Alaska Land Mobile Radio Communications System

Key Management Facility Procedure 400-17

Version 5

June 25, 2018

Table of Contents

Document Revision History ii
Acronyms and Definitions iii
1.0 Introduction 1
2.0 Roles and Responsibilities 1
2.1 Executive Council 1
2.2 User Council 1
2.3 Operations Management Office 1
2.4 System Management Office 1
2.5 Security Manager 2
2.6 Agencies 2
3.0 Naming Conventions 2
3.2 Unit ID Naming Convention 4
3.3 Unique Key Encryption Key (UKEK) Naming Convention 5
3.4 Traffic Encryption Key Naming Convention 5
3.5 Common Key Reference Naming Convention 6
4.0 Initial Provisioning of Radios 6
5.0 Crypto Period Management 7
5.1 Keyset Changeover 7
5.2 Crypto Period Duration 7
6.0 Cryptographic Material Process Flow 8
7.0 Radio Programming Recommendation 8
7.1 Infinite Key Retention (IKR) 8
7.2 Key Loss Key (KLK) 8
8.0 Compromised Radio Management 8
8.1 Zeroize 9
8.2 Inhibit 9
8.3 Lockout 9
9.0 Radio Maintenance and Crypto Management 9
10.0 Management of System-wide Shared Key Material 10
11.0 Console Key Management and Provisioning 12
11.1 Store and Forward Provisioning 12
11.2 CKR Provisioning 15
12.0 System Maintenance 15
13.0 Compliance 16

Document Revision History

Name	Date	Description	Version
Shafer, Sherry	6/23/2014	New document - approved by the User Council; final.	V1
Shafer, Sherry	6/29/2015	Annual review/update. Approved by the Operations Management Office – final.	V2
Shafer, Sherry	6/28/2016	Annual review/update. Approved by the Operations Management Office – final.	V3
Shafer, Sherry	6/28/2017	Annual review/update. Approved by the Operations Management Office – final.	V4
Shafer, Sherry	6/25/2018	Annual review/update. Approved by the Operations Management Office – final.	V5

Acronyms and Definitions

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that operate on the shared ALMR system infrastructure.

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, which uses but is separate from the State of Alaska Telecommunications System (SATS), as established in the Cooperative and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

Department of Defense – Alaska: Alaskan Command, US Air Force and US Army component services operating under United States Pacific Command and United States Northern Command.

Executive Council: the ALMR Executive Council which is made up of three voting members and two associate members representing the original four constituency groups: the State of Alaska, the Department of Defense, Federal Non-DOD agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage)**.**

For Official Use Only (FOUO): this designation is used within the Department of Defense and the Department of Homeland Security to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact the conduct of federal programs, or other programs or operations essential to the national interest.

Interoperable Communications: the ability of public safety, including emergency and other first responders, to talk to one another via radio and other communication systems, and to exchange voice and/or data with one another on demand in real time.

Local Governments: those Alaska political subdivisions defined as municipalities in AS 29.71.800(13).

Member: a public safety agency including, but not limited to, a general government agency (local, state or federal), its authorized employees and personnel (paid or volunteer), and its service provider, participating in and using the System under a Membership Agreement.

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of over 300,000. The MOA stretches from Portage, at the southern border,

to the Knik River at the northern border, and encompasses the communities of Girdwood, Indian, Anchorage, Eagle River, Chugiak/Birchwood, and the native village of Eklutna.

Operations Manager: represents the User Council interests and makes decisions on issues related to the day-to-day operation of the system and any urgent or emergency system operational or repair decisions. In coordination with the User Council, the Operations Manager establishes policies, procedures, contracts, organizations, and agreements that provide the service levels as defined in the ALMR Service Level Agreement.

Operations Management Office (OMO): develops recommendations for policy, procedures, and guidelines; identifies technologies and standards; and coordinates intergovernmental resources to facilitate communications interoperability with emphasis on improving public safety and emergency response communications.

Security Manager (SCM): the individual responsible for establishing and maintaining security controls that ensure the availability, confidentiality and integrity of the ALMR System.

State of Alaska (SOA): the primary maintainer of the SATS (the states' microwave system), and shared owner of the System.

System Management Office (SMO): the team of specialists responsible for management of maintenance and operations of the System.

User: an agency, person, group, organization or other entity which has an existing written Membership Agreement to operate on ALMR with one of the Parties to the Cooperative Agreement. The terms user and member are synonymous and interchangeable.

User Council (UC): responsible for recommending all operational and maintenance decisions affecting the System. Under the direction and supervision of the Executive Council, the User Council has the responsibility for management oversight and operations of the System. The User Council oversees the development of System operations plans, procedures and policies under the direction and guidance of the Executive Council.

1.0 Introduction

This document describes methods and processes used to distribute cryptographic key material to radio and infrastructure devices in a P25 multi-zoned, trunked, two-way radio system. These procedures use a combination of over-the-air key distribution, where key material is sent over the air in an encrypted fashion, and also distributed through local key fill devices known as key variable loaders (KVLs). It is assumed that the reader has some knowledge about the features and capabilities of the Motorola™ Key Management Facility (KMF) and the associated products.

2.0 Roles and Responsibilities

2.1 Executive Council

The Executive Council (EC) shall be responsible for the management and enforcement of sanctions when violations of the Key Management Facility Procedure warrant such action.

2.2 User Council

The User Council (UC) shall be responsible for:

- Formal approval of the Key Management Facility Procedure, and any substantial revisions hereafter
- Reviewing all notices of violations and the recommended actions in the form of sanctions to be implemented, as provided by the Operations Manager and System Manager, prior to submittal to the EC

2.3 Operations Management Office

The Operations Management Office (OMO) provides oversight of the day-to-day operations of the ALMR System on behalf of the Executive Council and will, in coordination with the System Manager/Security Manager make recommendations regarding any actions to be taken when violations occur.

2.4 System Management Office

The System Management Office (SMO) is responsible for:

- System Database Backup
- Motorola Gold Elite Gateway (MGEG)/MCC7000 series Key Material Loading
- Assigning and tracking of all Common Key Reference (CKR) numbers

- Development and enforcement of Key Management Facility processes and procedures
- Interoperability/Incident Command key generation, as required
- Notifying the OMO immediately when violations of the KMF procedure occur and recommend appropriate action to be taken
- Taking appropriate steps to secure the ALMR System when violations of KMF procedures constitute a valid threat

2.5 Security Manager

The Security Manager (SCM) shall be responsible for:

- Review and coordination of substantive changes to the Key Management Facility Policy and Procedure
- Validation of compliance with applicable controls under the Defense Information Assurance Risk Management Framework (DIARMF)
- Report noted violations of KMF procedures to the OMO/SMO, which constitute a threat to the ALMR System

2.6 Agencies

Agencies operating KMF units associated with ALMR are responsible for following all policies, process, recommendations and System conventions regarding KMF management and oversight.

3.0 Naming Conventions

The ALMR System consists of multiple KMF units. Therefore, the coordination and cooperation between KMF managers involved with both setting up the KMF, and day-to-day operations, is imperative for the functionality of the encryption system.

Duplication between KMF databases will cause errors and inconsistent results during KMF operations. Approved naming conventions are outlined in this section to maintain the required consistency between the KMF units.

3.1 KMF Naming Conventions, Locations and Agencies

The individual KMF client units are named according to their physical locations. Each KMF server must have a unique name. This name will be used to enable key sharing and unit roaming capabilities (a possible future KMF feature) between multiple KMFs.

The KMF name, locations, points of contact (POCs) and the supported agencies are listed below.

NOTE: The Air National Guard and the Army National Guard are not included below as they are supported according to their mission and/or per agreement.

South Zone:

- **SOA_KMF client**
  Location: 5900 East Tudor Road, Suite 121
  KMF ID: CEN01
  POC: ALMR Help Desk
  Contact phone: (907) 334-2567
  Agencies Supported:
  - State government
    - Department of Public Safety
    - Department of Transportation
    - Department of Military and Veterans Affairs
  - Local Governments
    - Valdez Police Department
    - Municipality of Anchorage
    - Kenai Peninsula Borough
    - Matanuska-Susitna Borough
    - North Star Borough

- **JBER ELM_KMF client**
  Location: Elmendorf AFB, Building 6230
  KMF ID: CEN03
  POC: 673rd Communications Squadron
  Contact phone: (907) 552-2608/3077
  Agencies Supported:
  - Joint Base Elmendorf-Richardson

North Zone:

In the North Zone (Zone 2), the KMF server is located in Bldg 1192 at the Birch Hill master site

- **FWA_KMF client**
  Location: Fort Wainwright, Building 1061, Room 133, in the ALMR office
  KMF ID: CEN05
  POC: ALMR Office
  Contact phone: (907) 353-7171
  Agencies Supported:
  - United States Army-Alaska (USARAK)

- **EIE_KMF client**

Location: Eielson AFB, Building 3109, Room 117
KMF ID: CEN04
POC: NCOIC Base Radio
Contact phone: (907) 377-3837
Agencies Supported:
- o Eielson AFB
- o 168th Wing
- o Clear AFS

3.2 Unit ID Naming Convention

There are three pieces of information that must be unique for each radio unit listed in the KMF database. They are: 1) the radio name or alias; 2) the radio identification (RID); and 3) the radio serial number. These names must also be unique in the visited KMF terminal (future roaming feature).

It is up to the manager of each KMF terminal to create and follow a written procedure that describes how their naming convention is maintained, while using the following guidelines.

3.2.1 Radio Naming

All unit IDs begin with the unit location. **NOTE:** The example provided is the naming convention used by United States Army-Alaska (USARAK).

There are three sections to the Unit ID naming convention. (Example: FW PMO 42)

- The location of the KMF terminal: “FW” represents Fort Wainwright
- Owning unit, activity, department or city: “PMO” represents the Provost Marshal Office on Fort Wainwright
- Sequence number of the radio: “42” represents the forty second radio listed for the PMO

This is just one example of the Unit ID naming convention. The naming convention must begin with the unit location and the rest of the identifier is an agency preference. There are up to 35 characters in the radio name block allowing flexibility with the entries.

3.2.2 Radio Set Identifier (RSI). Using the radio unit ID is the easiest way to avoid duplication.

3.2.3 Radio Serial number. Each radio has a unique manufacturer serial number

3.3 Unique Key Encryption Key (UKEK) Naming Convention

The Key Encryption Key (KEK) is an encryption key used to encrypt Key Management Messages (KMMs) either over the air or to a Key Variable Loader (KVL) (Store and Forward session).

The Unique Key Encryption Key (UKEK) is a KEK used for inner layer encryption of over-the-air-rekeying (OTAR) of KMMs. The UKEK can be assigned to a single radio unit, a group of radios or assigned to all agency radios. The UKEK needs to be present in all transport devices prior to any OTAR operations.

Typically, every radio in the system has its own distinct UKEK. Multiple radios can have the same UKEK, but the use of a UKEK in more than one radio is less secure than having different UKEKs in every radio.

The naming convention for UKEKs and all other keys follow the same naming convention as with the Unit ID naming convention discussed in paragraph 3.2.

- UKEK name: FW UKEK XXXX
- FW - represents Fort Wainwright
- UKEK - represents the type of key
- “XXXX” - where "X" represents the sequence number or date material is effective

3.4 Traffic Encryption Key Naming Convention

A Traffic Encryption Key (TEK) is used to encrypt voice, data or KMMs. A good practice for TEK naming is to include a designator for the functional group and the time period for which the TEK is valid.

For example, AST JAN 06 references a TEK intended to be used by the Alaska State Troopers (AST) for January of 2006. Assignment of TEKs is made easier by creating significant TEK names.

Keys are transferred between the KMF and the KVL using two layers of encryption: an inner and outer layer. The inner layer encryption is performed using a UKEK, and the outer layer is performed using a TEK.

When generating a TEK, a Key Identification (KEYID) in hexadecimal will automatically be assigned by the KMF.

The KEYID must be changed, so there is no duplication between KMFs. The System Manager will assign and track KEYID numbers.

3.5 Common Key Reference Naming Convention

The Common Key Reference (CKR) is used to distribute TEKs to radios. A CKR contains two TEKs, one is active and the other is inactive. The active TEK is used to encrypt voice and data, while the inactive TEK is reserved for use during the next cryptographic period. The CKR is created and managed using the KMF.

CKRs are associated with talkgroups during radio Customer Programming Software (CPS) programming. A single CKR could be associated with one or multiple talkgroups.

CKR numbers must be coordinated in order to interoperate with other users. The System Manager will assign and track all CKR numbers.

The CKR name can be no longer than eight characters for the display on ASTRO 25 compatible radios. While the CKR names can be longer in the KMF, it is recommended that CKR name length is limited to eight characters, so that CKR names can be common for radio and KMF. CKR names are programmed using the CPS.

4.0 Initial Provisioning of Radios

There are two ways of initially provisioning a radio for OTAR. The first is to use the Store and Forward function of the KVL3000. It requires that a KVL3000 download key material from the KMF specifically for the radio to be provisioned. The advantage of the Store and Forward procedure is that the radio, so provisioned, is ready for service. In addition, the Store and Forward technique allows for easy distribution of an individual UKEK to each radio. For these reasons, Store and Forward is the preferred method.

NOTE: When using the Store and Forward method with EF Johnson radios, it is recommended that the KVL record in the KMF be marked for RED (unsecured non-encrypted) Store and Forward only.

As an alternative, a radio may be provisioned via loading a UKEK into the radio using a KVL. The KMF will then use the UKEK to fully rekey the radio over the air. This approach is referred to as the “shop key” approach. Using this approach, a UKEK is defined for use with all radios. As a radio is provisioned, it is loaded with the SHOP UKEK. Then, once the unit is entered into the KMF database, the KMF can provide a unique UKEK over the air. This new UKEK is encrypted with the SHOP UKEK.

Since the shop key uses the same UKEK in all radios, it is less secure than the individual UKEK approach. This is true because if the shop key becomes known to an adversary, then the adversary can perform inner layer decryption of all OTAR traffic on the System and the OTAR traffic would only be protected by outer layer encryption.

It is recommended that if the shop key approach is used, the KMF administrator generate a unique UKEK for each unit on the System and change the UKEK for each unit over the air using the KMF. This procedure will be performed as soon as practical to minimize the security risk.

5.0 Crypto Period Management

Crypto period management refers to the methods and procedures used to change the cryptographic key in use for voice encryption on a regular basis. The frequent change of encryption keys is essential to preventing an adversary from using a brute-force attack where the adversary attempts to use every possible key variable to decrypt a given message or other more sophisticated attacks.

The more frequently keys are changed, the less time the adversary has to refine an attack.

5.1 Keyset Changeover

Using the KMF dual keyset feature, a short message can be sent over the air that causes the radios to switch keysets. The dual keyset feature allows for a seamless transition between keys and also reduces data loading on the system. The keyset change command is typically sent at the start of each crypto period. Midway through the current crypto period phase, the KMF manager creates new traffic keys for each CKR in accordance with key name conventions and with key material distribution procedures.

In some applications, the use of two keysets is not approved or desirable. For these applications, instead of sending keyset changeover commands, the KMF manager can send a new key at the start of each crypto period. The KMF manager would put the same traffic key in each keyset slot of the CKR to be distributed.

Individual agencies are responsible for their own changeover policy.

5.2 Crypto Period Duration

A crypto period refers to the duration when a given set of cryptographic keys is used. The KMF managers set and manage the crypto period duration in accordance with each agency's requirement.

A 30-day period (or some multiple of 30 days) is recommended to facilitate MGEG/MCC7000 series key management as described in paragraph 11.0.

6.0 Cryptographic Material Process Flow

Each KMF manager is responsible for generating, or obtaining through approved means, the key material for their individual agency. For a discussion of interoperability key requirements, refer to section 10.0.

Each KMF is capable of randomly generating keys, or the KMF can import a file of keys provided by an external entity.

7.0 Radio Programming Recommendation

Within the Motorola™ CPS there are several programming areas that require operator input for the OTAR operations to work correctly. This section discusses Infinite Key Retention (IKR) and Key Loss Key (KLK) programming options.

7.1 Infinite Key Retention (IKR)

This is a radio feature that stores encryption material in non-volatile memory. Due to security concerns, it is recommended that this feature be disabled.

7.2 Key Loss Key (KLK)

This is a parameter in Motorola™ radios that allows the radio to receive a Unique Key Encryption Key (UKEK) encrypted with the KLK. This KLK is stored in non-volatile memory so that it is preserved in situations where the battery is removed or discharged. This feature can be useful in scenarios where radios are stored for an extended time period and then put into service.

Motorola™ subscriber programming requirements can be found in the Motorola™ “Secure CPS parameter recommendation guide,” dated 22 Jul 05 version 1.

Consult software Help screens or manuals for proper configuration during the programming of subscribers from other manufacturers.

Agencies should consult ALMR System Management Office (SMO) for guidance as to the programming of radios and the use of IKR or KLK features.

8.0 Compromised Radio Management

The intent of this section is to describe procedures to be taken when it is discovered that a radio has been lost, stolen or otherwise compromised. The Network Management Terminal (NMT) and the KMF terminal have tools to deal with compromised radios. The tools that the KMF terminal provides are:

8.1 Zeroize

This encrypted command can be sent to a radio to cause ALL cryptographic material to be erased.

8.2 Inhibit

This inhibit command causes the radio to be disabled. Radios are not to be in inhibited status for longer than 30 days (see Asset Management Procedure 400-8). The radio can be enabled with a command from the KMF. Since all commands are encrypted, if the KMF manager inhibits and then zeroizes a radio, the radio cannot be enabled from the KMF, since the enable command is encrypted.

NOTE: The inhibit/enable feature in the KMF is for Motorola™ subscribers only. To inhibit or enable subscribers by other manufacturers use the Radio Control Manager (RCM) program in the NMT.

8.3 Lockout

When a radio is compromised it must be marked as locked out in the KMF. Locked out units cannot be rekeyed by the KMF.

If a compromised radio is inhibited and then zeroized from the KMF, the radio cannot be enabled from the KMF, because the keys have been erased and the radio has no way to process the encrypted enable command. However, the radio can be recovered by using the unencrypted enable command available through the RCM.

If a radio is recovered in this manner, it is also necessary to issue the "Enable" command from the KMF to the recovered radio. Otherwise, the KMF will still indicate that the radio is inhibited. Failure to issue the "Enable" command will cause all other OTAR transactions with this radio to be unsuccessful.

ALMR policy requires that lost or stolen radios be reported immediately, so that the agency KMF Manager and/or the System Manager can take the steps necessary to limit the amount of encrypted traffic that could be monitored by a potential adversary.

Agencies will define their own compromised radio policies and incorporate the above statement into their procedures.

9.0 Radio Maintenance and Crypto Management

This section describes how the cryptographic material in a radio is handled when the radio is sent for service.

Radios that are sent for service have their encryption material erased (zeroized) prior to shipment. Radios are manually zeroized by the agency radio technician or operator. The agency KMF manager will "lock out" the radio in the KMF, so that the KMF does not process any rekey request messages from the radio. Radios can then be serviced at a trusted or non-trusted facility without concern about unauthorized personnel monitoring encrypted communications.

If an unauthorized user attempts a re-key request with the radio in this configuration, the radio will not generate the message; all necessary keys have been erased. To test encryption features for service purposes, service personnel can load test encryption keys locally using a KVL. Once service is complete, service personnel must erase the test keys used for encryption feature testing.

Consideration of the process used to return the radio to the user must be addressed in the agency's internal procedures. The radio must not have encryption material reprogrammed into the radio until it can be securely transferred to the user.

Once the user is in secure possession of the radio, then the agency KMF manager must be notified with a request that the unit be restored to the System. Upon verification that the user is legitimate, the KMF manager can remove the lockout status for this unit and provision the radio, as required.

10.0 Management of System-wide Shared Key Material

There are some communications scenarios that involve radio interoperability from multiple agencies. To support these scenarios, key material is shared between each KMF.

Key generation and distribution for the Incident Command interoperability keying material is the responsibility of the SMO.

Key generation and distribution for interoperability keying material that is utilized by United States Army-Alaska (USARAK), and shared with outside agencies, will be generated and distributed by a designated KMF terminal as identified in the agency's internal procedures.

Each interoperability CKR will be identified and tracked by the ALMR System Manager, as well as a corresponding TRANSPORT CKR. This TRANSPORT CKR is not distributed to radios, but is used to distribute key material to KMFs, via KVL, through a modem connection over the Public Switched Telephone Network.

NOTE: Transfers of key material from KMF to KVL are encrypted in the same manner as over-the-air key distribution.

The TRANSPORT CKRs are required because when a KVL receives keys during a dialup session with the KMF, it receives the ACTIVE keyset key from each CKR assigned to that KVL. During the point in the crypto period when a new key is being distributed, new keys from a source KMF to receiving KMFs, these new keys (for the next crypto period) are typically in the INACTIVE keyset of the CKRs.

The TRANSPORT CKR is used as a mechanism to move the inactive keyset TEK from the source KMF to the receiving KMFs. Once the TRANSPORT CKR has been downloaded into a KVL, the new TEK can be created at the remote KMF.

During the creation process, the KVL is specified as the source of the key material. The KVL is connected to the crypto card located in the KMF application server. Refer to the Motorola™ Managing Secure Communications, 68P81007Y75 Procedure 4-19, pages 4-33, for details on how to use the KVL as a source of key material.

The CKR distribution process is as follows:

- At the appropriate point in the crypto period (typically the midpoint of the period) a new interoperability TEK is created using the KMF auto-generate function or other approved key generation mechanism.
- The SMO associates each TEK with its corresponding TRANSPORT CKR, filling both the ACTIVE and INACTIVE keysets with the same TEK.
- The SMO confirms that KVLs from each agency are properly built in the KMF database, and that each KVL unit is configured to receive the appropriate TRANSPORT CKR.
- The SMO informs other agency KMF managers that new interoperability key material is available. The System Manager designates a time window for each agency KMF manager to connect to the SOA_KMF to receive the new keys. By using designated time slots, the phone line will only be connected to the SOA_KMF when required, and the KMF is protected from unauthorized dialup access attempts.
- In the designated time window, each agency KMF manager dials the SOA_KMF using their KVL. The appropriate TRANSPORT CKR will be transferred to their KVL.
- Each agency KMF manager then creates a new TEK at their KMF, and specifies the KVL as the source of key material. The TRANSPORT CKR is selected in the KVL, and the new TEK created in the target KMF is now identical to the TEK created in the SOA_KMF. At this point, the agency KMF manager can associate the TEK with the appropriate interoperability CKR.

This procedure is also used to transfer key material between individual KMF managers or agencies.

This procedure describes the use of a KVL and dialup modems to transfer keys between KMFs. With the introduction of networked key sharing between KMFs (supported in currently available KMF software upgrades), the use of this KVL procedure will no longer be required.

11.0 Console Key Management and Provisioning

This section discusses methods of provisioning encryption key material for Motorola™ Gold Elite Gateway (MGEG) and MCC7000s series encryption devices when more than one KMF is involved. This procedure is required for each console dispatch operator, to take part in secure communications. Store and Forward and Common Key Reference (CKR) provisioning are the two approaches discussed in this section. The Zone System Managers, as outlined in section 13.0, are responsible to ensure proper console loading.

11.1 Store and Forward Provisioning

In Store and Forward provisioning, a KVL can connect with each KMF in the system via direct connection or via dialup modem as required, receive encrypted Key Management Messages (KMMs) intended for the target MGEGs/MCC7000 series, and then by physical connection to each MGEG/MCC7000 series, deliver these key management messages (rekey messages) to the MGEG/MCC7000 series.

While the KMMs are stored in the KVL, they can only be transferred to the target unit MGEG/MCC7000 series. In this way, the MGEG/MCC7000 series administrator can be responsible for MGEG/MCC7000 series rekey duties and the agencies that source the key material do not need to worry about inadvertent distribution of their key material to unauthorized units. Store and Forward provisioning is strongly recommended due to this security aspect, and due to the relative simplicity of the procedure compared to CKR provisioning.

On remote access to KMF by KVL, for installations where the KMF(s) involved are not co-located with the target MGEGs/MCC7000 series, the KVL can be equipped with a modem to support transfer of key material over the Public Switched Telephone Network. (KMF application servers are equipped with two modems as a standard feature).

For some customers, internal network security policies discourage dial-up connections to networked computer devices. These security concerns can be satisfied by connecting KMF modems to telephone lines for a short, pre-defined window during each crypto period when the system can be monitored by a KMF operator to insure that unauthorized access attempts would be detected.

11.1.1 Store and Forward Assumptions

- A KVL3000 PLUS (required for AES encryption) with CKR option is stored at the MGEG/MCC7000 series location.
- The KVL is equipped with a modem for dial-up operation.
- The KVL is built as a KVL unit in each KMF in the system.
- The KVL record as created in each KMF has the same Radio Set Identifier (RSI) and Unique Key Encryption Key (UKEK).
- Except for initial provisioning, all Store and Forward to MGEGs/MCC7000 series is done in BLACK (secure, encrypted) mode.
- All KMFs must use the same UKEK and RSI for a given target MGEG/MCC7000 series module.
- KMF administrators must coordinate CKR numbers and Traffic Encryption Key (TEK) KEY IDs to insure that CKRs and KEY IDs are not duplicated.
- Each agency that wants to have its key material loaded into the MGEGs/MCC7000 series shall provide two KVL3000 PLUS keyloaders, one at each MGEG/MCC7000 series location.

11.1.2 MGEG/MCC7000 series Rekey

It is recommended that all agencies set a cryptographic period of 30 days or some multiple of 30 days. When all KMFs are maintaining the same crypto period duration, there are two options for MGEG/MCC7000 series rekey timing.

- A KVL is used to manually rekey the MGEG/MCC7000 series during the first day of the crypto period. Since information about active keyset is included in the store-and-forward message sequence, this procedure is performed on the first day of the new crypto period, after the new keyset has been activated.
- The second procedure can be performed at any time during the last half of the crypto period, during the time that is normally associated with rekey of radio units. A KVL is used to manually add the inactive keyset and again to change keysets at the MGEG/MCC7000 series during the first day of the crypto period. Since this method requires that MGEGs/MCC7000 series be removed from service twice (once for rekey and once for keyset changeover), it is less desirable.

BLACK Store and Forward is specified for this procedure. BLACK and RED (unsecured, non-encrypted) Store and Forward are discussed on page 4-82 of the Motorola 6881009Y65 MANAGING SECURE COMMUNICATIONS document. BLACK Store and Forward is specified here to ensure that the KMMs transferred from KMF to KVL to MGEG are encrypted with key material contained in the target MGEG/MCC7000 series. In this way, they cannot be processed and decrypted by any other unit.

NOTE: The initial Store and Forward session will be RED due to the fact the KMF “knows” that the target MGEG/MCC7000 series has not yet been provisioned, so it has

no encryption keys to decrypt a BLACK Store and Forward. The initial Store and Forward session will be supervised by a representative of the agency that is sourcing the key material. Otherwise, the KMF manager is responsible to secure the key. If an adversary gains access to the KVL, they could use it to read the RSI of a target MGEG/MCC7000 series, configure a radio with the RSI, and then configure a radio to intercept the Store and Forward messages intended for the MGEG/MCC7000 series.

Since subsequent Store and Forward sessions are BLACK, no supervision is required. Refer to procedure 4.52 of the Motorola 68P81009Y65, MANAGING SECURE COMMUNICATIONS for details about the Store and Forward process. Prior to MGEG/MCC7000 series Store and Forward session, the Zone System Manager is required to open a case with the Motorola System Support Center to inform technicians that an MGEG/MCC7000 series will be going out of service.

11.1.3 MGEG/MCC7000 series Distribution Process

- The MCC7000 series uses a VPM encryption device and gets its keys via Over the Ethernet Rekeying (OTEK)
- At each agency KMF, the KMF Manager associates the target MGEGs series to the KVL to be used to load the MGEG. The ALMR system has two MGEGs per zone. Each MGEG has two crypto cards that require Store and Forward update. This step is performed only once per KMF
- For each MGEG crypto card, the Zone System Manager uses the KVL to set the Message Number Period (MNP) for each MGEG secure card to 65535. This step is performed once per MGEG crypto card. The MNP can be set as follows:
  - Disable the target MGEG from call processing using the Zone Configuration Manager (ZCM) and wait for the disable to complete.
  - Using the KVL, select TARGET/LOAD/MNP. Prompt message says “ENTER THE MNP”
  - Use KVL keypad to enter 65535
  - Connect KVL to MGEG crypto card and press LOAD. Repeat for the second crypto card
  - Enable the MGEG at the ZCM
- The Zone System Manager selects a KMF, establish a Store and Forward session via direct connection or modem as required, and initiate a KVL download to place the appropriate Store and Forward key management messages into the KVL. Refer to procedure 4.52 of the Motorola 68P81009Y65 for details about this procedure. This step is performed for the KVL/KMF combination for each agency that is supplying a Store and Forward session for the target MGEG.
- The Zone System Manager disables the target MGEG from call processing using the ZCM and wait for the disable to complete

- The Zone System Manager performs a Store and Forward update to each crypto card in the target MGEG. This step is repeated using the KVL from each agency supplying a store-and-forward session to the target MGEG
- Re-enable the MGEG using the ZCM
- Repeat steps 4 through 6 for each MGEG associated with the zone

If the encryption keys are lost in an MGEG/ for any reason, then BLACK Store and Forward sequences initiated by any KMF will fail. In this case, simply reconnect with each KMF (repeat steps 3-6) and the KMF will deliver RED Store and Forward to re-provision the MGEG.

NOTE: RED Store and Forward sessions must be supervised by agency representatives.

11.2 CKR Provisioning

CKR provisioning is only used for special circumstances when Store and Forward is not practical or possible. Like Store and Forward provisioning, a KVL is used to download key material from each KMF in the system. In this procedure, because of certain product constraints, significant manipulation of key material must be performed before the key material can be transferred to the MGEG/MCC7000 series. In addition, once the key material is downloaded to the KVL, it can be transferred to a radio or unit other than the intended MGEG/MCC7000 series. Consequently, participating agencies need to designate a representative to be present during the key transfer between the KVL and the MGEG/MCC7000 series, and verify that the key material is erased from the KVL after the MGEG/MCC7000 series key loading procedures are complete.

This procedure is resource intensive requiring personnel to travel to each of the zone controllers at least once per crypto period. The cost of travel and logistics involved quickly becomes prohibitive. This procedure is not laid out in detail in this document, because it is not recommended for use on the ALMR System.

12.0 System Maintenance

It is recommended that the KMF application server and the KMF database server be restarted at an interval not to exceed one month. By restarting the computers, certain cleanup operations can take place resulting in more stable, reliable system operation.
NOTE: A complete shutdown and restart will take the OTAR system out of service for approximately 20 minutes.

13.0 Compliance

Compliance with the Key Management Facility Procedure is outlined in ALMR Key Management Facility Policy Memorandum 400-17.