Complete list of Thales HSM commands

List of Thales HSM commands with their description.

Host Command (Response)	Function	Supported by BP-HSM	Note
A0 (A1)	Generate a Key	X	
A2 (A3, AZ)	Generate and Print a Component		Printer handling
A4 (A5)	Form a Key from Encrypted Components	X	
A6 (A7)	Import a Key	X	
A8 (A9)	Export a Key	X	
AA (AB)	Translate a TMK, TPK or PVK		
AC (AD)	Translate a TAK		
AE (AF)	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	X	
AG (AH)	Translate a TAK from LMK to TMK Encryption	X	
AS (AT)	Generate a CVK Pair		
AU (AV)	Translate a CVK Pair from LMK to ZMK Encryption	X	
AW (AX)	Translate a CVK Pair from ZMK to LMK Encryption		
AY (AZ)	Translate a CVK Pair from Old LMK to New LMK Encryption		
B0 (B1)	Translate Key Scheme	X	
B2 (B3)	Echo Command	X	
BA (BB)	Encrypt a Clear PIN	X	
BC (BD)	Verify a Terminal PIN Using the Comparison Method	X	
BE (BF)	Verify an Interchange PIN Using the Comparison Method	X	
BG (BH)	Translate a PIN and PIN Length		Missing KEY CHANGE STORAGE
BI (BJ)	Generate a BDK	X	
BK (BL)	Generate an IBM PIN Offset (of a customer selected PIN)	X	
BM (BN)	Load the Excluded PIN Table		
BQ (BR)	Translate PIN Algorithm		

BS (BT)	Erase the Key Change Storage		
BU (BV)	Generate a Key Check Value	X	
BW (BX)	Translate Keys from Old LMK to New LMK		
BY (BZ)	Translate ZMK from ZMK to LMK encryption		
C0 (C1)	Generate Initial Terminal Master Keys (AS2805)	X	
C2 (C3)	Generate a MAC (Message Authentication Code, large messages) (AS2805)	X	
C4 (C5)	Verify MAC (Message Authentication Code, large messages) (AS2805)	X	
C6 (C7)	Generate a Random Number (AS2805)	X	Term
C8 (C9)	Generate an Acquirer Master Key Encrypting Key (AS2805)		
CA (CB)	Translate a PIN from TPK to ZPK Encryption	X	
CC (CD)	Translate a PIN from One ZPK to Another	X	
CE (CF)	Generate a Diebold PIN Offset		
CG (CH)	Verify a Terminal PIN Using the Diebold Method	X	Custom Code
CI (CJ)	Translate a PIN from BDK to ZPK Encryption (DUKPT)	X	
CK (CL)	Verify a PIN Using the IBM Method (DUKPT)		
CM (CN)	Verify a PIN Using the VISA PVV Method (DUKPT)	X	
CO (CP)	Verify a PIN Using the Diebold Method (DUKPT)		
CQ (CR)	Verify a PIN Using the Encrypted PIN Method (DUKPT)		
CU (CV)	Verify & Generate a VISA PVV (of a customer selected PIN)	X	
CW (CX)	Generate a Card Verification Code/Value	X	
CY (CZ)	Verify a Card Verification Code/Value	X	
D0 (D1)	Generate a PIN Pad Authentication Code (AS2805)	X	Term
D2 (D3)	Verify a PIN pad Authentication code (AS2805)	X	Term
D4 (D5)	Translate a PIN Block to Encryption under a PIN Encryption Key (AS2805)		Term
D6 (D7)	Translate an Acquirer Master Key Encrypting Key (AS2805)		Term
D8 (D9)	Encrypt a CPAT Authentication Value (AS2805)		Term
DA (DB)	Verify a Terminal PIN Using the IBM Method		
DC (DD)	Verify a Terminal PIN Using the VISA Method	X	
DE (DF)	Generate an IBM PIN Offset (of an LMK encrypted PIN)	X	
DG (DH)	Generate a VISA PIN Verification Value (of an LMK encrypted PIN)	X	
DI (DJ)	Generate and Export a KML		
DK (DL)	Import a KML		
DM (DN)	Verify Load Signature S1 and Generate Load Signature S2		
DO (DP)	Verify Load Completion Signature S3		
DQ (DR)	Verify Unload Signature S1 and Generate Unload Signature S2		
DS (DT)	Verify Unload Completion Signature S3		
DU (DV)	Verify & Generate an IBM PIN Offset (of customer selected new PIN)		
DW (DX)	Translate a BDK from ZMK to LMK Encryption	X	

BP-Processing

BP-Sim

BP-Tools

DY (DZ)	Translate a BDK from LMK to ZMK Encryption	X	
E0 (E1)	Generate a KEKs Validation Request (AS2805)	X	
E2 (E3)	Generate a KEKr Validation Response (AS2805)	X	
E4 (E5)	Verify a PIN Pad Proof of End Point (POEP) (AS2805)	X	Term
E6 (E7)	Generate a PIN Pad Proof of Endpoint (AS2805)		
E8 (E9)	Generate a KCA and KMACH (AS2805)		Term
EA (EB)	Verify an Interchange PIN Using the IBM Method	X	
EC (ED)	Verify an Interchange PIN Using the VISA Method	X	
EE (EF)	Derive a PIN Using the IBM Method	X	
EG (EH)	Verify an Interchange PIN Using the Diebold Method	X	Custom Code
EI (EJ)	Generate an RSA Key Set	X	
EK (EL)	Load an RSA Secret Key	X	
EM (EN)	Translate an RSA Secret Key		
EO (EP)	Import a Public Key (Generate a MAC on an RSA Public Key)	X	
EQ (ER)	Validate a Public Key (Verify a MAC on an RSA Public Key)	X	
ES (ET)	Validate a Certificate and Generate a MAC on its RSA Public Key		
EU (EV)	Translate a MAC on an RSA Public Key		
EW (EX)	Generate an RSA Signature	X	
EY (EZ)	Validate an RSA Signature	X	
F0 (F1)	Verify a Terminal PIN using the IBM Method (AS2805)		Term
F2 (F3)	Verify a Terminal PIN using the VISA Method (AS2805)		Term
F4 (F5)	Calculate KMACI		Term
F6 (F7)	KEKGEN (AS2805)		
F8 (F9)	KEKREC (AS2805)		
FA (FB)	Translate a ZPK from ZMK to LMK Encryption	X	
FC (FD)	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	X	
FE (FF)	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	X	
FG (FH)	Generate a Pair of PVKs	X	
FI (FJ)	Generate ZEK/ZAK	X	
FK (FL)	Translate a ZEK/ZAK from ZMK to LMK Encryption	X	
FM (FN)	Translate a ZEK/ZAK from LMK to ZMK Encryption	X	
FO (FP)	Generate a Watchword Key		
FQ (FR)	Translate a Watchword Key from LMK to ZMK Encryption	X	
FS (FT)	Translate a Watchword Key from ZMK to LMK Encryption	X	
FU (FV)	Verify a Watchword Response		
FW (FX)	Generate a VISA PIN Verification Value (of a customer selected PIN)	X	
G0 (G1)	Translate a PIN from BDK to ZPK Encryption (3DES DUKPT)	X	
GA (GB)	Derive a PIN Using the Diebold Method		

GC (GD)	Translate a ZPK from LMK to ZMK Encryption	X	
GE (GF)	Translate a ZMK		
GG (GH)	Form a ZMK from Three ZMK Components		
GI (GJ)	Import Key under an RSA Public Key	X	
GK (GL)	Export Key under an RSA Public Key	X	
GM (GN)	Hash a Block of Data	X	
GO (GP)	Verify a PIN Using the IBM Method (3DES DUKPT)	X	
GQ (GR)	Verify a PIN Using the VISA PVV Method (3DES DUKPT)	X	
GS (GT)	Verify a PIN Using the Diebold Method (3DES DUKPT)	-	
GU (GV)	Verify a PIN Using the Encrypted PIN Method (3DES DUKPT)	X	Custom Code
GW (GX)	Generate/Verify a MAC (3DES DUKPT)	X	
GY (GZ)	Form a ZMK from 2 to 9 ZMK Components	X	
H0 (H1)	Decrypt a PIN Pad Public Key (AS2805)		Term
H2 (H3)	Generate a RSA Public Key Verification Code (AS2805)		
H4 (H5)	Generate a KEKs for use in Node to Node interchange using RSA (AS2805)		
H6 (H7)	Receive a KEKr for use in Node to Node interchange using RSA (AS2805)		
H8 (H9)	Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key (AS2805)		Term
HA (HB)	Generate a TAK	X	
HC (HD)	Generate a TMK, TPK or PVK	X	
I0 (I1)	Encrypt a Terminal Key under the Local Master Key (AS2805)		Term
I2 (I3)	Import MULTOS Transport Key Certifying Key		EMV Issuing
I4 (I5)	Import MULTOS Hash Modulus Key		EMV Issuing
I6 (I7)	Translate MULTOS KTU		EMV Issuing
I8 (I9)	MULTOS ALU Generator		EMV Issuing
IA (IB)	Generate a ZPK	X	
IC (ID)	Establish Secure Session with Chip Card		EMV Issuing
IE (IF)	Prepare Secure Message for Chip Card		EMV Issuing
JA (JB)	Generate a Random PIN	X	
JC (JD)	Translate a PIN from TPK to LMK Encryption	X	
JE (JF)	Translate a PIN from ZPK to LMK Encryption	X	
JG (JH)	Translate a PIN from LMK to ZPK Encryption	X	
K0 (K1)	Verify Encrypted Counters (EMV		
K2 (K3)	Verify Truncated Application Cryptogram (MasterCard CAP)		
K8 (K9)	Export a Key under a KEK		
KA (KB)	Generate a Key Check Value (Not Double-Length ZMK)	X	
KC (KD)	Translate a ZPK		
KE (KF)	Generate Issuer RSA Key Set and Public Key Certificate		EMV Issuing
KG (KH)	Validate an Issuer Public Key Certificate		EMV Issuing

KI (KJ)	Derive Card Unique DES Keys		EMV Issuing
KK (KL)	Import a Certification Authority Self-Signed Certificate		EMV Issuing
KM (KN)	Generate Static Data Authentication Signature		EMV Issuing
KO (KP)	Generate Card RSA Key Set and Public Key Certificate		EMV Issuing
KQ (KR)	ARQC Verification and/or ARPC Generation (EMV 3.1.1)	X	
KS (KT)	Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)		
KU (KV)	Generate Secure Message (EMV 3.1.1)		
KW (KX)	ARQC Verification and/or ARPC Generation (EMV 4.x)	X	
KY (KZ)	Generate Secure Message (EMV 4.x)		
L0 (L1)	Generate an HMAC Secret Key		
LA (LB)	Load Data to User Storage		
LC (LD)	Verify the Diebold Table in User Storage		
LE (LF)	Read Data from User Storage		
LG (LH)	Set HSM Response Delay	X	Custom Code, no real functionality yet
LI (LJ)	Load a PIN Text String		
LK (LL)	Generate a Decimal MAC		
LM (LN)	Verify a Decimal MAC		
LO (LP)	Translate Decimalisation Table from Old to New LMK		
LQ (LR)	Generate an HMAC on a Block of Data		
LS (LT)	Verify an HMAC on a Block of Data		
LU (LV)	Import an HMAC key under a ZMK		
LW (LX)	Export an HMAC key under a ZMK		
LY (LZ)	Translate a HMAC Key from Old LMK to New LMK		
M0 (M1)	Encrypt Data Block	X	
M2 (M3)	Decrypt Data Block	X	
M4 (M5)	Translate Data Block	X	
M6 (M7)	Generate MAC		
M8 (M9)	Verify MAC		
MA (MB)	Generate a MAC		
MC (MD)	Verify a MAC		
ME (MF)	Verify and Translate a MAC		
MG (MH)	Translate a TAK from LMK to ZMK Encryption	X	
MI (MJ)	Translate a TAK from ZMK to LMK Encryption	X	
MK (ML)	Generate a Binary MAC		
MM (MN)	Verify a Binary MAC		
MO (MP)	Verify and Translate a Binary MAC		
MQ (MR)	Generate MAC (MAB) for Large Message		

BP-Processing

BP-Sim

BP-Tools

MS (MT)	Generate MAC (MAB) using ANSI X9.19 Method for a Large Message		
MY (MZ)	Verify and Translate MAC		
NC (ND)	Perform Diagnostics	X	
NE (NF, NZ)	Generate and Print a Key as Split Components		
NG (NH)	Decrypt an Encrypted PIN	X	
NI (NJ)	Return Network Information		
NK (NL)	Command Chaining	X	
NO (NP)	HSM Status	X	
NY (Nz)	Generate IVCVC3 and Static CVC3		EM
OA (OB, OZ)	Print a PIN Solicitation Mailer		
OC (OD, OZ)	Generate and Print a ZMK Component		
OE (OF, OZ)	Generate and Print a TMK, TPK or PVK		
OI (OJ)	Generate a Set of Zone Keys (AS2805)	X	
OK (OL)	Translate a Set of Zone Keys to Encryption under the Local Master Key (AS2805)	X	
OU (OV)	Update Terminal Master Key 1 (Roll KEK 1) (AS2805)	X	Term
OW (OX)	Update Terminal Master Keys (Roll KEK 1 and KEK 2) (AS2805)	X	Term
P2 (P3)	Generate a VISA PVV (AS2805)		Term
P4 (P5)	Generate a Proof of Host value (AS2805)		Term
PA (PB)	Load Formatting Data to HSM		
PC (PD)	Load Additional Formatting Data to HSM		
PE (PF, PZ)	Print PIN/PIN and Solicitation Data		
PG (PH)	Verify PIN/PIN and Solicitation Mailer Cryptography		
PI (PJ)	Generate Terminal Key Set (AS2805)	X	Term
PK (PL)	Generate a PIN Pad Acquirer Security Number (AS2805)		Term
PM (PN)	Verify a Dynamic CVV (dCVV)		
PO (PP)	Verify and Generate a VISA PVV, translate a PIN Block to Encryption under a Zone PIN Key (AS2805)	X	Term
PQ (PR)	Generate a Message Authentication Code AS2805-1988 (AS2805)		
PS (PT)	Validate a Message Authentication Code AS2805-1988 (AS2805)		
PU (PV)	Encrypt data (AS2805)	X	
PW (PX)	Decrypt data (AS2805)	X	
PY (PZ)	Verify and Generate an IBM PIN Offset (AS2805)		Term
Q0 (Q1)	Translate Audit Record MAC key		
Q2 (Q3)	Retrieve Audit Record		
Q4 (Q5)	Archive (Print) Audit Record		
Q6 (Q7)	Delete Audit Record		
Q8 (Q9)	Audit Record Verification		

QA (QB)	Load Solicitation Data to User Storage		
QC (QD)	Final Load of Solicitation Data to User Storage		
QI (QJ)	Translate a PPASN from old to new LMK (AS2805)	X	Term
QM (QN)	Data Encryption Using a Derived Privacy Key (AS2805.6.2)		Term
QO (QP)	Data Decryption Using a Derived Privacy Key (AS2805.6.2)		
QQ (QR)	Verify a PIN at Card Issuer using IBM Method (AS2805.6.2)		Term
QS (QT)	Verify a PIN at Card Issuer using the Diebold Method (AS2805.6.2)		
QU (QV)	Verify a PIN at Card Issuer using Visa Method (AS2805.6.2)		Term
QW (QX)	Verify a PIN at Card Issuer using the Comparison Method (AS2805.6.2)		
RA (RB)	Cancel Authorised Activities		
RC (RD)	Verify Solicitation Mailer Cryptography		
RE (RF)	Verify a Transaction Request, without PIN (AS2805.6.2)		Term
RG (RH)	Verify a Transaction Request, with PIN, when CD Field Available (AS2805.6.2)		Term
RI (RJ)	Verify a Transaction Request, with PIN, when CD Field not Available (AS2805.6.2)		Term
RI (RJ)	Transaction Request With a PIN (T/AQ Key)		
RK (RL)	Generate Transaction Response, with Auth Para Generated by Acquirer (AS2805.6.2)		Term
RK (RL)	Transaction Request Without a PIN		
RM (RN)	Generate Transaction Response with Auth Para Generated by Card Issuer (AS2805.6.2)		Term
RM (RN)	Administration Request Message		
RO (RP)	Translate a PIN from PEK to ZPK Encryption (AS2805.6.2)		Term
RO (RP)	Transaction Response with Auth Para from Card Issuer		
RQ (RR)	Verify a Transaction Completion Confirmation Request (AS2805.6.2)		Term
RQ (RR)	Generate Auth Para and Transaction Response		
RS (RT)	Generate a Transaction Completion Response (AS2805.6.2)		Term
RS (RT)	Confirmation		
RU (RV)	Generate Auth Para at the Card Issuer (AS2805.6.2)		Term
RU (RV)	Transaction Request With a PIN (T/CI Key)		
RW (RX)	Generate an Initial Terminal Key (AS2805.6.2)		Term
RW (RX)	Translate KEYVAL		
RY (RZ)	Calculate Card Security Codes		
RY (RZ)	Verify Card Security Codes		
RY (RZ)	Generate a CSCK		
RY (RZ)	Export a CSCK		
RY (RZ)	Import a CSCK		
SC (SD)			
SE (SF)			
SI (SJ)			
SK (SL)	Generate ZAK, ZPK under BDK and MAC, PAC random numbers (Shell)		

TA (TB, TZ)	Print TMK Mailer

Any Thales HSM command missing? Please let us know.

< Prev Next >