THALES

www.thalesesecurity.com

‹Thales eSecurity›

payShield® 10K

Legacy Host Commands

Version: V1
Date: 2019
Doc. Number: PUGD0538-002

Copyright Statement

© Thales UK Limited 2019

The copyright herein is the property of Thales UK Limited. It is not to be reproduced, modified, adapted, published, translated in any material form (including storage in any medium by electronic means whether or not transiently or incidentally), in whole or in part nor disclosed to any third party without the prior written permission of Thales UK Limited. Neither shall it be used otherwise than for the purpose for which it is supplied.

Confidentiality Statement

The information contained herein is confidential and, subject to any rights of third parties, is proprietary to Thales UK Limited. It is intended only for the authorised recipient for the intended purpose, and access to it by any other person is unauthorised. The information contained herein may not be disclosed to any third party or used for any other purpose without the express written permission of Thales UK Limited.

Document Classification

Thales Group Classification: Thales Group Internal

Trademarks

Words and logos marked with ™ are trademarks of Thales UK Limited.

Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

End User Licence Agreement

Use of this product is subject to the Thales eSecurity End User License Agreement found at

https://www.thalesesecurity.com/eula.

Additional Information

Information in this document is subject to change without notice.

Where translations have been made in this document English is the canonical language.

Contents

1. Introduction 7

1.1. List of Host Commands (Alphabetical) 8

1.2. List of Host Commands (Functional) 12

2. General 16

3. Legacy Key Management Commands 17

Generate a TMK, TPK or PVK 19

Generate a TAK 20

Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK 22

Translate a TAK from LMK to TMK Encryption 24

Generate a CVK Pair 26

Generate and Print a TMK, TPK or PVK 27

Generate a Pair of PVKs 29

Generate a Watchword Key 31

Generate ZEK/ZAK 32

Generate a ZPK 34

Form a ZMK from Three ZMK Components 36

Form a ZMK from 2 to 9 ZMK Components 38

Generate and Print a ZMK Component 40

Print TMK Mailer 42

Translate a CVK Pair from Old LMK to New LMK Encryption 44

Translate a CVK Pair from LMK to ZMK Encryption 45

Translate a CVK Pair from ZMK to LMK Encryption 47

Translate a TMK, TPK or PVK 49

Translate a TMK, TPK or PVK from LMK to ZMK Encryption 50

Translate a TMK, TPK or PVK from ZMK to LMK Encryption 52

Translate a TAK 54

Translate a TAK from LMK to ZMK Encryption 55

Translate a TAK from ZMK to LMK Encryption 57

Translate a Watchword Key from LMK to ZMK Encryption 59

Translate a Watchword Key from ZMK to LMK Encryption 61

Translate a ZEK/ZAK from LMK to ZMK Encryption 63

Translate a ZEK/ZAK from ZMK to LMK Encryption 65

Translate a ZPK 67

Translate a ZPK from LMK to ZMK Encryption 68

Translate a ZPK from ZMK to LMK Encryption 70

Translate a ZMK 72

Generate a Key Check Value (Not Double-Length ZMK) 73

Generate a CSCK 75

Export a CSCK 76

© Thales UK Limited 2019

Import a CSCK 78
Generate a BDK 80
Translate a BDK from ZMK to LMK Encryption 81
Translate a BDK from LMK to ZMK Encryption 83
Generate and Export a KML 85
Import a KML 87
4. Legacy Message Integrity Commands 89
Generate a MAC 90
Verify a MAC 91
Verify and Translate a MAC 92
Generate MAC (MAB) for Large Message 94
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message 96
Generate a Binary MAC 98
Verify a Binary MAC 99
Verify and Translate a Binary MAC 100
Generate a MAC on a Binary Message 102
Verify a MAC on a Binary Message 104
5. Legacy Message Encryption Commands 106
Encrypt Data Block 107
Decrypt Data Block 108
6. Legacy DUKPT Commands 109
Translate a PIN from BDK to ZPK Encryption (DUKPT) 110
Verify a PIN Using the IBM Offset Method (DUKPT) 112
Verify a PIN Using the ABA PVV Method (DUKPT) 115
Verify a PIN Using the Diebold Method (DUKPT) 117
Verify a PIN Using the Encrypted PIN Method (DUKPT) 119
7. Legacy UnionPay Commands 121
ARQC Verification and/or ARPC Generation (UnionPay) 122
Generate Secure Message with Integrity and optional Confidentiality (UnionPay) 124
8. VisaCash Commands 127
Verify Load Signature S1 and Generate Load Signature S2 128
Verify Load Completion Signature S3 130
Verify Unload Signature S1 and Generate Unload Signature S2 131
Verify Unload Completion Signature S3 133
9. Watchword Commands 134
Verify a Watchword Response 135
Generate a Decimal MAC 136
Verify a Decimal MAC 137
10. Legacy WebPIN Commands 139
Verify PIN Block from Internet and Verify MAC 140
Verify PIN Block from Internet, Verify MAC & Return New Encrypted PIN 142

© Thales UK Limited 2019

Verify MAC *144*
Generate MAC *146*
Translate PIN Block from Internet, Verify MAC and Optionally Generate a MAC *148*
Decrypt Data *150*
Encrypt Data *152*
11. SEED Algorithm Commands 154
Verify an Interchange PIN using the comparison method with SEED encryption algorithm *155*
Verify a Terminal PIN using the comparison method with SEED encryption algorithm *156*
Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm *157*
Translate a PIN from TPK to ZPK with SEED encryption algorithm *159*
Encrypt Data Block with SEED algorithm *161*
Decrypt Data Block with SEED algorithm *163*
Translate Data Block with SEED algorithm *165*
Generate Round Key from SEED Key *167*
12. CEPS Commands 168
Decrypt R_1 and validate the MAC_{LSAM} *169*
Compute H_{CEP} *171*
Validate the S_1 MAC (Load and Unload) *172*
Validate the S_1 MAC (Currency Exchange) *174*
Generate the S_2 MAC (Linked load, declined unlinked load, unload) *176*
Generate the S_2 MAC (Currency Exchange) *177*
Generate the S_2 MAC (Approved Unlinked Load) *178*
Validate the S_3 MAC (Currency Exchange transactions) *179*
Validate the S_3 MAC (Load or Unload transactions) *181*
Validate the $H2_{LSAM}$ *183*
Unlinked Load Transaction Request *184*
Release R_{LSAM} *186*
Release $R2_{LSAM}$ *187*
Verify R_{CEP} *188*
Validate S_6 MAC *189*
Validate $S_{6'}$ MAC *190*
Validate $S_{6''}$ MAC *191*
Validate $S_{5',DLT}$ MAC *192*
Validate $S_{5',ISS}$ MAC *193*
Validate the S_4 MAC (Old Terminals) *194*
Validate the S_4 MAC (New Terminals) *195*
Validate the S_5 MAC (Old Terminals) *196*
Validate the $S_{5'}$ MAC (MAC of the PSAM for a Transaction) (New Terminals) *197*
Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals) *199*
Create the Acknowledgement MAC (Old Terminals) *201*
Create the Acknowledgement MAC (New Terminals) *202*

© Thales UK Limited 2019

Create the Update MAC *203*
Validate the S_{ADMIN} MAC (Administrative MAC of the PSAM) *204*
Create the Merchant Acquirer MAC *205*
Validate the Card Issuer MAC *206*
Export Electronic Purse Card Key Set *207*
13. Error Codes 213
14. WebPIN Appendices 216

© Thales UK Limited 2019

1. Introduction

The payShield 10K provides a variety of legacy host functions to support existing software applications. New applications should use functions described in the *payShield 10K Core Host Commands Manual*.

The remainder of this manual describes the legacy commands, and is divided into the following groupings:

- Legacy Key Management Commands
- Legacy Message Integrity Commands
- Legacy Message Encryption Commands
- Legacy DUKPT Commands
- Legacy UnionPay Commands
- VisaCash Commands
- Watchword Commands
- Legacy WebPIN Commands
- SEED Algorithm Commands
- CEPS Commands

© Thales UK Limited 2019

1.1. List of Host Commands (Alphabetical)

Command (Response)	Function	Page
AA (AB)	Translate a TMK, TPK or PVK	49
AC (AD)	Translate a TAK	54
AE (AF)	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	22
AG (AH)	Translate a TAK from LMK to TMK Encryption	24
AI (AJ)	Encrypt Data Block with SEED algorithm	161
AK (AL)	Decrypt Data Block with SEED algorithm	163
AM (AN)	Translate Data Block with SEED algorithm	165
AO (AP)	Generate Round Key from SEED Key	167
AS (AT)	Generate a CVK Pair	26
AU (AV)	Translate a CVK Pair from LMK to ZMK Encryption	45
AW (AX)	Translate a CVK Pair from ZMK to LMK Encryption	47
AY (AZ)	Translate a CVK Pair from Old LMK to New LMK Encryption	44
BI (BJ)	Generate a BDK	80
CI (CJ)	Translate a PIN from BDK to ZPK Encryption (DUKPT)	110
CK (CL)	Verify a PIN Using the IBM Offset Method (DUKPT)	112
CM (CN)	Verify a PIN Using the ABA PVV Method (DUKPT)	115
CO (CP)	Verify a PIN Using the Diebold Method (DUKPT)	117
CQ (CR)	Verify a PIN Using the Encrypted PIN Method (DUKPT)	119
DI (DJ)	Generate and Export a KML	85
DK (DL)	Import a KML	87
DM (DN)	Verify Load Signature S1 and Generate Load Signature S2	128
DO (DP)	Verify Load Completion Signature S3	130
DQ (DR)	Verify Unload Signature S1 and Generate Unload Signature S2	131
DS (DT)	Verify Unload Completion Signature S3	133
DW (DX)	Translate a BDK from ZMK to LMK Encryption	81
DY (DZ)	Translate a BDK from LMK to ZMK Encryption	83
FA (FB)	Translate a ZPK from ZMK to LMK Encryption	70
FC (FD)	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	52
FE (FF)	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	50
FG (FH)	Generate a Pair of PVKs	29
FI (FJ)	Generate ZEK/ZAK	32
FK (FL)	Translate a ZEK/ZAK from ZMK to LMK Encryption	65
FM (FN)	Translate a ZEK/ZAK from LMK to ZMK Encryption	63

© Thales UK Limited 2019

Command (Response)	Function	Page
FO (FP)	Generate a Watchword Key	31
FQ (FR)	Translate a Watchword Key from LMK to ZMK Encryption	59
FS (FT)	Translate a Watchword Key from ZMK to LMK Encryption	61
FU (FV)	Verify a Watchword Response	135
G2 (G3)	Verify an Interchange PIN using the comparison method with SEED encryption algorithm	155
G4 (G5)	Verify a Terminal PIN using the comparison method with SEED encryption algorithm	156
G6 (G7)	Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm	157
G8 (G9)	Translate a PIN from TPK to ZPK with SEED encryption algorithm	159
GC (GD)	Translate a ZPK from LMK to ZMK Encryption	68
GE (GF)	Translate a ZMK	72
GG (GH)	Form a ZMK from Three ZMK Components	36
GY (GZ)	Form a ZMK from 2 to 9 ZMK Components	38
HA (HB)	Generate a TAK	20
HC (HD)	Generate a TMK, TPK or PVK	19
HE (HF)	Encrypt Data Block	107
HG (HH)	Decrypt Data Block	108
IA (IB)	Generate a ZPK	34
JS (JT)	ARQC Verification and/or ARPC Generation (UnionPay)	122
JU (JV)	Generate Secure Message with Integrity and optional Confidentiality (UnionPay)	124
KA (KB)	Generate a Key Check Value (Not Double-Length ZMK)	73
KC (KD)	Translate a ZPK	67
LK (LL)	Generate a Decimal MAC	136
LM (LN)	Verify a Decimal MAC	137
MA (MB)	Generate a MAC	90
MC (MD)	Verify a MAC	91
ME (MF)	Verify and Translate a MAC	92
MG (MH)	Translate a TAK from LMK to ZMK Encryption	55
MI (MJ)	Translate a TAK from ZMK to LMK Encryption	57
MK (ML)	Generate a Binary MAC	98
MM (MN)	Verify a Binary MAC	99
MO (MP)	Verify and Translate a Binary MAC	100
MQ (MR)	Generate MAC (MAB) for Large Message	94

© Thales UK Limited 2019

Command (Response)	Function	Page
MS (MT)	Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	96
MU (MV)	Generate a MAC on a Binary Message	102
MW (MX)	Verify a MAC on a Binary Message	104
OC (OD, OZ)	Generate and Print a ZMK Component	40
OE (OF, OZ)	Generate and Print a TMK, TPK or PVK	27
R2 (R3)	Export Electronic Purse Card Key Set	207
RY (RZ)	Generate a CSCK	75
RY (RZ)	Export a CSCK	76
RY (RZ)	Import a CSCK	78
T0 (T1)	Unlinked Load Transaction Request	184
T2 (T3)	Release RLSAM	186
T4 (T5)	Release R2LSAM	187
T6 (T7)	Verify RCEP	188
TA (TB, TZ)	Print TMK Mailer	42
U0 (U1)	Decrypt R1 and validate the MACLSAM	169
U2 (U3)	Compute HCEP	171
U4 (U5)	Validate the S1 MAC (Load and Unload)	172
U6 (U7)	Validate the S1 MAC (Currency Exchange)	174
U8 (U9)	Generate the S2 MAC (Linked load, declined unlinked load, unload)	176
V0 (V1)	Generate the S2 MAC (Currency Exchange)	177
V2 (V3)	Generate the S2 MAC (Approved Unlinked Load)	178
V4 (V5)	Validate the S3 MAC (Currency Exchange transactions)	179
V6 (V7)	Validate the S3 MAC (Load or Unload transactions)	181
V8 (V9)	Validate the H2LSAM	183
W0 (W1)	Validate S6 MAC	189
W2 (W3)	Validate S6' MAC	190
W4 (W5)	Validate S6'' MAC	191
W6 (W7)	Validate S5',DLT MAC	192
W8 (W9)	Validate S5',ISS MAC	193
X0 (X1)	Validate the S4 MAC (Old Terminals)	194
X2 (X3)	Validate the S4 MAC (New Terminals)	195
X4 (X5)	Validate the S5 MAC (Old Terminals)	196
X6 (X7)	Validate the S5' MAC (MAC of the PSAM for a Transaction) (New Terminals)	197

© Thales UK Limited 2019

Command (Response)	Function	Page
X8 (X9)	Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals)	199
XK (XL)	Verify PIN Block from Internet and Verify MAC	140
XM (XN)	Verify PIN Block from Internet, Verify MAC & Return New Encrypted PIN	142
XO (XP)	Verify MAC	144
XQ (XR)	Generate MAC	146
XS (XT)	Translate PIN Block from Internet, Verify MAC and Optionally Generate a MAC	148
XU (XV)	Decrypt Data	150
XW (XX)	Encrypt Data	152
Y0 (Y1)	Create the Acknowledgement MAC (Old Terminals)	201
Y2 (Y3)	Create the Acknowledgement MAC (New Terminals)	202
Y4 (Y5)	Create the Update MAC	203
Y6 (Y7)	Validate the SADMIN MAC (Administrative MAC of the PSAM)	204
Y8 (Y9)	Create the Merchant Acquirer MAC	205
Z0 (Z1)	Validate the Card Issuer MAC	206

© Thales UK Limited 2019

1.2. List of Host Commands (Functional)

Function	Command (Response)	Page
Legacy Key Management Commands		
Generate a CVK Pair	AS (AT)	26
Generate and Print a TMK, TPK or PVK	OE (OF, OZ)	27
Generate a Pair of PVKs	FG (FH)	29
Generate a Watchword Key	FO (FP)	31
Generate ZEK/ZAK	FI (FJ)	32
Generate a ZPK	IA (IB)	34
Form a ZMK from Three ZMK Components	GG (GH)	36
Form a ZMK from 2 to 9 ZMK Components	GY (GZ)	38
Generate and Print a ZMK Component	OC (OD, OZ)	40
Print TMK Mailer	TA (TB, TZ)	42
Translate a CVK Pair from Old LMK to New LMK Encryption	AY (AZ)	44
Translate a CVK Pair from LMK to ZMK Encryption	AU (AV)	45
Translate a CVK Pair from ZMK to LMK Encryption	AW (AX)	47
Translate a TMK, TPK or PVK	AA (AB)	49
Translate a TMK, TPK or PVK from LMK to ZMK Encryption	FE (FF)	50
Translate a TMK, TPK or PVK from ZMK to LMK Encryption	FC (FD)	52
Translate a TAK	AC (AD)	54
Translate a TAK from LMK to ZMK Encryption	MG (MH)	55
Translate a TAK from ZMK to LMK Encryption	MI (MJ)	57
Translate a Watchword Key from LMK to ZMK Encryption	FQ (FR)	59
Translate a Watchword Key from ZMK to LMK Encryption	FS (FT)	61
Translate a ZEK/ZAK from LMK to ZMK Encryption	FM (FN)	63
Translate a ZEK/ZAK from ZMK to LMK Encryption	FK (FL)	65
Translate a ZPK	KC (KD)	67
Translate a ZPK from LMK to ZMK Encryption	GC (GD)	68
Translate a ZPK from ZMK to LMK Encryption	FA (FB)	70
Translate a ZMK	GE (GF)	72
Generate a Key Check Value (Not Double-Length ZMK)	KA (KB)	73
Generate a CSCK	RY (RZ)	75
Export a CSCK	RY (RZ)	76
Import a CSCK	RY (RZ)	78
Generate a BDK	BI (BJ)	80

© Thales UK Limited 2019

Function	Command (Response)	Page
Translate a BDK from ZMK to LMK Encryption	DW (DX)	81
Translate a BDK from LMK to ZMK Encryption	DY (DZ)	83
Generate and Export a KML	DI (DJ)	85
Import a KML	DK (DL)	87
Legacy Message Integrity Commands		
Generate a MAC	MA (MB)	90
Verify a MAC	MC (MD)	91
Verify and Translate a MAC	ME (MF)	92
Generate MAC (MAB) for Large Message	MQ (MR)	94
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	MS (MT)	96
Generate a Binary MAC	MK (ML)	98
Verify a Binary MAC	MM (MN)	99
Verify and Translate a Binary MAC	MO (MP)	100
Generate a MAC on a Binary Message	MU (MV)	102
Verify a MAC on a Binary Message	MW (MX)	104
Legacy Message Encryption Commands		
Encrypt Data Block	HE (HF)	107
Decrypt Data Block	HG (HH)	108
Legacy DUKPT Commands		
Translate a PIN from BDK to ZPK Encryption (DUKPT)	CI (CJ)	110
Verify a PIN Using the IBM Offset Method (DUKPT)	CK (CL)	112
Verify a PIN Using the ABA PVV Method (DUKPT)	CM (CN)	115
Verify a PIN Using the Diebold Method (DUKPT)	CO (CP)	117
Verify a PIN Using the Encrypted PIN Method (DUKPT)	CQ (CR)	119
Legacy UnionPay Commands		
ARQC Verification and/or ARPC Generation (UnionPay)	JS (JT)	122
Generate Secure Message with Integrity and optional Confidentiality (UnionPay)	JU (JV)	124
VisaCash Commands		
Verify Load Signature S1 and Generate Load Signature S2	DM (DN)	128
Verify Load Completion Signature S3	DO (DP)	130
Verify Unload Signature S1 and Generate Unload Signature S2	DQ (DR)	131
Verify Unload Completion Signature S3	DS (DT)	133

© Thales UK Limited 2019

Function	Command (Response)	Page
Watchword Commands		
Verify a Watchword Response	FU (FV)	135
Generate a Decimal MAC	LK (LL)	136
Verify a Decimal MAC	LM (LN)	137
Legacy WebPIN Commands		
Verify PIN Block from Internet and Verify MAC	XK (XL)	140
Verify PIN Block from Internet, Verify MAC & Return New Encrypted PIN	XM (XN)	142
Verify MAC	XO (XP)	144
Generate MAC	XQ (XR)	146
Translate PIN Block from Internet, Verify MAC and Optionally Generate a MAC	XS (XT)	148
Decrypt Data	XU (XV)	150
Encrypt Data	XW (XX)	152
SEED Algorithm Commands		
Verify an Interchange PIN using the comparison method with SEED encryption algorithm	G2 (G3)	155
Verify a Terminal PIN using the comparison method with SEED encryption algorithm	G4 (G5)	156
Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm	G6 (G7)	157
Translate a PIN from TPK to ZPK with SEED encryption algorithm	G8 (G9)	159
Encrypt Data Block with SEED algorithm	AI (AJ)	161
Decrypt Data Block with SEED algorithm	AK (AL)	163
Translate Data Block with SEED algorithm	AM (AN)	165
Generate Round Key from SEED Key	AO (AP)	167
CEPS Commands		
Decrypt R1 and validate the MACLSAM	U0 (U1)	169
Compute HCEP	U2 (U3)	171
Validate the S1 MAC (Load and Unload)	U4 (U5)	172
Validate the S1 MAC (Currency Exchange)	U6 (U7)	174
Generate the S2 MAC (Linked load, declined unlinked load, unload)	U8 (U9)	176
Generate the S2 MAC (Currency Exchange)	V0 (V1)	177
Generate the S2 MAC (Approved Unlinked Load)	V2 (V3)	178

© Thales UK Limited 2019

Function	Command (Response)	Page
Validate the S3 MAC (Currency Exchange transactions)	V4 (V5)	179
Validate the S3 MAC (Load or Unload transactions)	V6 (V7)	181
Validate the H2LSAM	V8 (V9)	183
Unlinked Load Transaction Request	T0 (T1)	184
Release RLSAM	T2 (T3)	186
Release R2LSAM	T4 (T5)	187
Verify RCEP	T6 (T7)	188
Validate S6 MAC	W0 (W1)	189
Validate S6' MAC	W2 (W3)	190
Validate S6'' MAC	W4 (W5)	191
Validate S5',DLT MAC	W6 (W7)	192
Validate S5',ISS MAC	W8 (W9)	193
Validate the S4 MAC (Old Terminals)	X0 (X1)	194
Validate the S4 MAC (New Terminals)	X2 (X3)	195
Validate the S5 MAC (Old Terminals)	X4 (X5)	196
Validate the S5' MAC (MAC of the PSAM for a Transaction) (New Terminals)	X6 (X7)	197
Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals)	X8 (X9)	199
Create the Acknowledgement MAC (Old Terminals)	Y0 (Y1)	201
Create the Acknowledgement MAC (New Terminals)	Y2 (Y3)	202
Create the Update MAC	Y4 (Y5)	203
Validate the SADMIN MAC (Administrative MAC of the PSAM)	Y6 (Y7)	204
Create the Merchant Acquirer MAC	Y8 (Y9)	205
Validate the Card Issuer MAC	Z0 (Z1)	206
Export Electronic Purse Card Key Set	R2 (R3)	207

© Thales UK Limited 2019

2. General

This section details all the commands available with their responses and possible error codes.

A number of abbreviations are used throughout. They are:

L	:	Encrypted PIN length. Set at installation.
m	:	Message header length. Set at installation.
n	:	Variable length field.
A	:	Alphanumeric (can include any non-control type) characters.
H	:	Hexadecimal character ('0'...'9', 'A'...'F').
N	:	Numeric Field ('0'...'9').
C	:	Control character.
B	:	Binary data (byte) (X'00...X'FF).
D	:	Binary coded decimal (BCD) character ('0'...'9').

For example:

32 H : Indicates that thirty-two hexadecimal characters are required.

m A : Indicates the string of "message header length" alphanumeric characters.

For convenience, the STX and ETX control characters, which bracket every command and response when using asynchronous communications, are not shown in the details that follow.

In a command to the payShield 10K, any key can be replaced by a reference to internal user storage. In the details that follow, a key is always shown as if it is to be sent with each command; in every case the key can be replaced by the index flag "K" and a three-hexadecimal-digit pointer value: the value of "K" for the index flag is used irrespective of the index flag used when storing the key in User Storage using the *LA* host command.

The payShield 10K can be used in systems where there may be Atalla security equipment at other network nodes. This is achieved by the inclusion of an Atalla variant in those commands that translate a key from/to encryption under a ZMK. This has the effect of modifying the ZMK before it is used to decrypt/encrypt in accordance with the method used by the Atalla equipment. The payShield 10K can support 1 or 2 digit Atalla variants.

When a disabled host command is invoked, the error code 68 is returned.

© Thales UK Limited 2019

3. Legacy Key Management Commands

The payShield 10K provides the following host commands to support generic key management operations:

Function	Command	Page
Generate a TMK, TPK or PVK	HC (HD)	19
Generate a TAK	HA (HB)	20
Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	AE (AF)	22
Translate a TAK from LMK to TMK Encryption	AG (AH)	24
Generate a CVK Pair	AS (AT)	26
Generate and Print a TMK, TPK or PVK	OE (OF, OZ)	27
Generate a Pair of PVKs	FG (FH)	29
Generate a Watchword Key	FO (FP)	31
Generate ZEK/ZAK	FI (FJ)	32
Generate a ZPK	IA (IB)	34
Form a ZMK from Three ZMK Components	GG (GH)	36
Form a ZMK from 2 to 9 ZMK Components	GY (GZ)	38
Generate and Print a ZMK Component	OC (OD, OZ)	40
Print TMK Mailer	TA (TB, TZ)	42
Translate a CVK Pair from Old LMK to New LMK Encryption	AY (AZ)	44
Translate a CVK Pair from LMK to ZMK Encryption	AU (AV)	45
Translate a CVK Pair from ZMK to LMK Encryption	AW (AX)	47
Translate a TMK, TPK or PVK	AA (AB)	49
Translate a TMK, TPK or PVK from LMK to ZMK Encryption	FE (FF)	50
Translate a TMK, TPK or PVK from ZMK to LMK Encryption	FC (FD)	52
Translate a TAK	AC (AD)	54
Translate a TAK from LMK to ZMK Encryption	MG (MH)	55
Translate a TAK from ZMK to LMK Encryption	MI (MJ)	57
Translate a Watchword Key from LMK to ZMK Encryption	FQ (FR)	59
Translate a Watchword Key from ZMK to LMK Encryption	FS (FT)	61
Translate a ZEK/ZAK from LMK to ZMK Encryption	FM (FN)	63
Translate a ZEK/ZAK from ZMK to LMK Encryption	FK (FL)	65
Translate a ZPK	KC (KD)	67
Translate a ZPK from LMK to ZMK Encryption	GC (GD)	68
Translate a ZPK from ZMK to LMK Encryption	FA (FB)	70
Translate a ZMK	GE (GF)	72

© Thales UK Limited 2019

Generate a Key Check Value (Not Double-Length ZMK)	KA (KB)	73
Generate a CSCK	RY (RZ)	75
Export a CSCK	RY (RZ)	76
Import a CSCK	RY (RZ)	78
Generate a BDK	BI (BJ)	80
Translate a BDK from ZMK to LMK Encryption	DW (DX)	81
Translate a BDK from LMK to ZMK Encryption	DY (DZ)	83
Generate and Export a KML	DI (DJ)	85
Import a KML	DK (DL)	87

© Thales UK Limited 2019

Generate a TMK, TPK or PVK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not required**	

Function: Generate a random key, and encrypt it under a TMK (TPK or PVK) and under LMK pair 14-15.

Notes: This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HC'.
Current TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'HD'.
Error Code	2 A	'00': No error '10': TMK, TPK or PVK parity error '68': Command disabled or a standard error code.
New key under the current key	16 H or 'U' + 32 H or 'T' + 48 H	The new key encrypted under the current key.
New key under LMK	16 H or 'U' + 32 H or 'T' + 48 H	The new key under LMK pair 14-15.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a TAK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not required**	

Function: Generate a random key, encrypt it under a TMK and under LMK pair 16-17.

Notes: If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", then PVKs and TPKs are encrypted under the same LMK pair and variant as TMKs. However, PVKs and TPKs must not be used with this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HA'.
TMK	16 H or 'U' + 32 H or 'T' + 48 H	The TMK encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y".
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'HB'.
Error Code	2 A	'00': No error '10': TMK parity error '68': Command disabled or a standard error code.
TAK under TMK	16 H or 'U' + 32 H or 'T' + 48 H	The random TAK encrypted under the TMK.
TAK under LMK	16 H or 'U' + 32 H or 'T' + 48 H	The random TAK under LMK pair 16-17.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not required**	

Function: Translate a TMK, TPK or PVK from encryption under LMK pair 14-15 to encryption under another TMK (TPK or PVK).

Note: The command is used to replace an existing key with another key from the database.
This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AE'.
Current TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Stored TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	The stored TMK, TPK or PVK under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AF'.
Error Code	2 A	'00': No error '10': Current TMK, TPK or PVK parity error '11': Stored TMK, TPK or PVK parity error '68': Command disabled or a standard error code.
Stored key under the current key	16 H or 'U' + 32 H or 'T' + 48 H	The stored key encrypted under the current key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not required**	

Translate a TAK from LMK to TMK Encryption

Function: Translate a TAK from encryption under the LMK to encryption under a TMK. Used to send a key to a terminal.

Notes: This command is superseded by host command 'A8'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AG'.
TMK	16 H or 'U' + 32 H or 'T' + 48 H	TMK encrypted under the LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y".
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under LMK pair 16-17.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or '0'). For a list of key schemes, see Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AH'.
Error Code	2 A	'00': No error '10': TMK parity error '11': TAK parity error '68': Command disabled or a standard error code.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	Translated TAK; encrypted under the TMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a CVK Pair

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a Visa CVK pair.
Output the key pair encrypted under a variant of LMK pair 14-15.

Note: This command is superseded by host command 'A0'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AS'.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. If present must be '0' or 'U'. For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible). Not available for keys generated using schemes. '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AT'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code..
CVK Key scheme = '0' or not specified		
CVK A	16 H	CVK A encrypted under variant 4 of LMK pair 14-15.
CVK B	16 H	CVK B encrypted under variant 4 of LMK pair 14-15.
CVK Key scheme not '0'		
CVK A/B	'U' + 32 H	CVK A/B encrypted under variant 4 of LMK pair 14-15.
KCV Type = '0' or not specified		
CVK A check value	16 H	The CVK A check value.
CVK B check value	16 H	The CVK B check value.
For KCV Type = '1'		
CVK A/B check value	6 H	The CVK A/B check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate and Print a TMK, TPK or PVK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **genprint.{keytype}.host**	

Function: Generate a random key, return it encrypted under LMK pair 14-15 and print it at the payShield 10K attached printer.

Notes: This command is superseded by host command 'NE'.
A printer must be attached to one of the USB ports on the payShield 10K Serial-to-USB and parallel-to-USB cables are available from Thales, on request.
The HSM must have a print format already defined.
The delimiter to separate optional fields is changed from ';' to '|'.
This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OE'.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
…	…	…
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Optional. If present the following three fields must be present. Value '|'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OF'.
Error Code	2 A	'00': No error '16': Printer not ready/not connected '68': Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	TMK, TPK or PVK encrypted under LMK pair 14-15.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

© Thales UK Limited 2019

Generate a Pair of PVKs

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **generate.002.host**	

Function: Generate two random keys and return them each encrypted under LMK pair 14-15 and under a ZMK.

Notes: This command is superseded by host command 'A0'.

The command is used to send the keys to another party.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FG'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
KCV type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode). Not available for keys generated using new schemes. '1': 6 digit KCV. Only available for keys generated under new key schemes. '2': 8 digit KCV. Only available for keys generated in backward compatibility mode.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FH'.
Error Code	2 A	'00': No error '10': ZMK parity error '68': Command disabled or a standard error code.
		No LMK Scheme specified
First TMK, TPK or PVK under LMK	16 H	First half of the new TMK, TPK or PVK, encrypted under LMK pair 14-15.
Second TMK, TPK or PVK under LMK	16 H	Second half of the new TMK, TPK or PVK, encrypted under LMK pair 14-15.
First TMK, TPK or PVK under ZMK	16 H	First half of the new TMK, TPK or PVK, encrypted under ZMK.
Second TMK, TPK or PVK under ZMK	16 H	Second half of the new TMK, TPK or PVK, encrypted under ZMK.
First KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the first half of the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '2'.
Second KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the second half of the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '2'.
		LMK Scheme specified
TMK, TPK or PVK under LMK	'U' + 32 H or 'T' + 48 H	New TMK, TPK or PVK; encrypted under LMK pair 14-15.
TMK, TPK or PVK under ZMK	'U' + 32 H or 'T' + 48 H	New TMK, TPK or PVK; encrypted under ZMK.
KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '2'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a Watchword Key

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a Watchword Key (WWK).

Notes: This command is superseded by host command 'A0'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FO'.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'. If an option is **Not Required** by the command fill with a valid value or '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10k Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FP'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
WWK	16 H or 'U' + 32 H or 'T' + 48 H	Watchword Key encrypted under LMK pair 22-23.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate ZEK/ZAK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a ZEK or ZAK.

Notes: This command is superseded by host command 'A0'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FI'.
Flag	1 N	'0': ZEK '1': ZAK.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10k Host Programmer's Manual*. Default '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10k Host Programmer's Manual*. Default '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FJ'.
Error Code	2 A	'00': No error '10': ZMK parity error '68': Command disabled or a standard error code.
ZEK or ZAK for transmission	16 H or 'U' + 32 H or 'T' + 48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
ZEK for storage	16 H or 'U' + 32 H or 'T' + 48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK for storage	16 H or 'U' + 32 H or 'T' + 48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a ZPK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a random PIN key and return it to the Host encrypted under a ZMK for transmission to another party and under the LMK for storage on the Host database.

Notes: This command is superseded by host command 'A0'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'IA'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IB'.
Error Code	2 A	'00': No error '10': ZMK does not have odd parity '68': Command disabled or a standard error code.
ZPK under ZMK	16 H or 'U' + 32 H or 'T' + 48 H	The ZPK encrypted under the ZMK.
ZPK under LMK	16 H or 'U' + 32 H or 'T' + 48 H	The ZPK encrypted under LMK pair 06-07.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Form a ZMK from Three ZMK Components

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **component.000.host**	

Function: Form a ZMK from three encrypted components and return the ZMK encrypted under LMK pair 04-05, and the check value.

Notes: This command is superseded by host command 'A4'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GG'.
First ZMK component	16 / 32 H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16 / 32 H	The second ZMK component encrypted under a variant of LMK 04-05.
Third ZMK component	16 / 32 H	The third ZMK component encrypted under a variant of LMK 04-05.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GH'.
Error Code	2 A	'00': No error '10': Parity error in first component '11': Parity error in second / third component '68': Command disabled or a standard error code.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZMK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Form a ZMK from 2 to 9 ZMK Components

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **component.000.host**	

Function: Form a ZMK from 2 to 9 encrypted components and return the ZMK encrypted under a variant of LMK pair 04-05, and the check value.

Notes: This command is superseded by host command 'A4'.

Use this command to provide inter-operation with non-Thales security equipment.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GY'.
Number of components	1 N	'2' – '9': Number of components.
First ZMK component	16 / 32 H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16 / 32 H	The second ZMK component encrypted under a variant of LMK 04-05.
…	…	…
Last ZMK component	16 / 32 H	The last ZMK component encrypted under a variant of LMK 04-05.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GZ'.
Error Code	2 A	'00': No error '10': Parity error in first component '11': Parity error second to ninth components '68': Command disabled or a standard error code.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZMK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate and Print a ZMK Component

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **genprint.000.host**	

Function: Generate a random ZMK component, print it at the payShield 10K attached printer and return the encrypted value to the host.

Notes: This command is superseded by host command 'A2'.

A printer must be attached to one of the USB ports on the payShield 10K. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The HSM must have a print format already defined.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

The delimiter to separate optional fields is changed from ';' to '|'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OC'.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
Last print field	n A	The last print field defined in the print format definition must not contain a ';' or '~' character).
Delimiter	1 A	Optional. If present the following three fields must be present. Value '|'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present, should be '0'.
Reserved	1 A	Optional. If present, should be '0'.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OD'.
Error Code	2 A	'00': No Error '16': Printer not ready/not connected '18': Format definition not loaded '68': Command disabled or a standard error code.
ZMK component	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK component encrypted under a variant of LMK pair 04-05.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

© Thales UK Limited 2019

Print TMK Mailer

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **command.ta.host**	

Function: Print the TMK at the HSM-attached terminal.

Notes: A printer must be attached to the HSM, and the print format must have been defined.

The clear TMK will be positioned in the mailer at the location of the '^P' symbol defined by the print format.

This command uses an extended specification of Print Formatting Symbols to provide up to 32 different fields:

^00 = Insert Print Field #0

^01 = Insert Print Field #1

…

^1F = Insert Print Field #31

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'TA'.
TMK	16 H or 'U' + 32 H or 'T' + 48 H	The Terminal Master Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y".
Print field 0	n A	The print field defined as print field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
Print field 1	n A	The print field defined in print field 1 in the print format definition (must not contain a ';' character).
…	…	…
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'TB'.

© Thales UK Limited 2019

Field	Length & Type	Details
Error Code	2 A	'00': No error '10': TMK parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'TZ'.
Error Code	2 A	'00': No error '16': Printer time out '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Translate a CVK Pair from Old LMK to New LMK Encryption

Function: Translate a CVK pair from encryption under a variant 4 of an old LMK pair 14-15 to encryption under a variant 4 of a new LMK pair 14-15.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AY'.
CVK A / B	32 H or 'U' + 32 H	CVK A / B pair encrypted under a variant 4 of the old LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AZ'.
Error Code	2 A	'00': No error '10': CVK A or B parity error '11': ZPK parity error '68': Command disabled or a standard error code.
CVK A / B	32 H or 'U' + 32 H	CVK A / B encrypted under a variant of LMK pair 14-15.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a CVK Pair from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a CVK pair from encryption under a variant of LMK pair 14-15 to encryption under a ZMK.

Notes: This command is superseded by host command 'A8'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AU'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32 H or 'U' + 32 H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode). Not available for keys generated using schemes. '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AV'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': CVK A or B parity error '68': Command disabled or a standard error code.
CVK A / B	32 H or 'U' + 32 H	CVK A / B encrypted under ZMK.
		KCV Type = 0 or not specified
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
		KCV Type = 1
Key Check Value	6 H	Result of encrypting 64 binary zeros with the key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a CVK Pair from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a CVK pair from encryption under a ZMK to encryption under a variant of LMK pair 14-15.

Notes: This command is superseded by host command 'A6'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AW'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32 H or 'U' + 32 H	CVK A / B encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode – not available for keys generated using schemes) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AX'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': CVK A or B parity error '68': Command disabled or a standard error code.
CVK A / B	32 H or 'U' + 32 H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
		KCV Type = '0' or not specified
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
		KCV Type = '1'
Key Check Value	6 H	Result of encrypting 64 binary zeros with the key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TMK, TPK or PVK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a TMK, TPK or PVK from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Notes: This command is superseded by host command 'BW'.

This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AA'.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	The TMK, TPK or PVK encrypted under the 'old' LMK.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AB'.
Error Code	2 A	'00': No error '10': TMK, TPK or PVK parity error '68': Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	The TMK, TPK or PVK translated to encryption under 'new' LMK pair 14-15.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TMK, TPK or PVK from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **export.{keytype}.host**	

Function: Translate a TMK, TPK or PVK from encryption under the LMK to encryption under a ZMK.

Notes: This command is superseded by host command 'A8'.

The command is used to send a key to another party.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FE'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	TMK, TPK or PVK encrypted under LMK pair 14-15.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FF'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': TMK, TPK or PVK parity error '68': Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	Translated TMK, TPK or PVK encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the key. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TMK, TPK or PVK from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **import.{keytype}.host**	

Function: Translate a TMK, TPK or PVK from encryption under a ZMK to encryption under the LMK.

Notes: This command is superseded by host command 'A6'.

The command is used to receive a key from another party.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FC'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	TMK, TPK or PVK encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FD'.

© Thales UK Limited 2019

Error Code	2 A	'00': No error '10': ZMK parity error '11': TMK, TPK or PVK parity error '68': Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 'U' + 32 H or 'T' + 48 H	Translated TMK, TPK or PVK; encrypted under LMK pair 14-15.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the key. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TAK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a TAK from encryption under the 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AC'.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	The TAK encrypted under the 'old' LMK.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AD'.
Error Code	2 A	'00': No error '10': TAK parity error '68': Command disabled or a standard error code.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	The TAK translated to encryption under the 'new' LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TAK from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a TAK from encryption under the LMK to encryption under a ZMK.

Used to send a key to another party.

Notes: This command is superseded by host command 'A8'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MG'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under LMK pair 16-17.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MH'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': TAK parity error '68': Command disabled or a standard error code.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the TAK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a TAK from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a TAK from encryption under a ZMK to encryption under the LMK.

Used to receive a key from another party.

Notes: This command is superseded by host command 'A6'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MI'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under ZMK.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MJ'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': TAK parity error '68': Command disabled or a standard error code.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under LMK pair 16-17.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the TAK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a Watchword Key from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a Watchword Key from encryption under the LMK to encryption under a ZMK.

Notes: This command is superseded by host command 'A8'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FQ'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
WWK	16 H or 'U' + 32 H or 'T' + 48 H	Watchword encrypted under LMK pair 22-23.
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FR'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': ZPK parity error '68': Command disabled or a standard error code.
WWK	16 H or 'U' + 32 H or 'T' + 48 H	WWK encrypted under ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a Watchword Key from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a Watchword Key from encryption under a ZMK to encryption under the LMK.

Notes: This command is superseded by host command 'A6'.

If using a 32-character ZMK, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FS'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
WWK	16 H or 'U' + 32 H or 'T' + 48 H	Watchword encrypted under ZMK.
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FT'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': Imported key all zero '68': Command disabled or a standard error code.
WWK	16 H or 'U' + 32 H or 'T' + 48 H	WWK encrypted under LMK pair 22-23.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a ZEK/ZAK from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a ZEK or ZAK.

Notes: This command is superseded by host command 'A8'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FM'.
Flag	1 N	'0': ZEK '1': ZAK.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
ZEK	16 H or 'U' + 32 H or 'T' + 48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK	16 H or 'U' + 32 H or 'T' + 48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FN'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': ZEK/ZAK parity error '68': Command disabled or a standard error code.
ZEK/ZAK	16 H or 'U' + 32 H or 'T' + 48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a ZEK/ZAK from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a ZEK or ZAK from ZMK to LMK.

Notes: This command is superseded by host command 'A6'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FK'.
Flag	1 N	'0': ZEK '1': ZAK.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
ZEK/ZAK	16 H or 'U' + 32 H or 'T' + 48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FL'.
Error Code	2 A	'00': No error '10': ZMK parity error '68': Command disabled or a standard error code.
ZEK	16 H or 'U' + 32 H or 'T' + 48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK	16 H or 'U' + 32 H or 'T' + 48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a ZPK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a ZPK from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KC'.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	The ZPK encrypted under the 'old' LMK.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KD'.
Error Code	2 A	'00': No error '10': ZPK parity error '68': Command disabled or a standard error code.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	The ZPK translated to encryption under the 'new' LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Translate a ZPK from LMK to ZMK Encryption

Function: Translate a ZPK from encryption under the LMK to encryption under a ZMK.

Used to transmit a ZPK to another party.

Notes: This command is superseded by host command 'A8'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GC'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	ZPK encrypted under LMK pair 06-07.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GD'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': ZPK parity error '68': Command disabled or a standard error code.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	Translated ZPK; encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a ZPK from ZMK to LMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a ZPK from encryption under a ZMK to encryption under the LMK.

Used to receive a ZPK from another party.

Notes: This command is superseded by host command 'A6'.

The command does not require the ZPK to have odd parity, but odd parity is forced on the encrypted output. Unlike other commands, if error 01 is returned, it does not inhibit the return of subsequent fields.

The command tests the ZPK, after decrypting it from under the ZMK, to ensure the key (including the parity bits) is not zero (i.e., X'0000 0000 0000 0000). If the key is zero, the HSM returns error code 11 (all zero ZPK with even parity) and terminates processing.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FA'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	ZPK encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FB'.
Error Code	2 A	'00': No error '01': ZPK parity error; advice only '10': ZMK parity error '11': All zero ZPK with even parity '68': Command disabled or a standard error code.
ZPK	16 H or 'U' + 32 H or 'T' + 48 H	Translated ZPK; encrypted under LMK pair 06-07.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a ZMK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a ZMK from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Notes: This command is superseded by host command 'BW'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GE'.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under the 'old' LMK.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GF'.
Error Code	2 A	'00': No error '10': ZMK parity error '68': Command disabled or a standard error code.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H	The ZMK translated to encryption under the 'new' LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a Key Check Value (Not Double-Length ZMK)

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a key check value for one of the following:

ZMK (single-length), ZPK, TMK, TPK, PVK, TAK

Notes: This command is superseded by host command 'BU'.

The command can be used to verify a key received from another party. The HSM generates the value by encrypting 64 binary zeroes under the key.

This command does not support the use of double-length ZMKs.

This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KA'.
Key	16 H or 'U' + 32 H or 'T' + 48 H	One of the following: ZMK, ZPK, TMK, TPK, PVK or TAK encrypted under the relevant LMK pair.
Key Type Code	2 N	The 2-digit key type code: '00': ZMK '01': ZPK '02': TMK, TPK or PVK '03': TAK.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KB'.
Error Code	2 A	'00': No error '10': Encrypted key parity error '68': Command disabled or a standard error code.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the key. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate a CSCK

Function: Generate a random dual-length CSCK and encrypt it under LMK 14-15 variant 4.

Note: This command is superseded by host command 'A0'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RY'.
Mode	1 N	Value '0'.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RZ'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
Mode	1 N	Value '0'.
CSCK	32 H or 'U' + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Export a CSCK

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Decrypt a CSCK from under LMK 14-15 variant 4 and re-encrypt it under a supplied ZMK.

Note: This command is superseded by host command 'A8'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RY'.
Mode	1 N	Value '1'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	The Zone Master Key, encrypted under LMK 04-05.
CSCK	32 H or 'U' + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Atalla variant	1 / 2 N	Optional.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'. If an option is **Not Required** by the command fill with a valid value or 0.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RZ'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': CSCK parity error '27': CSCK not double length '68': Command disabled or a standard error code.
Mode	1 N	Value '1'.
CSCK encrypted for export	32 H or 'U' + 32 H	The CSCK encrypted under the supplied ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Import a CSCK

Function: Decrypt a CSCK from under a supplied ZMK and re-encrypt it under LMK 14-15 variant 4.

Notes: This command is superseded by host command 'A6'.

Parity on the incoming CSCK is ignored, but odd parity will be forced before re-encryption. Error Code '01' will be returned if the incoming key did not have odd parity.

If the incoming key is found to be all zeros, Error Code 02 is returned and the key is not translated.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RY'.
Mode	1 N	Value '2'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	The Zone Master Key, encrypted under LMK 04-05.
CSCK	32 H or 'U' + 32 H	The CSCK, encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RZ'.
Error Code	2 A	'00': No error '01': Incoming key did not have odd parity '02': Incoming key was all zero '10': ZMK parity error '27': CSCK not double length '68': Command disabled or a standard error code.
Mode	1 N	Value '2'.
CSCK	32 H or 'U' + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Determined by KTT(G)** Activity: **generate.bdk.host**	

Generate a BDK

Function: Generate a BDK and encrypt it under LMK pair 28-29 for Host storage.

Notes: The use of key scheme '0' is not recommended.

This command is superseded by host command 'A0'. However, please note that 'A0' does not support the generation of a BDK using key scheme '0'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BI'.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BJ'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
BDK	32 H or 'U' + 32 H	The BDK encrypted under LMK pair 28-29.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Translate a BDK from ZMK to LMK Encryption

Function: Translate a BDK from encryption under a ZMK to encryption under LMK pair 28-29.

Notes:
This command is superseded by host command 'A6'.

The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command – the ZMK cannot be single length.

A key check value (KCV) is produced for the BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DW'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
BDK	32 H or 'U' + 32 H	The BDK encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional. For use in networks that use a ZMK variant.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
Reserved	1 A	Optional. If present must be 0.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 8 digit KCV (backward compatible mode) '1': 6 digit KCV '2': 8 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DX'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': BDK parity error '27': BDK not double length '68': Command disabled or a standard error code.
BDK	32 H or 'U' + 32 H	The BDK encrypted under LMK pair 28-29.
Key Check Value	6 / 8 H	Result of encrypting 64 binary zeros with the BDK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a BDK from LMK to ZMK Encryption

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a BDK from encryption under LMK pair 28-29 to encryption under ZMK.

Notes: This command is superseded by host command 'A8'.

The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command – the ZMK cannot be single length.

A key check value (KCV) is produced for the BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DY'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	The ZMK encrypted under LMK pair 04-05.
BDK	32 H or 'U' + 32 H	The BDK encrypted under LMK pair 28-29.
Atalla variant	1 / 2 N	Optional. For use in networks that use a ZMK variant.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Reserved	1 A	Optional. If present must be 0.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 8 digit KCV (backward compatible mode) '1': 6 digit KCV '2': 8 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DZ'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': BDK parity error '27': BDK not double length or triple length '68': Command disabled or a standard error code.
BDK	32 H or 'U' + 32 H	The BDK encrypted under the ZMK.
Key Check Value	6 / 8 H	Result of encrypting 64 binary zeros with the key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate and Export a KML

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a double-length Master Load Key (KML) and return it encrypted under Variant 2 of LMK pair 04-05, and also under a double length Zone Master Key (ZMK).

Notes: This command is superseded by host command 'A0'.

A check value for the KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DI'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*. Default '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0': 6 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DJ'.
Error Code	2 A	'00': No error '10': ZMK parity error '68': Command disabled or a standard error code.
KML (ZMK)	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under ZMK.
KML (under LMK)	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the KML and returning the 24 left-most bits of the result.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Import a KML

Function: Translate a double-length Master Load Key (KML) from encryption under a ZMK to encryption under Variant 2 of LMK pair 04-05.

Notes: This command is superseded by host command 'A6'.

A check value for the KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DK'.
ZMK	32 H or 'U' + 32 H or 'T' + 48 H	ZMK encrypted under LMK pair 04-05.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under ZMK.
Atalla variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix A of the *payShield 10K Host Programmer's Manual*.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 6 digit KCV (backward compatible mode) '1': 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DL'.
Error Code	2 A	'00': No error '10': ZMK parity error '11': KML parity error '68': Command disabled or a standard error code.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the KML and returning the left-most 24 bits of the result.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

4. Legacy Message Integrity Commands

The payShield 10K provides the following host commands to support legacy MAC operations:

Function	Command	Page
Generate a MAC	MA (MB)	90
Verify a MAC	MC (MD)	91
Verify and Translate a MAC	ME (MF)	92
Generate MAC (MAB) for Large Message	MQ (MR)	94
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	MS (MT)	96
Generate a Binary MAC	MK (ML)	98
Verify a Binary MAC	MM (MN)	99
Verify and Translate a Binary MAC	MO (MP)	100
Generate a MAC on a Binary Message	MU (MV)	102
Verify a MAC on a Binary Message	MW (MX)	104

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate a MAC

Function: Generate a MAC on a given block of data using a TAK.

Notes: This command is superseded by host command 'M6'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased up to 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MA'.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under LMK pair 16-17.
Data	0 - n	The data on which a MAC is to be generated, n = 16K. Must not contain a '~' character.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MB'.
Error Code	2 A	'00': No error '10': TAK parity error '68': Command disabled or a standard error code.
MAC	8 H	The calculated MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a MAC on given block of data using a TAK.

Notes: This command is superseded by host command 'M8'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MC'.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	TAK encrypted under LMK pair 16-17.
MAC	8 H	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n = 16K. Must not contain a '~' character.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MD'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': TAK parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify and Translate a MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a MAC on a block of data using a TAK and, if successful, generate a MAC on the same block of data with a different TAK.

Notes: This command is superseded by host command 'MY'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ME'.
Source TAK	16 H or 'U' + 32 H or 'T' + 48 H	The source TAK encrypted under LMK pair 16-17.
Destination TAK	16 H or 'U' + 32 H or 'T' + 48 H	The destination key encrypted under LMK pair 16-17.
MAC	8 H	The MAC generated with the source key.
Data	0 - n	The data on which to verify and generate a MAC, n = 16K. Must not contain a '~' character.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MF'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Source TAK parity error '11': Destination TAK parity error '68': Command disabled or a standard error code.
MAC	8 H	The MAC generated using the destination TAK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate MAC (MAB) for Large Message

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a MAC (MAB) for a large message using a ZAK.

Notes: When using 8 hex-digit MACs, this command is superseded by host command 'M6'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The command operates on binary data. If the HSM is set for Async/ASCII operation, ensure that:

The Host port has been set for 8 data bit operation by the CH (Configure Host) command.

The data for which the MAC is to be generated does not contain either EM (X'19) or ETX (X'03).

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

When generating a MAC using multiple message blocks (i.e. Message Block Number = '1', '2' or '3'), there is a minimum length to the separate message blocks:

- Each supplied message block must be at least 24 bytes (binary/text) or 48 hex characters.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MQ'.
Message Block Number	1 N	'0': The only block. '1': The first block. '2': A middle block. '3': The last block.
ZAK	16 H or 'U' + 32 H or 'T' + 48 H	ZAK encrypted under LMK pair 26-27
IV	16 H	Initialization value, present only when Message block number is '2' or '3'.
Message Length	3 H	Message length in bytes.
Message Block	n B	The clear text message block.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MR'.
Error Code	2 A	'00': No error '02': ZAK not single length '05': Invalid message block number '10': ZAK parity error '68': Command disabled or a standard error code.
MAB	16 H	Used as IV for next block when Message block number is '1' or '2'. Used as message authenticator when Message block number is '0' or '3'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate MAC (MAB) using ANSI X9.19 Method for a Large Message

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To generate a MAB for a large message using a TAK or ZAK.

Notes:

When using 8 hex-digit MACs, this command is superseded by host command 'M6'.

The MAC algorithm used is ANSI X9.19 using zero padding.

The command can operate on binary data or expanded Hex. If the HSM is set for Async/ASCII operation and binary data used ensure that:

The host port has been set for 8 data bit operation by the CH (Configure Host) console command.

The data for which the MAC is to be generated does not contain either EM (X'19) or ETX(X'03).

Expanded Hex mode uses 2 hexadecimal characters for each binary byte.

If the message block is the first or a middle block it must be a multiple of 8 bytes.

Consideration to the buffer size of the HSM must be made before the value n message length is selected.

When a MAC is required to be generated on a multi-block message, then the intermediate MABs will be encrypted under a key derived from the MAC key.

When generating a MAC using multiple message blocks (i.e. Message Block Number = '1', '2' or '3'), there is a minimum length to the separate message blocks:

- Each supplied message block must be at least 24 bytes (binary/text) or 48 hex characters.

© Thales UK Limited 2019

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MS'.
Message Block Number	1 N	Message block processing number: '0': Only Block '1': First Block '2': A Middle Block '3': Last Block.
Key Type	1 N	Key Type: '0': TAK (Terminal Authentication Key) '1': ZAK (Zone Authentication Key).
Key Length	1 N	Key length: 0 : Single Length DES Key 1 : Double Length DES Key.
Message Type	1 N	Message Type: '0': Message data is binary '1': Message data is expanded Hex.
Key	16 H or 'U' + 32 H or 'T' + 48 H	Key, encrypted under appropriate LMK pair. TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27.
IV	16 H	Initialization value, present only when Message block number is '2' or '3'.
Message Length	4 H	Length of message to be MAC'd (length of following field if message type binary; half the length of the following field if expanded hex).
Message Block	n B or H	The message block either in binary or as expanded Hex.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MT'.
Error Code	2 A	'00': No error '03': Invalid Message Type Code '04': Invalid Key Type Code '05': Invalid Message Block Number '06': Invalid Key Length Code '68': Command disabled or a standard error code.
MAB	16 H	Used as IV for next block when message block number is 1 or 2. Used as message authenticator when message block is 0 or 3.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate a Binary MAC

Function: Generate a MAC on a binary message using a TAK.

Note: This command is superseded by host command 'M6'.
The MAC algorithm used is ANSI X9.9 using zero padding.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MK'.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' ... '320' indicating the length of the data field (in hex).
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' ... '320' indicating the length of the data field (in hex).
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ML'.
Error Code	2 A	'00': No error '10': TAK parity error '68': Command disabled or a standard error code.
MAC	8 H	The computed MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a Binary MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a MAC on a binary message using a TAK.

Note: This command is superseded by host command 'M8'.

The MAC algorithm used is ANSI X9.9 using zero padding.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MM'.
TAK	16 H or 'U' + 32 H or 'T' + 48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' ... '320' indicating the length of the data field (in hex).
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' ... '320' indicating the length of the data field (in hex).
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MN'.
Error Code	2 A	'00': No error '01': MAC did not verify '10': TAK parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify and Translate a Binary MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a MAC on a binary message using a TAK, and if successful, generate a MAC on the same message with a different TAK.

Notes: This command is superseded by host command 'MY'.

The MAC algorithm used is ANSI X9.9 using zero padding.

If the verify fails no destination MAC is computed.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MO'.
Source TAK	16 H or 'U' + 32 H or 'T' + 48 H	The source TAK used to verify the MAC, encrypted under LMK 16-17.
Destination TAK	16 H or 'U' + 32 H or 'T' + 48 H	The destination TAK used to verify the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' ... '320' indicating the length of the data field (in hex).
Data	n B	Data to be MAC'd. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' ... '320' indicating the length of the data field (in hex).
Data	n H	Data to be MAC'd. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MP'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Source TAK parity error '11': Destination TAK parity error '68': Command disabled or a standard error code.
MAC	8 H	The computed MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate a MAC on a Binary Message

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate a MAC on a binary message.

Note: This command is superseded by host command 'M6'.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message to be MACed is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MU'.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block.
TAK	16 H or 1 A + 32/48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
Initialization Vector	16 H	Modes 2, 3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
	EITHER	
For Binary Communications Modes:		
Message length	3 H	'001' ... '320' indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
	OR	
For Standard Async Communications Mode:		
Message length	3 H	'002' ... '320' indicating the length of the next field.
Message	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MV'.
Error Code	2 A	'00': No error '10': TAK parity error '68': Command disabled or a standard error code.
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Present only in modes 0 and 3.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a MAC on a Binary Message

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a MAC on a binary message.

Note: This command is superseded by host command 'M8'.

If the Host is unable to support binary data transfers, the command can be used in standard 7-bit asynchronous mode, whereupon the message to be MACed is transferred in expanded hexadecimal notation.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MW'.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK 16-17.
Initialization Vector	16 H	Modes 2, 3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Modes 0, 3. The MAC received with the unsolicited message.
EITHER		
For Binary Communications Modes:		
Message length	3 H	'001' ... '320' indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	'002' ... '320' indicating the length of the next field.
Message	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MX'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': TAK parity error '68': Command disabled or a standard error code.
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

5. Legacy Message Encryption Commands

The payShield 10K provides the following host commands to support legacy message encryption operations:

Function	Command	Page
Encrypt Data Block	HE (HF)	107
Decrypt Data Block	HG (HH)	108

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Encrypt Data Block

Function: Encrypt a 64-bit data block with a TAK.

Notes: This command has been superseded by the M0 command, and should only be used where compatibility with legacy Host applications is required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HE'.
TAK	16 H or 1 A + 32/48 H	The TAK encrypted under LMK pair 16-17 variant 0.
Data	16 H	The data to be encrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'HF'.
Error Code	2 N	'00': No error '10': TAK parity error '12': No keys loaded in user storage '13': LMK error – report to supervisor '15': Error in input data '21': Invalid user storage or a standard error code.
Data	16 H	The data received in the command message encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Decrypt Data Block

Function: Decrypt a 64-bit data block with a TAK.

Notes: This command has been superseded by the M2 command, and should only be used where compatibility with legacy Host applications is required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HG'.
TAK	16 H or 1 A + 32/48 H	The TAK encrypted under LMK pair 16-17 variant 0.
Data	16 H	The data to be decrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'HH'.
Error Code	2 N	'00': No error '10': TAK parity error '12': No keys loaded in user storage '13': LMK error – report to supervisor '15': Error in input data '21': Invalid user storage or a standard error code.
Data	16 H	The data received in the command message decrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

6. Legacy DUKPT Commands

The payShield 10K provides the following host commands to support legacy DUKPT operations:

Function	Command	Page
Translate a PIN from BDK to ZPK Encryption (DUKPT)	CI (CJ)	110
Verify a PIN Using the IBM Offset Method (DUKPT)	CK (CL)	112
Verify a PIN Using the ABA PVV Method (DUKPT)	CM (CN)	115
Verify a PIN Using the Diebold Method (DUKPT)	CO (CP)	117
Verify a PIN Using the Encrypted PIN Method (DUKPT)	CQ (CR)	119

© Thales UK Limited 2019

Translate a PIN from BDK to ZPK Encryption (DUKPT)

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a PIN from encryption under the unique DUKPT key to encryption under an interchange key (ZPK) for transmission to another node.

This command supports the translation of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Translation*" has the value "Y".

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (G0).

The command performs the same function as CA and CC, except the Host supplies the HSM with the information necessary to compute the current key.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CI'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 'U' + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 'S' + n A	For a Key Block LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0' | **Algorithm**: 'T' | **Mode of Use**: 'N'
ZPK		The Zone PIN Key, used to re-encrypt the PIN block.
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 'S' + n A	For a Key Block LMK, the 'ZPK' must comply with the following: **Key Usage**: 'P0', '72' | **Algorithm**: 'D', 'T' | **Mode of Use**: 'B', 'E', 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see Chapter 4 of the *payShield 10K Host Programmer's Manual*.
Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. For further information on DUKPT, see Chapter 4 of the *payShield 10K Host Programmer's Manual*.
Source PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.

© Thales UK Limited 2019

Field	Length & Type	Details
Destination PIN Block Format Code	2 N	One of the following codes: '01': ANSI format '04': Plus format.
PAN/Token		If 'Source PIN Block' uses a token instead of the actual PAN, this field will contain the token number. Otherwise, it will contain the real PAN.
	18 H	If 'Destination PIN Block Format Code' = '04': The 18 digit PAN/Token excluding the check digit. If the PAN/Token is less than 18 digits, it must be right-justified and padded with 'F's on the left.
	or 12 N	For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the PAN/Token, excluding the check digit.
The following fields are required when the Source PIN Block was formed using a token (instead of the real PAN), and the Destination PIN Block needs to be formed using the real PAN.		
Destination PAN Delimiter	1 A	Value ';'. Optional; if present, the following field must be present. Only allowed if the security setting "*Enable use of Tokens in PIN Translation*" is set to "Y".
Destination PAN		Only present if 'Destination PAN Delimiter' is present.
	18 N	If 'Destination PIN Block Format Code' = '04': The 18 digit Destination PAN excluding the check digit. If the Destination PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.
	or 12 N	For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the Destination PAN, excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CJ'.
Error Code	2 A	'00': No error '10': BDK parity error '11': Interchange key parity error '27': BDK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN Length	2 N	Length of the translated PIN.
Encrypted PIN	16 H	The PIN block encrypted under the interchange key and formatted according to the destination PIN block format code.
Destination PIN block format code	2 N	Returned to the Host unchanged.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a PIN Using the IBM Offset Method (DUKPT)

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN using the IBM offset method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (GO).

The command performs the same function as DA and EA, plus it computes the PIN pad key. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

The plaintext decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned. Checking of the table is the default condition, but may be disabled using the CS console command. Disabling of the check is not recommended.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using TDES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

© Thales UK Limited 2019

<table>
<tr><th>Field</th><th>Length & Type</th><th>Details</th></tr>
<tr><td colspan="3">COMMAND MESSAGE</td></tr>
<tr><td>Message Header</td><td>m A</td><td>Subsequently returned to the Host unchanged.</td></tr>
<tr><td>Command Code</td><td>2 A</td><td>Value 'CK'.</td></tr>
<tr><td>BDK</td><td></td><td>The Base Derivation Key, used to decrypt the PIN block.</td></tr>
<tr><td></td><td>32 H
or
'U' + 32 H</td><td>For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.</td></tr>
<tr><td></td><td>or
'S' + n A</td><td>For a Key Block LMK, the 'BDK' must comply with the following:<table><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr><tr><td>'B0'</td><td>'T'</td><td>'N'</td></tr></table></td></tr>
<tr><td>PVK</td><td></td><td>The PIN Verification Key, used to verify the customer PIN.</td></tr>
<tr><td></td><td>16 H
or
'U' + 32 H
or
'T' + 48 H</td><td>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</td></tr>
<tr><td></td><td>or
'S' + n A</td><td>For a Key Block LMK, the 'PVK' must comply with the following:<table><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr><tr><td>'V1'</td><td>'D', 'T'</td><td>'C', 'V', 'N'</td></tr></table></td></tr>
<tr><td>KSN Descriptor</td><td>3 H</td><td>The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.</td></tr>
<tr><td>Key Serial Number</td><td>12 - 20 H</td><td>The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.</td></tr>
<tr><td>Source Encrypted PIN Block</td><td>16 H</td><td>Encrypted PIN block received from the POS PIN terminal.</td></tr>
<tr><td>Check Length</td><td>2 N</td><td>The minimum PIN length.</td></tr>
<tr><td>Account Number</td><td>12 N</td><td>The 12 right-most digits of the primary account number (PAN), excluding the check digit.</td></tr>
<tr><td>Decimalization Table</td><td>16 N
or
16 H
or
'K' + 3 H
or
'L' + 32 H</td><td>16 N when using Plaintext decimalization tables.
16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK.
'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area.
'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.</td></tr>
<tr><td>PIN Validation Data</td><td>12 A
or
'P' + 16 H</td><td>User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the account number;
or
User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.</td></tr>
<tr><td>Offset</td><td>12 H</td><td>The IBM offset value, left-justified and padded with 'F's.</td></tr>
<tr><td>Delimiter</td><td>1 A</td><td>Value '%'. Optional; if present, the following field must be present.</td></tr>
<tr><td>LMK Identifier</td><td>2 N</td><td>LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.</td></tr>
<tr><td>End Message Delimiter</td><td>1 C</td><td>Must be present if a message trailer is present. Value X'19.</td></tr>
<tr><td>Message Trailer</td><td>n A</td><td>Optional. Maximum length 32 characters.</td></tr>
</table>

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CL'.
Error Code	2 A	'00': No error '01': Verification failure '02': Warning PVK not single length (See the notes at the start of this section.0 '10': BDK parity error '11': PVK parity error '27': BDK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a PIN Using the ABA PVV Method (DUKPT)

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN using the ABA PVV method.

This command supports the verification of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Verification*" has the value "Y".

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (GQ).

The command performs the same function as DC and EC.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CM'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 'U' + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 'S' + n A	For a Key Block LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0' | **Algorithm**: 'T' | **Mode of Use**: 'N'
PVK		The PIN Verification Key, used to verify the customer PIN.
	32 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 'S' + n A	For a Key Block LMK, the 'PVK' must comply with the following: **Key Usage**: 'V2' | **Algorithm**: 'T' | **Mode of Use**: 'C', 'V', 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source Encrypted PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.

© Thales UK Limited 2019

Field	Length & Type	Details
PAN/Token	12 N	If 'PIN Block' uses a token instead of the PAN, this field will contain the Token Number. For all PIN Block formats, this is a 12 digit field, consisting of the 12 right-most digits of the PAN/Token Number, excluding the check digit.
The following 2 fields are required when the PIN Block was formed using a Token (instead of the real PAN), and the PIN Verification Value (PVV) needs to be formed using the real PAN.		
Verification PAN Delimiter	1 A	Value ';'. Optional; if present, the following field must be present. Only allowed if the security setting "*Enable use of Tokens in PIN Verification*" is set to "Y".
Verification PAN	12 N	Only present if 'Verification PAN Delimiter' is present. The 12 right-most digits of the PAN, excluding the check digit.
PVKI	1 N	The PIN Verification Key Indicator.
PVV	4 N	The PIN verification value from the card or data base.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CN'.
Error Code	2 A	'00': No error '01': Verification failure '10': BDK parity error '11': PVK parity error '27': BDK or PVK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a PIN Using the Diebold Method (DUKPT)

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN using the Diebold method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (GS).

The command performs the same function as CG and EG. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

The Diebold table must be stored in user storage before using this command.

- If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.
- If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CO'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 'U' + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 'S' + n A	For a Key Block LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0'; **Algorithm**: 'T'; **Mode of Use**: 'N'
Index Flag	1 A	Value 'K'.
Base Index	3 H	The index pointing to the start of the Diebold table in user storage.
Diebold Algorithm Number	2 H	The algorithm number required by the Diebold method.
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source Encrypted PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account Number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PIN Validation Data	16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the account number. The data must be right-justified and padded with 'F's.
Offset	4 N	The Diebold offset value.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CP'.
Error Code	2 A	'00': No error '01': Verification failure '10': BDK parity error '27': BDK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a PIN Using the Encrypted PIN Method (DUKPT)

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN using the Encrypted PIN method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (GU).

The command performs the same function as BC and BE. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CQ'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 'U' + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 'S' + n A	For a Key Block LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0'; **Algorithm**: 'T'; **Mode of Use**: 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source Encrypted Block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account Number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PIN	L N or L H or 'J' + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CR'.
Error Code	2 A	'00': No error '01': Verification failure '10': BDK parity error '27': BDK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

7. Legacy UnionPay Commands

The payShield 10K provides the following host commands to support Thales Watchword operations:

Function	Command	Page
ARQC Verification and/or ARPC Generation (UnionPay)	JS (JT)	122
Generate Secure Message with Integrity and optional Confidentiality (UnionPay)	JU (JV)	124

© Thales UK Limited 2019

ARQC Verification and/or ARPC Generation (UnionPay)

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Validate an ARQC (or TC/AAC) and, optionally, generate an ARPC. Alternatively, the command can be used to generate an ARPC alone.

Notes: Diagnostic data is produced by this command only if the HSM is in Authorised State. The diagnostic data consists of a generated ARQC, which is returned to the host if verification of the supplied ARQC fails.

Padding:

According to Part 5 of CUP doc (JR/T 0025.5-2010) Appendix D.2 and clarification from CUP, the data for ARQC calculation should be padded. If the data is multiple of 8 bytes, the padding bytes “hex 80 00 00 00 00 00 00 00” should be padded at the end of data. If the data is not multiple of 8 bytes, a padding byte “hex 80” and multiple bytes of hex 00 (between 0 and 7) to make padded data in multiple of 8 bytes.

A flag in this command allows application to control if the above padding rule is applied to the transaction data in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JS'.
Mode Flag	1 H	Mode of operation: 0 = Perform ARQC verification only 1 = Perform ARQC Verification and ARPC generation 2 = Perform ARPC Generation only
Scheme ID	1 N	Identifier of the CUP scheme 1 = CUP Card Key Derivation method (CUP ver4.2)
*MK-AC(LMK)	32 H or 1 A + 32 H	The Issuer Master Key for Application Cryptograms encrypted under Variant 1 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No.
ATC	2 B	Application Transaction Counter.
Padding Flag	1 N	Padding Flag to indicate if padding is applied to Transaction Data 0 = Input Transaction Data is not padded 1 = Input Transaction Data is padded Only present for Modes 0 and 1.
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes. Only present for Modes 0 and 1.
Transaction Data	n B	Variable length data. Only present for Modes 0 and 1. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional padding is added.
Delimiter	1A	Delimiter, to indicate end of Transaction Data, value “;”. Only present for Modes 0 and 1.
ARQC/TC/AAC	8 B	ARQC/TC/AAC to be validated and/or used for ARPC generation. Present for Mode 0, 1 and 2.
ARC	2 B	Authorisation Response Code to be used for ARPC Generation. **Not Required** for Mode Flag 0. Must be present for Mode Flag values '1' and '2'

© Thales UK Limited 2019

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JT'.
Error Code	2 N	00 : No error 01 : ARQC/TC/AAC verification failed 03 : Invalid Padding Flag 04 : Mode Flag not 0, 1 or 2 05 : Unrecognized Scheme ID 10 : MK parity error 67 : Command not licensed 80 : Data length error 81 : Zero length Transaction Data 82 : Transaction Data length not multiple of 8 bytes Any standard error code
ARPC	8 B	The calculated ARPC. Only present for Modes 1 and 2 if no error is encountered.
Diagnostic data	8 B	Calculated ARQC/TC/AAC returned only if the error code is 01 and the HSM is in Authorised State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate Secure Message with Integrity and optional Confidentiality (UnionPay)

Function: Generate a Secure Message with Integrity over data to be sent from the Issuer back to the Card. Optionally, Secure Messaging with Confidentiality for Message or Offline PIN Change.

Notes: Padding:

According to Part 5 of CUP doc (JR/T 0025.5-2010) Appendix C.2.4, the data for MAC calculation should be padded. If the data is multiple of 8 bytes, the padding bytes “hex 80 00 00 00 00 00 00 00” should be padded at the end of data. If the data is not multiple of 8 bytes, a padding byte “hex 80” and multiple bytes of hex 00 (between 0 and 7) to make padded data in multiple of 8 bytes.

A flag in this command allows application to control if the above padding rule is applied to the transaction data in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JU'.
Mode Flag	1 N	Mode of operation: 0 = Provide only Integrity functionality 1 = Provide Integrity and Confidentiality for message, using the same Issuer Master Key. 2 = Provide Integrity and Confidentiality for message, using different Issuer Master Keys 3 = Provide Integrity and Confidentiality for PIN Change, using the same Issuer Master Key. 4 = Provide Integrity and Confidentiality for PIN Change, using different Issuer Master Keys.
Scheme ID	1 N	Identifier of the CUP scheme; 1 = CUP using Card Key Derivation method (CUP ver 4.2)
*MK-SMI(LMK)	32 H or 1 A + 32 H	The Master Key for Secure Messaging with Integrity encrypted under Variant 2 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence number
ATC	2 B	Application Transaction Counter.
Padding Flag	1 N	Padding Flag to indicate if padding is applied to Plaintext Message Data 0 = Input Plaintext Message Data is not padded 1 = Input Plaintext Message Data is padded
MAC Message Data Length	4 H	Length in bytes of data in next field.
MAC Message Data	n B	MAC Message Data.
Delimiter	1 A	Delimiter of previous field, “;”.
*MK-SMC(LMK)	32 H or 1 A + 32 H	The Master Key for Secure Messaging with Confidentially encrypted under Variant 3 of LMK pair 28-29. Only present if Mode Flag = 2 or 4.
Offset	4 H	Position within MAC message data to insert Encrypted New PIN Block or re-encrypted data. Must be between 0000 and MAC Message Data length. If Offset = n, Encrypted New PIN Block or re-encrypted data is inserted AFTER the nth byte of the

© Thales UK Limited 2019

Field	Length & Type	Details
		MAC message data. (i.e. if length of Plaintext data or re-encrypted data is 0039, and Offset is 39, Encrypted New PIN Block is placed at the end of the plaintext message.) Only present if Mode Flag = 1, 2, 3 or 4.
Plaintext Message Data Length	4 H	Length in bytes of data in next field. Only present if Mode Flag = 1 or 2
Plaintext Message Data	n B	Plaintext Message Data. Only present if Mode Flag = 1 or 2
Delimiter	1 A	Delimiter of previous field, ";". Only present if Mode Flag = 1 or 2
Source PIN Encryption Key Type	1 N	0 = ZPK 1 = TPK Only present if Mode Flag = 3 or 4
Source PIN Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	Source PIN Encryption Key, encryption depending on the Source PIN Encryption Key Type:- ZPK: encrypted under LMK pair 06-07 variant 0 TPK: encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y" Only present if Mode Flag = 3 or 4
Source PIN Block Format	2 N	The format code for the source PIN block. Only Present if Mode Flag = 3 or 4.
Account Number	12 N or 18 H	Only Present if Mode Flag = 3 or 4. This field is used for PIN block translation. For a Source PIN Block Format ≠ 04, this field has length 12 N, and specifies the 12 right most digits of the account number, excluding the check digit. For a Source PIN Block Format = 04, this field has length 18 N, and specifies the entire 18 digit account number, excluding the check digit, padded with X'Fs on the left.
Destination PIN Block Format	1 N	The format code for the destination PIN block. 1 : destination PIN block with current (old) PIN 2 : destination PIN block without current (old) PIN Only Present if Mode Flag = 3 or 4.
Source New PIN Block	16 H	Source New PIN Block Only Present if Mode Flag = 3 or 4.
Source Current PIN Block	16 H	Source Current PIN Block Only Present if Mode Flag = 3 or 4 and Destination PIN Block Format = 1.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JV'.
Error Code	2 N	00 : No error 03 : Invalid Padding Flag 04 : Mode flag not set to 0, 1, 2, 3 or 4 05 : Unrecognised Scheme-ID 06 : Invalid Offset 09 : ZPK/TPK parity error 10 : MK-SMI parity error 11 : MK-SMC parity error 23 : Invalid Source PIN block format 50 : Source PIN Encryption Key Type, not set to 0 or 1 51 : Invalid Destination PIN Block Format 52 : Invalid Source New PIN Block 53 : Invalid Source Current PIN Block 67 : Command not licensed 80 : MAC Message Data length error 81 : Plaintext Message Data Length error 82 : Data length not multiple of 8 bytes Any standard error code
MAC	8 H	The calculated 4 byte MAC.
Encrypted Destination New PIN Block Data	32 H	Encrypted Destination New PIN Block Data Only Present if Mode Flag = 3 or 4.
Ciphertext Message Data Length	4 H	Ciphertext Message Data Length (i.e. length of next field) Only Present if Mode Flag = 1 or 2.
Ciphertext Message Data	n B	Ciphertext Message Data Only Present if Mode Flag = 1 or 2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

8. VisaCash Commands

This section describes the host commands which support the (legacy) VisaCash functionality.

Notes:

The use of the $ALGL_{IEP}$ and VKL_{IEP} fields in following commands deserves special mention as these fields are optional. There are three scenarios controlled by these fields.

Scenario	Applicable VisaCash cards	Single or Double length KDL used	Additional Notes
Neither VKL_{IEP} or $ALGL_{IEP}$ supplied to HSM	Version 1.5 and earlier DES cards	Single	May be used with cards which do not report VKL_{IEP} or $ALGL_{IEP}$. Backwards compatible with earlier versions of firmware
Only VKL_{IEP} supplied to HSM	Version 1.6 DES cards and Public Key cards	Double	May be used with later cards. Host must determine the value of $ALGL_{IEP}$ and supply VKL_{IEP} if required. Backwards compatible with earlier versions of firmware
Both VKL_{IEP} and $ALGL_{IEP}$ supplied to HSM	Any card.	Single if $ALGL_{IEP}$ has value 01, double if $ALGL_{IEP}$ has value 04	Allows host to send both $ALGL_{IEP}$ and VKL_{IEP} without concern about their values. VKL_{IEP} must always be supplied as a placeholder even if its value is not relevant (ie when $ALGL_{IEP}$ is of value 01)

This set of scenarios accommodates all relevant combinations of VisaCash cards and allows the host application to operate in one of two modes.

Host makes the decision about what $ALGL_{IEP}$ is relevant for the current transaction and either supplies VKL_{IEP} if $ALGL_{IEP}$ is of value 04, or does not supply VKL_{IEP} if $ALGL_{IEP}$ is of value 01. $ALGL_{IEP}$ itself is not sent to the HSM. Thus the first and second scenarios in the above table can be used to cater for all cards in use. This mode of operation is used by some (earlier) host systems and therefore must be supported for backwards compatibility. Note that earlier VisaCash cards do not report a value of $ALGL_{IEP}$ and so the host may have to determine this in other ways. Reference 4 discusses this point.

Host simply passes values of $ALGL_{IEP}$ and VKL_{IEP} to HSM as supplied in the current transaction. Thus if a card does not supply $ALGL_{IEP}$ or VKL_{IEP} no values are passed to the HSM and vice versa. Thus the first and third scenarios in the above table will be used. In this mode of operation the host is **Not Required** to make any decisions about the transaction; these are left to the HSM.

If Visa specifies alternative processing requirements in the future (and hence values of $ALGL_{IEP}$ other than 1 or 4) the HSM will be upgraded to accommodate them.

The earlier VisaCash cards which do not report $ALGL_{IEP}$ or VKL_{IEP} will all eventually expire making the first scenario in the above table redundant.

The payShield 10K provides the following host commands to support VisaCash operations:

Function	Command	Page
Verify Load Signature S1 and Generate Load Signature S2	DM (DN)	128
Verify Load Completion Signature S3	DO (DP)	130
Verify Unload Signature S1 and Generate Unload Signature S2	DQ (DR)	131
Verify Unload Completion Signature S3	DS (DT)	133

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Verify Load Signature S1 and Generate Load Signature S2

Function: Verify Load Signature S1 and generate Load Signature S2 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DM'.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
M_{LDA}	8 H	Amount to be loaded.
$CURR_{LDA}$	4 H	Load device currency code.
$CEXP_{LDA}$	2 H	Load device currency exponent.
BAL_{IEP}	8 H	IEP Current balance.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S_1	16 H	Load request signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DN'.
Error Code	2 A	'00': No error '01': S_1 verification failure '03': Invalid $ALGL_{IEP}$ '10': KML parity error '68': Command disabled or a standard error code.
S_2	16 H	Returned load signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify Load Completion Signature S3

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify Load Completion Signature S3 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DO'.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{IEP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC_{IEP}	4 H	Completion code.
S_3	16 H	Load completion signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DP'.
Error Code	2 A	'00': No error '01': S_3 verification failure '03': Invalid $ALGL_{IEP}$ '10': KML parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify Unload Signature S1 and Generate Unload Signature S2

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify Unload Signature S1 and generate Unload Signature S2 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DQ'.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{EP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
M_{LDA}	8 H	Amount to be unloaded.
$CURR_{LDA}$	4 H	Load device currency code.
$CEXP_{LDA}$	2 H	Load device currency exponent.
BAL_{EP}	8 H	IEP Current balance.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S_1	16 H	Unload request signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DR'.
Error Code	2 A	'00': No error '01': S_1 verification failure '03': Invalid $ALGL_{IEP}$ '10': KML parity error '68': Command disabled or a standard error code.
S_2	16 H	Returned unload signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify Unload Completion Signature S3

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify Unload Completion Signature S_3.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DS'.
KML	32 H or 'U' + 32 H or 'T' + 48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{EP}	4 H	IEP Transaction counter.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC_{IEP}	4 H	Completion code.
S_3	16 H	Unload completion signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DT'.
Error Code	2 A	'00': No error '01': S_3 verification failure '03': Invalid $ALGL_{IEP}$ '10': KML parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

9. Watchword Commands

The payShield 10K provides the following host commands to support Thales Watchword operations:

Function	Command	Page
Verify a Watchword Response	FU (FV)	135
Generate a Decimal MAC	LK (LL)	136
Verify a Decimal MAC	LM (LN)	137

© Thales UK Limited 2019

Verify a Watchword Response

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a Watchword response.

Notes: The cipher scheme used depends upon the key length.
Single length WWK – Cipher scheme code 0
Double length WWK – Cipher scheme code 1
Triple length WWK – Cipher scheme code 2

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FU'.
WWK		The Watchword Key, used to generate the response.
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'WWK' must be encrypted under LMK pair 22-23.
	or 'S' + n A	For a Key Block LMK, the 'WWK' must comply with the following: **Key Usage**: '01'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'C', 'V', 'N'
Flag	1 N	'1': response for PIN 1 '2': response for PIN 2.
Challenge	7 N	Watchword challenge.
Response	7 N	Watchword response.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FV'.
Error Code	2 A	'00': No error '01': Watchword Response verification failure '10': WWK parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate a Decimal MAC

Function: Generate a Decimal MAC on data.

Notes: This command assumes that the data on which the MAC is to be generated consists of characters only.

The cipher scheme used depends upon the key length.

Single length TAK – Cipher scheme code 0 (X9.9 MAC)

Double length TAK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LK'.
TAK		The Terminal Authentication Key, used to generate the MAC.
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'TAK' must be encrypted under LMK pair 16-17.
	or 'S' + n A	For a Key Block LMK, the 'TAK' must comply with one of the following: **Key Usage** / **Algorithm** / **Mode of Use** 'M1' / 'D' / 'C', 'G', 'N' 'M3' / 'T' / 'C', 'G', 'N'
MAC Length	1 H	Number of characters required in Decimal MAC (range 1 to 12).
Data	0 - n	The data on which a MAC is to be generated, n = 16K Must not contain a '~' character.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LL'.
Error Code	2 A	'00': No error '10': TAK parity error '68': Command disabled or a standard error code.
MAC	n N	The calculated decimal MAC with a length as specified in the command.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a Decimal MAC

Variant LMK ☑	Key Block LMK ☑
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To verify a decimal MAC of user defined length

Notes: This command assumes that the data on which the MAC is to be generated consists of characters only

The cipher scheme used depends upon the key length.

Single length TAK – Cipher scheme code 0 (X9.9 MAC)

Double length TAK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LM'.
TAK		The Terminal Authentication Key, used to verify the MAC.
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'TAK' must be encrypted under LMK pair 16-17.
	or 'S' + n A	For a Key Block LMK, the 'TAK' must comply with one of the following: **Key Usage** / **Algorithm** / **Mode of Use** 'M1' / 'D' / 'C', 'V', 'N' 'M3' / 'T' / 'C', 'V', 'N'
MAC length	1 H	The number of characters in the Decimal MAC (range 1 – 12).
MAC	n N	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n = 16K. Must not contain a '~' character.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LN'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': TAK parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

10. Legacy WebPIN Commands

The payShield 10K provides the following legacy host commands to support older versions of the WebPIN product:

Function	Command	Page
Verify PIN Block from Internet and Verify MAC	XK (XL)	140
Verify PIN Block from Internet, Verify MAC & Return New Encrypted PIN	XM (XN)	142
Verify MAC	XO (XP)	144
Generate MAC	XQ (XR)	146
Translate PIN Block from Internet, Verify MAC and Optionally Generate a MAC	XS (XT)	148
Decrypt Data	XU (XV)	150
Encrypt Data	XW (XX)	152

© Thales UK Limited 2019

Verify PIN Block from Internet and Verify MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To verify ISO PIN Block from Internet and verify MAC using ANSI X9.19.

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key and MAC Keys (both 128-bit) are derived from a Master Key encrypted under public key.

The PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XM'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be '01' for RSA. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*.
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be '01' for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*.
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except '99' which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is '99').
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is '99').
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is '99').
Account Number	12 N	Account number for formation of locally stored encrypted PIN.
PIN	L N or L H	The locally stored PIN encrypted under LMK pair 02-03.
PIN and MAC Message Length	4 N	Length of PIN and MAC Message
PIN and MAC Message	n A	PIN and MAC Message as received from client – see Appendix A for Format
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XN'.
Error Code	2 N	'00': No errors. '01': PIN verification failure. '02': MAC Verification Failure. '03': Invalid private key type. '04': Invalid private key flag. '06': Invalid encryption identifier. '07': Invalid pad mode identifier. '13': LMK error; report to supervisor. '14': Error in PIN from Host. '15': Error in input data. '20': PIN Block Error. '21': Invalid user storage index. '24': PIN Length error. '47': DSP error; report to supervisor. '49': Private Key error; report to supervisor. '76': Key block length error. '77': Clear data block error. '78': Private Key length error. '80': Incorrect Message Length. '83': Invalid Ver or Type in Message '84': Invalid Ver or Usage in Master Key Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify PIN Block from Internet, Verify MAC & Return New Encrypted PIN

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To verify ISO PIN Block from Internet, verify MAC using ANSI X9.19 and return New PIN.

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt – Encrypt). The Session PIN Key and MAC Key (both 128-bit) are derived from a Master Key encrypted under the public key.

Both old PIN and new PIN are supplied. After successful verification of old PIN, new PIN is translated to encryption under the LMK.

The Change PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XK'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be '01' for RSA. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be '01' for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except '99' which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is '99').
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is '99').
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is '99').
Account Number	12 N	Account number for formation of locally stored encrypted PIN.
PIN	L N or L H	The locally stored PIN encrypted under LMK pair 02-03.
Change PIN and MAC Message Length	4 N	Length of Change PIN and MAC Message
Change PIN and MAC Message	n A	Change PIN and MAC Message as received from client – see Appendix A for Format
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XL'.
Error Code	2 N	'00': No error '01': PIN verification failure Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To verify MAC using ANSI X9.19.

Notes: The Session MAC Key (128-bit) is itself encrypted under public key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XO'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the DES Key.
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process.
Encrypted MAC Key Length	4 N	Encrypted MAC Key Length (in bytes).
MAC Key	n B	MAC Key, encrypted under the public key.
Delimiter	1 A	Delimiter, indicates the end of the encrypted PIN Key field. Value ;
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except '99' which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is '99').
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is '99').
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is '99').
MAC	8 H	MAC.
Authentication Data Length	4 N	Length of Data to be authenticated.
Authentication Data	n A	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
		RESPONSE MESSAGE
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XP'.
Error Code	2 N	'00': No errors. '02': MAC Verification Failure. '03': Invalid private key type. '04': Invalid private key flag. '06': Invalid encryption identifier. '07': Invalid pad mode identifier. '10': MAC Key parity error. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '47': DSP error; report to supervisor. '49': Private Key error; report to supervisor. '76': Key block length error. '77': Clear data block error. '78': Private Key length error. '80': Incorrect Data Length. Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate MAC

Function: To Generate MAC using ANSI X9.19.

Notes: The Session MAC Key (128-bit) is itself encrypted under public key.

The Encryption Identifier should be 01 (i.e. RSA algorithm). The Pad Mode Identifier should also be 01 (i.e. PKCS#1).

All message authentication functions supported by the HSM use ASCII characters. If the host is using EBCDIC character set and the HSM is configured using EBCDIC, the HSM will convert the incoming EBCDIC MAC data to ASCII characters, prior to MAC verification/generation. (Please refer to the EBCDIC-to-ASCII translation table in HSM Programmer's Manual.) If the final message block of the authentication data is not an exact multiple of 64 bits, it will be padded, to the right, with binary zeros.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XQ'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the DES Key.
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process.
PK MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37 with Variant 1.
Public Key	n B	Public Key, DER encoded in ASN.1 format (sequence of modulus, exponent).
PK Authentication Data	n A	Optional. Additional data to be included in the PK MAC calculation for Public Key (must not include ';').
Delimiter	1 A	Delimiter, indicates the end of the PK authentication data field. Value ';'.
Authentication Data Length	4 N	Length of Data to be authenticated.
Authentication Data	n A	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value XR'.
Error Code	2 N	'00': No errors. '01': Public Key MAC Verification failure. '04': Public key does not conform encoding rules. '06': Invalid encryption identifier. '07': Invalid pad mode identifier. '13': LMK error; report to supervisor. '15': Error in input data. '47': DSP error; report to supervisor. '76': Public Key length error. '80': Incorrect Data Length. Or any standard error code
MAC	8 H	MAC.
Encrypted MAC Key Length	4 N	Encrypted MAC Key Length (in bytes).
MAC Key	n B	MAC Key, encrypted under the public key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate PIN Block from Internet, Verify MAC and Optionally Generate a MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To translate ISO PIN Block from Internet, verify MAC using ANSI X9.19 and optionally generate MAC using ANSI X9.9 or X9.19. The ZPK and ZAK can be 1, 2 or 3DES in the form of 16Hex, 1A+32Hex or 1A+48Hex.

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The input PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key and MAC Keys (both 128-bit) are derived from a Master Key encrypted under public key.

The Encryption Identifier should be 01 (i.e. RSA algorithm). The Pad Mode Identifier should also be 01 (i.e. PKCS#1).

All message authentication functions supported by the HSM use ASCII characters. If the host is using EBCDIC character set and the HSM is configured using EBCDIC, the HSM will convert the incoming EBCDIC MAC data to ASCII characters, prior to MAC verification/generation. (Please refer to the EBCDIC-to-ASCII translation table in HSM Programmer's Manual.) If the final message block of the authentication data is not an exact multiple of 64 bits, it will be padded, to the right, with binary zeros.

The PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XS'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be '01' for RSA. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be '01' for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See *payShield 10K Host Programmer's Manual, RSA Cryptosystem*
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except '99' which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is '99').
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is '99').
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value ';' (present only if the private key flag is '99').
MAC Flag	1 N	Flag to indicate MAC Generation '1': MAC Verification only '3': MAC Verification and Generation
Destination ZPK	16 H or 1A+32H or 1A+48H	Destination ZPK, encrypted under LMK pair 06-07.
PIN and MAC Message Length	4 N	Length of PIN and MAC Message
PIN and MAC Message	n A	PIN and MAC Message as received from client – see Appendix A for Format
Delimiter	1 A	Value ';'.
Destination ZAK	16 H or 1A+32H or 1A+48H	Destination ZAK, encrypted under LMK pair 26-27. (only present if MAC Flag is '3')
Output Authentication Data Length	4 N	Length of output authentication data to be authenticated (only present if MAC Flag is '3')

© Thales UK Limited 2019

Field	Length & Type	Details
Output Authentication Data	n A	Output data to be authenticated. (only present if MAC Flag is '3')
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XT'.
Error Code	2 N	'00': No errors. '02': MAC Verification Failure. '03': Invalid private key type. '04': Invalid private key flag. '06': Invalid encryption identifier. '07': Invalid pad mode identifier. '10': Destination ZPK parity error. '11': Destination ZAK parity error. '12': No Keys loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '20': PIN Block Error. '21': Invalid user storage index. '24': PIN Length error. '47': DSP error; report to supervisor. '49': Private Key error; report to supervisor. '76': Key block length error. '77': Clear data block error. '78': Private Key length error. '80': Incorrect input message length. '81': Incorrect output data length. '83': Invalid Ver or Type in Message '84': Invalid Ver or Usage in Master Key Or any standard error code
PIN Block	16 H	PIN Block, encrypted under Destination ZPK.
Destination MAC	8 H	Destination MAC, calculated using Destination ZAK. (only present if MAC Flag is 3)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Decrypt Data

Function: To decrypt data from Internet.

Notes: The input Data Block is encrypted by a 128-bit session data key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session Data Key (128-bit) from Internet is encrypted under public key. The data key should be translated to LMK pair 30-31 encryption by standard command “GI”.

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard.

The TCBC mode requires an Initialization Value (IV) to be input with the command. When more than one message block needs to be decrypted, then the final 8 bytes of ciphertext obtained from the previous message block will be returned to the host for use as the IV for the next message block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XU'.
Message Block Number	1 N	Message block processing number '0': Only block '1': First block '2': Second block '3': Last block
Decryption Mode	1 N	Mode of operation '0': ECB '1': CB
Data Key	32 H	TDES Data Key encrypted under LMK pair 30-31.
IV	16 H	Initialization Value.
Encrypted Message Length	5 N	Message length, in bytes.
Encrypted Message Block	n B	The cipher text message block
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XV.
Error Code	2 N	'00': No errors. '04': Invalid mode of operation. '05': Invalid Message Block Number. '09': Data Key Parity error. '12': No Keys loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '80': Incorrect input data length. Or any standard error code
Decrypted Message Block	n B	The decrypted message block.
IV	16 H	Initialization Value, to be used as IV for the next message block. (only returned if Message Block Number = 1 or 2)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Encrypt Data

Function: To encrypt data.

Notes: The input Data Block will be encrypted by a 128-bit session data key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session Data Key (128-bit) from Internet is encrypted under public key. The data key should be translated to LMK pair 30-31 encryption by standard command “GI”.

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard.

The TCBC mode requires an Initialisation Value (IV) to be input with the command. When more than one message block needs to be encrypted, then the final 8 bytes of ciphertext obtained from the previous message block will be returned to the host for use as the IV for the next message block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XW'.
Message Block Number	1 N	Message block processing number '0': Only block '1': First block '2': Second block '3': Last block
Decryption Mode	1 N	Mode of operation '0': ECB '1': CBC
Data Key	32 H	TDES Data Key encrypted under LMK pair 30-31.
IV	16 H	Initialization Value.
Message Length	5 N	Message length, in bytes.
Message Block	n B	The plaintext message block
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XX'.
Error Code	2 N	'00': No errors. '04': Invalid mode of operation. '05': Invalid Message Block Number. '09': Data Key Parity error. '12': No Keys loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '80': Incorrect input data length. Any standard error code
Encrypted Message Block	n B	The encrypted message block.
IV	16 H	Initialization Value, to be used as IV for the next message block. (only returned if Message Block Number = 1 or 2)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

11. SEED Algorithm Commands

These commands provide support for the SEED key block cipher developed by KISA (Korea Information Security Agency).

The HSM supports the use of SEED keys using the key scheme “J”:

Key Scheme Tag	Notes
J	Encryption of 128-bit SEED keys using the Thales Variant LMK.

The following host commands support the use of SEED keys using the “J” key scheme:

A0, A6, A8, AI, AK, AM, AO, G2, G4, G6, G8

The following console commands support the use of SEED keys using the “J” key scheme:

GC, FK, KG, KE, IK

Note: The procedure for generating a key check value for a SEED key is not currently defined, and therefore all SEED keys will have a key check value of “000000”.

The payShield 10K provides the following host commands to support the Korean SEED algorithm:

Function	Command	Page
Verify an Interchange PIN using the comparison method with SEED encryption algorithm	G2 (G3)	155
Verify a Terminal PIN using the comparison method with SEED encryption algorithm	G4 (G5)	156
Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm	G6 (G7)	157
Translate a PIN from TPK to ZPK with SEED encryption algorithm	G8 (G9)	159
Encrypt Data Block with SEED algorithm	AI (AJ)	161
Decrypt Data Block with SEED algorithm	AK (AL)	163
Translate Data Block with SEED algorithm	AM (AN)	165
Generate Round Key from SEED Key	AO (AP)	167

© Thales UK Limited 2019

Verify an Interchange PIN using the comparison method with SEED encryption algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN received from interchange by comparing it with a value held on the host database

Notes: This command is similar to standard host command “BE” in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is a block cipher with 16 bytes output and input. As the standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is added at the end of the PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is **Not Required** to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G2'.
ZPK	1A+32H	For a Variant LMK, the ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the “J” key scheme.
PIN Block	32 H	The PIN block containing the PIN for verification; encrypted under the ZPK
PIN Block format code	2 N	One of the valid PIN block format codes – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H	The PIN from the host database encrypted under the LMK
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'G3'.
Error Code	2 N	'00': No error '01': PIN verification failure Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Verify a Terminal PIN using the comparison method with SEED encryption algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Verify a PIN receive from an ATM (or terminal etc.) by comparing it with a value held on the host database

Notes: This command is similar to standard host command “BC” in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is **Not Required** to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G4'.
TPK	1A+32H	For a Variant LMK, the TPK must be encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N” or LMK pair 36-37 variant 7 if the setting has the value “Y”. Note: All SEED keys must use the “J” key scheme.
PIN Block	32 H	The PIN block containing the PIN for verification; encrypted under the ZPK
PIN Block format code	2 N	One of the valid PIN block format codes – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H	The PIN from the host database encrypted under the LMK
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'G5'.
Error Code	2 N	'00': No error '01': PIN verification failure Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a PIN Block from encryption under one ZPK to encryption under another ZPK and from one format to another. If the same ZPK is defined, only the PIN block is translated, and if the same PIN block format is defined, only the key is translated.

Notes: This command is similar to standard host command “CC” in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is **Not Required** to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G6'.
Source ZPK	1A+32H	For a Variant LMK, the Source ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the “J” key scheme.
Destination ZPK	1A+32H	For a Variant LMK, the Destination ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the “J” key scheme.
Maximum PIN Length	2 N	Value '12'.
Source PIN Block	32 H	The source PIN block encrypted under the source ZPK.
Source PIN Block Format Code	2 N	One of the valid PIN block format codes for source PIN Block – see Chapter 6 of the General Information Manual for details.
Destination Source PIN Block Format Code	2 N	One of the valid PIN block format codes for destination PIN Block – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'G7'.
Error Code	2 N	'00': No error Or any standard error code
PIN Length	2 N	Length of the returned PIN
Destination PIN Block	32 H	The destination PIN block encrypted under the destination ZPK
Destination PIN Block Format code	2 N	As received in the command message
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Translate a PIN from TPK to ZPK with SEED encryption algorithm

Function: Translate a PIN Block from encryption under TPK to encryption under another ZPK and from one format to another. If the same PIN block format is defined, only the key is translated.

Notes: This command is similar to standard host command “CA” in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is **Not Required** to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G8'.
Source TPK	1A+32H	For a Variant LMK, the Source TPK must be encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N” or LMK pair 36-37 variant 7 if the setting has the value “Y”. Note: All SEED keys must use the “J” key scheme.
Destination ZPK	1A+32H	For a Variant LMK, the Destination ZPK must be encrypted under LMK pair 06-07. Note: All SEED keys must use the “J” key scheme.
Maximum PIN Length	2 N	Value '12'.
Source PIN Block	32 H	The source PIN block encrypted under the source TPK.
Source PIN Block Format Code	2 N	One of the valid PIN block format codes for source PIN Block – see Chapter 6 of the General Information Manual for details.
Destination Source PIN Block Format Code	2 N	One of the valid PIN block format codes for destination PIN Block – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'G9'.
Error Code	2 N	'00': No error Or any standard error code
PIN Length	2 N	Length of the returned PIN
Destination PIN Block	32 H	The destination PIN block encrypted under the destination ZPK
Destination PIN Block Format code	2 N	As received in the command message
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Encrypt Data Block with SEED algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Encrypt a block of data with SEED algorithm.

Notes: This command is similar to standard host command “M0” in input/output and command processing. But the algorithm is SEED algorithm.

If a ZEK is used as the encryption key, the contents of the plaintext message must comply with the CS “ZEK encryption” setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK key is used.

The data to be encrypted by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

Note: When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

Note: No padding is applied – the input message must be a multiple of 16 (or 32 for hex-encoded messages).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AI'.
Mode Flag	2 N	Describes the encryption mode: '00': ECB '01': CBC (requires IV) '02': CFB8 (requires IV) '03': CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the input message: '0': Binary '1': Hex-Encoded Binary '2': Text.
Output Format Flag	1 N	Describes the format of the output message: '0': Binary '1': Hex-Encoded Binary
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33).
Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the “J” key scheme.
IV	32 H	The input IV, used in conjunction with the encryption Key. When encrypting the first of a series of blocks, this initial IV should be set by the caller – a typical initial IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the IV returned from encrypting the previous block. Only present if the Mode Flag is '01', '02' or '03'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Message	n B or n H or n A	The message to be encrypted. The length & type of the field will depend on the value of the Input Format Flag: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32. Input Format Flag = '2' (Text); n = multiple of 16.

© Thales UK Limited 2019

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AJ'.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
IV	32 H	The output IV. When encrypting a series of blocks, this IV should be supplied as input when encrypting the next block. Only present if the Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Encrypted Message	n B or n H	The encrypted message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Decrypt Data Block with SEED algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Decrypt a block of data with SEED algorithm.

Notes: This command is similar to standard host command “M2” in input/output and command processing. But the algorithm is SEED algorithm.

If a ZEK is used as the encryption key, the contents of the plaintext message must comply with the CS “ZEK encryption” setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK key is used.

The decrypted data block may be returned to the host in different formats, as indicated by the Output Format Flag field.

Note: When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

Note: No padding is applied – the input message must be a multiple of 16 (or 32 for hex-encoded messages).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AK'.
Mode Flag	2 N	Describes the encryption mode: '00': ECB '01': CBC (requires IV) 02': CFB8 (requires IV) '03': CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the output message: '0': Binary '1': Hex-Encoded Binary
Output Format Flag	1 N	Describes the format of the input message: '0': Binary '1': Hex-Encoded Binary '2': Text.
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33).
Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the “J” key scheme.
IV	32 H	The input IV, used in conjunction with the encryption Key. When encrypting the first of a series of blocks, this initial IV should be set by the caller – a typical initial IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the IV returned from encrypting the previous block. Only present if the Mode Flag is '01', '02' or '03'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Encrypted Message	n B or n H	The encrypted message. The type of the message will depend on the value of the Format Flag field: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.

© Thales UK Limited 2019

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AL.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
IV	32 H	The output IV. When decrypting a series of blocks, this IV should be supplied as input when encrypting the next block. Only present if the Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Decrypted Message	n B or n H or n A	The decrypted message. The type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32. Output Format Flag = '0' (Text); n = multiple of 16.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Translate Data Block with SEED algorithm

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Translate a block of data from encryption under one key, to encryption under another key with SEED algorithm.

Notes: This command is similar to standard host command “M4” in input/output and command processing. But the algorithm is SEED algorithm.

The data to be translated by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

The translated data block may be returned to the host in different formats, as indicated by the Output Format Flag field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AM'.
Source Mode Flag	2 N	'00': ECB '01': CBC (requires IV) '02': CFB8 (requires IV) '03': CFB128 (requires IV).
Destination Mode Flag	2 N	'00': ECB '01': CBC (requires IV) '02': CFB8 (requires IV) '03': CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the output message: '0': Binary '1': Hex-Encoded Binary
Output Format Flag	1 N	Describes the format of the input message: '0': Binary '1': Hex-Encoded Binary
Source Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33).
Source Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the “J” key scheme.
Destination Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33).
Destination Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the “J” key scheme.
Source IV	32 H	The source IV, used in conjunction with the source Key. When translating the first of a series of blocks, this initial Source IV should match the initial IV used to encrypt the original message. For subsequent blocks, this value should be the Source IV returned from translating the previous block. Only present if the Mode Flag is '01', '02' or '03'.
Destination IV	32 H	The input IV, used in conjunction with the Destination Key. When translating the first of a series of blocks, this initial Destination IV should be set by the caller – a typical value IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the Destination IV returned from translating the previous block. Only present if the Destination Mode Flag is '01', '02' or '03'.

© Thales UK Limited 2019

Field	Length & Type	Details
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Encrypted Message	n B or n H	The encrypted message. The type of the message will depend on the value of the Format Flag field: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AN'.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
Source IV	32 H	The output IV, calculated using the Source Key. When translating a series of blocks, this Source IV should be supplied as input when encrypting the next block. Only present if the Source Mode Flag is 01, 02 or 03.
Destination IV	32 H	The output IV, calculated using the Destination Key. When translating a series of blocks, this Destination IV should be supplied as input when encrypting the next block. Only present if the Destination Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Translated Message	n B or n H	The translated message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate Round Key from SEED Key

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Required** Activity: **command.AO.host**	

Function: Generate round key from SEED Key with key scheduling function in SEED algorithm.

Notes: This command is used for testing purposes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AO'.
SEED Key	1A+32H	For a Variant LMK, the Seed Key must be encrypted under LMK pair 30-31 Note: All SEED keys must use the "J" key scheme.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AP'.
Error Code	2 N	00 : No error 67 : Command not licensed 68 : command disabled Any standard error code
Round Key	256 H	Round Key
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

12. CEPS Commands

The payShield 10K provides the following host commands to support the WebPIN product:

Function	Command	Page
Decrypt R1 and validate the MACLSAM	U0 (U1)	169
Compute HCEP	U2 (U3)	171
Validate the S1 MAC (Load and Unload)	U4 (U5)	172
Validate the S1 MAC (Currency Exchange)	U6 (U7)	174
Generate the S2 MAC (Linked load, declined unlinked load, unload)	U8 (U9)	176
Generate the S2 MAC (Currency Exchange)	V0 (V1)	177
Generate the S2 MAC (Approved Unlinked Load)	V2 (V3)	178
Validate the S3 MAC (Currency Exchange transactions)	V4 (V5)	179
Validate the S3 MAC (Load or Unload transactions)	V6 (V7)	181
Validate the H2LSAM	V8 (V9)	183
Unlinked Load Transaction Request	T0 (T1)	184
Release RLSAM	T2 (T3)	186
Release R2LSAM	T4 (T5)	187
Verify RCEP	T6 (T7)	188
Validate S6 MAC	W0 (W1)	189
Validate S6' MAC	W2 (W3)	190
Validate S6'' MAC	W4 (W5)	191
Validate S5',DLT MAC	W6 (W7)	192
Validate S5',ISS MAC	W8 (W9)	193
Validate the S4 MAC (Old Terminals)	X0 (X1)	194
Validate the S4 MAC (New Terminals)	X2 (X3)	195
Validate the S5 MAC (Old Terminals)	X4 (X5)	196
Validate the S5' MAC (MAC of the PSAM for a Transaction) (New Terminals)	X6 (X7)	197
Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals)	X8 (X9)	199
Create the Acknowledgement MAC (Old Terminals)	Y0 (Y1)	201
Create the Acknowledgement MAC (New Terminals)	Y2 (Y3)	202
Create the Update MAC	Y4 (Y5)	203
Validate the SADMIN MAC (Administrative MAC of the PSAM)	Y6 (Y7)	204
Create the Merchant Acquirer MAC	Y8 (Y9)	205
Validate the Card Issuer MAC	Z0 (Z1)	206
Export Electronic Purse Card Key Set	R2 (R3)	207

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Decrypt R_1 and validate the MAC_{LSAM}

Function: To decrypt R_1 and validate the MAC_{LSAM}.

Notes: This command is complementary to the SA command in the Load Acquirer commands that generates the encrypted R_1.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U0'.
TPK	16 H or 1 A + 32 H	The Terminal PIN key encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". A single length TPK will be input as 16 hexadecimal characters. A double length TPK will be input as a 'U' character followed by 32 hexadecimal characters.
R_1Length	1 N	The length of the key R_1: '1': single length '2': double length.
R_1	16 / 32 H	The session key encrypted under the TPK.
DD_{CEP}Length	1 B	The length in bytes of the DD_{CEP} field. The length is specified in binary and must be in the range 00H to 20H (equivalent to 0 to 32 decimal).
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the card.
$CURR_{LDA}$	3 B	The Currency Indicator.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
S1	8 B	The CEP Card signature produced by the card during 'Card Initialise for Load'.
H_{CEP}	10 B	The SHA-1 Hash generated by the CEP card on the Load Transaction data.
H_{LSAM}	8 B	SHA-1 hash of internally generated R_{LSAM}.
$H2_{LSAM}$	8 B	SHA-1 hash of internally generated $R2_{LSAM}$.
DD_{CEP}	0 - 32 B	Discretionary Data.
MAC_{LSAM}	4 B	EMV MAC of Transactional data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'U1'.
Error Code	2 N	'00': No error (MAC validated successfully) '01': MAC validation failed '11': TPK parity error '70': Invalid R_1Length code '72': R_1 Parity Error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Compute H_{CEP}

Function: Create R_{CEP} and use the SHA-1 algorithm to compute H_{CEP}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U2'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'U3'.
Error Code	2 N	'00': No error '10': KML parity error or a standard error code, as listed in Chapter 4 of [2].
H_{CEP}	10 B	SHA hash of input data and R_{CEP} .
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_1 MAC (Load and Unload)

Function: Validate the S_1 MAC for load and unload transactions.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U4'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
TI	1 B	Transaction Indicator: '0C': load transactions '0A': unload transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$NT_{LASTLOAD}$	2 B	Transaction number of last load.
$NT_{LASTCANCEL}$	2 B	Transaction number of last cancel.
$CSTAT_{CEP}$	2 B	Card Status.
$TLfail_{CEP}$	1 B	Tag and length of failed update.
$DEXP_{CEP}$	3 B	Expiry date of the card, YYMMDD.
BAL_{CEP}	4 B	Balance of slot prior to completion.
$BALmax_{CEP}$	4 B	Maximum balance of the slot.
PVS_{CEP}	1 B	PIN verification status.
S_1	8 B	Signature for verification.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'U5'.
Error Code	2 N	'00': No error (S_1 validated successfully) '01': S_1 validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate the S_1 MAC (Currency Exchange)

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Validate the S_1 MAC for currency exchange transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U6'.
*KMX	32 H or 1 A + 32 H	Double length KMX encrypted under LMK pair 20-21 variant 2.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
TI	1 B	Transaction Indicator: '08' for currency exchange transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{SOURCE}$	3 B	The Currency Code for the source slot.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$NT_{LASTLOAD}$	2 B	Transaction number of last load.
$NT_{LASTCANCEL}$	2 B	Transaction number of last cancel.
$CSTAT_{CEP}$	2 B	Card Status.
$TLfail_{CEP}$	1 B	Tag and Length of failed update.
$DEXP_{CEP}$	3 B	Expiry date of the card, YYMMDD.
$CURR_{TARGET}$	3 B	The Currency Code.
BAL_{TARGET}	4 B	Balance of target slot .
$BALmax_{TARGET}$	4 B	Maximum balance of the target slot.
BAL_{SOURCE}	4 B	Balance of source slot.
S_1	8 B	Signature for verification.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'U7'.
Error Code	2 N	'00': No error (S_1 validated successfully) '01': S_1 validation failed '10': KDX parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate the S_2 MAC (Linked load, declined unlinked load, unload)

Function: Generate the S_2 MAC for Linked Load, Declined Unlinked Load or Unload transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U8'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $UPDATES_{ISS}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: '0C': Linked Load or Declined Unlinked Load transactions '0A': unload transactions.
S_1	8 B	Signature.
BAL_{ISS}	4 B	Balance of card for this currency.
$BALmax_{ISS}$	4 B	Maximum balance of the target slot.
$CALPHA_{ISS}$	3 B	Alphanumeric currency code.
$UPDATES_{ISS}$	0 - 24 B	Updates to CEP card data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'U9'.
Error Code	2 N	'00': No error '10': *KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Generate the S_2 MAC (Currency Exchange)

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Generate the S_2 MAC for currency exchange transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V0'.
*KMX	32 H or 1 A + 32 H	Double length *KMX encrypted under LMK pair 20-21 variant 2.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $UPDATES_{ISS}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: '08': currency exchange transactions
S_1	8 B	Signature.
$BAL_{ISS,TARGET}$	4 B	New Balance of target slot.
$BALmax_{ISS,TARGET}$	4 B	Maximum balance of the target slot.
$CALPHA_{ISS,\ TARGET}$	3 B	Alphanumeric representation of the target currency code.
$BAL_{ISS,SOURCE}$	4 B	New Balance of the source slot.
$UPDATES_{ISS}$	0 - 24 B	Updates to CEP card data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'V1'.
Error Code	2 N	'00': No error '10': KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Generate the S_2 MAC (Approved Unlinked Load)

Function: Generate the S_2 MAC for unlinked load transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V2'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $UPDATES_{ISS}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: '0C': unlinked load transactions.
S_1	8 B	S1 Signature.
BAL_{ISS}	4 B	Balance of CEP card.
$BALmax_{ISS}$	4 B	Maximum balance of the target slot.
$CALPHA_{ISS}$	3 B	Alphanumeric representation of the currency code for this slot.
H_{LSAM}	8 B	Left 8 bytes from SHA-1 hash of: ID_{LACQ},ID_{LDA},ID_{ISS},ID_{CEP},NT_{CEP},R_{LSAM}
$UPDATES_{ISS}$	0 - 24 B	Updates to CEP card data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'V3'.
Error Code	2 N	'00': No error '10': KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_3 MAC (Currency Exchange transactions)

Function: Validate the S_3 MAC for currency exchange transactions.

Notes: After a CEP card completes processing, it generates an S_3 MAC to prove to the issuer that the currency exchange transaction was completed successfully. The load processor uses this function to verify the S_3 MAC.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V4'.
*KM3X	32 H or 1 A + 32 H	Double length KM3X encrypted under LMK pair 20-21 variant 6.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
CC_{TRX}	2 B	Transaction Completion Code.
TI	1 B	Transaction Indicator: '08': currency exchanges.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA,SOURCE}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$CURR_{LDA,TARGET}$	3 B	The Currency Code.
$BAL_{CEP,TARGET}$	4 B	Balance of slot prior to completion.
$BAL_{CEP,SOURCE}$	4 B	Balance of slot prior to completion.
S_3	8 B	Signature for verification.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'V5'.
Error Code	2 N	'00': No error (S_3 validated successfully) '01': S_3 validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_3 MAC (Load or Unload transactions)

Function: Validate the S_3 MAC for load or unload transactions.

Notes: After a CEP card completes processing, it generates an S_3 MAC to prove to the issuer that the load or unload transaction was completed successfully. This function is used by the load processor to verify the S_3 MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V6'.
*KM3L	32 H or 1 A + 32 H	Double length *KM3L encrypted under LMK pair 20-21 variant 5.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KD3L.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
CC_{TRX}	2 B	Transaction Completion Code.
TI	1 B	Transaction Indicator: '0C': load transactions '0A': unload transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
BAL_{CEP}	4 B	Balance of slot prior to completion.
S_3	8 B	Signature for verification.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'V7'.
Error Code	2 N	'00': No error (S_3 validated successfully) '01': S_3 validation failed '10': KMX parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate the $H2_{LSAM}$

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Validate the $H2_{LSAM}$, creating a SHA-1 hash over the transaction data and comparing with the input $H2_{LSAM}$.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V8'.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
$R2_{LSAM}$	16 B	Random Number .
$H2_{LSAM}$	8 B	Verification code (SHA-1 hash).
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'V9'.
Error Code	2 N	'00': No error ($H2_{LSAM}$ validated successfully) '01': $H2_{LSAM}$ validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Unlinked Load Transaction Request

Function: Unlinked Load Transaction Request.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T0'.
S1	8 B	The CEP Card MAC produced by the card during 'Card Initialise for Load'.
H_{CEP}	10 B	The SHA-1 Hash generated by the CEP card on the Load Transaction data.
TPK	16 H or 1 A + 32 H	The Terminal PIN key encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".
REFNO	3 B	The Transaction Reference Number.
R_1Length	1 N	The required length of the generated key R_1: '1': single length '2': double length.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
$CURR_{LDA}$	3 B	The Currency Indicator.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
DD_{CEP}Length	1 B	The length in bytes of the DD_{CEP} field that follows.
DD_{CEP}	0 - 32 B	Discretionary Data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'T1'.
Error Code	2 N	'00': No error '11': TPK Parity Error or a standard error code, as listed in Chapter 4 of [2].
(DES)R_1	16 / 32 H	The generated session key encrypted under the TPK. (Note, if the supplied TPK is double length then this will also be double length.)
(DES)R_{LSAM}	64 H	The generated double length key R_{LSAM} and other data CBC encrypted under LMK pair 10-11.
(DES)$R2_{LSAM}$	64 H	The generated double length key $R2_{LSAM}$ and other data CBC encrypted under LMK pair 10-11.
H_{LSAM}	8 B	SHA-1 hash of internally generated R_{LSAM}.
$H2_{LSAM}$	8 B	SHA-1 hash of internally generated $R2_{LSAM}$.
(DES)HCEP	64 H	The HCEP, concatenated with REFNO and ID_{LACQ} and CBC encrypted under LMK pair 10-11.
MAC_{LSAM}	4 B	EMV MAC of Transactional data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Release R_{LSAM}

Function: Release R_{LSAM}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T2'.
REFNO	3 B	The Transaction Reference Number.
ID_{LACQ}	4 B	Load Acquirer ID.
$(DES)R_{LSAM}$	64 H	The generated double length key R_{LSAM} and other data CBC encrypted under LMK pair 10-11.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'T3'.
Error Code	2 N	'00': No error '01': Validation Error '10': R_{LSAM} parity error or a standard error code, as listed in Chapter 4 of [2].
R_{LSAM}	32 H	The clear text value of R_{LSAM} returned as 32 HEX characters.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Release $R2_{LSAM}$

Function: Release $R2_{LSAM}$.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T4'.
REFNO	3 B	The Transaction Reference Number.
ID_{LACQ}	4 B	Load Acquirer ID.
(DES)$R2_{LSAM}$	64 H	The generated double length key $R2_{LSAM}$ and other data CBC encrypted under LMK pair 10-11.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'T5'.
Error Code	2 N	'00': No error '01': Validation Error '10': $R2_{LSAM}$ parity error or a standard error code, as listed in Chapter 4 of [2].
$R2_{LSAM}$	32 H	The clear text value of $R2_{LSAM}$ returned as 32 HEX characters.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Verify R_{CEP}

Function: Verify R_{CEP}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T6'.
REFNO	3 B	The Transaction Reference Number.
$(DES)H_{CEP}$	64 H	The HCEP, concatenated with REFNO and ID_{LACQ} and CBC encrypted under LMK pair 10-11.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
R_{CEP}	16 B	The 16 Byte value returned by the CEP card following a Credit for Load rejection.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'T7'.
Error Code	2 N	'00': No error '01': Verification Failure or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate S_6 MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To validate an S_6 Message Authentication Code (MAC) calculated by a CEP card on a detailed transaction record.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W0'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for S_6 in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
$DEXPP_{CEP}$	3 B	CEP card expiration date for offline transactions.
TI_{CEP}	1 B	CEP card transaction indicator.
$DTHR_{PDA}$	5 B	PDA transaction date and time.
$CURR_{PDA}$	3 B	PDA currency.
AM_{CEP}	1 B	CEP card authentication method.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$MTOT_{CEP}$	4 B	CEP card total transaction amount.
M_{PDA}	4 B	PDA transaction amount.
BAL_{CEP}	4 B	CEP card slot balance.
S_6	8 B	Transaction MAC, to be validated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'W1'.
Error Code	2 N	'00': No error (S_6 verification successful) '01': S_6 verification failure '10': KMP parity error '70': Invalid ALGP2 or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate $S_{6'}$ MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To validate an $S_{6'}$ Message Authentication Code (MAC) calculated by a CEP card on an aggregated transaction.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W2'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for $S_{6'}$ in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
MAC Type	1 B	MAC type; must equal X'01.
$CURR_{PDA}$	3 B	PDA currency.
$MTOT_{AGG}$	4 B	Amount of aggregated transactions in the current record.
NT_{AGG}	2 B	Number of aggregated transactions in the current record.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{6'}$	8 B	Transaction MAC, to be validated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'W3'.
Error Code	2 N	'00': No error ($S_{6'}$ verification successful) '01': $S_{6'}$ verification failure '10': KMP parity error '70': Invalid ALGP2 '71': Invalid MAC type or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate $S_{6''}$ MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To validate an $S_{6''}$ Message Authentication Code (MAC) calculated by a CEP card on an Issuer backup total.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	m A	Value 'W4'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for $S_{6''}$ in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
MAC Type	1 B	MAC type; must equal X'02.
$CURR_{PDA}$	3 B	PDA currency.
$MTOTold_{IB}$	4 B	Signed amount of transactions in the batch for the Issuer.
$NTold_{IB}$	2 B	Signed number of transactions in the batch for the Issuer.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{6''}$	8 B	Transaction MAC, to be validated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'W5'.
Error Code	2 N	'00': No error ($S_{6''}$ verification successful) '01': $S_{6''}$ verification failure '70': Invalid ALGP2 '71': Invalid MAC type '10': KMP parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate $S_{5',DLT}$ MAC

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To validate an $S_{5',DLT}$ Message Authentication Code (MAC), which provides the Issuer with the ability to verify the integrity of a non-CEP transaction.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W6'.
$KI_{S5'}$	32 H	$S_{5'}$ Issuer Key, encrypted under variant 4 of LMK pair 20-21.
ALG_{KS}	1 B	Algorithm code for $S_{5'}$ transactions; must equal X'01.
NT_{PSAM}	4 B	PSAM transaction number.
TI_{PDA}	1 B	PDA transaction indicator.
$DTHR_{PDA}$	5 B	PDA transaction date and time.
ID_{PSAM}	4 B	Identifier of a PSAM.
M_{PDA}	4 B	PDA transaction amount.
$DEXP_{CARD}$	3 B	Card expiry date.
AM_{CEP}	1 B	CEP card authentication method.
BAL_{CEP}	4 B	CEP card slot balance.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{5',DLT}$	8 B	Transaction MAC, to be validated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'W7'.
Error Code	2 N	'00': No error ($S_{5',DLT}$ verification successful) '01': $S_{5',DLT}$ verification failure '10': $KI_{S5'}$ parity error '70': Invalid ALG_{KS} or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate $S_{5',ISS}$ MAC

Function: To validate an $S_{5',ISS}$ Message Authentication Code (MAC) which provides the Issuer with the ability to verify the integrity of a non-CEP transaction.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W8'.
$KI_{S5'}$	32 H	$S_{5'}$ Issuer Key, encrypted under variant 4 of LMK pair 20-21.
ALG_{KS}	1 B	Algorithm code for $S_{5'}$ transactions; must equal X'01.
NT_{PSAM}	4 B	PSAM transaction number.
MAC Type	1 B	MAC type; must equal X'01 or X'02.
MTOT	4 B	$MTOTold_{IB}$ or $MTOT_{AGG}$.
$CURR_{PDA}$	3 B	PDA currency.
NT	2 B	$NTold_{IB}$ or NT_{AGG}.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
$S_{5',ISS}$	8 B	Transaction MAC, to be validated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'W9'.
Error Code	2 N	'00': No error ($S_{5',ISS}$ verification successful) '01': $S_{5',ISS}$ verification failure '02': Invalid ALG_{KS} '03': Invalid MAC type '10': $KI_{S5'}$ parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Validate the S_4 MAC (Old Terminals)

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: Validate the S_4 MAC (MAC of the PSAM for a Batch) for old terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X0'.
*$KMAC_{S4}$	32 H	Double length $KMAC_{S4}$ encrypted under LMK pair 20-21 variant 7.
S_4	16 H	Signature for verification.
ID_{CAD}	4 B	Identifier for the CAD.
ID_{MCARD}	4 B	Identifier for the MCard.
Collection Number	1 B	Collection Number.
MCard Date	1 B	Month number as known by the MCard.
$MTOT_{BATCH}$	4 B	Total of all successful payments in the batch.
$CURR_{MCARD}$	2 B	Currency code for the batch.
NT_{BATCH}	2 B	Number of payment records in the batch.
$NTENQ_{BATCH}$	2 B	Number of successful balance enquiries in the batch.
$NTREJ_{BATCH}$	2 B	Total number of invalid records in the batch.
$NTFLT_{BATCH}$	2 B	Number of non-readable ICCs.
$NTSFLT_{BATCH}$	2 B	Number of system faults.
MCard Version	1 B	Firmware version of the MCard.
$CEXP_{MCARD}$	1 B	Currency exponent.
Batch Close Date Time	2 B	Batch close date and time (may be all a zeroes).
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'X1'.
Error Code	2 N	'00': No error (S_4 validated successfully) '01': S_4 validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_4 MAC (New Terminals)

Function: Validate the S_4 MAC for new terminals.

Notes: This command does not check the contents of the data block over which the MAC is generated. It is the responsibility of the user of the command to ensure the data format is correct.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X2'.
*$KMAC_{S4}$	32 H	Double length $KMAC_{S4}$ encrypted under LMK pair 20-21 variant 7.
S_4	16 H	Signature for verification.
ID_{PSAM}	4 B	Identifier for a PSAM.
ID_{BATCH}	2 B	Identifier for a POS Transaction Batch.
NT_{BATCH}	2 B	The number of payment and cancellation transactions in this batch.
Data Length	3 N	Length in bytes of the following data block.
Data Block D_4	n B	Binary data block.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'X3'.
Error Code	2 N	'00': No error (S_4 validated successfully) '01': S_4 validation failed '10': KMAC parity error '70': Data D_4 length error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_5 MAC (Old Terminals)

Function: Validate the S_5 MAC (MAC of the PSAM for a Batch) for old terminals.

Notes: The MACing process for old terminals has a different pad process than standard.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X4'.
*$KMAC_{S5}$	32 H	Double length $KMAC_{S5}$ encrypted under LMK pair 20-21 variant 8.
S_5	16 H	Signature for verification.
ID_{MCARD}	4 B	MCard Identifier.
Collection Number	1 B	Collection Number.
NT_{MCARD}	4 B	MCard Transaction Number.
C.C.	1 B	Proprietary Completion Codes.
Card Balance	4 B	New Card Balance.
$MTOT_{MCARD}$	4 B	Total Transaction Amount.
$CURR_{MCARD}$	2 B	Currency Code.
$CEXP_{MCARD}$	1 B	Currency Exponent.
$ID_{ISS,\ MCARD}$	3 B	Issuer BIN or zeroes (For reloadable or disposable cards).
$ID_{CARD,\ MCARD}$	5 B	Card Identifier.
NT_{IEP}	2 B	Card Transaction Number.
RFU	1 B	Reserved.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'X5'.
Error Code	2 N	'00': No error (S_5 validated successfully) '01': S_5 validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the $S_{5'}$ MAC (MAC of the PSAM for a Transaction) (New Terminals)

Function: Validate the $S_{5'}$ MAC for new terminals.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X6'.
*$KMAC_{S5}$	32 H	Double length $KMAC_{S5}$ encrypted under LMK pair 20-21 variant 8.
$S_{5'}$	16 H	Signature for verification.
Length of DD_{CEP}	1 B	Length of DD_{CEP} field: range 0 – 6.
Record Length	2 B	Record Length.
Record Type	1 B	Record Type.
ID_{RECORD}	2 B	Record number within batch.
RID_{PSAM}	5 B	The RID of the PSAM creator.
$ID_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID_{PSAM} owner.
ID_{PSAM}	4 B	Identifier for a PSAM.
ID_{BATCH}	2 B	Identifier for a POS Transaction Batch.
NT_{PSAM}	4 B	PSAM Transaction Number.
$MTOT_{PDA}$	4 B	Net value of transaction.
$CURR_{PDA}$	3 B	Currency of transaction.
ID_{SCHEME}	1 B	Reference number assigned to AID_{CEP} in AID table.
ID_{ISS}	4 B	Issuer Identifier.
ID_{CEP}	6 B	ID of CEP or IEP application.
NT_{CEP}	2 B	CEP card transaction number.
S_6	8 B	Signature from CEP card.
CC_{PDA}	2 B	CEPS completion code.
CC_{PROP}	2 B	Proprietary completion code.
Slot Balance	4 B	Slot balance at end of transaction.
TI_{PDA}	1 B	Transaction indicator.
M_{PDA}	4 B	Value of last successful increment.
$DTHR_{PDA}$	5 B	Date & Time stamp for transaction.
$DEXP_{CARD}$	3 B	Card expiration date.
ALG_{KS}	1 B	Algorithm to calculate S_4 & S_5.
AM_{CEP}	1 B	Authentication Method.
$VKP_{CA, ISS, CEP}$	1 B	Version number of the issuer CA key.
$ID_{REG, ISS}$	4 B	Issuer region ID.
$VKP_{REG, ISS}$	1 B	Version number of the regional CA key.
$CSN_{ISS, CEP}$	3 B	Issuer certificate serial number.
L_{DDCEP}	1 B	Length of the DD_{CEP} field.
DD_{CEP}	n B	DD_{CEP} response.
NUM_{SEG}	1 B	Number of Segments.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

© Thales UK Limited 2019

LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'X7'.
Error Code	2 N	'00': No error (S_5' validated successfully) '01': S_5' validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals)

Function: Validate the S_5 Variant MAC for new terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X8'.
*$KMAC_{S5}$	32 H	Double length $KMAC_{S5}$ encrypted under LMK pair 20-21 variant 8.
S_5 Variant	16 H	Signature for verification.
Length of DD_{CEP}	1 B	Length of DD_{CEP} field: range 0 to 16.
Record Length	2 B	Record Length.
Record Type	1 B	Record Type.
ID_{RECORD}	2 B	Record number within batch.
RID_{PSAM}	5 B	The RID of the PSAM creator.
$ID_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID_{PSAM} owner.
ID_{PSAM}	4 B	Identifier for a PSAM.
ID_{BATCH}	2 B	Identifier for a POS Transaction Batch.
NT_{PSAM}	4 B	PSAM Transaction Number.
$MTOT_{SIGNED}$	4 B	Net value of record.
$CURR_{PDA}$	3 B	Currency of transaction.
ID_{SCHEME}	1 B	Reference number assigned to AID_{CEP} in AID table.
ID_{ISS}	4 B	Issuer Identifier.
ID_{CEP}	6 B	ID of CEP or IEP application.
NT_{CEP}	2 B	CEP card transaction number.
$S_{6'}$ or $S_{6''}$	8 B	Signature from CEP card.
$NT_{ISS, SIGNED}$	2 B	Number of transactions accounted for in the signed MTOT in this summary.
$MTOT_{NOSIG}$	4 B	Unsigned net value of record.
$NT_{ISS, NOSIG}$	4 B	Number of transactions included in unsigned net value.
ALG_{KS}	1 B	Algorithm used to calculate S_4 and S_5 MACs.
L_{DDCEP}	1 B	Length of the DD_{CEP} field.
DD_{CEP}	N B	DD_{CEP} response.
NUM_{SEG}	1 B	Number of Segments.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'X9'.
Error Code	2 N	'00': No error (S_5 variant validated successfully) '01': S_5 variant validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Create the Acknowledgement MAC
(Old Terminals)

Function: Create the Acknowledgement MAC for old terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y0'.
*$KMAC_{ACQ}$	32 H	Double length $KMAC_{ACQ}$ encrypted under LMK pair 20-21 variant 9.
Rec. ID_{MCARD}	4 B	ID of the receiving Mcard.
Gen. ID_{MCARD}	4 B	ID of the MCard that generated the collection batch.
Coll. No.	1 B	Collection Number.
NT_{BATCH}	2 B	The total number of purchase and cancellation transactions included in the batch.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Y1'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S_{AQC}	16 H	Acknowledgement MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Create the Acknowledgement MAC
(New Terminals)

Function: Create the Acknowledgement MAC for new terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y2'.
Mode Flag	1 N	Mode Flag: '0': *$KMAC_{ACK}$ supplied '1': No *$KMAC_{ACK}$ supplied.
*$KMAC_{ACK}$	32 H	Double length $KMAC_{ACK}$ encrypted under LMK pair 20-21 variant 9, only supplied if Mode Flag = '0'.
CLA	1 B	CLA.
INS	1 B	INS.
P1P2	2 B	P1P2.
L_C	1 B	L_C.
ID_{THREAD}	1 B	ID_{THREAD}.
Action Requested	1 B	Action Requested.
RID_{PSAM}	5 B	The RID of the PSAM Creator.
$ID_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID_{PSAM} owner.
ID_{PSAM}	4 B	Identifier for a PSAM.
$DATE_{PSAM}$	2 B	Current month.
ID_{BATCH}	2 B	Identifier for a POS Transaction Batch.
NT_{RECORD}	2 B	The number of payment records in a batch.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Y3'.
Error Code	2 N	'00': No error '10': KMAC parity error '70': Invalid Mode Flag or a standard error code, as listed in Chapter 4 of [2].
S_{ACK}	16 H	Acknowledgement MAC
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Create the Update MAC

Function: Create the Update MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y4'.
*$KMAC_{UPD}$	32 H	Double length $KMAC_{UPD}$ encrypted under LMK pair 22-23 variant 1.
ID_{BATCH}	2 B	Identifier for a POS Transaction Batch.
ID_{PSAM}	4 B	PSAM Identifier assigned by the PSAM creator.
CLA	1 B	CLA.
INS	1 B	INS.
P1P2	2 B	P1P2.
L_C	1 B	L_C.
ID_{THREAD}	1 B	ID_{THREAD}.
Update Number	1 B	Update Number.
TAG	2 B	Tag identifying data in the update.
LEN	1 B	Length of the following data.
Update data	n B	Update data.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Y5'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S_{UPD}	16 H	Update MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the S_{ADMIN} MAC (Administrative MAC of the PSAM)

Function: Validate the S_{ADMIN} MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y6'.
S_{ADMIN}	16 H	Signature for verification.
Length	2 B	Length.
Record Type	1 B	Record Type.
RID_{PSAM}	5 B	The RID of the PSAM Creator.
$ID_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID_{PSAM} owner.
ID_{PSAM}	4 B	PSAM Identifier assigned by the PSAM creator.
Administrative Record ID	1 B	Operating data table content status.
CNT_{TABLE}	1 B	Number of tables whose status is being reported in this record.
Table ID_N	1 B	Identifies the table being reported.
HASH $value_N$	8 B	Hash value of data in the table.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Y7'.
Error Code	2 N	'00': No error (S_{ADMIN} validated successfully) '01': S_{ADMIN} validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Create the Merchant Acquirer MAC

Function: Create the Merchant Acquirer MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y8'.
*$KMAC_{MA}$	32 H	Double length $KMAC_{MA}$ encrypted under LMK pair 22-23 variant 2.
Date & Time	6 B	Date and Time.
Function Code	2 B	Function Code.
ID_{SOURCE}	4 B	ID_{SOURCE}.
$CURR_{CPDA}$	2 B	$CURR_{CPDA}$, can be all zeroes.
Block 1	9 B	Block 1 containing CNT_{BATCH}, CNT_{ACCEPT}, ID_{BATCH}, NT_{BATCH} and RESEND.
Block 2	9 B	Block 2 containing Amount and Net Reconciliation.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Y9'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S_{MA}	16 H	Merchant Acquirer MAC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Validate the Card Issuer MAC

Function: Validate the Card Issuer MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Z0'.
*$KMAC_{CI}$	32 H	Double length $KMAC_{CI}$ encrypted under LMK pair 22-23 variant 3.
S_{CI}	16 H	Signature for Verification.
Date & Time	6 B	Date and Time.
Function Code	2 B	Function Code.
ID_{DEST}	4 B	ID_{DEST}.
Block 1	2 B	Block 1, fixed to all zeroes.
Block 2	9 B	Block 2 containing CNT_{BATCH}, CNT_{ACCEPT}, ID_{BATCH}, NT_{BATCH} and RESEND.
Block 3	9 B	Block 3 containing Amount and Net Reconciliation.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Z1'.
Error Code	2 N	'00': No error (S_{CI} validated successfully) '01': S_{CI} validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

Export Electronic Purse Card Key Set

Variant LMK ☑	Key Block LMK ☒
License: **PS10-LIC-LEGACY**	
Authorization: **Not Required**	

Function: To export a member's electronic purse card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not supplied. The zero value will then be placed in the data block to be protected with a MAC.

The MasterCard documents refer to the KML as KDLiss, KM3X as K3Xiss etc.

All keys are passed in using key scheme U.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R2'.
Delimiter	1 A	Optional. If present the following field must be present. Value ';'.
ESP Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 03 02). Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
KMLiss	1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 1, using Key Encryption Scheme U.
The following section contains Extra KDLIss Key Data		

© Thales UK Limited 2019

Field	Length & Type	Details
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Mater Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID	1 N	'1': Algorithm 3. '2': Algorithm 5.
S1 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
S2 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KM3Liss	1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 5, using Key Encryption Scheme U.
The following section contains Extra KD3LIss Key Data		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
S3 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.

© Thales UK Limited 2019

Field	Length & Type	Details
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMXiss	1 A + 32 H	Double length master key encrypted under LMK pair 20-21 Variant 2, using Key Encryption Scheme U.
The following section contains Extra KDXIss Key Data		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
S1 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
S2 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KM3Xiss	1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 6, using Key Encryption Scheme U.
The following section contains Extra KD3XIss Key Data		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
S3 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.

© Thales UK Limited 2019

Field	Length & Type	Details
KMPiss	1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 3, using Key Encryption Scheme U.
The following section contains Extra KDPiss Key Data		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
S6 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMSIiss	1 A + 32 H	Double length master key, encrypted under LMK pair 22-23 Variant 3, using Key Encryption Scheme U.
The following section contains Extra KDSIiss Key Data		
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
MAC Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMSCiss	1 A + 32 H	Double length master key, encrypted under LMK pair 22-23 Variant 4, using Key Encryption Scheme U.
The following section contains Extra KDSCiss Key Data		
ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
Encryption Algorithm ID	1 N	'1': Reserved for future use.
H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
Transport Key ID	4 N	Key ID of the BKAM, BKEM used.
IDcep	6 B	Derivation Data.
MAC algorithm	1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.

© Thales UK Limited 2019

Field	Length & Type	Details
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

© Thales UK Limited 2019

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'R3'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': KML parity error '11': KM3L parity error '50': KMX parity error '51': Invalid message header '52': KM3X parity error '53': KMP parity error '54': KMSI parity error '55': KMSC parity error or a standard error code, as listed in Chapter 4 of [2].
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted KDL	32 H	BKEM Encrypted Key.
KDL Key Check Value	3 B	
Encrypted KD3L	32 H	BKEM Encrypted Key.
KD3L Key Check Value	3 B	
Encrypted KDX	32 H	BKEM Encrypted Key.
KDX Key Check Value	3 B	
Encrypted KD3X	32 H	BKEM Encrypted Key.
KD3X Key Check Value	3 B	
Encrypted KDP	32 H	BKEM Encrypted Key.
KDP Key Check Value	3 B	
Encrypted KSI	32 H	BKEM Encrypted Key.
KSI Key Check Value	3 B	
Encrypted KSC	32 H	BKEM Encrypted Key.
KSC Key Check Value	3 B	
MAC	16 H	MAC calculated over key set data using BKAM.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

© Thales UK Limited 2019

13. Error Codes

The standard error codes returned by the payShield 10K to the Host are listed in the table. Some error codes are specific to certain commands: these are documented in Chapter 2.

Note: Whilst the payShield 10K's host commands are backward compatible with those of the payShield 9000 and HSM 8000, the internal processing steps are occasionally different, resulting in different error codes being returned.

Note: All commands that have a data length field followed by a data field will return error 15 if the data is longer than the specified length and error 80 if the data is shorter than the specified length or if the value in the data length field is 0.

Code	Description
00	No error
01	Verification failure or warning of imported key parity error
02	Key inappropriate length for algorithm
04	Invalid key type code
05	Invalid key length flag
10	Source key parity error
11	Destination key parity error or key all zeros
12	Contents of user storage not available. Reset, power-down or overwrite
13	Invalid LMK Identifier
14	PIN encrypted under LMK pair 02-03 is invalid
15	Invalid input data (invalid format, invalid characters, or not enough data provided)
16	Console or printer not ready or not connected
17	HSM not authorized, or operation prohibited by security settings
18	Document format definition not loaded
19	Specified Diebold Table is invalid
20	PIN block does not contain valid values
21	Invalid index value, or index/block count would cause an overflow condition
22	Invalid account number
23	Invalid PIN block format code. (Use includes where the security setting to implement PCI HSM limitations on PIN Block format usage is applied, and a Host command attempts to convert a PIN Block to a disallowed format.)
24	PIN is fewer than 4 or more than 12 digits in length
25	Decimalization Table error
26	Invalid key scheme
27	Incompatible key length
28	Invalid key type
29	Key function not permitted
30	Invalid reference number

© Thales UK Limited 2019

Code	Description
31	Insufficient solicitation entries for batch
32	AES not licensed
33	LMK key change storage is corrupted
39	Fraud detection
40	Invalid checksum
41	Internal hardware/software error: bad RAM, invalid error codes, etc.
42	DES failure
43	RSA Key Generation Failure
46	Invalid tag for encrypted PIN
47	Algorithm not licensed
49	Private key error, report to supervisor
51	Invalid message header
65	Transaction Key Scheme set to None
67	Command not licensed
68	Command has been disabled
69	PIN block format has been disabled
74	Invalid digest info syntax (no hash mode only)
75	Single length key masquerading as double or triple length key
76	RSA public key length error or RSA encrypted data length error
77	Clear data block error
78	Private key length error
79	Hash algorithm object identifier error
80	Data length error. The amount of MAC data (or other data) is greater than or less than the expected amount.
81	Invalid certificate header
82	Invalid check value length
83	Key block format error
84	Key block check value error
85	Invalid OAEP Mask Generation Function
86	Invalid OAEP MGF Hash Function
87	OAEP Parameter Error
90	Data parity error in the request message received by the HSM
91	Longitudinal Redundancy Check (LRC) character does not match the value computed over the input data (when the HSM has received a transparent async packet)
92	The Count value (for the Command/Data field) is not between limits, or is not correct (when the HSM has received a transparent async packet)
A1	Incompatible LMK schemes
A2	Incompatible LMK identifiers

© Thales UK Limited 2019

Code	Description
A3	Incompatible key block LMK identifiers
A4	Key block authentication failure
A5	Incompatible key length
A6	Invalid key usage
A7	Invalid algorithm
A8	Invalid mode of use
A9	Invalid key version number
AA	Invalid export field
AB	Invalid number of optional blocks
AC	Optional header block error
AD	Key status optional block error
AE	Invalid start date/time
AF	Invalid end date/time
B0	Invalid encryption mode
B1	Invalid authentication mode
B2	Miscellaneous key block error
B3	Invalid number of optional blocks
B4	Optional block data error
B5	Incompatible components
B6	Incompatible key status optional blocks
B7	Invalid change field
B8	Invalid old value
B9	Invalid new value
BA	No key status block in the key block
BB	Invalid wrapping key
BC	Repeated optional block
BD	Incompatible key types
BE	Invalid key block header ID

© Thales UK Limited 2019

14. WebPIN Appendices

Appendix A - Message Formats

Definitions and Conventions

Definitions

ASCII-Hex Encoded: this is a printable ASCII string representation of a byte array expressed in base 16 (i.e. HEX). For example, an unsigned long decimal value of 1234567 would be represented in ASCII-Hex encoding as the string "12D687"

Conventions

Array indexing in this document will begin from index 0. That is to say, that it will follow the normal conventions of the 'C' language.

Additionally, array ranges will be noted with the ellipse '..' characters. For example, indexing between 0 and 5 would be noted as, message[0..5]. The upper bound value can be parameterized for indeterminant upper range values. For example, a message of indeterminate length can be referenced as, message[2..n] with 2 being the starting index value and 'n' being the ending index value.

© Thales UK Limited 2019

Message Formats

PIN and MAC Message Format

A PIN and MAC message has the following structure:

Ver	Type	HEMK	HEPB	Acct #	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The pin and mac message type is "05". This means that the message contains a hex encrypted master key, the hex encrypted pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HEPB** is the Hex Encrypted PIN Block. This field is 16 bytes long.

* **Acct #** is the 12 digit account number (in ASCII form) used to form the PIN block. This field is 12 bytes long.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

© Thales UK Limited 2019

Change PIN and MAC Message Format

A Change PIN and MAC message has the following structure:

Ver	Type	HEMK	HEPB-o	HEPB-n	Acct #	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The change pin and mac message type is "06". This means that the message contains a hex encrypted master key, the hex encrypted old pin block, the hex encrypted new pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HEPB-o** is the old Hex Encrypted PIN Block. This field is 16 bytes long.

* **HEPB-n** is the new Hex Encrypted PIN Block. This field is 16 bytes long.

* **Acct #** is the 12 digit account number (in ASCII form) used to form the PIN block. This field is 12 bytes long.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

Alphanumeric PIN and MAC

An Alpha-numeric PIN and MAC message has the following structure:

Ver	Type	HEMK	HM	EM	HEANPB	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The Alpha-numeric pin and mac message type is "10". This means that the message contains a hex encrypted master key, the hex encrypted A-N pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HM** is the Hash Mode used to generate the HEANPB. This field contains a ASCII character indicating the hash mode used to generate the HEANPB. This will also imply the length of the HEANPB field. Valid values for this field are:

  * "0" for NONE-SHORT (HEANPB will be 32 bytes long)
  * "1" for MD5-CLEAR (HEANPB will be 32 bytes long)
  * "2" for MD5-XOR (HEANPB will be 32 bytes long)
  * "3" for SHA1-XOR (HEANPB will be 48 bytes long)
  * "4" for NONE-LONG (HEANPB will be 48 bytes long)

  This field is one byte long.

* **EM** is the encryption mode used for encrypting the pin block. Valid values for this field are:

  * "1" for DES-ECB
  * "2" for DES-CBC

  This field is one byte long.

* **HEANPB** is the Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

© Thales UK Limited 2019

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

© Thales UK Limited 2019

Alphanumeric Change PIN and MAC

An Alpha-numeric Change PIN and MAC message has the following structure:

Ver	Type	HEMK	HM	EM	HEANPB-o	HEANPB-n	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The change A-N pin and mac message type is "11". This means that the message contains a hex encrypted master key, the hex encrypted old A-N pin block, the hex encrypted new A-N pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HM** is the Hash Mode used to generate the HEANPB. This field contains a ASCII character indicating the hash mode used to generate the HEANPB. This will also imply the length of the HEANPB field. Valid values for this field are:

  * "0" for NONE-SHORT (HEANPB will be 32 bytes long)
  * "1" for MD5-CLEAR (HEANPB will be 32 bytes long)
  * "2" for MD5-XOR (HEANPB will be 32 bytes long)
  * "3" for SHA1-XOR (HEANPB will be 48 bytes long)
  * "4" for NONE-LONG (HEANPB will be 48 bytes long)

  This field is one byte long.

* **EM** is the encryption mode used for encrypting the pin block. Valid values for this field are:

  * "1" for DES-ECB
  * "2" for DES-CBC

  This field is one byte long.

* **HEANPB-o** is the old Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

* **HEANPB-n** is the new Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

© Thales UK Limited 2019

Hex Encrypted Alphanumeric PIN Block (HEANPB)

A Hex Encrypted Alphanumeric PIN Block (HEANPB) is a PIN block containing a transformed Alphanumeric PIN and (sometimes) the account number. The format and size of this PIN block will change, based upon its construction. There are 5 separate formats (or constructions) for this PIN block. These are:

* Hash Mode NONE-SHORT -- this is the AN-PIN, left-justified, and right-padded with 0x20 bytes out to a total length of 16 bytes. The AN-PIN must be <= 16 bytes. The resulting PIN block is ASCII-Hex encoded.

* Hash Mode NONE-LONG -- this is the AN-PIN, left-justified, and right-padded with 0x20 bytes out to a total length of 20 bytes. The AN-PIN must be <= 20 bytes. The resulting PIN block is ASCII-Hex encoded.

* Hash Mode MD5 -- this is the AN-PIN, hashed by MD5. The AN-PIN can be of arbitrary length. The resulting PIN block is 32 ASCII-Hex encoded bytes.

* Hash Mode MD5-XOR -- this is the AN-PIN, hashed by MD5. The result is then ASCII-Hex encoded, XOR'd with the right most 12 digits of the account number, and finally TDES encrypted. The resulting PIN block is 32 ASCII-Hex encoded bytes.

* Hash Mode SHA1-XOR -- this is the AN-PIN, hashed by SHA1. The result is then ASCII-Hex encoded, XOR'd with the right most 12 digits of the account number, padded with 8 random bytes, and finally TDES encrypted. The resulting PIN block is 48 ASCII-Hex encoded bytes.

© Thales UK Limited 2019

Master Key Format and Hex Encrypted Master Key Format

Master Key Format

A Master Key is a piece of data which is used to derive subsequent related key sets and IVs.

It will have the following structure:

Ver	Usage	Key

Where:

* **Ver** is a single binary value representing the master key version. The Version field will be used for managing forwards compatibility issues. Currently, the only supported version value is 1.

* **Usage** is a single binary value representing the master key usage. This field will indicate the number, type, and usage parameters describing the keyset to be generated. Here are the supported usage types:

0x01 = keyset containing 1 double-length DES key for PIN encryption, a DES PIN IV, and 1 double-length MAC key for ANSI X9.19 MACing.

0x02 = Reserved

0x03 = Reserved

0x04 = Reserved

* **Key** is an array containing the actual master key bytes to be used for key derivation. The length of this value will always be 48 bytes.

Hex Encrypted Master Key (HEMK) Format

A Hex Encrypted Master Key (HEMK) is an RSA wrapped Master Key. This method always uses a 1024 bit RSA key.

The method employed is RSA v1.5 encryption with block type 02 of bytes making up the Master Key.

The resulting ciphertext is then converted into ASCII-Hex encoded form. Because this method always uses a 1024 bit RSA public key for wrapping, the resulting length of this field will always be 256 bytes.

© Thales UK Limited 2019

Key Derivation Algorithm and Key Block Format

Key Derivation Algorithm

The key bytes derivation algorithm is based upon the mechanism defined in the SSL 3.0 specification. Specifically, we utilize a variation on their mechanism to generate the bytes used to populate the key buffers.

Here is the process:

1) Identify the total number of bytes necessary to be generated. This is done by adding up all of the related key bytes and IVs. Let's call this value KeyBlockLen.

2) Next, we'll generate the actual KeyBlock using the following algorithm:

```
KeyBlock =  SHA1('A' + Master Key) +
            SHA1('BB' + Master Key) +
            SHA1('CCC' + Master Key) + [...];
```

Until enough data has been generated (i.e. KeyBlockLen) to fill the KeyBlock. Any extra KeyBlock data is discarded.

3) Finally, partition the KeyBlock as needed for the required operation. Any unused or unallocated KeyBlock data is discarded. See the following subsection for details on the allocation schemes.

Key Block Format

How the KeyBlock is partitioned is based upon the usage byte of the Master Key. It is partitioned as follows:

Usage	Partitions
0x01	KeyBlock[0..15] = 2DES Key[16] (for PIN encryption) KeyBlock[16..23] = DES IV[8] KeyBlock[24..39] = X9.19 MAC Key[16]
0x02	Reserved.
0x03	Reserved.
0x04	Reserved.

© Thales UK Limited 2019

Americas – Thales eSecurity Inc.
2860 Junction Avenue, San Jose, CA 95134 USA
Tel: +1 888 744 4976 or +1 954 888 6200
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 814 | 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

> thalesesecurity.com <