THALES

www.thales-esecurity.com

Thales e-Security

paySheld 9000 Application Note:

Packages & Licenses for v3.5

PPIF0543-037

3 April 2020

Contents

Packages

Packages are groups of licenses, and there are currently four different packages available for payShield 9000 running V3.5 software. Each payShield 9000 *must* include one (and only one) of these software packages. Customers can choose the package that includes the functionality they need, and some optional software licenses can be added to the package as required.

List of Packages

Package	Description
HSM9-PAC301	Standard Base Package
HSM9-PAC302	Card & Mobile Issuing Package
HSM9-PAC303	Premium Package
HSM9-PAC908	mPOS P2PE Software Package

Comparison of Packages

License	Description	HSM9-PAC301 Standard Base	HSM9-PAC302 Card & Mobile Issuing	HSM9-PAC303 Premium	HSM9-PAC908 mPOS P2PE
HSM9-LIC001	Base Software	☑	☑	☑	☑
HSM9-LIC002	RSA Algorithm		☑	☑	☑
HSM9-LIC003	AS2805 Commands	☐	☐	☐	
HSM9-LIC004	MasterCard OBKM & CEPS	☑	☑	☑	
HSM9-LIC005	User Authentication (HMAC/CAP/DPA)			☑	
HSM9-LIC006	X9 TR-31 Key Block		☑	☑	☑
HSM9-LIC007	AES Algorithm		☑	☑	☑
HSM9-LIC008	Data Protection		☑	☑	☑
HSM9-LIC011	Magnetic Stripe Contactless Card Data Preparation		☑	☑	
HSM9-LIC012	LMK x 2	☐	☐	☐	☐
HSM9-LIC013	LMK x 5	☐	☐	☐	☐
HSM9-LIC014	WebPIN Commands	☐	☐	☐	
HSM9-LIC016	Key & Data Prep for Cards & Mobile		☑	☑	
HSM9-LIC017	HE and HG Host Commands	☐	☐	☐	
HSM9-LIC018	Card Personalization & Mobile Provisioning		☑	☑	
HSM9-LIC019	Pre-master Secret Decryption (TLS/SSL handshake)		☑	☑	
HSM9-LIC020	Korean SEED Algorithm	☑	☑	☑	
HSM9-LIC021	LMK x 10	☐	☐	☐	☐
HSM9-LIC022	LMK x 20	☐	☐	☐	☐
HSM9-LIC023	MULTOS Card Data Preparation		☑	☑	
HSM9-LIC024	Magnetic Stripe Issuing	☑	☑	☑	
HSM9-LIC025	Magnetic Stripe Transaction Processing	☑		☑	*
HSM9-LIC026	EMV Transaction Processing	☑		☑	
HSM9-LIC027	PIN and Key Printing	☑	☑	☑	
HSM9-LIC028	VISA Cash Processing	☑		☑	
HSM9-LIC029	Legacy Commands	☑		☑	
HSM9-LIC030	Miscellaneous HSM 8000 Commands	☑		☑	
HSM9-LIC031	UnionPay Commands	☑		☑	
HSM9-LIC033	RSA Performance Booster				
HSM9-LIC034	MU and MW Host Commands	☑		☑	
HSM9-LIC036	Secure Host Communications	☑	☑	☑	☑
HSM9-LIC037	Remote payShield Manager	☐	☐	☐	☐
HSM9-LIC038	Ingenico BPS (FPE)		☐	☐	☐
HSM9-LIC039	Visa DSP Support		☐	☐	☐
HSM9-LIC041	NIST FF1 Support	☐	☐	☐	☐

Key:

☑	The license is included in the package.
☐	The license is not included in the package, but is available as an optional license.
<blank>	The license is not included in the package, and cannot be added.
*	HSM9-PAC908 includes host commands G0 and GW, which are otherwise found in HSM-LIC025. (No other commands from HSM9-LIC025 are included in HSM9-PAC908.)

HSM9-PAC301
Standard Base Package

Overview

This package is typically for organizations involved in merchant acquiring, transaction switching and payment authorization who might need to support remote ATM key loading, establishment of cryptographic key zones (with processors, card schemes, switches etc.), transaction authorization or need PIN block management functionality.

This package supports all the commands necessary for authorization of magnetic stripe and EMV card transactions but specifically excludes the commands relating to the issuing of these cards.

This package is for customers who previously purchased PAC001 and have little need for optional licenses.

Package Contents

License	Description
HSM9-LIC001	Base Software
HSM9-LIC004	MasterCard OBKM & CEPS
HSM9-LIC020	Korean SEED Algorithm
HSM9-LIC024	Magnetic Stripe Issuing
HSM9-LIC025	Magnetic Stripe Transaction Processing
HSM9-LIC026	EMV Transaction Processing
HSM9-LIC027	PIN and Key Printing
HSM9-LIC028	VISA Cash Processing
HSM9-LIC029	Legacy Commands
HSM9-LIC030	Miscellaneous HSM 8000 Commands
HSM9-LIC031	UnionPay Commands
HSM9-LIC034	MU and MW Host Commands
HSM9-LIC036	Secure Host Communications

HSM9-PAC302
Card & Mobile Issuing Package

Overview

This package is for financial institutions and third party service organizations involved in the card issuing or mobile provisioning processes and who do not require transaction processing capabilities. It includes commands to facilitate generation of data for magnetic stripe, EMV contact and contactless applications, and the provision of this data to cards & mobile devices.

It supports the key management, PIN management and basic data preparation commands to enable the issuer to produce a data file which could be used either by an in-house or external bureau card personalization and production facility.

Package Contents

License	Description
HSM9-LIC001	Base Software
HSM9-LIC002	RSA Algorithm
HSM9-LIC004	MasterCard OBKM & CEPS
HSM9-LIC006	X9 TR-31 Key Block
HSM9-LIC007	AES Algorithm
HSM9-LIC008	Data Protection
HSM9-LIC011	Magnetic Stripe Contactless Card Data Preparation
HSM9-LIC016	Key & Data Prep for Cards & Mobile
HSM9-LIC018	Card Personalization & Mobile Provisioning
HSM9-LIC019	Pre-master Secret Decryption (TLS/SSL handshake)
HSM9-LIC020	Korean SEED Algorithm
HSM9-LIC023	MULTOS Card Data Preparation
HSM9-LIC024	Magnetic Stripe Issuing
HSM9-LIC027	PIN and Key Printing
HSM9-LIC036	Secure Host Communications

HSM9-PAC303 Premium Package

Overview

This package is an enhanced package designed for customers who process transactions and who have additional RSA, AES, TR-31, User Authentication or Data Protection requirements. This package is also appropriate for customers with both issuing and processing requirements who want to standardize on software & licenses across their entire HSM estate.

Package Contents

License	Description
HSM9-LIC001	Base Software
HSM9-LIC002	RSA Algorithm
HSM9-LIC004	MasterCard OBKM & CEPS
HSM9-LIC005	User Authentication (HMAC/CAP/DPA)
HSM9-LIC006	X9 TR-31 Key Block
HSM9-LIC007	AES Algorithm
HSM9-LIC008	Data Protection
HSM9-LIC011	Magnetic Stripe Contactless Card Data Preparation
HSM9-LIC016	Key & Data Prep for Cards & Mobile
HSM9-LIC018	Card Personalization & Mobile Provisioning
HSM9-LIC019	Pre-master Secret Decryption (TLS/SSL handshake)
HSM9-LIC020	Korean SEED Algorithm
HSM9-LIC023	MULTOS Card Data Preparation
HSM9-LIC024	Magnetic Stripe Issuing
HSM9-LIC025	Magnetic Stripe Transaction Processing
HSM9-LIC026	EMV Transaction Processing
HSM9-LIC027	PIN and Key Printing
HSM9-LIC028	VISA Cash Processing
HSM9-LIC029	Legacy Commands
HSM9-LIC030	Miscellaneous HSM 8000 Commands
HSM9-LIC031	UnionPay Commands
HSM9-LIC034	MU and MW Host Commands
HSM9-LIC036	Secure Host Communications

HSM9-PAC908
mPOS P2PE Software Package

Overview

This package is designed for payment service providers who are implementing systems to provide Mobile Point Of Sale (mPOS – also referred to as Mobile Acceptance) solutions using Point-to-Point Encryption (P2PE).

Package Contents

License	Description
HSM9-LIC001	Base Software
HSM9-LIC002	RSA Algorithm
HSM9-LIC006	X9 TR-31 Key Block
HSM9-LIC007	AES Algorithm
HSM9-LIC008	Data Protection
HSM9-LIC036	Secure Host Communications

This package also provides the following Host commands:

Command	Description
G0	Translate a PIN from BDK to ZPK (DUKPT)
GW	Generate/Verify MAC (3DES DUKPT)

Note: HSM9-PAC908 includes host commands G0 and GW, which are otherwise found in HSM9-LIC025. (No other commands from HSM9-LIC025 are included in HSM9-PAC908.)

Licenses

Licenses are available to extend the payShield 9000's functionality, both in terms of commands and algorithm support. Each license is assigned a unique number (HSM9-LICxxx), and the functionality unlocked by each license is described later in this document.

The table below lists the complete set of licenses that are available for use with payShield 9000 v3.5 software. ***Many of these licenses are only available as part of one of the packages (see Packages).*** See the next section (List of Optional Licenses) for a list of the optional licenses available with V3.5 software onwards.

Complete List of Licenses

License	Description
HSM9-LIC001	Base Software
HSM9-LIC002	RSA Algorithm
HSM9-LIC003	AS2805 Commands
HSM9-LIC004	MasterCard OBKM & CEPS
HSM9-LIC005	User Authentication (HMAC/CAP/DPA)
HSM9-LIC006	X9 TR-31 Key Block
HSM9-LIC007	AES Algorithm
HSM9-LIC008	Data Protection
HSM9-LIC011	Magnetic Stripe Contactless Card Data Preparation
HSM9-LIC012	LMK x 2
HSM9-LIC013	LMK x 5
HSM9-LIC014	WebPIN Commands
HSM9-LIC016	Key & Data Prep for Cards & Mobile
HSM9-LIC017	HE and HG Host Commands
HSM9-LIC018	Card Personalization & Mobile Provisioning
HSM9-LIC019	Pre-master Secret Decryption (TLS/SSL handshake)
HSM9-LIC020	Korean SEED Algorithm
HSM9-LIC021	LMK x 10
HSM9-LIC022	LMK x 20
HSM9-LIC023	MULTOS Card Data Preparation
HSM9-LIC024	Magnetic Stripe Issuing
HSM9-LIC025	Magnetic Stripe Transaction Processing
HSM9-LIC026	EMV Transaction Processing
HSM9-LIC027	PIN and Key Printing
HSM9-LIC028	VISA Cash Processing
HSM9-LIC029	Legacy Commands
HSM9-LIC030	Miscellaneous HSM 8000 Commands
HSM9-LIC031	UnionPay Commands
HSM9-LIC034	MU and MW Host Commands
HSM9-LIC036	Secure Host Communications
HSM9-LIC037	Remote payShield Manager
HSM9-LIC038	Ingenico BPS (FPE)
HSM9-LIC039	Visa DSP Support
HSM9-LIC041	NIST FF1 Support

List of Optional Licenses

The following optional licenses are available to extend the payShield 9000's functionality, both in terms of commands and algorithm support.

Note that some optional licenses are only compatible with certain packages. For full details, refer to the descriptions of each license in this document.

License	Description
HSM9-LIC003	AS2805 commands
HSM9-LIC012	LMK x 2
HSM9-LIC013	LMK x 5
HSM9-LIC014	WebPIN Commands
HSM9-LIC017	HE & HG Host Commands
HSM9-LIC021	LMK x 10
HSM9-LIC022	LMK x 20
HSM9-LIC037	Remote payShield Manager
HSM9-LIC038	Ingenico BPS (FPE)
HSM9-LIC039	Visa DSP Support
HSM9-LIC041	NIST FF1 Support

HSM9-LIC001 Base Software

Overview

This license is automatically included in all payShield 9000 packages and cannot be disabled but can be replaced later by a future base version. It contains a set of core management, cryptographic and diagnostic commands that all HSMs need to provide (just to be of practical use) and are independent of any specific commands for the different application requirements that payShield 9000 is expected to address.

NOTE: Not all console commands and host commands can be used with Key Block LMKs. Most commands that fall into this category either have a newer, alternative command that should be used in their place, or relate to functionality in optional licenses. You should check the Key Block support indicator at the start of the section describing the command (or, if that is not present, the notes for the command) for all commands you intend to use to confirm that they function with Key Block LMKs.

Console Commands

Command	Description
$	Double-Length Key Calculator
A	Authorise Activity/State
A5	Configure Fraud Detection
A7	Re-enable PIN verification
AUDITLOG	Display the Audit Log
AUDITOPTIONS	Audit Options
AUDITPRINT	Print audit log
B	Generate a Zone PIN Key
BK	Form a Key from Components
C	Cancel Authorised Activity/State
CC	Configure Console Port
CH	Configure Host Port
CK	Generate a Check Value
CL	Configure Alarms
CLEARAUDIT	Clear the Audit Log
CLEARERR	Clear the Error Log
CM	Configure Management Port
CO	Create Authorising Officer Smartcard
CONFIGACL	Configure the Host Port ACL
CONFIGCMDS	Configure Commands
CONFIGPB	Configure PIN Block Formats
CP	Configure Printer Port
CS	Configure Security
CV	Generate a Card Verification Value
D	Form a ZMK From Encrypted Comps
DA	Generate and Export a KML
DC	Duplicate LMK Component Sets
DD	Generate a Double-Length ZMK Comp
DE	Form a ZMK from Clear Components
DG	Generate a Base Derivation Key (BDK)
DM	Delete LMK
DO	Delete "Old" LMK from Key Change Storage
DT	Diagnostic Test
EC	Encrypt Clear Component
ED	Encrypt Decimalisation Table

Command	Description
N	Single-Length Key Calculator
NETSTAT	Show Network Statistics
NP	Change a Smartcard PIN
PING	Test TCP/IP Network
PV	Generate a VISA PIN Verification Value
QC	View Console Port Configuration
QH	View Host Port Configuration
QL	View Alarm Configuration
QM	View Management Port Configuration
QP	View Printer Port Configuration
QS	View Security Configuration
R	Load the Diebold Table
RC	Read Unidentifiable Smartcard Details
RESET	Reset to Factory Settings
RH	Generate an HSM Certificate
RI	Initialize Domain Authority
ROUTE	Add a Static TCP/IP Route
RS	Retrieve HSM Settings from a Smartcard
RZ	Backup Domain Authority Card
SD	Delete Installed Certificate(s)
SE	Export HSM Certificate's Chain of Trust
SETTIME	Set the Time and Date
SG	Generate Certificate Signing Request
SI	Import Certificate
SK	Generate HRK
SL	Restore HRK
SP	Change HRK Passphrase
SNMP	View SNMP Settings
SNMPADD	Add an SNMP Community or User
SNMPDEL	Delete an SNMP Community or User
SS	Save HSM Settings to a Smartcard
ST	Set Time for Automatic Self-Tests
SV	View Installed Certificate(s)
T	Triple-Length Key Calculator
TD	Translate Decimalisation Table

Command	Description
EJECT	Eject a Smartcard
ERRLOG	Display the Error Log
F	Generate a Zone Master Key Component
FC	Format a Smartcard
FICONTEST	Check the FICON host interface
FK	Form Key from Components
GC	Generate Key Component
GETCMDS	View Licensed Host Commands
GETTIME	Query the Time and Date
GK	Generate LMK Component
GS	Generate Key & Write Components to Smartcard
GZ	Generate a ZMK and Write to Smartcards
HEALTHENABLE	Suspend/Resume Health Check Counts
HEALTHSTATS	View/Reset Health Check
IK	Import Key
IV	Import a CVK or PVK
KA	Generate a CVK Pair
KB	Translate a CVK Pair from LMK to ZMK
KD	Delete KTK
KE	Export Key
KG	Generate Key
KK	Import a Key encrypted under a KTK
KM	Generate KTK Components
KN	Install KTK
KT	View KTK Table
LK	Load LMK
LO	Load "Old" LMKs into Key Change Storage
LN	Load "New" LMKs into Key Change Storage
MI	Generate a MAC on an IPB

Command	Description
TRACERT	Trace TCP/IP route
TRAP	Configure SNMP Traps
TRAPADD	Add a new SNMP Trap
TRAPDEL	Delete an SNMP Trap
UTILCFG	View/Change Instantaneous Utilization Period
UTILENABLE	Suspend/Resume Collection of Utilization Data
UTILSTATS	View/Reset Utilization Data
V	Verify LMK Store
VA	View Authorised Activities
VC	Verify the Contents of a Smartcard
VR	View Software Revision Number
VT	View LMK Tables
WK	Translate a Zone PIN Key
XA	Add a RACC to the whitelist
XD	Decommission the HSM
XE	Remove RACC from the whitelist
XH	Commission the HSM
XI	Generate Customer Trust Anchor
XK	Make an RACC left or right key
XR	Commission a smartcard
XT	Transfer existing LMK to RLMK
XX	Decommission a smartcard
XY	View HSM commissioning status
XZ	Duplicate CTA share
YA	Generate a CSCK
YB	Export a CSCK
YC	Import a CSCK
Z	Encrypt a Clear Zone Master Key Component

Further details can be found in: *1270A544 payShield 9000 Console Command Reference Manual.*

Host Commands

Command	Description
A0	Generate a Key
A4	Form a Key from Encrypted Components
A6	Import a Key
A8	Export a Key
B0	Translate Key Scheme
B2	Echo Command
B8*	TR-34 Key Export
BS	Erase the Key Change Storage
BU	Generate a Key Check Value
BW	Translate Keys from Old LMK to New LMK
BY	Translate ZMK from ZMK to LMK
CS	Modify Key Block Header
EI*	Generate a Public/Private Key Pair
EK*	Load a Private Key
EM*	Translate a Private Key
EO*	Import a Public Key
EQ*	Validate a Public Key
ES*	Validate and Import a Public Key
EU*	Translate a Public Key
GI*	Import Key under an RSA Public Key
GK*	Export Key under an RSA Public Key
HY	Import a Key encrypted under a KTK
J2	Get HSM Loading

Command	Description
J4	Get Host Command Volumes
J6	Reset Utilization Statistics
J8	Get Health Check Accumulated Counts
JI	Reset Health Check Accumulated Accounts
JK	Get Instantaneous Health Check Status
LA	Load Data to User Storage
LE	Read Data from User Storage
LG	Set HSM Response Delay
N0	Generate a Random Value
N6Φ	Bancontact Session Key Import
N8Φ	Bancontact Session Key Export
NC	Perform Diagnostics
NI	Return Network Information
NK	Command Chaining
NO	HSM Status
Q0	Translate Audit Record MAC key
Q2	Retrieve Audit Record
Q4	Archive (Print) Audit Record
Q6	Delete Audit Record
Q8	Audit Record Verification
QE*	Generate a Certificate Request
RA	Cancel Authorised Activities

***** Requires additional license HSM9-LIC002 in order to perform RSA functionality.

Φ Requires additional license HSM9-LIC007 in order to perform AES functionality.

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC002
RSA Algorithm

Overview

This license gives the user the ability to perform asymmetric cryptographic operations using the RSA algorithm. The HSM supports key sizes 320 to 2048 bits (inclusive) in 8 bit steps. Any host command that requires the use of the RSA algorithm will require this license.

This license simply enables the HSM to perform operations using the RSA algorithm – ***no additional commands are enabled***. The appropriate license(s) for the commands that support RSA must also be installed in the HSM.

Host Commands

The following commands are RSA-enabled by HSM9-LIC002:

Command	Description	Command is licensed In HSM9-...
B8	TR-34 Key Export	LIC001
EI	Generate a Public/Private Key Pair	LIC001
EK	Load a Private Key	LIC001
EM	Translate a Private Key	LIC001
EO	Import a Public Key	LIC001
EQ	Validate a Public Key	LIC001
ES	Validate a Cert and Import the Public Key	LIC001
EU	Translate a Public Key	LIC001
EW	Generate an RSA Signature	LIC008 or LIC030
EY	Validate an RSA Signature	LIC008 or LIC030
GI	Import Key under an RSA Public Key	LIC001
GK	Export Key under an RSA Public Key	LIC001
KE	Generate Issuer RSA Key set and Public Key Certificate	LIC016
KG	Validate Issuer Public Key Certificate	LIC016
KK	Validate a Certification Authority Self-Signed Certificate	LIC016
KM	Generate Static Data Authentication Signature	LIC016
KO	Generate Card RSA Key Set and Public Key Certificate	LIC016
QE	Generate a Certificate Request	LIC001

HSM9-LIC002 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC003
AS2805 Commands

Overview

This license enables the AS2805 functionality within the payShield 9000 which supports the Australian AS2805 standards, and also provides the functionality to support the Australian Payments Clearing Association (APCA) Security Control Module specifications.

NOTE: These commands do not currently support Key Block LMKs.

Console Commands

Command	Description
EA	Convert $(KEK)_{ZMK}$ into a KEKr or KEKs

Host Commands

Command	Description
C0	Generate Initial Terminal Master Keys
C2	Generate a Message Authentication Code
C4	Verify a Message Authentication Code
C6	Generate a Random Number
C8	Generate an Acquirer Master KEK
D0	Generate a PIN Pad Authentication Code
D2	Verify a PIN Pad Authentication Code
D4	Translate a PIN Block
D6	Translate an Acquirer Master KEK
D8	Encrypt a CPAT Authentication Value
E0	Generate a KEKs Validation Request
E2	Generate a KEKr Validation Response
E4	Verify a PIN Pad Proof of End Point
E6	Generate a PIN Pad Proof of Endpoint (POEP)
E8	Generate a KCA and KMACH
F0	Verify a Terminal PIN using the IBM Method
F2	Verify a Terminal PIN using the VISA Method
F4	Calculate KMACI
F6	KEKGEN
F8	KEKREC
H0	Decrypt a PIN Pad Public Key
H2	Generate a RSA Public Key Verification Code
H4	Generate a KEKs for use in Node to Node (RSA)
H6	Receive a KEKr for use in Node to Node (RSA)
H8	Encrypt a Cross Acquirer KEK under an Initial TK
I0	Encrypt a Terminal Key under the LMK
OI	Generate a Set of Zone Keys
OK	Translate a Set of Zone Keys

Command	Description
OU	Update Terminal Master Key 1
OW	Update Terminal Master Keys
P0	Verify and Generate a VISA PVV
P2	Generate a VISA PVV
P4	Generate a Proof of Host value
PI	Generate a Set of Terminal Keys
PK	Generate a PIN Pad Acquirer Security Number
PO	Translate a PIN Block
PQ	Generate a Message Authentication Code
PS	Validate a Message Authentication Code
PU	Encrypt Data
PW	Decrypt Data
QM	Data Encryption Using a Derived Privacy Key
QO	Data Decryption Using a Derived Privacy Key
QQ	Verify a PIN at Card Issuer using IBM Method
QS	Verify a PIN at Card Issuer using Diebold Method
QU	Verify a PIN at Card Issuer using Visa Method
QW	Verify a PIN at Card Issuer using Comp. Method
RE	Verify a Transaction Request, without PIN
RG	Verify a Transaction Request, with PIN (CD)
RI	Verify a Transaction Request, with PIN (no CD)
RK	Generate Transaction Response (AP by Acquirer)
RM	Generate Transaction Response (AP by Issuer)
RO	Translate a PIN from PEK to ZPK Encryption
RQ	Verify a Transaction Completion Confirmation Req
RS	Generate a Transaction Completion Response
RU	Generate Auth Para at the Card Issuer
RW	Generate an Initial Terminal Key

HSM9-LIC003 is available as an optional license for use with the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A547 payShield 9000 Australian Standards LIC003.*

HSM9-LIC004
MasterCard OBKM & CEPS

Overview

This license provides commands that enable customers to interface to MasterCard Europe (previously Europay) using the Europay Security Platform (ESP) specifications. ESP functionality provides the issuer with the following capabilities:

- Pay Now/Pay Later mag stripe production support and transaction processing
- Pay Now/Pay Later chip card transaction processing (EMV)
- Integration with EPS-Net
- Use of the On-Behalf services offered by Europay (MasterCard Europe)

NOTE: These commands do not currently support Key Block LMKs.

Host Commands

Command	Description
J0*	Generate Issuer RSA Key Set
JO*	Validate a CA Self Signed Certificate
R2	Export Electronic Purse Card Key Set
R4	Export Chip Card Key Set
R6	Export Magnetic Stripe Card Key Set
R8*	Import Transport Key Set
T0	Unlinked Load Transaction Request
T2	Release R_{LSAM}
T4	Release R_{2LSAM}
T6	Verify R_{CEP}
U0	Decrypt R_1 and validate the MAC_{LSAM}
U2	Compute H_{CEP}
U4	Validate the S_1 MAC (Load and Unload)
U6	Validate the S_1 MAC (Currency Exchange)
U8	Generate the S_2 MAC (Linked load,…)
V0	Generate the S_2 MAC (Currency Exchange)
V2	Generate the S_2 MAC (Approved Unlinked Load)
V4	Validate the S_3 MAC (Currency Ex transactions)

Command	Description
V6	Validate the S_3 MAC (Load or Unload transactions)
V8	Validate the $H2_{LSAM}$
W0	Validate S_6 MAC
W2	Validate $S_{6'}$ MAC
W4	Validate $S_{6''}$ MAC
W6	Validate $S_{5,DLT}$ MAC
W8	Validate $S_{5,ISS}$ MAC
X0	Validate the S_4 MAC – Old Terminals
X2	Validate the S_4 MAC – New Terminals
X4	Validate the S_5 MAC – Old Terminals
X6	Validate the $S_{5'}$ MAC – New Terminals
X8	Validate the S_5 Variant MAC - New Terminals
Y0	Create the Ack MAC – Old Terminals
Y2	Create the Ack MAC – New Terminals
Y4	Create the Update MAC
Y6	Validate the S_{ADMIN} MAC (Admin MAC of the PSAM)
Y8	Create the Merchant Acquirer MAC
Z0	Validate the Card Issuer MAC

* Requires additional license HSM9-LIC002 in order to perform RSA functionality.

HSM9-LIC004 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A541 payShield 9000 OBKM & CEPS Command Addendum LIC004.*

HSM9-LIC005
User Authentication (HMAC/CAP/DPA)

Overview

This license consists of host commands needed to implement authentication commands for MasterCard's Chip Authentication Program (CAP) and Visa's Dynamic Passcode Authentication (DPA) as well as MasterCard's implementation of 3-D Secure which is based on the Keyed Hash Message Authentication Code (MAC), as defined in FIPS Pub 198-1. It also provides support for the legacy Thales WatchWord token commands which are also applicable to the Thales Personal Security Module (PSM).

Host Commands

Command	Description
FU	Verify a Watchword Response
K2	Verify Truncated Application Cryptogram (CAP)
L0	Generate an HMAC Secret Key
LK	Generate a Decimal MAC
LM	Verify a Decimal MAC
LQ	Generate an HMAC on a Block of Data
LS	Verify an HMAC on a Block of Data
LU	Import an HMAC key under a ZMK
LW	Export an HMAC key under a ZMK
LY	Translate a HMAC Key

HSM9-LIC005 is included in the following package:

- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC006
X9 TR-31 Key Block

Overview

This license enables the use of the Accredited Standards Committee (ASC) X9 TR-31 key block technique for key exchange, which is recognized as the long term replacement for the legacy ANSI X9.17 standard. Existing commands are extended to provide functionality to import and export keys in TR-31 format.

Console Commands

Command	Description
KG	Generate Key
IK	Import Key
KE	Export Key

Further details can be found in: *1270A544 payShield 9000 Console Reference Manual.*

Host Commands

Command	Description
A0	Generate a Key
A6	Import a Key
A8	Export a Key
BY	Translate ZMK from ZMK to LMK Encryption

HSM9-LIC006 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC007 AES Algorithm

Overview

Note: As of software release v3.2a, the HSM will support the generation/installation of AES Key Block LMKs regardless of whether HSM9-LIC007 is installed. However, the use of AES working keys still requires this license.

This license gives the user the ability to perform cryptographic operations using the AES algorithm. With this license installed, the HSM supports AES working keys of the following size: 128, 192 and 256 bits.

When using an AES LMK, only commands that use Thales Key Blocks will be available. Additionally, only a subset of those commands allows the use of AES working keys. See the table below for a list of these two sets of commands.

This license simply enables the HSM to perform AES operations – ***no additional commands are enabled by this license***.

Host Commands

With HSM9-LIC007 installed, the following commands will process Thales Key Blocks protected by an AES LMK:

Interface	Commands
Host	**A0, A2, A4, A6, A8, BA, BC, BE, BG, BK, BM, BQ, BS, BU, BW, BY, CA, CC, CE, CG, CI, CK, CM, CO, CQ, CS, CU, CW, CY, DA, DC, DE, DG, DU, EA, EC, EE, EG, EI, EK, EM, EO, EQ, ES, EU, EW, EY, FU, FW, G0, GA, GI, GK, GO, GQ, GS, GU, GW, JA, JC, JE, JG, K0, K2, KQ, KS, KU, KW, KY, L0, LA, LC, LE, LK, LM, LO, LQ, LS, LU, LW, LY, M0, M2, M4, M6, M8, MY, NE, NG, OA, PE, PG, PM, Q0, Q2, Q4, Q6, Q8, QA, QC, RA, RC, RC, RI, RK, RM, RO, RQ, RS, RU, RW, RY**
Console	**KG, FK, CK, IK, KE, GC, EC, CV, GS, PV, ED, MI, TD, R**

With HSM9-LIC007 installed, the following commands are able to process Thales Key Blocks containing an AES key:

Interface	Commands
Host	**A0, A2, A4, A6, A8, M0, M2, M4, M6, M8, MY**
Console	**KG, FK, CK, IK, KE, GC, EC, GS**

HSM9-LIC007 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual* and *1270A544 payShield 9000 Console Reference Manual.*

HSM9-LIC008
Data Protection

Overview

This functionality is to allow customers to protect messages that go to/from a remote device, typically an ATM or POS device. It also provides protection of selected data for local storage supporting requirements 3 and 4 of the PCI DSS standard. Its main purpose is to provide confidentiality (encryption) and integrity (message authentication) for potentially sensitive information. Until now all such data would typically have been in cleartext format in the message. The customer will have the option to make additional calls to the HSM to perform the encryption/authentication of the selected text prior to populating the text in the normal command.

Host Commands

Command	Description
EW*	Generate an RSA Signature
EY*	Validate an RSA Signature
GM	Hash a Block of Data
M0°	Encrypt Data Block
M2°π	Decrypt Data Block
M4°	Translate Data Block
M6°	Generate a MAC
M8°	Verify a MAC
MY°	Verify & Translate a MAC

***** Requires additional license HSM9-LIC002 in order to perform RSA functionality.

° Requires additional license HSM9-LIC007 in order to perform AES functionality.

π Requires additional license HSM9-LIC038 in order to perform Ingenico BPS (FPE) functionality.

HSM9-LIC008 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC011 Magnetic Stripe Contactless Card Data Preparation

Overview

Issuing the new contactless magnetic stripe based cards, such as MasterCard's PayPass and Visa's payWave, requires additional keys and data for personalization of the information for the contactless interface. Issuers can create this data, in addition to the current standard magnetic stripe data, or depend on a Personalization Bureau for creation of the additional keys and data. From a key management and security perspective, there is a clear advantage for an Issuer to create this data in order to maintain full control over security of the keys and the overall data preparation process.

Please note that this license is specifically for issuers of magnetic stripe contactless cards (mainly in the US) not the EMV-based contactless cards that are prevalent in Europe and Asia Pacific.

Host Commands

Command	Description
K8	Export a Key under a KEK
KI	Derive Card Unique DES Keys
NY	Generate IVCVC3 and Static CVC3

HSM9-LIC011 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A548 payShield 9000 Card & Mobile Issuance Manual.*

HSM9-LIC012
LMK x 2

Overview

With this license, customers can install two independent LMKs inside one payShield 9000 HSM. The two LMKs can consist of any combination of "Variant" (or traditional) LMKs and "Key Block" LMKs.

Each LMK is administered separately (using the traditional LMK processes), and allows complete cryptographic separation of the key material encrypted under the LMKs.

This license simply allows up to two LMKs to be installed in the HSM – no additional commands are added.

HSM9-LIC012 is available as an optional license for use with any package.

Further details can be found in: *1270A544 payShield 9000 General Information Manual.*

HSM9-LIC013
LMK x 5

Overview

With this license, customers can install five independent LMKs inside one payShield 9000 HSM. The five LMKs can consist of any combination of "Variant" (or traditional) LMKs and "Key Block" LMKs.

Each LMK is administered separately (using the traditional LMK processes), and allows complete cryptographic separation of the key material encrypted under the LMKs.

This license simply allows up to five LMKs to be installed in the HSM – no additional commands are added.

HSM9-LIC013 is available as an optional license for use with any package.

Further details can be found in: *1270A544 payShield 9000 General Information Manual.*

HSM9-LIC014 WebPIN Commands

Overview

WebPIN is a separate Thales application (which needs to be ordered separately) which uses the payShield 9000 HSM to provide strong security primarily for internet banking. Any payShield 9000 to be used with the WebPIN external application needs to have the WebPIN license enabled. This license supports a range of host commands relating to PIN block management, message authentication and message encryption specifically designed for WebPIN, which are not available in other license modules.

NOTE: These commands do not support Key Block LMKs.

Host Commands

Command	Description
XK	Verify and return new encrypted PIN
XM	Verify ISO PIN Block from Internet
XO	Verify MAC
XQ	Generate MAC
XS	Translate ISO PIN Block
XU	Decrypt Data
XW	Encrypt Data
ZA	Generate a Random Alphanumeric PIN
ZE	Print Alphanumeric PIN/Solicitation Data
ZK	Translate an Alphanumeric PIN
ZM	Translate PIN to Alphanumeric PIN
ZU	Verify PIN Block

HSM9-LIC014 is available as an optional license for use with the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A592 payShield 9000 Host Command Addendum LIC014.*

HSM9-LIC016
Key & Data Prep for Cards & Mobile

Overview

This license is designed for card issuers of EMV cards who require a secure method to create the cryptographic data as part of their host card management system rather than using an external package such as Thales P3. The commands enable their card issuing application to securely generate the full complement of data required for issuing American Express, Discover, MasterCard or Visa chip cards.

Host Commands

Command	Description
IK	EMV Sign Data
IM	EMV Recover Data
K8	Export a Key under a KEK
KE*	Generate Issuer RSA Key Set and Public Key Certificate
KG*	Validate an Issuer Public Key Certificate
KI	Derive Card Unique DES Keys
KK*ø	Validate a Certification Authority Self-Signed Certificate
KM*	Generate Static Data Authentication (SDA) Signature
KO*	Generate Card RSA Key Set and Public Key Certificate
L6	Import an RSA Private Key
L8	Export an RSA Private Key

***** Requires additional license HSM9-LIC002 in order to perform RSA functionality.

HSM9-LIC016 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A548 payShield 9000 Card & Mobile Issuance Manual.*

HSM9-LIC017
HE and HG Host Commands

Overview

This license is provides access to the HE and HG commands found in earlier Thales payment HSMs. These commands have been superseded by M0 and M2 commands, and ***should only be used where backwards compatibility with older HSMs and applications is required***.

NOTE: These commands do not currently support Key Block LMKs.

Host Commands

Command	Description
HE	Encrypt Data
HG	Decrypt Data

HSM9-LIC017 is available as an optional license for use with the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A589 payShield 9000 Host Command Addendum LIC017.*

HSM9-LIC018 Card Personalization & Mobile Provisioning

Overview

This license is designed for two types of users:

- issuers of EMV cards who require a secure method to personalize cards as part of their card issuance process based on EMV Common Personalization Specification (CPS) and Global Platform (GP) using Secure Channel Protocol 2 (SCP02). Only the Indirect/Explicit methods are supported. There is support for the specific process required for MasterCard PayPass Magnetic Stripe Cards.
- issuers of mobile payment applications, who require a secure method to provision the MPA (mobile phone application) onto the phone using OTA communication, using the Host Card Emulation (HCE) or Secure Element (SE) protocols.

Host Commands

Command	Description
IC	Generate Static Data Authentication Signature
IE	Prepare Secure Message for Chip Card
II	Verify and Decrypt Response Secure Message from Chip Card
IO	Generate Remote Management Session ID & Session Keys
IQ	Validate Authentication Code
IU	Generate Remote Management Secure Message
IW	Validate & Recover Remote Management Secure Message from the MPA
IY	Generate Digitized Card Single Use Keys
JW	JWT Encode
JY	JWT Decode

HSM9-LIC018 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A548 payShield 9000 Card & Mobile Issuance Manual.*

HSM9-LIC019 Pre-master Secret Decryption (TLS/SSL handshake)

Overview

As part of the TLS or SSL handshake process, the client generates a Pre-Master Secret which will be used by both client and server to calculate the Master Secret, from which both parties compute the symmetric keys used to protect the data to be transferred.

This license was developed for use in a 3-D Secure environment to support establishment of the TLS/SSL connection. It allows the HSM to decrypt the Pre-Master Secret generated by the host's communication partner (i.e. by the TLS/SSL client).

The HSM generates a Type 4 RSA key pair. The public key is passed to the host's communication partner which generates the Pre-master Secret and encrypts it using the public key. The pre-master Secret is then sent to the HSM's host (the TLS/SSL server), and the HSM decrypts the Pre-master Secret using the private key.

Although this capability was designed specifically for TLS/SSL Pre-master secret, it can be used for any data and so enables the payShield 9000 to be used to decrypt data encrypted under an RSA public key.

***NOTE**: this license does not relate to the use of TLS/SSL to secure the communications link between a payShield 9000 and the host computer. For that purpose, HSM9-LIC036 is appropriate.*

Host Commands

This license does not introduce any additional commands, but extends the capabilities of existing commands.

The EI command (for generation of RSA key pairs) is extended to allow generation of Type 4 RSA keys, which are required for this process.

The GI command (Import key encrypted under an RSA public key) can be used to decrypt the data (encrypted using the Type 4 RSA public key) using a Type 4 RSA private key.

HSM9-LIC019 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC020
Korean SEED Commands

Overview

This license enables a set of commands that provide cryptographic functionality using the Korean SEED algorithm.

NOTE: These commands do not currently support Key Block LMKs.

Host Commands

Command	Description
AI	Encrypt Data Block with SEED algorithm
AK	Decrypt Data Block with SEED algorithm
AM	Translate Data Block with SEED algorithm
AO	Generate Round Key from SEED algorithm
G2	Verify an Interchange PIN using the comparison method with SEED encryption algorithm
G4	Verify a Terminal PIN using the comparison method with SEED encryption algorithm
G6	Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm
G8	Translate a PIN from TPK to ZPK with SEED encryption algorithm

HSM9-LIC020 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A590 payShield 9000 Host Command Addendum LIC020.*

HSM9-LIC021
LMK x 10

Overview

With this license, customers can install up to ten independent LMKs inside one payShield 9000 HSM. The ten LMKs can consist of any combination of "Variant" (or traditional) LMKs and "Key Block" LMKs.

Each LMK is administered separately (using the traditional LMK processes), and allows complete cryptographic separation of the key material encrypted under the LMKs.

This license simply allows up to ten LMKs to be installed in the HSM – no additional commands are added.

HSM9-LIC021 is available as an optional license for use with any package.

Further details can be found in: *1270A544 payShield 9000 General Information Manual.*

HSM9-LIC022
LMK x 20

Overview

With this license, customers can install up to 20 independent LMKs inside one payShield 9000 HSM. The ten LMKs can consist of any combination of "Variant" (or traditional) LMKs and "Key Block" LMKs.

Each LMK is administered separately (using the traditional LMK processes), and allows complete cryptographic separation of the key material encrypted under the LMKs.

This license simply allows up to ten LMKs to be installed in the HSM – no additional commands are added.

HSM9-LIC022 is available as an optional license for use with any package.

Further details can be found in: *1270A544 payShield 9000 General Information Manual.*

HSM9-LIC023
MULTOS Card Data Preparation

Overview

This license is designed for card issuers of EMV cards who require a secure method to build MULTOS Application Load Units (ALU) and the associated data required for personalization of MULTOS cards, including step/one, based on the processes defined in the MULTOS documents "Guide to Generating Application Load Units" and "MULTOS step/one Off-Card Specification".

NOTE: These commands do not currently support Key Block LMKs.

Host Commands

Command	Description
I2	Import MULTOS Transport Key Certifying Key
I4	Import MULTOS Hash Modulus Key
I6	Translate MULTOS KTU
I8	MULTOS ALU Generator – provides following sub-commands:
	MULTOS ALU Generator – Allocate ALU Area
	MULTOS ALU Generator – Load Block
	MULTOS ALU Generator – Load Clear Data
	MULTOS ALU Generator – Load Cipher Data
	MULTOS ALU Generator – Generate Checksum
	MULTOS ALU Generator – Encrypt Area
	MULTOS ALU Generator – Generate Signature
	MULTOS ALU Generator – Generate KTU
	MULTOS ALU Generator – Return ALU
	MULTOS ALU Generator – Release ALU

HSM9-LIC023 is included in the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A548 payShield 9000 Contactless & EMV Issuing Manual.*

HSM9-LIC024
Magnetic Stripe Issuing

Overview

This license will be used both by issuers of magnetic stripe cards or issuers of EMV cards (who need to create a magnetic stripe image to load onto the chip card and to program the magnetic stripe).

Host Commands

Command	Description
BA	Encrypt a Clear PIN
BG	Translate a PIN and PIN Length
BK	Generate an IBM Offset (customer selected PIN)
BM	Load the Excluded PIN Table
CE	Generate a Diebold PIN Offset
CW	Generate a Card Verification Code/Value
DE	Generate an IBM PIN Offset (LMK enc'd PIN)
DG	Generate a VISA PVV (LMK enc'd PIN)
EE	Derive a PIN Using the IBM Method
FW	Generate a VISA PVV (customer selected PIN)
GA	Derive a PIN Using the Diebold Method

Command	Description
JA	Generate a Random PIN
JG	Translate a PIN from LMK to ZPK Encryption
LC	Verify the Diebold Table in User Storage
LO	Translate Decimalization Table
NG	Decrypt an Encrypted PIN
PG	Verify PIN/Solicitation Mailer
QA	Load Solicitation Data to User Storage
QC	Final Load of Solicitation Data to User Storage
QK *	Translate Account No. for LMK-encrypted PIN
RC	Verify Solicitation Mailer
RY	Calculate/Verify CSC & Manage CSCK

HSM9-LIC024 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC025
Magnetic Stripe Transaction Processing

Overview

This license will be used by any organization (for example a financial institution, switch, card scheme or third party processor) who is involved in merchant acquiring and/or authorization of magnetic stripe card transactions from ATM or POS terminals.

Host Commands

Command	Description
AQ	Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN
BA	Encrypt a Clear PIN
BC	Verify a Terminal PIN (Comparison Method)
BE	Verify an Interchange PIN (Comparison Method)
BG	Translate a PIN and PIN Length
BQ	Translate PIN Algorithm
CA	Translate PIN from TPK to ZPK
CC	Translate PIN from One ZPK to Another
CG	Verify a Terminal PIN Using the Diebold Method
CI	Translate a PIN from BDK to ZPK Encryption
CK	Verify a PIN (IBM Method, DUKPT)
CM	Verify a PIN (VISA Method, DUKPT)
CO	Verify a PIN (Diebold Method, DUKPT)
CQ	Verify a PIN (Encrypted Method, DUKPT)
CU	Verify & Generate a VISA PVV
CY	Verify a Card Verification Code/Value
DA	Verify a Terminal PIN (IBM Method)
DC	Verify a Terminal PIN (VISA Method)
DU	Verify & Generate an IBM PIN Offset
EA	Verify an Interchange PIN (IBM Method)
EC	Verify an Interchange PIN (VISA Method)
EG	Verify an Interchange PIN (Diebold Method)
G0	Translate a PIN from BDK to ZPK (DUKPT)
GO	Verify a PIN (IBM Method, 3DES/AES DUKPT)
GQ	Verify a PIN (VISA Method, 3DES/AES DUKPT)
GS	Verify a PIN (Diebold Method, 3DES/AES DUKPT)
GU	Verify a PIN (Encrypted Method, 3DES/AES DUKPT)
GW	Generate/Verify MAC (3DES/AES DUKPT)
HI Φ	Transaction Request With PIN (T/AQ Key)
HI *	Verify a Transaction Request, with PIN, when CD Field not Available
HK Φ	Transaction Request Without PIN
HK *	Generate Transaction Response, with Auth Para Generated by Acquirer
HM Φ	Administration Request Message

Command	Description
HM *	Generate Transaction Response with Auth Para Generated by Card Issuer
HO Φ	Transaction Response w/ Auth Para from Issuer
HO *	Translate a PIN from PEK to ZPK Encryption
HQ Φ	Generate Auth Para & Transaction Response
HQ *	Verify a Transaction Completion Confirmation
HS Φ	Verify MAC on Confirmation Message
HS *	Generate a Transaction Completion Response
HU Φ	Transaction Request With a PIN (T/CI Key)
HW Φ	Translate KEYVAL
JC	Translate a PIN from TPK to LMK
JE	Translate a PIN from ZPK to LMK
JG	Translate a PIN from LMK to ZPK
LC	Verify the Diebold Table in User Storage
LO	Translate Decimalization Table
PM	Verify a Dynamic CVV/CVC
P6	Store OPINPad to HSM memory
P8	Decode OPIN and translate to ZPK
QY	Generate a Visa Dynamic CVV
RI *	Transaction Request With PIN (T/AQ Key)
RI Φ	Verify a Transaction Request, with PIN, when CD Field not Available
RK *	Transaction Request Without PIN
RK Φ	Generate Transaction Response, with Auth Para Generated by Acquirer
RM *	Administration Request Message
RM Φ	Generate Transaction Response with Auth Para Generated by Card Issuer
RO *	Transaction Response w/ Auth Para from Issuer
RO Φ	Translate a PIN from PEK to ZPK Encryption
RQ *	Generate Auth Para & Transaction Response
RQ Φ	Verify a Transaction Completion Confirmation
RS *	Verify MAC on Confirmation Message
RS Φ	Generate a Transaction Completion Response
RU	Transaction Request With PIN (T/CI Key)
RW	Translate KEYVAL
RY	Verify Card Security Codes

***** These meanings of the command apply if the security setting *Transaction key scheme* is set to "Racal"

Φ These meanings of the command apply if the security setting *Transaction key scheme* is set to "Australian"

HSM9-LIC025 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC026
EMV Transaction Processing

Overview

This license will be used by any organization (for example a financial institution, switch, card scheme or third party processor) who is involved in merchant acquiring and/or authorization of EMV chip card transactions from ATM or POS terminals.

Host Commands

Command	Description
K0	Decrypt Encrypted Counters
KQ	ARQC/ARPC Processing (EMV 3.x)
KS	Data Auth Code & Dynamic No. Ver (EMV 3.x)
KU	Generate Secure Message (EMV 3.x)
KW	ARQC/ARPC Processing (EMV 4.x)
KY	Generate Secure Message (EMV 4.x)

HSM9-LIC026 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC027
PIN and Key Printing

Overview

This license is applicable to card issuers, ATM/POS network providers and third party bureaus that need to support various commands relating to PIN and key mailers.

Host Commands

Command	Description
A2	Generate & Print a Component
LI	Load a PIN Text String
NE	Generate & Print a Key as Split Components
OA	Print a PIN Solicitation Mailer
OC	Generate & Print a ZMK Component
OE	Generate & Print a TMP, TPK or PVK
PA	Load Formatting Data
PC	Load Additional Formatting Data
PE	Print PIN/Solicitation Data
TA	Print TMK Mailer

HSM9-LIC027 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC028
VISA Cash Processing

Overview

This license gives the user the ability to perform the functions necessary to process transactions related to the VISA-cash electronic purse scheme.

NOTE: These commands do not support Key Block LMKs.

Host Commands

Command	Description
DM	Verify Load Sig S1 & Generate Load Sig S2
DO	Verify Load Completion Sig S3
DQ	Verify Unload Sig S1 & Generate Unload Sig S2
DS	Verify Unload Completion Sig S3

HSM9-LIC028 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC029 Legacy Commands

Overview

This license contains a series of miscellaneous commands that have been present in the various Thales HSMs over the past 20 years, but which are now considered redundant because the equivalent functionality is available in the new base license (HSM9-LIC001). This license is made available for backward compatibility reasons, but customers are urged to migrate to the new commands in the base license if they have a dependency on any command contained in the 'legacy commands' license.

NOTE: Some of these commands do not support Key Block LMKs.

Host Commands

Command	Description
AA	Translate a TMK/TPK/PVK
AC	Translate a TAK
AE	Export a TMK/TPK/PVK
AG	Export a TAK
AS	Generate a CVK Pair
AU	Export a CVK Pair
AW	Import a CVK Pair
AY	Translate a CVK Pair
BI	Generate a BDK
DI	Generate & Export a KML
DK	Import a KML
DW	Import a BDK
DY	Export a BDK
FA	Import a ZPK
FC	Import a TMK/TPK/PVK
FE	Export a TMK/TPK/PVK
FG	Generate a PVK Pair
FI	Generate a ZEK/ZAK
FK	Import a ZEK/ZAK
FM	Export a ZEK/ZAK
FO	Generate a Watchword Key
FQ	Export Watchword Key

Command	Description
FS	Import Watchword Key
GC	Export a ZPK
GE	Translate a ZMK
GG	Form a ZMK from 3 Components
GY	Form a ZMK from 2 to 9 Components
HA	Generate a TAK
HC	Generate a TMK/TPK/PVK
IA	Generate a ZPK
KA	Generate a Key Check Value
KC	Translate a ZPK
MA	Generate a MAC
MC	Verify a MAC
ME	Verify & Translate a MAC
MG	Export a TAK
MI	Import a TAK
MK	Generate a Binary MAC
MM	Verify a Binary MAC
MO	Verify & Translate a Binary MAC
MQ	Generate MAC for Large Message
MS	Generate MAC (X9.19) for Large Message
RY	Generate/Export/Import a CSCK

HSM9-LIC029 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details, including whether Key Block LMKs are supported, can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC030
Miscellaneous HSM 8000 Commands

Overview

This license was created to ensure that all host commands that existed on the HSM 8000 could be made available to payShield 9000 users.

Note that HSM9-LIC030 is included in HSM9-PAC301 and HSM9-PAC303, and is not available for purchase and so cannot be added to other packages. All of the commands in HSM9-LIC030 are also available in other licenses (as indicated in the table below).

Host Commands

Command	Description	Command also in:
EW*	Generate an RSA Signature	HSM9-LIC008
EY*	Validate an RSA Signature	HSM9-LIC008
FU	Verify a Watchword Response	HSM9-LIC005
GM	Hash a Block of Data	HSM9-LIC008
LK	Generate a Decimal MAC	HSM9-LIC005
LM	Verify a Decimal MAC	HSM9-LIC005
M6°	Generate a MAC	HSM9-LIC008
M8°	Verify a MAC	HSM9-LIC008
MY°	Verify & Translate a MAC	HSM9-LIC008

***** Requires additional license HSM9-LIC002 in order to perform RSA functionality.

° Requires additional license HSM9-LIC007 in order to perform AES functionality.

HSM9-LIC030 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC031 UnionPay Commands

Overview

This license has been created to enable transactions from cards belonging to the UnionPay card scheme to be processed. (UnionPay was originally referred to as China UnionPay, or CUP.)

NOTE: These commands do not support Key Block LMKs.

Host Commands

Command	Description
JS	ARQC Verification and/or ARPC Generation (CUP)
JU	Generate Secure Message with Integrity and optional Confidentiality for Message or Offline PIN Change (CUP)

HSM9-LIC031 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details, including whether Key Block LMKs are supported, can be found in: *1270A591 payShield 9000 Host Command Addendum LIC031.*

HSM9-LIC033
RSA Performance Booster

Overview

This license has now been removed and is no longer used. The standard RSA license (HSM9-LIC002) now includes this performance booster as standard.

HSM9-LIC034
MU and MW Host Commands

Overview

This license is provides access to the MU and MW host commands found in earlier Thales payment HSMs. These commands have been superseded by M6 and M8 commands, and ***should only be used where backwards compatibility with older HSMs and applications is required***.

NOTE: These commands do not currently support Key Block LMKs.

Host Commands

Command	Description
MU	Generate MAC on Binary Message
MW	Verify MAC on Binary Message

HSM9-LIC034 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC303 Premium Package

Further details can be found in: *1270A614 payShield 9000 Host Command Addendum LIC034.*

HSM9-LIC036
Secure Host Communications

Overview

This license enables the use of TLS or SSL to protect the Ethernet communications link between the payShield 9000 and its host computer. It replaces license HSM9-LIC035, which has been withdrawn.

No additional console or host commands are enabled by this license, but any settings relating to Secure Host Communications will not have any effect unless this license is in place.

HSM9-LIC036 is included in the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A544 payShield 9000 Console Reference Manual* and *1270A593 payShield 9000 General Information Manual.*

HSM9-LIC037
Remote payShield Manager

Overview

This functionality is to allow customers with a payShield 9000 to have the HSM remotely managed using *payShield Manager*. This license does not provide any additional host commands.

Note that in previous versions of payShield 9000 software, HSM9-LIC009 was used to enable the remote management capability using Remote HSM Manager. HSM9-LIC009 is not available for payShield 9000 software v3, and has been replaced by HSM9-LIC037.

HSM9-LIC037 is available as an optional license for use with any standard package.

Further details can be found in: *1270A645 payShield 9000 payShield Manager User Guide.*

HSM9-LIC038
Ingenico BPS (FPE) Algorithm

Overview

This license gives the user the ability to perform cryptographic operations using the Ingenico BPS Format Preserving Encryption (FPE) algorithm.

Host command 'M2' (Decrypt Data Block) is currently the only command that supports the use of this license, and it is restricted to using a 3DES key.

This license simply enables the HSM to perform operations using the Ingenico BPS (FPE) algorithm– ***no additional commands are enabled***. The appropriate license(s) for the commands that support Ingenico BPS (FPE) must also be installed in the HSM.

Host Commands

The following commands are Ingenico BPS (FPE)-enabled by HSM9-LIC038:

Command	Description	Command is licensed In HSM9-...
M2	Decrypt Data Block	LIC008

HSM9-LIC038 is available as an optional license for use with the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC039
Visa DSP Support

Overview

This license gives authorized Visa DSP (Data Secure Platform) users access to specific functionality to provide data encryption/decryption using Visa Standard Encryption and Visa Format Preserving Encryption.

Note: Customers using HSM9-LIC039 must have and maintain a valid, binding and enforceable service agreement with Visa that gives them the right to use the Visa Data Secure Platform (DSP) technology, including Visa's Format Preserving Encryption (FPE) technology.

Host Commands

The following commands are DSP-enabled by HSM9-LIC039:

Command	Description	Command is licensed In HSM9-...
M0	Encrypt Data Block	LIC008
M2	Decrypt Data Block	LIC008
M4	Translate Data Block	LIC008

HSM9-LIC039 is available as an optional license for use with the following packages:

- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

HSM9-LIC041
NIST FF1 Support

Overview

This license gives users access to specific functionality to provide format preserving encryption/decryption using the NIST approved FF1 algorithm.

Host Commands

The following commands are FF1-enabled by HSM9-LIC041:

Command	Description	Command is licensed In HSM9-...
M0	Encrypt Data Block	LIC008
M2	Decrypt Data Block	LIC008
M4	Translate Data Block	LIC008

HSM9-LIC041 is available as an optional license for use with the following packages:

- HSM9-PAC301 Standard Base Package
- HSM9-PAC302 Card & Mobile Issuing Package
- HSM9-PAC303 Premium Package
- HSM9-PAC908 mPOS P2PE Software Package

Further details can be found in: *1270A546 payShield 9000 Host Command Reference Manual.*

THALES

www.thales-esecurity.com

About Thales e-Security

Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United Kingdom and United States. For more information, visit www.thales-esecurity.com

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com