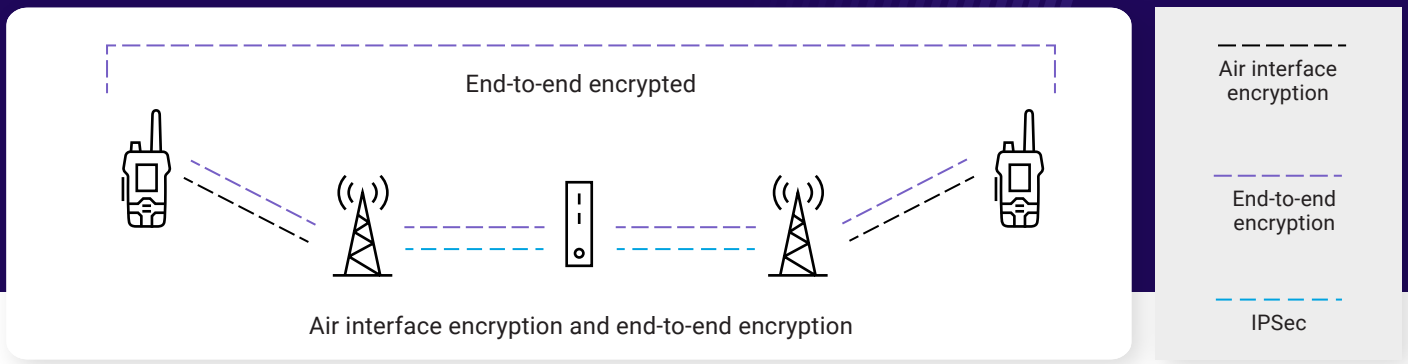
Data Sheet

KVL6K E2EE for DIMETRA systems

Key Variable Loader for end-to-end encryption

MOTOROLA SOLUTIONS

End-to-End Encryption (E2EE) provides an extra layer of security across your DIMETRA™ system for voice, data and location information: from end-point to end-point. This is in addition to Air-Interface Encryption between the base station and TETRA devices, and IPSec encryption between base stations and the DIMETRA core.



KVL6K E2EE

The KVL6K E2EE is a Key Variable Loader (KVL) that provides secure generation, secure storage, secure transportation and secure loading of keys to enable end-to-end encryption for DIMETRA TETRA infrastructure components and Motorola Solutions TETRA devices.[1]

The KVL6K E2EE consists of a USB Hardware Security Module (HSM) that provides secure storage and cryptographic operations and a KVL6K E2EE application that runs on a computer using the Microsoft® Windows® operating system. The KVL6K E2EE application has an intuitive user interface and allows users to easily manage and load keys. The KVL6K E2EE builds on the capabilities of the KVL 4000[2] E2EE with a new look and feel, improved usability and functionalities.

Key management

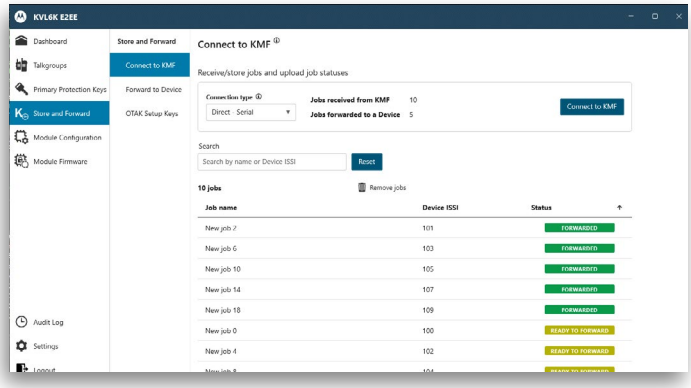
KVL6K E2EE provides means for creating and transferring encryption keys to Motorola Solutions TETRA devices (mobiles and portables) and infrastructure. Encryption keys can be entered manually by a KVL user, auto-generated by the KVL's HSM, or downloaded from a Key Management Facility (KMF) as part of the store-and-forward feature.

Automatic key loading of the end-to-end Encryption Key into Motorola Solutions TETRA devices is an option that helps to speed up the provisioning process. When a Motorola Solutions TETRA radio is connected to the KVL6K E2EE, the radio is detected automatically, and the key loading process starts.

The KVL6K E2EE provides the ability to define and load Primary Protection Keys to different infrastructure crypto modules, including the DIMETRA KMF's CryptR, in order to secure their databases. It can also be used for crypto module settings configuration and firmware updates.

Intuitive user interface

The KVL6K E2EE Windows application has an intuitive user interface and supports touch screen devices, as well as both night and day modes. The application dashboard helps with day-to-day operations and enables fast and easy key maintenance. Different views including Talkgroups, Cryptogroups and KMF related operations, provide an additional level of information to make key management more efficient.



[1] A full list of compatible devices is listed on page 4.
[2] KVL 4000 E2EE cables cannot be re-used with the KVL6K E2EE.

Secure solution

The security of keys is paramount. To help keep your keys secure and your DIMETRA TETRA systems protected, the KVL6K E2EE uses multiple security capabilities.

Physical USB HSM

The KVL6K E2EE allows the user to take advantage of using a standard "off the shelf" Windows device to run the KVL6K E2EE application while maintaining a high level of security. This is accomplished by utilising a USB HSM designed to meet FIPS 140-3 level 3 hardware specifications to protect, store and secure all sensitive key material and enable key transfer to the target devices.

The USB HSM utilises a secure boot so that only Motorola Solutions approved code can run on it, and has countermeasures like tamper protection built into the hardware to protect against exfiltration of data through probing of the HSM or from environmental attacks — such as extreme temperatures or over voltage.

Secure processing of key material

All the key material that the KVL6K E2EE creates, stores and transfers to target devices and infrastructure during the provisioning process is secure and never visible to the application or user in an unencrypted form. (The only exception is when a user enters a key - after which the key can never be seen in unencrypted form again.) Only the USB HSM is able to decrypt key material, and only when connected to a target TETRA device that needs its E2EE key loaded.

Environment protection

The KVL6K E2EE uses the Microsoft Package Integrity Check feature in Windows, which enables Windows to run integrity checks on the entire contents of the host application package. This enables Windows to initiate a package remediation and repair workflow before launching the application if it detects a tampered or corrupted package.

Multi-layer key material protection

The KVL6K E2EE includes multi-layer key material protection. Each key used by the KVL6K E2EE is encrypted using the USB HSM before storing it. In addition, the entire KVL6K E2EE keystore is encrypted by a key stored within the HSM, so the data remains protected while at rest.

Encrypted connection to USB HSM

The KVL6K E2EE provides an AES 256 encrypted USB connection between the USB HSM and the KVL6K E2EE application to keep data exchanged over the link secure.

Secure remote connection

Remote connection with the DIMETRA Key Management Facility is protected by a pre-shared key, which encrypts all transmitted key material. The KVL6K E2EE does not expose any endpoints, and a remote connection is only available on demand.

Authorisation and security

Access to the KVL6K E2EE is secured by requiring Windows user authentication, possession of the USB HSM, and authentication to enable the USB HSM.

Separate Administrator and Operator roles are available for users. Adopting roles enables users to have the appropriate authorisation of key management activities, including authorisation of firmware upgrades and critical parameter changes. In addition, having a mandatory password protects the KVL6K E2EE application, while user timeout automatically logs a user out of the application after a specified period of inactivity. The KVL6K E2EE also maintains an audit log of actions including managing and loading talkgroups, store-and-forward operations, settings changes, or firmware management.

PHYSICAL CHARACTERISTICS	
USB HSM dimensions (mm)	80 x 25 x 16
USB HSM ports	USB Type A, Hirose
USB HSM IP rating	IP52
KVL6K BOX	
The standard KVL6K E2EE ships with the following in the box:	USB HSM
	USB flash drive containing: • KVL6K E2EE application installer • KVL6K E2EE user guide • Drivers
	Quick Start Guide
SUPPORTED ENCRYPTION ALGORITHMS	
Algorithms	• 128-bit AES • 256-bit AES
MINIMUM PC REQUIREMENTS	
Operating System	Windows 10 (version 2004) or later
Processor	x64-based processor
Free disk space	500 MB
RAM	2 GB or RAM memory (4 GB recommended)
USB ports	1 x USB port type A for the KVL6K E2EE (KVL6K E2EE HSM will also work with USB-C with an adapter) Note: An additional USB type A port will be needed for provisioning devices that require key loading over USB. A USB type A port may also be needed for modem connectivity.
Recommended screen resolution	1920 x 1080
SUPPORTED DEVICES	
Portable radios	• MTP3000 Series • MTP6650 • MXP600 • MXP7000 • MTP8000Ex Series • ST7000 • ST7500
Mobile radios	• MTP3000 Series • MTP6650 • MXP600
Pagers	• ADVISOR™ TPG2200 two-way pager

To learn more, visit: **www.motorolasolutions.com/tetrasecurity**

MOTOROLA SOLUTIONS

Motorola Solutions Ltd., Nova South, 160 Victoria Street, London, SW1E 5LB, United Kingdom

All specifications are subject to change without notice