KVL6K AIEA FOR DIMETRA SYSTEMS

KEY VARIABLE LOADER FOR AIR INTERFACE ENCRYPTION AND AUTHENTICATION

The KVL6K AIEA is a Key Variable Loader (KVL) that provides secure storage, secure transportation and secure loading of keys to enable Air Interface Encryption and Authentication (AIEA) for DIMETRA™ TETRA infrastructure components and Motorola Solutions TETRA devices.

The KVL6K AIEA consists of a USB Hardware Security Module (HSM) that provides secure storage and cryptographic operations and a KVL6K AIEA application that runs on a computer using the Microsoft® Windows® operating system. The KVL6K AIEA application has an intuitive user interface and allows users to easily manage and load keys.

KVL6K AIEA is compatible with Motorola Solutions DIMETRA infrastructure and Motorola Solutions TETRA devices. It builds on the capabilities of the KVL 4000 AIEA and works with existing KVL 4000 AIEA-supported key loader cables (using an adapter) or with a new set of cables.[1]

[1] Please see the accessories catalogue
motorolasolutions.com/tetradeviceaccessories
for a full list of cables

MOTOROLA SOLUTIONS

SECURE SOLUTION

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

PHYSICAL USB HSM

The KVL6K AIEA allows the user to take advantage of using a standard "off the shelf" Windows device to run the KVL6K AIEA 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.

ENCRYPTED CONNECTION TO USB HSM

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

SECURE PROCESSING OF KEY MATERIAL

All the key material that the KVL6K AIEA transfers between the source (Authentication Centre or Provisioning Centre) and target components during the provisioning process is never visible to the KVL6K AIEA application in an unencrypted form, and only the USB HSM is able to decrypt it during connection with targets.

MULTI-LAYER KEY MATERIAL PROTECTION

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

ENVIRONMENT PROTECTION

The KVL6K AIEA 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.

SECURE REMOTE CONNECTION

Remote connections with the TETRA Authentication Centre and Provisioning Centre are protected by a pre-shared key, which encrypts all transmitted key material. The KVL6K AIEA does not expose any endpoints, and a remote connection is only available on demand.

AUTHORISATION AND SECURITY

Access to the KVL6K AIEA 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 authorization of firmware upgrades and critical parameter changes. In addition, having a mandatory password protects the KVL6K AIEA application, while user timeout automatically logs a user out of the application after a specified period of inactivity. The KVL6K AIEA also maintains an audit log of operations including settings changes, connections to infrastructure and devices, and key provisioning.

KEY MANAGEMENT

The KVL6K AIEA securely stores the Infrastructure Key generated by the DIMETRA Authentication Centre for secure transportation and loading into DIMETRA infrastructure components such as Zone Controllers, MTS TETRA Site Controllers and MTS Base Radio Controllers. It also securely stores the Authentication Key and Static Cipher Key generated by the Provisioning Centre for secure transportation of those keys and loading into Motorola Solutions TETRA devices.

The KVL6K AIEA also provides the ability to define and load master keys to provision Authentication Centre and Provisioning Centre crypto modules.

Automatic key loading of the Authentication Key and Static Cipher Key into Motorola Solutions TETRA devices is a selectable option. When a Motorola Solutions TETRA radio is connected to the KVL6K AIEA the radio is detected automatically, and the key loading process starts.

INTUITIVE USER INTERFACE

The KVL6K AIEA 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, such as the Base Station provisioning view with data about TETRA Site Controllers and MTS Base Radios, provide an additional level of information.
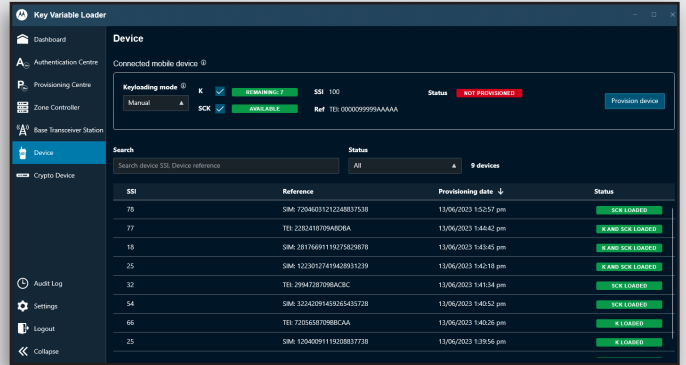
PHYSICAL CHARACTERISTICS

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 AIEA ships with the following in the box:	USB HSM
	USB Flash drive containing: • KVL6K AIEA Application Installer • KVL6K AIEA User Guide • Drivers
	Quick Start Guide

MINIMUM PC REQUIREMENTS

Operating System	Windows 10 (version 2004) or later
Processor	x64-based processor
Free Disk Space	500 MB
RAM	2 GB of RAM memory (4 GB recommended)
USB Ports	1 x USB port type A for the KVL6K AIEA (KVL6K AIEA 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

16 mm

25 mm

80 mm

For more information, please visit:
www.motorolasolutions.com/kvl6k

MOTOROLA SOLUTIONS