**APIC Encryption Task Group**

|  |  |
| --- | --- |
| Document Number: | ETG-17-005-R5 |
| Title: | TDMA Link Layer Encryption |
| Editor: | Thomas A. Hengeveld, Harris Corporation |
| Date: | 2017-06-05 |
| Print Date: | 2017-06-05 |
| Abstract: | This document is a proposal for Link Layer Security for TIA-102 TDMA air interfaces.  |

**COPYRIGHT STATEMENT**

This document has been prepared by the authors to assist the APIC Encryption Task Group. It is proposed to the Committee as a basis for discussion and is not to be construed as a binding proposal on the author or his employer. The author and author's employer specifically reserve the right to amend or modify the material contained herein and nothing herein shall be construed as conferring or offering licenses or rights with respect to any intellectual property of author or his employer other than provided in the copyright statement below.

 APIC DRAFT

 PROPOSAL

TDMA Link Layer Encryption (LLE)

 ETG-17-005

Patent Identification

The reader’s attention is called to the possibility that compliance with this document may require the use of one or more inventions covered by patent rights. By publication of this document no position is taken with respect to the validity of those claims or any patent rights in connection therewith. The patent holders so far identified have, we believe, filed statements of willingness to grant licenses under those rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such licenses.

The following patent holders and patents have been identified in accordance with the TIA intellectual property rights policy:

No patents have been identified.

TIA shall not be responsible for identifying patents for which licenses may be required by this document or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Trademark Identification

This specification references the following trademarks:

No trademarks identified.

TABLE OF CONTENTS

[Patent Identification i](#_Toc484427297)

[Trademark Identification i](#_Toc484427298)

[1 Introduction - 1 -](#_Toc484427299)

[1.1 Scope - 1 -](#_Toc484427300)

[1.2 Abbreviations - 2 -](#_Toc484427301)

[1.3 Definitions - 2 -](#_Toc484427302)

[1.4 References - 3 -](#_Toc484427303)

[2 Overview - 4 -](#_Toc484427304)

[2.1 High Level Description of TDMA LLE - 4 -](#_Toc484427305)

[2.2 Cryptographic Operations - 8 -](#_Toc484427306)

[2.2.1 Notation - 8 -](#_Toc484427307)

[2.2.2 Encryption Scheme and Notation - 9 -](#_Toc484427308)

[2.2.3 Initial Vector - 9 -](#_Toc484427309)

[2.2.4 Construction of LLEIV for TDMA LL Encryption - 10 -](#_Toc484427310)

[3 Link Layer Encryption of 2-slot TDMA Working Channels - 12 -](#_Toc484427311)

[3.1 Link Layer Encryption of Bursts Containing Voice - 12 -](#_Toc484427312)

[3.1.1 LLE of 4V Bursts - 12 -](#_Toc484427313)

[3.1.2 LLE of 2V Bursts - 13 -](#_Toc484427314)

[3.1.3 LLE of Voice Frames - 14 -](#_Toc484427315)

[3.1.4 LLE of End-to-End Encryption Sync Signaling - 16 -](#_Toc484427316)

[3.2 LLE of Bursts Containing Signaling (Data, Control) - 18 -](#_Toc484427317)

[3.2.1.1 LL Encrypted MAC PDU Format - 18 -](#_Toc484427318)

[3.2.1.2 LLE of a MAC PDU - 20 -](#_Toc484427319)

[4 Required Site Procedures - 21 -](#_Toc484427320)

[4.1 Broadcast OSPs for LLE - 21 -](#_Toc484427321)

[5 Information Elements - 22 -](#_Toc484427322)

[5.1 DUID Encoding - 22 -](#_Toc484427323)

LIST OF TABLES

[Table 1: Document Revision History iv](#_Toc484427293)

[Table 2, Information Content and Protection Conditions by Logical Channel - 6 -](#_Toc484427294)

[Table 3, Protected Fields by Burst Type - 7 -](#_Toc484427295)

[Table 7, DUID Information Bits - 22 -](#_Toc484427296)

LIST OF FIGURES

[Figure 1, TDMA Link Layer Encryption Architecture - 4 -](#_Toc484427282)

[Figure 2 , Notations - 8 -](#_Toc484427283)

[Figure 3, LLE of Voice Frames - 14 -](#_Toc484427284)

[Figure 4 , Voice Frame Packing for LLE - 15 -](#_Toc484427285)

[Figure 5, LLE of ESS - 16 -](#_Toc484427286)

[Figure 6 , Packing for ESS-B1 - 17 -](#_Toc484427287)

[Figure 7 , Packing for ESS-B2 - 17 -](#_Toc484427288)

[Figure 8 , Packing for ESS-B3 - 17 -](#_Toc484427289)

[Figure 9 , Packing for ESS-B4 - 17 -](#_Toc484427290)

[Figure 10, MAC PDU Formats - 18 -](#_Toc484427291)

[Figure 11, IECI and OECI MAC PDUs - 19 -](#_Toc484427292)

DOCUMENT REVISION HISTORY

Table 1: Document Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| R5 | June 2017 | Ready for transmission to TR8. |
| R3 | May 2017 | Final proposed comment resolutions per R4 of the comment matrix. |
| R1 | March 2017 | Proposed Comment Resolutions per R1 of the comment matrix. |
| R0 | January 2017 | Restarted Version Numbering. |

# Introduction

This document describes the specifications for link layer security provided by encryption of TDMA data bursts over the TDMA air interface. It includes an overview of link layer encryption for TDMA, a section to specify link layer encryption of bursts containing voice, a section for site procedures in the RF sub-system, and a section for information elements used for link layer encryption. Link layer security is generally applied to the data transmitted over the TDMA air interface including voice, control, and other signaling fields. It is not a substitute for end-to-end encryption of voice messages that is separately specified in TIA-102.AAAD for the block encryption protocol (ref. (2)). Other parts of the TIA-102 suite of standards provide link layer security specifications for other parts of a system, such as for FDMA channels, that are outside of the scope of this document.

## Scope

The scope of this document is link layer security for TDMA channels in the TIA-102 suite of standards. Link layer security applies encryption to fields of sensitive data transmitted over the TDMA air interface to protect the data from interception and interpretation by unauthorized receivers. The encryption function is often labeled as link layer encryption. The sensitive data that is to be encrypted on the air interface includes digital voice, control signals that affect calls, and data signals that affect RF sub system operation. The protection of sensitive data uses a cryptographic function that is synchronized with a time value so that sensitive data cannot be copied and replayed on the channel for any unauthorized purpose. This document includes an overview of the link layer security cryptographic operations; as well as specifications for link layer encryption of voice, data, and control; site procedures for the RF sub system; and relevant information elements used for link layer encryption. The scope of this document does not include link layer encryption of FDMA channels, or end-to-end encryption of digital voice. Both of those items are covered in other standards in the TIA-102 suite. Together the combination of end-to-end encryption of messages with link layer security of TDMA and FDMA channels provides improved security for systems using the TIA-102 suite of standards that includes resistance to interception, eavesdropping, misdirection, message replay, spoofing, and traffic analysis.

## Abbreviations

 2V,4V: 2 or 4 Voice (slots)

ALGID: Algorithm ID

ANSI: American National Standards Institute

Cryptosync: Cryptographic synchronization

DUID: Data Unit ID

E2E: End-to-End

ESS: Encryption Synch Symbols

FACCH: Fast Associated Control Channel

FEC: Forward Error Correction

IECI: Inbound Encoded Control Information

IEMI: Inbound Encoded MAC Information

I-OEMI: Outbound Encoded MAC Information (with Information)

ISCH: Inter-slot Signaling Channel

IV: Initial Vector

KID: Key ID

LL: Link Layer

LLE: Link Layer Encryption

MAC: Media Access Control

MI: Message Indicator

PDU: Protocol Data Unit

RFSS: RF Subsystem

SACCH: Slow Associated Control Channel

S-OEMI: Outbound Encoded MAC Information (with sync)

SU: Subscriber Unit

TIA: Telecommunications Industry Association

VTCH: Voice (Transport) Channel

WACN: Wide Area Communications Network

## Definitions

2V: Slots containing 2 voice frames

4V Slot: Slots containing 4 voice frames

## References

The following documents contain provisions that, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. The American National Standards Institute (ANSI), The Telecommunications Industry Association (TIA), and other organizations maintain registers of currently valid standards published by them.

References marked as "(INFORMATIVE)" are for informational purposes only and do not constitute normative provisions of this document.

Editor's Note: The references to TIA-102BABA-1 need to be updated to refer to the corresponding bits of TIA-102.BABA-A. The references have figure/table numbers, and so need to be carefully checked.

1. *Digital Land Mobile Radio Block Encryption Protocol.* **TIA.** s.l. : http://tiaonline.org/standards, August 2009. (NORMATIVE). TIA-102.AAAD-A.

2. *Link Layer Security Overview.* **TIA.** Year TBD. STANDARD#TBD.

3. *Recommendation for Block Cipher Modes of Operation,Methods and Techniques.* **Dworkin, Morris.** s.l. : National Institute of Standards and Technology, December 2001. (NORMATIVE). SP800-38A.

4. *Phase 2 Two-Slot TDMA Media Access Control Layer Description.* **TIA.** s.l. : http://tiaonline.org/standards, December 2010. (NORMATIVE). TIA-102.BBAC.

5. *Half-Rate Vocoder Annex.* **TIA.** s.l. : http://tiaonline.org/standards, July 2009. (NORMATIVE) {NEEDS TO BE REPLACED WITH REFTO BABA\_A}. TIA-102.BABA-1.

6. *TIA-102.BBAD: Two Slot TDMA Control Channel MAC Layer Specification.* **December TBD.**

**7. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators.* Elaine Barker, John Kelsey. June 2015. NIST SP800-90AR1.**

**8. *Trunking Control Channel Messages.* TIA. s.l. : http://tiaonline.org/standards, October 2009. (NORMATIVE). TIA-102.AABC-C.**

**9. *FDMA - Common Air Interface.* TIA. s.l. : http://tiaonline.org/standards, September 2003. (INFORMATIVE). TIA-102.BAAA-A.**

**10. *PLACEHOLDER: LLS KEY MANAGEMENT DOCUMENT.* TIA. s.l. : http://tiaonline.org/standards, Month Year. (NORMATIVE). TIA-102.WTF.**

**11. *PLACEHOLDER - REFERENCE FOR LL Encryption of FDMA MESSAGES.* TIA. s.l. : http://tiaonline.org/standards. (NORMATIVE).**

# Overview

## High Level Description of TDMA LLE



Figure , TDMA Link Layer Encryption Architecture

Figure 1 illustrates the high-level architecture for Link Layer Encryption (LLE) for TDMA channels. In the figure, the following conventions are used:

* x,a,b: Represents the information to be protected which may come from the site itself (a), from infrastructure (b), or from an Subscriber Unit (SU) (x).
* t: Represents an initial vector for encryption comprising a site identification and a time coordinate as specified herein;
* E(k,x,t): When used in a box, E(k,x,t) represents encryption of *x* using the key *k,* and initial vector *t.* When used to label a line, it represents the result of that encryption.
* D(k,x,t): Represents decryption of the input *x* using the key *k* and initial vector *t.*
* Red (dotted) Flow: Indicates an information flow carrying unencrypted information; and,
* Black Flow: Indicates an information flow carrying encrypted information.

When transmitting link layer protected information on TDMA channels, an SU (e.g., SU1) encrypts that information in accordance with this specification. The encryption key for a site is derived from a Common Link Encryption Key (CLEK) using the Wide Area Communications Network (WACN), System, RF Subsystem (RFSS), and Site ID to create a unique key for each site. The initial vector for any particular TDMA channel (see ref. (3)) comprises the downlink frequency of the channel, time and date information, and a two-bit source indicator. The time coordinate has a granularity of micro-slots (7.5 msec) and is synched to the control channel. The initial vector for TDMA LLE is implicit, that is, not carried in the TDMA bursts. Link Layer Encryption for TDMA therefore requires that TDMA channels be synchronized to the control channel timing.

A receiving site (e.g., Site 1) decrypts an LLE encrypted transmission and, when appropriate, forwards the information content throughout the network to other similar sites (e.g, Site 2), or processes it locally. If the information is to be forwarded out on the same TDMA site, the site re-encrypts it according to the time slot in which it will be forwarded, and transmits it over the air.

Sites also need to transmit information that is sourced from the site itself, or from infrastructure (e.g., *a* and *b* in Figure 1). Such information is likewise encrypted by the site using the site identification and time coordinate as the initial vector in the encryption.

An SU that is in possession of the appropriate key, site identifying information and time information, and receives an encrypted transmission (e.g., SU2 and SU3), can decrypt and process the transmission.

In Figure 1, in order to illustrate the flow, Site 1 is only shown processing information received from SU1 and Site 2 is only illustrated as processing information received from the infrastructure (or information that is self-generated). Likewise, SU2 and SU3 are only shown receiving information. It should be clear to one of ordinary skill in the art that these roles are non-restrictive in real systems, e.g., that under other circumstances, Site 1 may take on any of the roles illustrated by Site 2 in the figure, and vice versa. Likewise, the roles of SU1,SU2 and SU3 are illustrative only and under other circumstances than those illustrated, any SU may take on any of the illustrated roles.

Table 2 identifies the information content of the logical TDMA channels, and the conditions under which that information is protected. Only the Inter-slot Signaling Channel (ISCH) is never protected, as it never carries sensitive information. All other logical channels may be protected if the underlying information requires protection. When a logical channel requires protection, it is protected through link-layer encryption of voice frames, end-to-end (E2E) cryptographic synchronization (cryptosync), and Media Access Control (MAC) Protocol Data Units (PDUs) prior to the computation of FEC.

Table , Information Content and Protection Conditions by Logical Channel

|  |  |  |
| --- | --- | --- |
| Logical Channel | Information content | Protection Condition |
| Voice Transport Channel (VTCH) | Voice and End-to-end Cryptosync | Protected when target is a protected user[[1]](#footnote-1) or group, or when source is a protected user.  |
| Slow Associated Control Channel (SACCH) | MAC PDUs containing MAC Messages | Protected if MAC Messages require protection |
| Fast Associated Control Channel (FACCH) | MAC PDUs containing MAC Messages | Protected if MAC Messages require protection |
| Inter-slot Signaling Channel (ISCH) | TDMA superframe and voice channel indicators and synchronization | Not Protected |
| Logical Control Channel (LCCH) | MAC PDUs containing MAC Messages | Protected if MAC Messages require protection. |

Table 3 identifies protected and unprotected information at the burst level[[2]](#footnote-2). The Data Unit ID (DUID), as well as Parity, Ramp, Guard, Pilot, Synchronization and ISCH symbols are not protected. Voice information, end-to-end cryptosync, and MAC messages are protected when required.

Table , Protected Fields by Burst Type

|  |  |  |
| --- | --- | --- |
| Burst Type | LLE Protected Information | Unprotected Information |
| Inbound 4V | Voice Frames, E2E Encryption Sync (ESS-B) | Parity, DUID, Ramp, Guard and Pilot Symbols |
| Inbound 2V | Voice Frames | Parity, DUID, Ramp, Guard and Pilot Symbols |
| Outbound 4V | Voice Frames, E2E Encryption Sync (ESS-B) | Parity, DUID, ISCH |
| Outbound 2V | Voice Frames | Parity, DUID, ISCH |
| Inbound Burst with Signaling | MAC PDU in IEMI | Parity, DUID, Ramp, Guard, Sync, and Pilot Symbols |
| Outbound Signaling Burst with Synchronization | MAC PDU in S-OEMI | Parity, DUID, ISCH, Sync |
| Outbound Signaling Burst without Synchronization | MAC PDU in I-OEMI | Parity, DUID, ISCH |
| Inbound Encoded Control Information  | MAC PDU in IECI | Parity, DUID, Ramp, Guard, Sync and Pilot |
| Outbound Encoded Control Information | MAC PDU in OECI | Parity, DUID, ISCH |

LL Encrypted voice bursts are identified by DUID. LL Encrypted MAC PDUs are identified by the presence of a "protected" (P) bit in the MAC PDU header octet.

## Cryptographic Operations

### Notation

Unless otherwise specified, and excluding code fragments, the following notation, illustrated in Figure 2 is used to denote various information elements in this document:

* xy is used to denote the (y+1)th quantity in an array of quantities. For example, in an octet array X, X0 denotes the first octet in the array, and X17 denotes the 18th octet of the array. When x is a bit array, xz is used to denote the (z+1)th most significant bit of the quantity x. For example, in a bit array X, X0 denotes the least significant bit of the array.
* xy,z is used to denote the (z+1)th bit of the quantity xy. For example, in an octet array X, Xy,0 denotes the least significant bit of the octet Xy, and Xy,7 denotes its most significant bit.
* {Xa…Xb} is used to denote a ordered range of quantities within an array of quantities. For example, if X is an octet array, {X7…X10} denotes an array of 4 octets comprising X7,X8,X9,X10 in order.
* xb(y) is equivalent to xy,b and is used in some tables (particularly related to voice coding) to be consistent with nomenclature used elsewhere in TIA-102 specifications.



Figure 2 , Notations

### Encryption Scheme and Notation

TDMA LLE SHALL employ AES Counter Mode Encryption per ref. (4) where the Initial Vector (IV) of the counter is derived as defined in section 2.2.3, and the counter increments by one for each block of keystream generated.

Herein, this encryption scheme is represented functionally by two operations CtrInit(), and CtrEncrypt(), defined as follows:

CtrInit(K,IV)

CtrInit() initializes counter mode encryption with the key K and the initial vector IV where:

* K is the key;
* IV is the initial vector of the counter per section 2.2.3;

C = CtrEncrypt(P,L),

CtrEncrypt() uses counter mode encryption to encrypt or decrypt an octet array P of length L octets to produce an octet array C, likewise of L octets. Here:

P is the plaintext octet array to be encrypted, comprising L information octets. P must be null padded to an integral number of octets. Padding bit need not be transmitted;

L is the number of octets of P to be encrypted;

C is the cipher-text resulting from encryption, comprising L information octets; and,

If L is not an integral multiple of the blocksize of the cipher, CtrEncrypt preserves the unused keystream for use in its next invocation. Hence, regardless of the blocksize of the underlying cipher,

C0 = CtrEncrypt(P0,1)

C1 = CtrEncrypt(P1,1)

is equivalent to:

C = CtrEncrypt(P,2).

### Initial Vector

For TDMA operation, the Initial Vector (IV) SHALL be LLEIV per ref. (3). The LLEIV is derived from various programmed and over-the-air sources. The LLEIV is loaded at the beginning of each TDMA slot.

Editor’s Note: Per MS08, it may be beneficial to added additional information about the load event during the TR8 revisit of this document.

### Construction of LLEIV for TDMA LL Encryption

For TDMA LL Encryption, the fields of the LLEIV SHALL be constructed as follows:

* Downlink Frequency (24 Bits): The 24-bit downlink or direct mode frequency expressed in eighths of kilohertz.
* Year (7 bits): The UTC year less 2000.
	+ For 4V and 2V Voice Bursts, the Year SHALL be the year as of the beginning of the slot containing the burst.
	+ For MAC PDUs, the Year SHALL be the year as of the beginning of the slot containing the burst bearing the MAC PDU.
* Month (4 bits): The month of the year, January (0001) to December (1100).
	+ For 4V and 2V Voice Bursts, the Month SHALL be the month as of the beginning of the slot containing the burst.
	+ For MAC PDUs, the Month SHALL be the month as of the beginning of the slot containing the burst bearing the MAC PDU.
* Day (5 bits): The day of the month. Day may range from binary 00001 (1) to binary 11111 (31).
	+ For 4V and 2V Voice Bursts, the Day SHALL be the day as of the beginning of the slot containing the burst.
	+ For MAC PDUs, the Day SHALL be the day as of the beginning of the slot containing the burst bearing the MAC PDU.
* Hour (5 bits): The hour of the day. Hour may range from binary 00000 (0) to binary 10111 (23).
	+ For 4V and 2V Voice Bursts, the Hour SHALL be the hour as of the beginning of the slot containing the burst.
	+ For MAC PDUs, the Hour SHALL be the hour as of the beginning of the slot containing the burst bearing the MAC PDU.
* Minute (6 bits): The minute of the hour. Minute may range from binary 000000 (0) to binary 111011 (59).
	+ For 4V and 2V Voice Bursts, the Minute SHALL be the minute as of the beginning of the slot containing the burst.
	+ For MAC PDUs, the Minute SHALL be the minute as of the beginning of the slot containing the burst bearing the MAC PDU.
* Microslot (13 bits): The microslot count. Microslot may range from binary 0 (0) to 01111100111111 (7999).
	+ For Inbound 4V and 2V Voice Bursts, the Microslot SHALL correspond to the start of the slot containing the burst.
	+ For Inbound MAC PDUs, the microslot SHALL correspond to the start of the slot containing the burst.
	+ For Outbound 4V and 2V Voice Bursts, the Microslot SHALL correspond to the start of the slot containing the burst.
	+ For Outbound MAC PDUs, the microslot SHALL correspond to the start of the slot containing the burst.
* Source Indicator (2 bits: S1,S2): indicating the source of the transmission.
	+ SUs transmitting to an RFSS SHALL use the Inbound (00) source indicator. RFSS’s receiving such traffic assume the inbound source indicator (00).
	+ RFSSs transmitting on the outbound channel SHALL use the Outbound (01) source indicator. SU’s received such traffic assume the source indicator (01).

# Link Layer Encryption of 2-slot TDMA Working Channels

2-Slot TDMA working channels that employ LLE SHALL be time aligned per ref. (1) section 3.4.

## Link Layer Encryption of Bursts Containing Voice

LLE encrypted 4V voice bursts SHALL be labeled by the transmitting entity with the Encrypted 4V Voice DUID.

LLE encrypted 2V voice bursts SHALL be labeled by the transmitting entity with the Encrypted 2V Voice DUID.

### LLE of 4V Bursts

Link Layer Encryption of 4V bursts SHALL proceed as follows, or by any method that produces equivalent results:

Let K be the STEK of the TDMA channel per ref. (3);

Let V0, V1, V2, V3 be the 49 bit voice frames scheduled for transmission in the 4V Burst;

Let B be the 24-bit ESS information subfield scheduled for transmission in the 4V Burst;

Compute V'i, the encrypted voice fields of the burst, and B', the encrypted ESS-B field of the burst as follows:

1. Compute IV per section 2.2.3 by setting it to the value of the LLEIV per section 2.2.4.
2. Initialize the cipher as CtrInit(K,IV).
3. Compute B' from B as described in section 3.1.4.
4. Compute V'0 from V0 as described in section 3.1.3
5. Compute V'1 from V1 as described in section 3.1.3.
6. Compute V'2 from V2 as described in section 3.1.3.
7. Compute V'3 from V3 as described in section 3.1.3.
8. Transmit V'i in lieu of Vi, and compute FEC on and transmit B' in lieu of B.

Link Layer Decryption of 4V bursts SHALL proceed as follows, or by any method that produces equivalent results, following successful error correction and de-interleaving of the voice frame:

Let K be the STEK of the TDMA channel per ref. (3);

Let V’0, V’1,V’2, V’3 be the 49-bit LLE encrypted voice frames received in the burst;

Let B’ be the 24-bit LLE encrypted ESS information contained in the 4V Burst;

Compute Vi, the decrypted voice fields and B', the decrypted ESS information as follows:

1. Compute IV per section 2.2.3 by setting it to the value of the LLEIV per section 2.2.4.
2. Initialize the encryption scheme, i.e., CtrInit(K,IV).
3. Compute B from B’ as described in section 3.1.4.
4. Compute V0 from V’0 as described in section 3.1.3.
5. Compute V1 from V’1 as described in section 3.1.3.
6. Compute V2 from V’2 as described in section 3.1.3.
7. Compute V3 from V’3 as described in section 3.1.3.
8. Use Vi and B in subsequent processing of the voice frame.

### LLE of 2V Bursts

Link Layer Encryption of 2V bursts SHALL proceed as follows, or by any method that produces equivalent results:

Let K be the STEK of the TDMA channel per ref. (3);

Let V0, V1 be the 49-bit voice frames scheduled for transmission in the 2V Burst;

Compute V'i, the encrypted voice fields of the burst as follows:

1. Compute IV per section 2.2.3 by setting it to the value of the LLEIV per section 2.2.4.
2. Initialize the cipher as CtrInit(K,IV).
3. Compute V'0 from V0 as described in section 3.1.3.
4. Compute V'1 from V1 as described in section 3.1.3.
5. Transmit V'i in lieu of Vi.

Link Layer Decryption of 2V bursts SHALL proceed as follows, or by any method that produces equivalent results, following successful error correction and de-interleaving of the voice frame:

Let K be the STEK of the TDMA channel per ref. (3);

Let V’0, V’1 be the 49-bit LLE encrypted voice frames received in the burst;

Compute V0, V1 the decrypted voice fields of the burst as follows:

1. Compute IV per section 2.2.3 by setting it to the value of the LLEIV per section 2.2.4.
2. Initialize the encryption scheme, i.e., CtrInit(K,IV).
3. Compute V0 from V’0 as described in section 3.1.3.
4. Compute V1 from V’1 as described in section 3.1.3.
5. Use Vi in subsequent processing of the voice frame.

### LLE of Voice Frames

Figure 3illustrates how TDMA LL Encryption fits into the processing flow of voice frames. Per ref. (5), each individual voice frame comprises four discrete information vectors for a total of 49 bits. When end-to-end encryption is performed, it is applied immediately following the development of the information vectors. In the absence of LLE, the encrypted information vectors are forward error correction (FEC) coded, interleaved, and then assembled into a MAC burst for transmission. When LLE is applied, it is inserted immediately following end-to-end encryption (if present), or applied directly to the voice frame.

Decryption follows the inverse path, with de-interleaving followed by forward error correction, then LL decryption and E2E encryption as required by the received burst.

Figure 3 illustrates the complete processing of voice frames, without regard for whether the subscriber or site performs the operation. It should be noted that end-to-end encryption is only performed in subscriber (or console) units, not in the site.



Figure 3, LLE of Voice Frames

Each voice frame SHALL be encrypted as follows, or by any method that produces equivalent results:

1. X, the end-to-end encrypted (e.g., V’) or unencrypted (e.g., V) information elements of the voice frame, SHALL be packed into 7 octets (P) as illustrated in Figure 4. This is the same octet packing that is employed for end-to-end encryption in Table 5-7 of ref. (2).
2. Having previously initialized the encryption scheme, the packed voice frame (P) SHALL be encrypted with the next 7 octets of key stream, i.e.,:

P' = CtrEncrypt(P,7).

1. The resulting encrypted vector P' SHALL be unpacked, producing Y, which SHALL replace the original information elements (X, e.g., V’ or V) for further voice processing (i.e., Voice FEC). The 7 initially null bits in octet 6 are discarded.



Figure 4 , Voice Frame Packing for LLE

### LLE of End-to-End Encryption Sync Signaling

The information content of the (end-to-end) Encryption Synchronization Signaling (ESS), i.e., the end-to-end cryptosync, comprises an 8-bit Algorithm ID (ALGID), a 16- bit Key ID (KID), and a 72-bit Message Indicator (MI), which are transmitted in the ESS-B field of the 4V Bursts. The ESS-A field of the 2V bursts carries FEC for the ESS field, and is not link layer encrypted.



Figure 5, LLE of ESS

Figure 5 illustrates the processing of the end-to-end cryptosync to produce ESS-B and ESS-A. In the absence of link layer encryption, the algorithm ID and Key ID are partitioned into hexbits and inserted into ESS-B1. Likewise, subsets of the MI are partitioned into hexbits and inserted into ESS-B2, ESS-B3, and ESS-B4, respectively. FEC is subsequently computed and inserted into ESS-A(1 and 2).

When LLE is employed, the cryptosync is packed into four groups of three octets, each of which is encrypted, and subsequently unpacked to produce encrypted versions of the subfields. The encrypted subfields are then partitioned into hexbits, and FEC is subsequently computed on these encrypted versions of the subfields.

Figure 6, Figure 7, Figure 8, and Figure 9 illustrate the packing of the cryptosync into octets for Link Layer Encryption.



Figure 6 , Packing for ESS-B1



Figure 7 , Packing for ESS-B2



Figure 8 , Packing for ESS-B3



Figure 9 , Packing for ESS-B4

Each 24-bit portion (B) of the cryptosync SHALL be encrypted as follows, or by any method that produces equivalent results:

1. The information elements of the subfield SHALL be packed into 3 octets (S) as illustrated in Figure 6 through Figure 9.
2. Having previously initialized the encryption scheme, the packed subfield (S) SHALL be encrypted with the next 3 octets of key stream, i.e.,:

S' = CtrEncrypt(S,3).

1. The resulting encrypted vector S' SHALL be unpacked via the inverse of the packing function and the resulting 24-bit vector (B') SHALL replace the original information B for further processing (i.e., hexbit partitioning and FEC).

## LLE of Bursts Containing Signaling (Data, Control)

Bursts containing signaling (FACCH and SACCH bursts) are secured by encrypting the MAC PDU carried in the signaling burst. Each MAC PDU contains a "P" (Protected) bit that is used to identify whether the PDU is encrypted.

MAC PDUs SHALL be encrypted in accordance with the following subsections when carrying MAC messages associated with protected groups, individuals, or services. When a TDMA voice channel is assigned for an unprotected voice service, it shall not carry any MAC messages associated with protected groups, individuals or services. When a TDMA voice channel is assigned for a protected voice services, all MAC PDUs carrying MAC messages shall be protected.

#### LL Encrypted MAC PDU Format

Figure 10 and Figure 11 illustrate the MAC PDU formats. The "P" bit of the first octet is used to indicate the protected status of the entire PDU. The shaded areas in the figures identifies the encrypted content of the PDU. Except when the Opcode indicates that the PDU is a MAC\_END\_PDU, octets 1 through 20 of the MAC PDU are encrypted. For MAC\_END PDUs, octets 1 and 2, containing the color code, are not encrypted.



Figure , MAC PDU Formats

The fields of the MAC PDU are defined as follows:

P: Protected bit. The P bit is never encrypted.

0 if the PDU is not protected by LLE,

1 if the PDU is protected by LLE.

R: Reserved, always 0. The R bit is never encrypted.

Offset: See (1), section 8.4.2. The offset field is never encrypted.

Opcode: See (1), section 8.4.1. The opcode field is never encrypted.

MAC PDU Contents: Varies per Opcode. Encrypted via LLE if P = 1.

(Inverted) CRC-12: See (1). The CRC for TDMA LLE is the one’s compliment of the CC described in See (1). The CRC is never encrypted.

(Inverted) CRC-16: See (7). The CRC for TDMA LLE is the one’s compliment of the CC described in See (7). The CRC is never encrypted.

Figure 10 supersedes figures 8-2 and 8-3 of ref. (1). Likewise, the definitions of R and P supplant the *Res* fields in figures 8-1, and 8-4 through 8-10 of ref. (1).



Figure , IECI and OECI MAC PDUs

#### LLE of a MAC PDU

When a MAC PDU is to be protected, the PDU SHALL be encrypted as follows, or by any method that produces equivalent results:

Let K be the STEK of the TDMA channel per ref. (3);

Let L be the length of the MAC PDU contents (e.g., 18 or 21 octets);

Let M be the MAC PDU contents, an octet array of length L;

Compute M' as follows:

1. Construct the LLEIV per section 2.2.4.
2. Compute IV per section 2.2.3.
3. Initialize counter mode encryption, i.e., CtrInit(K,IV).
4. Compute M' = CtrEncrypt(M,L).
5. If the PDU is the MAC\_END PDU, set M’{0..1} = M{0..1}.
6. Substitute M' for M in all subsequent processing, and set the "P" bit of the MAC PDU prior to transmission.

When, upon receipt of a MAC PDU, the "P" bit of a MAC PDU is set, and following verification of the CRC, the PDU SHALL be decrypted by the receiver as follows or by any method that produces equivalent results:

Let K be the STEK of the TDMA channel per ref. (3);

Let L = the length of the MAC PDU in octets ( (e.g., 18 or 21 octets);

Let M' encrypted MAC PDU contents, of length L octets; then,

Compute M, the decrypted MAC PDU, as follows:

1. Construct the LLEIV per section 2.2.4.
2. Compute the IV per section 2.2.3.
3. Initialize counter mode encryption, i.e., CtrInit(K,IV).
4. Compute M = CtrEncrypt(M',L).
5. Substitute M for M' in all subsequent processing.

The null field of the Null Information MAC message that is used to fill empty space in MAC PDUs shall be filled with a cryptographically sound pseudo-random number per ref. (7).

# Required Site Procedures

## Broadcast OSPs for LLE

An RFSS with TDMA working channels synchronized to the FDMA control channel as described in (1) SHALL send SYNC\_BCST on the control channel with a maximum periodicity of 3 seconds.

# Information Elements

## DUID Encoding

Table 7 summarizes the meaning of the DUID information bits for TDMA channels. This table supersedes Table 5-3 in ref. (1). Note that scrambling with LLE follows the normal TDMA rules.

Table , DUID Information Bits

|  |  |  |
| --- | --- | --- |
| DUID Information Bits | Burst | Burst Types |
| 3 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | 4V Burst | Inbound 4V, Outbound 4V |
| 0 | 0 | 0 | 1 | Reserved |  |
| 0 | 0 | 1 | 0 | LLE 4V Burst | Inbound 4V, Outbound 4V |
| 0 | 0 | 1 | 1 | SACCH Burst with scrambling | IEMI, I-OEMI |
| 0 | 1 | 0 | 0 | LCCH with scrambling | IECI |
| 0 | 1 | 0 | 1 | Reserved |  |
| 0 | 1 | 1 | 0 | 2V Burst | Inbound 2V, Outbound 2V |
| 0 | 1 | 1 | 1 | LLE 2V Burst | Inbound 2V, Outbound 2V |
| 1 | 0 | 0 | 0 | Reserved |  |
| 1 | 0 | 0 | 1 | FACCH Burst with scrambling | IEMI, S-OEMI |
| 1 | 0 | 1 | 0 | Reserved |  |
| 1 | 0 | 1 | 1 | Reserved |  |
| 1 | 1 | 0 | 0 | SACCH Burst w/o scrambling | IEMI, I-OEMI |
| 1 | 1 | 0 | 1 | LCCH without scrambling | IECI, OECI |
| 1 | 1 | 1 | 0 | Reserved |  |
| 1 | 1 | 1 | 1 | FACCH Burst w/o scrambling | IEMI, S-OEMI |

1. The means by which a user or group is designated as "protected" is beyond the scope of this specification. [↑](#footnote-ref-1)
2. Specifics of the encryption, the protected information is defined in later sections of this document. [↑](#footnote-ref-2)