Security Policy
for
IBM S/390 CMOS Cryptographic Coprocessor

Version 1.1

December 15, 1998

Functional Area: S/390 System Architecture
Support Manager: Joe A. Wetzel
Department: E57A

Document Owner: Joe A. Wetzel
Author: Phil C. Yeh

Pyeh@us.ibm.com

Table of Contents

1. Scope of Document

This document describes the Security Policy for the IBM S/390 Cryptographic Module (SCM), also known as the IBM S/390 CMOS Cryptographic Coprocessor. SCM provides a wide range of security controls ranging from support for the highest level of security for the very sophisticated security-conscious customer to the simplest. The customer-initialization process can be used to establish the desired level of security control. This document is written from the standpoint of a high-level of security; it specifies the means for FIPS 140-1 compliance. The technical detail in this document is only to the level that is FIPS 140-1 relevant. The following paragraphs explain the level of detail of this document.

SCM supports a fine granularity of access authorization, including controls over individual security relevant data items (SRDIs) and detailed access modes within a service. This document describes access authorization only at the service level.

SCM provides a great flexibility with identity-based authentication to define a large number of roles. This document describes only two basic roles, a user role and a security-officer role.

SCM implements multiple domains with a separate set of master keys and controls in each domain. This document describes the SRDIs for one domain. SCM implements two master keys for protecting private keys, one to protect private keys for digital signature and the other to protect private keys for secret-key management. Using different master keys facilitates different key lengths allowed for these two applications, according to the U. S. export regulations. This document does not distinguish the two master keys for protecting private keys.

Services that are available only during module initialization are not included; non-security related services that do not have access to any SRDI are not all included. Services that have the same security effects are sometimes combined into a single, generic service.

SCM provides a large number of services for cryptographic operations, control functions, and initialization process. A summary of security related services is provided in the last section of this document. Note that not every service mentioned in this document is currently supported by the S/390 software and the terminology used in this document is not necessarily consistent with other IBM manuals or publications.

2. Applicable Documents

SCM supports the following FIPS standards:

FIPS PUB 46-2	Data Encryption Standard (DES)
FIPS PUB 180-1	Secure Hash Standard (SHA-1)
FIPS PUB 186	Digital Signature Standard (DSS)

SCM supports the following ANSI standards:

ANSI X3.92	Data Encryption Algorithm (DEA)

ANSI X3.106 Modes of DEA Operation -- Only the electronic-code-book and cipher-block-chaining modes are supported.
ANSI X9.9 Financial Institution Message Authentication -- Wholesale
ANSI X9.19 Financial Institution Message Authentication -- Retail

SCM supports the following algorithms:

Commercial Data Masking (CDM) Algorithm -- A 40-bit DES-based encryption algorithm
RSA Algorithm -- up to 1024 bits
Diffie-Hellman (DH) Key-Agreement Algorithm -- up to 1024 bits
Modification Detection Codes 2 and 4 (MDC-2 and MDC-4) -- DES-based hashing Algorithms

ANSI X9.52 (Draft) Triple Data Encryption Algorithm, Modes of Operation -- Only the electronic-code-book and cipher-block-chaining modes are supported.

SCM also implements all cryptographic services, PIN (personal identification number) algorithms, and PIN-block formats defined in the IBM Common Cryptographic Architecture (CCA), SC40-1675

3. Overview of S/390 Cryptographic Module

SCM is a single-chip cryptographic module; it supports both symmetric and public-key algorithms (PKA). The module is designed for IBM S/390 Enterprise Server computers. In most enterprises, these computers are interconnected by hundreds of links and are used to perform a large number of concurrent applications. And, the number of cryptographic keys that must be available and protected can be extremely large; it is impractical to store cryptographic keys for all applications in the module.

SCM implements three master keys within the module to protect other cryptographic keys. The data-protection master key (DMK) protects secret keys for symmetric algorithms, the signature-object master key (SMK) protects private keys for digital signature, and the receive-object master key (RMK) protects private keys for secret-key management. In this document, SMK and RMK are generally referred to as the PKA master key (PMK). Each encrypted private key and its associated public parameters are further encapsulated in a PKA object to protect against modification. Encrypted secret keys and encapsulated PKA objects are maintained outside SCM. When a service is requested, the associated keys or objects are provided to SCM as input operands of the service. SCM recovers the clear value of the secret or private key within the module and uses it for the designated operation. Before an object is accepted, integrity of the object is verified by SCM. If verification is unsuccessful, the object is rejected and the requested service is denied.

SCM recognizes two roles: a user role and a security-officer role. At any point in time, SCM supports one user operator in the user role and multiple operators in the security-officer role. Identity-based authentication using public-key technology is performed for each operator. Sixteen operator-identity registers are provided in SCM and each register holds the identity (RSA public key) of a legitimate operator. SCM uses the designated operator-identity register to authenticate and verify a service request signed by the RSA private key of an operator. Public-key technology is also used by SCM to ensure integrity of messages sent by the module. A unique 1024-bit RSA key pair is burnt inside every SCM. The module private key is used to sign messages sent by SCM so that anyone can authenticate the messages using the module public key. To protect against replay, a time-varying parameter is included in messages sent from or sent to SCM. SCM supports the Diffie-Hellman key-agreement protocol to establish secret keys shared between SCM and an external device. This approach allows security officers to initialize a SCM or perform normal control functions using a workstation at a remote site. The workstation can be connected to the Enterprise Server through a public, insecure network.

When a SCM is shipped with the Enterprise Server to the customer, all security-related cryptographic services are disabled. Two initialization processes must be performed before any user service is enabled; they are module initialization and customer initialization. An enablement diskette, that is unique to each SCM, is required for module initialization. The enablement diskette specifies the services and maximum key lengths that the customer is entitled to, according to the U. S. export regulations.

After the module initialization, SCM is in a reset state and is ready for customer initialization. Customer security officers can then install public authentication data, such as operator identity and access authorization, into SCM to establish the intended controls. Note that anyone could take control of the module before legitimate authentication data is installed. This is not a security exposure because the module does not yet contain any customer secret information. At each step of the customer-initialization process, public audit can be performed by anyone to ensure integrity of the module state. Customer secret parameters are installed into the module only after controls have been properly established. Customer master keys are installed into SCM using split knowledge, that is, each master key is split into multiple key parts and each key part is installed separately. Additionally, each key part is encrypted when transmitted to SCM and installation of each key part is subject to multiple control. After the master keys have been installed, appropriate user services are then enabled for applications. The same mechanism used to install master keys can be used to install all other secret keys.

SCM provides a set of user services for online secret-key generation, and secret-key distribution using DES, RSA or DH. It supports user services for data confidentiality, message-authentication-code (MAC) processing, and PIN processing. For data confidentiality, SCM supports CDM, DES, and Triple-DES (TDES) cipher algorithms. For MAC processing, single-key, double-key, and triple-key MAC are supported. PIN generation and verification services are provided for commonly used PIN algorithms and PIN-block formats. SCM also provides user services for hashing functions, including SHA-1, and RSA and DSS digital signature. SCM can generate DSS and DH key pairs, but does not generate RSA key pairs. User services are available to convert RSA, DSS, or DH private keys from the clear or encrypted form into an encapsulated object.

4. Security Level

SCM is designed to comply with the overall requirements applicable to Level 4 security of FIPS 140-1.

Security Requirement Section	Level
Cryptographic Module	4
Module Interfaces	4
Roles and Services	4
Finite State Machine	4
Physical Security	4
EFT	4
Software Security	N/A
Operating System Security	N/A
Key Management	4
Cryptographic Algorithm	4
EMI/EMC	4
Self-test	4

5. Roles and Services

SCM supports the following two distinct roles and enforces the separation of operators using identity-based authentication:

1. Security officer role

2. User role

All SCM services are classified into four kinds: non-controlled, profile-controlled, single-signature, and multiple-signature. Non-controlled services can be performed without requiring any authentication; they are not security-related services. All profile-controlled services are user services. Availability of these services is controlled by the contents of the user-profile register in SCM. Single-signature services are available to all operators, regardless of the role. Performance of a single-signature service requires only identity of the requesting operator to be authenticated. Performance of a multiple-signature service may require multiple signatures; it requires identity of the requesting operator to be authenticated, access authorization of the requesting operator to be verified, and the specified number of signatures to be provided by authorized operators. All multiple-signature services, except for the set-user-profile user service, are security-officer services.

The set-user-profile user service, when co-signed, allows the authorized user operator to enable or disable all other user services. Each bit in the user-profile register controls availability of a group of these user services.

5.1 Security Officer Role

This role is equivalent to the crypto officer role defined in FIPS 140-1. The security officer initializes the cryptographic module, and performs control services to establish operator identity, specify access authorization, and install master keys. The role may also perform a set of cryptographic key or object management services, including transfer master keys from one SCM to another and convert encrypted private key into object or vice versa.

A number of security-officer services are defined for the role; they are multiple-signature services and are summarized in Section 9. Every operator in the role also has access to all single-signature services. However, equal access to security-officer services is not necessarily assigned to all operators. Access authorization for security-officer services is specified in the signature-requirement array (SRA) for each operator.

5.2 User Role

This role is equivalent to the user role defined in FIPS 140-1. The user performs the set-user-profile user service. This service enables the profile-controlled services, including various cryptographic services for data confidentiality, MAC processing, PIN processing, secret-key management, and digital signature. A summary of user services is provided in Section 9. In addition to the user services, the user can also perform all single-signature services. The user operator cannot perform any security-officer service unless the operator also assumes the security-officer role.

6. Security Rules

The security rules for SCM are described below. Explanatory statements are indicated by an *italic* type.

1. SCM supports the FIPS PUB 46-2 Data Encryption Standard (DES).

2. SCM supports the FIPS PUB 180-1 Secure Hash Standard (SHA-1).

3. SCM supports the FIPS PUB 186 Digital Signature Standard (DSS).

4. SCM supports a maximum of 16 operators. The role an operator assumes is determined implicitly by the requested service.

5. SCM enforces the separation of operators using identity-based authentication. For single-signature and multiple-signature services, authentication of operator identity is performed by verifying the RSA digital signature contained in the service request. Verification of the

signature uses the public key, representing the requesting operator, in the designated operator-identity register. If authentication of operator identity fails, the requested service is not performed.

6. For multiple-signature services, verification of access authorization is performed as specified in the signature-requirement array. If the operator is not authorized to assume the role or to request the service, or the required number of signatures has not been fulfilled, the requested service is not performed.

   Since all security-officer services are multiple-signature services, authentication of operator identity and verification of access authorization is performed for every security-officer service.

7. Authentication of operator identity and verification of access authorization for the user operator is performed when the operator requests the set-user-profile user service, which is a multiple-signature service.

   Profile-controlled user services, when enabled, can be performed by the user operator without requiring any further authentication or verification. If the requested service is disabled by user profile, the service is not performed.

8. Single-signature services are authorized to all operators, regardless of the role the operator assumes. Performance of single-signature services requires authentication of the operator identity but does not require verification of role and access authorization.

9. Access authorization in the signature-requirement array can be established to require a different number of signatures from a different set of operators for each multiple-signature service.

10. The identity of each operator can be loaded into or removed from an operator-identity register in SCM by authorized operators with multiple control (*i.e., command co-signed by one or more operators*).

11. Each group of profile-controlled user services can be enabled or disabled by authorized operators with multiple control.

12. Secret keys can be loaded into SCM using split knowledge in the encrypted form by authorized operators with multiple control.

13. Master keys in one SCM can be transferred to another SCM by authorized operators with multiple control.

14. SCM supports public audit by providing status information through non-controlled services. Status information is digitally signed by the burnt-in RSA secret key to protect against modification or substitution, and includes a time-varying parameter provided by the requester to protect against replay.

15. User DSS, RSA, or DH objects can be converted from being protected under the PKA master key of a SCM to being protected under a transport key shared with another SCM by authorized operators with multiple control.

    This ability allows the objects to be securely imported from or exported to another computer systems.

16. Intermediate values generated when performing a service never leave the secure boundary of SCM. Only the output parameters specified for the service leave the secure boundary.

17. If primary power to SCM is removed, with the module connected to a back-up battery power, the module will cease to function. When primary power is reapplied the module will return to the state it was in prior to removal of the primary power.

18. If both primary and back-up battery power is removed, all SRDIs, except the burnt-in parameters, are zeroized and SCM must be reinitialized by module initialization when the power is restored.

19. Upon application of primary power, the module Error Detection/Fault Isolation (ED/FI) circuits are activated. Upon detection of an error, the module enters a failure state, in which all input and output interfaces are disabled, except for an error-recovery reset. If the error was a recoverable error, the error-recovery reset causes the module to return to its original state before the error was detected. Otherwise the module remains in the failure state and all SRDIs are erased, except the burnt-in parameters.

20. The module reset erases or reinitialized all SRDIs, except the burnt-in parameters, in the module.

21. The module reset is performed as part of power-on reset after both primary and back-up battery power is off, the module-initialization process, or a manual reset.

22. SCM is designed to comply with the Environmental Failure Test (EFT) requirements of FIPS 140-1.

23. SCM is designed to comply with the requirements of FCC Part 15, Subpart J, Class B.

7. FIPS 140-1 Compliance

The following provides a guideline for FIPS 140-1 compliance:

- FIPS approved algorithms shall be used.

- Identity of legitimate operators shall be loaded into operator-identity registers and access authorization shall be appropriately established in the signature-requirement array.

- Cryptographic keys shall be generated by outside systems; key generation functions provided by this module shall not be used.

- Cryptographic keys shall be installed in the encrypted form using public key technology.

- Only services that use keys provided to the module in encrypted form shall be used.

8. Security Relevant Data items (SRDIs)

Security relevant data items for SCM are defined as follows:

Crypto Configuration Control (CCC) The control specifies maximum lengths of key and availability of certain functions to comply with the U. S. export regulations. The control is set during the module-initialization process.

Crypto Module Public Modulus (CMPM) The unique 1024-bit RSA public modulus for this SCM. This modulus is set during the module-initialization process.

Crypto Module Public Exponent (CMPE) The fixed value of 65537 for all SCMs and is burnt-in at time of manufacture.

Crypto Module Secret Exponent (CMSE) The unique 1024-bit RSA secret exponent for this SCM and is burnt-in at time of manufacture.

Pending Command Register (PCR) It holds the multiple-signature service that is pending for all necessary signatures.

Signature Requirement Array (SRA) It specifies the signature requirements for each of the multiple-signature services, including access authorization for each operator, the number of signatures required, and which operators are allowed to provide the signature.

Operator-Identity Registers (OIRs) There are 16 operator-identity registers. Each register holds a 1024-bit RSA public modulus for an operator identity and a 128-bit transaction sequence number (TSN). The value of 65537 is used as public exponent for all operators.

TSN is a counter that is incremented each time a service signed by the associated operator is accepted. TSN is used to eliminate the possibility of replaying any previously signed service.

User-Profile Register (UPR) It specifies availability of all profile-controlled user services. Each bit in UPR controls availability of a group of these services (see Table 1).

Data Protection Master Key (DMK) A 128-bit secret key used to protect secret keys for symmetric algorithms.

Auxiliary Master Key (AMK) A 128-bit secret key used to facilitate dynamic change of DMK.

Signature Object Master Key (SMK) A 192-bit secret key used to protect private keys for digital signature.

Receive Object Master Key (RMK) A 192-bit secret key used to protect private keys for secret-key management.

Key Part Queue (KPQ) It contains several entries; each entry is 128 bits to hold a key part for key installation. The first entry is also called the key-part register (KPR).

Diffie-Hellman (DH) Registers These are used to derive a transport key using the DH key-agreement protocol and consist of the following four components:

DH Generator (DHg) The 1024-bit DH generator.

DH Modulus (DHm) The 1024-bit DH modulus.

DH Secret Exponent (DHx) The 1024-bit DH secret exponent.

DH First Key Part (DHf) $g^{x} \bmod m$, where g, x, and m are DHg, DHx, and DHm, respectively.

Transport Key (TK) A secret key derived from the DH key-agreement protocol. TK is 128-bit when used for protecting DMK or secret key; it is 384-bit for protecting PMK or private key.

Encrypted Extracted Key (EXK) The extracted AMK, DMK or PMK, or converted private key encrypted under TK.

9. Roles vs Services vs SRDIs vs Modes of Access

The relationships between roles, services, SRDIs and access modes are summarized in this section. The following symbols are used in Tables 1 – 3.

Symbols for keys:

MK	AMK, DMK, RMK, or SMK
KEK	Key-encrypting key
KPR	Key-part register
PMK	SMK or RMK
XMK	AMK or DMK
All MKs	AMK, DMK, RMK, and SMK

Access Modes:

C	To encrypt a supplied clear value for output
D	To decrypt an input operand for internal use
E	To encrypt a secret parameter for output
H	The hash value for the SRDI is output, or is compared with an input operand for equality.
K	To compare if it matches a specific value or an input operand
R	To be read out in an encrypted form
S	To sign the conclusion of service performance
U	The value is used or updated according to the prescribed operation.
V	The public key in the designated operator-identity register is used to verify the RSA digital signature signed over the requested service
W	The value is updated with a supplied clear value
Z	Zeroize

Profile-Controlled Service Group (PCSG): Each lower case alphabet in this column represents a separate user-service group. The following summarizes group symbols and names:

a	Basic symmetric-algorithm services
b	Clear PIN or clear key handling
c	DES or TDES cipher
d	CDM cipher
e	Generation of hash value for key
f	Reset XMK
g	Clear XMK entry
h	Reset PMK or clear PMK entry
i	Generation of hash value for PMK
j	Reset domain
k	Basic public-key-algorithm services
l	Conversion of encrypted private key to object
m	Set DMK

Signature: This column specifies the signature requirement using the following symbols:

SS Single signature
MS Multiple signature

Role: This column specifies the role who can have access to the service. The following summarizes symbols used in this column.

SO Security officer
ALL All identified operators

9.1 Non-Controlled Services

Performance of any non-controlled service does not require any authentication or verification. Except for initialize-crypto-module and query-crypto-information, non-controlled services listed below do not have access to any SRDI. Performance of the initialize-crypto-module service zeroizes all SRDIs, except the burnt-in ones. Performance of query-crypto-information reads out all public SRDIs and hash value for each secret SRDI. The conclusion of performing the initialize-crypto-module or query-crypto-information service is provided in a reply message, which is signed by using the module secret key (CMPM and CMSE).

1. Generate MDC
2. Generate SHA-1
3. Generate pseudo-random number
4. Verify DSS digital signature
5. Verify RSA digital signature
6. Query crypto information
7. Initialize crypto module

9.2 Profile-Controlled Services

All profile-controlled services are user services. A profile-controlled service can be performed only if it is enabled. If a profile-controlled service is assigned to multiple groups, the service is enabled when all groups the service is in are enabled.

Table 1: Summary of profile-controlled Services

Service	SRDI	Access Mode	PCSG
CDM encipher	DMK	D	a, d
CDM decipher	DMK	D	a, d
DES encipher	DMK	D	a, c
DES decipher	DMK	D	a, c
TDES encipher	DMK	D	a, c

TDES decipher	DMK	D	a, c
Reencipher Data	DMK	D	a, c
Generate MAC	DMK	D	a
Verify MAC	DMK	D, E	a
Generate TDES MAC	DMK	D	a
Verify TDES MAC	DMK	D, E	a
Generate PIN	DMK	D	a, b
Verify PIN	DMK	D	a
Reencipher PIN	DMK	D	a
Encipher under DMK	DMK	C	a
Encipher under KEK	DMK	D	a, b
Reencipher key between KEK and DMK	DMK	D, E	a
Reencipher key from DMK to AMK	DMK AMK	D E	a
Reencipher key from AMK to DMK	AMK DMK	D E	a
Generate DES key pair	DMK	D	a
Transform CDM key to DES key	DMK	D, E	a, d
Generate hash value from key	DMK	D	e
Test key parity	DMK	D	a
Adjust key parity	DMK	D, E	a
Reset XMK	XMK	Z	a, f
Reset KPR	KPR	Z	a
Read or combine key part from KPR	DMK KPR	D, E R, Z	a
Load or combine key part into AMK	KPR, AMK	U	a
Set DMK	AMK, DMK	U	m
Load or combine clear key part into XMK	XMK	W	a, g
Reset PMK	PMK	Z	h
Load or combine clear key part into PMK	PMK	W	h
Generate hash value from XMK	XMK	H	a
Generate hash value from KPR	KPR	H	a
Generate hash value from PMK	PMK	H	i
Reset domain	All MKs, KPR	Z	a, j
Generate DSS digital signature	PMK	D	k
Generate RSA digital signature	PMK	D	k
Create DH or DSS object	PMK	E	k
Extract DSS public key	PMK	D	k
Convert clear RSA, DSS, or DH private key into object	PMK	E	k
Convert encrypted RSA, DSS, or DH private key into object	DMK PMK	D E	l
Receive DES key under RSA or DH	PMK	D	k

9.3 Signed Services

Signed services, either single-signature or multiple-signature services, are listed in Table 3. SRDIs that are accessed by all signed services are summarized in Table 2. Information in Table 2 is not repeated in Table 3.

Table 2: SRDIs accessed by signed services

SRDI	Access Mode
OIR	V
CMID	K
TSN	K, U
PCR	U
SRA*	K
CMPM, CMSE	S

Explanation: * means only multiple-signature services have access to it.

Table 3: Summary of signed services (Table 2 contains additional SRDIs)

Service	SRDI	Access Mode	Signature	Role
Load user profile	UPR	W	MS	User
Load signature requirement array	SRA	W	MS	SO
Load operator identity	OIR	W	MS	SO
Load key part into KPQ	TK KPQ	H, D U	MS	SO
Load or combine MK key part	TK MK	H, D U	MS	SO
Load or combine clear XMK key part	XMK	W	MS	SO
Load clear key part into KPQ	KPQ	W	MS	SO
Reencipher object from PMK to TK	PMK TK EXK	D H, E U	MS	SO
Reencipher object from TK to PMK	TK PMK EXK	H, D E U	MS	SO
Extract and encrypt MK	TK MK EXK	H, E R U	MS	SO
Zeroize domain	All MKs, UPR, KPQ	Z	MS	SO

Co-sign	PCR	K, U	SS	All
Load DH modulus	DHm DHg, DHf, DHx, TK, EXK	W Z	SS	All
Load G and generate DH first part	DHg DHx, DHf, DHm TK, EXK	W U Z	SS	All
Derive transport keys using DH	DHm, DHx, TK EXK	U Z	SS	All

10. End of Document