Md. Budrul Hasan Bhuiyan (Shohagh)
Assistant Manager
aamra technologies ltd.

THALES

aamra
TECHNOLOGIES

About Aamra

Aamra is an combination of businesses focused towards catalyzing the modernization of Bangladesh by providing technology driven solutions to their clients in various market segments.

For more info please visit www.aamra.com.bd

THALES

aamra TECHNOLOGIES

Companies of Aamra

TEXTILE & APPARELS

ICT

OUTSOURCING AND PROFESSIONAL DEVELOPMENT

Textile and Apparels

- **aamra resources limited**
- **aamra embroideries limited**
- **aamra fashions (cepz) limited**

Information and Communication Technologies

- **aamra technologies limited**
- **aamra networks limited**
- **aamra infotainment limited**
- **aamra solutions limited**
- **aamra outsourcing limited**

Outsourcing and Professional Development

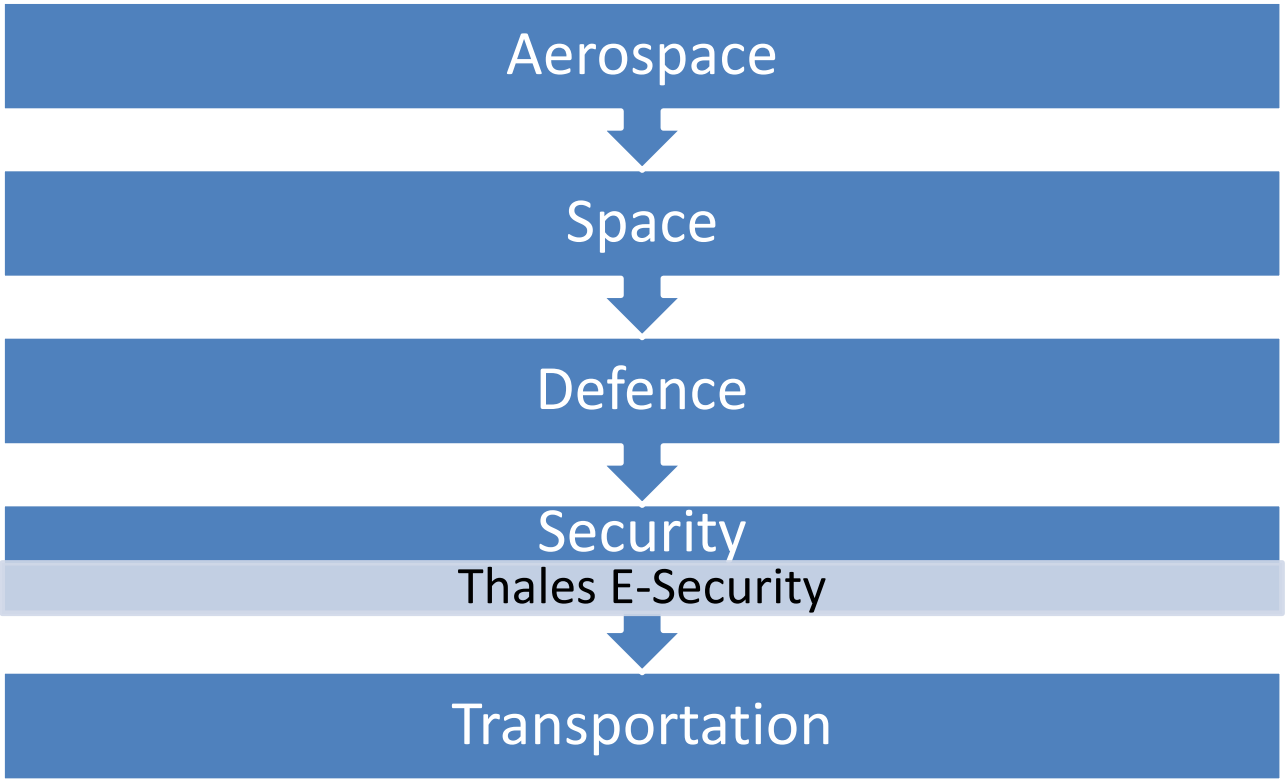
- **aamra fitness limited**
- **aamra management solutions**

THALES

aamra TECHNOLOGIES

THALES

www.thalesgroup.com



HSM ?

THALES

aamra TECHNOLOGIES

Hardware Security Modules (HSMs)

Hardware security modules (HSMs) is a tamper-resistant environment for performing secure cryptographic processing, key protection, and key management.

With these devices you can deploy high assurance security solutions that satisfy widely established standards for cryptographic systems and practices—while also maintaining high levels of operational efficiency.

HSMs are available in multiple form factors to support all common deployment scenarios ranging from portable devices to high-performance data center. Turn to nShield HSMs for general-purpose security, and turn to payShield 9000 for leading payment system security. Whichever HSMs you choose, you will gain confidence in system security *and* streamline administration and regulatory compliance.

THALES

aamra TECHNOLOGIES

Thales payShield 9000

THALES

aamra TECHNOLOGIES

Thales payShield 9000

Designed specifically for payments applications, payShield 9000 from Thales e-Security is a proven hardware security module (HSM) that performs tasks such as PIN protection and validation, transaction processing, payment card issuance, and key management.

payShield 9000 is the most widely deployed payment HSM in the world, used in an estimated 80% of all payment card transactions.

The payShield 9000 device is deployed as an external peripheral for mainframes and servers running card issuing and payment processing software applications for the electronic payments industry—delivering high assurance protection for Automated Teller Machine (ATM) and Point of Sale (POS) credit and debit card transactions.

THALES

aamra TECHNOLOGIES

Thales payShield 9000

The cryptographic functionality and management features of payShield 9000 meet or exceed the card application and security audit requirements of the major international card schemes, including American Express, Discover, JCB, MasterCard, UnionPay, and Visa.

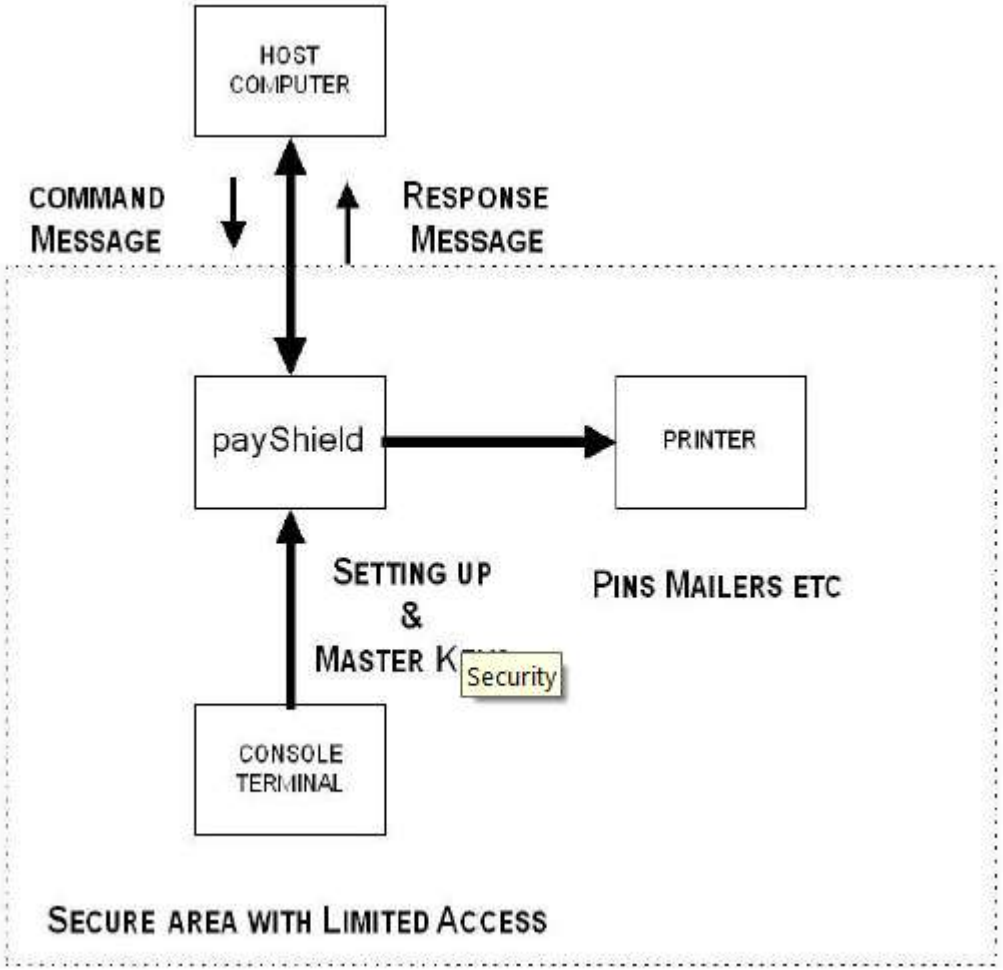
THALES

aamra TECHNOLOGIES

Thales payShield 9000 Standard functions

- Verifying and generating Personal Identification Numbers (PINs) such as those used with bank accounts and credit cards.
- Generating encrypted card values such as Card Verification Values (CVVs) for the plastic card industry.
- PIN solicitation, to obtain a new PIN from a card holder (against a reference number).
- Generating keys for use in Electronic Funds Transfer Point of Sale (EFTPOS) systems.
- Key management in non-EFTPOS systems.
- Generating and verifying Message Authorization Codes (MACs) for messages transferred via telecommunications networks.

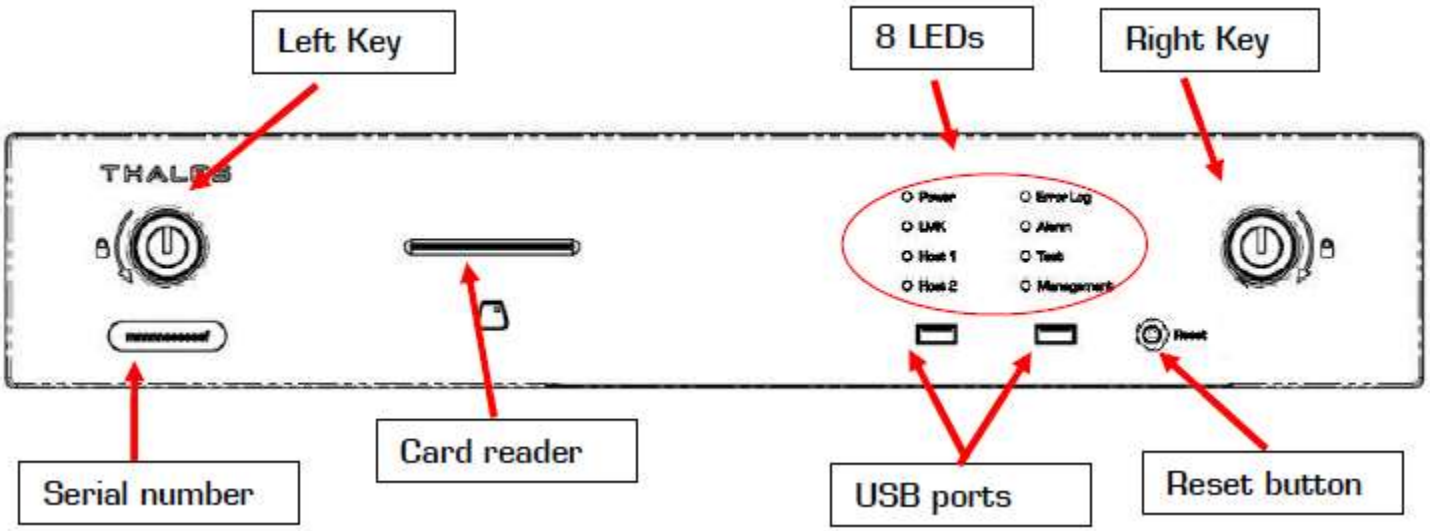
payShield 9000 HSM in a Typical System



THALES

aamra TECHNOLOGIES

Thales payShield 9000 Front view



THALES

aamra TECHNOLOGIES

States are supported by payShield 9000

State	Left hand lock	Right hand lock
Normal (online)	Locked (activated)	Locked (activated)
Offline	Locked	Unlocked
Offline	Unlocked	Locked
Secure	Unlocked	Unlocked

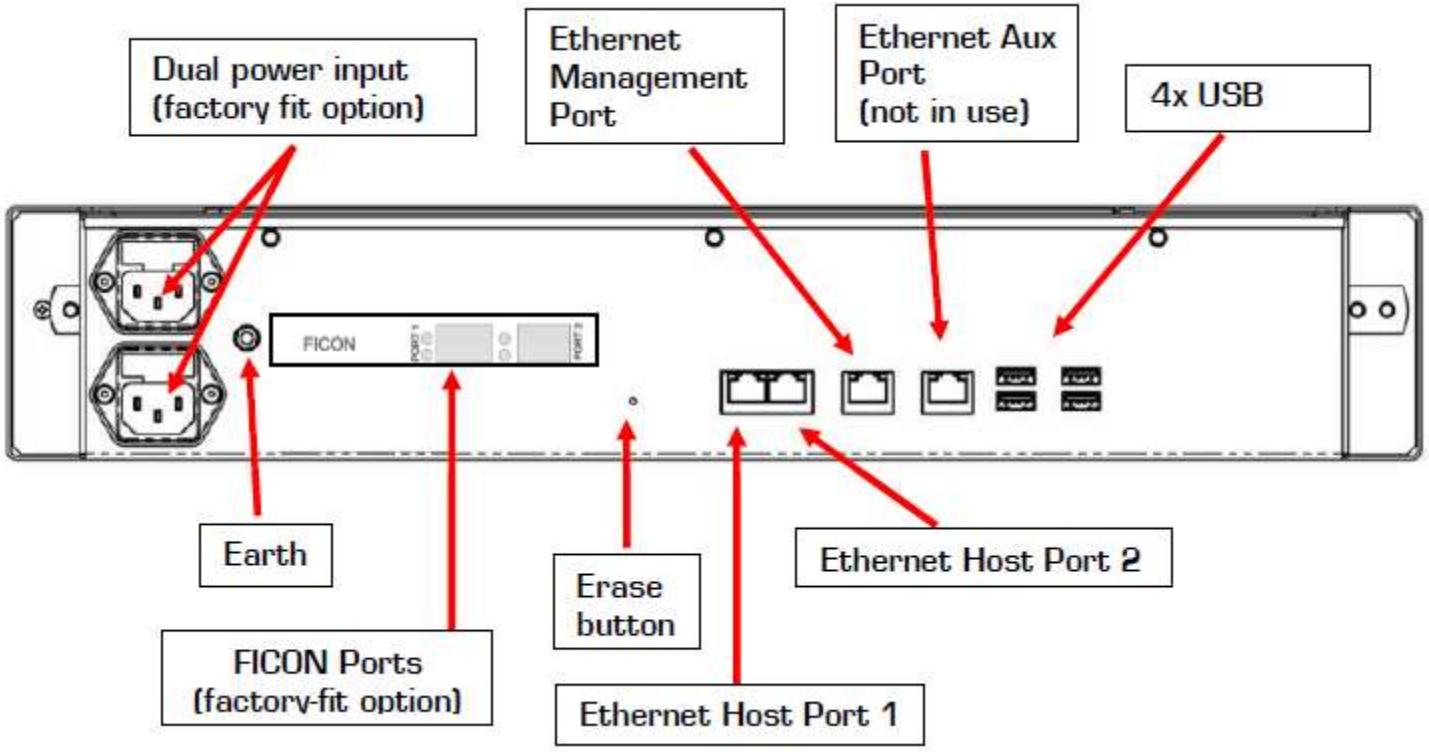
THALES

aamra TECHNOLOGIES

Power LED

LED indicator	Description
Green	For dual-power payShield 9000 units: Power is being supplied through both sockets. For single-power supply payShield 9000 units: Power supply is on.
Yellow (dual-power units only)	Power supplied through upper socket only. The lower socket is not providing power.
Red (dual-power units only)	Power supplied through lower socket only. The upper socket is not providing power.

Thales payShield 9000 rear view



THALES

aamra TECHNOLOGIES

Mechanical and Electrical Specifications

Dimensions		
Height	:	85 mm (3.35 in)
Width	:	478 mm (18.82 in)
Depth	:	417 mm (16.42 in)
Weight	:	7.5 kg (16 lb.) (Dual PSU unit)
Power (per Unit)		
Voltage	:	100 to 240 V AC Universal Input
Frequency	:	47 to 63 Hz
Consumption	:	100 W (maximum)
Rating	:	100-240Vac, 2.1 - 0.85A
Environmental		
Operating temperature	:	0 to +40° C
Humidity	:	10 to 90% (non-condensing)

THALES

aamra TECHNOLOGIES

HSM Smartcard

The smartcard is used in conjunction with the HSM 8000 and payShield 9000 to securely store:

Local Master Key components;
HSM configuration details;
Remote Manager key material

THALES

aamra TECHNOLOGIES

LMK and Authorizing officer cards

LMK Component 1

LMK Component 2

LMK Component 3

Key 1 and 2

Auth. Officer 1

Auth. Officer 2

THALES

aamra TECHNOLOGIES

Security Management Controls

Operational State	-	**Security Officer Keylocks**
No Keys	-	Online – Live Operation
1 Key holder	-	Offline – Config. and Maintenance
1 and 2 Keys Holder	-	Secure- Key Load, Config. Alarms

THALES

aamra TECHNOLOGIES

Connecting to the Console Terminal

The console is connected to one of the USB port on the console, using the USB-to-Serial converter cable supplied with the payShield 9000.

The USB ports on the HSM have a hierarchy, and it is important that no serial devices are attached to a USB port with a higher priority than the Console.
The port hierarchy (from highest to lowest) is:
Front left port
Front right port
Rear port labeled “1”
Rear port labeled “2”
Rear port labeled “3”

If a Console is being attached to a payShield 9000 that has already been in use, it must not be attached to a USB port which has been configured for a printer.

View the License

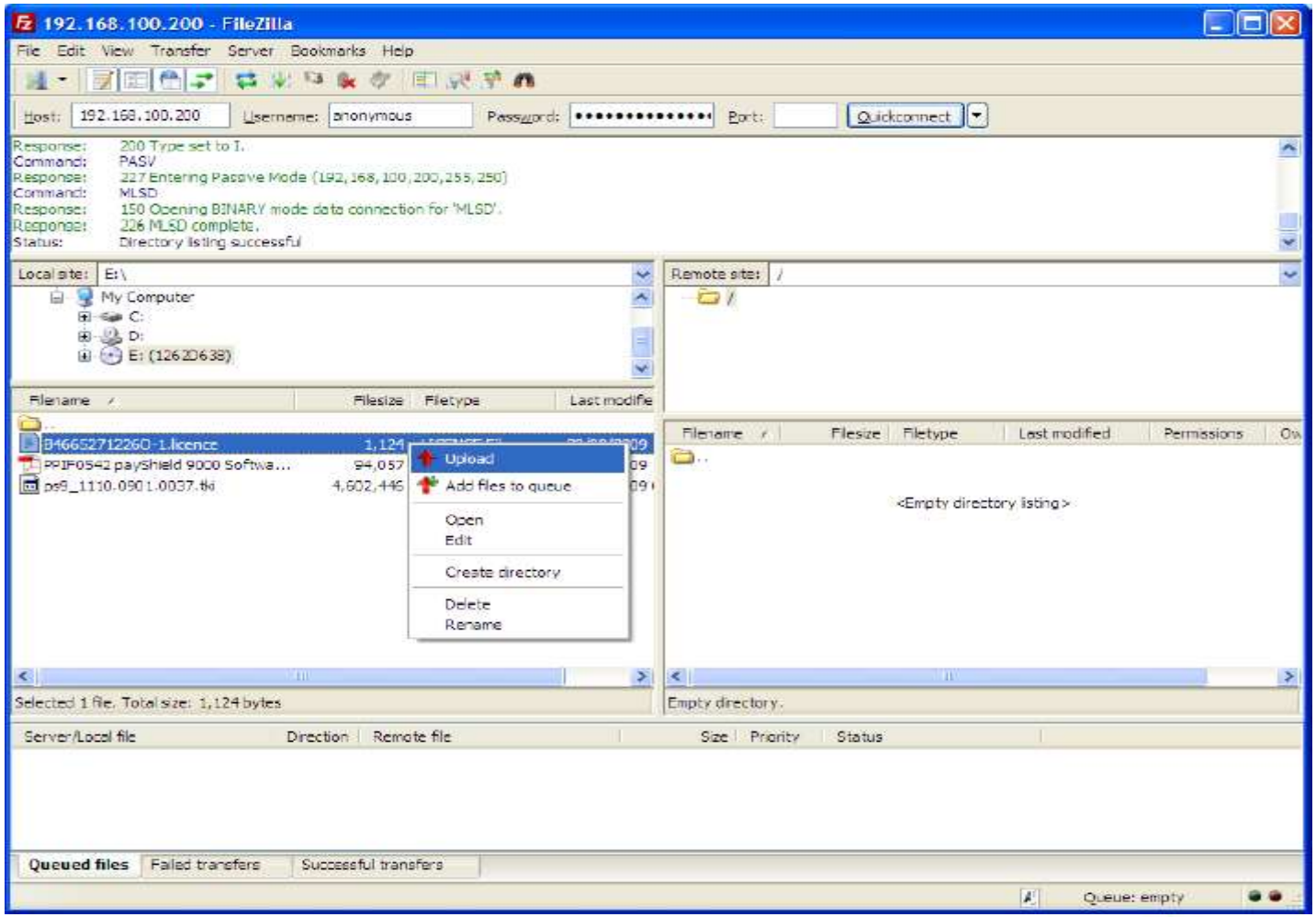
An HSM license is an electronic file which when loaded into a payShield 9000 HSM, determines the features available to the user. The license is associated with a particular unit's serial number and is therefore not transferable between units. The license will affect such areas as the communication interfaces and the cryptographic algorithms available

VR Command is used to view the HSM License information.

Base Versions payShield 9000

- 1.1a
- 1.1b
- 1.2a
- 1.4c
- 1.4d
- 2.2a (Obsolete because of Open SSL bug)
- 2.2b

Upload the License to HSM



THALES

aamra TECHNOLOGIES

Diagnostic commands

NETSTAT

Input Parameter	Description
-m	Use the HSM Management Ethernet port instead of the Host port.
-e	Display Ethernet statistics.
-c	Clear 'old' connection details. All UDP connections and closed TCP connections will be removed from the static data.

```
Online> netstat <Return>

Connections to Host port 193.240.101.65:

Protocol  Local Port  Remote Address        TCP State      Time(D:H:M:S)
--------  ----------  --------------        ---------      -------------
TCP       1032        193.240.101.1:3434    ESTABLISHED    2:04:12:55
TCP       1034        193.240.101.1:3437    CLOSED         2:03:41:45
TCP       1035        193.240.101.241:2338  ESTABLISHED    0:00:32:41
TCP       1036        193.240.101.1:3439    CLOSED         2:04:01:27
UDP       2043        193.240.101.1:4045                   1:43:10:19

Online>
```

```
Online> netstat -m <Return>

Connections to Management port 193.240.101.11:

Protocol   Local Port   Remote Address         TCP State      Time(D:H:M:S)
--------   ----------   --------------         ---------      -------------
TCP        1032         193.240.101.1:3434     ESTABLISHED    2:04:12:55
UDP                     193.240.100.163:4054                  1:52:07:11

Online>
```

THALES

aamra TECHNOLOGIES

Diagnostic commands

PING

Input Parameter	Description
-m	Use the HSM Management Ethernet port instead of the Host port.
-t	Keep executing the command until a console key is pressed.
-n *count*	The *count* value is the number of echo requests to send.
-l *TTL*	The *TTL* value is count which is used to prevent a request from getting stuck in a looping situation. Each time the command passes through a router or server the value is decremented by one. This will continue until the value reaches 0 at which point the error "TTL expired in transit" will be returned.
-w *timeout*	The *timeout* value is the time in milliseconds to wait for each reply.
target	This is the IP address of the target node.

```
Online> ping 213.158.224.29 <Return>

Pinging 213.158.224.29 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 213.158.224.29:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

Online>
```

THALES

aamra TECHNOLOGIES

Diagnostic commands

Input Parameter	Description
-m	Use the HSM Management Ethernet port instead of the Host port.
-h *maximum_hops*	The *maximum_hops* value defines the maximum number of hops to take before terminating the attempt.
-w *timeout*	The *timeout* value is the time in milliseconds to wait for each reply.
target	This is the IP address of the target node.

TRACERT

```
Online> tracert 213.158.224.29 <Return>

Tracing route to 213.158.224.29 over a maximum of 30 hops

  1     3 ms     3 ms     2 ms  193.240.100.1
  2   <10 ms   <10 ms   <10 ms  193.240.100.3
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  .
  .
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete

Online>
```

THALES

aamra TECHNOLOGIES

Diagnostic commands

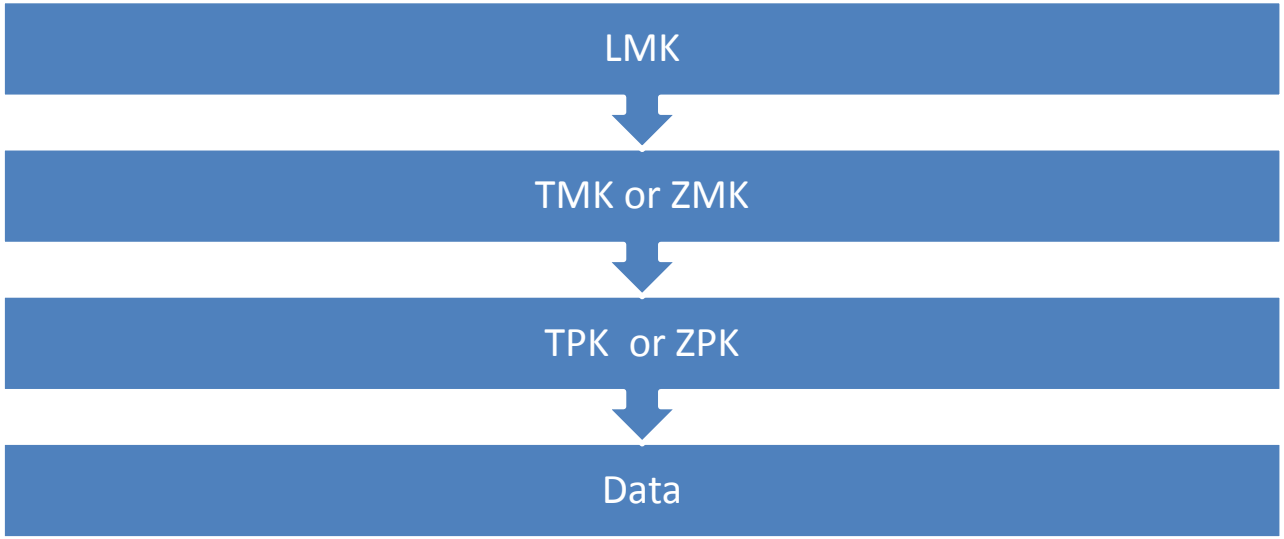
DT

all	run all the commands (default option)
verbose	be verbose in the output
battery	run the battery diagnostics
des	run the DES diagnostics
aes	run the AES diagnostics
health	run the health check diagnostics
md5	run the MD5 KAT
mem	run the memory diagnostics
psu	run the power supply diagnostics
rng	run the random number generator diagnostics
rsa	run the RSA KAT
rtc	run the real-time clock diagnostics
scr	run the smart card reader diagnostics
sha	run the SHA KAT
temp	run the temperature diagnostics
fans	run the fans diagnostics
volt	run the voltage diagnostics

LMK – Local Mater Key

The local master key is the master key for your HSM, used to protect all other keys in your system.

Often be hierarchy of keys.



LMK Component Generation

```
Secure> GK <Return>
Variant scheme or key block scheme? [V/K]: K <Return>
Key status? [L/T]: L <Return>
LMK component set [1-9]: 1 <Return>
Enter secret value A: <Return>
Enter secret value B: <Return>
Enter secret value C: <Return>
Insert blank card and enter PIN: **** <Return>
         Writing key
         Checking key
Device write complete, check: 0123 45
Make another copy? [Y/N]: Y <Return>
…
Secure>
```

THALES

aamra TECHNOLOGIES

LMK Loading

```
Secure> LK <Return>
Enter LMK id: 02 <Return>
Enter comments: Live LMK for PQR Bank <Return>
LMK in selected location must be erased before proceeding.
Erase LMK? Y <Return>
Load LMK from components
Insert card and enter PIN: **** <Return>
Check: 0123 45
Load more components? [Y/N]: Y <Return>
…
…
Check: 3967 23
Load more components? [Y/N]: N <Return>
LMK id: 02
LMK key scheme: Key block
LMK algorithm: 3DES (3key)
LMK status: Live
Comments: Live LMK for PQR Bank
Confirm details? [Y/N]: Y <Return>
…
Secure>
```

LMK Table

```
Online> VT <Return>

LMK table:
ID Scheme    Algorithm  Status Check  Comments                    Auth
00 Variant   3DES(2key) Live   123456 Default LMK, for RST Bank  Yes (3)
01 Key Block 3DES(3key) Test   999999 Test LMK for XYZ Bank      No
02 Key Block 3DES(3key) Live   396723 Live LMK for PQR Bank      No
03 Key Block 3DES(3key) Live   223344 Management LMK             No

Key change storage table:
ID Scheme    Algorithm  Status Check  Comments
01 Variant   3DES(2key) Test   876543 Old test LMK for XYZ Bank
02 Key Block 3DES(3key) Live   085392 Old LMK for PQR Bank

Online>
```

Multiple Authorization Activity

```
Online> A <Return>
Enter LMK id: 03 <Return>
No activities are authorized for LMK id 03
List of authorizable activities:
…
…
The following activities are pending authorization:
pin.mailer
First Officer:
Insert card for Security Officer and enter the PIN: **** <Return>
Second Officer:
Insert card for Security Officer and enter the PIN: **** <Return>
The following activities are authorized for LMK id 03:
pin.mailer

Online-AUTH>
```

THALES

aamra TECHNOLOGIES

Ethernet TCP Port

Command received on TCP Port	LMK Used
1500	Default LMK Id (LMK explicitly identified in host command)
1501	LMK Id 00
1502	LMK Id 01
1503	LMK Id 02
...	...

Host commands sent via TCP/IP have been directed to the HSM's Well-Known Port, and this continues to be supported. However, host commands directed to [the Well-Known Port +1] will automatically use LMK Id 00; host commands directed to [the Well-Known Port +2] will automatically use LMK Id 01

Configure HSM Settings

What is it?

- Configuration of sets security parameter and some processing parameters
- Pay Shield 9000 must be in secure state
- Requires reloading of LMK for security sensitive changes

Configure HSM Settings

PIN length: 04
Encrypted PIN length: 05
Echo: OFF
Atalla ZMK variant support: OFF
Transaction key support: RACAL
User storage key length: SINGLE
Select clear PINs: NO
Enable ZMK translate command: YES
Enable X9.17 for import: YES
Enable X9.17 for export: YES
Solicitation batch size: 1024
Single-DES: DISABLED
Prevent Single-DES keys masquerading as double or triple-length keys: NO
ZMK length: DOUBLE
Decimalization tables: PLAINTEXT
Decimalization table checks: DISABLED

Configure HSM Settings Continue …

PIN encryption algorithm: A
Card/password authorisation (local): C
Authorised State required when Importing DES key under RSA key: YES
Minimum HMAC key length in bytes: 10
Enable PKCS#11 import and export for HMAC keys: YES
Enable ANSI X9.17 import and export for HMAC keys: YES
Enable ZEK encryption of all printable ASCII chars: YES
Enable ZEK encryption of "Base94" ASCII chars: YES
Enable ZEK encryption of "Base64" ASCII chars: YES
Enable ZEK encryption of "Hex-only" ASCII chars: YES
Restrict Key Check Values to 6 hex chars: YES
Enable multiple authorised activities: NO
Enable variable length PIN offset: NO
Enable weak PIN checking: NO
Enable Pin Block Format 34 as output format for PIN Translations to ZPK: YES
Default LMK identifier: 00

Configure HSM Settings Continue …

Management LMK identifier: 00
Use HSM clock for date/time validation: NO
Additional padding to disguise key length: NO
Key export and import in trusted format only: NO
Protect MULTOS Cipher Data Checksums: NO

Document

QS Console Command to view the HSM Settings

Configure HSM Host

CH Console Command to configure the HSM Host. From version 2.2b H1 and H2 host port are active. And Version lower 2.2b H1 host is active.

Document

Configure HSM PIN Printer

CP command is to configure the PIN Mailer Printer. And QP command is to view the settings.

Document

THALES

aamra TECHNOLOGIES

Printer Communication

Serial Printer

The payShield 9000 HSM can communicate with a printer via an asynchronous serial connection by employing a USB-to-serial converter cable (supplied by Thales). The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM; the serial cable end should be connected to the printer. The console (CP command) or HSM Manager (Edit > Printer Interface menu) can then be used to select the appropriate configuration for the port.

Parallel Printer

The payShield 9000 HSM can communicate with a printer via an industry-standard IEEE 1284 parallel connection by employing a USB-to-parallel converter cable (supplied by Thales). The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM; the parallel cable end should be connected to the printer. The console (CP command) or HSM Manager (Edit > Printer Interface menu) can then be used to select the appropriate configuration for the port.

Configure Console Port

To set the baud rate and word format for the console port. The new settings come into effect immediately after the command has completed. The default settings for the Console Port are: 9600 baud, eight data bits, no parity and one stop bit.

CC command is to configure the console port and QC is to view the console port configuration.
Inputs:
Console baud rate.
Console word format.
Console parity.
Console flow control.
Document

Configure Management Port

To configure the Management port, which is an Ethernet port used only for management of the HSM. If connection to the host is via Ethernet then the Ethernet host port is used for that purpose. The Management Ethernet port is used to update the HSM's internal software, updating licensing information, and for enabling management of a HSM via the Local or Remote HSM Manager.

CM command is to configure the management port and QM is to view the management port configuration.

Document

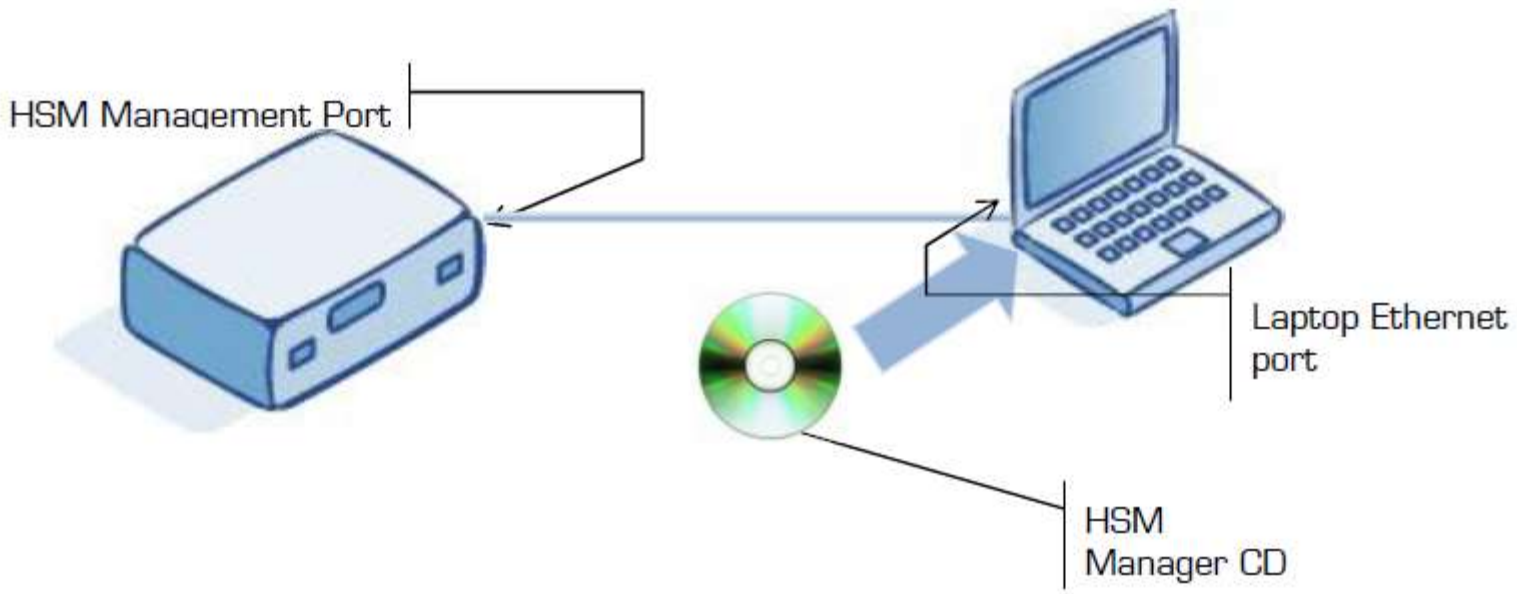
Save Configuration Security Settings

Command SS to save the configuration security settings

- Save configure security settings to smartcard
- Card needss to be correctly formatted (not formatted for LMK)
- Saves just settings form configure commands.

RS Command to past configuration settings to HSM

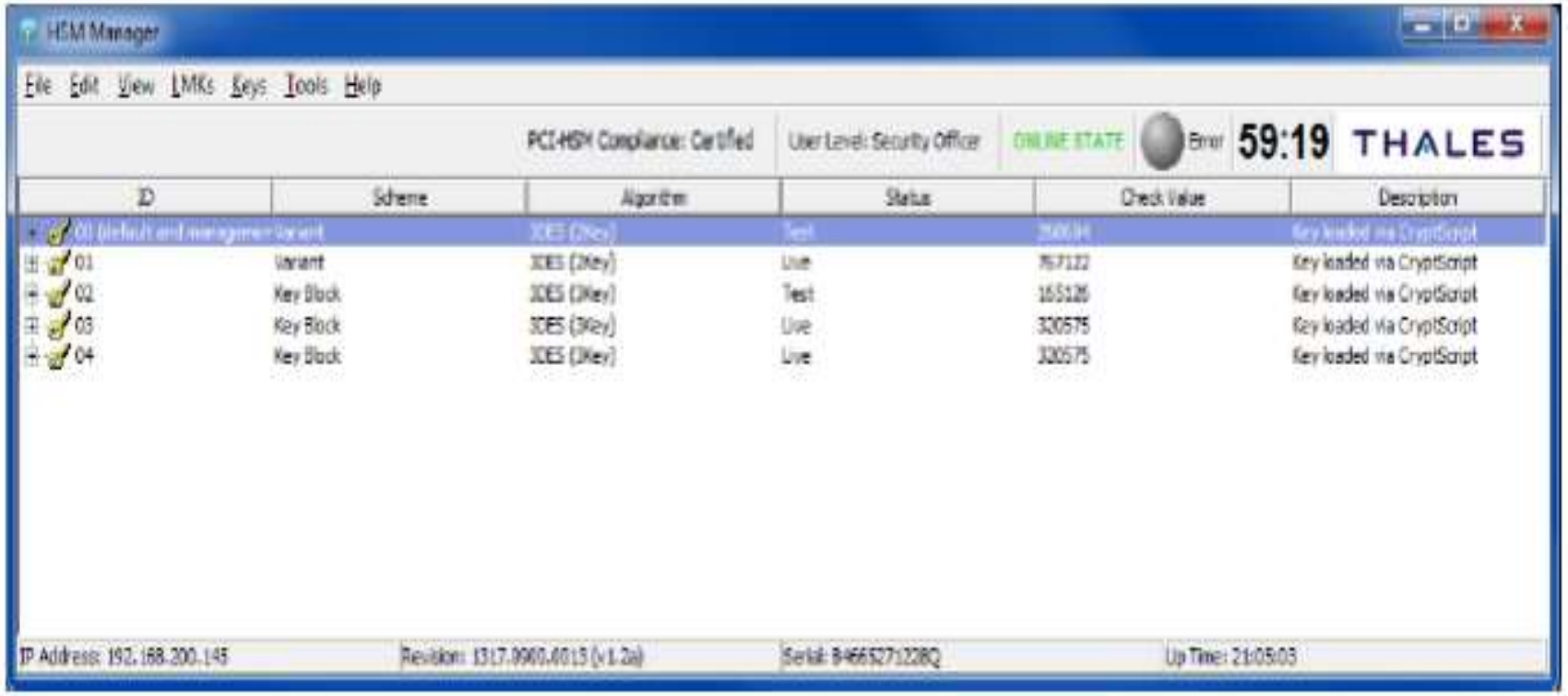
Local HSM Manager



THALES

aamra TECHNOLOGIES

Main Screen LHM



THALES

aamra TECHNOLOGIES

LHM File Menu

Connect – establish a connection with an HSM.
Disconnect – terminate an established connection with an HSM.
Login – login using one or two smartcards, to access Operator or Security Officer functions.
Logout – terminate the current role, and return to Guest.
Load Settings – load HSM settings from a previously saved file.
Save Settings – save HSM settings to a selected file.
Load Firmware – download a different version of firmware into the HSM.
Load Licence – download a different licence into the HSM.
Exit – disconnects you from the HSM and closes down the HSM Manager application

LHM Edit Menu

General Settings – to view/modify general HSM settings.
Advanced Settings – to view/modify important system settings.
Initial Settings – to view/modify sensitive security settings.
Host Interface – to view/modify host communications settings.
Printer Interface – to view/modify serial and parallel printer communications settings.
Management Interface – to view/modify management communications settings.
Host Commands – to view/enable/disable individual or groups of host commands.
PIN Blocks – to view/enable/disable individual PIN block formats.
Auditing – to view/modify the list of audited events.
HSM Date/Time – to view/set the HSM's internal clock.
Authorize – to view/set the HSM's authorized state/activities.

LHM View Menu

Logs – to view/erase the HSM's internal error and audit logs.
HSM Information – to view the HSM information (firmware, licenses, etc.).
Remote Details – to view remote management configuration details.

LHM LMKs Menu

Generate Keys – to generate a new LMK onto smart cards.
Install LMK – to load a new LMK from smart cards into the HSM.
Install 'Old' LMK – to load an old LMK from smart cards into the "key change storage" area.
Copy LMK Component Card – to create a copy of an existing LMK component card.
Create Authorizing Officer Card – to create an LMK Authorizing Officer smartcard from an existing LMK Component Card.
Uninstall LMK – to uninstall an LMK from the HSM.

LHM Keys Menu

Generate Keys – to generate specific keys under the LMK.
Key Import – to import keys from a different cryptographic zone.
Key Export – to export keys to a different cryptographic zone.
Generate Components – to generate new key components.
Encrypt Components – to encrypt supplied key components using the LMK.
Form Key from Components – to form keys from supplied key components.

LHM Tools Menu

Smartcard – to perform smart card management functions.
Diagnostics – to perform network management diagnostic functions.
Utilities – to perform general utility functions, including:
- Calculate Key Check Value
- Encrypt Decimalization Table
- Translate Decimalization Table
- Generate MAC on Issuer Proprietary Bitmap (for CAP/DPA)
- Generate CVV/CVC
- Generate VISA PVV

Utilisation and Health Check Data (*payShield 9000 only*) – to view and manage the HSM's utilization and health check data:
- Configure Statistics
- Health Check Data
- HSM Loading Value Host Command Statistics
- Reset Statistics

LHM Tools Menu

SNMP (*payShield 9000 only*) – to configure the SNMP interfaces:
- Display – show SNMP Communities/Users
- Add – add SNMP Communities/Users
- Delete – remove SNMP Communities/Users

> **Secure Host Communications** *(payShield 9000 only)***:**
- Generate Certificate Signing Request
- Export HSM CA Certificate
- Import Signed Certificate
- Generate HMK
- Recover HMK
- Change HMK Passphrase
- View Certificates
- Delete Certificates

> **Reset Fraud Detection** – to restore operation after fraud detection.

> **Return to Factory Settings** – to remove all settings that have been made since the HSM was shipped from the factory

Audit and Health Check

- Alarms
- Utilization Statistics
- Health Checks
- Error Log
- Audit Log

THALES

aamra TECHNOLOGIES

Alarms

CL Command to configure the alarms:

Secure> **CL**
Please make a selection. The current setting is in parentheses.
Motion alarm [Low/Med/High/ofF] (OFF): **H**
Save ALARM settings to smart card? [Y/N]: **n**

QL Command to view the alarms configuration:

Online> **QL**
Temperature alarm enabled
Motion alarm enabled high sensitivity
Online>

Alarms will log at Audit log and Error log

Utilization Statistics

UTILSTATS - Command View/Reset Utilization Data

Document

THALES

aamra TECHNOLOGIES

Health Check

HEALTHSTATS -- To display Health Check counts at the Console

Document

ERROR LOG

ERRLOG -- To display the entries in the error log

CLEARERR -- To clear the entries in the error log

Document

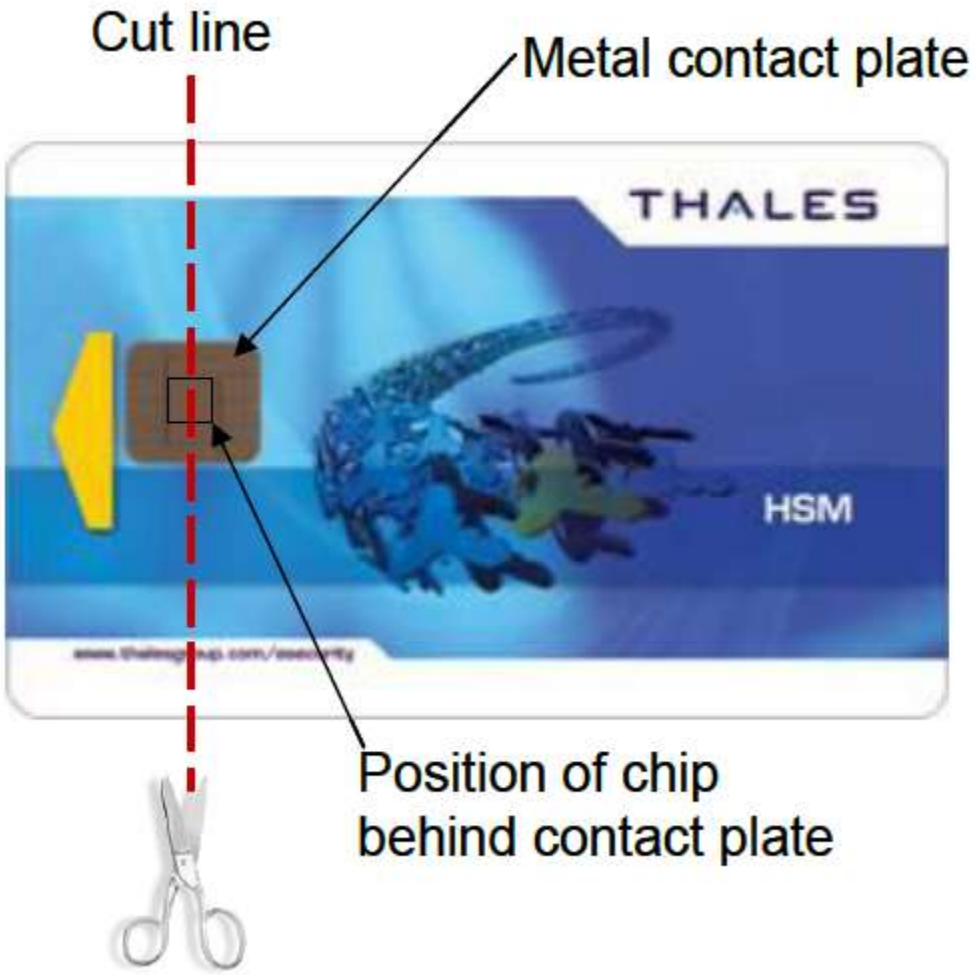
Audit Log

AUDITLOG -- To display the entries in the audit log

CLEARAUDIT -- To clear the entries in the audit log.

Document

Decommissioning an LMK smart card



THALES

aamra TECHNOLOGIES

Permanent HSM Decommissioning

Permanent decommissioning may become necessary when an HSM reaches the end of its normal operational life. For example it could be replaced by a newer model or by a higher speed model, or the application to which it provides security services is to be discontinued.

END of the Session

THALES

aamra TECHNOLOGIES