THALES

Security Policy

THALES 25 PORTABLE RADIO

(PRC6894)

THALES COMMUNICATIONS, INC.
22605 GATEWAY CENTER DRIVE
CLARKSBURG, MD 20871
www.thalescomminc.com

TABLE OF CONTENTS

List of Tables

CHAPTER 1.0 INTRODUCTION

This manual contains the security policy for the Thales 25 portable radio (T25). The T25 supports Project 25 (P25) digital voice and data encryption operation, Over The Air Rekeying (OTAR), Motorola Key Variable Loader (KVL) , as well as analog wideband Continuously Variable Slope Delta (CVSD) encrypted voice. This security policy defines the rules that must be followed to allow the radio to be operated in a secure manner. This document does not provide detailed user guidance for the radio operation to follow these rules, but will refer to the T25 user documentation as needed.

The entire radio is considered the crypto module for FIPS 140-2 validation purposes. The critical security parameters are the AES encryption keys, HMAC authentication key, programming password and zone password. These parameters are described as used in the following sections.

REVISION HISTORY

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
0.1	Nov 2005	J. Kent	Initial Version	
01		W. Wykoff	Update headers, added revision history	Prepare for release
02	Nov 2006	M. Hess	Additional description for programming password and zone password. Added statement concerning OTAR not being a FIPS approved mode.	Changed for slightly higher security rating. Standard statement for OTAR.
03	Nov 2006	M. Hess	Revision History	Clarify REASON FOR CHANGE on REV 02

Table 1 Revision History

REFERENCES

Item	Document Number	Version	Title
01	84326	F	Thales 25 Detailed User Manual
02	84328	A	Thales 25 Technical Service Manual with Illustrated Parts Breakdown

Table 2 References

CHAPTER 2.0 IDENTIFICATION AND AUTHENTICATION

The T25 radio includes several security related roles and authentication methods (passwords or key data). However as a public safety tool the radio must be considered a limited access device and should be physically secured and in the possession of authorized users at all times. This is in contrast to a publicly accessible device such as a cell phone or cable modem which will require stronger authentication methods since they must be designed to be in potentially "malicious" hands as part of normal operation.

ROLES AND AUTHENTICATION METHOD

Role	Description	Authentication Method
User	Uses the portable to communicate (RF) with other Users.	Programming Password Zone Password Encryption Lock OTAR RSI/uKEK OTAR Feature License
Administrator	Loads software and configuration data in the portable.	Zone Password
Crypto Officer	Loads keys in the portable. Often the Administrator and crypto officer roles are fulfilled by the same person.	Zone Password Motorola KVL Possession KVL Feature License OTAR Feature License

Table 3 Roles and Authentication

Authentication Methods

Possession

The first layer of protection in the T25 portable is physical access to the radio. The portable includes several functions that require no authentication. For example until a configuration is loaded in the portable with a zone password (see description below) anyone with the applicable PC Programmer software, cable, and access to the radio can program the portable. However these are all proprietary items and even a modest, common sense access control policy for the portables and accessories will go a long way in securing T25 operation.

Programming Password

The Administrator may configure the T25 portable with a programming password. This is a 6 digit PIN stored internally to the portable. The password protects modification of all channel programming data, including frequencies and other channel parameters.

Programming password entries are not provided for viewing on the T25 Portable's LCD display. An asterisk (*) symbol will be displayed for each valid keypad entry of the password. Only three unsuccessful attempts at entering the correct password are allowed. After the third unsuccessful attempt, further password entries are locked out until the T25 Portable's power switch is cycled OFF then ON or the battery is removed and replaced. This feature is compliant with FIPS 140-2 Level 2 requirements.

The programming password does allow encryption to be enabled or disabled on a channel, and allows the channel encryption key to be changed – either manually through the keypad, or through an OTAR re-key request if the portable is licensed and configured for OTAR operation.

Once a programming password is entered it is valid until power is cycled on the portable. Be sure to turn the portable OFF whenever it will be out of use to force the next user to have to enter the programming password again.

The Administrator can overwrite the programming password from the PC Programmer, without having to know the existing programming password. This password is intended to restrict operator access and is not intended to authenticate an Administrator or Crypto officer.

Zone Password

The zone password allows more complete protection of specific zones in the portable. Each zone (collection of up to 16 channels assigned to the channel selection knob) can be configured as a "Protected Zone". A single Zone Password can also be assigned, and is applicable for all protected zones. The Zone Password provides similar access protection as the programming password with the following exceptions:

- Only applies to protected zones. Unprotected zones can be modified without requiring entry of the Zone Password.

- If ANY zone in the portable is protected the Administrator cannot reprogram the radio without first entering the Zone Password. This allows the Zone Password to provide the User with protection against others, including Maintainers from modifying his configuration.

Zone password entries are not provided for viewing on the T25 Portable's LCD display. An asterisk (*) symbol will be displayed for each valid keypad entry of the password. An unlimited number of attempts can be made to enter the correct zone password. This feature is compliant with FIPS 140-2 requirements.

The zone password can be used for Administrator authentication. Like the programming password, the Zone Password once entered remains in effect until power is cycled on the portable.

Encryption Lock

Each channel in the portable can be programmed by the Administrator, using the PC Programmer for "Encryption Lock". When this parameter is enabled a User cannot disable encryption on a channel that is configured for encrypted operation. This ensures that the User cannot transmit on the secure channel without using encryption. This parameter can only be changed by using the PC Programmer and can be protected by a Zone Password.

Motorola KVL Possession

A Motorola KVL is an expensive piece of equipment that is not readily available. A KVL with a system's encryption keys is a critical part of a system's security and must be handled in an appropriate manner (beyond the scope of this security policy). Restricted physical access to the key loading device is the primary authentication method for KVL key loading, and the transfer of keys from the device is neither encrypted nor authenticated further.

CHAPTER 3.0 ACCESS CONTROL

ROLES

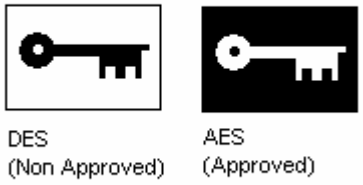
The security related roles available were introduced in Roles and Authentication Method. This section details the available security services and the access to security parameters (cryptographic keys and CSPs) that can be accessed by each role.

APPROVED MODES OF OPERATION

The T25 Portable supports P25 AES encryption as the FIPS 140-2 Level 1 approved mode of operation.

FIPS Approved Mode Indication

The T25 Portable uses a “key” ICON on the status display to indicate encrypted operation. When AES encryption is being used the key ICON is displayed inverted (white key icon on black field). Refer to the T25 Detailed User guide Default Display section for the location of this ICON. Note that the drawings in the user manual only show the normal non-inverse version of the ICON.



FIPS Approved Mode Invocation

The FIPS approved mode (AES) is invoked whenever a channel is selected that is configured for AES encryption and contains a valid AES encryption key resident in its AES key position. Additionally encryption may be enabled or disabled on an AES channel (see encryption toggle below). This encryption toggling is considered a manual bypass operation of the FIPS approved AES encryption mode. Whenever the AES encryption is enabled the “inverse” key ICON will be displayed on the LCD screen.

Non FIPS Approved Modes of Operation

The T25 Portable supports P25 DES encryption, P25 DES OTAR operations, and Analog CVSD DES voice encryption. NIST no longer supports validation of DES based modes of operation, so all of these modes are non FIPS approved. The portable’s encryption icon (a “key” icon) is displayed normally, as shown above, when operating in these modes. The icon is left “normal” in these modes for backwards compatibility with pre FIPS approved versions of T25 software.

The non FIPS approved DES encryption modes can be disabled by not loading any DES encryption keys in the Portable, or by not including the DES Licensed features. This allows a T25 Portable to support only FIPS approved encryption operation if that is desired by a customer.

SERVICES

The T25 portable supports the services specified in **Table 4 Services**. The table also lists the typical role that requires this service, and the encryption algorithm supported by the service.

Service	**Role**	**CVSD DES**	**P25 DES**	**P25 AES**
Portable Maintenance				
Load operational software	Administrator	X	X	X
Configure Licensed Options	Administrator	X	X	X
PC Programmer Configuration				
Encryption Key Entry	Crypto Officer, Administrator	X	X	X
Channel Configuration	Administrator	X	X	X
Encryption Toggle Configuration	Administrator	X	X	X
Zeroize Keys Configuration	Administrator	X	X	X
OTAR Configuration	Administrator		X	
Programming Password	Administrator	X	X	X
Zone Password	Administrator	X	X	X
KVL Encryption Key Load				
Load encryption keys, keysets, and crypto-groups	Crypto Officer	X	X	X
Portable Operation				
Enable/Disable encryption	User	X	X	X
Select channel encryption key	User	X	X	X
Request OTAR rekey	User		X	
Change Channel parameters	User	X	X	X
Zeroize Keys	User	X	X	X
Encrypted Voice Calls – Analog	User	X		
Encrypted Voice Calls - Digital	User	X	X	X
Encrypted GPS data	User		X	X
Self Test				
AES Algorithm KAT	Crypto Officer, Administrator, User (Power On)			X
SHA-1 HMAC KAT	Administrator (Load Operational Software)	X	X	X
Bypass Operation Conditional Test	User	X	X	X

Table 4 Services

SELF TEST SERVICE

The T25 portable contains the following self tests that are run on power-up or on demand:

AES Algorithm Known Answer Test (KAT)	Run on power up, tests each used mode of AES
SHA-1 HMAC KAT	Run before operational software load (SHA-1 HMAC used to authenticate the loaded software). This test is run on any operational software load, regardless of supported (licensed) encryption algorithms
Bypass Operation Conditional Test	This test is run before each transmission. It is run in all FIPS operational modes as well as non FIPS operational modes

CRYPTO OFFICER

The crypto officer is responsible for key establishment. The person fulfilling this role will have access to the actual encryption key data. Other roles will have access to encryption key ID's and their use, but will not be able to access the actual encryption key data.

Encryption Key Entry – PC Programmer

Encryption keys are entered manually in plain-text hexadecimal form at the PC Programmer. Once an encryption key is entered and accepted it is stored to a file encrypted using the AES algorithm and a hard-coded AES key that is shared by the PC Programmer and Portable software. Once an encryption key is encrypted it is displayed as "*"'s on the screen and there is no way to retrieve the original key data. The key data is transferred to the Portable in encrypted form and cannot be retrieved or output from the Portable.

The original key data must be stored securely by some means outside of the T25 PC programmer/Portable system if it needs to be reused.

For OTAR configurations the Crypto Officer must also enter an uKEK (Unique Key Encryption Key).

Encryption Key Entry – Motorola KVL

Encryption keys are manually entered in the Motorola KVL key load device. The uKEK required for OTAR operation (described above) can also be loaded via the KVL. The KVL does not encrypt key data, or "hide" it at the display. Access control to this key data is purely a matter of physically securing the KVL device.

ADMINISTRATOR

The Administrator loads software and configuration data in the T25 Portable.

T25 OPERATIONAL LOAD OPERATIONAL SOFTWARE

T25 operational software is distributed in a self-installing windows executable file. All operational software is signed with a SHA-1 HMAC that is calculated from a secret key embedded in all T25 portables. This key is hard coded, but since it is derived from known data loaded in the radio at manufacture time the key is not known (included in any form) in the downloaded software image, or the update utility itself.

The software update executable is available on TCI's customer service web-site to persons with a valid TCI service account. There are no access restrictions on the ability to reload the T25 Portable software other than obtaining the update executable file, and physical possession of the T25 Portable and a programming cable.

The T25 Portable however will ONLY accept software with a valid HMAC signature which is generated by TCI when the software is built. Loading any operational software without a valid HMAC signature will cause the Portable to be inoperable. It must be forced to boot mode by applying an external signal (refer to Technical Service Manual) and loaded with valid signed software before it can be used for any function other than loading software.

CONFIGURE LICENSED OPTIONS

The T25 Portable licensed features are configured as part of loading operational software. The licensed features are stored in an encrypted file on a TCI FTP server. The Administrator must order specific features for specific Portable serial numbers through their TCI customer service or sales representative. The Portable software update utility automatically loads the encrypted feature file and sends it to the radio as part of a loading the operational software. The Administrator has no other means for changing any licensed features.

The T25 Portable FIPS validation includes all of these licensed features, although only the AES encryption feature is part of the validated FIPS approved mode of operation. The T25 portable includes indicators (described elsewhere in this document) to show if it is operating in a FIPS approved mode.

The user cannot directly tell which features are licensed in a particular portable, however if a license is disabled, the feature is fully disabled including removal of menu items related to the feature. Each license description below includes a brief description of how the portable's operation differs if the license is disabled. (Thales Customer Support also has a database of all licenses based on the portable's serial number).

CVSD Analog DES Encryption Feature License

CVSD Analog DES allows encrypted voice operation on analog conventional channels (non P25). This is a non FIPS approved mode of operation for interoperability on legacy systems that use this

encryption method. For situations where this feature is not needed or only FIPS approved modes are allowed the feature can be fully disabled by not including this feature license.

When disabled:

- Encryption cannot be enabled on an analog channel through the channel programming menu, KMGR menus, or PC Programmer.

P25 DES Encryption Feature License

P25 DES allows DES encrypted voice and data operations on P25 digital conventional channels. This is a non FIPS approved mode of operation for interoperability on P25 systems that use this encryption method. For situations where this feature is not needed or only FIPS approved modes are allowed the feature can be fully disabled by not including this feature license.

When disabled:

- DES Encryption cannot be enabled on a P25 digital channel through the channel programming menu, or PC Programmer.
- The KMGR menus will not display an AES/DES choice for key management operations.
- If P25 DES and CVSD DES are both disabled DES keys cannot be loaded into the T25 portable. The PC Programmer will download the keys but the radio will not store them.

P25 AES Encryption Feature License

P25 AES allows AES encrypted voice and data operations on P25 digital conventional channels. This is the FIPS approved mode of operation, so this license must be included for any FIPS approved operation.

When disabled:

- Encryption cannot be enabled on a P25 digital channel through the channel programming menu, KMGR menus, or PC Programmer.
- The KMGR menus will not display an AES/DES choice for key management operations.
- AES keys cannot be loaded into the T25 portable. The PC Programmer will download the keys but the radio will not store them.

KVL Feature License

KVL key load support allows loading of either DES or AES encryption keys with a P25 Key Variable Loader (KVL) device. The T25 is tested with the Motorola KVL-3000 and KVL-3000+ devices. Keys can be loaded in FIPS approved and non FIPS approved modes with either the PC Programmer or a KVL. If a customer system does not use KVL devices then this feature is not needed.

When disabled:

- Encryption keys cannot be loaded with a KVL device. The portable will not acknowledge that a KVL is connected.

OTAR Feature License (DES non FIPS approved mode only)

The portable can support Over The Air Re-keying (OTAR) of DES encryption keys. This feature is not supported for AES encryption keys. OTAR is a licensed extra cost feature and can be completely disabled in systems that do not use OTAR by not ordering the feature. T25 portable feature licenses are maintained in an encrypted form on the Thales Communication Inc (TCI) software upgrade server. This is a proprietary encryption method and is not necessarily cryptographically strong. All security features that are feature license enabled require further effort and authentication for use. For example OTAR has strong authentication procedures as defined in the TIA specifications. As a matter of security policy however systems should not be configured with security features that are not expected to be used as part of the system's normal security policy and operation.

OTAR RSI (OTAR authentication details)

OTAR operation requires several identification and authentication items to be programmed in the radio. These parameters are mentioned here, but the user is referred to the "Thales 25 Detailed User Manual" and the TIA specifications for details. All of these parameters can be set only from the PC Programmer (PCP) and can be protected from unauthorized modification by a Zone Password. These parameters are specific to the OTAR Key Management Facility and should only be available on a need-to-know basis. The uKEK can be loaded from the PCP or from a KVL just like other encryption keys.

- KMF RSI
- Group RSI
- Individual RSI
- Unique Key Encryption Key (uKEK)

The Individual RSI is displayed by the Portable, but the User does not have access to the other parameters.

When disabled:

- The main menu does not display "ROPTNS" and "OTAR" choices
- You cannot enable OTAR or perform any OTAR operations on any channel.

PROGRAMMING PASSWORD

The programming password is entered at the PC programmer. The Administrator can set, change or clear a portable's programming password, without needing to know the existing programming password.

ZONE PASSWORD

The Zone Password is entered at the PC Programmer. The Administrator can set, change or clear a Portable zone password. Unlike the programming password the Administrator must know a Portable's existing Zone Password before it can modify it. The Portable checks its Zone password before accepting any configuration data from a PC Programmer. The Zone password must then be

entered at the PC programmer before the Portable will accept any changes (including changing the Zone Password)

CHANNEL CONFIGURATION

The Administrator configures all Portable channel parameters at the PC programmer. The security related parameters that can be set at the PC programmer are:

Parameter	Description
Channel Type	Analog Narrow, Analog Wide or P25 Digital. Analog narrow does not support encryption, Analog Wide supports CVSD DES encryption, and P25 Digital supports either P25 DES or P25 AES encryption
Locked	When enabled the channel parameters cannot be modified by the User, including changing the encryption key. Encryption enable/disable is allowed.
Encryption Lock	When enabled encryption cannot be disabled on the channel. Key selection is allowed.
OTAR enabled (FIPS Non Approved Mode)	When enabled an OTAR rekey can be performed on the channel. This of course requires the OTAR feature license and proper OTAR configuration and authentication at the KMF.
Encryption Type	A channel encryption type may be set to none, AES, DES or SLN (Storage Location Number) encryption. SLN encryption is an indirect key assignment. The SLN points to a key location. The encryption type depends on what type of key is loaded in that location.
Assigned Key	All loaded keys with the proper encryption type may be assigned to an encrypted channel.
Key Lock / Any key	This is a global setting that affects channel operation (all channels). Keylock causes channels to receive calls only on the encryption key assigned to the channel. Anykey causes the channels to receive calls on any encryption key loaded in the Portable.

Table 5 Channel Configuration Parameters

ENCRYPTION TOGGLE CONFIGURATION

The Portable may have a side-key programmed to enable or disable encryption. Each press of the assigned side-key will toggle the setting. When disabled all channels will transmit in the clear regardless of the channel encryption configuration. However an encryption locked channel will always transmit encrypted regardless of this toggle setting.

ZEROIZE KEYS CONFIGURATION

A User will always have the ability to zeroize keys from the keypad regardless of the Portable configuration. The Administrator may also program the red “emergency” button to function as a panic zeroize. When configured this way the User can zeroize all keys in the Portable by pressing the red button.

OTAR CONFIGURATION (NON APPROVED MODE)

In order to use OTAR the channel must be enabled for OTAR operation and the OTAR parameters must be specified. Refer to the PC Programmer user's manual for OTAR parameter configuration instructions. An uKEK must also be loaded for OTAR operation.

GENERAL

The Crypto Officer and Administrator roles are filled by the same individual, and that person has full access to all Portable programming parameters. Access control is generally concerned with ensuring the Users have access to only the channels and encryption parameters to which they are authorized. This section lists the typical and recommended means of using the parameters described in this section.

Key Load

The primary access control should be to load only the encryption keys needed for a particular mission into a Portable. This ensures that the Portable can only communicate with others on the same mission, and limits the amount of key data that could be compromised if the portable was lost.

Key lock/Any Key

If use of a common configuration is desired where encryption keys for multiple users/missions are loaded into all Portables the "Key lock" configuration should be used. This limits a channel to breaking squelch only on the key assigned to the channel. This allows different user groups to share a channel with their communications separated by using different encryption keys. The "Any Key" configuration causes the Portable to break squelch on a received call using any key stored in the Portable.

A shared configuration using "Key lock" allows users to voluntarily isolate their communications. There are no access protections however to enforce this separation (i.e. any user can switch to any programmed channel) so it cannot be used where the various users must not be able to use each others crypto settings.

Encryption Lock

Sensitive missions where all communications must be encrypted should have channel encryption lock enabled. This prevents intentional or accidental disabling of encryption on the sensitive channels.

Programming/Zone Passwords

The User can be further restricted by setting programming and/or zone passwords. These prevent restricted users from being able to change any channel settings. From a security standpoint this prevents the users from being able to manually enter un-authorized frequencies or other channel parameters which could be used to monitor or block (interfere) with those channels.

CHAPTER 4.0 PHYSICAL SECURITY

TAMPER

The T25 Portable does not include physical security mechanisms such as tamper evident seals or locks.

ZEROIZE

The T25 Portable can be programmed to use the Emergency Push Button (See Technical Service Manual Introduction) for Panic Zeroize. If a User is in a situation where the encryption keys may be compromised the Panic Zeroize feature should be used to allow rapid dumping of the encryption keys.

This feature can also be used as a convenient means of clearing encryption keys from a Portable before storage. Since this function does not require rapid zeroization it is more common to keep the Emergency button programmed for P25 Emergency call declaration and make it a matter of policy to zeroize the encryption keys from the keypad menus whenever the Portable will be stored, or potentially otherwise used by someone who should not have access to the loaded keys.

OTAR

The P25 OTAR feature is designed to allow encryption keys to be changed frequently in the Portable. Use of this feature limits the value of any particular encryption keys and somewhat negates the need for physical security mechanisms. OTAR can only be used in the FIPS non-approved mode of operation.

SUMMARY

The primary means of physical security for the T25 Portable is the possession of the device. A customer security policy should be based on ensuring that only authorized personal have access to the Portable at all times.

To further secure the system Users should be directed to zeroize encryption keys whenever they are not immediately needed for a mission. This is especially important when storing the Portable, or having it repaired.

Note that if a Portable malfunctions while loaded with Encryption keys there may be no way to zeroize these keys prior to repair. This requires either that the “Administrator” must have authorization to use those encryption keys (trusted), or the used encryption keys must be changed before the radio is repaired. The portable must be sent to Thales customer service for repair or replacement, and Thales as a policy clears all user data from the portable before performing any repair activities.

In general a policy of limited Portable, PC Programmer and KVL access, along with periodically changing encryption keys should be implemented to minimize potential compromises.

CHAPTER 5.0 MITIGATION OF OTHER ATTACKS

The T25 Portable does not contain any specific mitigation of other attacks.

THALES COMMUNICATIONS, INC.
22605 GATEWAY CENTER DRIVE
CLARKSBURG, MD 20871
www.thalescomminc.com

Customer Service
1-800-914-0303
Email: customer.service@thalescomminc.com