MOTOROLA SOLUTIONS

A SECURE, SCALABLE, AND PROVEN KEY MANAGEMENT SOLUTION

TETRA KEY MANAGEMENT FACILITY

Cybercriminals continue to increase both their speed and sophistication of cyber attacks. You are facing both economic and technical barriers that hinder your ability to ensure secure interoperable communications. Your organization is looking for the most effective and secure way to manage encryption keys across a growing number of devices within your network. You need a scalable, easy to deploy platform that provides greater visibility, allows for more control, and delivers enhanced security enabling you to respond faster, minimize risks, and stay ahead of cyber attacks.

The TETRA Key Management Facility (KMF) provides a robust and feature rich platform for effectively managing secure interoperable communications across all of your security enabled devices including TETRA two-way radios and dispatch consoles. The KMF removes the inherent complexity out of administrating and managing encryption keys. Keep your voice and data communications secure with encryption keys that update over-the-air without the delays, inconvenience or administrative costs of having users bring their devices into the shop for manual rekeying. The KMF gives you greater visibility and control of your deployed devices, so you can respond faster to changes in your environment and minimize the risk of compromising sensitive information. With the ability to generate, load, and delete keys on-demand via an intuitive interface you can stay ahead of your adversaries and better insulate yourself from attacks.

FEATURES:

Supported Devices

- TETRA Two-Way Radios with OTAR
- TETRA Dispatch Consoles

Greater Control of Your Operations

- Over the Air Rekeying (OTAR)
- Over the Ethernet Rekeying (OTEK)
- Automatic Rekey Opportunities
- Store and Forward
- Secure User Group Management

Greater Visibility of Your Devices

- KMF Hello
- Group Key Currency

SYSTEM COMPONENTS INCLUDE:

- Windows Server ®
- KMF Server and Client Software
- Windows ® Client
- KMF CRYPTR

HIGH ASSURANCE KEY MATERIAL STORAGE

All key material storage and key management messages within the system are backed by our CRYPTR hardware security module (HSM). The CRYPTR provides an attack-resistant and tamper-evident high assurance protection of all key material. The KMF can intelligently replenish encryption keys when inventories drop below the necessary volume freeing your reliance on 3rd party suppliers or manual key material generation.

HAVE GREATER CONTROL OF YOUR OPERATIONS

OVER THE AIR REKEYING (OTAR)

Keep your devices deployed in the field where they matter most, not in the shop. Eliminate the logistical and time consuming burden of manually rekeying devices on a regular basis by remotely and securely loading the essential key management updates to your devices via Over-the-Air Rekeying (OTAR). With OTAR you reduce the time to re-key devices and gain greater control of those devices by being able to update a device's keys, poll the device, and or erase the device's keys. OTAR simplifies the process of your key management strategy by making it easier to frequently change encryption keys for a greater cyber security posture. Simplified key management with OTAR makes it easier to eliminate threats like eavesdropping, man-in-the-middle attacks, and impersonation.

OVER-THE-ETHERNET KEYING (OTEK)

With Over-the-Ethernet Keying (OTEK) you can provide the same mechanisms for managing encryption keys as OTAR with the exception that messages are delivered over an ethernet connection. This is ideal for agencies with infrastructure products such as dispatch positions. OTEK eliminates the need to physically touch any of the dispatch positions and ensures that your dispatchers can communicate across multiple talk groups enabling secure interoperable communications.

AUTOMATIC REKEY OPPORTUNITIES

When devices are out of OTAR range and or powered down automatic rekey opportunities will intelligently update the devices when they are back on the system or powered back on so devices never miss a key update. Automatic rekey opportunities ensures your entire fleet of devices are loaded with current encryption keys.

EXTEND THE CAPABILITY OF OTAR WITH STORE AND FORWARD

When devices are out of OTAR range but require an immediate update you can take advantage of our TETRA Key Variable Loader (KVL 4000). The TETRA KVL 4000 provides a more localized tool for key distribution. The KVL 4000 transfers key management messages to out of range devices and acts as an intermediary between the KMF server and the device. Encryption key currency is maintained when the TETRA KVL 4000 is connected back to the KMF.

SECURE USER GROUP MANAGEMENT

In order to effectively manage secure communications among user groups a Common Key Reference (CKR) is utilized with the KMF. A CKR is a permanent system-wide three-digit key reference assigned to each talk group. With a CKR, an operator can visually track the members of a group and their associated encryption key. With the KMF, operators can send a new key to all members of a secure group with a single gesture.

HAVE GREATER VISIBILITY OF YOUR DEVICES

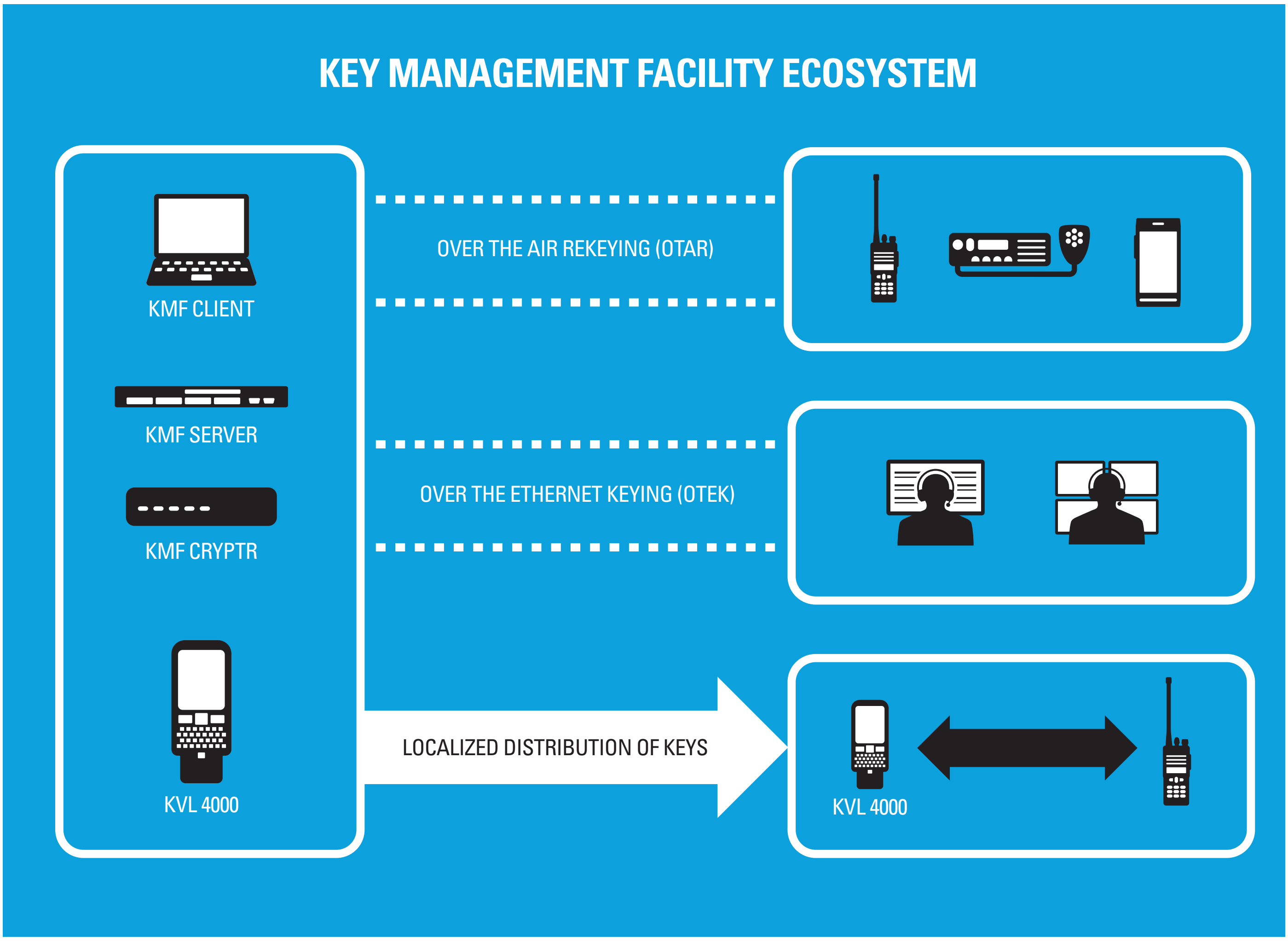
KMF HELLO

With KMF Hello you can easily see whether your devices are within range of the system network without introducing unnecessary voice traffic.

GROUP KEY CURRENCY

Group Key Currency ensures greater visibility of your devices in the field and allows you to know exactly which devices are not up to date with the latest encryption key.

KEY MANAGEMENT FACILITY ECOSYSTEM


KMF CLIENT
KMF SERVER
KMF CRYPTR
KVL 4000
OVER THE AIR REKEYING (OTAR)
OVER THE ETHERNET KEYING (OTEK)
LOCALIZED DISTRIBUTION OF KEYS
KVL 4000

KEY MANAGEMENT FACILITY SPECIFICATIONS

TETRA & SFPG FEATURES
Add, Modify, and Delete Keys
Zeroize
Change-Over
Rekey
Hello
Warm Start
AES Algorithms

MOTOROLA SPECIFIC FEATURES	
Multiple Encryption Algorithms Supported	AES 128 AES 256

PERFORMANCE AND CAPACITY
Up to 10 clients supported

KMF CRYPTR ELECTRIAL AND PHYSICAL SPECIFICATIONS	
Power	12VDC@ 500 mA
Dimensions (mm)	29.5 x 92 x142
Weight	300 g

KMF CRYPTR SECURITY AND CERTIFICATIONS	
Key Storage Capacity	1 Master Key per algorithm
FCC CRF 47	Part 15 subpart B for class B equipment
CE Certification	EN55022: 1998 EN55024: 1998

For more information on how you can quickly and easily manage encryption keys across your TETRA enabled two-way radios and dispatch consoles visit us at www.motorolasolutions.com/tetra