14 March 2006
First Draft

Motorola Two-Way Encryption Products and Protocols

Disclaimer

There is no document from Motorola that details all of the information contained in this article. Whether it be radio service manuals, RSS/CPS help files or keyloader operators manuals, you will not be able to find this information in one place. I have attempted to compile all of the posts on encryption from batlabs (http://www.batlabs.com) plus the information contained in other manuals into a single document. This is certainly not 100% technically accurate, but I've made a reasonable attempt to ensure the information presented is correct. Corrections and additional information are gladly welcomed and appreciated and may be sent to me in confidence on http://batboard.batlabs.com via private message to "batdude". This will become a living document that I'll upgrade over time, so check the date in the upper right hand corner to make sure you have the most recent copy. Another document has been generated to catalog most of the Motorola secure modules that exist for Motorola two-way radios. Formatted in Microsoft Excel, can be viewed and/or downloaded at http://members.aol.com/batlabsdotcom/secure_modules.xls. Please note that there are plenty of copyrighted terms in this document – all of which are property of Motorola, Inc.

Introduction

Secure radios and infrastructure are nothing new for Motorola. Beginning in the era of the Expo and MX300, Motorola's digital encryption gained a majority share of the market for those customers with the money to invest in the subscriber equipment and infrastructure required to support digital encryption. Over 10 years ago, I wrote a fairly simple article that provided a method to explain what I knew about Motorola encryption products. It has some errors, but I think it was fairly well received and is still available: http://www.radioreference.com/trunked/stuff/encrypt.html. At the time, this was a pretty good description of Motorola two-way encryption products and protocols but technology has changed significantly since I wrote the original article. Most of the basics still apply, but it's seriously lacking in that it doesn't even touch on Astro products. Realizing the need to update the information in the original document, I have written this one. This document replaces the original in its entirety.

One aspect of encryption that wasn't touched on in the original article is the role of the National Institute of Stanards and Technology (NIST) (http://www.nist.gov). NIST certifies all public use encryption products using government standards known as "FIPS", or Federal Information Processing Standards. The five FIPS that are most pertinent to this document are:

- FIPS 46-2 (http://www.itl.nist.gov/fipspubs/fip46-2.htm)
- FIPS 81 (http://www.itl.nist.gov/fipspubs/fip81.htm)
- FIPS 140-1 (http://www.itl.nist.gov/fipspubs/fip140-1.htm)
- FIPS 140-2 (http://csrc.nist.gov/cryptval/140-2.htm)
- FIPS 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

There are many other documents that provide good information on the NIST website but are beyond the scope of this document (and probably some that I've missed). I encourage you to visit their website to review some of the history behind the products that are discussed in this article.

Motorola SECURENET^{TM}

Although there are still some non-digital encryption devices still in use, including simple speech inversion products, the majority of devices currently in use are of the digital variety. Motorola voice privacy is referred to simply as "SECURENET", which is a trademarked term that Motorola uses to identify their digital encryption products. There are five different basic encryption protocols, two of which have distinct variations, for a total of eight unique (and non-compatible) encryption protocols. They are (in no particular order): DVP, DVP-XL, DES, DES-XL, DES-OFB, DVI-XL, ADP and AES-256. Each of the eight protocols use a field inserted "key", which is what makes the communications secure. It's a simple concept – without the proper encryption key loaded into your radio to decrypt the inbound audio, you will not be able to hear intelligible radio traffic. Starting with plain analog FM wideband voice – **NOT** Astro VSELP or IMBE digital voice – the DVP and DES algorithms convert the analog carrier (i.e. voice) to digital using a technique known as CVSD (Continuously Variable Slope Delta) modulation with a sample rate of 12kbps. (Don't ask – beyond the scope of this document) This digital bit stream is then sent to the cryptographic module for encryption and finally to the PA circuitry for transmission. This end-to-end process from analog voice to digitization to transmission and back is now known as "12kbps Analog Securenet" and sounds like white noise (open squelch) with a faint beep at the end of the transmission (i.e. SSSSSHHHHHHHHHHHHHH…beep) Keep in mind that all radios must use the exact same type of encryption to intercommunicate in the secure mode (DVP-DVP, DES-XL-DES-XL, etc.), with one notable exception: DES-XL radios are capable of software configuration to disable their "-XL" features, enabling them to communicate with non-XL DES equipped radios.

The Original, DVP^{TM}

DVP was a term that Motorola used for their initial entry into the digital voice encryption product market and is a proprietary protocol that utilizes the CVSD modulation scheme previously discussed. Depending on who you ask and which book your read, the acronym DVP can have two different breakdowns: Digital Voice Privacy or Digital Voice Protection (both refer to the same thing – first generation Securenet products). DVP uses a self-synchronizing encryption technique known as cipher feedback (CFB). The basic DVP algorithm is capable of 2.36×10^{21} different "keys" based on a key length of 32 bits. There are many different patents discussing voice privacy techniques, but I think this one from 1972 best describes DVP (even though DVP is not used to describe it): http://www.freepatentsonline.com/3639690.pdf. Another document that does specifically discuss DVP can be accessed at:

http://www.freepatentsonline.com/4167700.pdf. The first-generation DVP protocol and associated infrastructure equipment is no longer supported by Motorola.

The Data Encryption Standard (DES)

In the middle 1970's, the federal government standardized all federal agencies on a common encryption protocol to protect sensitive (unclassified) data. Several different schemes were proposed, but the one approved by the National Bureau of Standards was a protocol that became the Data Encryption Standard, or DES. Broaden your mind for just a minute and forget about radio traffic. There are several other forms of communication and data that must be protected from prying eyes (and ears). IRS records, Federal Banking data, etc. are not "classified" in the military sense, but require protection from eavesdropping. The Data Encryption Standard, once standardized, allowed all federal agencies to use the same encryption protocol and intercommunicate when and if the need should arise. DES is capable of using 7.2 x 10^{16} different key combinations and utilizes cipher feedback for synchronization. DES encryption key length is 56 bits, plus 8 bits for parity (64 bits total).

DES is not authorized to encrypt classified information. Secure modules used for transmission of classified information are considered “Type 1” encryption modules and are Controlled Cryptographic Items (CCIs), meaning that their manufacture, distribution, use and disposal is controlled by the National Security Agency. All of the other devices in this article are considered “Type III” encryption products are not regulated by NSA. Type 1 secure modules should never be in private hands but you never know what is going to end up on Ebay!. Some of the Type 1 encryption protocols can be reviewed here: http://venona.antioffline.com/ceg.html). The Fascinator Type I secure module for analog Saber/Systems Saber (NTN7298/NTN5874) required modifications to the radio to function and requires a Secure Interface Box (SIB) (T5164), the TKN8516 SIB to Saber cable and either a KOI-18 or KYK-13 keyfill device. Type 1 modules do **NOT** use the standard Motorola Key Variable Loader (KVL). Occasionally you can find analog Saber radios on Ebay that still have the red and white “CCI” sticker on the rear of the radio housing (some of them are still equipped with their encryption modules as well). These are valued to some as collector’s items since they should not have been released into the public in that configuration. Fascinator is a fairly old encryption protocol and probably hasn’t been used for some time since the Saber/Systems Saber family was discontinued in the late 1990’s.

As the processing ability of the average home PC increased over the years since DES was implemented, the National Institute of Standards and Technology (NIST) http://nist.gov realized that the original DES key length of 64 bits was vulnerable to cracking just by trying every single possible key. A new method of securing information exchange was developed called Triple-DES (often written as 3DES or TDES) that basically encrypts the information three times using the DES algorithm. 3DES is NOT a standard protocol for encrypting two way radio transmissions, but it is used inside some of the newer encryption modules for firmware upgrade validation. It should be noted that any attempt by a hobbyist to decrypt any DES encrypted transmission using samples of digital voice would be difficult (but not impossible) since the voice samples are relatively short in duration and the average user simply does not have the processing power or software to accomplish the feat.

Variations of the Originals (-XL)

After DVP and DES products gained acceptance and their use became more common, instances of reduced transmission range were observed. When using their radios in the encrypted mode, it was apparent that the radios did not seem to have the same “talk distance” as they did when in the clear mode. In response to these observations, two new variations of the original protocols were introduced, each with the added acronym "XL", giving us two new (but different) encryption protocols: DVP-XL and DES-XL. The “-XL” variants change the encryption feedback method to counter addressing vice cipher feedback to alleviate the reduced range problems associated with the original protocol. From what I have read and learned over the years, the reduction in “talk distance” when using DVP and DES was due to the inability of the receiving radio to synchronize with the incoming encrypted bit stream. The counter addressing (“-XL”) method corrected this synchronization problem and provided talk distances comparable with analog voice. Note that “-XL” variants are proprietary Motorola variations of the original protocol and are not compatible (i.e. a radio equipped with DVP cannot communicate with a DVP-XL radio). When using DVP-XL, the number of operator selectable keys increases to 7.9 X 10^{28} with an encryption key length of **96** bits. A little known (or realized) FACT – DVP-XL is *MORE SECURE* than DES-XL based upon the number of available keys! After the “-XL” variants were released to the marketplace, Motorola started using the label “CFB” (Cipher Feedback) on DES modules manufactured *without* the “-XL” hardware . Most early DES modules (NTN1152) for the Astro Saber and Astro Spectra radios were marked “DES-CFB”, meaning that they were plain DES modules without “-XL” features. One can normally visually identify an XL module from a non-XL module simply by the presence of an additional gold IC on the board. Non-XL secure modules (for example, the TRN4836 DES hybrid has a single gold IC chip on it, whereas the “XL” version (TRN7036) will have two gold ICs. A third variation of the DES algorithm, known as DES-OFB (Output Feedback), is part of the APCO P25 digital voice and data standard. DES-OFB is a relatively new variation to the DES family and is unique since it will only encrypt IMBE or VSELP digital voice – It will not encrypt standard wideband FM analog voice

Digital Voice International

The unique encryption protocol known as DVI-XL (Digital Voice International) is based upon the DVP-XL algorithm. There is some contrary information in the public domain regarding the encryption key length of DVI. Some documents say 24 bits, some documents say 32 bits. Since DVI-XL is based upon DVP-XL, I am going to assume that the key length remains the same as DVP-XL at 96 bits. Many people have speculated that since DVI was destined for the international marketplace, there is a hidden back door into this protocol. Of course, no one knows this with any certainty, but it would make sense. DVI is unique as it requires what is called a “system key” to function and uses two different keyloaders for loading encryption keys in subscriber radios. The DVI-XL system key is completely different from the system keys used to prevent unauthorized access to trunking systems. The DVI-XL system key consists of a 128 bit key variable that is loaded into the keyfill device in addition to the encryption key. There are two different KVLs for DVI-XL, the T3012 and T3013. Each is capable of loading a subscriber radio, but the T3013 "Operator" model is **NOT** capable of entry of the key variable data. The T3012 is referred to as the "Supervisor" model and allows key data entry. To load a T3013 loader with keys, you must clone the key data from either another T3013 or a T3012 Supervisor KVL. DVI-XL is not a common algorithm and is rarely seen in the used marketplace.

Advanced Encryption Standard (AES)

With the security offered by DES rapidly eroding, NIST solicited proposals for a new encryption algorithm in 1997. In 2001, FIPS 197 was released by NIST and details all of the pertinent facts about the new protocol, the Advanced Encryption Standard (AES). It can be viewed at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Most of the technical aspects of AES are beyond the scope of this document, but the FIPS standard is quite detailed. With this new standard and push to move all encrypted federal information exchanges to this new protocol, several new encryption modules and a new keyloader (the KVL 3000+) were developed. Only the KVL3000+ is able to keyfill AES devices. With a key length of 256 bits, the new algorithm promises to provide very good security for the foreseeable future, but it is not considered a "Type I" algorithm; therefore it cannot be used to safeguard classified information. It should be noted that AES is available with variable key lengths of 128, 192 and 256 bits but only AES-256 is currently offered by Motorola for land mobile products. AES encryption utilizes Output Feedback (OFB) for synchronization.

Advanced Digital Privacy (ADP)

Advanced Digital Privacy (ADP) is a new enhancement to Astro portable and mobile radios. I have not been able to review very much documentation regarding this algorithm, other than the fact that it uses a public domain 40-bit encryption algorithm known as RC4 which was released by RSA (the same group who developed PGP). ADP is unique when compared to the other secure modules that have been discussed. ADP is available as a firmware (DSP) based flash option or as hardware (UCM based) option. When a radio is equipped with ADP as a flash option, the encryption key is loaded via Customer Programming Software (CPS). Once keys are entered into the CPS, they are not visible when the codeplug is read for review – ensuring that if a radio is lost or stolen, the encryption key cannot be decoded just by a review of the radio codeplug. When hardware based, it is loaded with a KVL3000+ keyloader. It should be noted that ADP is only compatible with conventional (non-trunked) P25 IMBE digital voice – it cannot encrypt analog FM voice. While relatively weak when compared to DES or AES, ADP does offer significant security benefits for those users needing a less secure and/or less expensive alternative for encryption.

Advanced Securenet^{TM}

Advanced Securenet (ASN) is a term that is normally associated with two different enhanced features of Securenet products, OTAR and Multikey. OTAR (Over-the-Air-Rekeying) allows radios in the field to be recoded with new encryption keys without a physical connection to the keyloader. 12kbps Analog Securenet uses MDC to signal key changes to the radio. Subscriber radios in the field can request a new key by sending a request to the Key Management Controller (KMC). OTAR can be incredibly complicated when you factor in the number of radios in the field and the coverage area of the radio system. Subscriber radios in the field are normally equipped with two separate “indexes” of encryption keys. Normal radio traffic is encrypted and decrypted using “TEKs”, or Traffic Encryption Keys. Inbound OTAR keys (i.e. new keys) are sent to the subscriber radios via MDC using KEKs (Key Encryption Keys). KEKs are also referred to as “shadow” keys. KEKs prevent unauthorized radios from being able to utilize the OTAR MDC data packets containing the new encryption key data (Note: the term KEK is synonymous with USK (Unique Shadow Key), but USKs are only used between the KMC and KVL, not between the KVL and subscriber radio). Subscriber radios must be loaded with both the current TEK and KEK to function properly in OTAR systems. The new TEK index can be setup using software to create a new key index or replace the current index being used by the radio. This allows the field user to switch between active key sets at will (for example, rekey all radios towards the end of the month and allow users to switch to a new key set on the 1st of the upcoming month) or the ability to completely replace the current TEK index immediately. If the TEKs are erased but the KEK is intact, the radio can be OTARd by a few keystrokes at the KMC. However, if all of the TEKs and KEK is lost, the radio must be rekeyed via a physical connection to a keyloader. It is not uncommon for radio service facilities to maintain a keyloader with the KEK loaded to enable the service facility technicians to load a newly serviced radio with the shadow key set and then request OTAR via the KMC.

Multikey is the other aspect of ASN that allows multiple encryption keys to be loaded into a single device. In legacy radios (Saber and SYTEMS Saber), multikey was a function of the secure module in that the secure module was physically different from a non-multikey module. Analog Spectra used one of two methods for Multikey operation: Dual-code or Dual-hybrid. Dual code is a software configured option that enabled a Securenet option board with a single hybrid to hold two encryption keys. Dual-hybrid optioned radios are configured with two encryption hybrids and can store a maximum of four encryption keys. In the Astro product line, multikey is a function of the radio firmware and flashcode, not a function of the encryption module.

Astro^{TM} Digital and It’s Relation to Securenet^{TM}

Since our subscriber units are now becoming multi-mode radios that support both analog and digital (IMBE/Apco P25) communications, many of the range and quality drawbacks associated with digitizing and encrypting analog voice have disappeared. With high speed DSP chips now handling the coding of the voice, the secure hardware is now encrypting an already digital signal. The result is that you literally can’t tell the difference in audio quality between a secure and non-secure IMBE transmission. Gone are the days of the raspy sounding DES calls with muffled, raspy sounding audio and reduced range.

In the mid 1990's, the Astro series of digital radios were introduced prior to the release of the APCO P25 digital voice specification. The two original products, the Astro Saber portable and the Astro Spectra mobile were initially released with a digital voice codec called VSELP (Vector Sum Excited Linear Predictor). VSELP is a unique and proprietary digital signaling format that is not compatible with the P25 IMBE-based digital voice specification. Only Motorola has manufactured two-way radio equipment utilizing the VSELP codec and it is no longer available or commonly used. After the phase out of the VSELP LAPD system to IMBE digital, the only other major city that use(d) VSELP was the city of Memphis, Tennessee, but to my knowledge that system has been converted to IMBE. After the APCO P25 digital voice specification was finalized and the vocoder chosen, the Astro product line switched to the IMBE (Improved Multi-Band Excitation) vocoder. Both VSELP and IMBE transmit digital voice at 9.6kpbs but they are <u>not</u> compatible. There are some limitations regarding Securenet products and their use in the Astro series of radios. To encrypt VSELP or IMBE voice, you must use DES-XL, DVP-XL, DVI-XL, DES-OFB, ADP or AES-256. DES and DVP in their original cipher feedback (CFB) form can only encrypt analog FM – they cannot encrypt VSELP or IMBE digital voice. The newer DES-OFB encryption algorithm utilizes the same encryption key variable length as DES (64 bits) and must be loaded with a T3011DX or an appropriately equipped KVL3000/KVL3000+.

Evolution and the UCM

The ease of changing firmware instead of altering a hardware design has changed the way cryptographic modules are constructed. One can consider all modules prior to the UCM (Universal Cryptographic Module) *LEGACY* modules. These modules are all physically different based on the encryption type that they were designed to support. In other words, there are physical differences between a Saber DES-XL module and a Saber DVP module. This is not the case with a UCM. Instead, the UCM is flashed (programmed) with the encryption algorithms in firmware, based on the needs of the customer – reducing the number of physical designs and hardware differences that were required with legacy modules. UCMs are also capable of being re-flashed to new firmware in the field – something that was not possible with legacy modules. It should be noted that Motorola uses different "kit" numbers (NTNxxxx) for different variations of the same UCM depending on the algorithms loaded in the module. There is no publicly available information that describes the transition from the legacy Astro secure modules, which are referred to as "EMC" (Encryption Management Controller) modules and the newer UCMs. From what I can tell, the release of the UCM coincides with Astro System release 6.3 in 2003. UCM devices have firmware revisions of 3.00 or higher when a subscriber radio is placed into self test – EMC modules have firmware revisions as low as 0.6 (early Astro Saber) up to 2.xx. This even more confusing since the subscriber radios still report "EMC 3.xx" when placed in self test (on Astro Saber/Spectra and XTS 3000), even though the radio is equipped with a UMC (v3.xx) encryption module. There is a relationship that must be drawn between the host firmware revision of the subscriber radio and their compatibility with encryption modules. Before installing a UCM, you must ensure that the secure module being installed is compatible with the host firmware of the radio, or you may have problems with the radio based on the software setup of the secure hardware. Firmware 7.xx or higher is required in Astro XTS 3000 portable and firmware 11.xx or higher is required in an Astro Spectra mobile to support UCM-based encryption. There is a workaround to allow radios with relatively recent HOST firmware revisions to function with older v2.xx EMC modules: Do NOT enable "CKR" (Common Key Reference) key management since this is a function of UCM secure modules and do not enable the radio lock function (when secure equipped, the radio lock feature is controlled by the secure module in the radio – not the host firmware; this feature will not work properly when using an older EMC-type module in a newer radio). Note that in newer subscriber equipment, (namely the XTS 5000 and XTL5000) there is no known compatibility issues with secure modules since the radios were released well after the introduction of the UCM (these radios report "SECURE VER" in self test). However, when using an older T301_DX keyloader for keyloading on the XTS 5000/XTL5000, you MUST check the PID KEY MANAGEMENT block in the secure hardware tab to allow the T3011DX to load the encryption key. CKR encryption key management is NOT COMPATIBLE when using the T301_DX KVLs. UCM compatibility will, however, come into play when attempting to install or upgrade an Astro Saber, Astro Spectra or XTS 3000.

The Keyloaders

The original KVL was the P1001_x, pictured at the end of this document. This device looked like a MX300 with a calculator keypad on the front and the characteristic RED display. They have gotten to be fairly rare these days since it hasn't been manufactured in about 20 years! The P1001 was strictly a DVP keyfill device; it was never manufactured for any other protocol. All of the keyloaders prior to the KVL3000 series are extremely susceptible to ESD damage due to the first generation CMOS chips used in their construction, so you must be incredibly careful when you open a keyloader to prevent damaging the components. The small connector shown below in the picture is the programming key. To change the encryption key, this connector had to be attached to the side of the programmer. Within a few years and with the advent of DES encryption, Motorola changed the layout and style of the keyloaders to the more familiar plastic T30xx chassis. These loaders all look VERY similar. The T3010, also pictured at the end of this document, was the replacement for the original P1001 series loaders. It is easily recognized because the front panel has a keypad with the numbers 0-7 (due to the limited key length), but the case is the newer style dark grey plastic.

With DES encryption becoming the federal standard for encrypting land mobile radio traffic in the early 1980's, Motorola again changed the T30xx series keyloaders to support the (then) new DES algorithm, releasing the T3020 DES KVL. Since DES used a 64-bit key, a hexadecimal keypad was added to enable the user to enter hex numbers as part of the key variable. All of the T-series loaders other than the T3010 have hexadecimal keypads for operator entry of the key data. The T3011 (DES/DES-XL), T3012/3013 (DVI-XL) and T3020 (DES) keyloaders all look exactly the same when viewed from the outside. Only the model number tag on the rear of the chassis will reveal what model you are looking at. The T3014 keyloader has a characteristic that makes it relatively unique. Instead of the standard dark grey keypad, the T3014 DVP-XL keyloader has a WHITE or SILVER keypad. This makes identification of the unit fairly easy, but you should still check the model number on the rear of the chassis for confirmation, since there are KVLs out there that have been re-cased into new housings with the silver/grey keypad.

The most desirable legacy keyfill device for hobbyists is the T3011DX KVL since it will function with all of the older and less expensive legacy equipment and the newer Astro equipment. The T3011DX will load key variables into DES, DES-XL and DES-OFB equipped radios and will function with everything from a first generation DES Expo HT to an XTS 5000. It is possible to upgrade a keyloader from earlier firmware revisions to the “D” series firmware. Although these kits are no longer available directly from Motorola, it is possible to locate them on the used market. If upgrading an “A” or “B” version keyloader to “D” firmware, both the memory and firmware chips must be changed. If upgrading from a “C” to a “D” model, only a new firmware chip is required. The part number of the T3011-T3014 AX/BX to DX upgrade kit was TLN3412 and consisted of a new firmware PROM (U103) and memory IC (U104). If you cannot ascertain the identity of a keyloader, you can open it and look at the main circuit board part number – the main circuit board you want is TRN7136A as it is upgradeable to “DX” specifications. Note that KVLs upgraded via this kit are considered “Limited DX” KVLs. They are “limited” in that they lack the ability to communicate via modem with a KMF/KMC – a feature that is not required for hobbyists.

The T3011DX keyloader was replaced in the late 90’s with a much more modern device that is capable of evolutionary changes with firmware upgrades as well – the KVL 3000, pictured at the end of this document. The original next generation keyloader, the KVL 3000 enabled the user to have a single device capable of loading up to two different encryption algorithms. The KVL3000 was discontinued in 2003 and replaced with the KVL 3000 *Plus*. Although there are other minor differences between the KVL 3000 and the newer 3000 Plus model, the biggest differences are that the original KVL 3000 does not support AES-256 or ADP encryption and it only supports TWO different algorithms (i.e. DES and DVP, DES and DVI-XL, etc.). The KVL 3000+ supports all encryption protocols except the non-XL version of DVP. In essence, Motorola has built a keyfill device that is capable of loading multiple algorithms without changing anything other than a menu selection on the KVL. Of course, this is not without drawbacks – as you must be able to power on the KVL3000 and navigate the menu screens to determine which algorithms are loaded into the KVLs firmware. Most units found in the used marketplace are ex-government (they’ve shown up on http://govliquidation.com) and most are equipped with a minimum of DES. When the DES option is shown on the KVL 3000, it will load DES-CFB, DES-XL and DES-OFB.

Here is a table showing the KVL model numbers and capabilities:

	Algorithm							
	DVP	DVP-XL	DES	DES-XL	DES-OFB	DVI-XL	AES-256	ADP
T3010	X							
T3011			X	X	X			
T3012						X		
T3013						X		
T3014		X						
T3020			X					
KVL 3000	X	X	X	X	X	X		
KVL 3000+		X	X	X	X	X	X	X

NOTE: The T3014 DVP-XL KVL will **NOT** load a DVP key. The T3020 DES KVL will **NOT** load DES-XL or DES-OFB. The T3010 will **NOT** load a DVP-XL key.

NOTE: KVL 3000 and KVL3000+ options are FIRMWARE driven, not hardware. KVL 3000 can support DES and any ONE other algorithm (except AES and ADP). KVL3000+ can support any combination of algorithms and supports AES and ADP.

NOTE: T30xx KVL's are available in A, B, C and D firmware revisions. Jedi series radios (MTS2000 and MCS2000) require a "C" firmware revision or higher. Astro series radios require the "D" firmware revision.

NOTE: It is possible to perform a field upgrade on any series loader to "D" firmware. A and B series loaders require both a new firmware PROM and a new memory chip. C series loaders only require a new firmware PROM. Once upgraded, the loaders are considered "Limited" DX loaders in that the ability to download keys via modem from a KMC is not functional (N/A to hobbyists).

NOTE: The T3012 is the "Supervisor" model DVI-XL KVL. All functions including key generation are available on this model. The T3013 is the "operator" model and does NOT allow entry of the key variable data. T3013 models require their keys to be transferred from either a T3012 Supervisor model or another T3013.

The older T30xx series loaders were capable of storing up to 16 traffic and 16 shadow keys. The newer KVL3000 and KVL3000+ models can store 1024 encryption keys and allow the operator to partition the 1024 memory locations at will. Shadow keys are discussed in the ASN section above.

Sections yet to be written:

Secure modules
Secure radios
Secure repeaters
LID / CKR / PID discussion

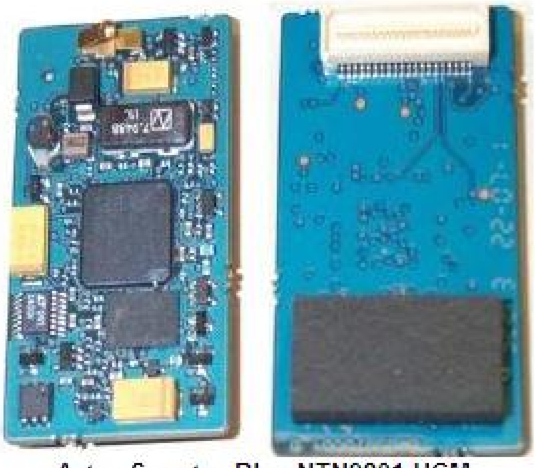
References

(not in any particular order and incomplete)

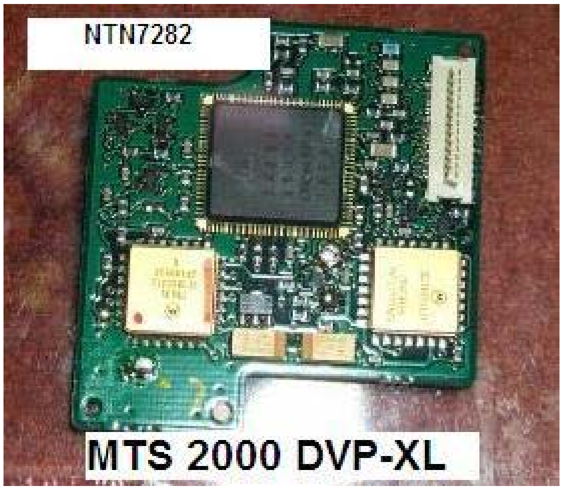
Publication #	Description
6881090E30	T3010DX DVP KVL
6881090E20	T3011DX DES/DES-XL KVL
6881090E40	T3012DX DVI-XL Supervisor KVL
6881090E25	T3013 DVI-XL Operator KVL
6881090E35	T3014DX DVP-XL KVL
6881090E60	KVL Retrofit Manual T3010 – T3014 CX to DX
6881090E55	KVL Retrofit Manual T3010 – T3014 AX/BX to DX
6880801G95	KVL3000 Plus Service Manual
6881132E29	KVL3000 Plus User’s Guide
6881131E16	KVL3000 User’s Guide

Important Part Numbers

TLN3199	T3014AX/BX Retrofit (allows sharing keys to CX/DX)
TLN3096	T3014AX/BX Retrofit to Limited DX (no Remote capability)
TLN3412	T3011AX/BX Retrofit to Limited DX

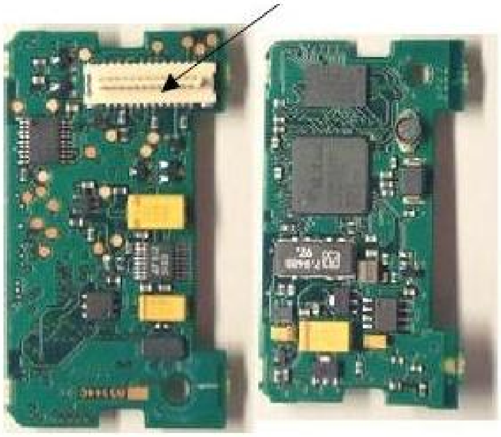


Astro Spectra Plus NTN9801 UCM

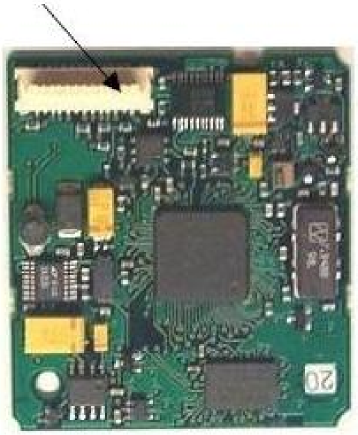


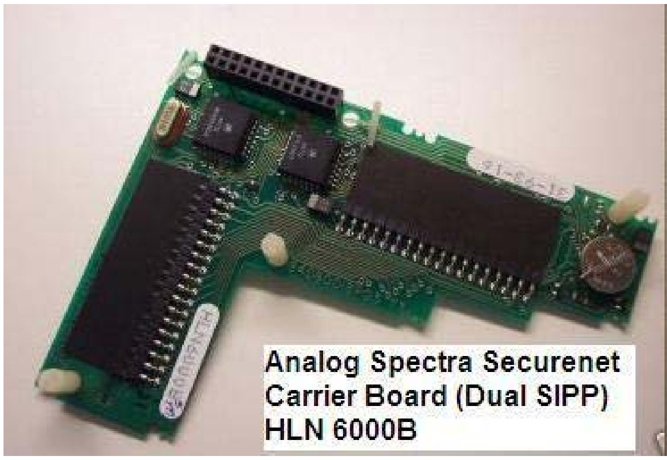
MTS 2000 DVP-XL

Astro Saber / Astro Spectra UCM (Typical)

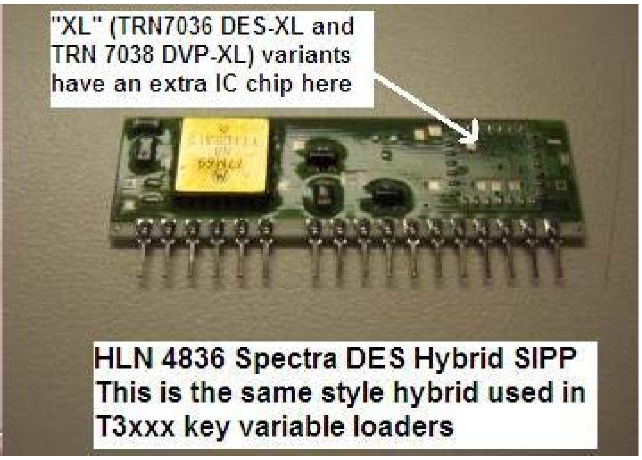


Astro XTS 3000 UCM (Typical)



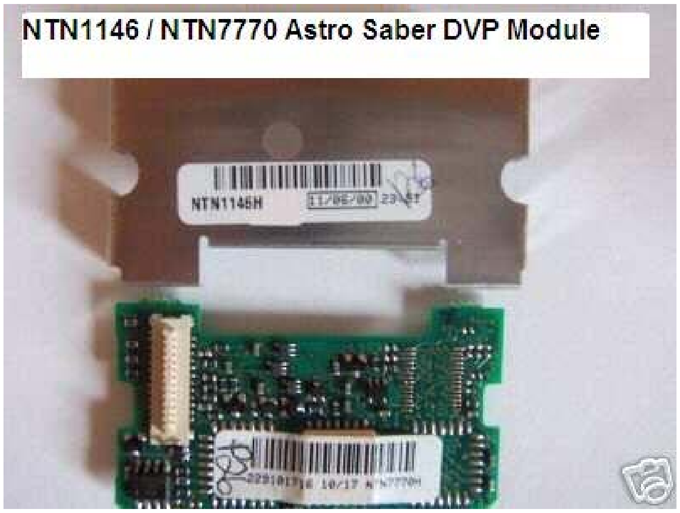


Analog Spectra Securenet Carrier Board (Dual SIPP) HLN 6000B

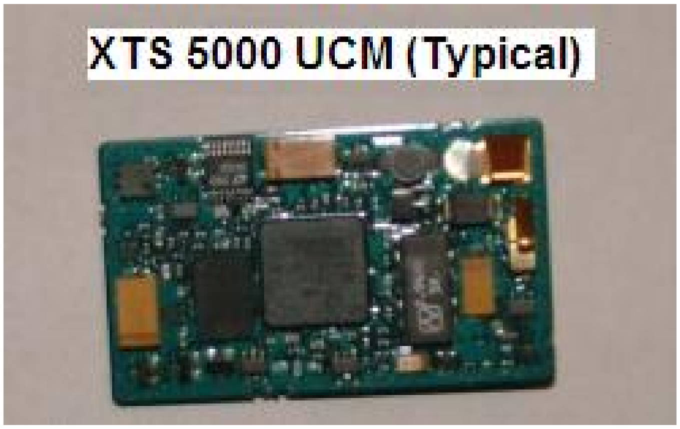


"XL" (TRN7036 DES-XL and TRN 7038 DVP-XL) variants have an extra IC chip here

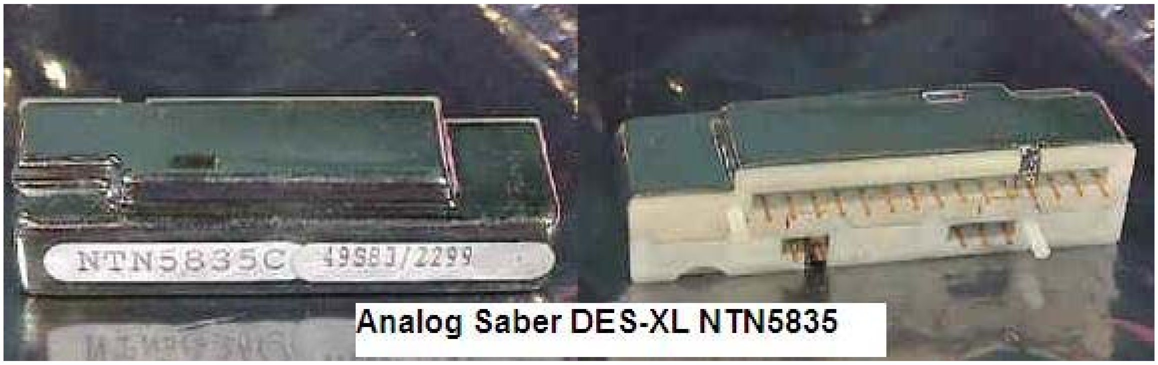
HLN 4836 Spectra DES Hybrid SIPP
This is the same style hybrid used in T3xxx key variable loaders



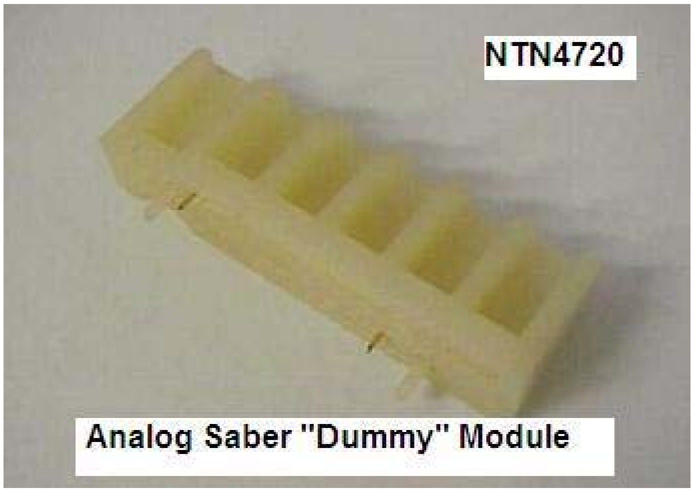
NTN1146 / NTN7770 Astro Saber DVP Module



XTS 5000 UCM (Typical)

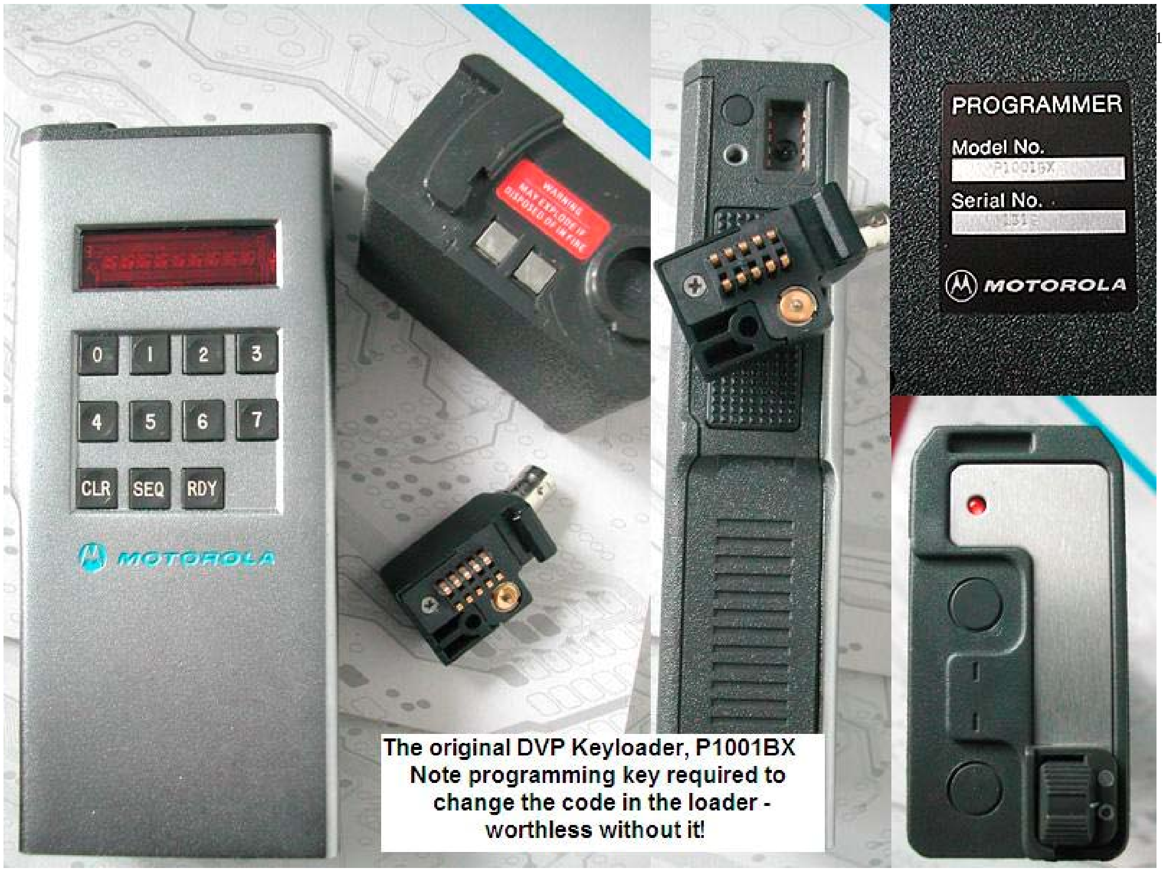


Analog Saber DES-XL NTN5835

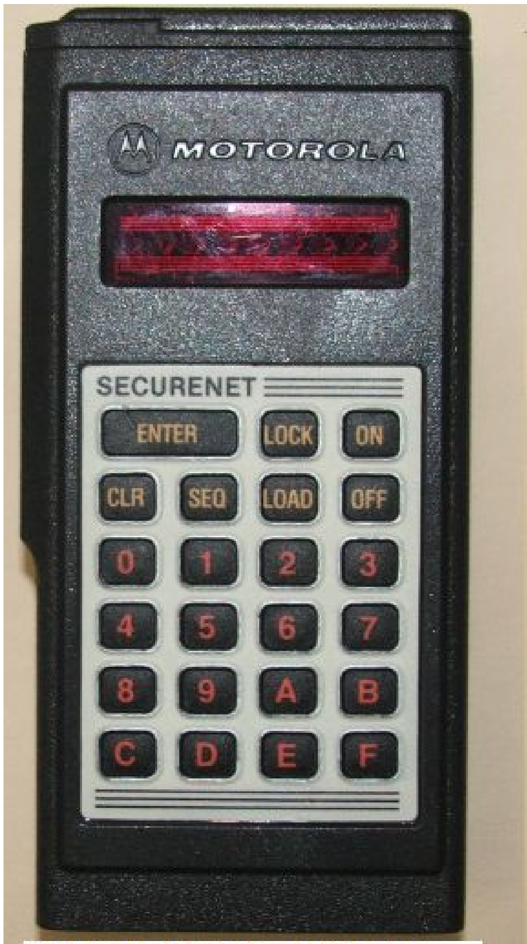


NTN4720

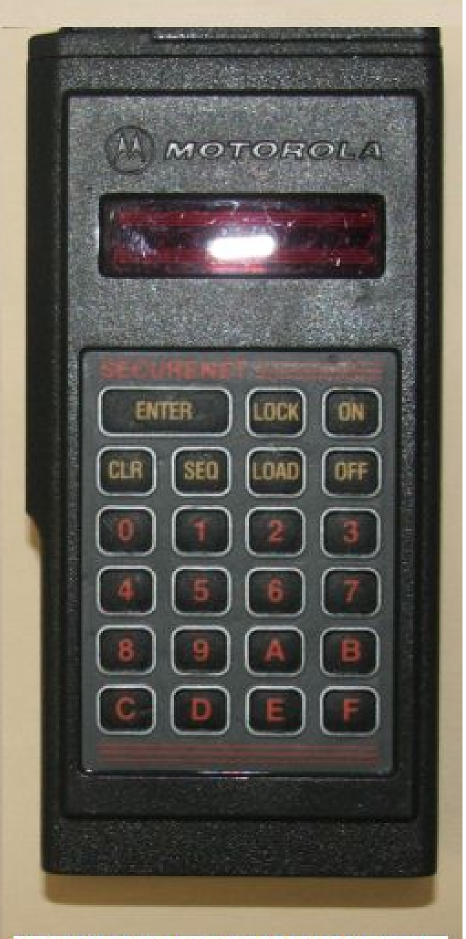
Analog Saber "Dummy" Module



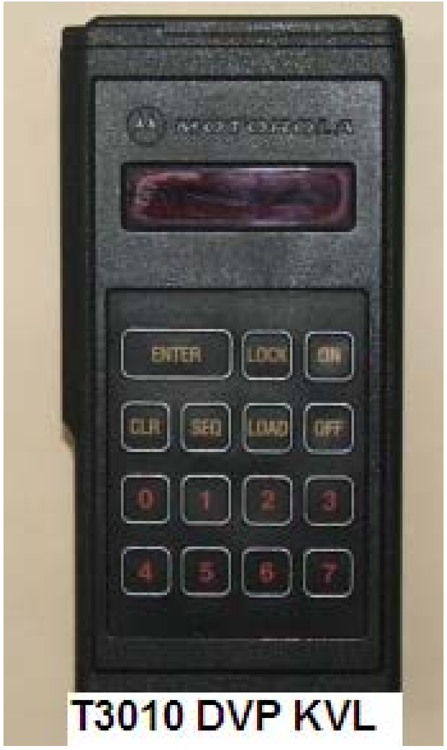
The original DVP Keyloader, P1001BX
Note programming key required to change the code in the loader - worthless without it!



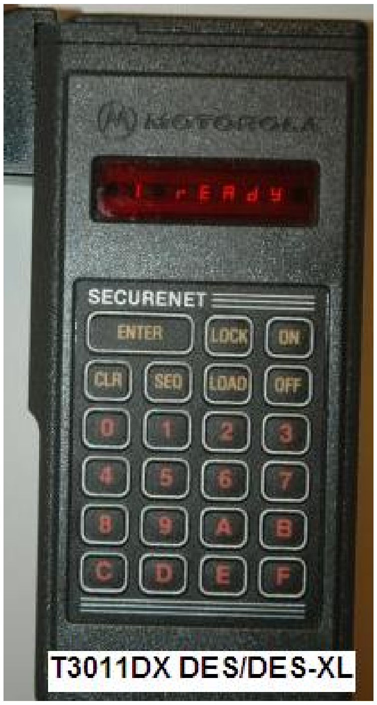
T3014DX DVP-XL Keyloader



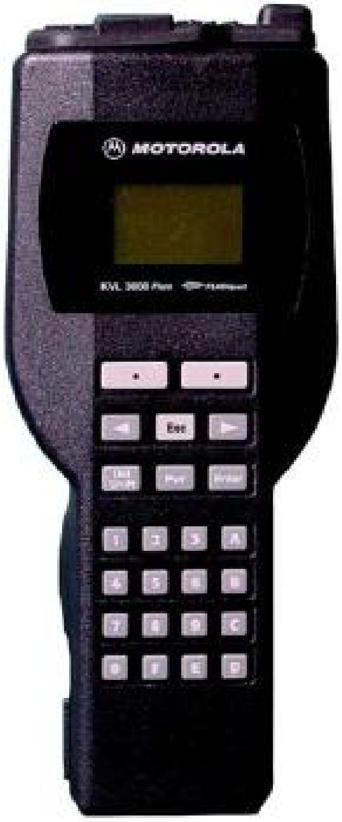
T3012DX "Supervisor" DVI-XL



T3010 DVP KVL



T3011DX DES/DES-XL



KVL 3000 Plus