KEY-UP Cryptographic Module

V 5.1

Security Policy

Document *Version 0.3*

Ian Donnelly Systems, Inc.

(IDS)

October 8, 2010

Table of Contents

Tables

Figures

1 Module Overview

The KEY-UP V5.1 Cryptographic Module is a multi-chip standalone cryptographic module encased in a hard opaque commercial grade steel case. The primary purpose for this device is to provide data security for Electronic Funds Transfer (EFT) transactions. The device provides power, status and activity output (Version II-A only) via LEDs. The device provides network interfaces for data input and output. The figures below illustrate these interfaces and define the cryptographic boundary.

The boundary of the module is the outer perimeter of the metal enclosure. No components are excluded from the cryptographic boundary.

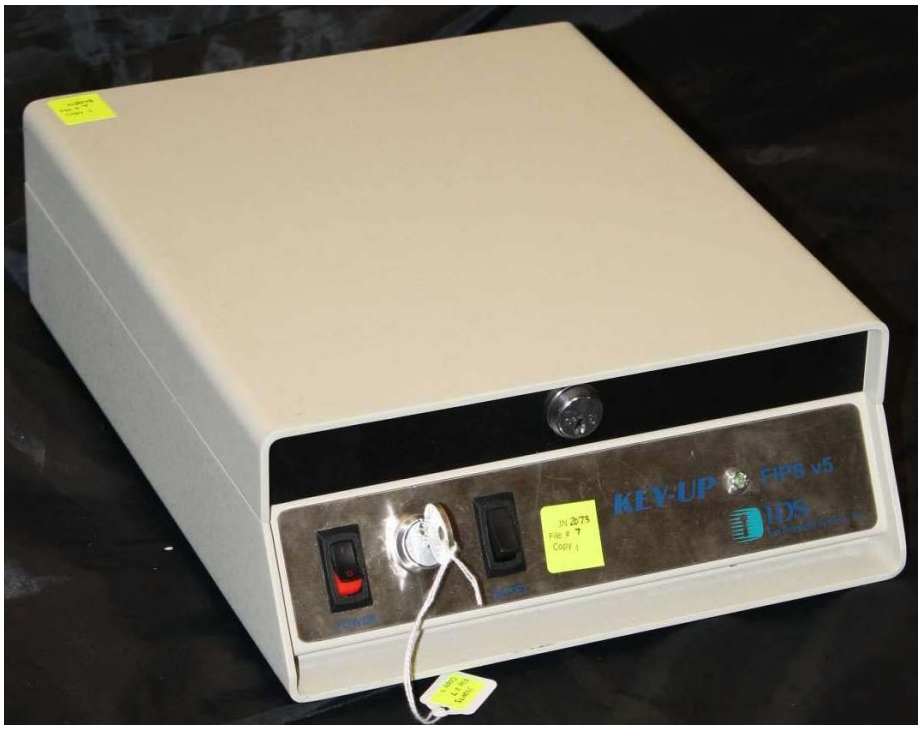
The configuration of hardware and firmware for this validation is:

Hardware: P/N KEY-UP, Versions II-A and III-A

Firmware: Version 5.1

Figure 1: KEY-UP Version III-A

Figure 2: KEY-UP Version II-A



2 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

The KEY-UP Cryptographic Module operates in the FIPS mode of operation by default from the factory. The following FIPS Approved algorithms are supported:

- Triple-DES (TECB and TCBC modes, two-key and three-key) for encryption and decryption (Cert. #900)
- Triple-DES MAC (ECB) for data integrity (Cert. #900, vendor affirmed)
- SHA-1 for hashing (Cert. #359)
- ANSI X9.31 RNG (Cert. #127)

The following non-FIPS Approved algorithms are supported, but are not used to provide any cryptographic strength to the module's security (all are further encrypted using Triple-DES):

- Derived Unique Key Per Transaction (DUKPT) for decryption
- DES (ECB) for encryption and decryption (non-compliant)
- TR-31 for operability with financial institutions

Execute the KEY-UP Show Status service to view which mode the module is operating in.

3.2 Non-FIPS Approved Mode of Operation

The KEY-UP Cryptographic Module may also be configured for operation in a non-Approved mode. In order to configure the module for non-Approved mode, execute the KEY-UP Operating Mode service and select not to operate in the Approved mode.

Note: The module supports the same algorithms in the Approved mode and the non-Approved mode.

4 Ports and Interfaces

The cryptographic module supports a data input, data output, control input, status output, and a power interface. The following table describes the physical ports that the cryptographic module provides and also lists the logical interfaces associated with these ports:

Table 2: KEY-UP FIPS 140-2 Ports and Interfaces

Physical Ports	Logical Interfaces
Asynchronous RS232 (Keys)	Data input, Data output, Control Input, Status Output
Asynchronous RS232 (Data)	Data input, Data output, Control Input, Status Output
Ethernet (1 on IIIA, 2 on IIA) Second port on IIA not used	Data Input, Data Output
LEDs (4 on IIIA, 1 Status only on IIA)	Status, Power, Command, Response: Outputs
Mechanical Lock	Control Input
Reset Switch	Control Input
Power Switch	Control Input, Power
Power Port	Power

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module shall support *four* distinct roles (User, Key Custodian/Cryptographic Officer, Administrator, and Operator). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. An operator must enter a user-name and password to authenticate or must provide a user-name and prove knowledge of a 128-bit shared secret to log in. The user-name is an alphanumeric string of up to eight characters. The password is an alphanumeric string of eight characters randomly chosen or user selected from the 62 alphanumeric characters: A-Z, a-z, 0-9. No previous authentications are maintained across power downs.

Table 3: Roles and Required Identification and Authentication

Role	Authentication Type	Authentication Data
User	Identity-based operator authentication	User ID, Shared Secret (128-bit shared secret)
Cryptographic-Officer	Identity-based operator authentication	User ID, Password
Administrator	Identity-based operator authentication	User ID, Password
Operator	Identity-based operator authentication	User ID, Password

Table 4: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password Entry	The IDS KEY-UP passwords are 8 characters in length composed of the 62 characters 0-9, A-Z, a-z. The probability of guessing a password on one attempt is $1 / 62^8$ or 1/218,340,105,584,896 which is less than 1/1,000,000. KEY-UP is configured using a serial connection at a speed of 9600 bps. There could at the very most be 75 attempts at password entry in one minute. Therefore, probability of guessing the password in one minute is $(75 * 1/62^8)$, which is less than 1/100,000.
Shared Secret	The shared secret is a 128-bit Triple-DES key. The probability of guessing the shared secret on one attempt is $1 / 2^{128}$ which is less than 1/1,000,000. KEY-UP is configured using a serial connection at a speed of 9600 bps. There could at the very most be 75 authentication attempts in one minute. Therefore, the probability of guessing the password in one minute is $(75 * 1/2^{128})$, which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 5: Services Authorized for Roles

Role	Authorized Services
User:	• PIN Translation: Decrypt Personal Identification Number (PIN) using PIN Encryption Key and encrypt it using another specified encryption key. • PIN Verification: Verify an encrypted PIN block. • PIN Change: Change a PIN and optionally verify the PIN. • PIN Offset Generation: Generate a PIN offset for use in PIN verification. • VISA PVV Generation: Generate a Visa PIN Verification Value (PVV) for use in PVV Verification. • Data Encrypt: Encrypt data using Triple-DES. • Data Decrypt: Decrypt data using Triple-DES. • CVV/CVC Generation: Generate a Card Verification Value (CVV) or Card Verification Code (CVC) for the purpose of verifying a credit card. • CVV/CVC Verification: Verify a CVV or CVC of a credit card. • MAC Generation: Generate a Message Authentication Code (MAC) for the purpose of providing data integrity. • MAC Verification: Verify a MAC. • Generate "Working" Key: Generate a Triple-DES key for the encryption of various data. • Key Translation: Decrypt a key using one key and re-encrypt using another key. • Change ATM Key: Generate a Triple-DES key and encrypt it with the ATM A or B Key.
Key Custodian/ Cryptographic-Officer:	• Key Entry: Manually establish, electronically enter a split knowledge key. • KEY-UP Show Status: Show the status of the module (i.e., version of the module, state of the keys, checksums, etc.) • Install Key: Install the entered key into persistent memory. (This service is only available when a MFK or KEK has been entered.) • Display Cryptogram: Triple-DES encrypt the last key entered with the MFK and output to console. • Generate Random Value: Generate a random value • Log out
Operator:	• KEY-UP Show Status: Show the status of the module (i.e., version of the module, state of the keys, checksums, etc.) • Log out

Role	Authorized Services
Administrator:	• All of the functions listed for Cryptographic Officer and Operator in addition to those listed below: • Configure TCP/IP: Configure the TCP/IP settings. • Configure KEY-UP Operating Mode: Configure the baud rate and protocol in use for communication. Select or deselect the FIPS mode of Operation • User Maintenance: Add user, list user, delete user, update user. • Clear KEY-UP Security Keys: FIPS140-2 Zeroization service. This service actively zeroizes all keys, both persistently stored and non-persistently stored CSPs, from memory

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- LED status: This service provides the current status of the cryptographic module via the LEDs: Power, Status, Activity (Command and Response LEDs).
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power-cycling the module.
- Monitor: This service is used to verify the status and general information of the module

6.3 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Table 6: Private Keys and CSPs

Key	Description/Usage
Master File Key (MFK)	*112-bit or 168-bit TDES key used to encrypt all keys used by the module. All key data entering/exiting the module is decrypted/encrypted by the module.*
Key Exchange Key	*112-bit or 168-bit TDES key used to encrypt/decrypt outgoing/incoming session keys.*
PIN Encryption Key	*112-bit or 168-bit TDES key used to encrypt PINs*
Data Encryption Key	*112-bit or 168-bit TDES key used to encrypt data.*
Message Authentication Key	*112-bit or 168-bit TDES key used to generate/verify TDES message authentication codes of 32, 48, or 64 bits in length.*
ATM A Key	*112-bit or 168-bit TDES key used to facilitate the generation of ATM encryption keys (encrypts the ATM B key OR is encrypted by the ATM B key).*
ATM B Key	*112-bit or 168-bit TDES key used to facilitate the generation of ATM encryption keys (may encrypt the ATM A key OR is encrypted by the ATM A key).*

Key	Description/Usage
Seed Key	*128-bit value used by the ANSI X9.31 DRNG for the creation of random numbers and cryptographic keys.*
Passwords	*Used to authenticate operators to the module.*

6.4 Definition of Public Keys

The module does not support public keys.

6.5 Definition of CSPs Modes of Access

Table 7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- Generate: The module generates the CSP.
- Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- Destroy: The module zeroizes the CSP.

Table 7: Service to CSP Access Rights

Service	Cryptographic Keys and CSPs Accessed									
PIN Translation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X		X						
	Write									
	Destroy									
PIN Verification		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X		X						
	Write									
	Destroy									

Service	Cryptographic Keys and CSPs Accessed									
PIN Change		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X		X						
	Write									
	Destroy									
PIN Offset Generation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X		X						
	Write									
	Destroy									
VISA PVV Generation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X		X						
	Write									
	Destroy									
Data Encrypt		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X			X					
	Write									
	Destroy									
Data Decrypt		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X			X					
	Write									
	Destroy									
CVV/CVC Generation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X				X				
	Write									
	Destroy									

Service	Cryptographic Keys and CSPs Accessed									
CVV/CVC Verification		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X				X				
	Write									
	Destroy									
MAC Generation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X				X				
	Write									
	Destroy									
MAC Verification		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X				X				
	Write									
	Destroy									
Generate “Working Key”		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate		X	X	X	X	X	X	X	
	Read	X	X							
	Write									
	Destroy									
Key Translation		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X	X	X	X	X	X	X		
	Write									
	Destroy									
Change ATM Key		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate						X	X		
	Read	X					X	X		
	Write									
	Destroy									

Service	Cryptographic Keys and CSPs Accessed									
Key Entry		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X	X	X	X	X	X	X	X	
	Write	X	X	X	X	X	X	X	X	
	Destroy									
Install key		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X	X							
	Write	X	X							
	Destroy									
KEY-UP Show Status		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X	X							
	Write									
	Destroy									
Configure of TCP/IP		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read									
	Write									
	Destroy									
Display Cryptogram		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read	X	X	X	X	X	X	X		
	Write									
	Destroy									
Clear KEY-UP Security Keys		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read									
	Write									
	Destroy	X	X	X	X	X	X	X	X	X

Service	Cryptographic Keys and CSPs Accessed									
Generate Random Value		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read								X	
	Write								X	
	Destroy									
Logout		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read									
	Write									
	Destroy									
Configure KEY-UP Operating Mode		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									
	Read									
	Write									
	Destroy									
User Maintenance		MFK	KEK	PEK	DEK	MAK	ATM A	ATM B	Seed Key	Pass-words
	Generate									X
	Read									
	Write									
	Destroy									

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the KEY-UP Cryptographic Module is a non-modifiable operational environment.

8 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The cryptographic module shall provide four distinct roles. These are the User role, Administrator role, Operator role, and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:
   A. Power up Self-Tests:
      1. Cryptographic algorithm tests
         a. TDES Known Answer Tests (2 key and 3 key)
         b. RNG Known Answer Test
         c. SHA-1 Known Answer Test
      2. Firmware Integrity Test: 16-bit CRC
      3. Critical Functions Tests
         a. BB-SRAM Read/Write Test
   B. Conditional Self-Tests:
      1. Continuous Random Number Generator (RNG) Test
      2. Split-Knowledge Key Integrity Test
5. At any time the cryptographic module may be commanded to perform power up self-tests by power-cycling the module.
6. Power-up self tests do not require any operator action.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. The module shall not support concurrent operators.

9. Split key entry is required for all plain text keys entered into the module, whether they are loaded into the module, or used externally. The module supports from 2 to 9 key parts which are combined to create the key. The only possible way to ascertain the final key is to know all parts entered to create the key. There is no way to obtain the resulting key with only one key component.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone cryptographic modules include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with pick-resistant locks.
- Automatic zeroization when enclosure is opened.
- Tamper response and zeroization circuitry.
- Protected vents (KU-IIA only).

The end user must check the module for signs of tampering every 3 months. The signs of tampering would include scratches, dents, and any other indication that the module has been tampered with. If identified, the module should be removed from service and inspected further.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.