SC20-DES Security Policy

Version 0.3
26-Mar-98

Scope:

This document describes the security policy of the SC20-DES module. The security policy lists the roles and services supported by the SC20-DES and also describes the rules under which the module operates.

Security Level:

The SC20-DES module meets the overall requirements applicable to FIPS 140-1 Level 1 security. Within the 12 categories of FIPS 140-1, the SC20-DES meets the following security levels.

Cryptographic Module	1
Module Interfaces	1
Roles & Services	1
Finite State Machine	1
Physical Security	1
EFP/EFT	n/a
Software Security	1
Operating System Security	n/a
Key Management	1
Cryptographic Algorithms	1
EMI/EMC	1
Self-Tests	1

Module status is to be output on the four external status lines. The DSP transmits the current status, via its serial port, to the PIC microprocessor. The PIC, which is outside the cryptomodule, then displays the status on the four external status lines. The DSP sends status to the microprocessor upon entry to each state.

Physical security is achieved by using hard coating to protect the DSP. This coating prevents probing the DSP pins to read the flash.

Roles & Services:

The SC20-DES supports two operator roles. These roles are:

1-User
2-Crypto Officer

The user role provides all services necessary to encrypt and decrypt information passing through the module. This includes the following services:

- Encrypt
- Decrypt
- Show Status
- Self Test

The Crypto Officer role provides all the services necessary to load a key into the module. This includes the following services:

- Key Load
- Zeroize

NOTE: The crypto officer also has access to all user services as well.

The SC20-DES Module does not require either role-based or identity-based authentication.

The exempted software can undergo revision changes without need for certification. The DSP is the only hardware device in the boundary and cannot be substituted or changed without recertification.

Security Rules:

The following security rules are enforced by the SC20-DES to achieve Level 1 security:

- The SC20-DES supports a User role and a Crypto Officer role.

- The SC20-DES encrypts and decrypts information using the Data Encryption Standard (DES) and described in FIPS46-2 operating in the 64-bit output feedback mode (OFB) described in FIPS81.

- Each message encrypted by the SC20-DES will be preceeded by a 64-bit initialization vector (IV) which is generated as described in ANSI X9.17 Annex C.

- Throughout each message encrypted by the SC20-DES, a new initialization vector (IV) will be inserted into the message every 22 blocks of 64 bits (I.e. every 1408 bits) for the purpose of facilitating late entry resynchronization.

- All initialization vectors (IVs) are encrypted with the Data Encryption Standard (DES) operating in electronic codebook mode (ECB) before being used to encrypt or decrypt information.

- The SC20-DES will perform a set of self tests when power is applied to the module. These self tests perform the following functions:
    - Program Memory Integrity Check (Software / Firmware Test)
    - Data Memory Functionality Check (Subclass of “Critical Functions Test”)
    - Key Integrity Check (Subclass of “Critical Functions Test”)

    - Cryptographic Algorithm Known Answer Test

- The SC20-DES stores the traffic encryption key (TEK) in encrypted form, and will decrypt it using the key encryption key (KEK) when necessary.

- The SC20-DES provides a zeroization function which will set the traffic encryption key (TEK) to zero, rendering the module inoperable in the secure mode until a new TEK has been loaded.

- Key Loading is performed in accordance with an applicable subset of the reaquirements od FIPS171, ANSI X9.17, ANSI X9.9, using the KL30-DES key loading software.

Security Relevant Data Items:

The SC20-DES has six security relevant data items. These are:

1. traffic encryption key (TEK)
2. key encryption key (KEK)
3. IV generation key (IGK)
4. initialization vector (IV)
5. working key encryption key (WKEK)
6. key randomizer (KR)

SRDI Modes of Access:

The SC20-DES makes use of the following security relevant data items in providing the following services:

Encrypt:
This operation uses the IV generation key (IGK) to generate an initialization vector (IV), using DES, and along with the traffice encryption key (TEK) encrypt the message information.

Decrypt:
This operation uses the traffic encryption key (TEK) to encrypt the initialization vector (IV), which is subsequently used to decrypt the message information.

Key Load:
This operation uses the key encryption key (KEK) to decrypt the new traffic encryption key (TEK) contained in the key service message (KSM). It also uses the newly aquired traffic encryption key (TEK) to verify the message authentication code (MAC) contained in the key service message (KSM).

Zeroize:
This operation sets the traffic encryption key (TEK) to zero, rendering the module inoperable in the secure mode until a new (TEK) has been loaded.

Roles & Services Matrix:

	encrypt	decrypt	show status	self test	key load	zeroize
User	x	x	x	x	*	*
Crypto Officer	x	x	x	x	x	x

* Requires possession of key loader. User does not possess key loader and and thus cannot perform zeroize or key load

SRDI & Services Matrix:

	encrypt	decrypt	show status	self test	key load	zeroize
TEK	x	x		x	x	x
KEK				x	x	x
IGK	x			x		x
IV	x	x				
WKEK					x	
KR					x	

SRDI & Roles & Services Matrix:

	User encrypt	User decrypt	User show status	User self test	Crypto Officer encrypt	Crypto Officer decrypt	Crypto Officer show status	Crypto Officer self test	Crypto Officer key load	Crypto Officer zeroize
TEK	x	x		x	x	x		x	x	x
KEK				x				x	x	x
IGK	x			x	x			x		x
IV	x	x			x	x				
WKEK									x	
KR									x	

Identification Requirements:

The SC20-DES does not have any identification requirements.

Authentication Basis:

The SC20-DES does not require operator authentication to access the module.