



# **TIA STANDARD**

## **Project 25**

### **Digital Land Mobile Radio- Key Fill Device (KFD) Interface Protocol**

**TIA-102.AACD-A  
(Revision of TIA-102.AACD)**

**September 2014**

**TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION**

**[tiaonline.org](http://tiaonline.org)**

This is a preview. [Click here to purchase the full publication.](#)

## NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Standards and Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Standards and Publications. Neither shall the existence of such Standards and Publications preclude their voluntary use by Non-TIA members, either domestically or internationally.

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

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

Any use of trademarks in this document are for information purposes and do not constitute an endorsement by TIA or this committee of the products or services of the company.

(From Project No. TIA-PN-102.AACD-A, formulated under the cognizance of the TIA TR-8 Mobile and Personal Private Radio Standards, TR-8.3 Subcommittee on Encryption).

Published by  
©TELECOMMUNICATIONS INDUSTRY ASSOCIATION  
Technology & Standards Department  
1320 N. Courthouse Road, Suite 200  
Arlington, VA 22201 U.S.A.

**PRICE: Please refer to current Catalog of  
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS  
AND ENGINEERING PUBLICATIONS  
or call IHS, USA and Canada  
(1-877-413-5187) International (303-397-2896)  
or search online at <http://www.tiaonline.org/standards/catalog/>**

All rights reserved  
Printed in U.S.A.

# NOTICE OF COPYRIGHT

**This document is copyrighted by the TIA.**

**Reproduction of these documents either in hard copy or soft copy (including posting on the web) is prohibited without copyright permission.** For copyright permission to reproduce portions of this document, please contact the TIA Standards Department or go to the TIA website ([www.tiaonline.org](http://www.tiaonline.org)) for details on how to request permission. Details are located at:

<http://www.tiaonline.org/standards/catalog/info.cfm#copyright>

or

Telecommunications Industry Association  
Technology & Standards Department  
1320 N. Courthouse Road, Suite 200  
Arlington, VA 22201 USA  
+1.703.907.7700

Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. For information, contact

IHS  
15 Inverness Way East  
Englewood, CO 80112-5704  
or call  
USA and Canada (1.800.525.7052)  
International (303.790.0600)



## **NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY**

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Procedures for American National Standards and TIA Engineering Committee Operating Procedures, the current and predecessor versions of which are available at <http://www.tiaonline.org/standards/ec-procedures>) TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. TIA will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

If the Document contains one or more Normative References to a document published by another organization ("other SSO") engaged in the formulation, development or publication of standards (whether designated as a standard, specification, recommendation or otherwise), whether such reference consists of mandatory, alternate or optional elements (as defined in the TIA Procedures for American National Standards) then (i) TIA disclaims any duty or obligation to search or investigate the records of any other SSO for IPR or letters of assurance relating to any such Normative Reference; (ii) TIA's policy of encouragement of voluntary disclosure (see TIA Procedures for American National Standards Annex C.1.2.3) of Essential Patent(s) and published pending patent applications shall apply; and (iii) Information as to claims of IPR in the records or publications of the other SSO shall not constitute identification to TIA of a claim of Essential Patent(s) or published pending patent applications.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NONINFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

[This is a preview. Click here to purchase the full publication.](#)



## Table of Contents

1	INTRODUCTION .....	11
1.1	Purpose.....	11
1.2	Scope.....	11
1.3	Revision History .....	11
1.4	References.....	11
1.5	Definitions, Acronyms, and Abbreviations.....	12
2	MANUAL REKEYING OVERVIEW.....	14
2.1	KFD Based Key Management.....	14
2.2	KMF Based Key Management .....	15
2.3	Manual Rekeying Features .....	15
2.3.1	Keyload .....	15
2.3.2	Key Erase.....	16
2.3.3	Erase All Keys .....	16
2.3.4	View Key Info .....	16
2.3.5	View Individual RSI .....	16
2.3.6	Load Individual RSI .....	16
2.3.7	View KMF RSI.....	16
2.3.8	Load KMF RSI.....	17
2.3.9	View MNP .....	17
2.3.10	Load MNP .....	17
2.3.11	View Keyset Info.....	17
2.3.12	Activate Keyset.....	17
2.4	Manual Rekeying Features for Authentication .....	17
2.4.1	Load Authentication Key .....	17
2.4.2	Delete Authentication Key .....	18
2.4.3	View SUID Info .....	18
2.4.4	View Active SUID Info .....	18
3	INTERFACE PROTOCOL DEFINITION .....	19
3.1	KFD-MR Interface .....	19
3.2	Physical Layer (RS232) .....	20
3.3	Physical Layer (USB) .....	20
3.4	Link Layer .....	20
3.5	Network Layer.....	20
3.6	Transport Layer.....	21
3.7	KFD Interface Protocol Application Sublayer .....	21
3.7.1	Message Format .....	21
3.7.2	Exchange Procedure.....	22
3.8	Manual Rekeying Application Sublayer.....	26
3.8.1	Keyload .....	26
3.8.2	Load Individual RSI .....	28
3.8.3	Load KMF RSI.....	29
3.8.4	Load MNP .....	30
3.8.5	Erase Keys.....	31
3.8.6	Erase All Keys .....	33

3.8.7	View Key Info .....	33
3.8.8	View Individual RSI .....	34
3.8.9	View KMF RSI.....	35
3.8.10	View MNP .....	36
3.8.11	View Keyset Info .....	37
3.8.12	Activate Keyset .....	38
3.8.13	Load Authentication Key .....	39
3.8.14	Delete Authentication Key.....	40
3.8.15	View SUID Info.....	41
3.8.16	View Active SUID Info.....	42
3.9	KMMs .....	43
3.9.1	KMM Header Definition .....	44
3.9.2	KMM Body Definitions.....	45
3.9.2.1	Change-RSI-Command .....	45
3.9.2.2	Change-RSI-Response .....	45
3.9.2.3	Changeover-Command .....	45
3.9.2.4	Changeover-Response.....	45
3.9.2.5	Inventory-Command (List Active Kset IDs).....	45
3.9.2.6	Inventory-Response (List Active Kset IDs) .....	45
3.9.2.7	Inventory-Command (List RSI Items) .....	45
3.9.2.8	Inventory-Response (List RSI Items).....	46
3.9.2.9	Inventory-Command (List Keyset Tagging Info) .....	46
3.9.2.10	Inventory-Response (List Keyset Tagging Info).....	46
3.9.2.11	Inventory-Command (List Active Keys) .....	46
3.9.2.12	Inventory-Response (List Active Keys).....	47
3.9.2.13	Inventory-Command (List MNP) .....	47
3.9.2.14	Inventory-Response (List MNP) .....	47
3.9.2.15	Inventory-Command (List KMF RSI).....	47
3.9.2.16	Inventory-Response (List KMF RSI) .....	48
3.9.2.17	Modify-Key-Command.....	48
3.9.2.18	Negative-Acknowledgment.....	50
3.9.2.19	Rekey-Acknowledgment.....	50
3.9.2.20	Zeroize-Command.....	51
3.9.2.21	Zeroize-Response .....	51
3.9.2.22	Load-Config-Command .....	51
3.9.2.23	Load-Config-Response.....	51
3.9.2.24	Unable to Decrypt Response.....	51
3.9.2.25	Load Authentication Key – Command .....	52
3.9.2.26	Load Authentication key – Response .....	54
3.9.2.27	Delete Authentication Key – Command.....	56
3.9.2.28	Delete Authentication Key-Response .....	57
3.9.2.29	Inventory-Command (List SUID Items).....	58
3.9.2.30	Inventory-Response (List SUID Items) .....	59
3.9.2.31	Inventory-Command (List Active SUID).....	60
3.9.2.32	Inventory-Response (List Active SUID) .....	60
3.9.2.33	Session Control KMM.....	61



Annex A (Normative): CRC Generation (Register & State Table) .....	63
Annex B (Normative): Three Wire Half Duplex Interface.....	66
B.1 Physical Layer (Three Wire Half Duplex Interface) .....	66
B.1.1 K/F Line Description .....	66
B.1.1.1 Sending a Key Signature .....	66
B.1.2 Keyload* Line Description .....	67
B.1.3 GND Line Description.....	67
B.2 Link Layer (4kbps Transfer Protocol) (Three Wire Half Duplex Interface).....	67
B.2.1 4kbps Transfer Protocol Byte Format.....	68
B.2.2 4kbps Transfer Protocol Flow Control .....	68
B.2.3 4kbps Transfer Protocol Line Turnaround .....	68
B.2.4 Timeout Considerations .....	69
B.2.5 Transmitting a Byte (TXBYTE) .....	70
B.2.6 Receiving a Byte (RXBYTE).....	70
B.2.7 Application Layer (3WI KFD Interface Protocol) .....	70
B.2.7.1 KFD Interface Protocol OPCODES .....	71
B.2.7.2 KMM Frame .....	72
B.2.7.2.1 Length.....	73
B.2.7.2.2 Control .....	73
B.2.7.2.3 Destination RSI.....	73
B.2.7.2.4 Body.....	73
B.2.7.2.4.1 Body-Esync Block Format.....	74
B.2.7.2.4.2 KMM .....	74
B.2.7.2.5 CRC .....	74
B.2.7.3 Exchange Procedure .....	74
B.2.8 Application Layer (Manual Rekeying Application) .....	76
B.2.8.1 Keyload.....	76
B.2.8.2 Load Individual RSI.....	78
B.2.8.3 Load KMF RSI .....	79
B.2.8.4 Load MNP .....	80
B.2.8.5 Erase Keys .....	82
B.2.8.6 Erase All Keys .....	83
B.2.8.7 View Key Info .....	84
B.2.8.8 View Individual RSI .....	85
B.2.8.9 View KMF RSI .....	86
B.2.8.10 View MNP .....	87
B.2.8.11 View Keyset Info .....	88
B.2.8.12 Activate Keyset .....	90
B.2.8.13 Load Authentication Key .....	91
B.2.8.14 Delete Authentication Key.....	92
B.2.8.15 View SUID Info .....	93
B.2.8.16 View Active SUID Info.....	94

## Figures

Figure 1.KFD-MR Protocol Stack (RS232) .....	19
Figure 2.KFD-MR Protocol Stack (Three Wire Half Duplex Interface) .....	20
Figure 3.KFD-MR Protocol Stack (USB).....	20
Figure 4.Data Link Independent KMM Datagram .....	22
Figure 5.Exchange Session defined by the KFD- Interface Protocol .....	25
Figure 6.Exchange Session for the Keyload feature.....	27
Figure 7.Exchange Session for the Load Individual RSI feature .....	29
Figure 8.Exchange Session for the Load KMF RSI feature .....	30
Figure 9.Exchange Session for the Load MNP feature.....	31
Figure 10.Exchange Session for the Erase Keys feature .....	32
Figure 11.Exchange Session for the Erase All Keys feature .....	33
Figure 12.Exchange Session for the View Key Info feature.....	34
Figure 13.Exchange Session for the View Individual RSI feature.....	35
Figure 14.Exchange Session for the View KMF RSI feature .....	36
Figure 15.Exchange Session for the View MNP feature.....	37
Figure 16.Exchange Session for the View Keyset Info feature .....	38
Figure 17.Exchange Session for the Activate Keyset feature .....	39
Figure 18.Exchange Session for the Load Authentication Key feature .....	40
Figure 19.Exchange Session for the Delete Authentication Key feature .....	41
Figure 20.Exchange Session for the View SUID Info feature .....	42
Figure 21.Exchange Session for the View Active SUID Info feature.....	43
Figure 22.Shift Register Depiction of the CRC Generation.....	63
Figure 23.State Table for CRC Generator Shift Register.....	64
Figure 24.KFD Physical Interface Lines (Three Wire Half Duplex Interface) .....	66
Figure 25.Sending a Key Signature (Three Wire Half Duplex Interface) .....	67
Figure 26.Anatomy of a Byte (Three Wire Half Duplex Interface).....	68
Figure 27.Timeout Values (Three Wire Half Duplex Interface) .....	69
Figure 28.KMM Frame Header Format.....	72
Figure 29.3WI Exchange Session defined by the KFD- Interface Protocol.....	75
Figure 30.3WI Exchange Session for the Keyload feature .....	77
Figure 31.3WI Exchange Session for the Load Individual RSI feature .....	79
Figure 32.3WI Exchange Session for the Load KMF RSI feature.....	80
Figure 33.3WI Exchange Session for the Load MNP feature .....	81
Figure 34.3WI Exchange Session for the Erase Keys feature .....	83
Figure 35.3WI Exchange Session for the Erase All Keys feature .....	84
Figure 36.3WI Exchange Session for the View Key Info feature .....	85
Figure 37.3WI Exchange Session for the View Individual RSI feature .....	86
Figure 38.3WI Exchange Session for the View KMF RSI feature .....	87
Figure 39.3WI Exchange Session for the View MNP feature.....	88
Figure 40.3WI Exchange Session for the View Keyset Info feature.....	89
Figure 41.3WI Exchange Session for the Activate Keyset feature.....	90
Figure 42.3WI Exchange Session for the Load Authentication Key feature .....	91
Figure 43.3WI Exchange Session for the Delete Authentication Key feature .....	92
Figure 44.3WI Exchange Session for the View SUID Info feature .....	94

Figure 45.3WI Exchange Session for the View Active SUID Info feature.....	95
---	----