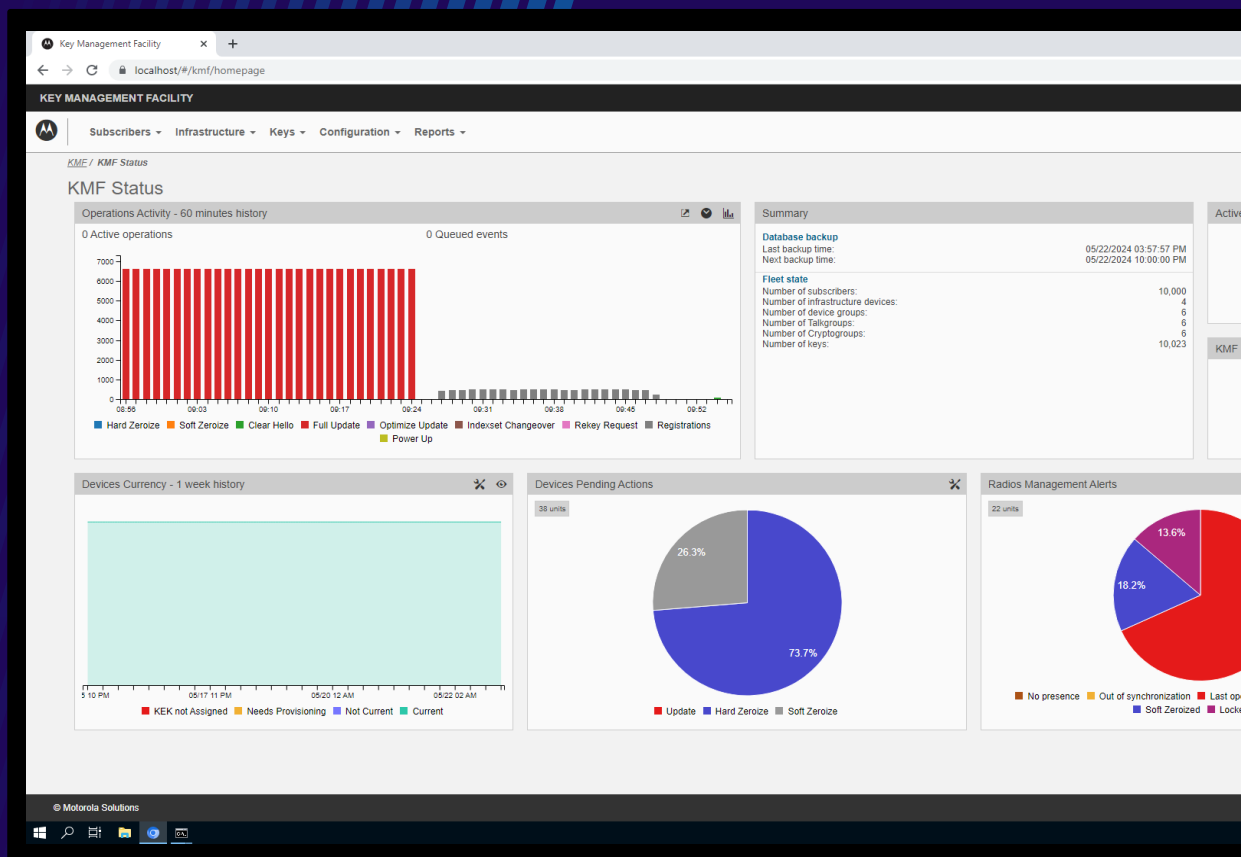
Data Sheet

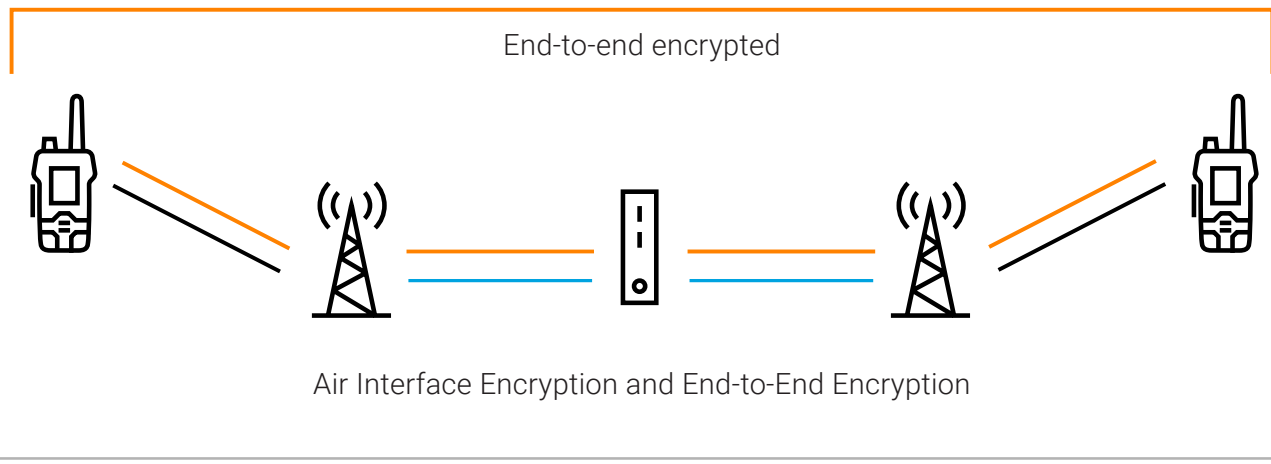
DIMETRA™ Key Management Facility (KMF) for End-to-End Encryption



MOTOROLA SOLUTIONS

Threats against public safety communications and critical infrastructure are growing in reach and sophistication. That's why it's important that your communications system uses modern security practices and complies with security guidelines.

In addition to Air-Interface Encryption between the base station and TETRA devices, and IPSec encryption between base stations and the DIMETRA™ core, 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.



Air Interface Encryption and End-to-End Encryption

Air Interface Encryption

End-to-End Encryption

IPSec

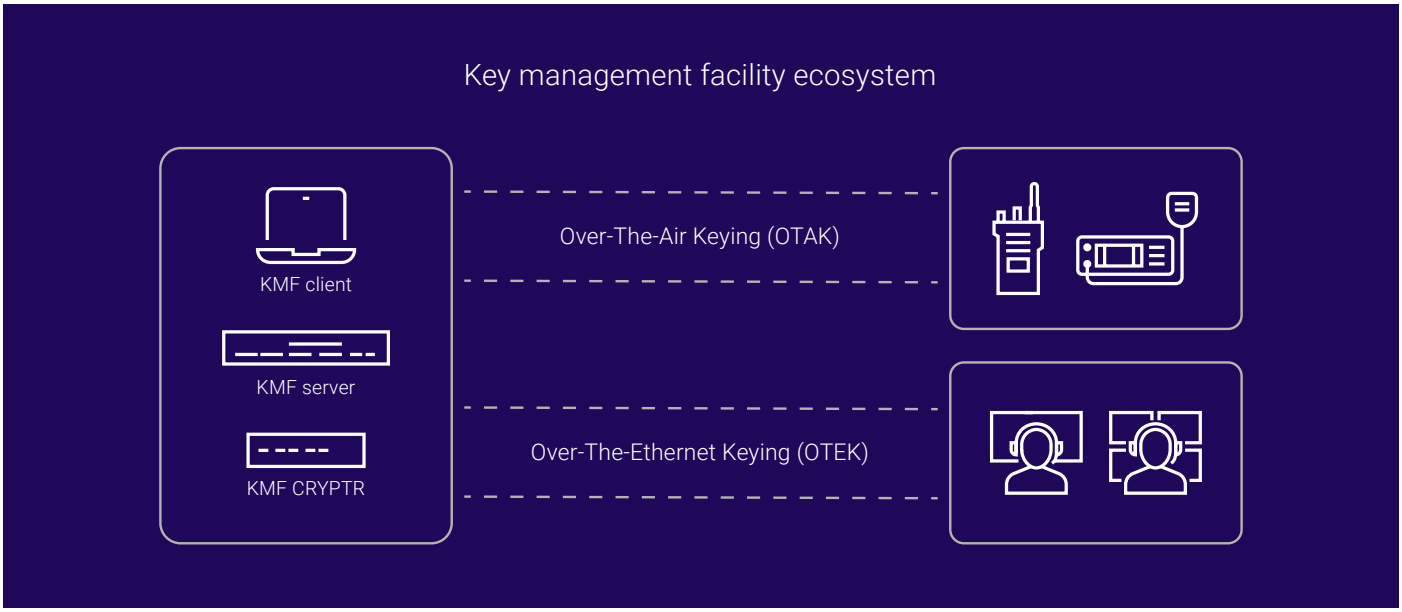
With a growing and geographically dispersed number of TETRA devices it becomes increasingly costly and impractical to manually update your E2EE keys on each device via an E2EE Key Variable Loader (KVL). There is a solution: the DIMETRA Key Management Facility (KMF).

The DIMETRA KMF provides a robust and easy to use platform for effectively managing your E2EE keys over your DIMETRA network for your E2EE enabled devices, including TETRA portable and mobile radios, and dispatch consoles. With the DIMETRA KMF you can generate, load, and delete keys to help keep your voice and data communications secure. You can update your E2EE keys using Over-The-Air Keying (OTAK) or Over-The-Ethernet Keying (OTEK) of devices or dispatch consoles remotely, out in the field. This eliminates the delays, inconvenience and administrative costs of having users bring their devices to a centralised location or taking KVLs out to the field for manual rekeying.

By making it easy to rekey devices and dispatch consoles, you can update the keys more frequently to help stay ahead of your adversaries and better insulate yourself from potential attacks. The DIMETRA KMF also provides reporting tools to help you keep up to date with your fleet of devices and dispatch consoles.

The DIMETRA KMF consists of a server, a browser-based client and a CRYPTR.

- The KMF Server is the host for the KMF server application and database. It runs all of the key management operations[1] and stores all key material and configuration settings. It also manages E2EE key distribution via OTAK and OTEK.
- The browser-based KMF client provides a user interface for all KMF operations.
- The KMF CRYPTR is responsible for generating and protecting encryption keys, as well as for encrypting and decrypting key material so that it is never transmitted or stored in plaintext. It also performs encryption operations for key management messages (OTAK and OTEK).



[1] The initial loading of E2EE keys to a TETRA radio or dispatch console needs to be done via an E2EE Key Variable Loader (KVL).

Main features of the DIMETRA KMF

Key management and transmission

Over-The-Air Keying (OTAK)

OTAK removes the burden of manually rekeying TETRA portable and mobile radios with secure, remote, over-the-air distribution and management of E2EE keys. With OTAK you reduce the time needed for rekeying devices and gain greater control by being able to poll a device and update or erase its E2EE keys. OTAK makes it easier to frequently change E2EE keys out in the field.

Over-The-Ethernet Keying (OTEK)

OTEK provides the same mechanisms for remotely managing encryption keys as OTAK with the exception that the messages are delivered over an Ethernet connection for products such as dispatch consoles. OTEK eliminates the need to physically touch any of the dispatch consoles to update them with E2EE keys and enables your dispatchers to communicate securely across multiple talkgroups.

Retry Opportunities

The Retry Opportunities feature enables the KMF to automatically retry OTAK and OTEK commands to reach devices that did not positively acknowledge receiving the commands. If an operation fails due to a device being out of range, turned off or in a call, an automatic update is triggered next time a device initiates communication with the KMF.

Extend the capability of OTAK with store and forward

If devices are out of OTAK range you can load their E2EE keys from the KMF to a TETRA Key Variable Loader (KVL), and then use the KVL to manually update those devices. Encryption key status is updated when the KVL is connected back to the KMF server.

Radio group management

To provide the flexibility to have cryptographic separation between talkgroups, the KMF assigns each talkgroup a different E2EE key.

Talkgroup Secure Mode

Each talkgroup is specified with a Secure Mode attribute that defines how a call is secured during voice and data communication: full encryption, clear or mixed mode. This attribute is set via the KMF so that users out in the field communicate with the right level of protection for each talkgroup they use.

Voice and data key rotation

To effectively manage and track the keys for a talkgroup, a cryptogroup is assigned to the talkgroup. To aid E2EE key rotation, the KMF supports three keys within each cryptogroup: current, past and future, each key in a separate indexset. The indexsets allow the KMF operator to switch between Active (current) and Inactive (past and future) keys. In case not all devices update their keys at exactly the same time, the three keys approach enables devices to communicate with E2EE as long as each device is using one of those three keys.

Automated key material generation

This is an automated way of creating keys using the CRYPTR, and it doesn't expose the key values to the KMF operator or administrator. This also frees operators from reliance on third party suppliers for keys or manual key material generation.

Key Kettle

For greater flexibility in key generation the Key Kettle repository contains unlabeled and unassigned keys that can be used as source material when creating new E2EE keys.

Key Export / Import

Key Export is a feature to export selected keys to an encrypted text file. Key Import enables you to import keys from an encrypted text file, which could be from another KMF or a third-party vendor.

KMF Hello

KMF Hello is a quick and efficient method of determining whether a radio or any other device is turned on, within the range of the system, and is properly configured for OTAK or OTEK commands.

Zeroize

The Zeroize command can be sent from the KMF client application to a device to prevent it from communicating in secure mode. This is useful if a radio is lost, stolen or sent for service repair.

Event Logging

The KMF Server maintains logs of all KMF events and user activities, such as OTAK operations, server processes and entity management.

Backups

The DIMETRA KMF can perform manual and scheduled backups, providing the ability to restore vital data in the event of a data loss or failure of the KMF.

Visibility and reporting

KMF status

KMF Status view shows the state of your fleet and the KMF server. It includes operations activities, fleet size and information about talkgroups and keys, latest backup, active users, KMF load (performance), and more detailed information about devices (currency, pending actions and alerts).

Dashboard

The KMF client application dashboard allows users to monitor the basic parameters of the KMF workflow in real time. It also notifies the KMF administrators about any E2EE related system issues.

KMF reporting

KMF reports provide an easy way to have visibility of your radio fleet. They show device status, KMF performance, and help with running and managing OTAK/OTEK operations. You can choose from a wide range of reports including Summary Reports, Detailed Reports, Cryptogroup Reports, Operation Status and Inspect Operation.

Fleet key currency

Provides visibility of your devices in the field and allows you to know the current E2EE key status of each device within your fleet of radios. Currency indicates if the radio or dispatch console positively acknowledges OTAK/OTEK commands sent by the KMF and if devices are loaded with the latest key as defined in the KMF.

Health state

For greater visibility of your end-to-end encrypted devices, the heath state is determined for each device separately, and it is calculated on the basis of several different parameters including: Last Inbound Timestamp, Zeroized, Currency and Locked out statuses. Additionally a graph with health information for all the devices is included in the Summary report. It is also an efficient way to find all the radios that did not communicate with KMF for the last 90 days or radios that have failed permanently.

The DIMETRA KMF is a secure solution

The DIMETRA KMF uses the hardware CRYPTR, with 128-bit or 256-bit Advanced Encryption Standard (AES) encryption, to provide secure key management features:

Key generation

The DIMETRA KMF uses the CRYPTR to generate E2EE keys to secure your voice and data communications.

KMF material protection

All keys stored on the DIMETRA KMF server are encrypted using a special key in the CRYPTR: the Primary Protection Key (PPK), which is needed to decrypt locally stored keys and never leaves the CRYPTR.

Secure transmission of keys

The DIMETRA KMF CRYPTR will encrypt the E2EE keys being sent out, and at the other end a CRYPTR or a Hardware Security Module (HSM) is used to decrypt the keys.

Hardware CRYPTR / Hardware Security Modules

Motorola Solutions provides strong security to protect your encryption keys and critical communications. This protection is achieved through the use of hardware-based cryptographic modules designed according to FIPS 140-3 specifications.

The cryptographic modules are used for both end-point encryption and decryption of E2EE communications, as well as by the KMF for key management operations. A cryptographic module in a TETRA portable or mobile radio is called a Micro Hardware Security Module (MicroHSM), and a cryptographic module used with a dispatch console or the KMF is called a CRYPTR module. The CRYPTR / MicroHSM modules provide a number of security mechanisms to protect your communications, including:

- **Secure boot:** Motorola Solutions CRYPTR / MicroHSM platforms only run signed code that is built by Motorola Solutions, to safeguard against malware being used to extract keys or modify cryptographic services.
- **Tamper protection and response:** The Motorola Solutions hardware CRYPTR / MicroHSM have tamper detection and response built in. Any attempt to try to probe or otherwise tamper with the crypto chip results in the keys being erased.
- **Environmental attack protection:** The CRYPTR / MicroHSM are also protected against environmental attacks that could push the crypto chip outside its normal operating parameters and compromise key security.

Specifications

The DIMETRA KMF supports:

- TETRA radios: Motorola Solutions TETRA mobile and portable radios that support E2EE
- Dispatch consoles:
  - Secure Dispatch Console - DIMETRA MCC7500S
  - Secure Dispatch Communications Server (S-DCS)
- Infrastructure: DIMETRA X Core running system release D9.4 or above

Supported encryption algorithms

- 128-bit AES
- 256-bit AES

Required hardware and software

- KMF server: Hewlett-Packard DL360 Gen10 server, running Microsoft ® Windows® Server 2019 operating system configured for DIMETRA
- Browser-based KMF client: Supported browsers are Google Chrome, Microsoft Edge or Chromium browser, on a PC running a Microsoft Windows operating system[2].
- Motorola Solutions KMF CRYPTR

Optional hardware

- USB modem for remote connection between E2EE KVL and the KMF

KMF CRYPTR electrical and physical specifications

- Power 12 V DC, 500 mA
- Dimensions 30 x 92 x142 mm
- Weight 300 g

KMF CRYPTR security and certifications

- FCC Part 15, Class A
- EN55022: 2010 Class A
- EN55024: 2010

[2] It is recommended to purchase a PC from Motorola Solutions and run Microsoft Windows 10 operating system configured for DIMETRA.

To learn more, visit:
www.motorolasolutions.com/dimetrakmf

MOTOROLA SOLUTIONS

All specifications are subject to change without notice

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