), and the coded digital color code (DCC). The 7 bit coded DCC is obtained by translating the received DCC according to Table 2.7.1-1.

Table 2.7.1-1 Coded digital color code

Received DCC	7-Bit Coded DCC
00	0000000
01	0011111
10	1100011
11	1111100

Each word contains 48 bits, including parity, and is repeated five times; it is then referred to as a word block. A word is formed by encoding 36 content bits into a (48, 36) BCH code that has a distance of 5, (48, 36; 5). The left-most bit (i.e., earliest in time) shall be designated the most significant bit. The 36 most significant bits of the 48 bit field shall be the content bits. The generator polynomial for the code is the same as for the (40, 28; 5) code used on the forward control channel (see §3.7.1).

2.7.1.1 RECC messages

Each RECC message can consist of one to seven words. The types of messages to be transmitted over the reverse control channel are:

- Page Response Message
- Origination Message
- Order Confirmation Message
- Order Message

These messages are made up of combinations of the following seven words. Note: If included, words are to be transmitted in the order shown.

Word A - Abbreviated Address Word

F = 1	NAWC	T	S	E	ER	SCM (3-0)	$MIN1_{23-0}$	P
1	3	1	1	1	1	4	24	12

Word B - Extended Address Word

F = 0	NAWC	LOCAL/ MSG_TYPE	ORDQ	ORDER	LT	EP	SCM(4)	MPCI	
1	3	5	3	5	1	1	1	2	

	SDCC1	SDCC2	$MIN2_{33-24}$	P
	2	2	10	12

Word C - Serial Number Word

F = 0	NAWC	SERIAL	P
1	3	32	12

Word C - Authentication Word

F=0	NAWC	COUNT	RANDC	AUTHR	P
1	3	6	8	18	12

Word C - Unique Challenge Order Confirmation Word

F=0	NAWC	RSVD=0...0	AUTHU	P
1	3	14	18	12

Word C - Base Station Challenge Word

F=0	NAWC	RANDBS	P
1	3	32	12

Word C - Protocol Capability Indicator Word

F=0	NAWC	MSPC	MSCAP	RSVD	P
1	3	4	3	25	12

Word D - First Word of the Called-Address

F = 0	NAWC	1st DIGIT	2nd DIGIT	...	...	...	...	7th DIGIT	8th DIGIT	P
1	3	4	4	4	4	4	4	4	4	12

Word E - Second Word of the Called-Address

F = 0	NAWC	9th DIGIT	10th DIGIT	...	...	...	...	15th DIGIT	16th DIGIT	P
1	3	4	4	4	4	4	4	4	4	12

Word F - Third Word of the Called-Address

F = 0	NAWC	17th DIGIT	18th DIGIT	...	...	...	...	23rd DIGIT	24th DIGIT	P
1	3	4	4	4	4	4	4	4	4	12

Word G - Fourth Word of the Called-Address

F = 0	NAWC = 000	25th DIGIT	26th DIGIT	...	...	...	...	31st DIGIT	32nd DIGIT	P
1	3	4	4	4	4	4	4	4	4	12

The interpretation of the data fields is as follows:

F	First word indication field. Set to '1' in first word and '0' in subsequent words.
NAWC	Number of additional words coming field.
T	T field. Set to '1' to identify the message as an origination or an order (including any registration); set to '0' to identify the message as an order response (including Protocol Capability Indicator response) or page response.
S	Send serial number field. If the serial number word is sent, set to '1'; if the serial number word is not sent, set to '0'.
E	Extended address field. If the extended address word is sent, set to '1'; if the extended address word is not sent, set to '0'.

SCM (3-0)	The station class mark field (see §2.3.3).
SCM (4)	The station class mark field (see §2.3.3).
MPCI	00 indicates ANSI TIA/EIA 553A, ANSI EIA/TIA 553, or IS-54A mobile stations. 01 indicates ANSI TIA/EIA 627 dual-mode mobile stations. 10 indicates TIA/EIA-95 dual-mode mobile stations. 11 indicates IS-136 dual-mode mobile stations.
ORDER	Order field. Identifies the order type (See Table 3.7.1-1).
ORDQ	Order qualifier field. Qualifies the order confirmation to a specific action (see Table 3.7.1-1).
LOCAL	Local control field. This field is specific to each system. The ORDER field shall be set to local control (see Table 3.7.1-1) for this field to be interpreted.
MSG_TYPE	Message type field. Qualifies the order to a specific action (see Table 3.7.1-1).
ER	Extended Protocol Reverse Channel. (Set to zero. Zero indicates not extended protocol capable. For other values see ANSI TIA/EIA 691).
EP	Extended Protocol Capable. (Set to zero for ANSI TIA/EIA 553A systems. Zero indicates not extended protocol capable. For other values see ANSI TIA/EIA 691).
LT	Last-try code field (see §2.6.3.8).
SDCC1, SDCC2	Supplementary Digital Color Codes. If the Supplementary Digital Color Code feature is utilized, the combination of SDCC1 and SDCC2 transmitted by the base station shall be a non-zero number. Mobile stations which respond with a non-zero SDCC combination are capable of supporting SDCC. Mobile stations which respond with a zero SDCC combination are not capable of supporting SDCC. The zero SDCC combination is used to indicate either that SDCC1 and SDCC2 are not used or are not supported.
MIN1	First part of the mobile identification number field (see §2.3.1).
MIN2	Second part of the mobile identification number field (see §2.3.1).
SERIAL	Electronic Serial Number field. Identifies the electronic serial number of the mobile station (see §2.3.2).
DIGIT	Digit field (see Table 2.7.1-2).
RSVD	Reserved for future use; all bits shall be set as indicated.
P	Parity field.
COUNT	A modulo-64 count maintained by the mobile station and used for authentication and anti-fraud purposes
RANDC	An 8 bit number used to confirm the last RAND received by the mobile station
AUTHR	Output response of the authentication algorithm.
AUTHU	Output of the authentication algorithm when responding to a Unique Challenge order (see §2.3.12.1.5).
RANDBS	Random number used in the SSD update procedure (see §2.3.12.1.8)
MSPC	Mobile Station Protocol Capability field 0000 - reserved for backward compatibility. 0001 - indicates mobile station is IS-91A or ANSI TIA/EIA 691. 0010 - indicates mobile station is IS-136B. 0011 - indicates mobile station is IS-95B or ANSI TIA/EIA 95. Other values are Reserved.

MSCAP Mobile Station Core Analog Protocol field

000 reserved for backward compatibility.

001 indicates mobile station core analog support for ANSI TIA/EIA 553A.

Other values are reserved.

Examples of encoding called-address information into the called-address words are given below:

I. If the number 2# is entered, the word is:

NOTE	0010	1100	0000	0000	0000	0000	0000	0000	P
4	4	4	4	4	4	4	4	4	12

II. If the number 13792640 is entered, the word is:

NOTE	0001	0011	0111	1001	0010	0110	0100	1010	P
4	4	4	4	4	4	4	4	4	12

III. If the number *24273258 is entered, the words are:

Word D - First Word of the Called-Address

NOTE	1011	0010	0100	0010	0111	0011	0010	0101	P
4	4	4	4	4	4	4	4	4	12

Word E - Second Word of the Called-Address

NOTE	1000	0000	0000	0000	0000	0000	0000	0000	P
4	4	4	4	4	4	4	4	4	12

NOTE: These four bits depend on the type of message.

Table 2.7.1-2 Digit code

Digit	Code	Digit	Code
1	0001	7	0111
2	0010	8	1000
3	0011	9	1001
4	0100	0	1010
5	0101	*	1011
6	0110	#	1100
		Null	0000

NOTES:

1) The digit 0 is encoded as binary "ten"; not binary "zero."

2) The code 0000 is the null code, indicating no digit present.

3) All other four bit sequences are reserved, and shall not be transmitted.

2.7.2 Reverse voice channel

The reverse voice channel (RVC) is a wideband data stream sent from the mobile station to the base station. This data stream shall be generated at a 10 kbit/s±1 bit/s rate. Figure 2.7.2-1 depicts the format of the RVC data stream.

A 37 bit dotting sequence (1010....101) and an 11 bit word sync sequence (11100010010) are sent to permit base stations to achieve synchronization with the incoming data, except at the first repeat of word 1 of the message where a 101 bit dotting sequence is used. Each word contains 48 bits, including parity, and is repeated five times together with the 37 bit dotting and 11 bit word sync sequences; it is then referred to as a word block. For a multi-word message, the second word block is formed the same as the first word block including the 37 bit dotting and 11 bit word sync sequences. A word is formed by encoding the 36 content bits into a (48, 36) BCH code that has a distance of 5, (48, 36; 5). The left-most bit (i.e., earliest in time) shall be designated the most significant bit. The 36 most significant bits of the 48 bit field shall be the content bits. The generator polynomial for the code is the same as for the (40, 28; 5) code used on the forward control channel (see §3.7.1).

Figure 2.7.2-1 Reverse voice channel message stream

DOTTING	W.S.	REPEAT 1 OF WORD 1	DOT.	W.S.	REPEAT 2 OF WORD 1
101	11	48	37	11	48

DOT.	W.S.	REPEAT 3 OF WORD 1	DOT.	W.S.	REPEAT 4 OF WORD 1	DOT.	W.S.	REPEAT 5 OF WORD 1
37	11	48	37	11	48	37	11	48

DOT.	W.S.	REPEAT 1 OF WORD 2	...	REPEAT 5 OF WORD 2
37	11	48		48

DOTTING = 1010....101

W.S. (WORD SYNC) = 11100010010

2.7.2.1 RVC messages

Each RVC message can consist of one to four words. The types of messages to be transmitted over the reverse voice channel are:

- Order Confirmation Message
- Unique Challenge Order Confirmation
- Base Station Challenge Order Message
- Called-Address Message
- Serial Number Response Message
- Protocol Capability Indicator Report Message

The message formats are as follows:

Order Confirmation Message

F = 1	NAWC = 00	T = 1	LOCAL/ MSG_TYPE	ORDQ	ORDER	RSVD = 000...0	P
1	2	1	5	3	5	19	12

Unique Challenge Order Confirmation Message

F=1	NAWC =00	T=1	LOCAL/ MSG_TYPE =0...0	ORDQ	ORDER	AUTHU	RSVD =0	P
1	2	1	5	3	5	18	1	12

Base Station Challenge Order Message:

Word 1 of Base Station Challenge Order Message

F=1	NAWC =01	T=1	LOCAL/ MSG_TYPE =0...0	ORDQ	ORDER	RSVD =0...0	P
1	2	1	5	3	5	19	12

Word 2 of Base Station Challenge Order Message

F=0	NAWC=00	T=1	RANDBS	P
1	2	1	32	12

Called-Address Message:

Word 1 - First Word of the Called-Address

F = 1	NAWC	T = 0	1st DIGIT	2nd DIGIT	...	...	...	...	7th DIGIT	8th DIGIT	P
1	2	1	4	4	4	4	4	4	4	4	12

Word 2 - Second Word of the Called-Address

F = 0	NAWC	T = 0	9th DIGIT	10th DIGIT	...	...	...	...	15th DIGIT	16th DIGIT	P
1	2	1	4	4	4	4	4	4	4	4	12

Word 3 - Third Word of the Called-Address

F = 0	NAWC	T = 0	17th DIGIT	18th DIGIT	...	...	...	...	23rd DIGIT	24th DIGIT	P
1	2	1	4	4	4	4	4	4	4	4	12

Word 4 - Fourth Word of the Called-Address

F = 0	NAWC = 00	T = 0	25th DIGIT	26th DIGIT	...	...	...	...	31st DIGIT	32nd DIGIT	P
1	2	1	4	4	4	4	4	4	4	4	12

Serial Number Response Message:

Word 1 - First Word of the Serial Number Response Message

F = 1	NAWC = 01	T = 1	LOCAL / MSG_TYPE= =00000	ORDQ	ORDER	RSVD = 0...0	P
1	2	1	5	3	5	19	12

Word 2 - Second Word of the Serial Number Response Message

F = 0	NAWC = 00	T = 1	ESN	P
1	2	1	32	12

Protocol Capability Indicator Report Message

F = 1	NAWC = 00	T = 1	LOCAL/ MSG_TYPE	ORDQ	ORDER	MSPC	MSCAP	RSVD	P
1	2	1	5	3	5	4	3	12	12

1 The interpretation of the data fields is as follows:

F	First word indication field. Set to '1' in first word and '0' in second word.
NAWC	Number of additional words coming field.
T	T field. Set to '1' to identify the message as an order or order confirmation. Set to '0' to identify the message as a called-address.
DIGIT	Digit field (see Table 2.7.1-2).
ORDER	Order field. Identifies the order type (see Table 3.7.1-1).
ORDQ	Order qualifier field. Qualifies the order confirmation to a specification (See Table 3.7.1-1).
LOCAL	Local Control field. This field is specific to each system. The ORDER field shall be set to local control (see Table 3.7.1-1) for this field to be interpreted.
MSG_TYPE	Message type field. Qualifies the order to a specific action (see Table 3.7.1-1).
RSVD	Reserved for future use; all bits shall be set as indicated.
P	Parity field.
AUTHU	Output of the authentication algorithm when responding to a Unique Challenge order (see §2.3.12.1.5)
RANDBS	Random number used in the SSD update procedure (see §2.3.12.1.8)
MSPC	Mobile Station Protocol Capability field 0000 - reserved for backward compatibility. 0001 - indicates mobile station is IS-91A or ANSI TIA/EIA 691. 0010 - indicates mobile station is IS-136B. 0011 - indicates mobile station is IS-95B or ANSI TIA/EIA 95. Other values are Reserved.
MSCAP	Mobile Station Core Analog Protocol field 000 reserved for backward compatibility. 001 indicates mobile station core analog support for ANSI TIA/EIA 553A. Other values are reserved.

2

3 Base Station

3.1 Transmitter

3.1.1 Frequency parameters

3.1.1.1 Channel spacing and designation

Channel spacing shall be 30 kHz and the base station transmit channel at 870.030 MHz (and the corresponding mobile station transmit channel at 825.030 MHz) shall be termed channel number 1. The 20 MHz range of channels 1 through 666 as shown in Table 2.1.1-1 for System A and System B and the additional 5 MHz of channels 667 through 799 and (wrap-around) 991 through 1023 for extending Systems A and B are basic. The station class mark (SCM, see §2.3.3) of a mobile station shall be taken into account in the consideration of assignment of a channel in this extended band.

3.1.1.2 Frequency tolerance

The base station carrier frequency shall be maintained within ±1.5 parts per million (ppm) of any assigned channel frequency.

3.1.2 Power output characteristics

Maximum effective radiated power (ERP) and antenna height above average terrain (HAAT) shall be coordinated locally on an ongoing basis.

3.1.3 Modulation characteristics

3.1.3.1 Voice signals

The (FM) modulator is preceded by the following four voice processing stages (in the order listed):

- Compressor
- Pre-Emphasis
- Deviation Limiter
- Post Deviation-Limiter Filter.

3.1.3.1.1 Compressor

This stage shall include the compressor portion of a 2:1 syllabic compandor. For every 2 dB change in input level to a 2:1 compressor within its operating range, the change in output level is a nominal 1 dB. The compressor shall have a nominal attack time of 3 ms and a

nominal recovery time of 13.5 ms as defined by the ITU-T (Reference: Recommendation G.162, 1989). The nominal reference input level to the compressor is that corresponding to a 1000 Hz acoustic tone at the expected nominal speech volume level. This level shall produce a nominal ±2.9 kHz peak frequency deviation of the transmitted carrier.

3.1.3.1.2 Pre-emphasis

The pre-emphasis characteristic shall have a nominal +6 dB/octave response between 300 and 3000 Hz.

3.1.3.1.3 Deviation limiter

For audio (voice) inputs applied to the transmitter voice-signal processing stages, a base station shall limit the instantaneous frequency deviation to ±12 kHz. This requirement excludes supervision signals (see §3.4) and wideband data signals (see §3.1.3.2).

3.1.3.1.4 Post deviation-limiter filter

The deviation limiter shall be followed by a low-pass filter whose attenuation characteristics shall exceed:

Frequency band	Attenuation relative to 1000 Hz
3000-15000 Hz	≥ 40 log (f/3000) dB
above 15000 Hz	≥ 28 dB

3.1.3.2 Wideband data signals

3.1.3.2.1 Encoding

The forward control channel (FOCC) and forward voice channel (FVC) wideband data streams (see §3.7) shall be further encoded such that each nonreturn-to-zero binary one is transformed to a zero-to-one transition, and each nonreturn-to-zero binary zero is transformed to a one-to- zero transition.

3.1.3.2.2 Modulation and polarity

The filtered wideband data stream shall then be used to modulate the transmitter carrier using direct binary frequency shift keying. A one (i.e., high state) into the modulator shall correspond to a nominal peak frequency deviation 8 kHz above the carrier frequency, and a zero into the modulator shall correspond to a nominal peak frequency deviation 8 kHz below the carrier frequency.

3.1.4 Limitations on emissions

3.1.4.1 Bandwidth occupied

Modulation products outside the region ±20 kHz from the carrier shall not exceed a level of 26 dB below the unmodulated carrier. Modulation products outside the region of ±45 kHz from the carrier shall not exceed a level of 45 dB below the unmodulated carrier. Modulation products outside the region of ±90 kHz from the carrier shall not exceed a level of:

(a) 60 dB below the unmodulated carrier, or

(b) 43 + 10 $\log_{10}$ (mean output power in Watts) dB below the unmodulated carrier.

Measurement techniques are defined in the current edition of ANSI TIA/EIA 712, *Recommended Minimum Standard for 800 MHz Cellular Base Stations*.

3.1.4.2 Conducted spurious emissions

Current FCC rules shall apply.

3.1.4.3 Radiated spurious emissions

Current FCC rules shall apply.

3.1.4.4 Intermodulation

Radiated products from co-located transmitters shall not exceed FCC spurious and harmonic level requirements that would apply to any of the transmitters operated singly.

3.2 Receiver

3.2.1 Frequency parameters

3.2.1.1 Channel spacing and designation

See §3.1.1

3.2.2 Demodulation characteristics

3.2.2.1 Voice signals

The demodulator is followed by the following two voice-signal processing stages:

- De-emphasis
- Expandor.

3.2.2.1.1 De-emphasis

The de-emphasis characteristic shall have a nominal -6 dB per octave response between 300 and 3000 Hz.

3.2.2.1.2 Expandor

This stage shall include the expandor portion of a 2:1 syllabic compandor. For every 1 dB change in input level to a 1:2 expandor, the change in output level is a nominal 2 dB. The signal expansion shall follow all other demodulation signal processing (including the 6 dB/octave de-emphasis and filtering). The expandor shall have a nominal attack time of 3 ms and a nominal recovery time of 13.5 ms as defined by the ITU-T (Reference: Recommendation G.162, 1989).

The nominal reference input level to the expandor is that corresponding to a 1000 Hz tone from a carrier with a ±2.9 kHz peak frequency deviation.

3.2.3 Limitations on emissions

Current FCC rules shall apply.

3.2.4 Other receiver parameters

System performance is predicated upon receivers meeting ANSI TIA/EIA 712, *Recommended Minimum Standard for 800 MHz Cellular Base Stations.*

3.3 Security and identification

3.3.1 Authentication

The term "authentication" refers to the process during which information is exchanged between a mobile station and the base station for the purposes of enabling the base station to confirm the identity of the mobile station. In short, a successful outcome of the authentication process occurs only when it can be demonstrated that the mobile station and base station possess identical sets of Shared Secret Data (SSD). Details of the procedures are given in §2.3.12.

3.3.2 Identification

Cellular systems are defined by a 15 bit system identification (SID).

3.4 Supervision

3.4.1 Supervisory audio tone

3.4.1.1 SAT detection

Reserved.

3.4.1.2 SAT transmission

Except during signaling data transmission, whenever a base station transmitter is active on a voice channel, one of the following tones shall be modulated on the carrier with a frequency deviation of ±2 kHz±10%:

- 5970 Hz.
- 6000 Hz.
- 6030 Hz.

The frequency tolerance of the tone shall be ±1 Hz.

3.4.1.3 Fade timing status

Reserved.

3.4.2 Signaling tone detection

Reserved.

3.5 Malfunction detection

Reserved.

3.6 Call processing

The following sections describe the base station operation to control the mobile station. Frequent references are made to the corresponding sections in the mobile section and to the messages that flow between the base station and the mobile station. It is helpful to read §2.6 and §3.6 in parallel and examine the message formats in §2.7 and §3.7 at the same time.

3.6.1 Overhead functions for mobile station initiation

To control mobile stations executing the Initialization Task (see §2.6.1), the following information shall be sent in the overhead message train (see §3.7.1.2 for the formats of the messages):

- First part of the system identification (SID1).
- Number of paging channels (N).

3.6.2 Mobile station control on the control channel

3.6.2.1 Overhead information

To control mobile stations monitoring a control channel, the following overhead information shall be sent in the system parameter overhead message (see §3.7.1.2 for the message formats):

- First part of the system identification (SID1).
- Authentication (AUTH). To permit the mobile station to use the authentication procedures described in §2.3.12 and §3.3.1, set this bit to 1.
- Serial number (S): To require that all mobile stations send their serial numbers during a system access, the S field shall be set to '1'; otherwise it shall be set to '0'.
- Registration (REGH, REGR): To enable registration for home mobile stations, the REGH field shall be set to '1'; otherwise it shall be set to '0'. To enable registration for roaming mobile stations, the REGR field shall be set to '1'; otherwise it shall be set to '0'.
- Extended Address (E): To require that all mobile stations send both MIN1 and MIN2 during a system access, the E field shall be set to '1'; otherwise it shall be set to '0'.
- Discontinuous transmission (DTX): To permit mobile stations to use the discontinuous transmission mode on the voice channel, the DTX field shall be set to '10' or '11'; otherwise it shall be set to '00'. A setting of '10' indicates that the DTX-low level shall equal or exceed a level 8 dB below the DTX-high level. A setting of '11' indicates that no minimum applies to the DTX-low level. (See §2.3.11.)
- Number of paging channels (N).
- Read control-filler message (RCF): To require that all mobile stations read a control-filler message before accessing a system on a reverse control channel, the RCF field shall be set to '1'; otherwise it shall be set to '0'.
- Combined paging/access (CPA): If the access functions are combined with the paging functions on the same set of control channels, the CPA field shall be set to '1'. If the access functions are not on the same set of channels as the paging functions, the CPA field shall be set to '0'.
- Number of access channels (CMAX).

The following overhead information is sent as required in messages appended to a system parameter overhead message (see §3.7.1.2 for messages formats):

- Local control: A system may customize operation for home mobile stations and for those roaming mobile stations whose home systems are members of a group by sending local control global action messages.

- New Access channels: If the access channel set is not the default set (see §2.6.2.1), the new access channel global action message shall be sent with the NEWACC field set to the first access channel.
- Registration increment: Each time a mobile station registers, it increments its next registration ID by a fixed value ($REGINCR_S$; see §2.6.3.11). To change this value, the registration increment global action message shall be sent with the REGINCR field appropriately set.
- Registration ID: The registration ID message shall be sent in order to require that all mobile stations with a given or lower next registration ID ($NXTREG_{s-p}$) register.
- Location Area message: The Location Area message identifies the location area associated with the control channel on which it is sent.
- Rescan: To require that all mobile stations enter the Initialization Task and scan the dedicated control channels, the rescan global action message shall be sent.
- RAND1_A. Used by a mobile station to construct the 16 most significant bits of the 32 bit RAND value.
- RAND1_B. Used by a mobile station to construct the 16 least significant bits of the 32 bit RAND value.

3.6.2.2 Page

To page a mobile station, a mobile station control message shall be sent (see §3.7.1.1). Home mobile stations may be paged with a one-word or a two-word message. Roaming mobile stations shall be paged with a two-word message.

3.6.2.3 Order

Orders and order confirmations shall be sent to mobile stations with a two-word mobile station control message (See §3.7.1.2). The following orders may be transmitted:

- Abbreviated Alert
- Audit
- Base Station Challenge order confirmation
- Local control
- Message Waiting
- Protocol Capability Indicator
- SSD Update order
- Unique Challenge order

3.6.2.4 Local control

A cellular system may customize operation for home mobile stations, and for those roaming mobile stations whose home systems are members of a group, by sending local orders with the order field set to local control (which informs the mobile station to examine the local control field), and by sending one or both of two local control global action overhead messages (see §§3.7.1.1, 3.7.1.2.2, and 3.7.2).

A group of systems could be formed by participating systems agreeing to a common set of local control protocols and whose system identifications (SID) are recognized by mobile stations as a common group.

3.6.3 Base station support of system access by mobile stations

3.6.3.1 Overhead information

The following information shall be sent on a forward control channel to support system access by mobile stations (see §3.7.1.2 for message formats):

- Digital color code (DCC): The DCC, SDCC1, and SDCC2 are transmitted from the base station to the mobile station. The mobile station then uses the DCC, SDCC1, and SDCC2 to identify to the base station which base station transmitter the mobile station is receiving. If the Supplementary Digital Color Code feature is utilized, the combination of SDCC1 and SDCC2 transmitted by the base station shall be a non-zero number. Mobile stations which respond with a non-zero SDCC combination are capable of supporting SDCC. Mobile stations which respond with a zero SDCC combination are not capable of supporting SDCC. The zero SDCC combination is used to indicate either that SDCC1 and SDCC2 are not used or are not supported.

- Control mobile attenuation code (CMAC): The CMAC shall be transmitted from the base station to the mobile station in the control-filler message if the mobile station shall adjust its transmitter power level before accessing a system on a reverse control channel. The translation of the CMAC field to transmitter power level depends on the mobile station's power class as indicated by its station class mark (SCM_p see §2.1.2.2 and §2.3.3). When not required, the CMAC field shall be set to '000'. To require that mobile stations read a control-filler message prior to system access, the RCF field shall be set to '1' in the system parameter overhead message.

- Wait-for-overhead-message (WFOM): If the mobile station shall wait for an overhead message train before accessing a system on a reverse control channel, then the WFOM field shall be set to '1' in the control-filler message; otherwise it shall be set to '0'.

- Overload control (OLC): If the mobile stations assigned to one or more of the 16 overload classes shall not access the system for originations on the reverse control channel, the overload control global action message shall be appended to a system parameter overhead message. When this message is appended, the overload class fields corresponding to the restricted overload classes shall be set to '0', and the remaining overload class fields shall be set to '1'.

- Access type parameters: If a mobile station shall not check for an idle-to-busy status transition on the reverse control channel when accessing a system, then the access type parameters global action message with the BIS field set to '0' shall be appended to a system parameter overhead message; otherwise the BIS field shall be set to '1'

whenever the message is appended. The system shall set the BSPC to indicate its air interface protocol and the BSCAP to indicate its core analog air interface. Also, the system shall set the PCI ROAM field and the PCI HOME field, to indicate whether mobile stations shall report their protocol capability.

- Access attempt parameters: If the default values for the number of seizure attempts or the limit on the number of busy occurrences for mobile stations accessing the reverse control channel shall not be used, then the access attempt parameters global action message shall be appended to a system parameter overhead message.

3.6.3.2 Reverse control channel seizure by mobile stations

If mobile stations are required to check for an idle-to-busy transition of the busy-idle bits in the corresponding FOCC when accessing a system (that is, the BIS field is set to '1'), then whenever the base station receives a seizure precursor (see §2.7.1) that matches its encoded form of the DCC with 1 or no bit errors, it shall begin transmitting busy-idle bits as busy on the FOCC between 0.8 ms and 2.9 ms, inclusive, after the reception of the last bit of the mobile station's precursor (i.e., bit times 56 through 77 of the mobile station's message). The busy-idle bits shall remain busy until the 30 ms after the last bit of the last word of the mobile station's message has been received, if this can be determined; otherwise, until the time equal to (24N + 55) ms after transmitting the first busy-idle bit as busy, where N is the maximum number of words the base station has been designed to receive.

3.6.3.3 Response to mobile station messages

Whenever the mobile station sends a message to the base station, it is not required that the base station respond to the message. During periods of overload or high usage, it may be desirable to permit mobile stations to "time-out" rather than sending release or other orders that use system capacity.

The following responses to mobile station messages may be sent:

- Origination message. Send one of the following orders:
  - Initial voice channel designation
  - Directed retry
  - Intercept
  - Reorder.
- Page response message. Send one of the following orders:
  - Initial voice channel designation
  - Directed retry
  - Release.
- Order message. Send one of the following orders:
  - Order confirmation
  - Release.

- Order confirmation message. No message is sent.
- Protocol Capability Indicator Order Confirmation. Send one of the following orders:
  - Release
  - Message Waiting Order.

3.6.4 Mobile station control on voice channel

Whenever the mobile station is transmitting on a voice channel, changes in the status of the supervisory audio tone (SAT) and signaling tone (ST) are used to signal the occurrence of certain events during the progress of a call. These events include confirming orders, sending a release request, sending a flash request, and loss of radio-link continuity. The mobile station will signal these events by changing in a prescribed manner (see §2.6.4) the status of the SAT and ST, abbreviated in the following sections (SAT, ST) where SAT and ST have the value '0' when not present and '1' when present. These status changes shall be detected by the base station and interpreted within the context of the task the base station is in as a message that identifies the event signaled by the mobile station. Requirements concerning these base station actions are described below. In the following sections, the (0,1) status shall always be treated as the (0,0) status.

In addition to the analog signaling to and from the mobile station, digital messages can be sent to the mobile station and received from the mobile station. The response to a digital message sent to the mobile station will be either be a digital message or a change of SAT,ST status.

3.6.4.1 Loss of radio link continuity

Reserved.

3.6.4.2 Initial voice channel confirmation

Confirmation that a mobile station has successfully tuned to its initial designated voice channel will be received by the base station as a change in the SAT, ST status from (0,0) to (1,0).

If the confirmation is not received, the base station shall either resend the message or turn off the voice channel transmitter.

Following confirmation, if the mobile station was paged, the base station shall enter the Waiting for Order Task (see §3.6.4.3.1); otherwise, the base station shall enter the Conversation Task (see §3.6.4.4).

3.6.4.3 Alerting

3.6.4.3.1 Waiting for order

When the mobile station confirms the initial voice channel designation after having been paged, it enters this task. The following orders can be sent to the mobile station, with the resultant confirmation and action to be taken as follows:

- Handoff: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1) with the (1,1) status held for 50 ms. The base station shall remain in the Waiting for Order Task.
- Alert or Alert With Info: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1). The base station shall then enter the Waiting for Answer Task (see §3.6.4.3.2).

  Note: The Alert With Info order was not defined for ANSI EIA/TIA 553 (1989) mobile stations, therefore, a 553 (1989) mobile station will not turn on signaling tone to confirm an Alert With Info order. If the system does not receive a confirmation for an Alert With Info order, in addition, the system shall send an Alert order to provide backwards compatibility for ANSI EIA/TIA 553 (1989) mobile stations.
- Release: The mobile station confirms the order by a change of the SAT, ST status from (1,0) to (1,1) with the (1,1) status held for 1.8 seconds. The base station shall then turn off the transmitter.
- Audit: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Order Task.
- Message Waiting: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Order Task.
- Maintenance: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1). The base station shall then enter the Waiting for Answer Task (see §3.6.4.3.2).
- Change power: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Order Task.
- Serial Number Request. The mobile station confirms the order by a Serial Number Response message. The base station shall remain in the Waiting For Order Task.
- SSD Update Order. The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, mobile stations conforming to this specification will begin transmitting a Base Station Challenge Order (mobile stations conforming to other standards may take up to 5 seconds). Process the order as described below and remain in the Waiting for Order Task.
- Unique Challenge Order. The mobile executes the Unique Challenge Response Procedure (see §2.3.12.1.5) and within 750 ms, mobile stations conforming to this specification will begin transmitting a confirmation containing the output of the Authentication Process(mobile stations conforming to other standards may take up to 5 seconds).. The base station shall remain in the Waiting for Order Task.
- Message Encryption Mode Order. The mobile station enables or disables message encryption mode as indicated in the order (see §2.3.12.2.1) and confirms the order

with a digital message (see §2.7.2). The base station shall remain in the Waiting for Order Task.

- Parameter Update Order. The mobile station executes the parameter updating procedure (see §2.3.12.1.3 and §2.3.12.1.7) and confirms the order by sending a Parameter Update Confirmation. The base station shall remain in the Waiting for Order Task.

- Protocol Capability Indicator Order. The mobile station confirms the order by a Protocol Capability Indicator report message (see §2.7.2). The base station shall remain in the Waiting for Order Task.

- Local control: The confirmation and action depend on the message.

In addition, the following message can be received autonomously from the mobile station:

- Base Station Challenge Order: When the base station receives a Base Station Challenge Order it shall process the RANDBS contained in the order as described in §2.3.12.1.8, and within 10 seconds (mobile stations conforming to other air interface standards may require faster response time), send the result (AUTHBS) back to the mobile station in the associated order confirmation. The base station shall remain in the Waiting for Order Task.

3.6.4.3.2 Waiting for answer

When this task is entered, an alert timer may be set. The following orders can be sent with the confirmation and action to be taken as follows:

- Handoff: The mobile station confirms the order by changing the SAT, ST status from (1,1) to (1,0) for 500 ms followed by a change in the status from (1,0) to (1,1), with the (1,1) status held for 50 ms on the old channel. Then a (1,1) status is sent on the new channel. The base station shall remain in the Waiting for Answer Task.

- Alert or Alert With Info: No confirmation is received. The base station may reset the alert timer and remain in the Waiting for Answer Task.

  Note: The Alert With Info order was not defined for ANSI EIA/TIA 553 (1989) mobile stations, therefore, a 553 (1989) mobile station will not turn on signaling tone to confirm an Alert With Info order. If the system does not receive a confirmation for an Alert With Info order, in addition, the system shall send an Alert order to provide backwards compatibility for ANSI EIA/TIA 553 (1989) mobile stations.

- Stop alert: The mobile station confirms the order by a change in the SAT, ST status from (1,1) to (1,0). The base station shall then enter the Waiting for Order Task.

- Release: The mobile station confirms the order by a change in the SAT, ST status from (1,1) to (1,0) for 500 ms followed by a change in the status from (1,0) to (1,1), with the (1,1) status held for 1.8 seconds. The base station shall then turn off the transmitter.

- Audit: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Answer Task.

- Flash With Info. The mobile station confirms the order by a digital message (see 2.7.2). The base station shall remain in the Waiting For Answer Task.

- Message Waiting: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Answer Task.

- Maintenance: No confirmation is received. The base station may reset the alert timer and remain in the Waiting for Answer Task.
- Change power: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Waiting for Answer Task.
- Serial Number Request. The mobile station confirms the order by a Serial Number Response Message. The base station shall remain in the Waiting For Answer Task.
- SSD Update Order. The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, mobile stations conforming to this specification will begin transmitting a Base Station Challenge Order(mobile stations conforming to other standards may take up to 5 seconds). Process the order as described below and remain in the Waiting for Answer Task.
- Unique Challenge Order. The mobile executes the Unique Challenge Response Procedure (see §2.3.12.1.5) and within 750 ms, mobile stations conforming to this specification shall begin transmitting a confirmation containing the output of the Authentication Process (mobile stations conforming to other standards may take up to 5 seconds). The base station shall remain in the Waiting for Answer Task.
- Parameter Update Order. The mobile station executes the parameter updating procedure (see §2.3.12.1.3 and §2.3.12.1.7) and confirms the order by sending a Parameter Update Confirmation. The base station shall remain in the Waiting for Answer Task.
- Message Encryption Mode Order. The mobile station enables or disables message encryption mode as indicated in the order (see §2.3.12.2.1) and confirms the order with a digital message (see §2.7.2). The base shall remain in the Waiting for Answer Task.
- Protocol Capability Indicator Order. The mobile station confirms the order by a Protocol Capability Indicator report message (see §2.7.2). The base station shall remain in the Waiting for Answer Task.
- Local control: The confirmation and action depend on the message.

In addition, the following message can be received autonomously from the mobile station:

- Base Station Challenge Order: When the base station receives a Base Station Challenge Order it shall process the RANDBS contained in the order as described in §2.3.12.1.8, and within 10 seconds (mobile stations conforming to other air interface standards may require faster response time), send the result (AUTHBS) back to the mobile station in the associated order confirmation. The base station shall remain in the Waiting for Answer Task.

The mobile station signals an answer by a change in the SAT, ST status from (1,1) to (1,0). The base station shall then enter the Conversation Task (see §3.6.4.4).

3.6.4.4 Conversation

While the base station is in the Conversation Task, the following orders can be sent to the mobile station, with confirmation and action to be taken as follows:

- Handoff: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1), with the (1,1) status held for 50 ms. The base station shall remain in the Conversation Task.

- Send called address: The mobile station confirms the order by a digital message with the called-address information (see §2.7.2). The action to be taken will depend on the called-address information.

- Alert or Alert With Info: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1). The base station shall then enter the Waiting for Answer Task (see §3.6.4.3.2).

  Note: The Alert With Info order was not defined for ANSI EIA/TIA 553 (1989) mobile stations, therefore, a 553 (1989) mobile station will not turn on signaling tone to confirm an Alert With Info order. If the system does not receive a confirmation for an Alert With Info order, in addition, the system shall send an Alert order to provide backwards compatibility for ANSI EIA/TIA 553 (1989) mobile stations.

- Release: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1), with the (1,1) status held for 1.8 seconds. The base station shall turn off the transmitter.

- Audit: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Conversation Task.

- Flash With Info. The mobile station confirms the order with a digital message (see 2.7.2). The base station shall remain in the Conversation Task.

- Message Waiting: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Conversation Task.

- Maintenance: The mobile station confirms the order by a change in the SAT, ST status from (1,0) to (1,1). The base station shall then enter the Waiting for Answer Task (see §3.6.4.3.2).

- Change power: The mobile station confirms the order by a digital message (see §2.7.2). The base station shall remain in the Conversation Task.

- Serial Number Request. The mobile station confirms the order by a Serial Number Response Message. The base station shall remain in the Conversation Task.

- SSD Update Order. The mobile station computes SSD_A_NEW and SSD_B_NEW and selects a RANDBS as described in §2.3.12.1.8. Within 750 ms, mobile stations conforming to this specification will begin transmitting a Base Station Challenge Order (mobile stations conforming to other standards may take up to 5 seconds). Process the order as described below and remain in the Conversation Task.

- Unique Challenge Order. The mobile executes the Unique Challenge Response Procedure (see §2.3.12.1.5) and within 750 ms, mobile stations conforming to this specification shall begin transmitting a confirmation containing the output of the Authentication Process (mobile stations conforming to other standards may take up to 5 seconds). The base station shall remain in the Conversation Task.

- Parameter Update Order. The mobile station executes the parameter updating procedure (see §2.3.12.1.3 and §2.3.12.1.7) and confirms the order by sending a Parameter Update Confirmation. The base station shall remain in the Conversation Task.

- Disable DTMF Order: The mobile station confirms the order by a digital message (see §2.7.2). The mobile station disables the DTMF tone generator upon receipt of this order until the Called Address Message is transmitted. The base station shall remain in the Conversation Task.
- Message Encryption Mode Order. The mobile station enables or disables message encryption mode as indicated in the order (see §2.3.12.2.1) and confirms the order with a digital message (see §2.7.2). The base shall remain in the Conversation Task.
- Protocol Capability Indicator Order. The mobile station confirms the order by a Protocol Capability Indicator report message (see §2.7.2). The base station shall remain in the Conversation Task.
- Local control: The confirmation and action depend on the message.

In addition, the following messages can be received autonomously from the mobile station:

- Flash request: The mobile station signals a flash by a change in the SAT, ST status from (1,0) to (1,1) with the (1,1) status held for 400 ms followed by a transition to the (1,0) status.
- Release: The mobile station signals a release by a change in the SAT, ST status from (1,0) to (1,1) with the (1,1) status held for 1.8 seconds. The base station shall turn off the transmitter.
- Base Station Challenge Order: When the base station receives a Base Station Challenge Order it shall process the RANDBS contained in the order as described in §2.3.12.1.8, and within 10 seconds (mobile stations conforming to other air interface standards may require faster response time), send the result (AUTHBS) back to the mobile station in the associated order confirmation. The base station shall remain in the Conversation Task.

3.6.5 Delivery of Character Information

Character information is delivered to a mobile station via the Mobile Station Control Message over the forward voice channel. The Alert With Info and Flash With Info orders are designated in the Mobile Station Control Message.

Whenever two sets of character information need to be delivered to a mobile station, the base station shall transmit the second set of character information using the Flash With Info order.

3.7 Signaling formats

In the message formats used between the mobile stations and base stations, some bits are marked as reserved (RSVD). Some or all of these reserved bits may be used in the future for additional messages. Therefore, all mobile stations and base stations shall set all bits that they are programmed to treat as reserved bits to '0' (zero) in all messages that they transmit. All mobile stations and base stations shall ignore the state of all bits that they are programmed to treat as reserved bits in all messages that they receive.

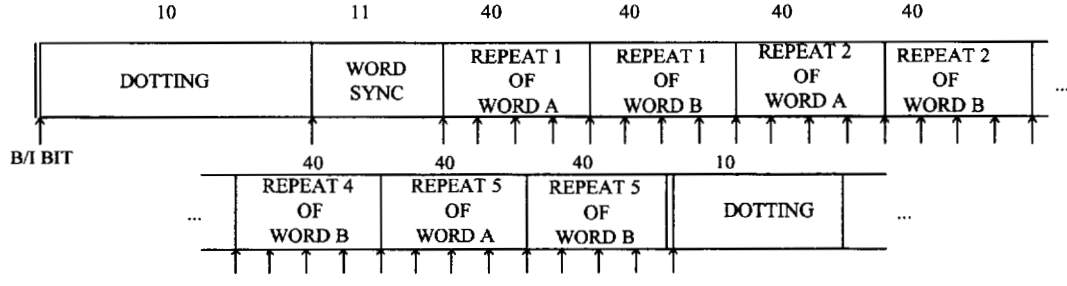
In the specific case of overhead messages on the Forward Control Channel, if the mobile station receives a BCH-code-correct but unrecognizable overhead message (including Global Action Message types), the mobile station shall count that message as part of the train for NAWC-counting purposes, but shall not attempt to execute the message. All other messages and fields of an overhead message train that carries a message type herein indicated as 'Reserved' shall be decoded and used as appropriate.

Implementors of mobile stations are cautioned that many other functions and features are deployed on the FOCC than those described in this standard. These functions frequently employ bits indicated herein as 'Reserved.' Reference may be made to the current version of TSB-70 for details.

3.7.1 Forward control channel

The forward control channel (FOCC) is a continuous wideband data stream sent from the base station to the mobile station. This data stream shall be generated at a 10 kbit/s±0.1 bit/s rate. Figure 3.7.1-1 depicts the format of the FOCC data stream.

Figure 3.7.1-1 Forward Control Channel Message Stream



DOTTING = 1010...101
W.S. (WORD SYNC) = 11100010010 ···

NOTES:

1. A given mobile reads only one of the two interleaved messages (A or B).
2. Busy-Idle bits are inserted at each arrow.

Each forward control channel consists of three discrete information streams, called stream A, stream B, and busy-idle stream, that are time-multiplexed together. Messages to mobile stations with the least significant bit of their mobile identification number (see §2.3.1) equal to '0' are sent on stream A, and those with the least significant bit of their mobile identification number equal to '1' are sent on stream B.

The busy-idle stream contains busy-idle bits, which are used to indicate the current status of the reverse control channel. The reverse control channel is busy if the busy-idle bit is equal to '0' and idle if the busy-idle bit is equal to '1'. A busy-idle bit is located at the beginning of each dotting sequence, at the beginning of each word sync sequence, at the beginning of the first repeat of word A, and after every 10 message bits thereafter.

A 10 bit dotting sequence (1010101010) and an 11 bit word sync sequence (11100010010) are sent to permit mobile stations to achieve synchronization with the incoming data. Each word contains 40 bits, including parity, and is repeated five times; it is then referred to as a word block. For a multi-word message, the second word block and subsequent word blocks are formed the same as the first word block including the 10 bit dotting and 11 bit word sync sequences. A word is formed by encoding 28 content bits into a (40, 28) BCH code that has a distance of 5, (40, 28; 5). The left-most bit (i.e., earliest in time) shall be designated the most significant bit. The 28 most significant bits of the 40 bit field shall be the content bits. The generator polynomial for the (40, 28; 5) BCH code is:

$$G_b(x) = x^{12} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^0.$$

The code, a shortened version of the primitive (63, 51; 5) BCH code, is a systematic linear block code with the leading bit as the most significant information bit and the least significant bit as the last parity-check bit.

Each FOCC message can consist of one or more words. The types of messages to be transmitted over the forward control channel are:

- Mobile station control message
- Overhead message
- Control-Filler message.

Control-filler messages may be inserted between messages and between word blocks of a multi-word message.

The following sections contain descriptions of the message formats that the base station transmits over either stream A or B. For purposes of format presentation and explanation, the busy-idle bits have been deleted in the discussion of the message formats.

3.7.1.1 Mobile station control message

The mobile station control message can consist of one to eight words.

Word 1 - Abbreviated Address Word

T1T2	DCC	$MIN1_{23-0}$	P
2	2	24	12

Word 2 - Extended Address Word

2	2	10	1	5	3	5	12
T1T2 =	SCC = 11	$MIN2_{33-24}$	EF = 0	LOCAL/ MSG_TYPE	ORDQ	ORDER	P
10	SCC≠11		VMAC		CHAN		
2	2	10	3		11		12

Word 3 - First Directed-Retry Word

T1T2=10	SCC=11	CHANPOS	CHANPOS	CHANPOS	RSVD=000	P
2	2	7	7	7	3	12

Word 3 - Base Station Challenge Order Confirmation Word

T1T2=10	SCC=11	RSVD=00	AUTHBS	RSVD=0000	P
2	2	2	18	4	12

Word 3 - Unique Challenge Order Word

T1T2=10	SCC=11	RANDU	P
2	2	24	12

Word 3 - First SSD Update Order Word

T1T2=10	SCC=11	RANDSSD_1	P
2	2	24	12

Word 4- Second SSD Update Order Word

T1T2=10	SCC=11	RANDSSD_2	P
2	2	24	12

Word 4 - Second Directed-Retry Word

T1T2=10	SCC=11	CHANPOS	CHANPOS	CHANPOS	RSVD=000	P
2	2	7	7	7	3	12

Word 5- Third SSD Update Order Word

T1T2=10	SCC=11	RSVD=0...0	RANDSSD_3	RSVD=0000	P
2	2	12	8	4	12

The interpretation of the data fields is as follows:

T1T2	Type field. If only Word 1 is sent, set to '00' in Word 1. If a multiple-word message is sent, set to '01' in Word 1 and set to '10' in each additional word.
DCC	Digital color code field.
MIN1	First part of the mobile identification number field (see §2.3.1).
MIN2	Second part of the mobile identification number field (see §2.3.1).
SCC	SAT color code (see Table 3.7.1-2).
ORDER	Order field. Identifies the order type (see Table 3.7.1-1).
ORDQ	Order qualifier field. Qualifies the order to a specific action (See Table 3.7.1-1).
LOCAL	Local control field. This field is specific to each system. The ORDER field shall be set to local control (see Table 3.7.1-1) for this field to be interpreted.
MSG_TYPE	Message type field. Qualifies the order to a specific action (see Table 3.7.1-1).
EF	Extended Protocol Forward Channel Indicator. (Set to zero. For other values see ANSI TIA/EIA 691).
VMAC	Voice mobile attenuation code field. Indicates the mobile station power level associated with the designated traffic channel (see Table 2.1.2-1).
CHAN	Channel number field. Indicates the designated RF channel (see §2.3.3).
CHANPOS	Channel position field. Indicates the position of a control channel relative to the first access channel (FIRSTCHA).
RSVD	Reserved for future use, all bits shall be set as indicated.
P	Parity field.
RANDU	The 24 bit random number issued by the base in the Unique Challenge Order.
RANDSSD_1	The most significant 24 bits of the random number issued by the base in the SSD Update Order.
RANDSSD_2	The subsequent 24 bits (following RANDSSD_1) of the random number issued by the base in the SSD Update Order.
RANDSSD_3	The least significant 8 bits of the random number issued by the base in the SSD Update Order.
AUTHBS	Output response of the authentication algorithm initiated by the Base Station Challenge Order.

1 **Table 3.7.1-1 Order and order qualification codes**

Order Code	Order Qualification Code	Message Type	Function
00000	000	00000	Page (or Origination) Authentication Word C not included
00001	000	00000	Alert
00001	001	00000	Abbreviated Alert
00011	000	00000	Release
00100	000	00000	Reorder
00101	000	XXXXX	Message Waiting (Type field indicates # of messages)
00110	000	00000	Stop Alert
00111	000	00000	Audit
01000	000	00000	Send Called-address
01001	000	00000	Intercept
01010	000	00000	Maintenance
01011	000	00000	Change Power to Power Level 0 (see §2.1.2.2)
01011	001	00000	Change Power to Power Level 1
01011	010	00000	Change Power to Power Level 2
01011	011	00000	Change Power to Power Level 3
01011	100	00000	Change Power to Power Level 4
01011	101	00000	Change Power to Power Level 5
01011	110	00000	Change Power to Power Level 6
01011	111	00000	Change Power to Power Level 7
01100	000	00000	Directed Retry - not last try
01100	001	00000	Directed Retry - last try
01101	000	00000	Non-autonomous Registration - Do not make whereabouts known, Authentication Word C not included
01101	001	00000	Non-autonomous Registration - Make whereabouts known, Authentication Word C not included
01101	010	00000	Autonomous Registration - Do not make whereabouts known, Authentication Word C not included
01101	011	00000	Autonomous Registration - Make whereabouts known, Authentication Word C not included
01101	011	00001	Autonomous Registration - Power Down, PCI Registration Word C not included, Authentication Word C not included: Authentication Word C not included on the reverse control channel. This order/order qualifier/message type is also used on the reverse voice channel where Authentication Word C does not apply.
10001	000	00000	Alert With Info
10010	000	00000	Flash With Info

Table 3.7.1-1 Order and order qualification codes (cont'd)

Order Code	Order Qualification Code	Message Type	Function
01111	000	00000	Parameter Update Order/Confirmation
01111	001	00000	Serial Number Request/Response
01111	100	00000	Reserved
11000	000	00000	Non-autonomous Registration - Do not make whereabouts known, Authentication Word C included
11000	001	00000	Non-autonomous Registration - Make whereabouts known, Authentication Word C included
11000	010	00000	Autonomous Registration - Do not make whereabouts known, Authentication Word C included
11000	011	00000	Autonomous Registration - Make whereabouts known, Authentication Word C included
11000	011	00001	Autonomous Registration - Power Down, Authentication Word C included
11010	100	00000	Protocol Capability Indicator; Protocol Capability Registration - Authentication Word C not included
11010	100	00001	Protocol Capability Registration - Authentication Word C included
11110	000	XXXXX	Local control
[Base station initiated messages only - Subscriber Authentication]			
10011	000	00000	Base Station Challenge Confirmation
10100	000	00000	Unique Challenge Order
10101	000	00000	SSD Update Order
10110	000	00000	Disable DTMF Order
10111	000	00000	Message Encryption Mode order with disable indication
10111	001	00000	Message Encryption Mode order with enable indication
[Mobile station initiated messages only - Subscriber Authentication]			
10011	000	00000	Base Station Challenge Order
10100	000	00000	Unique Challenge Confirmation
10101	000	00000	SSD Update Confirmation with failure indication
10101	001	00000	SSD Update Confirmation with success indication

All other codes are reserved.

Table 3.7.1-2 SAT Color Code (SCC)

Bit pattern	SAT frequency
00	5970 Hz
01	6000 Hz
10	6030 Hz
11	Not an analog channel designation

3.7.1.2 Overhead message

A three bit OHD field is used to identify the overhead message types. Overhead message type codes are listed in Table 3.7.1-3 and are grouped into the following functional classes:

- System parameter overhead message
- Global action overhead message
- Registration identification message
- Control-filler message.

Overhead messages are sent in a group called an overhead message train. The first message of the train shall be the system parameter overhead message. The desired global action messages or a registration ID message shall be appended to the end of the system parameter overhead message. The total number of words in an overhead message train is one more than the value of the NAWC field contained in the first word of the system parameter overhead message. The last word in the overhead message train is identified by a '1' in the END field of that word; the END field of all other words in the train shall be set to '0'. For NAWC-counting purposes, inserted control-filler messages (see §3.7.1) shall not be counted as part of the overhead message train.

The system parameter overhead message shall be sent every 0.8±0.3 seconds on each of the following control channels:

- All dedicated control channels (see §2.6.1.1.1)
- Combined paging-access forward control channel (i.e., CPA = 1, see §3.7.1.2.1)
- Separate paging forward control channel (i.e., CPA = 0)
- Separate access forward control channel (i.e., CPA = 0) when the control-filler message is sent with the WFOM bit set to '1' (see §3.7.1.2.4).

The global action messages and the registration identification message are sent on an as needed basis.

Table 3.7.1-3 Overhead message types

Code	Order
000	Registration ID
001	Control-filler
010	Reserved
011	Reserved
100	Global action
101	Reserved
110	Word 1 of system parameter message
111	Word 2 of system parameter message

3.7.1.2.1 System parameter overhead message

The system parameter overhead message consists of two words.

Word 1

T1T2 = 11	DCC	SID1	EP	AUTH	PCI	NAWC	OHD = 110	P
2	2	14	1	1	1	4	3	12

Word 2

T1T2=11	DCC	S	E	REGH	REGR	DTX	
2	2	1	1	1	1	2	

	N-1	RCF	CPA	CMAX-1	END	OHD=111	P
	5	1	1	7	1	3	12

The interpretation of the data fields is as follows:

T1T2 — Type field. Set to '11' indicating an overhead word.

OHD — Overhead message type field. The OHD field of word 1 is set to '110' indicating the first word of the system parameter overhead message. The OHD field of word 2 is set to '111' indicating the second word of the system parameter overhead message.

DCC — Digital color code field.

SID1 — First part of the system identification field.

EP	Extended Protocol Bit. Enables the use of(Set to zero in ANSI TIA/EIA 553A systems. For other values see ANSI TIA/EIA 691).
AUTH	Set to 1 if the base station supports the authentication procedures described in sections §2.3.12 and §3.3.1.
PCI	Set to zero for ANSI TIA/EIA 553A systems. For other values, see ANSI TIA/EIA 627 and IS-136.
NAWC	Number of additional words coming field. In word 1 this field is set to one fewer than the total number of words in the overhead message train.
S	Serial number field.
E	Extended address field.
REGH	Registration field for home stations.
REGR	Registration field for roaming stations.
DTX	Discontinuous transmission field.
N-1	N is the number of paging channels in the system.
RCF	Read-control-filler field.
CPA	Combined paging/access field.
CMAX-1	CMAX is the number of access channels in the system.
END	End indication field. Set to '1' to indicate the last word of the overhead message train; set to '0' if not last word.
RSVD	Reserved for future use, all bits shall be set as indicated.
P	Parity field.

3.7.1.2.2 Global action overhead message

Each global action overhead message consists of one word. The global action message types are listed in Table 3.7.1-4. Any number of global action messages can be appended to a system parameter overhead message.

The formats for the global action commands are as follows:

Rescan Global Action Message

T1T2 =11	DCC	ACT= 0001	RSVD= 000...00	END	OHD= 100	P
2	2	4	16	1	3	12

Registration Increment Global Action Message

T1T2 =11	DCC	ACT =0010	REGINCR	RSVD = 0000	END	OHD =100	P
2	2	4	12	4	1	3	12

Location Area Global Action Message

T1T2 =11	DCC	ACT =0011	PUREG	PDREG	LREG	RSVD =0	LOCAID	END	OHD =100	P
2	2	4	1	1	1	1	12	1	3	12

New Access Channel Set Global Action Message

T1T2 =11	DCC	ACT =0110	NEWACC	RSVD = 00000	END	OHD =100	P
2	2	4	11	5	1	3	12

Overload Control Global Action Message

T1T2= 11	DCC	ACT= 1000	0 LC 0	0 LC 1	0 LC 2	0 LC 3	0 LC 4	0 LC 5	0 LC 6	0 LC 7	
2	2	4	1	1	1	1	1	1	1	1	

	0 LC 8	0 LC 9	0 LC 10	0 LC 11	0 LC 12	0 LC 13	0 LC 14	0 LC 15	END	OHD= 100	P
	1	1	1	1	1	1	1	1	1	3	12

Access Type Parameters Global Action Message

T1T2 =11	DCC	ACT= 1001	BIS	PCI HOME	PCI ROAM	BSPC	BSCA P	RSVD	END	OHD =100	P
2	2	4	1	1	1	4	3	6	1	3	12

Access Attempt Parameters Global Action Message

T1T2 =11	DCC	ACT= 1010	MAXBUSY –PGR	MAXSZTR –PGR	MAXBUSY– OTHER	MAXSZTR– OTHER	END	OHD =100	P
2	2	4	4	4	4	4	1	3	12

Random Challenge A Global Action Message

T1T2 =11	DCC	ACT= 0111	RAND1_A	END	OHD= 100	P
2	2	4	16	1	3	12

Random Challenge B Global Action Message

T1T2 =11	DCC	ACT= 1011	RAND1_B	END	OHD= 100	P
2	2	4	16	1	3	12

Local Control 1 Message

T1T2= 11	DCC	ACT= 1110	LOCAL CONTROL	END	OHD= 100	P
2	2	4	16	1	3	12

Local Control 2 Message

T1T2= 11	DCC	ACT= 1111	LOCAL CONTROL	END	OHD= 100	P
2	2	4	16	1	3	12

The interpretation of the data fields is as follows:

T1T2	Type field. Set to '11' indicating overhead word.
ACT	Global action field. See Table 3.7.1-4.
BIS	Busy-idle status field.
DCC	Digital color code field.
OHD	Overhead message type field. Set to '100' indicating the global action message.
REGINCR	Registration increment field.
NEWACC	New access channel starting point field.
MAXBUSY-PGR	Maximum busy occurrences field (page response).

MAXBUSY-OTHER	Maximum busy occurrences field (other accesses).
MAXSZTR-PGR	Maximum seizure tries field (page response).
MAXSZTR-OTHER	Maximum seizure tries field (other accesses).
OLC N	Overload class field (N = 0 to 15). (See NOTE for recommended overload control bit assignments.)
END	End indication field. Set to '1' to indicate the last word of the overhead message train; set to '0' if not last word.
PUREG	Power up registration status field (enabled = 1, disabled = 0).
PDREG	Power down registration status field (enabled = 1, disabled = 0).
LREG	Location Area ID registration status field (enabled = 1, disabled = 0).
LOCAID	Location area identity field.
RSVD	Reserved for future use, all bits shall be set as indicated.
PCI HOME	Home Protocol Capability Indicator. When set to '1' the mobile with the ROAM status disabled shall report its protocol Capability.
PCI ROAM	Roam Protocol Capability Indicator. When set to '1' the mobile with the ROAM status enabled shall report its protocol Capability
BSPC	Base Station Protocol Capability field 0000 - Reserved for backward compatibility. 0001 - IS-91A or ANSI TIA/EIA 691. 0010 - IS-136B. 0011 - IS-95B or ANSI TIA/EIA 95. Other values are Reserved.
BSCAP	Base Station Core Analog Protocol 000 - Reserved for backward compatibility. 001 - ANSI TIA/EIA 553A. Other values are reserved.
LOCAL CONTROL	May be set to any bit pattern.
P	Parity field.
RAND1_A	The 16 most significant bits of the 32 bit RAND variable stored by a mobile for use in the authentication process.
RAND1_B	The 16 least significant bits of the 32 bit RAND variable stored by a mobile for use in the authentication process.

NOTE: The recommended overload control bit assignments are:

0	0	0	0	....	0	0	0	0	....	0
L	L	L	L		L	L	L	L		L
C	C	C	C		C	C	C	C		C
0	1	2	3		9	10	11	12		15

Uniform distribution assigned to normal subscribers = OLC 0 through OLC 9

Test mobiles = OLC 10

Emergency mobiles = OLC 11

Reserved = OLC 12 through OLC 15

For more information, refer to EIA Telecommunications Systems Bulletin No. 16 (March 1985), *Assignment of Access Overload Classes in the Cellular Telecommunications Services.*

Table 3.7.1-4 Global action message types

Action code	Type
0000	Reserved
0001	Rescan paging channels
0010	Registration increment
0011	Location Area
0100	Reserved
0101	Reserved
0110	New access channel set
0111	Random Challenge A
1000	Overload control
1001	Access type parameters
1010	Access attempt parameters
1011	Random Challenge B
1100	Reserved
1101	Reserved
1110	Local control 1
1111	Local control 2

3.7.1.2.3 Registration ID message

The registration ID message consists of one word. When sent, the message shall be appended to a system parameter overhead message in addition to any global action messages.

T1T2=11	DCC	REGID	END	OHD=000	P
2	2	20	1	3	12

The interpretation of the data fields is as follows:

T1T2 — Type field. Set to '11' indicating overhead word.

DCC — Digital color code field.

OHD — Overhead message type field. Set to '000' indicating the registration ID message.

REGID — Registration ID field.

END — End indication field. Set to '1' to indicate last word of the overhead message train; set to '0' if not last word.

P — Parity field.

3.7.1.2.4 Control-filler message

The control-filler message consists of one word. It is sent whenever there is no other message to be sent on the forward control channel. It may be inserted between messages as well as between word blocks of a multi-word message. The control-filler message is chosen so that when it is sent, the 11 bit word sync sequence (11100010010) will not appear in the message stream, independent of the busy-idle bit status.

The control-filler message is also used to specify a control mobile attenuation code (CMAC) for use by mobile stations accessing the system on the reverse control channel, and a wait-for-overhead-message bit (WFOM) indicating whether or not mobile stations shall read an overhead message train before accessing the system, and read the supplementary digital color code which mobile stations will return in Word B of the reverse control channel message when mobile stations are requested to read control-filler before system access in the system parameter overhead message.

T1T2=11	DCC	010111	CMAC	SDCC1	11	SDCC2	1	WFOM	1111	OHD=001	P
2	2	6	3	2	2	2	1	1	4	3	12

The interpretation of the data fields is as follows:

T1T2	Type field. Set to '11' indicating overhead word.
DCC	Digital color code field.
CMAC	Control mobile attenuation field. Indicates the mobile station power level associated with the reverse control channel (see Table 2.1.2-1).
RSVD	Reserved for future use; all bits shall be set as indicated.
SDCC1, SDCC2	Supplementary Digital Color Codes. If the Supplementary Digital Color Code feature is utilized, the combination of SDCC1 and SDCC2 transmitted by the base station shall be a non-zero number. Mobile stations which respond with a non-zero SDCC combination are capable of supporting SDCC. Mobile stations which respond with a zero SDCC combination are not capable of supporting SDCC. The zero SDCC combination is used to indicate either that SDCC1 and SDCC2 are not used or are not supported.
WFOM	Wait-for-overhead-message field.
OHD	Overhead message type field. Set to '001' indicating the control-filler word.
P	Parity field.

3.7.1.3 Data restrictions

The 11 bit word-sync sequence (11100010010) is shorter than the length of a word, and therefore can be embedded in a word. Normally, embedded word-sync will not cause a problem because the next word to be sent will not have the word-sync sequence embedded in it. There are, however, three cases in which the word-sync sequence may appear periodically in the FOCC stream. They are:

- The overhead message
- The control-filler message
- Mobile station control messages with pages to mobile stations with certain central office codes.

These three cases are handled by

1. restricting the overhead message transmission rate to about once per second,
2. designing the control-filler message to exclude the word- sync sequence, taking into account the various busy-idle bits, and
3. restricting the use of certain central office codes.

If the mobile station control message (see §3.7.1.1) is examined with the MIN1 separated into NXX-X-XXX as described in §2.3.1 (where NXX is the central office code, N represents a number from 2-9, and X represents a number from 0-9), Table 3.7.1-5 identifies the central office codes that are troublesome when used in the 1-word page mode. Use of the 2-word page mode alleviates the possibility of improper word-sync when using troublesome central office codes. For completeness, all 3-digit combinations that may be troublesome are shown even though they may be unrealistic, e.g., beginning with 0 or 1.

Table 3.7.1-5 Troublesome central office codes

Bit pattern thousands					Central office	
T1T2	Digit DCC	NXX	X	XXX	Code	
00	ZZ	111110(0)0100	10YY	...	007	0,8,9
00	ZZ	111011(1)0001	0010	...	056	2
00	ZZ	111100(0)1001	0ZZZ	...	070	1-7
00	ZZ	000011(1)0001	0010	...	150	2
00	ZZ	000111(1)0001	0010	...	224	2
00	ZZ	000111(0)0010	010Z	...	225	4,5
00	ZZ	001011(1)0001	0010	...	288	2
00	ZZ	001110(0)0100	10YY	...	339	0,8,9
00	ZZ	001111(1)0001	0010	...	352	2
00	ZZ	001111(0)0010	010Z	...	353	4,5
00	ZZ	010011(1)0001	0010	...	416	2
00	ZZ	010111(1)0001	0010	...	470	2
00	ZZ	010111(0)0010	010Z	...	481	4,5
00	ZZ	011111(1)0001	0010	...	508	2
00	ZZ	011111(0)0010	010Z	...	509	4,5
00	ZZ	011011(1)0001	0010	...	544	2
00	ZZ	011100(0)1001	0ZZZ	...	568	1-7
00	ZZ	011110(0)0100	10YY	...	595	0,8,9
00	11	100010(0)1000	....	...	663	0-9
00	11	100010(0)1001	....	...	664	0-9
00	11	100010(0)1010	....	...	665	0-9
00	11	100010(0)1011	....	...	666	0-9
00	ZZ	100011(1)0001	0010	...	672	2
00	ZZ	100111(1)0001	0010	...	736	2
00	ZZ	100111(0)0010	010Z	...	737	4,5
00	ZZ	101011(1)0001	0010	...	790	2
00	ZZ	101110(0)0100	10YY	...	851	0,8,9
00	ZZ	101111(1)0001	0010	...	864	2
00	ZZ	101111(0)0010	010Z	...	865	4,5
00	Z1	110001(0)0101	....	...	890	0-9
00	Z1	110001(0)0100	....	...	899	0-9
00	ZZ	111000(1)0010	....	...	909	0-9
00	ZZ	110011(1)0001	0010	...	928	2
00	ZZ	110111(1)0001	0010	...	992	2
00	ZZ	110111(0)0010	010Z	...	993	4,5
00	ZZ	111111(0)0010	010Z	...	---	4,5*
00	ZZ	111111(1)0001	0010	...	---	2*

Notes:

1. YY bits can be '0', but both cannot be '1' at the same time.
2. Z represents a bit that may be '1' or '0'.

3. The bit in parentheses is the busy-idle bit.

4. * - Central Office Code above 999.

5. Central Office Codes beginning with '1' and '0' have been included for completeness.

3.7.2 Forward voice channel

The forward voice channel (FVC) is a wideband data stream sent by the base station to the mobile station. This data stream shall be generated at a 10 kbit/s±0.1 bit/s rate. Figure 3.7.2-1 depicts the format of the FVC data stream.

Figure 3.7.2-1 Forward voice channel message stream

DOTTING	W.S.	REPEAT 1 OF WORD 1	DOT	W.S.	REPEAT 2 OF WORD 1	
101	11	40	37	11	40	

	DOT	W.S.	REPEAT 9 OF WORD 1	DOT	W.S.	REPEAT 10 OF WORD 1	DOT	W.S.	REPEAT 11 OF WORD 1
	37	11	40	37	11	40	37	11	40

DOTTING	W.S.	REPEAT 1 OF WORD 2	DOT	W.S.	REPEAT 2 OF WORD 2	
101	11	40	37	11	40	

	DOT	W.S.	REPEAT 9 OF WORD 2	DOT	W.S.	REPEAT 10 OF WORD 2	DOT	W.S.	REPEAT 11 OF WORD 2
	37	11	40	37	11	40	37	11	40

DOTTING = 1010....101

W.S. (WORD SYNC) = 11100010010

A 37 bit dotting sequence (1010....101) and an 11 bit word sync sequence (11100010010) are sent to permit mobile stations to achieve synchronization with the incoming data, except at the first repeat of the word, where the 101 bit dotting sequence is used. Each word contains 40 bits, including parity, and is repeated eleven times together with the 37 bit dotting and 11 bit word sync sequences; it is then referred to as a word block. A word is formed by encoding the 28 content bits into a (40, 28) BCH code that has a distance of 5, (40, 28; 5). The left-most bit (i.e., earliest in time) shall be designated the most significant bit. The 28 most significant bits of the 40 bit field shall be the content bits. The generator polynomial is the same as that used for the forward control channel (see §3.7.1).

3.7.2.1 Mobile station control message

The Mobile Station Control Message is the only message transmitted over the forward voice channel. The Mobile Station Control Message consists of one or more words.

Mobile Station Control Message Word 1

2	2	2	1	8	5	3	5	12
T1T2=10	SCC=11	PSCC	EF=0	RSVD=000...0	LOCAL/MSG_TYPE	ORDQ	ORDER	P
	SCC≠11		RSVD=0	RSVD=0000000	VMAC	CHAN		
2	2	2	1	7	3	11		12

Word 2 - Base Station Challenge Order Confirmation

T1T2=01	RSVD=0000	AUTHBS	RSVD=0000	P
2	4	18	4	12

Word 2 - Unique Challenge Order Word

T1T2=01	RSVD=00	RANDU	P
2	2	24	12

Word 2 - First SSD Update Order Word

T1T2=01	RANDSSD_1	RSVD=00	P
2	24	2	12

Word 2 - First Alert With Info Word

T1T2 = 01	RL_W	SIGNAL	CPN_RL	PI	SI	RSVD = 000	P
2	5	8	6	2	2	3	12

Word 2 - First Flash With Info Word

T1T2 = 01	RL_W	CPN_RL	PI	SI	RSVD = 000...000	P
2	5	6	2	2	11	12

Word 3 - Second SSD Update Order Word

T1T2 = 01	RANDSSD_2	RSVD = 00	P
2	24	2	12

Word 3 - Second Alert With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word 3 - Second Flash With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word 4 - Third SSD Update Order Word

T1T2 = 01	RANDSSD_3	RSVD = 000...000	P
2	8	18	12

Word 4 - Third Alert With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word 4 - Third Flash With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word 5 - Fourth Alert With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word 5 - Fourth Flash With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

•

•

•

Word N - (N-1)th Alert With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

Word N - (N-1)th Flash With Info Word

T1T2 = 01	RSVD = 00	CHARACTER	CHARACTER	CHARACTER	P
2	2	8	8	8	12

The interpretation of the data fields is as follows:

T1T2 — Type field. Set to '10' in Word 1. Set to '01' in Word 2 and all subsequent Words. Additional words are sent after Word 1 only when the order is one of the following orders or order confirmations:

- Base Station Challenge Order Confirmation
- Unique Challenge Order
- SSD Update Order
- Alert With Info
- Flash With Info

SCC — SAT color code for new channel (see Table 3.7.1-2).

PSCC — Present SAT color code. Indicates the SAT color code associated with the present channel.

EF — Extended Protocol Forward Channel Indicator field. Set to zero for ANSI TIA/EIA 553A systems.

ORDER — Order field. Identifies the order type (see Table 3.7.1-1).

ORDQ — Order Qualifier field. Qualifies the order to a specific action (See Table 3.7.1-1).

LOCAL — Local Control field. This field is specific to each system. The ORDER field shall be set to local control (see Table 3.7.1-1) for this field to be interpreted.

MSG_TYPE — Message type field. Qualifies the order to a specific action (see Table 3.7.1-1).

VMAC — Voice mobile attenuation code field. Indicates the mobile station power level associated with the designated traffic channel (see Table 2.1.2-1).

CHAN — Channel number field. Indicates the designated voice channel (see §2.3.3).

RANDU — The 24 bit random number issued by the base in the Unique Challenge Order.

RANDSSD_1 — The most significant 24 bits of the random number issued by the base in the SSD Update Order.

RANDSSD_2 — The subsequent 24 bits (following RANDSSD_1) of the random number issued by the base in the SSD Update Order.

RANDSSD_3 The least significant 8 bits of the random number issued by the base in the SSD Update Order.

AUTHBS Output response of the authentication algorithm initiated by the Base Station Challenge Order.

RL_W The remaining length, in Words, of the Alert With Info or Flash With Info order.

SIGNAL An 8-bit information element that causes the mobile station to generate tones and alerting signals, coded as specified below:

This 8-bit field comprises two subfields: pitch, the two most-significant bits, and cadence, the six least-significant bits. Pitch represents a distinction between tones, usually based on frequency. Cadence is the on/off pattern of the tones. *Standard Alert* is pitch '00' in combination with cadence '000001'. If the mobile station supports distinctive alerting, it should generate the pitches and cadences recommended in the following tables. Recommended pitches and their corresponding codes are as follows:

Description	Code
Medium pitch	00
High pitch	01
Low pitch	10
Reserved	11

Recommended cadences and their corresponding codes are as follows:

Description	Code
No Tone: Off	000000
Long: 2.0 s on, 4.0 s off, repeating	000001
Short-Short: 0.8 s on, 0.4 s off, 0.8 s on, 4.0 s off, repeating	000010
Short-Short-Long: 0.4 s on, 0.2 s off, 0.4 s on, 0.2 s off, 0.8 s on, 4.0 s off, repeating	000011
Short-Short-2: 1.0 s on, 1.0 s off, 1.0 s on, 3.0 s off, repeating.	000100
Short-Long-Short: 0.5 s on, 0.5 s off, 1.0 s on, 0.5 s off, 0.5 s on, 3.0 s off, repeating.	000101
Short-Short-Short-Short: 0.5 s on, 0.5 s off, 0.5 s on, 0.5 s off, 0.5 s on, 0.5 s off, 0.5 s, 2.5 s off, repeating.	000110
PBX Long: 1.0 s on, 2.0 s off, repeating.	000111
PBX Short-Short: 0.4 s on, 0.2 s off, 0.4 s on, 2.0 off, repeating.	001000
PBX Short-Short-Long: 0.4 s on, 0.2 s off, 0.4 s on, 0.2 s off, 0.8 s on, 1.0 s off, repeating.	001001
PBX Short-Long-Short: 0.4 s on, 0.2 s off, 0.8 s on, 0.2 s off, 0.4 s on, 1.0 s off, repeating.	001010
PBX Short-Short-Short-Short: 0.4 s on, 0.2 s off, 0.4 s on, 0.2 s off, 0.4 s on, 0.2 s off, 0.4 s, 0.8 s off, repeating.	001011
Reserved	001100
...	...
Reserved	111111

CPN_RL — A 6-bit field used to indicate the number of CHARACTERs in the Alert With Info or Flash With Info order.

PI — Presentation indicator. A 2-bit field used to indicate whether or not the calling number should be displayed.

Description	Code
Presentation allowed	00
Presentation restricted	01
Number not available	10
Reserved	11

SI — Screening Indicator. A 2-bit field indicating how the calling number was screened.

Description	Code
User-provided, not screened	00
User-provided, verified and passed	01
User-provided, verified and failed	10
Network-provided	11

1

CHARACTER An 8-bit representation of an ASCII character, coded as described below and in the references cited therein. Note that in the absence of a sufficient number of characters to completely fill the last Alert With Info or Flash With Info Word, null characters(00000000) are to be used as filler.

2

3 Each character is an 8-bit field coded as follows:

4 • The most-significant bit is set to '0'.

5 • The remaining seven bits represent an ASCII character as defined in ANSI X3.4.

6

RSVD Reserved for future use; all bits shall be set as indicated.

P Parity field.

7

4 Reserved

5 Reserved

6 Change History

6.1 Chronology of Revisions for IS-3-B

Adopted	Section	Change
3/7/84	§§ 4, 5, 6	Added option and history sections.
3/7/84	§§ 4.1, 5.1	Added requirement for 32-digit dialling option.
5/16/84	PREFACE	Added description of each section.
5/16/84	NOTES	Added Notes 7 and 8.
5/16/84	§§ 2.7, 3.7	Added text of Note 8 to these sections.
5/16/84	§§ 3.7.1.2	Added clarifying statement that the system parameter overhead message shall be sent on all dedicated control channels.

6.2 Chronology of Revisions for IS-3-C

ADOPTED	SECTION	CHANGE
8/28/85	§ 1.1	Added general statement of tolerances on time and timing.
8/28/85	§§ 1, 2.3.3, 2.3.11, 2.6.4.2, 2.6.4.3.1, 2.6.4.3.2, 2.6.4.4, 2.6.4.5, 3.6.2.1, 3.7.1.2.1	Made changes and additions to define DTX operation and DTX operational requirements.
8/28/85	§ 2.3.2	Added Serial Number (SN) bit assignment requirements.
8/28/85	§ 2.3.8	Added System Identification (SID) bit assignment requirements.
8/28/85	§ 2.4.1.2	Changed to relax SAT phase requirements.
8/28/85	§§ 2.6.3.7, 2.7	Added references to section headings for options.
8/28/85	§§ 2.7.1.1, 2.7.2.1, 3.7.2.1	Added section headings for clarification.
8/28/85	§ 3.6.2.4	Updated second paragraph.
8/28/85	§ 3.6.3.2	Changed to correct the Busy/Idle bit operation and allow mobile station to land station messages of more than five words.
8/28/85	§ 3.6.4.3.2	Changed to make an Alert Timer optional.
8/28/85	§ 3.7.1.2.2	Added recommended use of the Overload Class field bits.
8/28/85	§ 3.7.1.3	Changed to clarify the troublesome office code problem and to correct office code table.
8/28/85	§ 4.1	Added text of Note 8 and deleted redundant material from excerpted § 2.7.1.1.
8/28/85	§§ 4.2, 5.2	Added sections for Extended Protocol.
8/28/85	§6.2	Listed revisions for IS-3-C.

6.3 Chronology of Revisions for IS-3-D

ADOPTED	SECTION	CHANGE
10/30/86	§ 1	Changed SIDs-p to SIDREGs-p under Numeric Information.
10/30/86	§ 2.3.4	Reduced memory requirement to a single registration.
10/30/86	§ 2.3.8	Deleted reserved notations and assigned '01' to "Other countries".
10/30/86	§ 2.6.1.2.2	Corrected "equal" sign to "not equal".
10/30/86	§ 2.6.2.1	Reduced memory requirement to a single registration.
10/30/86	§ 2.6.3.11	Reduced memory requirement to a single registration.
10/30/86	§ 3.7.1.2.2	Corrected section number.
1/28/87	NOTES	Deleted all of Note 7 except first sentence. Updated Note 9 for IS-3-D.
1/28/87	§ 2.1.1.1	Added extended spectrum requirements and Table 2.1.1.1-1.
1/28/87	§ 2.2.1.1	Added extended spectrum requirements.
1/28/87	§ 2.3.2	Deleted FCC serial number notice.
1/28/87	§ 2.3.3	Revised SCM requirements for extended spectrum.
1/28/87	§ 3.1.1.1	Added extended spectrum requirements.
1/28/87	§ 3.2.1.1	Added extended spectrum requirements.
1/28/87	§ 3.7.1.1	Added reference to § 2.3.3 for CHAN.
1/28/87	§ 3.7.2.1	Added reference to § 2.3.3 for CHAN.
1/28/87	§ 6.3	Listed revisions for IS-3-D.

6.4 Chronology of Revisions from IS-3-D to EIA/TIA 553

ADOPTED	SECTION	CHANGE
2/2/88	PREFACE	Changed to clarify experiences with commercial systems.
2/2/88	NOTES	Updated Note 9 for EIA-553. Added Note 11.
2/2/88	§ 1	Added Extended Protocol definition. Changed SIDREGs-p to SIDs-p under Numeric Information.
2/2/88	§ 2	Added reference to § 4.
2/2/88	§ 2.1.4.1	Added reference to measurement technique.
2/2/88	§ 2.6.2.1	Corrected NXTREGs-r to NXTREGs-p under Registration ID Message.
2/2/88	§ 2.6.3.7	Deleted reference to § 4.1.
2/2/88	§ 2.6.3.11	Revised first paragraph and first bullet item.
2/2/88	§ 2.7	Deleted reference to § 4.1.
2/2/88	§ 2.7.11	Deleted reference to § 4.1.
2/2/88	§ 3	Added reference to § 5.
2/2/88	§ 3.1.4.1	Added reference to measurement technique.
2/2/88	§ 3.7.1.3	Corrected office code 609 to be 509.
2/2/88	§ 4.2	Added requirements for Extended Protocol signaling and message structure option.
2/2/88	§ 5.2	Added requirements for Extended Protocol signaling and message structure option.
2/2/88	§ 6.4	Listed revisions for EIA-553.
10/21/88	NOTES	Added Notes 12 and 13.

6.5 Chronology of Revisions from EIA/TIA 553 to TIA/EIA 553-A

ADOPTED	SECTION	CHANGE
8/22/95	§2.6.3.9	Eliminate rescan in cases where paging and access channel sets are the same.
10/11/95	All sections	Adopted text of IS-91 as baseline making authentication mandatory in mobile stations.
11/2/95	§§2.1.1, 2.2.1, 3.1.1, 3.2.1	Made extended spectrum mandatory for MSs.
11/2/95	§2.3.1	Removed obsolete description of IMSI from IS-91.
12/5/95	§1	Added definitions of new terms in support of authentication.
12/5/95	§1, 2.6.1.2.1, 2.6.2.1, 2.6.3.1, 2.6.3.9,	Removed unnecessary registration after crossing paging area boundary.
12/5/95	§2.3.2	Removed obsolete reference to ESN procedures.
12/5/95	Note 8, §§2.6.2.1, 2.7, 3.7	Clarified interpretation of ignoring reserved bits.
12/5/95	§§1, 2.6.1.1, 2.6.1.1.1, 2.6.1.1.2, 2.6.2.1	Set $RAND_S$ to 0 when mobile station crosses system boundaries.
12/5/95	§2.6.2.1	Deleted random challenge received status used in IS-91 to assure consistency with TSB-47.
12/5/95	§2.6.3.4	Assure mobile stations test authentication capabilities of access channels.
12/5/95	§§2.6.5.3.1.A, 2.6.5.3.2.A, 2.6.5.4.A	Begin processing of SSD_A_NEW and SSD_B_NEW after receipt of all RANDSSD data during SSD update procedure.
12/5/95	Note 15	Added informative note concerning new global action messages.
12/5/95	§2.3.12.1.8	Clarified location of SSD update processing.
12/5/95	§3.3.2	Added section on system identification
12/5/95	§3.4.1.2	Clarified SAT transmission
12/5/95	§3.6.4	Clarified statement of SAT,ST status changes.
12/5/95	§§3.6.5.3.1.A, 3.6.5.4.A	Clarified confirmation of Base Station Challenge Order
12/5/95	§6.5	Added revision block for 553-A
4/6/99	Various	editorial changes as a result of comparision against common sections of IS-91-A and TIA/EIA-691

Annex A Message Encryption

This annex is available as a separate document whose distribution is controlled by TIA.