Security Policy

MOTOROLA ACCOMPLI™ 009 PERSONAL COMMUNICATOR

ENCRYPTION SERVICES MODULE

MOTOROLA
intelligence everywhere™

REV 1.2, 10/2002

CONTENTS

MODULE OVERVIEW

The software cryptographic boundary is the Encryption Services Module (ESM), which is a software component of the Motorola Accompli 009 operating system.

Accompli 009 Personal Communicator

The Accompli 009 Personal Communicator integrates mobile e-mail, wireless internet access and GSM phone features in a small, handheld wireless communicator. The device features a 56-key QWERTY keyboard, tri-band GSM/GPRS phone and internet-enabled browser.

Motorola MyMail™ Enterprise and *Motorola MyMail* Desktop Plus offer secure wireless e-mail capability for the Accompli 009. Both solutions provide secure, wireless e-mail capability by using the Accompli 009 as a wireless e-mail device. *Motorola MyMail* Enterprise installs on the Motorola Messaging Server while *Motorola MyMail* Desktop Plus installs on an individual user's PC. Both solutions allow subscribers to have wireless access and management of desktop e-mail, providing a complete client/server solution.

SCOPE OF DOCUMENT

The following document constitutes the security policy for the cryptographic module within the Motorola Accompli 009 wireless messaging device. This security policy addresses all of the applicable requirements of FIPS 140-1, includes an overview of the cryptographic module, and lists roles and services of the module and how they are related, including the different types of security relevant data items (keys, key components), capabilities and protections.

TERMS AND DEFINITIONS

Term	Definition
ANSI X9.31	Standard of “Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry”
DAC	Data authentication code
DDK	Default device key
DES	Data encryption standard
DESMAC	A type of integrity-checking (checksum) based on DES
ESM	Encryption services module
GSM	Groupe Special Mobile, a second generation cellular phone standard
KAT	Known answer test
KMR	Key management request
PRNG	Pseudo-random number generator
RC4	A stream cipher not approved under FIPS
SHA-1	A hashing algorithm
SRDI	Security relevant data items
Subscriber	User, application
TDES	Triple-DES, a block cipher approved under FIPS
UDK	Unique device key

SECURITY LEVEL

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-1. The module embodiment is a multi-chip embedded device.

Security Requirements Section	Level
Cryptographic Module	1
Module Interfaces	1
Roles and Services	1
Finite State Machine	1
Physical Security	1
Software Security	3
Operating System Security	1
Key Management	3
Cryptographic Algorithms	1
EMI/EMC	3

Self Test	1

ROLES AND SERVICES

The cryptographic module supports three distinct roles. These roles are:

- **Application Role (User Role):** This is a software application that calls the lower layer services available in the module.
- **Crypto-Officer Role:** The purpose of this role is to load a Subscriber key. The module will verify the password before performing the requested service.
- **Superuser Role:** The purpose of this role is to allow updates of the system-level operating software. The superuser must be authenticated.

The cryptographic module enforces the separation of roles using role-based authentication.

The User Role provides access to the following authenticated FIPS services:

- **Update:** This service generates a new Subscriber Key and stores it (TDES encrypted) in flash memory. Since the key replaces an existing key, the old key is updated with the new value, provided authentication succeeds. Subsequent access to subscriber keys is controlled by the passwords provided when they were created.
- **Encrypt:** This service is used to TDES encrypt data. This service also supports a non-FIPS encryption algorithm: RC4. All encryption keys are tagged with algorithm type to ensure that keys generated in a FIPS-approved manner are used only with FIPS-approved algorithms.
- **Decrypt:** This service is used to TDES decrypt data. This service also supports a non-FIPS decryption algorithm: RC4. All encryption keys are tagged with algorithm type to ensure that keys generated in a FIPS-approved manner are used only with FIPS-approved algorithms.

The Crypto-Officer Role provides access to the following services:

- **Process:** This key exchange (key receipt) service accepts the newly generated Subscriber Key (see Create), decrypts it, verifies the sender, and stores the key (TDES encrypted) in flash memory.

The Superuser Role provides access to the following services:

- **Read/Write Device Memory:** This service allows read/write access to flash memory. Access is denied to sensitive areas of memory, including the areas where the default device key (DDK) and unique device key (UDK) are stored.

The following services are not authenticated:

- **Create:** This service generates a new Subscriber Key and stores it (TDES encrypted) in flash memory. Subsequent access to subscriber keys is controlled by the passwords provided when they were created.
- **Zeroize Keys:** This service zeroizes all plaintext cryptographic keys stored in the device.
- **Self-Test:** This service performs the following self-tests at power-up and upon demand:
  - Software/Firmware integrity test via DESMAC
  - TDES KAT
  - DES KAT
  - SHA-1 KAT

- **Get Status:** This service provides status information regarding the cryptographic module, specifically whether services are disabled.
- **SHA-1:** The device has the ability to perform a SHA-1 hash on a block of data.
- **RollData:** The device has the ability to perform a SHA-1 data reduction (folding operation) on a block of data.
- **Encode:** This service converts binary data into expanded text.
- **Decode:** This service converts expanded text into binary data.
- **Rand:** This service is used to generate a random number using the ANSI X9.31 PNRG.
- **Init KMR:** This service is used to initialize memory allocated by the ESM in preparation for calling the Encrypt and Decrypt services.
- **Deinit KMR:** This service is used to de-initialize memory allocated by the ESM after calling the Encrypt and Decrypt services.

SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-1 Level 1 module[1].

1. The cryptographic module supports three roles, the Application Role (User Role), the Crypto-Officer Role and the Superuser Role. The module does not support a maintenance role.
2. The cryptographic module provides role-based authentication for some services.

   Note: *Presently the module can potentially support a maximum of 3,000 subscribers.*

3. The module does not support a Bypass state.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The chips are of production-grade quality, which includes standard passivation techniques.
6. The module is implemented as a production-grade multi-chip embodiment.
7. The module supports the following FIPS approved cryptographic algorithms:
   - TDES
   - DESMAC
   - SHA-1
   - PRNG per ANSI X9.31

   Note: *The module also supports the RC4 algorithm; this algorithm is not used in FIPS mode.*

8. 99.9% of the module is written using a high level language, C; the other 0.1% is written in Motorola 68000 assembly.

   Note: *The rationale for the limited use of assembly is that the crypto module interface mechanism cannot be implemented in 'C' since it requires Motorola 68000 trap instructions.*

9. The operating system present in the module is Microware OS-9, version 2.2.
10. The cryptographic software/firmware is installed only as executable code.
11. A FIPS approved authentication technique is applied to the cryptographic software within the module. This cryptographic mechanism is incorporated as part of the Software/Firmware via a DESMAC.

---

1. Rules are contained in the numbered paragraphs. Other information is included for background purposes only and are shown in italics.

12. The cryptographic module is limited to a single user at a time.
13. Use of the cryptographic module is dedicated to the cryptographic process during the time the cryptographic process is in use.
14. The module does not distribute cryptographic keys in plaintext form.
15. The module does not support manual key entry/output.
16. The module provides a mechanism to ensure that keys are associated with the correct entity by the following means:
    - Before keys can be accessed, the subscriber ID is checked to verify that a valid subscriber is requesting access to the cryptographic keys.
    - Each key is identified with a key index.
    - Each key contains an algorithm identifier.
    - Each key is stored with a password provided when the key is created. Any subsequent requests involving that key are allowed only if the password supplied in the request matches the password when the key was initially created.
    - Each key includes an encrypted CRC value designed to protect key material from unauthorized modification.
17. The cryptographic module assists in archiving cryptographic keys. All archived keys are TDES encrypted via the UDK.
18. The module supports up to eight Subscriber keys per subscriber.
19. The module performs the following conditional tests:
    - Continuous random number generator test
    - Software/firmware load test (DESMAC). Immediately after a software download, the module's power is cycled and the module performs a DAC verification over the loaded image.

DEFINITION OF SECURITY RELEVANT DATA ITEMS (SRDI)

The following lists the cryptographic keys that are contained in the module:

- **Default Device Key (DDK):** This is a TDES key used to decrypt all cryptographic keys that are initially delivered with the module (before it powers up / initializes for the first time.)
- **Unique Device Key (UDK):** This is a TDES key used to encrypt/decrypt all critical security parameters (CSPs) stored within the module. It is created via ANSI X9.31 during the personalization process (when the module initializes for the first time).
- **Root Key:** This is a TDES key used to encrypt the Subscriber key before transport.
- **Subscriber (User) Key:** This is a TDES key used to encrypt data.
- **PRNG Key:** This is the key used during the PRNG process per ANSI X9.31.
- **DAC Key:** This is a DESMAC key used to authenticate the Software/Firmware power-up self-test.

The following lists the other SRDIs that are contained in the module:

- **Server Password:** This is the password used to authenticate the Crypto-officer role.
- **Key Password:** This is used to access keys contained in the module.
- **Subscriber ID:** This is used to authenticate the User role.
- **Superuser Password:** This is used to authenticate the Superuser role.