**APIC Encryption Task Group**

|  |  |
| --- | --- |
| Document Number: | ETG-16-049-R17 |
| Title: | Link Layer Encryption Overview |
| Editor: | Thomas A. Hengeveld, Harris Corporation |
| Date: | 2018-02-02 |
| Print Date: | 2018-02-06 |
| Abstract: | This document is a proposal for a TIA Standard regulating Link Layer Security for TIA-102 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

Link Layer Encryption Overview

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](#_Toc505701273)

[Trademark Identification i](#_Toc505701274)

[1 Introduction 1](#_Toc505701275)

[1.1 Open Issues in this Revision (Delete before publication) 1](#_Toc505701276)

[1.2 Scope 2](#_Toc505701277)

[1.3 Abbreviations 3](#_Toc505701278)

[1.4 Definitions 7](#_Toc505701279)

[1.5 References 8](#_Toc505701280)

[2 Overview 10](#_Toc505701281)

[2.1 High-Level Overview 10](#_Toc505701282)

[2.2 LLE Keys 19](#_Toc505701283)

[2.3 Crypto-Synchronization 22](#_Toc505701284)

[2.4 Affected Interfaces 24](#_Toc505701285)

[2.5 Operational Overview 26](#_Toc505701286)

[2.5.1 Trunking Operational Description 26](#_Toc505701287)

[2.5.1.1 Trunking Key Selection and Time Synchronization 26](#_Toc505701288)

[2.5.1.2 Mobility Management 26](#_Toc505701289)

[2.5.1.2.1 Full Registration 26](#_Toc505701290)

[2.5.1.2.1.1 Mixed Mode Operation 28](#_Toc505701291)

[2.5.1.2.2 Location Registration 29](#_Toc505701292)

[2.5.1.2.2.1 Mixed Mode Operation 29](#_Toc505701293)

[2.5.1.3 Group Voice Services 30](#_Toc505701294)

[2.5.1.4 Individual Voice Services 31](#_Toc505701295)

[2.5.1.5 Supplementary Services 35](#_Toc505701296)

[2.5.1.6 Data Services 35](#_Toc505701297)

[2.5.2 Direct and Repeated Mode Conventional Operations 38](#_Toc505701298)

[2.5.2.1 Key selection and time synchronization 38](#_Toc505701299)

[2.5.2.2 Voice, Data and Supplementary Services 38](#_Toc505701300)

[2.5.2.3 Mixed Mode Operation 39](#_Toc505701301)

[2.5.3 CFN Conventional Operations 39](#_Toc505701302)

[2.5.3.1 Key selection and time synchronization 39](#_Toc505701303)

[2.5.3.2 Voice and Supplementary Services with explicit synchronization 39](#_Toc505701304)

[2.5.3.3 Data operation with implicit synchronization 40](#_Toc505701305)

[3 LLE Cryptographic Overview and Critical Information Elements 42](#_Toc505701306)

[3.1 Cryptographic Overview 42](#_Toc505701307)

[3.1.1 Nomenclature 42](#_Toc505701308)

[3.1.2 Zero Padding 42](#_Toc505701309)

[3.1.3 LL Encryption Scheme 43](#_Toc505701310)

[3.1.4 Message Authentication 45](#_Toc505701311)

[3.1.5 Key Derivation 47](#_Toc505701312)

[3.1.6 Key Wrapping 48](#_Toc505701313)

[3.2 Link Layer Encryption Information Elements 49](#_Toc505701314)

[3.2.1 LLE Domain Identifier (LDID) 49](#_Toc505701315)

[3.2.2 LLE Key Type (LKT) 49](#_Toc505701316)

[3.2.3 LLE Security Suite Identifier (LALG) 49](#_Toc505701317)

[3.2.4 Common Link Encryption Key (CLEK) 50](#_Toc505701318)

[3.2.5 CLEK Update Parameter (ULLE) 50](#_Toc505701319)

[3.2.6 Common Link Encryption Key ID (CKID) 50](#_Toc505701320)

[3.2.7 Root Link Encryption Key (RLEK) 50](#_Toc505701321)

[3.2.8 Root Link Encryption Key ID (RKID) 50](#_Toc505701322)

[3.3 Operational Keys 50](#_Toc505701323)

[3.3.1 Site Traffic Encryption Key (STEK) 50](#_Toc505701324)

[3.3.2 Site Traffic Authentication Key (STAK) 51](#_Toc505701325)

[3.4 Common Data Elements 52](#_Toc505701326)

[3.4.1 LLE Initial Vector (LLEIV) 52](#_Toc505701327)

[3.4.2 LLE Source Indicator (SI) 53](#_Toc505701328)

[4 Key Management for Link Layer Encryption 54](#_Toc505701329)

[4.1 Key Management Information Elements 55](#_Toc505701330)

[4.1.1 Broadcast Rekeying Information Elements 55](#_Toc505701331)

[4.1.1.1 Common Key Encryption Key (CKEK) 56](#_Toc505701332)

[4.1.1.2 Common Message Authentication Key (CMAK) 56](#_Toc505701333)

[4.1.1.3 Root Key Encryption Key (RKEK) 56](#_Toc505701334)

[4.1.1.4 Root Message Authentication Key (RMAK) 56](#_Toc505701335)

[4.1.2 Individual Key Management Information Elements 56](#_Toc505701336)

[4.1.2.1 Individual Link Encryption Key (ILEK) 56](#_Toc505701337)

[4.1.2.2 Individual LLE Key Security Parameter (IKSP) 57](#_Toc505701338)

[4.1.2.3 Individual LLE Key Derivation Seed (SI) 58](#_Toc505701339)

[4.1.2.4 Individual LLE Credential (CI) 58](#_Toc505701340)

[4.1.2.5 Individual Key Encryption Key (IKEK) 58](#_Toc505701341)

[4.1.2.6 Individual Message Authentication Key (IMAK) 58](#_Toc505701342)

[4.1.3 Group Rekeying Information Elements 58](#_Toc505701343)

[4.1.3.1 LLE Group Key (GLEK) 58](#_Toc505701344)

[4.1.3.2 LLE Group Key Identifier (GKID) 58](#_Toc505701345)

[4.1.3.3 LLE Group Identifier (LGID) 58](#_Toc505701346)

[4.1.3.4 LLE Group Key Encryption Key (GKEK) 59](#_Toc505701347)

[4.1.3.5 LLE Group Key Message Authentication Key (GMAK) 59](#_Toc505701348)

[4.1.4 Zeroization Information Elements 60](#_Toc505701349)

[4.1.4.1 Zeroization Key Scope 60](#_Toc505701350)

[4.2 Key Management Architecture and Use Cases 61](#_Toc505701351)

[4.2.1 Key Management Architecture 61](#_Toc505701352)

[4.2.1.1 Distribution of RLEKs and CLEKs 62](#_Toc505701353)

[4.2.1.2 ILEK Management in Conventional Systems 64](#_Toc505701354)

[4.2.1.3 ILEK Management in Trunked System 65](#_Toc505701355)

[4.2.2 LLE Key Provisioning and Management Scenarios 66](#_Toc505701356)

[4.2.2.1 Preparing infrastructure for LLE 66](#_Toc505701357)

[4.2.2.2 SU Enablement in Trunking Systems 66](#_Toc505701358)

[4.2.2.3 SU Enablement in Conventional Systems 68](#_Toc505701359)

[4.2.2.4 Periodic Key Refresh 69](#_Toc505701360)

[4.2.2.5 Key Compromise 69](#_Toc505701361)

[4.2.2.6 Key Zeroization Scenarios 70](#_Toc505701362)

[4.3 Key Distribution by KFD and OTAR 72](#_Toc505701363)

[4.3.1 LLE Key Distribution via Key Fill Device 72](#_Toc505701364)

[4.3.2 LLE Key Distribution via OTAR 72](#_Toc505701365)

[4.4 Broadcast Key Distribution 73](#_Toc505701366)

[4.4.1 Broadcast Key Derivations 74](#_Toc505701367)

[4.4.2 Key Determination 74](#_Toc505701368)

[4.4.3 Future Key Request 75](#_Toc505701369)

[4.4.4 Key Survey 75](#_Toc505701370)

[4.4.5 Key Broadcast Message Construction 75](#_Toc505701371)

[4.5 Individual Key Distribution 79](#_Toc505701372)

[4.5.1 Distribution of LLE keys via IKD 79](#_Toc505701373)

[4.5.2 Individual Key Derivations 80](#_Toc505701374)

[4.5.3 Individual Key Distribution Message Security 81](#_Toc505701375)

[4.5.4 ILEK Sharing 84](#_Toc505701376)

[4.6 Group Key Distribution 85](#_Toc505701377)

[4.6.1 Group Key Derivations 85](#_Toc505701378)

[4.6.2 Group Key Distribution Description 86](#_Toc505701379)

[4.6.3 Group Key Message Security 86](#_Toc505701380)

[4.6.4 Management of Group Membership and Keys 89](#_Toc505701381)

[4.7 Key Zeroization 92](#_Toc505701382)

[4.7.1 Zeroization using OTAR/Key-Fill Techniques 92](#_Toc505701383)

[4.7.2 Zeroization of LLE keys by an LEF 92](#_Toc505701384)

[4.7.3 Construction of Zeroization Messages 92](#_Toc505701385)

[5 Example Cryptographic Operations 94](#_Toc505701386)

LIST OF TABLES

[Table 1, LLS Applicability by System Type 10](#_Toc505701387)

[Table 2, TIA-102 Channel Type Summary and Content 14](#_Toc505701388)

[Table 3, Affected Standardized Interfaces (To Be Revised) 24](#_Toc505701389)

[Table 4, New Standards (To Be Revised) 24](#_Toc505701390)

[Table 5, Affected Standards 25](#_Toc505701391)

[Table 6, LLE Key Type Values 49](#_Toc505701392)

[Table 7, LALG Values 49](#_Toc505701393)

[Table 8, Source Indicator 53](#_Toc505701394)

[Table 9, Key Management Methods applicable to each Key LLE Type 54](#_Toc505701395)

[Table 10, Zeroization Key Scope Values 60](#_Toc505701396)

LIST OF FIGURES

[Figure 1, Comparison of LLE and E2E Encryption (Trunking) 11](#_Toc505701397)

[Figure 2, Comparison of LLE and E2E Encryption (Conventional) 12](#_Toc505701398)

[Figure 3, Air Interface Modes 15](#_Toc505701399)

[Figure 4, LLE in Trunking Sites and CFN Repeaters 18](#_Toc505701400)

[Figure 5, LLE in Direct Mode and Transparent Repeaters 19](#_Toc505701401)

[Figure 6, LLE Key Distribution Concept 20](#_Toc505701402)

[Figure 7, LLE Key Derivation 21](#_Toc505701403)

[Figure 8, LLE Full Registration 28](#_Toc505701404)

[Figure 9, LLE Location Registration 29](#_Toc505701405)

[Figure 10, Protection of Group Voice Services (Trunking) 30](#_Toc505701406)

[Figure 11, Protection of Individual Call without Availability Check 32](#_Toc505701407)

[Figure 12, Protection of Individual Call with Availability Check 34](#_Toc505701408)

[Figure 13, Individual Data Service Site Configurations 36](#_Toc505701409)

[Figure 14, Counter Mode Encryption for Link Layer Encryption 43](#_Toc505701410)

[Figure 15, Message Authentication for LLE 45](#_Toc505701411)

[Figure 16, Key Derivation for LLE 47](#_Toc505701412)

[Figure 17, Key Wrapping for LLE 48](#_Toc505701413)

[Figure 18, Common Link Encryption ID (CKID) 50](#_Toc505701414)

[Figure 19, LLE Initial Vector 52](#_Toc505701415)

[Figure 20, Relationships of Broadcast Key Distribution Information Elements 55](#_Toc505701416)

[Figure 21, Relationships of IKD Information Elements 57](#_Toc505701417)

[Figure 22, Relationships of Group Rekeying Information Elements 59](#_Toc505701418)

[Figure 23, Interfaces for RLEK and CLEK Distribution 62](#_Toc505701419)

[Figure 24, ILEK Management interfaces in CFN Systems 64](#_Toc505701420)

[Figure 25, ILEK Management Interfaces in Trunked RFSS 65](#_Toc505701421)

[Figure 26, “Home” SU Enablement 67](#_Toc505701422)

[Figure 27, “Visiting” SU Enablement 67](#_Toc505701423)

[Figure 28, CFN SU Enablement 68](#_Toc505701424)

[Figure 29, KFD Based Key Distribution 72](#_Toc505701425)

[Figure 30, OTAR LLE Key Distribution 72](#_Toc505701426)

[Figure 31, Broadcast Key Distribution 73](#_Toc505701427)

[Figure 32, Broadcast Key Derivation 74](#_Toc505701428)

[Figure 33, Broadcast Distribution Security 77](#_Toc505701429)

[Figure 34, High-Level Flow for Conventional Individual Key Distribution 79](#_Toc505701430)

[Figure 35, High-Level Flow for Trunking Individual Key Distribution 80](#_Toc505701431)

[Figure 36, Individual Distribution Key Derivation 81](#_Toc505701432)

[Figure 37, Individual Distribution Security 83](#_Toc505701433)

[Figure 38, Group Key Derivations 86](#_Toc505701434)

[Figure 39, Group Distribution Security 88](#_Toc505701435)

[Figure 40, High Level Flow for Group Key Inventory and Management 90](#_Toc505701436)

[Figure 41, Inventory Summary 91](#_Toc505701437)

[Figure 42, Key Zeroization Message Protection 93](#_Toc505701438)

DOCUMENT REVISION HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| R17 | 2-Feb-2018 | Added KFD to means to share credentials without ISSI. |
| R16 | 30-Jan-2018 | Incorporated Group Key Management section, accepted all changes, deleted all comments. |
| R15 | 29-Jan-2018 | Working version from conference call. |
| R14 | 29-Dec-2017 | Released Draft with Zeroization Updates. Lots of editorial changes (spelling and grammer check) with change tracking turned off. Also see comment matrix R11. |
| R13 | N/A | Working Draft with Zeroization Changes |
| R12 | 09-Jan-2017 | Accepted all changes. |
| R11 | 09-Jan-2017 | Change Tracked Draft. |
| R10 | 05-Jan-2017 | Draft Changes for Zeroization |
| R09 | 29-Nov-2016 | Clean copy with all changes to date. |

# Introduction

This document provides an overview of TIA-102 Link Layer Encryption (LLE). LLE is applicable to all types of TIA-102 air interfaces, and provides confidentiality and replay protection. LLE is not a substitute for end-to-end encryption that is separately specified in TIA-102.AAAD-A (ref. (1)).

## Open Issues in this Revision (Delete before publication)

The following technical issues, previously captured in editor’s notes, need to be resolved prior to publication (new):

1. Number of bits in the LLE Key Type (section 3.2.2) and Security Suite (section 3.2.3)
2. Sizes of GKID (section 4.1.3.2) and LGID (section 4.1.3.3) are to be finalized later.

Other editorial issues continue to be captured throughout the document with editor’s notes.

## Scope

Editor’s Note: TR8 should determine the status (standard vs TSB) of this document and revise this section as necessary prior to publication.

The scope of this addendum to the TIA-102.AAAB-A Digital Land Mobile Radio – Security Services Overview (ref. (2)) is an overview of link layer security for TIA-102 systems. Link layer security applies encryption to fields of sensitive data transmitted over the air interface to protect the data from interception and interpretation by unauthorized receivers. The sensitive data that is to be encrypted on the air interface includes user data traffic, digital voice, control signals that affect calls, and data signals that affect RF subsystem 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 (or another channel) for any unauthorized purpose.

This addendum includes:

* A high-level overview of the standard including a statement of purpose, and identification of the standardized interfaces affected by Link Layer Encryption (Section 2);
* A cryptographic overview and information elements for LLE Key management, and of key data items that are common to a multiplicity of the implementing standards (Section 3);
* A description of LLE Key Management (Section 4); and,
* Example cryptographic results corresponding to various LLE operations (Section 5).

## Abbreviations

||: Concatenation Operator

AES: Advanced Encryption Standard

ANSI: American National Standards Institute

APIC: APCO/P25 Interface Committee

CAI: Common Air Interface

CCH: Control Channel

CFN: Conventional Fixed Network

CFNC: Conventional Fixed Network Channel

CFNS: Conventional Fixed Network Station

CI: Individual LLE Credential

CKEK: Common Key Encryption Key

CKID: Common Link Encryption Key ID

CLEK: Common Link Encryption Key

CMAC: Cipher based message Authentication Code

CMAK: Common Message Authentication key

CONOPS: Concept of Operations

CtrEncrypt: Counter mode encryption encrypting or decrypting function (see section 3.1)

CtrInit: Counter Mode Encryption Initialization Function (see section 3.1)

E2E: End-to-end (as in E2E encryption)

Ef:Project 25 fixed station interface reference designator

FDMA: Frequency Division Multiplexing

FNC: Fixed Network Channel

FNE: Fixed Network Equipment

G: Project 25 inter-RF subsystem interface reference designator

GKEK: LLE Group Key Encryption Key

GKID: Group LLE Key Identifier

GLEK: Group LL Encryption Key

GMAK: Group LLE Key Message Authentication Key

GPS: Global Positioning System

HDU: Header Data Unit

HMAC: Hashed Message Authentication Code

ID: Identifier

IKD: Individual Key Distribution

IKEK: Individual Key Encryption Key

IKI: Inter-KMF Interface

IKSP: Individual LLE Key Security Parameter

ILEK: Individual Link Encryption Key

IMAK: Individual Message Authentication Key

ISP: Inbound Signaling Packet

ISSI: Inter-RF SubSystem Interface

IV: Initial Vector

KDF: Key Derivation Function (see section 3.1)

KFD: Keyfill Device

KMF: Key Management Facility

LALG: LLE Security Suite Identifier

LDID: LLE Domain Identifier

LDIDC: Conventional LDID

LDIDT: Trunking LDID

LDU: Logical Data Unit

LEF: Link Encryption Facility

LGID: LLE Group Identifier

LIRP: LLE Individual Reception Policy

LKT: LLE Key Type

LL: Link Layer

LLA: Link Layer Authentication

LLE: Link Layer Encryption

LLEIV: LLE Initial Vector

LSB: Least Significant Bit

L-SU: Legacy SU

MAC: Medium Access Control (e.g., the MAC layer of the phase 1 or 2 air interface)

Mac: Message authentication consolidated function (see section 3.1)

MacContinue: Message authentication computation function (see section 3.1)

MacFinish: Message authentication finalization function (see section 3.1)

MacInit: Message authentication initialization function (see section 3.1)

MBT: Multiple Block Trunking

MSB: Most Significant Bit

N/A: Not Applicable

NAC: Network Access Code

NIST: National Institute of Standards and Technology

Nx: An unsigned integer of length x bits

OSP: Outbound Signaling Packet

OTAR: Over-The-Air Rekeying

PDU: Protocol Data Unit

P-Group: Protected Group

PO: Protected Only

P-SU: Protected SU

RF Subsystem: Project 25 RF Subsystem (RFSS)

RFSS: RF Subsystem

RKEK: Root Key Encryption Key

RKID: Root Link Encryption Key ID

RLEK: Root Link Encryption Key

RMAK: Root Message Authentication Key

SI: Individual LLE Key Derivation seed

SI: LLE Source Indicator

STAK: Site LL Authentication Key

STEK: Site Link Layer Traffic Encryption Key

SU: Subscriber Unit

SUID: Subscriber Unit ID

TBD: To Be Determined

TCH: Traffic Channel

TDMA: Time Division Multiplexing

TSBK: Trunking Signaling Blocks

UA: Unprotected Allowed

U-Group: Unprotected Group

ULLE: CLEK Update Parameter

Um:Project 25 phase 1 air interface reference designator

Um2: Project 25 phase 2 air interface reference designator

Unwrap: Key Unwrapping Function (see section 3.1)

U-SU: Unprotected SU

UTC: Universal Time Coordinate

WACN: Wide Area Communication Network, usually referring to the 20-bit identifier of a P25 WACN.

Wrap: Key Wrapping Function (see section 3.1)

ZPAD: Zero padding function (see section 3.1)

ZS Zeroization Scope (see section **Error! Reference source not found.**)

Zx: An signed integer of length x bits

## Definitions

The following definitions apply to specific terms in the text that require clarification. Some cryptographic terminology is taken from ref. (3).

Ciphertext: Data in its encrypted form.

Conventional Fixed Network Channel:

A conventional station that can repeat traffic, or relay traffic between SU and fixed network infrastructure.

Crypto-Synch: Information that is either carried in a communications channel, or derived from a communications channel, that is used to create an initial vector for crypto-graphic operations.

Downlink: A TIA-102 communications channel in which information is transmitted by a infrastructure (e.g., by a trunking site or conventional fixed station ) and received by SU.

Initial Vector: Information required to prime certain encryption schemes, including those used herein (aka, Initialization Vector).

Initialization Vector: Initial Vector

Keystream: Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce keys.

LLE Domain: A key management and encryption domain for LLE. Entities in the same LLE domain use the same root keys for link layer encryption. In trunked systems, an LLE Domain equates to the system (i.e., it is identified by the (WACN,System) ordered pair). In conventional, domains are identified by an arbitrary string.

Plaintext: Unencrypted Information.

Transparent Repeater: A conventional repeater that is transparent to SU in that it performs minimal processing on the uplink before repeating it on the downlink. In particular, transparent repeaters do not participate in cryptographic functions related to link layer security.

Uplink: A TIA-102 communications channel in which information is transmitted by an SU and received by infrastructure, e.g., by a trunking site or conventional fixed station.

## References

Editor’s Note:

For convenience during the development of this document, the Word “Citations and Bibliography” function has been used to generate the following list of references. This tool does not provide a means of generating separate lists. TR8 needs to sort and update this section prior to publication, separating the informative and normative references as desired.

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.

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

2. *Digital Land Mobile Radio Security Services Overview.* **TIA.** s.l. : http://tiaonline.org/standards, January 2005. (INFORMATIVE). TIA-102.AAAB-A.

3. **Committee on National Security Systems.** *National Information Assurance Glossary.* 2010. (INFORMATIVE). CNSSI No. 4009.

4. *Digital Land Mobile Link Layer Authentication.* **TIA.** s.l. : http://tiaonline.org/standards, April 2011. (INFORMATIVE). TIA-102.AACE-A.

5. *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.

6. *The Advanced Encryption Standard (AES).* **U.S. Department of Commerce, National Institute of Standards and Technology.** November 26, 2001. (NORMATIVE). FIPS-PUB-197.

7. *The Keyed-Hash Message Authentication Code (HMAC).* **s.l. : National Institute of Standards and Technology, July 2008. (NORMATIVE). FIPS-198-1.**

**8. *Recommendation for Key Derivation Using Pseudorandom Functions.* Chen, Lilly. s.l. : National Institute of Standards and Technology, October 2009. (NORMATIVE). SP800-108.**

**9. *Secure Hash Standard.* s.l. : National Institute of Standards and Technology, March 2012. (NORMATIVE). FIPS-180-4.**

**10. *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.* Dworkin, Morris. s.l. : National Institute of Standards and Technology, December 2012. (NORMATIVE). SP800-38F.**

**11. *KMF to KMF Interface.* TIA. s.l. : http://tiaonline.org/standards, April 2012. (INFORMATIVE). TIA102.BAKA.**

**12. *Key Fill Device (KFD) Interface Protocol Addendum 2: Key Fill for Link Layer Encryption.* TIA. s.l. : http://tiaonline.org/standards, Month Year. (INFORMATIVE). TIA-102.AACD-A-2.**

**13. *Key Fill Device (KFD) Interface Protocol.* TIA. s.l. : http://tiaonline.org/standards, September 2014. (INFORMATIVE). TIA-102.AACD-A.**

**14. *Digital Radio Over-the-Air Rekeying (OTAR) Protocol.* TIA. April 2001. (INFORMATIVE). TIA/EIA-102.AACA.**

**15. *TIA-102 ControL Channel Messages.* TIA. April 2015. (INFORMATIVE). TSB-102-AABC-D.**

# Overview

## High-Level Overview

This standard provides an overview of TIA-102 Link Layer Encryption (LLE). Link Layer Encryption provides protection for information being exchanged between air-interface peers, i.e., between TIA-102 SU and TIA-102 RFSSs, and between TIA-102 SU communicating in simplex mode or through a transparent (simple) repeater. As a side effect of the cryptographic methods used, LLE also provides protection from replay of recorded messages, and protection against certain types of spoofing.

The degree of protection afforded by LLE should not be confused with the protection afforded by End-to-End encryption (described in ref. (1) and related specifications). As shown in Figure 1 for trunking and Figure 2 for conventional, whereas End-to-End encryption provides security for communications between SU without regard for intervening wired or wireless interfaces, LLE only provides protection on a particular air interface. Intervening transport networks (e.g., transport networks connecting a fixed station to RFSS infrastructure or within a site or fixed station) are not protected by LLE. Also, whereas with End-to-End encryption, keys are typically generated with a high degree of cryptographic separation between different keys, all of the LLE keys within a domain are derived from a common ancestor key using cryptographically sound methods.

LLE is designed to be compliant with relevant NIST SP-800 series documents for encryption, message authentication, and key derivation in force as of the date of publication.

Table 1 notes the applicability of LLE to the various system and channel types defined by the TIA-102 standards. For reference, the applicability of Link Layer Authentication (LLA, see ref. (4)) to each system and channel type is also reflected in the table, in which the following abbreviations apply:

* S – Supported;
* T – Supported through transparent repeat of uplink to downlink without active participation by the repeater;
* N/A – Not Applicable; and,
* x – Not supported by the standard.

Table 1, LLS Applicability by System Type

|  |  |  |  |
| --- | --- | --- | --- |
| System Type | Mode/Channel Type | LLA | LLE |
| Trunked | Control Channel (CCH) | S | S |
| FDMA Traffic Channel (TCH) | N/A | S |
| TDMA Traffic Channels | N/A | S |
| Conventional | Direct Mode | x | S |
| Repeated (Simple) | x | T |
| Repeated (Fixed Network (FN)) | x | S |



Figure 1, Comparison of LLE and E2E Encryption (Trunking)



Figure , Comparison of LLE and E2E Encryption (Conventional)

Link Layer Encryption can be applied to all TIA-102 over-the-air channel types and information flows. Figure 3 illustrates the four architectures defined by the TIA-102 standards:

* Trunking (including Control Channels, FDMA Voice and Data Traffic Channels and TDMA Voice Traffic Channels): Trunking Sites comprise a trunking control channel and one or more traffic channels, which may be FDMA or TDMA traffic channels.
* Conventional Direct Mode: Direct mode provides simplex communications between geographically proximate Subscriber Units (SU) on the same radio channel. Information exchanged may be voice, data or control signaling.
* Conventional Repeat (Simple) Mode (aka Transparent Repeated mode): In Transparent Repeated mode, a fixed station “repeats” received information from SU to other SU dwelling on a paired radio channel without injecting additional content or modifying the received content. Information exchanged may be voice, data or control signaling.
* Conventional Fixed Network mode: In Conventional Fixed Network mode, Conventional Fixed Network Stations (CFNS) are interconnected through infrastructure, allowing information to flow between geographically distant SU. In Conventional Fixed Network mode, a fixed station “repeats” received information from SU to other SU dwelling on a paired radio channel and may inject additional content or modify the received content before retransmission. In this configuration, a fixed station may also transmit information from a data host, a dispatch console or another CFNS.

Any channel type can support either protected or unprotected traffic. Several types of SU need to be considered:

* Protected SU (P-SU) are those that that are aware of messages associated with LLE operation AND have the capability of operating with or without LLE protection, and are authorized to operate with LLE in a particular domain.
* Unprotected SU (U-SU) are those that are aware of messages associated with LLE operation AND DO NOT have the capability of operating with LLE protection (e.g., are not authorized for a particular domain).
* Legacy SU (L-SU) are SU that are not aware of messages associated with LLE operation AND are not capable of operating with LLE protection.
* Each channel type can carry one or more information flows, comprising Voice, (User) Data, Trunking Control Messages, and Conventional Control Messages.

Table 2 summarizes the applicability of each information flow to each channel type. Within the table, the following abbreviations apply:

* S – Supported;
* T – Supported through transparent repeat of uplink to downlink without active participation by the repeater; and,
* N/A – Not Applicable.

Table , TIA-102 Channel Type Summary and Content

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Channel Type | Information Flows | | | |
| Voice | Packet  Data | Trunking Control Messages | Conventional Control Messages |
| Trunking Control Channel | N/A | N/A | S | N/A |
| Trunking FDMA Traffic Channel | S | S | S | N/A |
| TDMA Traffic Channel | S | N/A | S[[1]](#footnote-1) | N/A |
| Conventional: Direct Configuration | S | S | N/A | S |
| Conventional: Transparent Configuration | T | T | N/A | T |
| Conventional: Fixed Network Configuration | S | S | N/A | S |



Figure , Air Interface Modes

LLE is applied at Layer 2 as follows:

* Control Channels: Control Channels carry Inbound Signaling Packets (ISPs) and Outbound Signaling Packets (OSPs) via Trunking Signaling Blocks (TSBKs) or Multiple Block Trunking Packets (MBTs).
  + TSBKs: TSBKs are LL encrypted depending on their content (e.g., ISP or OSP). Both uplinks and downlinks can contain mixed LL encrypted and unencrypted TSBKs. TSBKs are encrypted with implicit crypto-synchronization.
  + MBTs: MBTs are LL encrypted depending on their content. The control channel uses implicit crypto-sync for LLE, so MBTs on the control channel are encrypted with implicit crypto-synchronization, in contrast to MBTs on Conventional Channels (see below).
* FDMA Common Air Interface Traffic Channels (including FDMA Traffic Channels for Trunking, and all conventional configurations): These channels carry user voice and data, trunking control messaging (in Link Control Words), and conventional control messaging.
  + FDMA voice channels are LL encrypted by using special forms of Header Data Units (HDU), Logical Data Units (LDU1 and LDU2), and TDUs with Link Control (TDU-LC). LLE covers all user information in these data units including end-to-end crypto-synch, digital voice, and link control. Low speed data is not supported coincident with LLE.

LLE crypto-sync is included within the voice header, superframe, and terminator with link control. The normal Terminator Data Unit (without link control) contains no information that requires link layer encryption.

FDMA voice channels are LL encrypted on a transmission by transmission basis, that is, either an entire transmitted talk-spurt is encrypted or not based on security policy; and both LL encrypted and unencrypted transmissions can be arbitrarily interleaved on the same channel.

In a protected call (group or individual), LCs are protected and carry information about either protected or unprotected activity. In an unprotected call (group or individual), LCs are unprotected and do not carry information about protected activity.

* + FDMA data is encrypted on a packet by packet basis, that is, a data packet is encrypted or not based on security policy; and both LL encrypted and unencrypted packets can be arbitrarily interleaved on the same channel. Where possible, FDMA data in trunking systems may use implicit synchronization aligned to the control channel or explicit crypto-sync.
  + Conventional Control: Conventional control can be carried on conventional channels in Trunking Signaling Blocks (TSBKs) or Multi-block Trunking Signaling Packets (MBTs).
    - TSBKs: TSBKs are not link layer encrypted for conventional control. Conventional control messages that require link layer encryption are transmitted in MBTs.
    - MBTs: Unlike MBTs carried on the control channel, MBTs for conventional control are LL encrypted, by prefixing LLE crypto-synch to the MBT data unit. These secure MBT control messages can include radio inhibit and other sensitive control functions that would be sent as a single TSBK if they were not secure.
* 2-Slot TDMA:
  + Voice: Voice carried on the 2-Slot TDMA air interface is LL encrypted by encrypting the voice frames and the end-to-end encryption synchronization carried in 2V and 4V bursts.
  + Data and Control: On 2-Slot TDMA channels, all non-voice information flows are carried in MAC Protocol Data Units (PDUs). Except for the color code contained in MAC\_END PDUs, the entire information content of MAC PDUs is LL encrypted when the TDMA traffic is LL encrypted. MAC PDUs can carry multiple MAC messages. All the messages within any particular MAC PDU are either LL encrypted or not LL encrypted. Protected PDUs can carry information about unprotected services/activities. Unprotected PDUs never carry information about protected services/activities.

For all channel types, unprotected operation is equivalent to the operation of legacy equipment. That is, an unprotected SU can fully interoperate with legacy RFSSs, fixed stations and SU. Likewise, all unprotected information flows from an RFSS or fixed station that supports LLE are fully interoperable with legacy SU.



Figure , LLE in Trunking Sites and CFN Repeaters

Figure 4 illustrates the link layer encryption operations performed at trunking sites and conventional fixed network stations. In the figure, solid black lines represent public (i.e., link layer encrypted private information or other information that does not require link layer encryption) information, red dashed lines represent private information which needs to be protected, and red dotted-dashed lines represent mixed information flows, a portion of which needs protection. The site processing block in the figure represents all the normal processing (i.e., with LLE) that is performed by a site.

SUs LL encrypt private information, combine it with public information in the same information stream, and transmit it to the site. At the site, public information is separated from the encrypted private information, and either forwarded to infrastructure, repeated on the downlink, or both. Meanwhile, encrypted private information is link layer decrypted and then forwarded to the infrastructure, processed by the site itself, or re-encrypted and repeated on the downlink.

For information destined for the air interface downlink, public and private information is received by the site from the infrastructure, or generated internally. Private information is encrypted and combined with encrypted repeated information streams, and with the public information streams for transmission on the downlink.



Figure , LLE in Direct Mode and Transparent Repeaters

Figure 5 illustrates link layer encryption in direct mode, and through transparent repeaters. In these configurations, all the encryption operations occur within the SU.

## LLE Keys

Figure 6 illustrates Link Layer Encryption key distribution. All operational LLE keys within an LLE Domain are derived from a Root LLE Key (RLEK). RLEKs are identified by an RLEK Key ID (RKID).

A Common Link Encryption Key (CLEK) is derived from the RLEK by the application of a public “update parameter” (ULLE) described later. A CLEK is identified by a CKID comprising the RKID of the RLEK from which it was derived, and the update parameter

The RLEK itself is provided by a Link Encryption Facility (LEF), a virtual component that might exist as a standalone entity, or be incorporated into P25 Key Management facilities, for example. Depending on specific system needs, the LEF might develop the RLEK from a cryptographically sound pseudo-random number generator, or receive the key from a “Key Source” that produces appropriately strong keys.



Figure , LLE Key Distribution Concept

The RLEK may be provided to trusted trunking sites and CFNS capable of creating broadcast key management messages (see section 4) and to fully trusted SUs. Fully trusted SUs are those that are expected to operate within the LLE domain for extended periods of time and are used by highly trusted personnel. Note that if an RLEK is compromised or needs to be rotated, the RLEK needs to be changed and subsequently all keys derived from an RLEK also change. The current RLEK is needed by devices participating in broadcast distribution of future RLEKs.

The CLEK may be provided to trusted trunking sites and CFNS capable of creating broadcast key management messages and to less trusted SUs. Less trusted SUs are those that are either not expected to operate within the LLE domain for extended periods of time or that may be considered more susceptible to compromise. The population of less trusted SUs is expected to be significantly less than the population of trusted SUs. Accordingly, the rotation of CLEKs is expected to be more frequent than the rotation of RLEKs. Note that if a CLEK is compromised or to be rotated, the CLEK needs to be changed and subsequently all keys derived from a CLEK also change. The current CLEK is needed by devices participating in broadcast distribution of future CLEKs.

Devices possessing the current CLEK (or the RLEK from which is was derived) may derive the Site Traffic Encryption Key (STEK) and Site Traffic Authentication Key (STAK) once they know appropriate identifying parameters of the site or CFNS from broadcast messaging or programming. Operational keys (STEKs and STAKs) are derived through a second application of the KDF. For these keys, the context is a fixed value, and the K1 (as defined in section 3.1.5) is the resulting STEK, and K2 is the resulting STAK.

Figure 7 illustrates the derivation of operational keys from a CLEK.



Figure , LLE Key Derivation

Between sites in trunking systems using the same CLEK, the construction of the context guarantees that key derivation is globally unique[[2]](#footnote-2), i.e., each site has a unique key. Likewise, the construction guarantees that no conventional channels use the same key as any trunking site. The definition of the IV guarantees that no two trunking channels at the same site use the same key stream.

Within a collection of conventional channels using the same CLEK, no two conventional channels with different NAC codes, or with different downlink frequencies use the same derived traffic key. To avoid potential duplication of keystream, it is incumbent on system administrators to assure that no two conventional channels with the same downlink frequency share the same NAC code.

The STEK and STAK may be provided to Conventional Fixed Stations and trunking sites that are not capable of creating broadcast key management messages. Note that if an STEK/STAK is compromised or to be rotated, the CLEK needs to be changed and subsequently all keys derived from a CLEK also change.

Distribution of LLE operational keys to trunking sites is beyond the scope of the standard. Distribution of keys necessary for LLE operation to Conventional Fixed Stations may use the Conventional Digital Fixed Station Interface. Distribution of keys necessary for LLE operation to trunking SUs occurs using individual, broadcast or group delivery methods described later in this document. These same distribution methods may be used for conventional SUs operating in an LLE domain that includes at least one channel operating in a conventional fixed network configuration. For conventional domains that do not include at least one channel operating in a conventional fixed network configuration, the keys necessary for LLE operation may be delivered using a key fill device or OTAR operating on a channel outside the conventional LLE domain.

Depending on the audience of SU being keyed, key distribution to SU can be performed using OTAR/Key Fill methods, or via Individual Key Distribution, Broadcast Key Distribution, or Group Key Distribution described in section 4. Broadcast key distribution uses keys derived from either the RLEK or CLEK to provide keys to fully trusted or less trusted SU, respectively. Individual Key Distribution uses a unique key associated with each SU to provide keys only to that SU. Group Key Distribution allows SU to be divided into groups, each of which can be separately keyed.

## Crypto-Synchronization

Encryption operations need to include a “crypto-synchronization” (aka “initial vector”) to provide for unique key streams. When the initial vector includes a time element, it can also be used to provide some protection from replay and spoofing attacks, as it allows the receiver to verify that the time of transmission (i.e., the time contained in the synchronization) is within suitable limits.

The 128-bit Link Layer Encryption Initial Vector (LLEIV) comprises the following fields:

1. Channel Frequencies – The downlink frequency (in eighths of kilohertz, 24 bits each) of the channel;
2. Source Indicator – A two-bit field that provides information about the source of the transmission and, in specified circumstances, the content of the time coordinate; and,
3. Time Value – The 40-bit time that the transmission is encrypted. Under certain circumstances, indicated by the Source Indicator, the time coordinate is replaced with a 40-bit random value generated by the transmitter.

The defined portions yield 66 information bits in the IV. The remaining bits are defined to be zero.

For Trunking Control Channels, the downlink frequency is determined prior to using the control channel, while for trunking traffic channels it is obtained from traffic channel assignment OSPs. For conventional channels, the downlink frequency is determined by programing.

The source indicator is implied by the direction of the transmission for the control channel, for trunking FDMA data, and for TDMA traffic channels. It is explicitly carried in all FDMA voice transmissions.

For FDMA voice channels, the time value is explicitly carried in the voice transmission. The time value for trunking control channels and TDMA traffic channels is derived by SU from broadcast messaging from on the control channel. The time value for FDMA trunking data is either derived from the control channel time broadcast or is derived a time coordinate embedded in the data downlink. For FDMA direct and repeated mode conventional data, the time value is explicitly carried in the data transmission. For FDMA CFNS data, the CFNS periodically broadcasts the time, and SU are required to synchronize to that time signal.

## Affected Interfaces

Editor’s Note: The following list of standards and so on may change and will need to be revised prior to publication.

Aspects of link layer encryption affect the TIA-102 standardized interfaces identified in Table 3. New standards developed for link layer security are identified in Table 4.

The impact on existing standards is summarized in Table 5.

Table 3, Affected Standardized Interfaces (To Be Revised)

|  |  |  |
| --- | --- | --- |
| Interface | Designation | Affect |
| 2-slot TDMA Air Interface | Um2 | Encryption of 2-slot TDMA Air Interface. |
| FDMA CAI | Um | Encryption of FDMA Traffic Channel. |
| Fixed Station Interface | Ef | Addition of LLE key management. |
| Inter-Subsystem Interface | G | Addition of information related to key management. |
| Key Fill Device/ LL Encryption Facility | KFD-LLE (New) | Addition of LLE manual key management. |
| Key Fill Device/Mobile Radio | KFD-MR | Addition of LLE manual key management. |
| OTAR Service | N/A | Addition of LLE key management. |
| Trunking Control Channel | Um | Addition of LLE, additional messaging for key management and identification. |

Table 4, New Standards (To Be Revised)

|  |  |  |
| --- | --- | --- |
| Standard Number (TIA-102.x) [[3]](#footnote-3) | Title | Content |
| TBD | Link Layer Encryption Overview (this standard) | Overview of link layer encryption services and key management. |
| TBD | Key Management Messages and Procedures for Link Layer Encryption | Detailed specification of key management for link layer security. |

Table 5, Affected Standards

|  |  |  |  |
| --- | --- | --- | --- |
| Standard Number (TIA-102.x) | Title | Effect | Addendum (TIA-102.x) [[4]](#footnote-4) |
| AABB-B | Trunking Control Channel Formats | Modification of formats for LLE control channel TSBKs and MBTs. | TBD |
| AABC-D | Trunking Control Channel Messages | Addition of ISPs and OSPs in support of LLE operations and LLE key management. | TBD |
| AABD-B | Trunking Procedures | Addition of procedures for LLE operations. | TBD |
| BAAD-A | Conventional Procedures | Addition of procedures for LLE operations. | TBD |
| BBAC | Phase 2 Two-Slot TDMA Media Access Control Layer Description | Modification of formats and descriptions of LLE operations. | TBD |
| BAAA-A | FDMA Common Air Interface | Addition of new LDUs and packet data formats for LLE operations. | TBD |
| BACA-B | ISSI Messages and Procedures | Addition of inter-subsystem information in support of LLE key management. | TBD |
| BAHA | Fixed Station Interface | Addition of messaging and procedures for LLE key management. | TBD |
| AACD-A | KFD Interface Protocol | Addition of messaging and procedures for LLE key management. | TBD |
| AACA-A | OTAR Protocol | Addition of messaging and procedures for LLE key management. | TBD |

## Operational Overview

The following sections provide operational overviews for Trunking operation (section 2.5.1) and Conventional operation (section 2.5.2) of Link Layer Encrypted SU, sites and channels. Each section describes operations for the situation where both the SU and the site or channel are LLE capable and includes subsections describing additional applicable behaviors when either one or the other (site or SU) is not LLE capable. Under these circumstances, “local policy” is applied by the LLE capable entity. “Local policy” is a decision that is made in the LLE capable entity to determine whether to proceed with an operation when the partner in that operation is not able to provide LLE protection. For the purposes of this discussion, local policy is assumed to be programmable to allow the owner of the equipment to determine the behavior in these circumstances.

### Trunking Operational Description

Link Layer Encryption is applicable to information associated with trunking Mobility Management, Voice, Data and Supplementary services including voice, data and link control transmissions over traffic channels, LLE key management information, and OSPs and ISPs on the trunking control channel.

#### Trunking Key Selection and Time Synchronization

The trunking control channel advertises the key ID for the active CLEK and time information for implicit synchronization. By knowing the active CLEK, and relevant WACN/System/RFSS/Site ID information, protected SUs can derive the STEK/STAK for the trunking site. The time information broadcast on the control channel is used for implicit synchronization of control channel traffic and TDMA voice channel traffic and optionally for implicit synchronization of (FDMA) data channel traffic. Alternatively, time information for implicit synchronization of FMDA data traffic may be obtained from time information provided on the data channel itself.

Explicit synchronization is used for FDMA voice channel traffic. Time information for explicit synchronization of FDMA voice channel traffic is embedded in the FDMA voice stream.

#### Mobility Management

##### Full Registration

Figure 8 illustrates the effect of LLE on the full unit registration sequence. Legacy SU are unaffected, and go through normal registration, and optional authentication and affiliation. An LLE capable SU needs additional information before it can proceed. LLE Capable SU must determine whether the site supports LLE and, if so, the identity of the current key in use on the site, and the time synchronization of the site. This information is periodically sent on the control channel using broadcast messaging. The LLE capability of the site can also be inferred from the presence of link layer encrypted data OSPs on the control channel.

If the site supports LLE and the SU possesses the current CLEK[[5]](#footnote-5), registration proceeds normally except that all registration exchanges are link layer encrypted, and that fact implies to the site that the SU is LLE capable.

If the SU does not possess the current CLEK for the site, it sends an unprotected registration request indicating its need for the current CLEK. The site may initiate link layer authentication, and then, if the site has possession of the IKSP derived from the SU’s ILEK, the site delivers the CLEK to the SU via individual key management methods.

Once registered, the SU then performs a group affiliation (protected with LLE) with the RFSS. The group affiliation for LLE includes the SU’s Future Key Status to allow the RFSS to determine whether opportunistic provisioning of future CLEKs or RLEKs should be performed. It also includes the LLE Individual Reception Policy (LIRP) that identifies whether the SU will only accept protected individual transactions (Protected Only, PO), or will entertain individual exchanges with unprotected SU (Unprotected Allowed, UA). In the response, the RFSS indicates the protection condition for the group and its announcement group. An unprotected group affiliation for a protected talkgroup is always rejected or denied.



Figure , LLE Full Registration

###### Mixed Mode Operation

An SU that is not LLE capable (i.e., a Legacy SU) can register normally with an LLE capable site.

A protected SU applies its local policy to determine whether to proceed with unprotected registration and authentication on the site that doesn’t support LLE, or to continue to search for suitable site/system that is LLE capable.

An LLE protected site that receives an unprotected registration asking for the current key, but that does not possess the ILEK for the SU, informs the SU that it cannot be provisioned with the current key. The SU then applies local policy to determine whether to proceed with unprotected operation on the site, or to continue hunting for a new site.

##### Location Registration

When switching sites within a system (i.e., an LLE domain), an LLE capable SU determines if the new site is LLE capable. As with full unit registration, this can be inferred by the presence of protected OSPs on the control channel, from periodic broadcast messaging, or from the presence of the Key Announcement. If the site is LLE capable, and the SU is protected, the SU always sends the location request in protected mode regardless of whether the talk group is protected.

Having found a site capable of LLE operation, the SU obtains the information to derive the LLE operational keys for the site and exchanges LLE protected location registration messages associated with the FNE. If the FNE receives an unprotected location registration request that includes a protected Talkgroup ID, the FNE provides an unprotected response that rejects or denies the request. The FNE does not indicate “protected talkgroup” in such a response. Likewise, if the FNE receives an unprotected location registration request from an SU that it believes is protected, it rejects the request.

As with group affiliation, location registration includes the LIRP and the location registration response includes the protection condition for the group identified in the location registration ISP.

Legacy SU perform normal unprotected location registration on protected sites.



Figure , LLE Location Registration

###### Mixed Mode Operation

A protected SU that switches to a non-LLE capable site within the same system, must apply local policy to determine whether to proceed with unprotected location registration with the unprotected site, or to search for a different site or system that is LLE capable.

#### Group Voice Services



Figure , Protection of Group Voice Services (Trunking)

Figure 10 illustrates the protection of group voice services in an LLE protected trunking system. For unprotected talkgroups used by unprotected SU, all related control channel and traffic channel traffic is unprotected in both directions. SU local policy can allow a protected SU to affiliate with unprotected groups, and participate in unprotected group calls. Protected SUs that have affiliated to an unprotected talkgroup send voice service requests protected, but traffic for that talkgroup without LLE protection, and depending on local policy, may use the “no one” reserved ID to maintain the user’s anonymity. Grants, updates, and downlink voice traffic for unprotected talkgroups are always unprotected.

For protected talkgroups, all related control channel and traffic channel traffic (including service requests, grants, updates and voice traffic) is LLE protected at all sites within the system. If an unprotected voice service request is received for a protected talkgroup the FNE provides an unprotected response that rejects or denies the request. The FNE does not indicate “protected talkgroup” in such a response.

For FDMA voice traffic, link control words associated with an LLE protected service are not sent on unprotected traffic channels. For TDMA voice traffic, MAC messages associated with an LLE protected service are not sent on unprotected traffic channels.

#### Individual Voice Services

LLE supports protection of individual calls with and without availability checks.

Between SU, when an individual call is setup the initiator does not know whether the recipient is operating with or without link layer encryption. Therefore, the protected initiator includes an LLE policy flag in the call setup messaging that indicates

1. That the call should only be setup if the recipient is link layer encrypted (Protected Only (PO)); or,
2. That the call should be setup even if the recipient is not link layer encrypted (Allowed Unprotected (AU)).

Likewise, if a call is setup by an unprotected SU to a protected recipient the call should only be setup if the recipient has told its serving site/RFSS that it’s policy for receipt of calls (LIRP) is AU (Allow Unprotected).

Figure 11 illustrates individual calls without availability checks.



Figure , Protection of Individual Call without Availability Check

Having knowledge of the LLE capability of every registered SU, the RFSSs of the participants are responsible for enforcing the policy provided by the initiator. Calls between unprotected SU proceed normally. Between two protected SU, the policy flag is irrelevant and the call is setup with protection on both air interfaces.

When a protected SU calls an unprotected one, if policy is PO and the recipient is not protected, the call fails with an indicator to the initiator. If the policy is AU and the recipient is not protected, the call succeeds and is setup in unprotected mode.

An unprotected SU can also attempt to call a protected one. In this case, the request is sent unprotected, and the destination RFSS enforces the LLE Individual Reception Policy (LIRP) of the destination. If the LIRP is protected only, the destination RFSS will not send the call setup to the protected destination SU. Otherwise, the unprotected call is forwarded to the protected destination SU, and the protected SU either silently discards the call setup, or joins the call in unprotected mode.

When an individual call is setup with availability check (Figure 12), Legacy SU operate normally, and calls between protected SU are fully protected. Calls from protected to unprotected SU, the destination RFSS enforces the policy of the source SU (as with calls without availability checks). When the call is from an unprotected to a protected SU, the destination SU enforces the LIRP of the destination. If the LIRP is PO, then the call setup is rejected as if the recipient was not present at the RFSS. If the LIRP is AU, then the recipient SU enforces its local policy and either silently discards the availability check, or joins in unprotected mode.



Figure , Protection of Individual Call with Availability Check

When a protected SU initiates an individual call with availability check to FNE (i.e., a wireline console) it still includes the AU/PO indication in the call setup, but in this case, the RFSS of the FNE will never block the call due to the policy indicator. When the FNE is the initiator of the call and the console and target SU are in separate RFSSs, for consistency in the ISSI the RFSS of the console includes the AU policy indicator. Traffic to and from the protected SU is protected, and traffic to and from unprotected SU is not.

#### Supplementary Services

Because trunking Supplementary Services are individual services, the procedures for applying LLE protection are similar to those for individual voice services without availability check.

Supplementary Services use control channel signaling, and use both TSBK and MBT formats. As with voice services, supplementary service messages may originate from an SU or an FNE (e.g., a wireline dispatcher) and the destination of the service may be an SU or the FNE. In trunking, except for Emergency Alarm, the destination is always an individual. Emergency Alarm is sent inbound only and includes a Group identifier but the FNE (in particular the wireline dispatcher equipment) is the default destination.

When the originator and destination are both SU, there is typically an ISP/OSP exchange between the originator and its RFSS, and another between the destination and its RFSS. Often the destination messaging is different from the originator messaging, but both sets of messages typically contain identifiers for both the originator and the destination.

The initiator may not know whether the recipient is operating with or without link layer encryption. Therefore, as with individual voice services without availability check, a protected SU initiating a supplementary service includes the PO/AU policy flag in the protected service request ISP. The RFSS enforce the policy flag exactly as for individual voice services without availability check. When the destination is another SU, the RFSS determine whether to deny or allow the operation based on the protection condition of the destination and the stated policy of the initiator. When the destination is FNE, the RFSS allow the operation regardless of the policy condition.

When the initiator is an unprotected SU and the destination is a protected SU, the initiating ISP is rejected if the destination’s LIRP is PO. Otherwise, an unprotected OSP is sent to the protected destination SU and the destination applies local policy to determine whether to ignore the OSP or respond to the OSP unprotected. Finally, when the initiator is FNE, the signaling to a protected SU is protected.

#### Data Services

Prior to performing LLE protected data exchanges an SU must complete successful registration or location update (see section 2.5.1.2) and determine the specific LLE capabilities of the trunking site. A trunking site may have any of 8 configurations, as shown in Figure 13:

1. It may not support data services;
2. It may assign data channels only for unprotected data services (no protected data);
3. It may assign data channels that only for protected data services (no unprotected data services allowed) and use implicit synchronization tied to control channel timing;
4. It may assign data channels only for protected data services (no unprotected data services allowed) and use explicit synchronization included on the data channel itself;
5. It may assign separate data channels for unprotected and protected data, using implicit synchronization for the protected data channels;
6. It may assign separate data channels for unprotected and protected data, using explicit synchronization for the protected data channels;
7. It may interleave protected and unprotected data, using implicit synchronization for protected data; and,
8. It may interleave protected and unprotected data using explicit synchronization.

SU determine the protected data capabilities of the site from various broadcast messages. If LLE protected data services are available at a site, both the site and the SU use the protected data services for all individual data between them. When operating on a site with no LL-protected data channels, the LLE-capable SU determines whether to transact data in unprotected mode, based on local policy. An originating site without protected data services may send unprotected data to an SU based on control signals provided by the FNE originating the data.



Figure , Individual Data Service Site Configurations

When an SU or an FNE determines that LLE protected Individual Data Service is appropriate:

• LLE protection shall be applied to all Data Service control channel messages and all data channel messages specific to that SU.

• The SU may use local policy to decide whether to accept or ignore unprotected Data Service control channel messages and/or unprotected data channel messages.

• The FNE may use local policy to decide whether to accept or ignore unprotected Data Service control channel messages and/or unprotected data channel messages associated with an SU that it believes to be capable of LLE protection.

### Direct and Repeated Mode Conventional Operations

LLE is applicable to voice, data and supplementary services (i.e., conventional control messaging) in direct mode and when operating with simple repeaters. Protected and unprotected voice, data and conventional control transmissions can be arbitrarily interleaved on direct and repeated conventional channels, and LLE transmissions on these channels use explicit crypto-synchronization (i.e., the crypto-synch is included in the transmission).

Standalone repeaters are passive participants in LLE, forwarding traffic from the uplink to the downlink without modification.

#### Key selection and time synchronization

In direct and repeated modes, all LL encrypted conventional transmissions include an embedded time, source indication, and key identifier that are used to form the initial vector for encryption. Programmed NAC code and channel frequency information are used to derive the encryption key (STEK) from the CLEK identified by the key identifier.

Transmitting devices use their local time for crypto-sync. SU that do not maintain local time indicate that fact in the source indicator of the transmission, and use a pseudo-random number for the time.

In direct mode and on standalone repeated channels, SUs determine the current key to use for transmissions by programming (either directly or from LLE key management on related channels within the domain). When receiving a transmission, SUs interpret the key id in the transmission and use the corresponding key from the programmed domain for the channel. The key identifier embedded in the channel is unique within a conventional domain, so SU must have local knowledge of the domain of a particular channel in order to select the correct key.

#### Voice, Data and Supplementary Services

In direct mode and on standalone repeated channels, SUs originating a transmission determine whether to apply LLE protection based on local knowledge. An SU receiving an LL encrypted transmission checks the key identifier in the received voice stream. If the receiving device does not have an LLE traffic key that matches this identifier, the voice stream cannot be decoded. Otherwise, the receiving device uses the embedded time for LLE decryption.

Protected SU receiving protected transmissions determines whether to trust the source of the LLE protected transmission based on a comparison of embedded time vs. local time and based on local policy. Local policy may identify a trusted tolerance between embedded and local time and may generate warnings and/or ignore the received signal if the tolerance is exceeded. Local policy acceptance criteria may also use other signal qualifiers including but not limited to; Group ID, Individual ID, NAC, etc.

When a receiving device decides to accept a received LLE protected message, it applies LLE protection to any appropriate response. When a receiving device decides to ignore a received LLE protected data packet, it shall send no response.

#### Mixed Mode Operation

Protected SU receiving an unprotected stream (including link control) use local policy to decide whether to accept or reject the received stream.

If an LLE capable device decides to accept a transmission without LLE protection, any response is also sent without LLE protection. Note that this reveals the identity of the originator and so, LLE capable SUs should have a local policy that allows or disallows origination of a transmission to an unprotected destination group or individual.

### CFN Conventional Operations

Link Layer Encryption is applicable to voice, data, and supplementary services (i.e., conventional control messaging) over CFN channels. Individual voice, data and conventional control transmissions can be arbitrarily interleaved on CFN channels. All CFN information streams except data services always use explicit crypto-synchronization. Data services, however, use implicit synchronization in order to minimize the impact of LLE on conventional data performance.

Note that an SU may not know a priori if it is operating on a direct mode/repeated or CFN configuration. Conventional SU can infer that they are operating on a CFNS when:

1. They observe on the downlink channel a source indicator indicating “Encrypted at the RFSS; or,
2. They observe on the downlink channel key broadcast messaging enunciating the current key.

Prior to engaging in LLE operations on a CFN channel, SU must have the CLEK applicable to the channel, and the Network Access Code (NAC) and downlink frequency that is used for traffic key derivation.

CFN channels use broadcast messaging similar to trunking channels to advertise the current and future keys applicable to the channel (Key Announcement), and to advertise the current time. An SU on an active CFN channel can also learn the current key from downlink traffic, or it can send an anonymous request (thus protecting its identity) for the CFN to broadcast a key announcement. It can also surmise the current key from other means (e.g., programming, or recent experience in the same domain).

If the SU has the announced current key, it can then participate in LLE. If not, it can express the need for the key to the CFNS, which initiates individual key distribution to provide it with the current key.

#### Key selection and time synchronization

On CFN channels, the key used for LLE is identified in broadcast messaging. Time synchronization differs for voice and supplementary services with explicit synchronization and data services with implicit synchronization, and is described in the following sections.

#### Voice and Supplementary Services with explicit synchronization

When explicit crypto-synchronization is used, transmitting devices include an embedded time, source indication and key identifier in the information stream. These fields are used to form the initial vector for encryption. Transmitting devices use time derived from the station time provided by the periodic broadcast messaging.

An LLE capable receiving device checks the key identifier in the received information stream. If the receiving device does not have an LLE traffic key that matches this identifier, the voice stream cannot be decoded. Assuming the receiving device has the correct LLE traffic key, the receiving device shall use the embedded time for LLE decode.

If the key identifier does not match the key identifier determined for the CFN channel, the protected SU should silently reject the transmission. A protected SU on a CFN channel determines whether to trust the source of the explicitly synched LLE protected transmission based on a comparison of embedded time vs. local time and based on local policy. Local policy may identify a trusted tolerance between embedded and local time and may generate warnings and/or ignore the received signal if the tolerance is exceeded. Local policy may also verify received signal qualifiers including but not limited to; Group ID, Individual ID, NAC, etc.

When operating in an SU to FNE (CFN) configuration, an SU may obtain LLE encryption coordinates and may acquire/maintain LLE time synchronization with the FNE in any of four ways:

1. By receiving an unsolicited message from the FNE advertising the time;
2. By soliciting the time advertisement, and waiting for the response from the FNE;
3. From special Terminator Data Unit messages containing the time that are transmitted during hang-times; and,
4. From embedded signaling in the other LLE encrypted frames.

Messages from the FNE intended to provide LLE time synchronization shall be authenticated.

When a receiving device decides to accept a received LLE protected message, it applies LLE protection to any appropriate response. When a receiving device decides to ignore a received LLE protected data packet, it shall send no response.

If an LLE capable device decides to accept a transmission without LLE protection, any response is also sent without LLE protection. Note that this reveals the identity of the originator and so, LLE capable SUs should have a local policy that allows or disallows origination of a Supplementary Services message to an unprotected destination group or individual.

#### Data operation with implicit synchronization

LLE encrypted packet data exchanges may be performed without embedding LLE encryption coordinates (LLE key ID, source indication and time) in a data packet header block. This implicit LLE synchronization approach avoids embedding the LLE coordinate information in every data packet header block and permits the LLE protected Data Service throughput performance to more closely match the unprotected Data Service throughput performance.

When implicit synchronization is used, SU must acquire and maintain fine grained time synch with the infrastructure. When operating in a CFNS configuration, an SU acquires and maintains LLE time synchronization with the FNE by monitoring traffic on the outbound channel. Alternatively, a radio may acquire LLE encryption coordinates including time synch with the FNE by sending a clear LLE information request to the FNE (new message).

An LLE capable transmitting device determines whether to apply LLE protection to the data packet based on local knowledge. An LLE capable receiving device applies LLE protection when responding to receipt of an LLE protected data packet. An LLE capable receiving device uses local policy to determine whether to accept or ignore a received data packet without LLE protection. If an LLE capable device decides to accept a data packet without LLE protection, any associated response shall be sent without LLE protection.

# LLE Cryptographic Overview and Critical Information Elements

## Cryptographic Overview

### Nomenclature

Herein, when it is necessary to refer to the size of an unsigned integer data element, it is described as a member of Nx, where x is the size (in bits) of the data element. When it is necessary to refer to the size of a signed integer data element, it is described as a member of **Zx,** where x is the size (in bits) of the data element. For example, a 4-bit data element U which can take on the values 0,1,2 or 3 is described as U ∈ N2, and a data element S which can take on the values of -1,0,1,2 is described as S ∈ Z2.

### Zero Padding

Zero padding of a bit field is represented herein by the abstract function ZPAD as:

P = ZPAD(I,n)

Where:

* I = the bit field of length K to be zero padded;
* n = the total length of the resulting zero padded field P; and,
* P = the concatenation of (n-K) binary zeros with I, such that P ∈ Nn and I ∈ NK are “equal” (i.e., the padding is applied as most significant bits).

### LL Encryption Scheme

Link Layer Encryption uses counter mode encryption per ref. (5), which is illustrated in Figure 14. Each channel type (e.g., trunking control, TDMA traffic) or information element to be encrypted has a defined method of developing a “Crypto-Synch” word, and of translating the crypto-synch into an initial vector (IV). The initial vector is computed and loaded at a specific defined time relative to the plaintext being encrypted or cipher text being decrypted. Likewise, each channel type or information element has a defined method of extracting the plaintext (to be encrypted) from the totality of the information element or channel content. These methods can be found in the relevant specifications.



Figure , Counter Mode Encryption for Link Layer Encryption

LLE operates under the influence of a Site Traffic Encryption Key (STEK) that varies depending on the specific channel, site, etc. carrying the plaintext.

Moreover, each key is associated with a cipher to be used for LLE. In the current revision, the cipher associated with all keys is AES-256 (see ref. (6)).

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; and,
* IV is the initial vector.

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

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

C0 = CtrEncrypt(P0,1)

C1 = CtrEncrypt(P1,1)

Is equivalent to:

C = CtrEncrypt(P,2).

### Message Authentication

To facilitate LLE key management, RFSS broadcast various messages that contain information that requires cryptographic authentication. Such messages are message authenticated using the Keyed-Hash based Message Authentication Code (HMAC) per ref. (7). Figure 15 illustrates Message Authentication for LLE related messages. For each message that requires authentication, an authentication code is computed using HMAC and an authentication key (Ka[[6]](#footnote-6)). The message and resulting authentication code is transmitted over the air. Receivers compute the authentication code (Tc) from the received message, and compare it to the received authentication code. If the two are equal, the receiver concludes that message has not been modified in transit and originated with some holder of the Link Authentication Key. Message authentication does not provide protection from replay. Any message that requires replay protection must include a time coordinate in the message body.



Figure , Message Authentication for LLE

LLE uses SHA-256 as the underlying hash for HMAC.

Herein, computation of a message authentication code is denoted by three operations: MacInit(), MacContinue(), and MacFinish(), defined as follows:

MacInit(K)

MacInit() initializes the message authentication code with the key K.

MacContinue(Fragment1[,Fragment2]…)

When computing a message authentication code, the message being authenticated can be broken up in to ordered “Fragments” that are processed in a known order. MacContinue() includes the specified message fragments (of implied length) in the message to be authenticated.

M = MacFinish([N])

MacFinish(N) completes the MAC computation and returns the first N bits of the result. If N is unspecified, MacFinish() returns the entire computed authentication code.

Where appropriate, the three operations can be expressed as the single operation Mac() defined as:

M = Mac(K, N, Fragment1, [Fragment2,]…);

Where K, Fragment, M, and N are as previously defined.

### Key Derivation

To minimize key management operations, LLE uses a hierarchy of derived keys. Keys are derived in accordance with NIST SP-800-108 (ref. (8)). SP-800-108 defines counter mode key derivation functions as illustrated in Figure 16. The KDF derives key material (KO) of length L from a Higher-Level Key (KI). SP-800-108 allows for two additional inputs: a Label and a Context, either of which may be null. For LLE, we set the “Label” input to null (i.e., zero length), and use the “Context” input to derive different sets of keys. The key material KO produced by the KDF is subdivided into keys that are used for different cryptographic purposes.



Figure , Key Derivation for LLE

LLE SHALL use the Counter Mode KDF of ref. (8) to produce derived key material for key management. The counter length shall be 16 bits, and the 0x00 byte separating the Label from the Context in the KDF’s fixed input data string shall be included. LLE SHALL use the Hash Message Authentication Code (HMAC) of ref. (7) for the pseudo-random function of the KDF. HMAC requires the specification of an underlying hash function, which SHALL be SHA-256 as specified in ref. (9).

Within this specification, the LLE key derivation function is denoted as:

K1,K2,… = KDF(K,Context)

Where:

“K1,K2…” are the series of derived keys produced by the KDF of lengths N1,N2, etc. Furthermore, K1 comprises the first N1 bits of the output of the KDF; K2 the next N2 bits, etc.;

“K” is the Higher Level Key (KI) from which the subkeys are to be derived; and,

“Context” is the unique context information provided to the KDF.

The input L of the KDF is implied and is equal to the sum of the respective N’s. Ref. (8) suggests that the length L be included in the text used to derive the key material. However, the NIST test vectors (<http://csrc.nist.gov/groups/STM/cavp/documents/KBKDF800-108/CounterMode.zip>) DO NOT include the length in the computations. Therefore, for the purposes of LLE, the length L is not included in the derivation.

### Key Wrapping

In TIA-102 LLE, whenever keys are transported between entities they are protected with key wrapping algorithm compliant with SP-800-38F (ref. (10)). Specifically, LLE uses the KW function defined in SP-800-38F and illustrated in Figure 17. The Key Wrapping function (KW‑AE) takes a plaintext key (P) of length L (an integral multiple of the block size 128 bits) and a Key Encryption Key (K), and produces a cipher text (C) of length L plus half the block size (i.e., 64 bits). Conversely, the authenticated decryption (KW-AD) produces a plaintext form the input cipher text. If the decryption function determines that the cipher text was modified during transmission, it returns “Fail” in lieu of a plaintext key.



Figure , Key Wrapping for LLE

SP-800-38F requires an underlying 128-bit block cipher. TIA-102 LLE SHALL use AES‑256 (ref. (6)) for the underlying cipher, and the Key Encryption Key (K) SHALL be of length 256.

Within this specification, the TIA-102 Key Wrapping is denoted as:

Ciphertext = Wrap(Key,K)

Where:

“Ciphertext” is the cipher text output (C) of the key wrapping;

“Key” is the key to be protected; and,

“K” is the Key Encryption Key (K).

Likewise, TIA-102 Key Unwrapping is denoted as:

Key = Unwrap(Ciphertext,K)

Where:

“Key” is the decrypted key, or “Fail”;

“Ciphertext” is the cipher text output (C) from key wrapping; and,

“K” is the Key Encryption Key (K).

## Link Layer Encryption Information Elements

The following information elements are applicable to multiple parts of the cryptographic and key management schemes described in section 4.

### LLE Domain Identifier (LDID)

The LLE Domain Identifier (LDIDT ∈ N32) for trunked systems shall comprise the concatenation of the WACN ID (WACN ∈ N20) and System ID (System ∈ N12).

The LLE Domain Identifier for conventional systems (LDIDC ∈ N32) shall the same size (32 bits) as the concatenation of the WACN and System ID used in trunking. Moreover, the conventional LDID should be carefully selected to avoid overlap with other conventional systems and with trunking systems.

### LLE Key Type (LKT)

The LLE Key Type (LKT ∈ N4) identifies the use of associated keys. Table 7 summarizes the values of the LKT.

Table , LLE Key Type Values

|  |  |  |
| --- | --- | --- |
| Key Type | Key Type Value | Reference |
| ILEK | 0 | Sec. 4.1.2 |
| RLEK | 1 | Sec. 3.2.7 |
| CLEK | 2 | Sec. 3.2.4 |
| GLEK | 3 | Sec. 4.1.3 |
| STEK/STAK | 4 | Sec. 3.3 |

The STEK/STAK value is used to identify keys provided to sites only, and is not required in transactions with SU. All other values are reserved.[[7]](#footnote-7)

Editor’s Note: We may decide to make this 8 bits sometime in the future, but at the moment 4 seems fine.

### LLE Security Suite Identifier (LALG)

The LLE Security Suite Identifiers (LALG ∈ N4) identifies the algorithms, key lengths, and modes associated with a given key. For example, a key encryption key with LALG = 1 may be used for Key Wrapping using AES-256 as the underlying cipher. Table 7 summarizes the values of the LALG field.

Table , LALG Values

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| LALG | LLE | MAC | KDF Mode | KDF PRF | Key Wrap |
| 1 | AES-256 Counter Mode | HMAC-SHA256 | Counter | SHA-256 | AES-256 |

All other values are reserved.

Editor’s Note: We may decide to make this 8 bits sometime in the future, but at the moment 4 seems fine.

### Common Link Encryption Key (CLEK)

The Common Link Encryption Key (CLEK ∈ N256) is as described earlier, being the key from which site/channel specific traffic keys and other keys (e.g., CKEKs) are derived within a domain. The CLEK of a domain is itself derived from the RLEK of the same domain (see below), through the application of a KDF in the presence of the update parameter ULLE. The CLEK is fully specified by its LLE Domain (LDID) and CKID and its associated security suite (LALG) and Key Type (LKT), i.e. the tuple {LDID,LALG,LKT,CKID }, along with the key material of the key itself.

### CLEK Update Parameter (ULLE)

The CLEK Update Parameter (ULLE ∈ N7) is a public quantity included in the CKID that is used to derive an instance of a CLEK from its corresponding RLEK.

### Common Link Encryption Key ID (CKID)

The CLEK ID (CKID ∈ N12) is carried in the air interface in the KIDLLE field and identifies an instance of the CLEK used to derive traffic encryption keys. It comprises the concatenation of the RKID and the update parameter ULLE, as illustrated in Figure 18.

|  |  |
| --- | --- |
| 11 7 | 6 0 |
| Root Link Encryption Key ID (RKID) | CLEK Update Parameter (ULLE) |

Figure , Common Link Encryption ID (CKID)

### Root Link Encryption Key (RLEK)

The Root Link Encryption Key (RLEK ∈ N256) is unique for each LLE domain. CLEKs and other keys (e.g., RKEKs) are derived from the Root Link Encryption Key. RLEKs are fully specified by their LLE Domain (LDID), security suite (LALG), Key Type (LKT), and RKID, i.e. the tuple {LDID,LALG,LKT,RKID }, along with the key material of the key itself.

### Root Link Encryption Key ID (RKID)

The Root Link Encryption Key ID (RKID ∈ N5) identifies an instance of an RLEK in an LLE Domain. It also forms a portion of the CKID described previously.

## Operational Keys

The following are the operational keys used for LLE. Operational keys are identified, when required, by the CKID of the CLEK from which they are derived.

### Site Traffic Encryption Key (STEK)

The Site Traffic Encryption Key (STEK ∈ N256) is a key derived from the CLEK and used to encrypt and decrypt LL traffic. A completely specified STEK comprises the specification of the CLEK from which it was derived, and the derivation parameters used to derive it, along with the key material itself.

### Site Traffic Authentication Key (STAK)

The Site Traffic Authentication Key (STAK ∈ N256) is a key derived from the CLEK and used to authenticate messages between the site and SU. A completely specified STAK comprises the specification of the CLEK from which it was derived, and the derivation parameters used to derive it, along with the key material itself.

## Common Data Elements

The following data elements are used in multiple standards related to link layer encryption and are provided here to facilitate maintenance of the standards.

### LLE Initial Vector (LLEIV)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 7 | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | | 0 | |
| 0 | Downlink Frequency (MSBs) | | | | | | | | | | | | | | |
| 1 | Downlink Frequency (Middle SBs) | | | | | | | | | | | | | | |
| 2 | Downlink Frequency (LSBs) | | | | | | | | | | | | | | |
| 3 | Year | | | | | | | | | | | | | Mon | |
| 4 | Mon | | | | | Day | | | | | | | | | |
| 5 | Hours | | | | | | | | | Min | | | | | |
| 6 | Minutes | | | | | Microslots | | | | | | | | | |
| 7 | Microslots | | | | | | | | | | | | | | |
| 8 | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | S1 | | S2 |
| 9 | 0 | | | | | | | | | | | | | | |
| 10 | 0 | | | | | | | | | | | | | | |
| 11 | 0 | | | | | | | | | | | | | | |
| 12 | 0 | | | | | | | | | | | | | | |
| 13 | 0 | | | | | | | | | | | | | | |
| 14 | 0 | | | | | | | | | | | | | | |
| 15 | 0 | | | | | | | | | | | | | | |

Figure 19, LLE Initial Vector

The LLE Initial Vector is illustrated in Figure 19 and contains the following fields. Different air interfaces may populate the Initial Vector from different sources.

Downlink Frequency: The 24-bit downlink or direct mode frequency expressed in eighths of kilohertz.

Year: The UTC year expressed as the 7-bit number of years past the year 2000 (i.e., Year = UTCyear – 2000).

Month: The month of the Gregorian calendar year referenced to UTC and expressed as a 4-bit value with January being expressed as 0001.

Day: The 5-bit UTC day of the calendar month where the first day of the month is 1.

Hours: The 5-bit UTC hour of the day where midnight is 0.

Minutes: The 6-bit UTC number of minutes past the hour.

Microslots: The 13-bit number of 7.5 usec microslot intervals that have passed since the beginning of the hour.

S1,S2: Source indicator, see Table 8.

NULL: All zeros.

### LLE Source Indicator (SI)

Table 8 illustrates the values of the LLE Source Indicator:

Table , Source Indicator

|  |  |  |
| --- | --- | --- |
| S1 | S2 | Encryption Source |
| 0 | 0 | Encrypted at SU |
| 0 | 1 | Encrypted at RFSS |
| 1 | 0 | Reserved |
| 1 | 1 | Encrypted at SU using pseudo-time |

# Key Management for Link Layer Encryption

Four means are defined for the distributing the various keys for trunking and conventional fixed networks:

1. OTAR and KeyFill which provides for distribution of individual keys (ILEKs) for conventional fixed networks and trunking RFSSs, and for distribution of RLEKs and CLEKs for networks with conventional repeater and direct mode channels only;
2. Individual key distribution, which provides a way for suitably enabled sites to provision keys to individual SU;
3. Broadcast key distribution, which provides a way for SU to be efficiently rekeyed or provided with key updates; and,
4. Group key distribution, which provides a way for groups of SU to be efficiently key managed.

Table 9 summarizes the key management methods that are applicable to each LLE key type.

Table , Key Management Methods applicable to each Key LLE Type

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Distribution Method | | | | |
| Key Type | Key Fill | OTAR | Individual | Broadcast | Group |
| Root LL Encryption Keys (RLEK) | D | D | X | X | X |
| Common LL Encryption Keys (CLEK) | D[[8]](#footnote-8) | D | X | X | X |
| Site Operational Keys (STEK & SMAK) | Derived from CLEK[[9]](#footnote-9) | | | | |
| Individual LL Encryption Keys (ILEK) | X | X | U[[10]](#footnote-10) | N/A[[11]](#footnote-11) | N/A |
| Group LL Encryption Keys (GLEK) | N/A | N/A | X | N/A | X |

The following sections provide more detailed information about key management for link layer encryption, including:

1. Key Management Information Elements in section 4.1;
2. Key Management Architecture and Use Cases in section 4.2;
3. Key Distribution by KFD and OTAR in section 4.3;
4. Broadcast Key Distribution in section 4.4;
5. Individual Key Distribution in section 4.5;
6. Group Key Distribution in section 4.6; and,
7. Key Zeroization in section 4.7.

## Key Management Information Elements

LLE Key Management information elements are described in the following sections.

### Broadcast Rekeying Information Elements

The relationship of broadcast rekeying information elements to each other is summarized in Figure 20[[12]](#footnote-12). Specific definitions of these elements follow in the subsequent subsections.



Figure , Relationships of Broadcast Key Distribution Information Elements

#### Common Key Encryption Key (CKEK)

The Common Key Encryption Key (CKEK∈ N256) is a key derived from the active CLEK and used exclusively for key wrapping of keys included in broadcast key distribution messaging between an RFSS and SUs. The specification of a CKEK is that of its parent CLEK with a different key type (LKT) and key material.

#### Common Message Authentication Key (CMAK)

The Common Message Authentication Key (CMAK∈ N256) is a key derived from the active CLEK and used exclusively for authenticating broadcast key distribution messaging between an RFSS and SUs. The specification of a CMAK is that of its parent CLEK with a different key type (LKT) and key material.

#### Root Key Encryption Key (RKEK)

The Root Key Encryption Key (RKEK∈ N256) is a key derived from the active RLEK and used exclusively for key wrapping future RLEKs in broadcast key distribution between an RFSS and SUs. The specification of a RKEK is that of its parent RLEK with a different key type (LKT) and key material.

#### Root Message Authentication Key (RMAK)

The Root Message Authentication Key (RMAK∈ N256) is a key derived from the active RLEK and used exclusively for authenticating RLEK related broadcast key distribution messaging between an RFSS and SUs. The specification of a RMAK is that of its parent RLEK with a different key type (LKT) and key material.

### Individual Key Management Information Elements

The following sections describe the keys, key derivation parameters, and other information elements required for Individual key management. Figure 21 illustrates the relationship of the various parameters to each other.

#### Individual Link Encryption Key (ILEK)

The ILEK (ILEK ∈ N256) is unique per SUID within a domain and is the root key for Individual LLE key distribution as described in section 4.5. An ILEK is fully specified by its Key Type (LKT), and the tuple comprising the Domain ID of the ILEK, an SUID, Security Suite (LALG), and the key material of the ILEK itself.



Figure , Relationships of IKD Information Elements

#### Individual LLE Key Security Parameter (IKSP)

The Individual Key Security Parameter (IKSP ∈ N64) is derived from an ILEK, random seed (SI), and LEF domain. For each SU, the IKSP is unique for each LEF domain in which it will operate. An SU’s IKSP is fully specified by the tuple comprising the LEF domain, the SUID of the associated SU, the security suite (LALG), and the IKSP itself (i.e., the tuple {LEF Domain, SUID, LALG, IKSP}).

Note: The security policy of the home system determines whether it provides a new credential (i.e., based on a new seed) with each request for the credential from a visited system.

#### Individual LLE Key Derivation Seed (SI)

The Individual Key Derivation Seed (SI ∈ N32) is a cryptographically sound random number and public quantity that is used to derive an IKSP and is included in the credential CI.

#### Individual LLE Credential (CI)

The Individual LLE Credential CI is unique for each SUID within a domain (LEF Domain) and comprises the tuple {LALG, IKSP, SI}. It is employed as part of Individual LLE Key Distribution as described in section 4.5. A fully specified CI comprises the tuple {LEF Domain, SUID, LALG, IKSP, SI}.

#### Individual Key Encryption Key (IKEK)

The individual key encryption key (IKEK∈ N256) is derived from the IKSP during individual key management, is unique for each key management exchange, and is used to wrap the key being delivered to the SU from the infrastructure. IKEKs are fully specified by their LEF Domain, security suite (LALG), and key type (LKT), and the SUID to which they apply, along with their key material.

#### Individual Message Authentication Key (IMAK)

The individual message authentication key (IMAK∈ N256) is derived from the IKSP during individual key management, is unique for each key management exchange, and is used to authenticate the distribution of the key being delivered to the SU from the infrastructure. The full specification of an IMAK is that of the IKEK from which it is derived, with a different key type and key material.

### Group Rekeying Information Elements

The following sections summarize the keys and other information elements relevant to LLE group rekeying.

#### LLE Group Key (GLEK)

LLE Group Keys (GLEK ∈ N256) are used for protection group distribution of RLEKs, CLEKs, and future GLEKs, and are associated with a GLEK Identifier (GKID) and identified by a LLE Group Identifier (LGID). A fully specified GLEK comprises the LLE Domain (LDID), Key Type (LKT), LGID, and GKID of the group, as well as the key itself and its associated security suite (LALG) (i.e., the tuple {LDID, LKT, LALG, LGID, GKID, GLEK}). Figure 22 illustrates this relationship.

#### LLE Group Key Identifier (GKID)

Editor’s note: Size of GKID and LGID to be finalized later.

The Group Key Identifier (GKID ∈ N4) identifies an instance of a LLE Group Key within an LLE domain. The GKID allows for seamless update of LLE group keys.

#### LLE Group Identifier (LGID)

LLE Group Identifiers (LGID ∈ N12), with the GKID, identify a specific LLE Group Key within an LLE domain.

#### LLE Group Key Encryption Key (GKEK)

Group Key Encryption Keys (GKEK∈ N256) are a derived from GLEKs and used exclusively for key wrapping keys in group rekeying operations.

#### LLE Group Key Message Authentication Key (GMAK)

Group Key Message Authentication Keys (GMAK∈ N256) are derived from GLEKs and used exclusively for authenticating group key distribution messaging between RFSSs or CFNSs and SUs.



Figure , Relationships of Group Rekeying Information Elements

### Zeroization Information Elements

The following information elements relate to key zeroization.

#### Zeroization Key Scope

The Zeroization Key Scope (ZK ∈ N2) identifies the keys to be zeroized by a zeroization operation as described in section 4.7. It takes on the values identified in Table 10:

Table , Zeroization Key Scope Values

|  |  |
| --- | --- |
| Value | Meaning |
| 0 | Zeroize all keys in the domain except the ILEK |
| 1 | Zeroize all keys for the domain |
| 2 | Reserved |
| 3 | Reserved |

ZK set to zero commands a SU to delete RLEKs, CLEKs, GLEKs associated with that domain, and all keys derived from those RLEKs, CLEKs, and GLEKs. ZK set to 1 is only applicable in the home domain, and instructs the SU to zeroize all keys all keys for that domain including its ILEK, and, if it stores the IKSPs, any instances of the IKSPs related to that ILEK. An SU that receives ZK=1 outside of its home domain, should silently discard the command.

## Key Management Architecture and Use Cases

### Key Management Architecture

Figure 23 illustrates the interfaces involved in management of RLEKs, CLEKs and GLEKs for both trunking sites and conventional Fixed Stations. RLEKs and GLEKs can either be sourced external to the Link Encryption Facility (LEF) of the RFSS, or generated by the LEF itself. In the former case, the Key Source, which could be a P25 KMF, uses either extensions to the P25 Inter-KMF Interface (IKI, ref. (11)), or the KeyFill I/F (ref. (12)) to provide the RLEK or GLEK to the LEF.

In a trunking domain, the RLEK itself, or keys derived from the RLEK (e.g., the CLEK), as well as GLEKS, are obtained from the LEF. Either GLEKs and either RLEKs or CLEKs are delivered to SUs via the control channel based on trust level of the SU.

In a conventional domain with at least 1 channel operating in the Conventional Fixed Network configuration, the Fixed Station may obtain keys derived from the CLEK via extensions to the Fixed Station Interface. Again, GLEKs, and RLEKs or CLEKs are delivered to SUs via the Conventional Fixed Network channel based on trust level of the SU.

SUs capable of operating in direct mode or standalone repeat mode obtain CLEKs in one of two ways. If the LLE domain includes a channel operating in the Conventional Fixed Network configuration or trunking configuration, the CLEK for the domain may be obtained as described above. If the LLE domain does not include such channels, the CLEK for the domain may be obtained via an extension to the Key Fill Interface or an extension to the OTAR service using a trunked or conventional channel. In the latter scenario, the Key Fill Device or the OTAR KMF may obtain the CLEK from the LEF managing the LLE domain.

#### Distribution of RLEKs and CLEKs



Figure , Interfaces for RLEK and CLEK Distribution

Figure 23 illustrates the interfaces involved in management of RLEKs and CLEKs for both trunking sites and conventional Fixed Stations. RLEKs can either be sourced external to the Link Encryption Facility (LEF) of the RFSS, or generated by the LEF itself. In the former case, the Key Source, which could be a P25 KMF, uses either extensions to the P25 Inter-KMF Interface or the KeyFill I/F. to provide the RLEK to the LEF.

In a trunking domain, the RLEK itself, or keys derived from the RLEK (e.g., the CLEK, STEK/STAK) are obtained from the LEF. RLEKs or CLEKs are delivered to SUs via the control channel based on trust level of the SU. In a conventional domain with at least 1 channel operating in the Conventional Fixed Network configuration, the Fixed Station may obtain keys derived from the CLEK via extensions to the Fixed Station Interface. RLEKs or CLEKs are delivered to SUs via the Conventional Fixed Network channel based on trust level of the SU. SUs capable of operating in direct mode or standalone repeat mode obtain CLEKs in one of two ways. If the LLE domain includes a channel operating in the Conventional Fixed Network configuration or trunking configuration, the CLEK for the domain may be obtained as described above. If the LLE domain does not include such channels, the CLEK for the domain may be obtained via an extension to the Key Fill Interface or an extension to the OTAR service using a trunked or conventional channel. In the latter scenario, the Key Fill Device or the OTAR KMF may obtain the CLEK from the LEF managing the LLE domain.

#### ILEK Management in Conventional Systems



Figure , ILEK Management interfaces in CFN Systems

ILEKs are the shared secret that provides the essential security of the Individual (individual) key distribution methods described herein. The interfaces involved in ILEK management for CFNS are illustrated in Figure 24.

For each conventional domain in which they operate, Conventional SU have a unique ILEK that must be shared with the LEF of that domain. ILEKs can originate in the LEF of the CFN, and be shared with the conventional SU either by Keyfill or by OTAR.

In the figure, SU1 is shown receiving its initial ILEK, sourced from the LEF, via either KeyFill or OTAR. In the keyfill case, extensions to the keyfill interface allow the LEF to provide keys to a KFD, and the KFD to provide keys to the SU. Likewise, in the OTAR case, extensions to the IKI and OTAR protocols provide the delivery of the ILEK.

Alternatively, a KMF or keyfill device can be used to provide an SUs ILEK to the SU itself and the LEF of the CFN system. In the figure, SU2 and the LEF are provided with the ILEK for SU2 by the KFD or KMF associated with SU2.

#### ILEK Management in Trunked System



Figure , ILEK Management Interfaces in Trunked RFSS

For trunking, an SU’s ILEK is managed in or by the home LEF of the SU. For an SU registered outside its home domain (automatic roaming), a credential derived from its ILEK is shared with the visited domain to allow it to distribute its unique operational keys (i.e., the RLEKs or CLEKs for the domain). An SU using manual roaming between systems has a unique ILEK for each system identity. The ILEKs for a domain can only be provisioned or managed by the SUs home domain. All other keys for the domain can only be managed using the sites of that domain.

Figure 25 illustrates ILEK management in trunked systems. As with a conventional SU, the ILEK can be sourced either by the LEF of the SU’s home domain and distributed to the SU via the IKI and OTAR or via key fill, or it can be sourced by a KFD or KMF and delivered to the LEF via keyfill or IKI, and to the SU via keyfill or OTAR. ILEK replacements are made over-the-air via the trunking control channel, or via OTAR and keyfill. Over-the-air replacement of the ILEK via the control channel can only be made within the home domain of the SU.

Visiting SU have their ILEKs managed in their home domains, and a credential is shared by its home domain with the domain it is visiting.

### LLE Key Provisioning and Management Scenarios

The following sections describe important key management scenarios addressed by these specifications. Specifically,

* Preparing conventional and trunking infrastructure for LLE in section 4.2.2.1;
* Enabling trunking SU to operate on an LLE system in section 4.2.2.2;
* Enabling conventional SU to operate with LLE in section 4.2.2.3;
* Periodic refresh of keys in section 4.2.2.4; and,
* Responding to key compromise in section 4.2.2.5.

#### Preparing infrastructure for LLE

Trunking or conventional infrastructure is prepared for LLE by providing each trunking site and conventional fixed network channel with suitable operational keys derived from the RLEK for the domain. In conventional systems, the CFNSs are provided with their STEK/STAK via the fixed station interface. In trunking systems, trunking RFSS possess the RLEK, and distribute CLEKs, STEKs/STAKs in accordance with the trust levels of the sites involved. Note that interfaces within the RFSS (specifically to the trunking site infrastructure) are not addressed in these standards.

#### SU Enablement in Trunking Systems

Once an infrastructure has been prepared for LLE, individual SUs need to be enabled to operate within the LLE domain by providing each with a suitable key. SU Enablement is necessarily an individual operation.

Figure 26[[13]](#footnote-13) illustrates SU Enablement in a trunking SU’s home domain. First, a long-lived individual key needs to be shared by the LEF and the SU. The long-lived individual key can be created by the LEF and provisioned to the SU by OTAR or Keyfill (i), or can be developed elsewhere and shared with the LEF and the SU, again by OTAR or Keyfill (ii). An “Individual LLE Credential (CI)” derived from that key is then shared with the home RFSS of the SU. When the SU attempts to register with an RFSS within the LLE domain, it is provisioned with suitable operational keys via individual techniques that use information from the credential to secure the distribution of the keys. Whether the SU is provisioned with an RLEK or a CLEK for the domain is determined by the trust level of the SU as determined by the LEF/RFSS.

An SU that will visit an LLE domain other than its home domain is enabled using the techniques illustrated in Figure 27. Normally, the home RFSS of the SU shares the SU’s credential with the visited RFSS. Alternatively, in the absence of an ISSI, the SU’s credential must be pre-shared with the visited system via the IKI or via Keyfill. Keys derived from the credential allow the visited RFSS to provision CLEKs or RLEKs to the SU via individual methods.

Having received the RLEK or CLEK, the SU uses provisioned channel information to derive an STEKs and STAKs unique per operating channel.



Figure , “Home” SU Enablement



Figure , “Visiting” SU Enablement

#### SU Enablement in Conventional Systems

Once a conventional infrastructure has been prepared for LLE, individual SUs need to be enabled to operate within the LLE domain by providing each with a suitable key. SU Enablement is necessarily an individual operation.

When operating on a CFN channel, an SU may be provisioned using similar methods to those for trunking, as shown in Figure 28. As with trunking systems, a long-lived individual key needs to be shared by the LEF and the SU. For CFN systems, however, an explicit key request is used in lieu of SU registration, and the CFN site serves as a proxy between the SU and the LEF. As with trunking systems, the trust level of the SU determines whether it is provisioned with an RLEK or a CLEK for the conventional domain.



Figure , CFN SU Enablement

Having received the RLEK or CLEK, the SU uses provisioned channel information to derive the respective STEK/STAK channel operational keys. An SU may have multiple “personalities” associated with a conventional LLE domain. Having the RLEK and CLEK for the domain enable the SU to operate on any channel configuration within the domain.

If a conventional domain does not include a FNC, the SU must obtain the CLEK (and associated parameters; CKID, LALG) for the domain via a key fill device or via OTAR.

#### Periodic Key Refresh

Good security practice requires the periodic replacement (refresh) of keys even in the absence of key compromise. The appropriate frequency of key refreshes is determined by the amount of data being secured by the key, the strength of the key, and other factors. Whereas key compromise requires immediate action (i.e., rekeying) to restore security, and needs to take place over a short time horizon, periodic key refresh can be accomplished over time, opportunistically, so long as means are provided to not strand units that “miss” the refresh.

LLE accommodates key refresh primarily through “broadcast” key distribution combined with individual key distribution to catch “stragglers”.

#### Key Compromise

When a key is compromised, the key must be replaced and the new key activated, and an attempt should be made to zeroize the keys of the compromised unit. Zeroization scenarios are discussed in section 4.2.2.6.

For LLE, should an RLEK be compromised, then all SU and all LLE channels of the LLE domain need to be rekeyed, that is:

* Entities authorized to possess the RLEK of the domain need to be rekeyed with a new RLEK, and if a future RLEK had been provisioned, with a new future RLEK;
* Entities authorized to possess the current CLEK need to be rekeyed with a new CLEK, and if a future CLEK had been provisioned, with a new future CLEK; and,
* Trunking sites and conventional fixed stations need to be rekeyed with new site-specific keys (the pair STEK and STAK).

In each case, because the RLEK, when combined with suitable public information is sufficient to generate every operational key in the domain, only individual and group methods may be used for the rekeying.

Should either a CLEK or STEK/STAK be compromised, then:

* The CLEK needs to be updated. Holders of the RLEK can derive the new keys from the CLEK update value.
* Entities authorized to possess the CLEK but not the RLEK need to be rekeyed with a new CLEK, and if a future CLEK had been provisioned, with a new future CLEK; and,
* Trunking Sites and conventional fixed stations need to be rekeyed with new site-specific keys (STEK and STAK).

Because the CLEK, when combined with suitable public information is sufficient to generate operational keys in the domain, only individual and group means may be used for the rekeying.

Should a GLEK be compromised, then:

* The GLEK needs to be updated; and,
* Entities authorized to possess the GLEK need to be rekeyed with a new GLEK, and if a new future GLEK has been provisioned, with a new future GLEK.

Because a GLEK compromise affects every member of an LLE key management group, only individual delivery, or delivery through group keying with other groups that don’t include the compromised unit, may be used for the rekeying.

Finally, compromise of an ILEK only affects the SU of the ILEK. If an ILEK is compromised, the SU and its home LEF must provisioned with a new ILEK for the SU, using the same methods used for initial SU enablement.

#### Key Zeroization Scenarios

When a conventional radio or trunking SU is compromised (e.g., stolen), or temporarily or permanently deauthorized for operation in an LLE domain, it is desirable to zeroize the radio’s keys for that domain.

If authorization for some domain has been permanently withdrawn, all LLE keys associated with the given SUID or conventional UID and domain should be zeroized. If authorization has been temporarily withdrawn, it may be desirable for the SU to retain its ILEK for that domain to facilitate subsequent re-authorization.

For conventional LLE domains, a UID is associated with a conventional domain (LDID) and the associated keys (ILEK, RLEK, CLEK and GLEKs) for the domain. On conventional fixed network channels, when a radio is deauthorized in a conventional domain, the LEF of the domain can zeroize the keys for that domain, and that domain only. The conventional LEF sends a Zeroization OSP to the target radio when the radio is present on a CFN channel within the domain. The OSP indicates whether the zeroization should include the ILEK. The SU then zeroizes those LLE keys associated with the UID and current operational domain.

For conventional LLE domains that do not include a CFN channel (direct mode and/or standalone repeat channels only) and are not associated with a trunking LLE domain, zeroization must be performed using either a KMF or KFD.

A manually roaming Trunking SU is considered to be “home” to the trunking domain identified by the WACN ID/System ID portion of the selected SUID. When a manual roaming trunking SU is deauthorized, the LEF of the domain may zeroize the LLE keys associated with that SUID and the manual roaming trunking domain, and that domain only. To do so, the LEF sends a zeroization OSP to the target radio when the radio is present on a control channel within the trunking domain. The OSP indicates whether the zeroization should include the ILEK. The SU then zeroizes those LLE keys associated with the SUID and current domain.

An automatic roaming Trunking SU is considered to be “home” to the trunking domain identified by the WACN ID/System ID portion of the selected SUID. When the SU auto roams to another system (different WACN ID/System ID than the selected SUID) the SU registers using the home SUID and obtains LLE key material for the visited domain using a unique IKSP derived from the ILEK of the home LLE domain.

When an automatic roaming trunking SU registered in its home domain is deauthorized, the LEF of its home domain may zeroize the LLE keys associated with the SUID and domain, and that domain only. This may be a temporary deauthorization (operational keys only) or a permanent deauthorization (ILEK and Operational keys). If the automatically roaming SU is registered in some other, visited, domain, the LEF of that domain may zeroize only the operational keys associated with that domain.

Note that no means is anticipated by which the LEF of one domain will use the ISSI to send commands to a radio currently operating in another domain.

In either trunking case, the LEF sends a zeroization OSP to the target radio when the radio is present on a control channel within the trunking domain.

## Key Distribution by KFD and OTAR

In both conventional and trunking systems, SUs are provisioned with ILEKs via Key Fill Devices (KFD) and OTAR. In trunking and CFN systems, the provisioning an SU with an ILEK is sufficient to allow it to operate within the domain.

SUs operating in a conventional LLE domain that includes conventional repeated channels, or direct mode channels and does not include a channel operating in the Fixed Network Configuration, may receive RLEKs or CLEKs via OTAR and Keyfill.

The following subsections provide more detail on key distribution by OTAR and Keyfill.

### LLE Key Distribution via Key Fill Device

LLE key distribution via the Key Fill Device requires the operations of loading, deleting, and inventorying ILEKs, RLEKs and CLEKs. Distribution of keys from the LLE Key Facility to a KFD and distribution of keys from the KFD to SU are both governed by the KFD Interface protocol. Details of the interface and the required operations are provided in the relevant addendum to the KFD Interface protocol (ref. (13)).



Figure , KFD Based Key Distribution

### LLE Key Distribution via OTAR

LLE key distribution via OTAR requires the operations of loading, deleting, and inventorying ILEKs, RLEKs and CLEKs. Distribution of keys from the LLE Key Facility to a KMF and distribution of keys from the KMF to SU are governed by extensions to the Inter KMF Interface and/or the Key Fill Interface along with extensions to the OTAR Service.

Details are provided in the relevant addendums to the KFD Interface protocol (ref. (12)), the Inter KMF Interface protocol (ref. (11)) and the OTAR service (ref (14)).



Figure , OTAR LLE Key Distribution

## Broadcast Key Distribution

Broadcast LLE key distribution, illustrated in Figure 31, can be used by an RFSS or CFNS to opportunistically provide a planned future key to SU. Broadcast key distribution is applicable to RLEKs, and CLEKs.

Broadcast key distribution is only suitable for periodic updates to LLE keys, not for SU enablement, or SU repudiation.



Figure , Broadcast Key Distribution

SUs monitor the outbound trunking control channel or the outbound conventional Fixed Network Channel to determine the current and future keys (“Key Determination”). From this information, an SU can determine whether it needs the advertised future key and make an opportunistic expression of that need (a “Future Key Request”). The RFSS uses information from Future Key Requests (from all SU) and its local store to determine which future keys (if any) should be broadcast distributed by the RFSS.

### Broadcast Key Derivations

The derivations of broadcast key management keys from RLEKs, and CLEKs are illustrated in Figure 32. The derivations are identical except for the input and output keys. Each comprises the application of the security suite KDF to the input key to produce a key encryption key and an authentication key. In each case, the first bits of the KDF are used for the key encryption key, and the later bits of output from the KDF for the authentication key. Also, in each case, the “Context” is the string “KEY MANAGEMENT KEYS”.



Figure , Broadcast Key Derivation

Formally,

* RKEK,RMAK = KDF(RLEK,”KEY MANAGEMENT KEYS”); and,
* CKEK,CMAK = KDF(CLEK,”KEY MANAGEMENT KEYS”).

### Key Determination

Key Determination consists of monitoring the control channel or conventional fixed network channel for the LLE Key Announcement OSP, which contains the CKID of the current CLEK and, optionally, the CKID of a future CLEK. The LLE Key Announcement OSP also indicates whether the site is currently periodically broadcasting the future key.

The identities of the STEK and STAK are inherited from the CLEK from which the keys are derived, and the identity of the current RLEK is embedded in the CKID. Therefore, broadcast of the CKID in the key announcement is sufficient for determining the current and future keys at all trust levels.

### Future Key Request

Trunking SU indicate whether they possess the advertised future key through the Future Key Status field of the Group Affiliation Request. Conventional SU use a LLE Key Request ISP to request needed future keys.

### Key Survey

Upon determining from registration messaging or Key Requests that one or more SU dwelling on the site need future keys, the site/RFSS should opportunistically transmit the future RLEK and CLEK, per section 4.4.5.

A site, RFSS or LEF that is aware of the type (RLEK, CLEK) of key required by an SU may independently keep track of which keys need to be transmitted and only transmit the RLEK or CLEK rather than both.

When an SU is deregistered from a trunking site, the site, RFSS or LEF should remove the SU from its count of the number of demanding SU at the site. CFNS and trunking sites may also apply other criteria to determine when to discontinue opportunistic sending of LL keys.

### Key Broadcast Message Construction

Broadcast distribution is accomplished by the transmission of LLE\_KEY\_DIST OSPs via trunking or conventional control messaging. The information contained in the OSP includes four parts:

1. Security Key Identification: This part identifies the key being used to secure the message, and comprises:
   1. Security Key Type (SKT): the LLE Key Type (LKT, see section 3.2.2) type of the key being used to secure the message. For broadcast messaging, either an RLEK or a CLEK can be used to secure the message;
   2. Security Key Security Suite Identifier (SALG): the LLE Security Suite Identifier (LALG) of the key securing the message; and,
   3. Security Key Identifier (SKI), comprising the following:
      1. The Root Key ID (SRKID, see section 3.2.8)) of the CLEK or RLEK securing the message; and
      2. The CLEK Update Parameter (SULLE, see section 3.2.5) of the CLEK or RLEK securing the message. When an RLEK is used, ULLE is set to all zeros and need not be transmitted in the message.
2. Delivered Key Identification: This part identifies the key contained in the message and comprises:
   1. Delivered Key Type (DFKT): the LLE Key Type (LKT, see section 3.2.2) of the key being secured which may be an RLEK, CLEK, or GLEK;
   2. Delivered Key Security Suite Identifier(DALG): the LLE Security Suite Identifier (LALG) of the key being secured; and,
   3. Delivered Key ID (DKID) comprising:
      * 1. For RLEKs, the Root Key ID (RKID, see section 3.2.8)) of the RLEK; or,
        2. For CLEKs, the CKID of the CLEK being delivered; or,
      1. For GLEKs,
         1. The LLE Group ID (LGID) of the group key being delivered; and
         2. The Group Identifier (GKID) of the group key being delivered.
3. Key Wrapped Key Material (KM): The key wrapped key material conveyed (see section 3.1.6); and,
4. Message Authentication Code (AUT): An authentication code for the message (see section 3.1.4)

The construction of these parts proceeds as follows. Given:

Skey = the key encryption key derived from the key being used to secure the message;

Mkey = the message authentication key derived from the key being used to secure the message, and,

Fkey = the key being carried in the message.

Then:

KM = Wrap(Fkey,SKey);

W1 = SKT || SALG || SKI;

W2 = FKT || SALG || DKID;

Finally,

AUT = MAC(MKey, 32, W1, W2, KM)



Figure , Broadcast Distribution Security

## Individual Key Distribution

Individual key distribution (IKD) provides a means by which LLE keys (RLEKs, CLEKs, and GLEKs) may be securely delivered to specific SU. The security of IKD is rooted in the Individual Link Encryption Key (ILEK), which needs to be pre-provisioned to the SU and LEF.

### Distribution of LLE keys via IKD

For conventional Fixed Network Configurations (see Figure 34), the LEF and SU have a common ILEK specific to the SU (1a,1b) and the LLE domain. The LEF derives an Individual Key Security Parameter (IKSP) from the ILEK and a random Individual Key Derivation Seed (SI). The LEF derives the IKEK and IMAK for the SU, encrypts the key to be delivered, and passes the seed and the encrypted key to the SU via the CFNS (2,3). The SU receives the seed and encrypted key from the CFNS, derives the IKSP from the ILEK by applying the security suite KDF, and can then decrypt the delivered key.



Figure , High-Level Flow for Conventional Individual Key Distribution

Individual key distribution on trunking systems (Figure 35) operates identically, except that for trunking, the serving RFSS receives the Individual Key Distribution Seed (Si) from the home RFSS of the SU via the ISSI or the credential is delivered via the IKI in real-time or non-real-time mode (3), or via a KFD. The SU has possession of the ILEK, receives the seed (Si) and encrypted key from the serving RFSS, and derives the IKSP from the ILEK. It can then decrypt the delivered key.



Figure , High-Level Flow for Trunking Individual Key Distribution

### Individual Key Derivations

The derivations of individual key management keys from ILEKs are illustrated in Figure 36. The derivation comprises the application of the security suite KDF to the ILEK to produce the individual key security parameter (IKSP), and a subsequent application of the KDF to derive an IKEK and IMAK. For the IKSP derivation, the “Context” is the binary representation of the Individual LLE Key Derivation Seed (SI) concatenated with the domain identifier of the LEF that will use the keys. The first bits of the KDF output are used for the key encryption key, and the later bits of output from the KDF for the authentication key.

Formally:

* IKSP = KDF(ILEK,Si || LEF Domain); and,
* Both the serving RFSS and the SU can then derive the individual operational keys (IKEK,IMAK) from the IKSP by suitable application of the KDF, formally: IKEK,IMAK = KDF(IKSP,”KEY MANAGEMENT KEYS”).



Figure , Individual Distribution Key Derivation

### Individual Key Distribution Message Security

The information contained in the IKD Key OSP includes four parts:

1. Security Key Identification: This part contains the information required to select and generate the IKEK and IMAK used for encryption and authentication of the message. It comprises:
   1. Individual LLE Key Derivation Seed (SI, see section 4.1.2.3); and,
   2. Security Key Security Suite Identifier (SALG): the LLE Security Suite Identifier (LALG) of the key securing the message; and,
2. Delivered Key Identification: This part identifies the key contained in the message and comprises:
   1. Delivered Key Type (DKT): the LLE Key Type (LKT, see section 3.2.2) of the key being delivered which may be an RLEK,CLEK, or GLEK;
   2. Delivered Key Security Suite Identifier(DALG): the LLE Security Suite Identifier (LALG) of the key being delivered; and,
   3. Delivered Key ID (DKID) comprising:
      1. If the key being conveyed is an RLEK, the RKID (DRKID, see section 3.2.8) of the key being conveyed;
      2. If the key is a CLEK, the CKID of the key being conveyed.,
      3. If the key being conveyed is a group key, the LGID and GKID of the group key being conveyed.
3. Key Wrapped Key Material (KM): The key wrapped key material conveyed; and,
4. Message Authentication Code (AUT): An authentication code for the message.

The construction of these parts proceeds as follows. Given:

ZERO = a null octet;

Skey = the key encryption key derived from the key being used to secure the message;

Mkey = the message authentication key derived from the key being used to secure the message, and,

Dkey = the key being carried in the message.

Then:

KM = Wrap(Dkey,SKey);

W1 = SALG

If FKT indicates a CLEK or RLEK, then

W2 = DKT || DALG || ZPAD(DRKID,8) || ZPAD(DULLE,8);

Or If DKT indicates a GLEK then

W2 = DKT || DALG || ZPAD(LGID,8) || ZPAD(GKID,8);

Finally,

AUT = MAC(MKey, 32, W1, W2, Wrap(Skey,DKey))



Figure , Individual Distribution Security

### ILEK Sharing

Before any individual key distribution can be performed for an SU, the SU and its home LEF must share an ILEK. To allow for operational flexibility, transportation of a fully specified ILEK is supported OTAR, Keyfill, and the IKI. ILEKs can therefore be shared between an LEF and SU by a variety of means:

1. The ILEK can be generated in the LEF, and shared with the SU via OTAR or Keyfill;
2. The ILEK can be generated in the KMF of the SU, and shared with both the LEF and the SU via Keyfill;
3. The ILEK can be generated in the KMF of the SU, and shared with the LEF via the IKI, and with the SU via OTAR and Keyfill; and,
4. The ILEK can be generated by a third party (e.g., a key kettle), and shared with both the LEF and the KMF of the SU via the IKI, and with the SU via OTAR or Keyfill.

Other combinations may be available depending on the interfaces supported by each involved entity.

## Group Key Distribution

Group Key Distribution may be used by a trunking RFSS or a conventional fixed station to opportunistically distribute CLEKs, RLEKs, and future GLEKs to groups of SU. The management of LLE Key Management Groups and their associated group keys is the responsibility of the LEF of each LLE Domain.

Group distribution is used for delivering future group keys and for delivering replacement keys in key compromise recovery scenarios. The SU population of an LLE domain may be divided by the LEF into a multiplicity of key management groups, each of which should be composed exclusively of fully trusted SU (those that derive keys from RLEKs) or less trusted SU (those that derive keys from CLEKs).

For addressing purposes, each key management group is identified by an LLE Group ID (LGID). Group membership is established by provisioning SU with Group Keys using individual or Group methods.

Each key management group has an active and potentially future Group LLE key assigned by the LEF and identified by a Group Key ID (GKID). Together the LGID and GKID identify a specific GLEK that is associated with the given LLE Group.

Key derivations from GLEKs; the secure delivery of keys using Group Key Distribution; and the management of GLEKs are described in the following sections.

### Group Key Derivations

The derivation of group key management keys from GLEKs is illustrated in Figure 38. The derivation comprises the application of the security suite KDF to the GLEK to produce a group key encryption key (GKEK) and authentication key (GMAK). The first bits of the KDF are used for the key encryption key, and the later bits of output from the KDF for the authentication key. The “Context” is the string “KEY MANAGEMENT KEYS”.



Figure , Group Key Derivations

Formally:

* GKEK,GMAK = KDF(GLEK,”KEY MANAGEMENT KEYS”).

### Group Key Distribution Description

To send a key to all the members of a group, the trunking RFSS or conventional LEF constructs a group key distribution message (see section 4.6.3) secured with the current group key of the given group. Members of the group receiving the message can authenticate and decrypt it and subsequently use the given key as required.

### Group Key Message Security

The information contained in the Group Key Distribution includes four parts:

1. Security Key Identification: This part identifies the key being used to secure the message, and comprises:
   1. Security Key Security Suite Identifier (SALG): the LLE Security Suite Identifier (LALG) of the key securing the message; and,
   2. Security Key Identifier (SKI), comprising the following:
      1. Group Key ID (SGKID, see section 4.1.3.3) of the GLEK securing the message; and,
      2. LLE Group ID (SLGID, see section 4.1.3.2) of the GLEK securing the message.
2. Delivered Key Identification: This part identifies the identity of the key contained in the message which is either an RLEK, CLEK, or GLEK:
   1. Delivered Key Type (DKT): the LLE Key Type (LKT, see section 3.2.2) of the key being secured which may be an RLEK, CLEK, or future GLEK.
   2. Delivered Key Security Suite Identifier(DALG): the LLE Security Suite Identifier (LALG) of the key being secured; and,
      1. Delivered Key ID (DKID) comprising the RKID, CKID, or GKID/LGID of the key being delivered.
3. Key Wrapped Key Material (KM): The key wrapped key material conveyed; and,
4. Message Authentication Code (AUT): An authentication code for the message.

The construction of these parts proceeds as follows. Given:

Skey = the group key encryption key derived from the key being used to secure the message;

Mkey = the group message authentication key derived from the key being used to secure the message, and,

Dkey = the key being carried in the message.

Then:

KM = Wrap(Dkey,SKey);

W1 = SALG || ZPAD(SLGID,8) || ZPAD(SGKID,8);

If the DKT indicates a CLEK or RLEK:

W2 = DKT || DALG || ZPAD(DRKID,8) || ZPAD(DULLE,8);

Or if the DKT indicates a GLEK:

W2 = DKT || DALG || DLGID || ZPAD(FGKID,8);

Finally,

AUT = MAC(MKey, 32, W1, W2, Wrap(Skey,DKey))



Figure , Group Distribution Security

### Management of Group Membership and Keys

The membership and organization of groups within a domain is up to the LEF of the domain. For interoperability purposes, SU should support some standard minimum of number of groups, and a current and future key for each group. Group Key Management consists of a series of opportunistic exchanges between SU and the LEF of a domain.

Editor’s Note: FBI representative to ETG say that without specifying that group rekeying is required, then operations are compromised for organizations that buy radios from multiple vendors.

Group keys may be distributed using individual or group methods. An LEF determines which methods to use based on its understanding of the group key inventories of the SU’s under its control, and of which SU may be present in the domain. When an SU receives a group key (either individually or by group methods) for a group that it is not currently a member of, it implicitly becomes a member of the group.

The high-level flow of Group Key Management is illustrated in Figure 40[[14]](#footnote-14) and relies on the inventory summary of Figure 41. The inventory summary contains the number of LLE groups of which the SU is a member, an SHA-256 digest of the LGIDs of those groups, and an SHA-256 digest of the current and future GKIDs of its groups. By comparing the summary provided by the SU to that computed from the ‘desired state’ of the SU, the FNE can determine whether the SU’s group membership is correct, and whether its group key inventory is correct.

When a trunking SU completes its full registration within a domain, it sends an Inventory Summary (1), at the earliest opportune time, to the LEF to help the LEF determine whether it needs to send any group keys to the SU. (Alternatively, an LEF can request an Inventory Summary from an SU at any time (5).) Likewise, conventional SU operating in a CFN domain should send an inventory summary to the LEF at a convenient time upon entering a CFN domain. Based on the inventory summary, the LEF can determine which detailed inventory information (if any) is required to determine how to bring the SUs keys up to date. If the LGID inventory doesn’t match, the LEF requests more a detailed inventory information group membership (2a,b) and corrects the LGID membership list of the SU (2c), and provides the keys for any missing groups (2d). Subsequently, the LEF should request a new inventory summary.

If only the key summary is incorrect, the FNE requests a detailed key inventory (3a,b), and subsequently uses individual or group methods (4) to provide or remove the mismatched keys.

LEF opportunistically send OSPs to announce the current and future group key ids for LLE group. SU that are members of the group and lack one or more keys can request the given key or keys from the LEF. The LEF then uses suitable individual or group methods to provide the keys, if appropriate.

All group key messaging is LLE encrypted.



Figure , High Level Flow for Group Key Inventory and Management



Figure , Inventory Summary

## Key Zeroization

When a unit is compromised or decommissioned for operation in a domain, an attempt should be made to zeroize the keys. This section describes the techniques available for LLE key zeroization.

### Zeroization using OTAR/Key-Fill Techniques

End-to-end key management techniques (OTAR and Key-Fill) provide means for a crypto-officer (usually associated with an agency) to zeroize end-to-end keys. SU that support LLE and OTAR or Key-fill should zeroize LLE keys along with end-to-end keys when end-to-end keys are zeroized.

In addition, LLE extends the key management messages of (see ref. (12)) to provide for OTAR/KFD zeroization of some or all LLE keys associated with an SU, independently of end-to-end keys. This allows a crypto-officer to deauthorize the SU for use in a domain.

### Zeroization of LLE keys by an LEF

In the case of deauthorization or compromise of an SU, an LEF should attempt to zeroize LLE keys previously provisioned to the SU. Zeroization of LLE keys by an LEF is accomplished by means of the LLE Key Zeroization OSP which is secured with the ILEK of the SU. A domain LEF can zeroize an SUs keys for that domain. When a domain LEF zeroizes an SU’s keys, it may zeroize all keys associated with the domain, or all keys except the ILEK.

Zeroization messages are authenticated using the IMAK of the SU that is applicable to the current domain.

### Construction of Zeroization Messages

LLE Key Zeroization commands comprise 3 parts:

1. Security Key Identification: This part contains the information required to select and generate the IMAK used for authentication of the message. It comprises:
   1. Individual LLE Key Derivation Seed (SI, see section 4.1.2.3); and,
   2. Security Key Security Suite Identifier (SALG): the LLE Security Suite Identifier (LALG) of the key securing the message; and,
2. Zeroization Command Body: This part identifies the key contained in the message and comprises:
   1. Zeroization Key Scope (ZK): The Zeroization Key Scope (see section 4.1.4.1) to be applied by the SU;

1. Message Authentication Code (AUT): An authentication code for the message.

The message authentication code is computed as follows, as shown in Figure 42:

Given:

Mkey = the message authentication key derived from the key being used to secure the message, i.e., the IMAK of the SU in the domain of the LEF performing the Zeroization.

Then:

Command = ZPAD(ZK,8).

Finally:

AUT = MAC(Mkey,32,SALG,Command)



Figure , Key Zeroization Message Protection

# Example Cryptographic Operations

Editor’s Note: To be provided in a later revision.

1. All MAC PDUs for TDMA are LL encrypted subject to LLE per applicable policy. [↑](#footnote-ref-1)
2. Within the collision probability of the key derivation algorithm. [↑](#footnote-ref-2)
3. To be provided by the standardizing TR8 subcommittee. [↑](#footnote-ref-3)
4. To be provided by the standardizing TR8 subcommittee. [↑](#footnote-ref-4)
5. Or RLEK. An SU with the current RLEK can derive the CLEK. In this section, “CLEK” should be taken to mean “CLEK (or RLEK)”. [↑](#footnote-ref-5)
6. Note that Ka is a placeholder. Depending on the particular circumstances, different keys are used for authentication. [↑](#footnote-ref-6)
7. Note that no identifiers are required for working keys derived from the keys listed in the table. The subkey derivation and use is always known from context. [↑](#footnote-ref-7)
8. D: Direct mode and Transparent repeated conventional channels only [↑](#footnote-ref-8)
9. STEK/SMAK may be delivered to sites/CFNS via keyfill, but are not directly delivered to SU> [↑](#footnote-ref-9)
10. U: Individual rekeying can be used to update ILEK, but not for their initial distribution. [↑](#footnote-ref-10)
11. N/A: Not Applicable. [↑](#footnote-ref-11)
12. In this figure, and similar figures that follow, the LDID, LALG, and LKT information elements are shown to the side of the figure for the sake of legibility. They are used throughout the rest of the figure, and constitute part of the identity of each key. [↑](#footnote-ref-12)
13. Note that these figures illustrate some means for enablement etc., but are not intended to be exhaustive. [↑](#footnote-ref-13)
14. For simplicity, routine acknowledgements are not illustrated in the figure. [↑](#footnote-ref-14)