Application Note

AEROFLEX
A passion for performance.

Using the IFR 2975 for Advanced Project 25 Keyloading Capabilities and AES/DES Encryption

by Rob Barden

Secure communications are vital to national security interests and are of paramount importance to police and federal agencies throughout the world.

The use of encryption allows users to transmit traffic (either voice or data) across the air with minimal chance of unintended observers capturing the transferred information and monitoring voice or data information in a communications network. Gone are the days where a police scanner can pick up analog transmissions and various (unauthorized) users can listen in to law enforcement or other private communications. This has become a mission critical component in the fight against terrorism and advanced encryption systems like AES are being deployed in P25 digital wireless communication systems.

The P25 standard calls out specific modes of operation for loading encryption keys into radios and then managing those keys through an external Key Fill Device. These devices are not specific to any manufacturer however Motorola is currently supporting the market with the KVL-3000+™ Keyloader.

Encryption of the P25 traffic and control channels are well defined in the TIA/EIA-102 specification, specifically in TIA/EIA-102-AAAA and TIA/EIA-102-AAAD for which DES and AES (respectively) encryption are defined. AES or Advanced Encryption System, which is further described in the FIPS 197 AES standard, provides a 256 bit key for encryption, where DES, or Digital Encryption System utilizes a 64 bit key. Obviously, the larger the bit sequence used for the encryption key, the tougher it is to crack the code and the higher the transmission security.

Understanding Encryption

Encryption keys can be viewed as the "key" to unlocking the secure communication "safe". The key is the single most important aspect of the secure communication system. If you compromise the key, you compromise your communications. That is why key management within a secure organization is critical to the success of their cryptographic system. Within the P25 standard, the key used to encrypt data is called the TEK or Traffic Encryption Key.

Modern encryption systems almost exclusively apply to digital transmission where voice information is turned into data and the digital "ones" and "zeros" being transmitted can be easily encrypted without any degradation of the transmission. Older, analog encryption systems utilized voice scramblers that provided marginal security and poor voice quality. The P25 standard (Phase I) utilizes an IMBE vocoder that digitizes the voice information for transmission over the air, allowing for the voice information to be treated as "data". A simple diagram of how an encryption/decryption system works is shown in figure 1.0.

The key is the item that first sets the process in place. The length of the key along with the encryption type determines the strength of the security. The larger the key (in bits) the more protection it provides to the communication path. The key used to encrypt the data is also used to decrypt.

The P25 encryption systems take this approach a step further. Instead of directly encrypting the clear data, the DES and AES algorithms generate encryption blocks that are exclusively-or'ed with the clear data to produce encrypted data. The advantage of this process is that less overhead processing is required to encrypt the clear data and the same encryption algorithm can be used to decrypt the information as is used to encrypt the desired secure data. To accomplish this, a LFSR or Linear Feedback Shift Register, which is essentially a pseudo-random function generator, is utilized. The LFSR creates a MI or Message Indicator, which is used to synchronize the encryption process. Figure 2.0 shows the use of the LFSR in an encryption system.

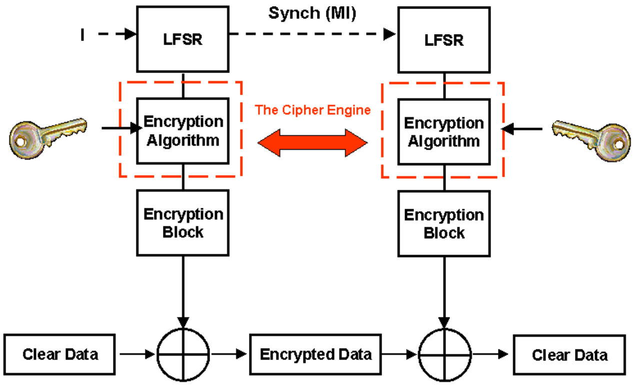


Figure 2.0 Encryption System using Linear Feedback Shift Register

As you can see, the LFSR generates synchronization between the encryption engines. Since the same process is used on both ends, there is no longer a requirement for a decryption engine. They both generate the same encryption block with the same key. The synchronization is the MI and since it is a polynomial driven shift register, it is constantly changing. For the P25 standard, it changes at the super-frame rate of the traffic channel or every 360 ms.

In the P25 standard, the MI is sent in the header data unit before the start of the traffic LDU1 or Logical Data Unit Link and LDU2 frames that comprise the P25 super-frame. It is also sent during

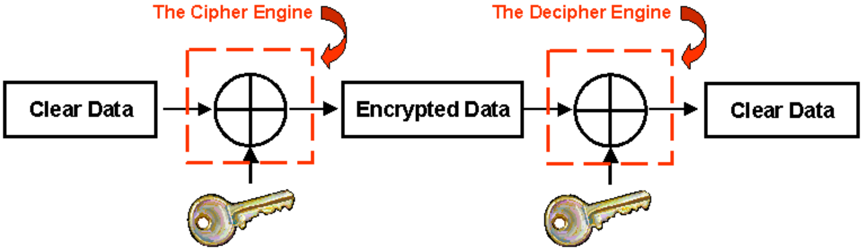


Figure 1.0 The Encryption Process

the LDU2 frame in the ES or Encryption Synch portion that proceeds each voice frame within the LDU2. When matched with the proper key, the output of the encryption algorithm produces the same encryption block that is then exclusive-or'ed with either the clear data to produce encrypted data, or encrypted data to produce clear data.

Remember that during this process, the Key is never transmitted over the air. The key is identified by its KID or Key ID, which is sent in the header data unit and as part of the ES portion of LDU2. This KID is a reference look up that the RFSS or Radio Frequency Sub-System and the portable unit use to identify the proper key to use. Along with the KID, an ALGID or Algorithm ID, is also sent to denote the type of encryption being utilized. DES and AES use ALGID codes of 81 (hex) and 84 (hex) respectively. Figure 3.0 shows how the MI, ALGID and KID are mapped into the P25 super-frame.

Differences Between DES and AES

Encryption systems use a defined algorithm (AES, as an example) to process the digital information with the key to produce an encrypted output. These algorithms or "Cipher Engines" as they are often referred to, use a variety of methods to protect the data. The AES standard uses the Rijndael Algorithm processing 128 bits of clear data at a time and both AES and the DES standard used in P25 utilize Output Feedback or OFB techniques. These algorithms are not limited to P25 use exclusively. Any data source can be encrypted using these standards.

The AES standard can use key lengths of 128 bits, 196 bits or 256 bits. P25 only specifies use of a 256 bit key. The DES standard uses a 56 bit key length with 8 bits of parity for a total of 64 bits. The P25 standard for AES uses 256 bits and thus, is much more robust than DES in protecting data. Since the AES standard processes 128 bits of user information (clear data), then encrypts with a 256 bit key, the output is highly secure.

For the purposes of this application note, we will not delve into the actual encryption process as this can be readily viewed by obtaining the FIPS-197 encryption standard. Associated parameters for AES are available at the CSOR or Computer Security Objects Register , located at http://csrc.nist.gov/csor.

The Key Fill Device: The KVL-3000+™ Versus Earlier Key Variable Loaders

Many users currently employ different KFD or Key Fill Device products manufactured primarily by Motorola. Motorola has marketed these devices as KVL's or Key Variable Loaders. It is important to understand that most older KVL's produced by Motorola utilized a proprietary mode of operation to transfer the "key" to the radio for use in the field or for testing purposes. Most KVL's, including the KVL-3000™, utilize a mode of operation known as ASN for transferring key information to the radio. This is a proprietary information transfer process licensable from Motorola. The IFR 2975, at this time, does not support the older ASN mode of key transfer.

Within the P25 standards committee, there is currently a standard in development that will become TIA/EIA-102 AACD which deals specifically with the interface for a P25 open standard KFD. The Motorola KVL-3000+™ is the first key-loader to conform to this specification as well as legacy support for the ASN mode. At the time of this writing, this standard is currently in the ballot stage and the IFR 2975 can be used with the KVL-3000+™.

Methods of Loading Encryption Keys in Radios

Currently, the primary method of loading encryption keys into the radio involves using a KFD connected to the radio through a specialized cable that interfaces the KFD to the radio. The KFD is used to create and then load the key into the radio. In no instance is the radio used to create a key. This is always done from an external source. A single key or a group of keys can be loaded and also erased using the KFD.

An alternative method of loading keys into a radio involves a process called OTAR or Over-The-Air-Rekeying. This process involves the actual transfer of keys over the air to the radio using a specialized key called the KEK or Key Encryption Key. This allows the system to set up periodic rekeying of radios or groups of radios so that a continuously rotating key structure is introduced to the user base, thus further minimizing any compromise of the secure communication system. It also allows for emergency rekeying in the event of a security breach.

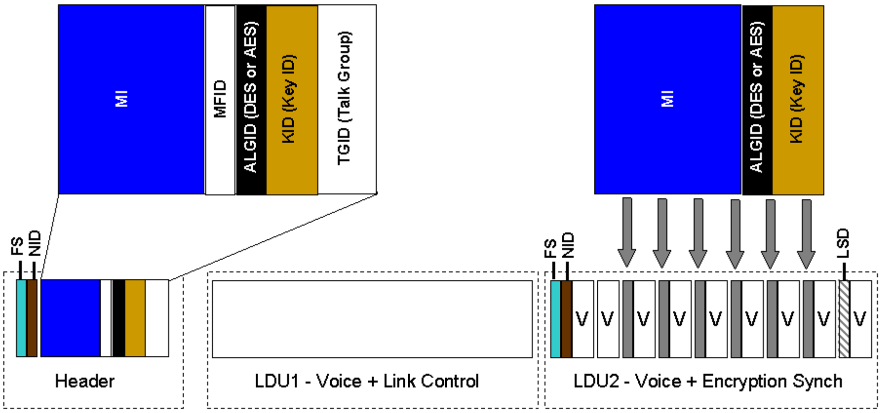


Figure 3.0 The P25 Super-frame and Mapping of the MI, ALGID and KID (Error Correction Coding not shown).

Why Do We Test With Real Keys?

Although it is not necessary to test a radio with a real key loaded, it is desirable at times to test radios using a "live" situation to isolate potential problems in the key loading process and to verify voice reproduction quality.

The actual parametric measurements (Power, Frequency Error, Modulation Accuracy, etc…) can be performed in clear mode, with a test key or with a live key with no impact on the accuracy of the measurements.

Configuring The IFR 2975 for AES and KVL-3000+™ Support

The IFR 2975, with the proper options, supports any KFD conforming to the P25 TIA/EIA-102-AACD standard. Aeroflex is licensed by Motorola to provide support for the KVL-3000+™. The IFR 2975 provides two modes of operation to load a key into the IFR 2975 and the radio under test to verify encrypted operation using either a DES or AES key.

To enable the IFR 2975 to provide Keyloader support, option number IFR2975OPT12 should be purchased from Aeroflex. To add support for AES, IFR2975OPT10 should be purchased. DES is provided as a standard feature on the IFR 2975. Call 1-800-835-2352, or go to our web site at www.aeroflex.com for more information. These options do not require that your IFR 2975 be returned to Aeroflex for upgrade, as the option can be loaded with a simple software download. These downloads are exclusive to the serial number of the IFR 2975 to be loaded and are available only to users in the United States and Canada.

Important Note: An AES enabled IFR 2975 cannot be exported without explicit consent from the appropriate US Government Agencies.

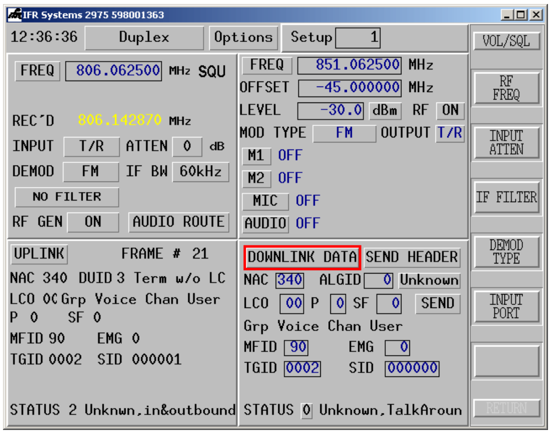
Note: Since the AES algorithm itself is encrypted, the software installation time for this option takes more time than other software enabled options.

If your IFR 2975 has not been previously enabled to provide AES and Keyloader support, you can install the option in the field by calling Aeroflex at 1-800-835-2352.

Loading and Managing Encryption Keys with the IFR 2975

The IFR 2975 with option IFR2975OPT12 allows the user to connect a KVL-3000+™ and load keys directly into the IFR 2975. Keys can also be loaded into the IFR 2975 manually.

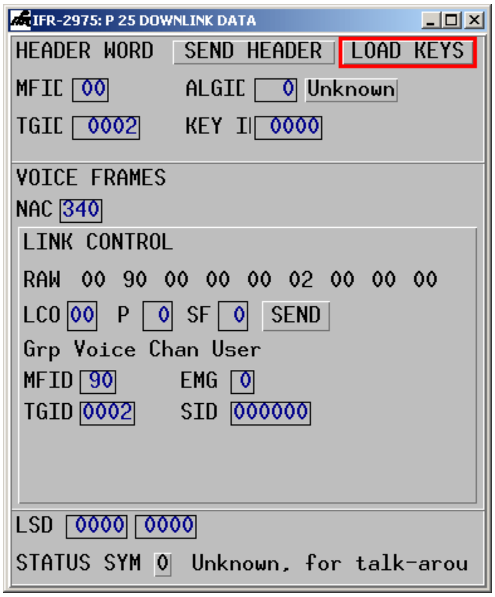
Figure 4.0 shows the initial screen to control and manage keys with the IFR 2975.



```
IFR Systems 2975 598001363
12:36:36   Duplex   Options   Setup 1

FREQ 806.062500 MHz SQU
REC´D 806.142870 MHz
INPUT T/R   ATTEN 0 dB
DEMOD FM    IF BW 60kHz
NO FILTER
RF GEN ON   AUDIO ROUTE

FREQ 851.062500 MHz
OFFSET -45.000000 MHz
LEVEL -30.0 dBm   RF ON
MOD TYPE FM   OUTPUT T/R
M1 OFF
M2 OFF
MIC OFF
AUDIO OFF

UPLINK          FRAME # 21
NAC 340  DUID 3 Term w/o LC
LCO 0C Grp Voice Chan User
P 0     SF 0
MFID 90     EMG 0
TGID 0002   SID 000001
STATUS 2 Unknwn,in&outbound

DOWNLINK DATA   SEND HEADER
NAC 340   ALGID 0 Unknown
LCO 00 P 0 SF 0   SEND
Grp Voice Chan User
MFID 90       EMG 0
TGID 0002     SID 000000
STATUS 0 Unknown,TalkAroun
```

Figure 4.0 The IFR 2975 P25 Uplink and Downlink Data Tiles

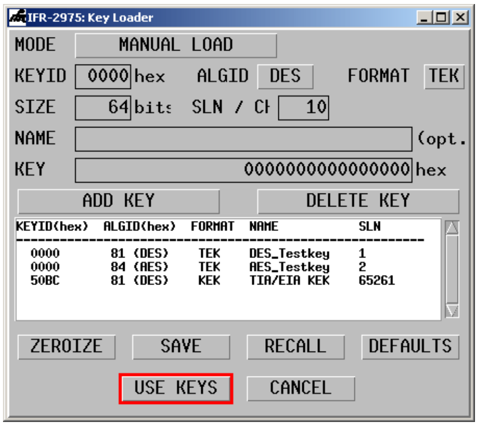
As you can see, the IFR 2975 is initially set in the DUPLEX mode with the P25 Uplink and Downlink Data tiles enabled. This is due to the fact that encryption is done at the traffic channel level and this setup is the primary traffic channel configuration area for the IFR 2975. By selecting the DOWNLINK DATA button on the lower right hand tile, the IFR 2975 will expand the P25 Down Link Data tile as shown in figure 5.0.



```
IFR-2975: P 25 DOWNLINK DATA
HEADER WORD   SEND HEADER   LOAD KEYS
MFIC 00        ALGIC 0 Unknown
TGIC 0002      KEY II 0000

VOICE FRAMES
NAC 340
LINK CONTROL
RAW  00 90 00 00 00 02 00 00 00
LCO 00  P 0  SF 0  SEND
Grp Voice Chan User
MFID 90       EMG 0
TGID 0002     SID 000000

LSD 0000 0000
STATUS SYM 0  Unknown, for talk-arou
```

Figure 5.0 Expanding the IFR 2975 P25 Downlink Data Tile

From this screen, the key loading function of the IFR 2975 can be accessed. Selecting the "Load Keys" button directs the IFR 2975 to the main key loading location as shown in figure 6.0.



IFR-2975: Key Loader

MODE: MANUAL LOAD

KEYID 0000 hex ALGID DES FORMAT TEK

SIZE 64 bit: SLN / Cł 10

NAME (opt.

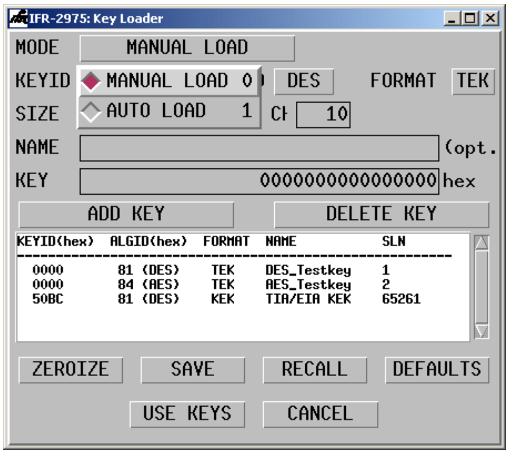
KEY 0000000000000000 hex

KEYID(hex)	ALGID(hex)	FORMAT	NAME	SLN
0000	81 (DES)	TEK	DES_Testkey	1
0000	84 (AES)	TEK	AES_Testkey	2
50BC	81 (DES)	KEK	TIA/EIA KEK	65261

Figure 6.0 The IFR 2975's primary key loading screen

From this screen, the IFR 2975 can load keys, create keys and store keys, as well as set up the interface for using an actual DES or AES key in the test process. The first decision the user needs to make is whether to manually load a key into the IFR 2975 or to Auto Load a key using the KVL-3000+™.

Figure 7.0 shows how to select either the manual or Auto Load modes.



IFR-2975: Key Loader

MODE: MANUAL LOAD

KEYID ◆ MANUAL LOAD 0 DES FORMAT TEK

SIZE ◇ AUTO LOAD 1 Cł 10

NAME (opt.

KEY 0000000000000000 hex

KEYID(hex)	ALGID(hex)	FORMAT	NAME	SLN
0000	81 (DES)	TEK	DES_Testkey	1
0000	84 (AES)	TEK	AES_Testkey	2
50BC	81 (DES)	KEK	TIA/EIA KEK	65261

Figure 7.0 Selecting Manual or Auto Load

If Auto Load Mode is selected, the IFR 2975 will prompt the user to connect the KVL device to the front test port of the IFR 2975 as shown in figure 8.0. Aeroflex supplies the required interface cable when IFR2975OPT12 is purchased as an option.

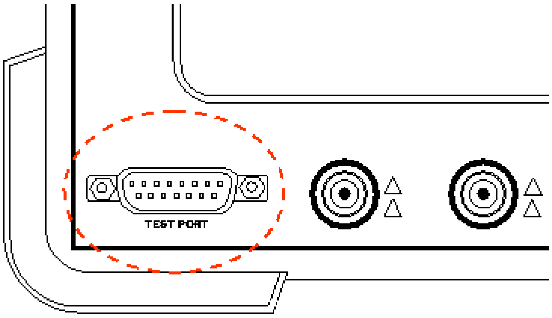
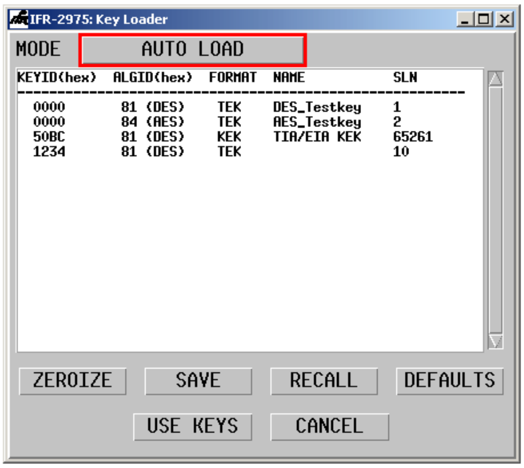


Figure 8.0 The IFR 2975 KFD Test Port on the front of the instrument

Once the KVL-3000+™ is connected to the IFR 2975 test port, keys can be loaded directly into the IFR 2975 just like a radio. As keys are added, the unit automatically displays the keys loaded. The IFR 2975 comes with standard TEK or Test Traffic Keys for DES and AES, as specified by the standard as well as the standard KEK or Key Encryption Key . Figure 9.0 shows the Auto Load mode of the IFR 2975. Notice that the key values are not displayed for security.



IFR-2975: Key Loader

MODE: AUTO LOAD

KEYID(hex)	ALGID(hex)	FORMAT	NAME	SLN
0000	81 (DES)	TEK	DES_Testkey	1
0000	84 (AES)	TEK	AES_Testkey	2
50BC	81 (DES)	KEK	TIA/EIA KEK	65261
1234	81 (DES)	TEK		10

Figure 9.0 The Auto Load mode of the IFR 2975

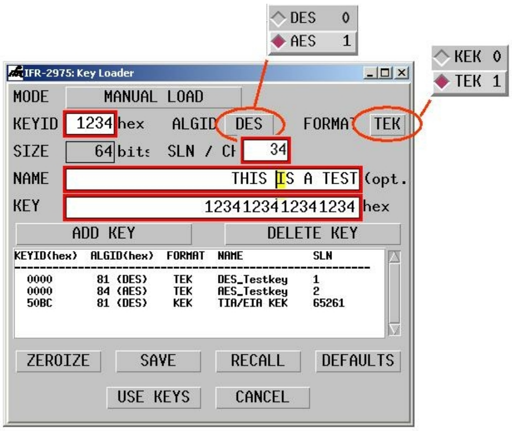
All the test keys plus the newly loaded key from the KVL-3000+™(1234) are now present.

Keys can also be loaded manually. Simply select the Manual Load mode, where entry of the Key ID information, the encryption type (DES or AES), whether it is a TEK or KEK, and the SLN can be accomplished.

The SLN/CKR or Storage Location Number/Common Key Reference refers to the location established in the radio for the use of a particular key on a particular channel. The valid range for TEKs are 1-4095 and 61440-65535 for KEKs.

The SLN within the IFR 2975 is a reference and is not broadcast over the air to the radio. It is possible to establish a Key and KID within the radio with one SLN and establish the same Key and KID and a different SLN on the IFR 2975 and the radio will still decrypt the incoming data. This is due to the fact that the radio is looking for the proper programmed KID for the particular channel regardless of the SLN. It is recommended that the user set up the same SLN in the IFR 2975 as is used in the radio to keep continuity with the programming of the radio. One of the strengths of the IFR 2975 is that multiple key-sets can be stored in the instrument for different key configuration profiles.

Figure 10.0 shows how to enter the Key, Key ID and SLN selecting either DES or AES encryption and how to select the type of key format, either TEK or KEK.


IFR-2975: Key Loader

MODE: MANUAL LOAD
KEYID: 1234 hex
ALGID: DES
FORMAT: TEK
SIZE: 64 bits
SLN / CH: 34
NAME: THIS IS A TEST (opt.
KEY: 1234123412341234 hex

```
KEYID(hex)  ALGID(hex)  FORMAT  NAME          SLN
---------------------------------------------------
  0000       81 (DES)    TEK    DES_Testkey   1
  0000       84 (AES)    TEK    AES_Testkey   2
  50BC       81 (DES)    KEK    TIA/EIA KEK   65261
```

◇ DES 0
◆ AES 1

◇ KEK 0
◆ TEK 1

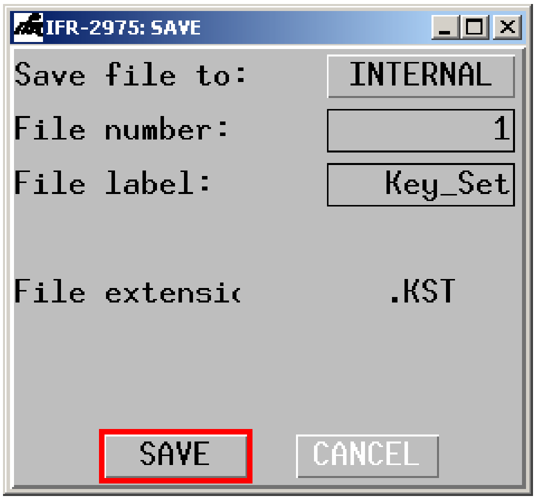
Figure 10.0 Setting up Encryption Key Parameters on the IFR 2975

Once the key has been configured, the user has the options of leaving the keys in volatile RAM so that keys are not stored on the IFR 2975's internal hard-drive or the user can save the Key Set to the hard-drive.

In either instance, the first step is to add the key to the Key Set. This is accomplished by selecting the Add Key button. To delete a key, simply select the Delete Key.

If the decision is made not to save the Key Set to the hard-drive, those keys will "go away" if there is an interruption of power to the unit. Conversely, the user can save the Key Set to the IFR 2975's internal hard-drive where they reside until the user deletes the Key Set. To add security to keys stored internally, the IFR 2975 encrypts each key using a standard DES encryption with an Aeroflex proprietary key.

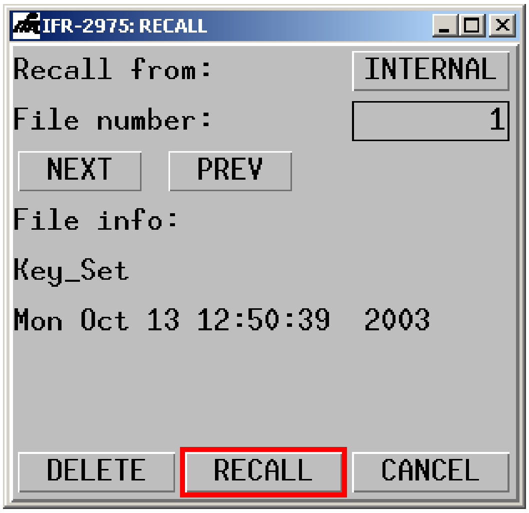
To save the Key Set to the internal hard-drive, simply click on the "Save" button and the IFR 2975 will prompt you to specify the file number and label for the Key Set as shown in figure 11.0.


IFR-2975: SAVE

Save file to: INTERNAL
File number: 1
File label: Key_Set
File extensic .KST

Figure 11.0 Saving a Key Set

If there is an existing Key Set file associated with that number, the IFR 2975 will prompt you whether you want to replace that Key Set with the new Key Set. Once the Key Set is saved, you can then recall that Key Set or any other stored Key Set using the Recall button. The recall function also provides you with the ability to delete Key Sets stored on the hard-drive as shown in figure 12.0.

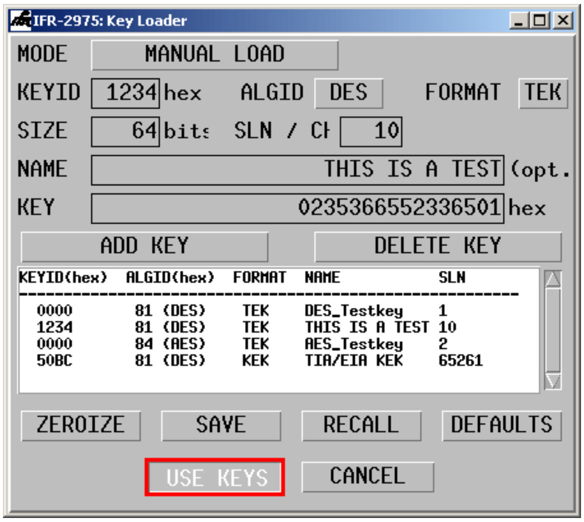

IFR-2975: RECALL

Recall from: INTERNAL
File number: 1
File info:
Key_Set
Mon Oct 13 12:50:39 2003

Figure 12.0 The Recall and Delete Key Set Function

To erase all the keys in use, the IFR 2975 provides the user with a "Zeroize" function. This function allows the user to completely erase all keys currently loaded into the IFR 2975. If the user wishes to restore the default test keys discussed earlier, selecting the defaults button will restore these keys for use.

The user should be aware that the IFR 2975 uses a two-stage process to load keys. The first process is the loading of the key into the IFR 2975's RAM memory or the hard-drive. The second process is where the IFR 2975 downloads the key to the physical layer for use in an actual transmission or reception. This is accomplished by depressing the "Use Keys" button as shown in figure 13.0.



IFR-2975: Key Loader

MODE MANUAL LOAD
KEYID 1234 hex ALGID DES FORMAT TEK
SIZE 64 bits SLN / CI 10
NAME THIS IS A TEST (opt.
KEY 0235366552336501 hex

```
KEYID(hex)  ALGID(hex)  FORMAT  NAME            SLN
---------------------------------------------------------
  0000        81 (DES)    TEK     DES_Testkey     1
  1234        81 (DES)    TEK     THIS IS A TEST  10
  0000        84 (AES)    TEK     AES_Testkey     2
  50BC        81 (DES)    KEK     TIA/EIA KEK     65261
```

Figure 13.0 Loading keys using the Load Key function

Testing Radios on the IFR 2975 with a DES/AES Key Loaded

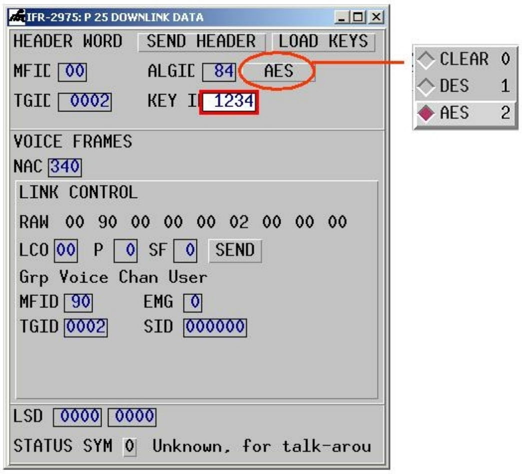
Once the "Use Keys" button has been selected, the keys are now available for use. These include all the keys, not just one specific key. Now the user can test a radio with either a test key or a "Live" key. It also means that the IFR 2975 can move between DES and AES encryption on the fly, allowing testers to quickly check operation of differently configured channels. This will greatly enhance testing of mobiles designed to inter-operate between different organizations or agencies using different encryption modes.

To start testing the radio, make sure that the proper Key ID for the channel under test is utilized. If all the channels use the same Key ID, then things are relatively easy. If they do not, make sure that the Key ID matches the expected Key ID for the channel being tested. Remember that the proper use of the SLN in the Key Set provides the user with a convenient look up reference to match to the radio's programming.

Once the "Use Keys" button has been selected, the Key Loader screen will disappear and the P25 Down Link Data tile comes back, now enabled for use with the keys that have been loaded.

The P25 Down Link Data tile allows the user to select the type of encryption to be used for the transmission. By selecting the clear mode, Algorithm ID 80 (hex) becomes the ALGID in the header and Encryption Synch portion of the P25 LDU 2 and the mobile knows to treat the data as clear data with no encryption.

If DES is selected, Algorithm ID 81 is utilized and if AES is chosen, Algorithm ID 84 is used. Once the algorithm has been selected, the Key ID to be used can be entered. This will set up the actual encryption key to be used for that channel. Figure 14.0 shows that Key ID 1234 and the AES algorithm is being utilized.



IFR-2975: P 25 DOWNLINK DATA

HEADER WORD
MFIC 00 ALGIC 84 AES
TGIC 0002 KEY I 1234

VOICE FRAMES
NAC 340
LINK CONTROL
RAW 00 90 00 00 00 02 00 00 00
LCO 00 P 0 SF 0
Grp Voice Chan User
MFID 90 EMG 0
TGID 0002 SID 000000

LSD 0000 0000
STATUS SYM 0 Unknown, for talk-arou

◇ CLEAR 0
◇ DES 1
◆ AES 2

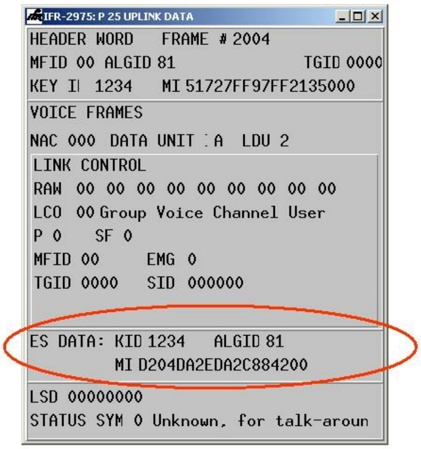
Figure 14.0 The P25 Down Link Data Tile showing AES and Key ID fields

Once the Key ID and ALGID is selected, the traffic channel - either a conventional channel or a trunked traffic channel - is now encrypted from the IFR 2975 to the radio. All the P25 patterns including the 1011, Calibration, Silence and Speech are now encrypted for use in communicating to the radio. Also, any voice data from the microphone will be encrypted. The standard test patterns, however, cannot be encrypted since they need to be "bit" exact.

To receive encrypted data from the radio, select the expanded P25 Uplink Data tile. This is done by selecting the "Uplink" button on the minimized P25 Uplink Data tile. Once this is expanded, the user will be able to see the decoded ALGID, Key ID and the MI from the radio. Remember that the MI is initialized at the start of every P25 super-frame so the MI depicted will change or "Roll" approximately 3 times per second (360 ms per super-frame).

If the MI is not rolling, then the IFR 2975 is not decoding the received data correctly. If this is the case, the radio may be in a "Clear" mode or the Key ID is not matched. The user will also not be able to hear decrypted voice data from the radio.

Figure 15.0 shows the IFR 2975's P25 Uplink Data tile indicating the Key ID, ALGID and the MI vector currently being decoded.



```
HEADER WORD   FRAME # 2004
MFID 00 ALGID 81              TGID 0000
KEY II  1234   MI 51727FF97FF2135000
VOICE FRAMES
NAC 000  DATA UNIT :A  LDU 2
LINK CONTROL
RAW  00 00 00 00 00 00 00 00 00
LCO  00 Group Voice Channel User
P 0    SF 0
MFID 00      EMG  0
TGID 0000    SID  000000

ES DATA: KID 1234    ALGID 81
         MI D204DA2EDA2C884200
LSD 00000000
STATUS SYM 0 Unknown, for talk-aroun
```

Figure 15.0 The P25 Uplink Data tile showing encryption parameter

Summary

Encryption is becoming an important feature in keeping vital communications secure. The IFR 2975 has the industry's most extensive support for loading and managing keys for use in testing radio systems utilizing secure communications with either the DES or AES standard. The ability to load and manage individual and multiple keys, plus the IFR 2975's ability to track keys easily allows the user to quickly and accurately test P25 radio systems.

CHINA
Tel: [+86] (21) 6282 8001
Fax: [+86] (21) 6282 8002

EUROPE
Tel: [+44] (0) 1438 742200
Fax: [+44] (0) 1438 727601

FRANCE
Tel: [+33] 1 60 79 96 00
Fax: [+33] 1 60 77 69 22

HONG KONG
Tel: [+852] 2832 7988
Fax: [+852] 2834 5364

SCANDINAVIA
Tel: [+45] 9614 0045
Fax: [+45] 9614 0047

SPAIN
Tel: [+34] (91) 640 11 34
Fax: [+34] (91) 640 06 40

UNITED KINGDOM
Tel: [+44] (0) 1438 742200
Toll Free: [+44] (0800) 282 388 (UK only)
Fax: [+44] (0) 1438 727601

USA
Tel: [+1] (316) 522 4981
Toll Free: [+1] (800) 835 2352 (US only)
Fax: [+1] (316) 522 1360

AEROFLEX
A passion for performance.

As we are always seeking to improve our products, the information in this document gives only a general indication of the product capacity, performance and suitability, none of which shall form part of any contract. We reserve the right to make design changes without notice. All trademarks are acknowledged. Parent company Aeroflex, Inc. ©Aeroflex 2003.

www.aeroflex.com

info-test@aeroflex.com

Our passion for performance is defined by three attributes represented by these three icons: solution-minded, performance-driven and customer-focused.