TrustField
Crypto Key Server

CRYPTOGRAPHIC MODULE SECURITY POLICY

Your Total Business Solution

TrustField Crypto Key Server (CKS) Cryptographic Module Security Policy
Version 2.0, 22 Dec, 2001

Document History

Status	Version	Date	By	Remarks
Draft	1.1	Feb 14, 2000	Hon Luen	Creation
Draft	1.2	June 07, 2000	John Koh	Revision
Draft	1.3	June 28, 2000	John Koh	Revision
Draft	1.4	July 19, 2000	John Koh	Revision
Draft	1.5	Feb 10, 2001	Arthur Loo	Revision
Draft	1.6	Apr 2, 2001	Arthur Loo	Updated for FIPS
Draft	1.7	Apr 17, 2001	Arthur Loo	Amendment
Release	1.8	May 25, 2001	Arthur Loo	Final for FIPS
Revision	1.9	Nov 2, 2001	Arthur Loo	Amendment
Revision	2.0	Dec 22, 2001	PrivyLink	Release for FIPS

Comments and suggestions should be directed to:

SINGAPORE

PrivyLink Pte Ltd
77 Science Park Drive
#02-05/07 CINTECH III
Singapore Science Park 1
Singapore 118256
Tel: (65) 882 0700 Fax: (65) 872 5490
URL: http://www.privylink.com
Sales support: sales @privylink.com.sg

Abbreviations used in this document

This section contains the list of abbreviations used in this document.

Auth	- Authenticate or Authenticated
DES	- Data Encryption Standard
ID	- Identity Number
IP	- Internet Protocol Address
I/O	- Input / Output
PIN	- Personal Identification Number
KSA	- CKS Administrator Program
RAM	- Random Access Memory
RSA	- Rivest-Shamir Adleman
SRDI	- Security relevant data items
TMK	- Terminal Master Key
UTP	- Unshielded twisted pair
wKEY	- Working Key
3DES	- Triple Data Encryption Standard
SID	- Session ID
CKS	- Cryptographic Key Server
APC UPS	- American Power Conversion Corp Uninterruptible Power Supplies (UPS)

Objective

This document seeks to address the security policy requirements of FIPS 140-1 as well as the validation requirements imposed by the Derived Test Requirements (DTR). This document completely specifies the CKS security policy, that is, the security rules that the CKS operates on. The security policy includes the security rules derived from the security requirements of this standard and the security rules derived from any additional security requirements by the manufacturer.

The main objectives for this security policy are:

1. To allow the developers of the CKS to assign correct access rights only to the authorized persons, to design a secure way for different system elements to be accessed, and to ensure the protection of various system elements.

2. To provide a precise specification for the cryptographic security. The adherence of the cryptographic security substantiates the implementation that conforms to a stated security policy.

3. To describe the access rights that the CKS Cryptographic Officers will have when in use.

Security Level

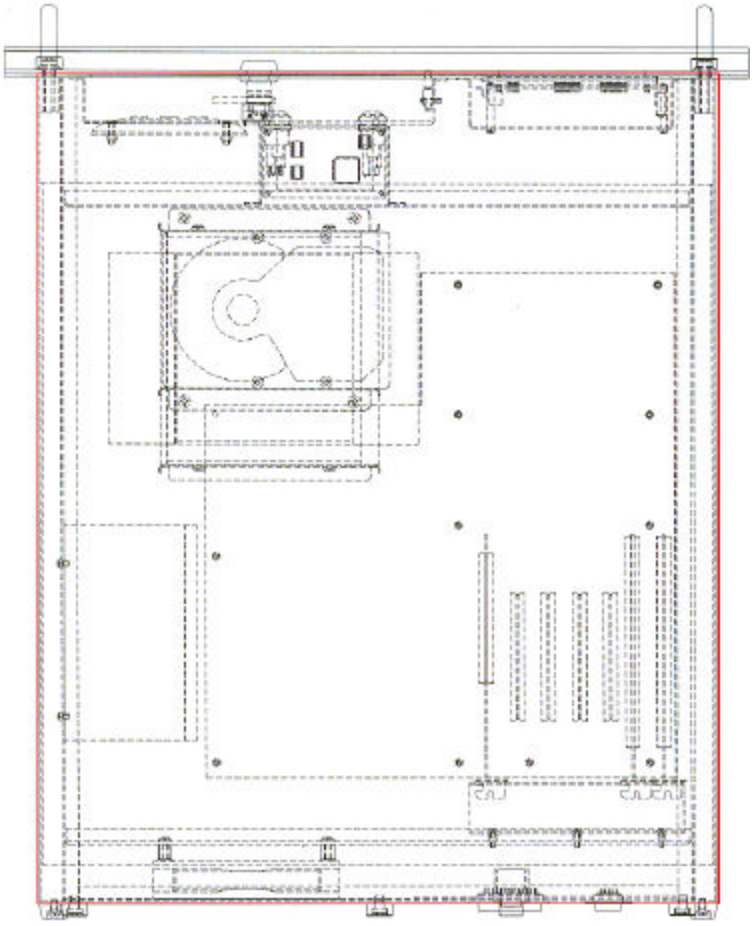
The CKS shall meet the overall requirements applicable to Level 3 security of FIPS 140-1. The following table shows the security requirements applicable for each section:

Security Requirements Section	Level
Cryptographic Module	3
Module Interfaces	3
Roles and Services	3
Finite State Machine	3
Physical Security	3
Software Security	3
Operating System Security	N/A
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Test	4

Cryptographic Boundary and Physical Interfaces of CKS

The CKS is an integrated software - and hardware -based cryptographic system designed to comply with FIPS-140-1 Level 3 for a multi-chip standalone cryptographic module. The cryptographic boundary is defined to be the entire system area of the CKS.

The following diagram depicts the CKS casing border as the cryptographic boundary.



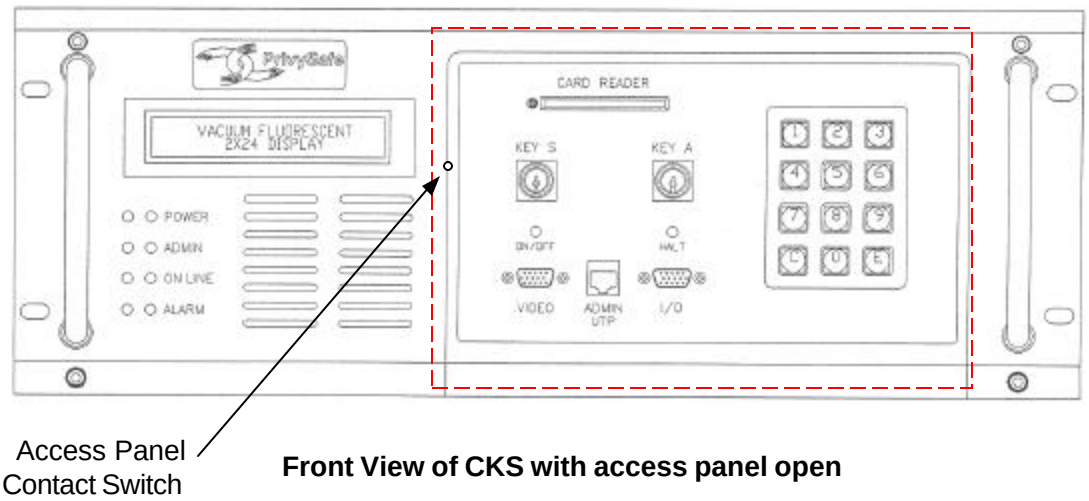
Interfaces into the Cryptographic Boundary

The following sections describe the various interfaces of CKS.

The CKS has a total of 17 physical interfaces used for data input, data output, control input, status output and power input. This section examines these physical interfaces and describes the use of the interfaces.

Interfaces on the Front Panel

These interfaces are normally used for administrative purposes.



Front View of CKS with access panel open

Access Panel (Front)

As depicted by the dashed line shown in the figure above, these interfaces are located at the front of the CKS behind the Front Access Panel. The Front Access Panel key is used to open the panel for access.

Data Input Only

1. 12-key Numeric Key Pad — This Key Pad is used to do numeric data entry, such as authentication data.

2. I/O Port (Keyboard/Mouse) — This is a specialized 9-pin adaptor that is used to interface with the keyboard and mouse. (This is disabled.)

Data Output Only

3. Video Adaptor Port — This is the standard VGA adaptor that is used to interface with the standard VGA monitor. (This is disabled.)

Both Data Input/Output

4. Smart Card Reader — This reader is used to interface with Smart Cards for Master Key-related functionality (please refer to the Service Description section).

5. Admin UTP Port — This is a protected channel used by the CKS Superusers and Operators to send their commands.

Control Input

6.	Precision Turn Key Locks (Key A and Key S)	These locks are incorporated as part of the "Authentication" mechanism for the module (please refer to Roles section).
7.	ON/OFF Button	This is the ATX Power Supply Switch that controls the power supply to the system.
8.	HALT Button	This switch is used to trigger a recommended shutdown sequence of the system.
9.	Access Panel Contact Switch	This contact switch is used to detect the "open/close" state of the Access Panel.

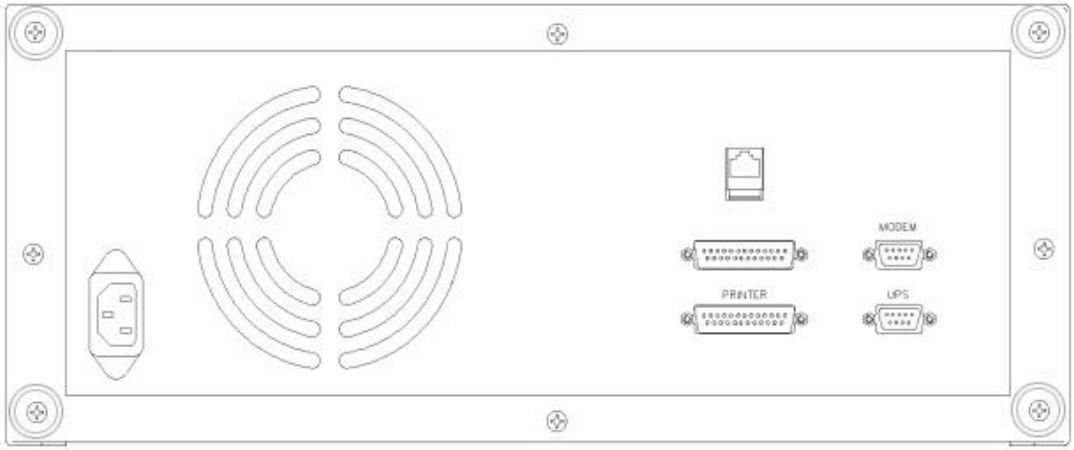
Exposed Interfaces (Front)

Status Output

10.	Eight Status LEDs	Two columns of Status LEDs to reflect the system status.
11.	LCD Panel	24-character by 2-line vacuum fluorescent display to reflect the system status and prompt for menu selection.

Interfaces on the Rear Panel

These interfaces are for the operation of the CKS.



Rear View of CKS

Exposed Interfaces (Rear)

There are six interfaces on the back panel.

Data Output Only

12. DB-9 Serial Port	This is disabled.
13. DB-25 Parallel Port	This port is dedicated to the output of Authentication Data, such as User ID and PIN information.

Both Data Input/Output

14. Operation UTP Port	This port is used to receive services listed in the Start Operation Service description (please refer to the Service Description section).
15. DB-25 SNA interface (RS 232)	This is disabled.

Control Input

Not Applicable.

Status Output

16. UPS Port	This port is used for communication with industry-standard APC UPS devices.

Power Input

17. Power socket	This is used to connect the power supply (factory selectable for 115V or 240V).

Roles

The CKS supports and uses ID-based forms of authentication.

At the basic level, the CKS deploys the traditional method of "keys and locks" to restrict the physical and operation mode access. The three keys are labelled as follows.

- Access Panel Key
- Key_S
- Key_A

Thereafter, the User ID and Access PIN are used to enforce ID-based Authentication.

Root Administrator

The Root Administrator is defined as the Crypto-Officer, as per FIPS 140-1. The Root Administrator manages the system Master key and the superusers for the system.

Authentication: The assigned Access PIN and ownership of all three precision keys that the Root Administrator must possess is used to authenticate the Root Administrator. The Access PIN and physical keys ensure the stringent authentication of the Root Administrator.

Services: Please refer to Services Description section.

Superuser

The Superuser is defined as a User, as per FIPS 140-1. The CKS' Crypto Superusers are those who perform key management and configuration services for the system via the Admin UTP Port.

Authentication: The assigned ID, Access PIN and the Access Panel Key are used to authenticate the Superuser. In addition, Key S is required to perform crypto key generation and system configuration services.

Services: Please refer to Services Description section.

Operator

The CKS' Crypto Operator is defined as the person who retrieves system information and can perform restricted key management services via the Admin UTP Port.

Authentication: The assigned ID, PIN and Access Panel Key are used to authenticate the Operator.

Services: Please refer to Services Description section.

Summary of Services

The table below shows the access control to the services and commands for each Role.

Services	Root Administrator	Superuser	Operator
Master Key Generate	YES	NO	NO
Master Key Duplication	YES	NO	NO
Change Master Key PIN	YES	NO	NO
Change own PIN	YES	NO	NO
Create Superuser	YES	NO	NO
Delete Superuser	YES	NO	NO
Load Master Key	YES	NO	NO
Key Generate	NO	YES	NO
Key Loading	NO	YES	YES
Key Generate RSA	NO	YES	NO
Key Unloading	NO	YES	YES
Configure Printer Port	NO	YES	NO
System Check	NO	YES	YES
Retrieve Event Log	NO	YES	YES
Retrieve System Log	NO	YES	YES
Start Operation *	NO	YES	YES
Stop Operation	NO	YES	YES
Shutdown	NO	YES	YES
Load Operation Policy	NO	YES	NO
Clear Operation Policy	NO	YES	NO
Install Operation Policy	NO	YES	NO
Retrieve Operation Policy	NO	YES	YES
Retrieve Available Operations	NO	YES	YES
Create Operator	NO	YES	NO
Delete Operator	NO	YES	NO
User Change Pin	NO	YES	YES
User Log out	NO	YES	YES
User Auth	NO	YES	YES

* See description for start operation.

Services Descriptions

1. System Administration Group

Function Name: Master Key Generate

Description: This function is used to generate 128-bit System Master Keys and store them in the Security Core. The Master key is also written into the two smart cards in split-knowledge form.

Function Name: Master Key Duplication

Description: This function is used to duplicate another set of smart cards.

Function Name: Change Master Key PIN

Description: This function is used to change the System Master Key Smart Card Access PIN.

Function Name: Change Root Administrator PIN

Description: This function is used to change the Root Administrator Access PIN.

Function Name: Create Superuser

Description: This function is used to create a new Superuser for the system.

Function Name: Delete Superuser

Description: This function is used to delete an existing Superuser from the system.

Function Name: Load Master Key

Description: The Master Key must be loaded at startup to perform any crypto operation or function.

2. Key Management Group

Function Name: Key Generate

Description: This function is used to generate new keys for DES or TDES cryptographic functions. Only a 64-bit key length is supported for use with DES, and both 64-bit and 128-bit key lengths are supported for use with 3DES cryptographic functions. On the CKS, the new key is loaded into the Key Index number specified during Key Generation.

Function Name: Key Loading

Description: This function is used to load all encrypted keys into the CKS. Note that only CKS-generated keys can be loaded into the system.

Function Name: Key Generate RSA

Description: This function is used to generate 1024-bit RSA keys that are used for RSA cryptographic operations. In the CKS, the private key is loaded into the Key Index number specified.

Function Name: Key Unloading

Description: This function is used to unload or destroy the keys that are loaded into CKS. The key at the position specified will be overwritten with '0's for the length of the key. The master key cannot be unloaded using this method.

3. System Management Group

Function Name: Configure Printer Port

Description: This function is used to enable or disable the DB25 parallel port. The setting set by this command will determine whether the printer can be used by the CKS. Please note that the configured settings are retained even after a system shutdown. The default setting for the printer port setting is set to "enabled."

Function Name: System Check

Description: This function is used to perform a system check on the CKS. It includes a self-test check on the CKS as well as general information on the current sensor readings. This command is used by the Superuser to initiate system self-tests. Upon request, the CKS shall perform the following tests:

- Random Number Generator Statistical Test
- DES Encryption Algorithm Known Answer Test
- 3DES Encryption Algorithm Known Answer Test
- CKS file Integrity test (which covers SHA-1 Algorithm Test)

4. Log Management Group

Function Name: Retrieve Event Log

Description: This function is used to retrieve the event logs on CKS. The retrieved data are then written into a file via the CKS Administrator Program.

Please note that all Administrative Commands are logged into this event log. The logs are logged in a round-robin fashion within the security core with up to a maximum of 500 log entries at any one time.

Function Name: Retrieve System Log

Description: This function is used to retrieve the system logs on CKS. The retrieved data are then written into a file via the CKS Administrator Program.

Please note that all system events are logged into the system log. The logs are logged in a round-robin fashion within the security core with up to a maximum of 500 log entries at any one time.

5. Operation Management Group

Function Name: Start Operation

Description: This function is used to control the following cryptographic services depending on the policy configuration.

Function Name: des_encrypt

Description: This function is used to provide DES encryption.

Function Name: des_decrypt

Description: This function is used to provide DES decryption.

Function Name: tdes_encrypt

Description: This function is used to provide 3DES encryption.

Function Name: tdes_decrypt

Description: This function is used to provide 3DES decryption.

Function Name: rsa_encrypt

Description: This function is used to generate an RSA cryptogram used to protect keys for distribution.

Function Name: rsa_decrypt

Description: This function is used to decrypt an RSA cryptogram used to protect keys for distribution.

Function Name: ewkey_generate

Description: This function is used to generate an encrypted working key.

Function Name: hash_sha

Description: This function is used to hash a message using SHA-1.

Function Name: mac_x919_generate

Description: This function is used to generate a DESMAC conforming to X.9.19 standard. The resulted MAC is 32 bits.

Function Name: mac_x919_verify

Description: This function is used to verify a DESMAC generated using X.9.19 standard.

Function Name: mac_fips113_generate

Description: This function is used to generate a DESMAC conforming to the FIPS-113 standard. The resulted MAC is selectable between 16 to 64 bits

Function Name: mac_fips113_verify

Description: This function is used to verify a DESMAC generated using the FIPS-113 standard.

Function Name: Stop Operation

Description: This function is used to stop the cryptographic services that have been previously started.

Function Name: Shutdown

Description: This function is used to perform a graceful shutdown for CKS.
For this function to be successful, the cryptographic services must be have stopped in advance. Before the CKS is shut down, all key information in the volatile memory is zeroized. After the zeroization is complete, the CKS will be shut down. To restart the CKS, the “start” button on the front panel must be pressed.

6. Services Configuration Management Group

Function Name: Load Operation Policy

Description: This function is used to perform the loading of the selected cryptographic services from the Operation Management Group. The cryptographic services that have been loaded will not be available until the functions have been installed.

Function Name: Clear Operation Policy

Description: This function is used to clear the selected cryptographic services that have been loaded. All loaded cryptographic functions are cleared from the CKS.

Function Name: Install Operation Policy

Description: This function is used to install the cryptographic functions that have been loaded. This function provides a mean to control the list of cryptographic functions to be made available for the start operation.

For the function to be successful, the CKS must not be in the operations started state. Upon success of this function, the list of loaded cryptographic functions will be available when the start command is invoked.

The install command would overwrite the existing cryptographic functions that were previously installed with the new set of loaded cryptographic functions. If the CKS is shut down with the installed cryptographic functions or services, these services will be recovered when the CKS starts up again.

Function Name: Retrieve Operation Policy

Description: This function is used to retrieve the cryptographic functions that have been previously installed.

Function Name: Retrieve Available Operations

Description: This function is used to retrieve all cryptographic functions that can be loaded and installed.

7. Operators Management Group

Function Name: Create Operator

Description: This function is used to create a new Operator ID. The new Access PIN will be output to the DB-25 parallel path upon the successful creation of an operator.

Function Name: Delete Operator

Description: This function is used to delete an existing Operator ID.

Function Name: User Change Pin

Description: This function allows the current Superuser or Operator who owns the session to change their PIN.

8. Session Management Group

Function Name: User Log out

Description: This function is used to terminate an existing session. The current session ID is thus removed from the CKS.

Function Name: User Auth

Description: This function is used to request a session ID. The Superuser ID and PIN or Operator ID and PIN are processed, and the results are sent to the CKS for validation.

Security Rules

This section documents the security rules enforced by the CKS to implement the security requirements of this FIPS 140-1 Level 3 module.

1. Special Keys Zeroization Service
   Key A is used as a means to zeroize and erase all sensitive data (including Master Key) from the system. This can be achieved by turning Key A during the bootup.

2. The module does not permit multi-concurrent Administration Services for Superusers or Operators.

3. All keys are output in encrypted form or split-knowledge form.

4. The CKS uses ID-Based Authentication.

5. No Raw PINs are stored in the CKS. Instead, only Cryptographic Officer IDs and their respective Cryptographic Officer user salts will be stored on each CKS.

6. Under the ID-based mode, any user will be given an administrative session ID from the CKS when the user has performed a successful login. This session has a total session-alive time of five (5) minutes. After the five-minute-timeout period, the user will be required to re-authenticate himself.

7. At any point in time, if the CKS receives an invalid session ID, the command accompanying the invalid session ID will be disregarded.

8. At any point in time, if the CKS receives a command at the administrative port but the access panel is still detected as being closed, the command will be disregarded. This is a preventive measure against any attempt to bypass the access panel by cutting a hole in the panel.

9. All sensitive data files stored in the CKS must have a hash of it being stored in the security core. At startup, a hash comparison of the stored hash and the actual file is conducted. If there is a mismatch, the CKS will abort the startup process.

10. After the first unsuccessful PIN code validation attempt, the CKS enforces a wait period of fifteen (15) seconds before the second login attempt can be performed. If a second unsuccessful PIN code validation attempt occurs, the CKS enforces a wait period of thirty (30) seconds before the third login attempt can be made. If a third unsuccessful PIN code validation attempt occurs, the CKS enforces a wait period of forty-five (45) seconds before returning the authentication failure result to the Cryptographic Officer. Subsequent attempts to log in using this ID will result in failure.

    The failure count can be reset one of two ways:

    - A successful login
    - Cycling of power

11. Upon application of power, the CKS shall perform the following tests:

    - Firmware Test
    - Firmware Integrity Test
    - Random Number Generator Statistical Test
    - DES Encryption Algorithm Known Answer Test
    - 3DES Encryption Algorithm Known Answer Test
    - Public Key Encryption Algorithm Key Pair Test
    - SHA-1 Algorithm Test
    - Unit Files Integrity tests

    Failure in any of these tests will result in failure in startup of the CKS and initiate shutdown.

12. The CKS performs the following conditional tests:

    - Pairwise consistency test
    - Continuous PRNG test

13. 5% of the CKS system firmware/source code is coded in assembly language for speed and efficiency within the system. The remaining 95% of the source code is written in C language.

Definition of Security Relevant Data Items

This section identifies all the roles, services, and security relevant data items of the CKS. It specifies the access a user has, when performing a service within the context of a given role, to each of the security relevant data items. It addresses the question, "What access does User X, performing service Y while in role Z, have to security relevant data item K?" for every role, service, and security relevant data item contained in the CKS.

The types of **security relevant data items** are:

1. Master Key (MK) – This is a 16-byte binary key, which is used to encrypt the various keys loaded onto the CKS.
2. Key Encrypting Key (KEK) – This is either a DES or 3DES Key, which is used to encrypt the Working Key (wKEY).
3. Working Key (wKEY) – This is a short-lived key, which is generated and refreshed on a regular basis. Each cryptographic request can be executed using a unique Working Key.
4. Key Transport Key (KTK) – This refers to the RSA key pair used to encrypt/decrypt keys for transport purposes.
5. Smart Card PIN – This PIN is used by the appointed Cryptographic Officer to unlock and retrieve the Master Key from the Smart Card.
6. Access PIN – These PINs are assigned to the Root Administrator, Superuser and Operator for authentication purposes. Only the hash of the ID and PIN are stored in the CKS.
7. Session ID (SID) – These are User Authentication session IDs generated by the CKS for administration services.
8. Session Key (SK) – 3DES key used to transport authentication data in a protected form.
9. Transport Key (TK) – This is the set of system RSA keys used to transport the Session Key in protected form into the module.
10. Transport Encryption Key (TEK) – This is a system generated 3DES key used to encrypt the Private Key component of the Transport Key for non-volatile storage in the module.

Definition of SRDI Modes of Access

The table below shows the relationship between access to SRDIs and Services.

Legend used
G : Generate
D : Delete
R : Read
W : Write
V : Verify (Read & Compare)
U : Usage

Services vs SRDI Access

Services	Master Key (MK)	Key Encrypt Key (KEK)	Key Transport Key (KTK)	Smart Card PIN	User Access PIN	User Auth Session ID (SID)	Working Key (wKEY)	Session Key (SK)	Transport Keys (TK)	Transport Encryption Keys (TEK)
Master Key Generation	G			G					G	G
Smart Card Change PIN				V W						
Master Key Duplication	R W			V G						
Create Superuser Delete Superuser					G D					
Change Root Admin PIN					V W					
Master Key Loading	R W			V						
User Auth					V	G		U	U	R
Key Generate	U	G				V				
Key Loading	U	R W	R W			V				
Key Generate RSA	U		G			V				
Key Unloading		D	D			V				
Configure Printer Port						V				
System Check						V				

Services	Master Key (MK)	Key Encrypt Key (KEK)	Key Transport Key (KTK)	Smart Card PIN	User Access PIN	User Auth Session ID (SID)	Working Key (wKEY)	Session Key (SK)	Transport Keys (TK)	Transport Encryption Keys (TEK)
Retrieve Event Log						V				
Retrieve System Log						V				
Start Operation						V				
• des_encrypt		U					U			
• des_decrypt		U					U			
• tdes_encrypt		U					U			
• tdes_decrypt		U					U			
• rsa_encrypt			U				U			
• rsa_decrypt			U				U			
• ewkey_generate		U					G			
• hash_sha										
• mac_x919_generate		U					U			
• mac_x919_verify		U					U			
• mac_fips113_generate		U					U			
• mac_fips113_verify		U					U			
Stop Operation						V				
Shutdown						V				
Load Operation Policy						V				
Clear Operation Policy						V				
Install Operation Policy						V				
Retrieve Operation Policy						V				
Retrieve Available Operations						V				
Create Operator					G	V				
Delete Operator					D	V				
User Change Pin					V W	V		U	U	U
User Log out						V				

Your Total Business Solution…

HONG KONG
PrivyLink (HK) Ltd
Portion B, 38/F Bank of China Tower
1 Garden Road, Hong Kong
Tel: (852) 2523 3908 Fax: (852) 2501 5503
Sales support: sales@privylink.com.hk

SINGAPORE
PrivyLink Pte Ltd
77 Science Park Drive
#02-05 CINTECH III
Singapore Science Park 1
Singapore 118256
Tel: (65) 882 0700 Fax: (65) 872 5490
URL: http://www.privylink.com
Sales support: sales @privylink.com.sg

Privylink
Privylink
Privylink