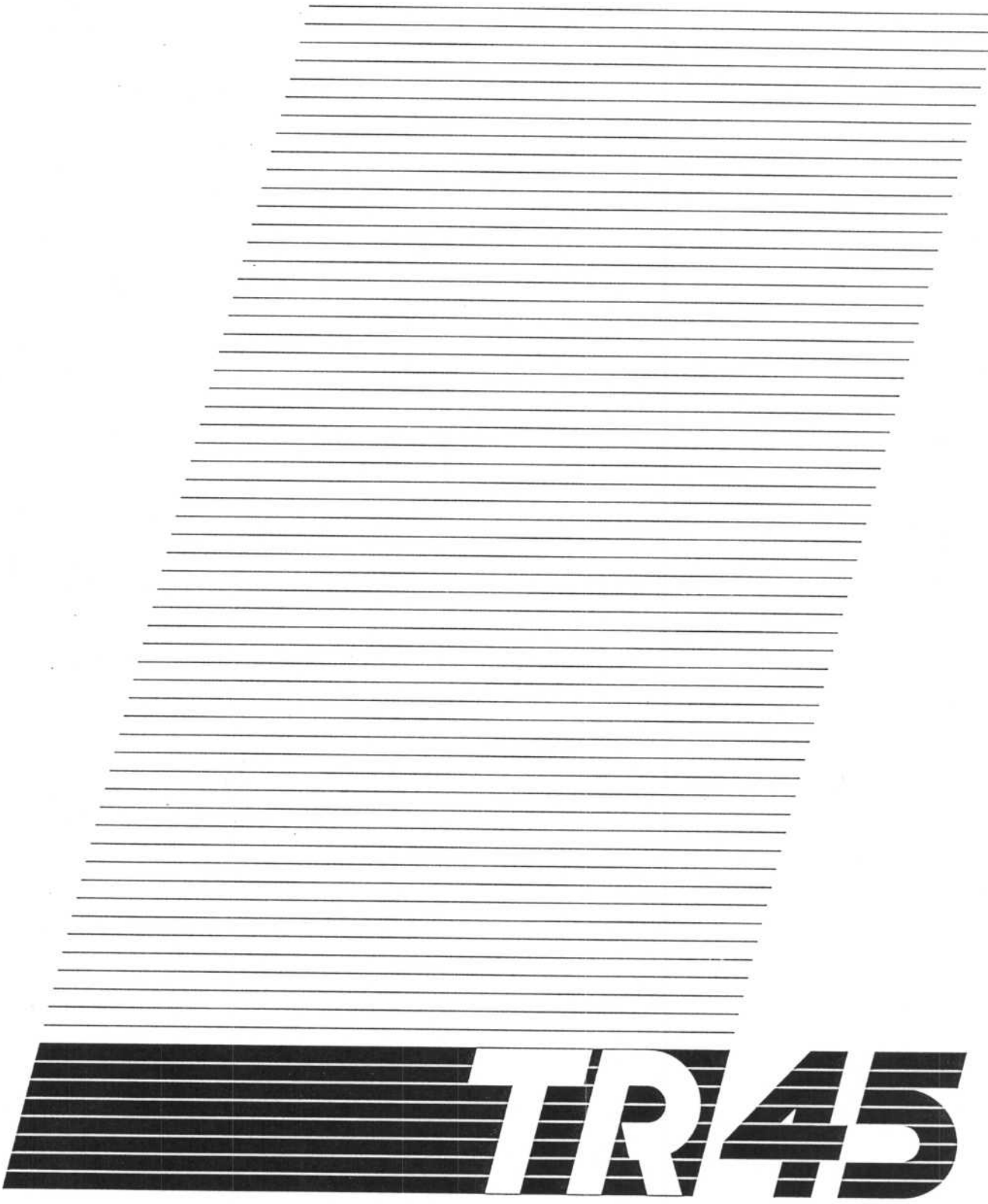

Appendix A to PN-3474 (IS-136)

October 16 1995

NOTICE

EIA/TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating inter-changeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. Existence of such Standards and Publications shall not in any respect preclude any member or non-member of EIA or TIA 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 EIA or TIA members, whether the standard is to be used either domestically or internationally.

Standards and Publications are adopted by EIA/TIA without regard to whether or not their adoption may involve patents or articles, materials, or processes. By such action, EIA/TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Recommended Standard or Publication.

TIA TR45 Ad Hoc Authentication Group Documents

TIA TR45 Ad Hoc Authentication Group Documents contain information deemed to be of technical value to the industry, and are published at the request of the TR45 Ad Hoc Authentication Group without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of an EIA/TIA Standard.

TIA TR45 Ad Hoc Authentication Group Documents bear on or are subject to the export jurisdiction of the US Department of State as specified in International Traffic in Arms Regulations (ITAR), Title 22 CFR parts 120 through 130 inclusive. An export license may be required for the transmission of such material in any form outside of the United States of America.

Contact

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Engineering Department
2001 Pennsylvania Avenue, N.W., Suite 800
Washington, D.C. 20006-1813

Document History

Revision	Date	Remarks
0	Aug 2,94	Frozen for PN3011 Ballot
0	Nov 14, 94	Reproduced for IS-136
1	Sep 13, 95	Added R-DATA unit for PN3474 (IS-136-A)
1	Oct 26, 95	Editorial change to §2.2.2.3. Frozen for PN-3474 Ballot

Table of Contents

1. Introduction 1

2. Message Encryption 1

2.1 Analog Voice Channels 1
2.1.1 Forward Analog Voice Channel 1
2.1.1.1 Alert With Info (See PN-3474•2§3.7.2.1.) 1
2.1.1.2 Flash With Info (See PN-3474•2§3.7.2.1.) 2
2.1.2 Reverse Analog Voice Channel 2
2.1.2.1 Called Address Message (See PN-3474•2§2.7.2.1 and PN-3474•2§4.1.3.1.) 2

2.2 Digital Traffic Channels 2
2.2.1 Forward Traffic Channel 2
2.2.1.1 Alert With Info (See PN-3474•2§3.7.3.1.3.2.1) 3
2.2.1.2 Flash With Info (See PN-3474•2§3.7.3.1.3.2.14) 3
2.2.1.3 R-DATA (See PN-3474•2§3.7.3.1.3.2.23) 3
2.2.2 Reverse Traffic Channel 3
2.2.2.1 Flash With Info (see PN-3474•2§2.7.3.1.3.2.8) 3
2.2.2.2 Send Burst DTMF (see PN-3474•2§2.7.3.1.3.2.9) 4
2.2.2.3 Send Continuous DTMF (See PN-3474•2§2.7.3.1.3.2.10) 4
2.2.2.4 R-DATA(See PN-3474•2§2.7.3.1.3.2.19) 4

3. Voice Privacy 5

1. Introduction

This document contains requirements for message encryption and voice privacy for cellular systems described in PN-3474•1, "800MHz TDMA Cellular – Radio Interface – Mobile Station - Base Station Compatibility – Digital Control Channel," and in PN-3474•2, "800MHz TDMA Cellular – Radio Interface – Mobile Station - Base Station Compatibility – Traffic Channels and FSK Control Channel." Related documents are the latest revisions of:

"Common Cryptographic Algorithms", TIA

"Interface to Common Cryptographic Algorithms", TIA

Note: The notation PN-3474•1§nn is used to indicate a referenced section in part 1 of PN-3474•1. The notation PN-3474•2§nn is used to indicate a referenced section in part 2 of PN-3474.

2. Message Encryption

The following is a description of the messages that are enciphered. For each message, the enciphered fields are designated. The messages are grouped by channel designation.

Message encryption is enabled/disabled by the field Message Encryption Mode, see PN-3474•2§2.7.1.3.3.

2.1 Analog Voice Channels

2.1.1 Forward Analog Voice Channel

2.1.1.1 Alert With Info (See PN-3474•2§3.7.2.1.)

The Alert with INFO message is encrypted. Word 1 of the Mobile Station Control Message contains the order and order qualifier fields that identify this message as **ALERT WITH INFO.** No field in Word 1 is encrypted. No field in Word 2 - First Alert With Info Word is encrypted.

The subsequent words contain a character representation. Each character transmitted is represented in IA5 form in a field of 8 bits. Each word contains up to three characters. The 24 bits that comprise the three characters in each FVC word are treated by CMEA as a single message.

No other fields in the *Alert With Information Message* are encrypted.

2.1.1.2 Flash With Info (See PN-3474•2§3.7.2.1.)

The Flash with INFO message is encrypted. Word 1 of the Mobile Station Control Message contains the order and order qualifier field that identify this message as **FLASH WITH INFO**. No field in Word 1 is encrypted. No field in Word 2 - Flash With Info Word is encrypted.

The subsequent words contain a character representation. Each character transmitted is represented in IA5 form in a field of 8 bits. Each word contains up to three characters. The 24 bits that comprise the three characters in each FVC word are treated by CMEA as a single message.

No other fields in the *Flash With Information Message* are encrypted.

2.1.2 Reverse Analog Voice Channel

2.1.2.1 Called Address Message (See PN-3474•2§2.7.2.1 and PN-3474•2§4.1.3.1.)

The 32 bits in Word 1 - First Word of the **Called Address Message** which comprise digits 1-8 are encrypted. These 32 bits are treated by CMEA as a new single message. No additional fields in Word 1 are encrypted.

The 32 bits in each Word 2 (and Word 3 and 4 when sent for 32-Digit Dialing) of the **Called Address Message** which comprise further dialed digits are encrypted. These 32 bits are treated by CMEA as a new single message.

No other fields in the *Called Address Message* are encrypted.

2.2 Digital Traffic Channels

When encryption is disabled, all fields of all signaling messages sent by the mobile station and base station are unencrypted.

Encryption shall apply only to the part of the message body specified below. The message CRC shall never be encrypted.

2.2.1 Forward Traffic Channel

When encryption is enabled, the encryptable fields of the following Forward Traffic Channel messages, as listed below, shall be encrypted. All other Forward Traffic Channel messages shall be unencrypted.

2.2.1.1 Alert With Info (See PN-3474•2§3.7.3.1.3.2.1)

The FACCH message contains up to n characters each represented as 8 bits in the IA5 format. These are enciphered prior to convolutional coding. The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

2.2.1.2 Flash With Info (See PN-3474•2§3.7.3.1.3.2.14)

The FACCH message contains up to n characters each represented as 8 bits in the IA5 format. These are enciphered prior to convolutional coding. The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

No other fields in the *Flash With Information Message* are encrypted.

2.2.1.3 R-DATA (See PN-3474•2§3.7.3.1.3.2.23)

The SACCH/FACCH message contains up to n octets of binary information formatted according to specific TeleService ID contained in Higher Layer Protcol ID of the R-DATA Unit (See PN-3474•2§2.7.3.1.3.3). These are enciphered prior to convolutional coding, and only if the TeleService ID indicates Over-theAir Activation (See PN-3474•2§7·2). The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

2.2.2 Reverse Traffic Channel

When encryption is enabled, the encryptable fields of the following Reverse Traffic Channel messages, as listed below, shall be encrypted. All other Reverse Traffic Channel messages shall be unencrypted.

2.2.2.1 Flash With Info (see PN-3474•2§2.7.3.1.3.2.8)

The FACCH message contains up to 63 characters each represented as 8 bits in the IA5 format. These are enciphered prior to convolutional coding. The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

No other fields in the *Flash With InfoMessage* are encrypted.

2.2.2.2 Send Burst DTMF (see PN-3474•2§2.7.3.1.3.2.9)

The FACCH message contains up to 64 digits each represented as 4 bits. These are enciphered prior to convolutional coding. The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

2.2.2.3 Send Continuous DTMF (See PN-3474•2§2.7.3.1.3.2.10)

The FACCH message contains 40 bits, 4 of which represent 1 digit. The message is enciphered prior to convolutional coding. All fields except the Message Type (40 bits total) are encrypted by CMEA. The CRC is computed on the resultant 48 bits.

2.2.2.4 R-DATA(See PN-3474•2§2.7.3.1.3.2.19)

The SACCH/FACCH message contains up to n octets of binary information formatted according to specific TeleService ID contained in Higher Layer Protcol ID of the R-DATA Unit (See PN-3474•2§2.7.3.1.3.3). These are enciphered prior to convolutional coding, and only if the TeleService ID indicates Over-theAir Activation (See PN-3474•2§7·2). The CRC is computed on the resultant 48 bits. For the first slot of a multi-slot message (Continuation Flag = 0) all fields except the Message Type (40 bits total) are encrypted by CMEA. For the subsequent slots of a multi-slot message (Continuation Flag =1) all fields are encrypted (total of 48 bits) by CMEA.

3. Voice Privacy

A Voice Privacy Mask (VPM) comprising two different 260-bit binary data values is generated. One is XORed with the bits in the Forward Digital Traffic Channel and the other is XORed with the bits in the Reverse Digital Traffic Channel to provide so-called "voice privacy." The VPM used for BS to MS transmission is the Forward VPM; that for MS to BS transmission is the Reverse VPM (see "Common Cryptographic Algorithms", April 21, 1993, TIA)

If VPM is not available at the time of an initial traffic channel designation upon entering the Conversation task, (typically due to calculation delay in its generation) then a VPM of all zeros is to be used until the operational VPM has been completely generated.

Enciphering shall take place after error correction coding and before interleaving. In particular, note that user voice is enciphered while still represented as bits rather than quaternary symbols. Similarly, deciphering occurs after deinterleaving.