CCA coprocessor access controls and zO/S ICSF callable services and utilities

Introduction

When ICSF sends a request to a CCA coprocessor, the execution of that request is governed by access controls in the domain role. These access controls must be enabled in order for the coprocessor to permit execution of the request. The access controls available depends on the firmware level of the specific coprocessor receiving the request.

A new coprocessor or a zeroized coprocessor (or domain) comes with an initial set of access control points (ACPs) that are enabled by default. The tables of access controls list the default setting of each access control.

When a firmware upgrade is applied to an existing cryptographic coprocessor, the upgrade may introduce new ACPs.

- If a TKE workstation has been used to manage a cryptographic coprocessor, the firmware upgrade does not retroactively enable the new ACPs that would be enabled by default. These ACPs must be enabled via the TKE (or subsequent zeroize) in order to utilize the new support they control.
- If a TKE workstation has not been used to manage a cryptographic coprocessor, the firmware upgrade retroactively updates the new ACPs that would be enabled by default.

If an access control is disabled, the corresponding ICSF callable service or utility will fail during execution with an access denied error (8/90).

The tables list usage information using the following abbreviations:

AE Always enabled, cannot be disabled.

ED Enabled by default.

DD Disabled by default.

SC Usage of this access control requires special consideration.

The rest of this document contains tables describing the all of the access controls used by ICSF.

Tables 1 and 2 lists the access controls for individual services and the parameters that are affected by the control. Table 1 is ordered by access control name and Table 2 is ordered by the offset.

Table 3 lists the access controls that affect multiple services or coprocessor configuration.

Table 4 lists the access controls for ICSF utilities.

Table 5 is a cross reference between coprocessor code levels, licensed internal code releases, Crypto Express adapters and z servers.

Table 6 is a cross reference of the ICSF access controls with the IBM 4764/4765/4767 cryptographic coprocessor commands. The table is ordered by the offset.

For information about PKCS #11 access controls, see 'PKCS #11 Coprocessor Access Control Points' in *z/OS Cryptographic Services ICSF Writing PKCS #11 Applications.*

Document Currency

The information in this document is current as of April 30, 2010. The ICSF information is current for FMID HCR77D0 and APAR OA57089. The IBM model 4767/4748 information is current for releases 5.5 and 6.3.

References

- *CCA Basic Services Reference and Guide for the IBM 4767 and IBM 4765 PCIe Cryptographic Coprocessors Releases 5.5, 5.4, 5.3, 4.4, and 4.2,* Thirty-fifth edition (April 2019)
- *z/OS Cryptographic Services Integrated Cryptographic Service Facility Application Programmer's Guide* SC14-7508-08
- *z/OS Cryptographic Services Integrated Cryptographic Service Facility Administrator's Guide* SC14-7506-08

Callable services

The access controls listed in tables 1 and 2 are for individual services or related services. Table 1 is ordered by the ICSF access control name. Table 2 is ordered by the offset.

The **Name** column contains the control name as it appears on the TKE workstation and ICSF Domain Role panels

The **Callable services** column contains the service name of all services affected by the control.

The **Parameters affected when enabled** column contains the service parameters that are affected when the control is enabled. The control may restrict the value of the a parameter or allow a value to be used. When the field is blank, the access control applies to the service in general. That is, the access control must be enabled to use the service regardless of any other controls for the service.

The **Offset** column contains the hexadecimal offset of the access control point in the domain role.

The **Usage** column contains the default value of the access control. See the introduction for a discussion of the values.

The **Release** column contains the coprocessor code level the access control first became available. When the field is blank, the access control is available for all servers and coprocessors. See table 5 for CCA code levels.

Table 1. Access controls – Callable Services

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Authentication Parameter Generate	CSNBAPG		02B1	ED	4.4
Authentication Parameter Generate - Clear	CSNBAPG	The AP Protection Method *rule_array* keyword CLEAR is allowed.	02B2	DD	4.4
Cipher Text Translate2	CSNBCTT2 CSNBCTT3		01C0	ED	4.3
Cipher Text Translate2 – Allow translate from AES to TDES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be a DES key when the key supplied in the *key_identifier_in* parameter is an AES key.	01C1	ED	4.3
Cipher Text Translate2 – Allow translate to weaker AES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be a weaker AES key than the AES key supplied in the *key_identifier_in* parameter.	01C2	ED	4.3

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Cipher Text Translate2 – Allow translate to weaker DES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be a weaker DES key than the DES key supplied in the *key_identifier_in* parameter.	01C3	ED	4.3
Cipher Text Translate2 – Allow only cipher text translate types	CSNBCTT2 CSNBCTT3	The *key_identifier_in* and *key_identifier_out* parameters must be a key with key type CIPHERXI, CIPHERXL, or CIPHERXO for DES and key type CIPHER with the C-XLATE key usage bit on for AES.	01C4	DD	4.3
Clear Key Import/Multiple Clear Key Import - DES	CSNBCKI		00C3	ED	
	CSNBCKM	The Algorithm *rule_array* keyword DES is allowed.			
Clear PIN Encrypt	CSNBCPE		00AF	ED	
Clear PIN Generate - 3624	CSNBPGN	The Process rule *rule_array* keywords IBM-PIN and IBM-PINO are allowed.	00A0	ED	
Clear PIN Generate - GBP	CSNBPGN	The Process rule *rule_array* keyword GBP-PIN is allowed.	00A1	ED	
Clear PIN Generate - VISA PVV	CSNBPGN	The Process rule *rule_array* keyword VISA-PVV is allowed.	00A2	ED	
Clear PIN Generate - Interbank	CSNBPGN	The Process rule *rule_array* keyword INBK-PIN is allowed.	00A3	ED	
Clear Pin Generate Alternate - 3624 Offset	CSNBCPA	The PIN calculation method *rule_array* keyword IBM-PINO is allowed.	00A4	ED	
Clear PIN Generate Alternate - VISA PVV	CSNBCPA	The PIN calculation method *rule_array* keyword VISA-PVV is allowed.	00BB	ED	
Control Vector Translate	CSNBCVT		00D6	ED	
Cryptographic Variable Encipher	CSNBCVE		00DA	ED	
CVV Key Combine	CSNBCKC		0155	ED	4.2
CVV Key Combine – Allow wrapping override keywords	CSNBCKC	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	0156	ED	4.2
CVV Key Combine - Permit mixed key types	CSNBCKC	The key supplied by *key_a_identifier* parameter and the key supplied by *key_b_identifier* parameter need not be the same key type.	0157	ED	4.2
Data Key Export	CSNBDKX		010A	ED	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Data Key Export - Unrestricted	CSNBDKX	The key-encrypting key identified by the *exporter_key_identifier* parameter may have equal key halves	0277	ED	
Data Key Import	CSNBDKM		0109	ED	
Data Key Import - Unrestricted	CSNBDKM	The key-encrypting key identified by the *importer_key_identifier* parameter may have equal key halves	027C	ED	
Decipher - DES	CSNBDEC		000F	ED	
	CSNBEVF	Action *rule_array* keyword DECCNT is allowed			
Digital Signature Generate	CSNDDSG		0100	ED	
Digital Signature Generate – PKCS-PSS allow small salt	CSNDDSG	For the PKCS-PSS formatting method, the salt length specified in the *data* parameter is required to be zero, the length of the hash specified, or longer. When the access control is enabled, the salt length may be less than the length of the hash.	033B	DD	5.3
DSG - ZERO-PAD restriction lifted	CSNDDSG	The value of the *hash_length* parameter may be greater than 36 when the data input type keyword is HASH.	030C	DD	
Digital Signature Verify	CSNDDSV		0101	ED	
Digital Signature Verify – PKCS-PSS allow not exact salt length	CSNDDSV	For the PKCS-PSS formatting method, the salt length derived from the signature must be an exact match for the salt length specified in the *data* parameter. When the access control is enabled, the NEXMATCH keyword may be specified in the *rule_array* parameter. When the NEXMATCH keyword is specified, the salt length derived from the signature need not be an exact match for the salt length specified with the *data* parameter.	033C	DD	5.3
Diversified Key Generate - CLR8–ENC	CSNBDKG	Processing method *rule_array* keyword CLR8-ENC is allowed	0040	ED	
Diversified Key Generate - SESS-XOR	CSNBDKG	Processing method *rule_array* keyword SESS-XOR is allowed	0043	ED	
	CSNBEAC	Key mode *rule_array* keyword VISA is allowed			
	CSNBESC	Action *rule_array* keywords SMINT, SMCON, and SMCONPIN are allowed			
	CSNBEVF	Action *rule_array* keywords DECCNT and DYNVER are allowed			

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Diversified Key Generate - TDES-ENC	CSNBDKG	Processing method *rule_array* keyword TDES-ENC is allowed	0041	ED	
	CSNBDSK	Key mode *rule_array* keyword MC and VISA are allowed			
	CSNBEAC	Key mode *rule_array* keyword MC and VISA are allowed			
	CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed			
	CSNBEVF	Action *rule_array* keywords DECCNT are DYNVER are allowed			
Diversified Key Generate - TDES-CBC	CSNBDKG	Processing method *rule_array* keyword TDES-CBC is allowed	02B8	ED	4.4
Diversified Key Generate - TDES-DEC	CSNBDKG	Processing method *rule_array* keyword TDES-DEC is allowed.	0042	ED	
Diversified Key Generate - TDES-XOR	CSNBDKG	Processing method *rule_array* keyword TDES-XOR is allowed.	0045	ED	
	CSNBDSK	Key mode *rule_array* keyword VISA is allowed.			
	CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed.			
Diversified Key Generate - TDESEMV2/TDESEMV4	CSNBDKG	Processing method *rule_array* keywords TDESEMV2 and TDESEMV4 are allowed.	0046	ED	
	CSNBDSK	Key mode *rule_array* keyword EMV is allowed.			
	CSNBEAC	Key mode *rule_array* keyword EMV is allowed.			
	CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed.			
	CSNBEVF	Action *rule_array* keyword DECCNT is allowed.			
Diversified Key Generate - Allow wrapping override keywords	CSNBDKG	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	013D	ED	4.1
Diversified Key Generate - single length or same halves	CSNBDKG	When the processing method *rule_array* keyword is TDES-ENC or TDES-DEC, the *generated_key_identifier* parameter may specify a single-length key or a double-length key with equal key-halves.	0044	ED	
Diversified Key Generate - DKYGENKY - DALL	CSNBDKG CSNBPCU	When the key-generating key is a DKYGENKY key type, the control vector bits (19 – 22) may be B'1111'.	0290	DD, SC	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Diversified Key Generate2 – SESS-ENC	CSNBDKG2	Diversification process *rule_array* keyword SESS-ENC is allowed.	02CC	ED	4.4
Diversified Key Generate2 - Allow length option with KDFFM-DK	CSNBDKG2	When the Diversification process *rule_array* keyword is KDFFM-DK, the bit length *rule_array* keyword may be KLEN192 or KLEN256.	02D4	DD	4.4.5
Diversified Key Generate2 - DALL	CSNBDKG2	The key-generating key specified may have key-usage fields indicate that all key types may be derived.	02CD	DD, SC	4.4
Diversified Key Generate2 – KDFFM-DK	CSNBDKG2	Diversification process *rule_array* keyword KDFFM-DK is allowed.	02D3	ED	4.4.5
Diversified Key Generate2 - MK-OPTC	CSNBDKG2	Diversification process *rule_array* keyword MK-OPTC is allowed.	02D2	ED	4.4.5
Diversify Directed Key	CSNBDDK		0080	ED	4.5
Diversify Directed Key – Allow KDFFM DERIVE	CSNBDDK	Function *rule_array* keyword DERIVE is allowed.	0081	DD	4.5
Diversify Directed Key – Allow KDFFM GENERATE	CSNBDDK	Function *rule_array* keyword GENERATE is allowed.	0082	DD	4.5
DK Deterministic PIN Generate	CSNBDDPG		02C6	DD	4.4
DK Migrate PIN	CSNBDMP		02CE	DD	4.4
DK PAN Modify in Transaction	CSNBDPMT		02C5	DD	4.4
DK PAN Translate	CSNBDPT		02C6	DD	4.4
DK PIN Verify	CSNBDPV		02C1	DD	4.4
DK PIN Change	CSNBDPC		02C2	DD	4.4
DK PRW Card Number Update	CSNBPNU		02C3	DD	4.4
DK PRW Card Number Update2	CSNBDCU2		0025	DD	5.5/6.3
DK PRW CMAC Generate	CSNBDPCG		02C4	DD	4.4
DK Random PIN Generate	CSNBDRPG		02C0	DD	4.4
DK Random PIN Generate2	CSNBDRG2		0024	DD	5.5/6.3
DK Regenerate PRW	CSNBDRP		02C8	DD	4.4

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
ECC Diffie-Hellman	CSNDEDH		0360	ED	4.2
ECC Diffie-Hellman – Allow DERIV02	CSNDEDH	The key agreement *rule_array* keyword DERIVE02 is allowed.	03F5	ED	5.2
ECC Diffie-Hellman – Allow Prime Curve 192	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 192.	0363	ED	4.2
ECC Diffie-Hellman – Allow Prime Curve 224	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 224.	0364	ED	4.2
ECC Diffie-Hellman – Allow Prime Curve 256	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 256.	0365	ED	4.2
ECC Diffie-Hellman – Allow Prime Curve 384	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 384.	0366	ED	4.2
ECC Diffie-Hellman – Allow Prime Curve 521	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 521.	0367	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 160	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 160.	0368	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 192	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 192.	0369	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 224	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 224.	036A	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 256	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 256.	036B	ED	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
ECC Diffie-Hellman – Allow BP Curve 320	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 320.	036C	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 384	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 384.	036D	ED	4.2
ECC Diffie-Hellman – Allow BP Curve 512	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 512.	036E	ED	4.2
ECC Diffie-Hellman – Allow PASSTHRU	CSNDEDH	Key agreement *rule_array* keyword PASSTHRU is allowed.	0361	ED	4.2
ECC Diffie-Hellman – Allow key wrap override	CSNDEDH	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	0362	ED	4.2
ECC Diffie-Hellman – Prohibit weak key generate	CSNDEDH	The *output_key_identifier* parameter may specify a key that is stronger than the generating key.	036F	DD, SC	4.2
Encipher - DES	CSNBENC		000E	ED	
	CSNBESC	Action *rule_array* keywords SMCON and SMCONINT are allowed.			
	CSNBEVF	The action *rule_array* keyword is DACVER and DYNVER are allowed.			
Encrypted PIN Generate - 3624	CSNBEPG	Process rule *rule_array* keyword IBM-PIN is allowed.	00B0	ED	
Encrypted PIN Generate - GBP	CSNBEPG	Process rule *rule_array* keyword GBP-PIN is allowed.	00B1	ED	
Encrypted PIN Generate - Interbank	CSNBEPG	Process rule *rule_array* keyword INBK-PIN is allowed.	00B2	ED	
Encrypted PIN Translate - Translate	CSNBPTR CSNBPTRE	Process rule *rule_array* keyword TRANSLAT is allowed.	00B3	ED	
Encrypted PIN Translate - Reformat	CSNBPTR CSNBPTRE CSNBPTR2	Process rule *rule_array* keyword REFORMAT is allowed.	00B7	ED	
Encrypted PIN Translate Enhanced	CSNBPTRE		02D5	ED	5.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Encrypted PIN Translate2 – Permit ISO-0 to ISO-4 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-0, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed.	038E	ED	5.4
Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 RFMT1TO4.	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-1, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed. The output_PIN_encrypting_key_identifier must have key attribute RFMT1TO4 enabled.	0393	DD	5.4
Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-1, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed.	038C	ED	5.4
Encrypted PIN Translate2 – Permit ISO-4 to ISO-0 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-0, and the the *rule_array* mode keyword REFORMAT is allowed.	038F	ED	5.4
Encrypted PIN Translate2 – Permit ISO-4 to ISO-1 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-1, and the the *rule_array* mode keyword REFORMAT is allowed.	038D	ED	5.4
Encrypted PIN Translate2 – Permit ISO-4 to ISO-4 Translate	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword TRANSLAT is allowed.	038A	ED	5.4
Encrypted PIN Translate2 – Permit ISO-4 Reformat w/ PAN Chg	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT and the PAN change keyword PAN-CHG is allowed.	038B	DD	5.4
Encrypted PIN Translate2 - Permit ISO-4 to ISO-4 PTR2AUTH	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the rule_array mode keyword REFORMAT and the PAN change keyword PAN-CHG is allowed. In addition, the AES MAC key identified by the *authentication_key_identifier* must have the PTR2AUTH key usage attribute enabled.	0395	DD	5.5
Encrypted PIN Translate2 – REFORMAT with AES token	CSNBPTR2	Process rule rule_array keyword REFORMAT is allowed.	0391	ED	5.4

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Encrypted PIN Translate2 – TRANSLAT with AES token	CSNBPTR2	Process rule *rule_array* keyword TRANSLAT is allowed.	0392	ED	5.4
Encrypted PIN Verify - 3624	CSNBPVR	Algorithm value rule *rule_array* keywords IBM-PIN and IBM-PINO are allowed.	00AB	ED	
Encrypted PIN Verify - GPB	CSNBPVR	Algorithm value rule *rule_array* keyword GBP-PIN is allowed.	00AC	ED	
Encrypted PIN Verify - VISA PVV	CSNBPVR	Algorithm value rule *rule_array* keyword VISA-PVV is allowed.	00AD	ED	
Encrypted PIN Verify - Interbank	CSNBPVR	Algorithm value rule *rule_array* keyword INBK-PIN is allowed.	00AE	ED	
FPE Decrypt	CSNBFPED		02D0	ED	5.0
FPE Encrypt	CSNBFPEE		02CF	ED	5.0
FPE Translate	CSNBFPET		02D1	ED	5.0
HMAC Generate – SHA-1	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-1 is allowed.	00E4	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-1 is allowed.			
HMAC Generate – SHA-224	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-224 is allowed.	00E5	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-224 is allowed.			
HMAC Generate – SHA-256	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-256 is allowed.	00E6	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-256 is allowed.			
HMAC Generate – SHA-384	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-384 is allowed.	00E7	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-384 is allowed.			
HMAC Generate – SHA-512	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-512 is allowed.	00E8	ED	4.1

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-512 is allowed.			
HMAC Verify – SHA-1	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-1 is allowed.	00F7	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-1 is allowed.			
HMAC Verify – SHA-224	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-224 is allowed.	00F8	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-224 is allowed.			
HMAC Verify – SHA-256	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-256 is allowed.	00F9	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-256 is allowed.			
HMAC Verify – SHA-384	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-384 is allowed.	00FA	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-384 is allowed.			
HMAC Verify – SHA-512	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-512 is allowed.	00FB	ED	4.1
	CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-512 is allowed.			
Key Encryption Translate – CBC to ECB	CSNBKET	Key translation *rule_array* keyword CBCTOECB is allowed.	030D	DD ED on z13 and later servers	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Key Encryption Translate – ECB to CBC	CSNBKET	Key translation *rule_array* keyword ECBTOCBC is allowed.	030E	DD ED on z13 and later servers	
Key Export	CSNBKEX		0013	ED	
	CSNBDCM	Key encryption *rule_array* keyword XPORT is allowed.			
	CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.			
Key Export - Unrestricted	CSNBKEX	The key identifier specified in the *exporter_key_identifier* parameter may be an exporter with equal key halves.	0276	ED	
Key Generate – OP	CSNBKGN	This combination is allowed: the value of the *key_form* parameter OP and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the OP column.	008E	ED	
	CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.			
	CSNBRNG				
Key Generate – Key set	CSNBKGN	These combinations are allowed: • The value of the *key_form* parameter is EX and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the EX column. • The value of the *key_form* parameter is IM and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the IM column. • The value in the *key_form* parameter is OPEX, EXEX, OPIM, OPOP, IMIM, or IMEX and the key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key Generate Valid Key Types and Key Forms for a Key Pair* table in the column matching the key form.	008C	ED	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Key Generate – Key set extended	CSNBKGN	This combination is allowed: the value of the *key_form* parameter is OPEX, OPIM, OPOP, IMIM, or IMEX and the key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key Generate Valid Key Types and Key Forms for a Key Pair* table in the column matching the key form.	00D7	ED	
Key Generate - SINGLE-R	CSNBKGN	A value of SINGLE-R is allowed in the *key_length* parameter.	00DB	ED	
	CSNDRKX	A single-length source key will be replicated when the following conditions are met: 1. The key token returned using the *sym_encrypted_key_identifier* parameter is a fixed-length DES key token, as defined in the rule section identified by the *rule_id* parameter 2. The rule section identified by the *rule_id* parameter has a common export key parameters subsection defined, and the control vector in the subsection is 16 bytes in length with key-form bits of B'010' for the left half and B'001' for the right half. 3. The token identified by the *source_key_identifier* parameter is single length, either a fixed-length DES token or an RKX token.			
Key Generate2 – DK PIN admin1 key MAC	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX, OPIM, OPOP, IMIM, or IMEX and key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	02BE	DD	4.4
Key Generate2 – DK PIN admin1 key PINPROT	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	02BD	DD	4.4
Key Generate2 – DK PIN admin2 key MAC	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	02BF	DD	4.4

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Key Generate2 – DK PIN key set	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPIM, OPOP, or IMIM and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	02BB	DD	4.4
Key Generate2 – DK PIN print key	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	02BC	DD	4.4
Key Generate2 – Key set	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX, EXEX, OPIM, OPOP, IMIM, or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key Generate2 Valid key type and key forms for two AES or HMAC keys* table or the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	00EB	ED	4.1
Key Generate2 – Key set extended	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key Generate2 Valid key type and key forms for two AES or HMAC keys* table in the column matching the key form.	00EC	ED	4.3
Key Generate2 – OP	CSNBKGN2	Key form *rule_array* keywords OP, IM, and EX are allowed.	00EA	ED	4.1
Key Import	CSNBKIM		0012	ED	
	CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.			
Key Import - Unrestricted	CSNBKIM	The key identifier specified in the *importer_key_identifier* parameter may be an importer with equal key halves.	027B	ED	
Key Part Import - First key part	CSNBKPI	Key part *rule_array* keyword FIRST is allowed.	001B	ED	
Key Part Import - Middle and final	CSNBKPI	Key part *rule_array* keywords MIDDLE and FINAL are allowed.	001C	ED	
Key Part Import - ADD-PART	CSNBKPI	Key part *rule_array* keyword ADD-PART is allowed.	0278	ED	
Key Part Import - COMPLETE	CSNBKPI	Key part *rule_array* keyword COMPLETE is allowed.	0279	ED	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Key Part Import - Allow wrapping override keywords	CSNBKPI	Key wrapping method *rule_array* keywords WRAP-ECB or WRAP-ENH are allowed.	0140	ED	4.1
Key Part Import - Unrestricted	CSNBKPI	The key identifier specified in the *key_identifier* parameter may be a key with equal key halves.	027A	ED	
Key Part Import2 – Load first key part, require 3 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN3PART is allowed.	0297	ED	4.1
Key Part Import2 – Load first key part, require 2 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN2PART is allowed.	0298	ED	4.1
Key Part Import2 - Load first key part, require 1 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN1PART is allowed.	0299	ED	4.1
Key Part Import2 - Add second of 3 or more key parts	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	029A	ED	4.1
Key Part Import2 - Add last required key part	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	029B	ED	4.1
Key Part Import2 - Add optional key part	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	029C	ED	4.1
Key Part Import2 – Complete key	CSNBKPI2	Key part *rule_array* keyword COMPLETE is allowed.	029D	ED	4.1
Key Test and Key Test2	CSNBKYT CSNBKYTX CSNBKYT2		001D	AE	
Key Test2 – AES, ENC-ZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword AES and Verification pattern calculation algorithm *rule_array* keyword ENC-ZERO is allowed.	0021	AE	4.2
Key Test2 – AES, CMACZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword AES and the Verification pattern calculation algorithm *rule_array* keyword CMACZERO is allowed.	0022	ED	5.2
Key Test2 – DES, CMACZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword DES and the Verification pattern calculation algorithm *rule_array* keyword CMACZERO is allowed.	0023	ED	5.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Key Test - Warn when keyword inconsistent with key length	CSNBKYT CSNBKYTX	The key rule *rule_array* keyword specified does not match the DES encrypted key token in the *key_identifier* parameter.	01CB	DD	4.4
Key Translate	CSNBKTR		001F	ED	
Key Translate2 - Translate	CSNBKTR2		0149	ED	4.2
Key Translate2 - Allow use of REFORMAT	CSNBKTR2	Encipherment *rule_array* keyword REFORMAT is allowed.	014B	ED	4.1
Key Translate2 - Allow wrapping override keywords	CSNBKTR2	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	014A	ED	4.1
Key Translate2 - COMP-CHK	CSNBKTR2	Encipherment *rule_array* keyword COMP-CHK is allowed.	02F8	ED	6.0
Key Translate2 - COMP-TAG	CSNBKTR2	Encipherment *rule_array* keyword COMP-TAG is allowed.	02F9	ED	6.0
Key Translate2 - Disallow AES ver 5 to ver 4 conversion	CSNBKTR2	When the key token supplied in the *input_key_token* parameter is a version 5 AES key token, the token cannot be converted to a version 4 token.	032A	DD	4.2
Key Translate2 – Translate fixed to variable payload	CSNBKTR2	The key token supplied in the *input_key_token* parameter with a fixed-length payload will be re-enciphered with a variable-length payload.	0334	DD, SC	4.4
MAC Generate	CSNBEAC	Action *rule_array* keyword GENARPC and VERGEN are allowed.	0010	ED	
	CSNBESC	Action *rule_array* keywords SMINT, SMCONINT, and SMCIPIN are allowed.			
	CSNBMGN				
MAC Generate2 – AES CMAC	CSNBMGN2 CSNBMGN3	Token algorithm *rule_array* keyword AES is allowed.	0336	ED	4.4
MAC Verify	CSNBEAC	Action *rule_array* keywords VERARQC and VERGEN is allowed.	0011	ED	
	CSNBMVR				
MAC Verify2 – AES CMAC	CSNBMVR2 CSNBMVR3	Token algorithm *rule_array* keyword AES is allowed.	0337	ED	4.4
Multiple Clear Key Import/Multiple Secure Key Import - AES	CSNBCKM	Algorithm *rule_array* keyword AES is allowed.	0129	ED	3.30
	CSNBSKM	The combination of algorithm *rule_array* keyword AES and the value of OP specified in the *key_form* parameter is allowed.			

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Multiple Clear Key Import - Allow wrapping override keywords	CSNBCKM	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	0141	ED	4.1
Multiple Secure Key Import - Allow wrapping override keywords	CSNBSKM	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	0142	ED	4.1
Permit X.509 without PKI root validation	CSNDDSV CSNDPKE CSNDSYX CSNDSYG CSNDT34B CSNDT34C CSNDT34D CSNDT34R	Public Key Infrastructure Usage *rule_array* keyword PKI-NONE is allowed.	01FF	ED	6.3
PIN Change/Unblock – change EMV PIN with OPINENC	CSNBESC	Action *rule_array* keyword VISAPIN is allowed.	00BC	ED	
	CSNBPCU	The key type of the PIN block encrypting key may be OPINENC.			
PIN Change/Unblock – change EMV PIN with IPINENC	CSNBESC	Action *rule_array* keyword VISAPIN is allowed.	00BD	ED	
	CSNBPCU	The key type of the PIN block encrypting key may be IPINENC.			
PKA Decrypt	CSNDPKD		011F	ED	
PKA Decrypt – Disallow PKCS-1.2	CSNDPKD	Recovery Method *rule_array* keyword can not be PKCS-1.2.	020A	DD	4.4.5
PKA Decrypt – Disallow ZEROPAD	CSNDPKD	Recovery Method *rule_array* keyword can not be ZEROPAD.	020B	DD	4.4.5
PKA Decrypt – Disallow PKCSOAEP	CSNDPKD	Recovery Method *rule_array* keyword can not be PKCSOAEP.	020C	DD	4.4.5
PKA Encrypt	CSNDPKE		011E	ED	
PKA Encrypt – Disallow PKCS-1.2	CSNDPKE	Recovery Method *rule_array* keyword can not be PKCS-1.2.	0206	DD	4.4.5
PKA Encrypt – Disallow ZEROPAD	CSNDPKE	Recovery Method *rule_array* keyword can not be ZEROPAD.	0207	DD	4.4.5
PKA Encrypt – Disallow MRP	CSNDPKE	Recovery Method *rule_array* keyword can not be MRP.	0208	DD	4.4.5
PKA Encrypt – Disallow PKCSOAEP	CSNDPKE	Recovery Method *rule_array* keyword can not be PKCSOAEP.	0209	DD	4.4.5
PKA Key Generate	CSNDPKG		0103	ED	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
PKA Key Generate – Clear RSA keys	CSNDPKG	The combination of Private Key Encryption *rule_array* keyword CLEAR and the algorithm of the skeleton key supplied in the *skeleton_key_identifier* parameter being RSA is allowed.	0205	ED	
PKA Key Generate – Clear ECC keys	CSNDPKG	The combination of Private Key Encryption *rule_array* keyword CLEAR and the algorithm of the skeleton key supplied in the *skeleton_key_identifier* parameter being ECC is allowed.	0326	ED	4.0
PKA Key Generate – Clone	CSNDPKG	Private Key Encryption *rule_array* keyword CLONE is allowed.	0204	ED	
PKA Key Generate - Permit Regeneration Data	CSNDPKG	The use of the *regeneration_data* parameter is allowed with the Private Key Encryption *rule_array* keywords MASTER, XPORT, and CLEAR.	027D	ED	
PKA Key Generate - Permit Regeneration Data Retain	CSNDPKG	The use of the *regeneration_data* parameter is allowed with the Private Key Encryption *rule_array* keyword RETAIN.	027E	ED	
PKA Key Import	CSNDPKI		0104	ED	
PKA Key Import – Disallow clear key import	CSNDPKI	The key token supplied in the *source_key_token* parameter can not contain a clear key.	003A	DD	5.2
PKA Key Import - Import an external trusted block	CSNDPKI	The token supplied in the *source_key_token* parameter may be a trusted block.	0311	ED	
PKA Key Token Change RTCMK	CSNDKTC		0102	ED	
PKA Key Translate - from CCA RSA to SC Visa format	CSNDPKT	Output format *rule_array* keyword SCVISA is allowed.	0318	ED	3.60
PKA Key Translate - from CCA RSA to SC ME format	CSNDPKT	Output format *rule_array* keyword SCCOMME is allowed.	0319	ED	3.60
PKA Key Translate - from CCA RSA to SC CRT format	CSNDPKT	Output format *rule_array* keyword SCCOMCRT is allowed.	031A	ED	3.60
PKA Key Translate – Translate internal key token	CSNDPKT	Output format *rule_array* keyword INTDWAKW is allowed.	00FE	ED	4.3
PKA Key Translate – Translate external key token	CSNDPKT	Output format *rule_array* keyword EXTDWAKW is allowed.	00FF	ED	4.3

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
PKA Key Translate - from source EXP KEK to target EXP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an EXPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an EXPORTER key-encrypting key is allowed	031B	ED	3.60
PKA Key Translate - from source IMP KEK to target EXP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an IMPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an EXPORTER key-encrypting key is allowed	031C	ED	3.60
PKA Key Translate - from source IMP KEK to target IMP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an IMPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an IMPORTER key-encrypting key is allowed	031D	ED	3.60
PKA Key Translate - from CCA RSA CRT to EMVDDA format	CSNDPKT	Output format *rule_array* keyword EMVDDA is allowed	0338	ED	4.4
PKA Key Translate - from CCA RSA CRT to EMVDDAE format	CSNDPKT	Output format *rule_array* keyword EMVDDAE is allowed	0339	ED	4.4
PKA Key Translate - from CCA RSA CRT to EMVCRT format	CSNDPKT	Output format *rule_array* keyword EMVCRT is allowed	033A	ED	4.4
PKA Key Translate – allow COMP-CHK	CSNDPKT	Conversion service rule_array keyword COMP-CHK is allowed.	01EF	ED	6.3
PKA Key Translate – allow COMP-TAG	CSNDPKT	Conversion service rule_array keyword is COMP-TAG allowed.	01EE	ED	6.3
PKA Key Translate – allow INTUSCHG	CSNDPKT	Conversion service rule_array keyword is INTUSCHG allowed.	02EE	ED	6.3
Prohibit Export	CSNBPEX		00CD	ED	
Prohibit Export Extended	CSNBPEXX		0301	ED	
Public Infrastructure Certificate	CSNDPIC		0070	ED	6.0
Public Infrastructure Certificate - PK10SNRQ	CSNDPIC		007C	ED	6.0
Recover PIN From Offset	CSNBPFO		02B0	ED	4.4

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Remote Key Export - Gen or export a non-CCA node key	CSNDRKX		0312	ED	
Remote Key Export - include RKX in default wrap config	CSNDRKX	Key wrapping method *rule_array* keywords USECONFG, WRAP-ECB, WRAP-ENH, and ENH-ONLY are allowed	013F	DD	4.4
Remote Key Export – Allow wrapping override keywords	CSNDRKX	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	02BA	DD	4.4
Restrict Key Attribute – Export Control	CSNBRKA	Token type *rule_array* keywords AES and HMAC are allowed.	00E9	ED	4.1
Restrict Key Attribute – Permit setting the TR-31 export bit	CSNBRKA	Token type *rule_array* keyword DES is allowed and Export control keyword NOT31XPT is allowed.	0154	ED	4.2
Retained Key Delete	CSNDRKD		0203	ED	
Retained Key List	CSNDRKL		0230	ED	
Secure Key Import – DES, IM	CSNBSKI	The value of the *key_form* parameter may be IM.	00DC	ED	
	CSNBSKM	The combination of the Algorithm *rule_array* keyword being DES and the value of the *key_form* parameter being IM is allowed.			
Secure Key Import – DES, OP	CSNBSKI	The value of the *key_form* parameter may be OP.	00C4	ED	
	CSNBSKM	The combination of the Algorithm *rule_array* keyword being DES and the value of the *key_form* parameter being OP is allowed.			
Secure Key Import2 - OP	CSNBSKI2	Key form *rule_array* keyword OP is allowed.	00F2	ED	4.1
Secure Key Import2 - IM	CSNBSKI2	Key form *rule_array* keyword IM is allowed.	00F3	ED	4.1
Secure Messaging for Keys	CSNBSKY		0273	ED	
Secure Messaging for PINs	CSNBESC	Action *rule_array* keyword SMCIPIN is allowed.	0274	ED	
	CSNBSPN				
SET Block Compose	CSNDSBC		010B	ED	
SET Block Decompose	CSNDSBD		010C	ED	
SET Block Decompose - PIN ext IPINENC	CSNDSBD	The combination of the Formatting information *rule_array* keyword being PINBLOCK and the key type of the PIN block encrypting key being IPINENC is allowed.	0121	ED	

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
SET Block Decompose - PIN ext OPINENC	CSNDSBD	The combination of the Formatting information *rule_array* keyword being PINBLOCK and the key type of the PIN block encrypting key being OPINENC is allowed.	0122	ED	
Symmetric Algorithm Decipher - GCM/Counter mode AES	CSNBSAD CSNBSAD1	Processing rule *rule_array* keyword GCM is allowed.	01CE	ED	5.2
Symmetric Algorithm Decipher - Secure AES keys	CSNBSAD CSNBSAD1		012B	ED	3.30
Symmetric Algorithm Encipher - GCM/Counter mode AES	CSNBSAE CSNBSAE1	Processing rule *rule_array* keyword GCM is allowed.	01CD	ED	5.2
Symmetric Algorithm Encipher - Secure AES keys	CSNBSAE CSNBSAE1		012A	ED	3.30
Symmetric Key Export with Data	CSNDSXD		02B5	ED	4.4
Symmetric Key Export with Data - Special	CSNDSXD	The key identifier supplied in the *source_key_identifier* parameter need not be key type DATAC or key type DKYGENKY with subtype DKYL0.	02B6	DD	4.4
Symmetric Key Export – AES, PKCSOAEP, PKCS-1.2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and the Key formatting method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	0130	ED	3.30
	CSNDSXD	The combination of the *rule_array* keywords being AES and PKCS-EXT is allowed			
Symmetric Key Export – AES, PKOAEP2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being PKOAEP2 is allowed.	00FC	ED	4.1
Symmetric Key Export – AES, ZERO-PAD	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	0131	ED	3.30
Symmetric Key Export - AESKW	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES or HMAC and and Key formatting method *rule_array* keyword being AESKW is allowed.	0327	ED	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Symmetric Key Export - AESKWCV	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being AESKWCV is allowed.	02B3	ED	4.4
Symmetric Key Export – DES, PKCS-1.2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and and Key formatting method *rule_array* keyword being PKCS-1.2 is allowed.	0105	ED	
	CSNDSXD	The combination of the *rule_array* keywords being DES and PKCS-EXT is allowed			
Symmetric Key Export – DES, ZERO-PAD	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	023E	ED	
Symmetric Key Export – HMAC, PKOAEP2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being HMAC and and Key formatting method *rule_array* keyword being PKOAEP2 is allowed.	00F5	ED	4.1
Symmetric Key Generate - AES, PKCSOAEP, PKCS-1.2	CSNDSYG	The combination of the Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	012C	ED	3.30
Symmetric Key Generate - AES, ZERO-PAD	CSNDSYG	The combination of the Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	012D	ED	3.30
Symmetric Key Generate - DES, PKCS-1.2	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and and Key formatting method *rule_array* keyword being PKCS-1.2 is allowed.	023F	ED	
Symmetric Key Generate - DES, ZERO-PAD	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	023C	ED	
Symmetric Key Generate – DES, PKA92	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being PKA92 is allowed.	010D	ED	
Symmetric Key Generate - Allow wrapping override keywords	CSNDSYG	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	013E	ED	4.1

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Symmetric Key Import – AES, PKCSOAEP, PKCS-1.2	CSNDSYI	The combination of the Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	012E	ED	3.30
Symmetric Key Import – AES, ZERO-PAD	CSNDSYI	The combination of the Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being ZEROPAD is allowed.	012F	ED	3.30
Symmetric Key Import – DES, PKCS-1.2	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and and Recovery method *rule_array* keyword being PKCS-1.2 is allowed.	0106	ED	
Symmetric Key Import – DES, ZERO-PAD	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword being ZEROPAD is allowed.	023D	ED	
Symmetric Key Import – DES, PKA92 KEK	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword being PKA92 is allowed.	0235	ED	
Symmetric Key Import - Allow wrapping override keywords	CSNDSYI	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	0144	ED	4.1
Symmetric Key Import2 – AES, PKOAEP2	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being PKOAEP2 is allowed.	00FD	ED	4.2
Symmetric Key Import2 - AESKW	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being AES or HMAC and Recovery method *rule_array* keyword being AESKW is allowed.	0329	ED	4.2
Symmetric Key Import2 - AESKWCV	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword i being s AESKWCV is allowed.	02B4	ED	4.4
Symmetric Key Import2 - Allow wrapping override keywords	CSNDSYI2	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH is allowed.	02B9	ED	4.4
Symmetric Key Import2 – disallow weak import	CSNDSYI	The key identifier supplied in the *RSA_private_key_identifier* parameter may not be weaker than the key being imported in the *RSA_enciphered_key* parameter.	032B	DD, SC	4.2
	CSNDSYI2	The key identifier supplied in the *transport_key_identifier* parameter may not be weaker than the key being imported in the *encipher_key* parameter.			

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
	CSNBUKD	The key identifier supplied in the *transport_key_identifier* parameter may not be weaker than the keys being derived and returned in the *generated_key_identifier1, generated_key_identifier2*, and *generated_key_identifier3* parameters.			
Symmetric Key Import2 – HMAC, PKOAEP2	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being HMAC and recovery method *rule_array* keyword being PKOAEP2 is allowed.	00F4	ED	4.1
T31I - Permit version A TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID A.	0150	ED	4.2
T31I - Permit version B TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID B.	0151	ED	4.2
T31I - Permit version C TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID C.	0152	ED	4.2
T31I - Permit version D TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID D.	0386	DD	4.5
T31I - Permit override of default wrapping method	CSNBT31I	The key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	0153	ED	4.2
T31I - Permit C0:G/C/V to DES MAC/MACVER:CVVKEY-A	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *V TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	015A	DD	4.2
T31I - Permit C0:G/C/V to DES MAC/MACVER:AMEX-CSC	CSNBT31I		015B	DD	4.2
T31I - Permit K0:E to DES EXPORTER/OKEYXLAT	CSNBT31I		015C	DD	4.2
T31I - Permit K0:B to DES EXPORTER/OKEYXLAT	CSNBT31I		015E	DD	4.2
T31I - Permit K0:D to DES IMPORTER/IKEYXLAT	CSNBT31I		015D	DD	4.2
T31I - Permit K0:B to DES IMPORTER/IKEYXLAT	CSNBT31I		015F	DD	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31I - Permit K1/K4:E to DES EXPORTER/OKEYXLAT	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	0160	DD	4.2
T31I - Permit K1/K4:D to DES IMPORTER/IKEYXLAT	CSNBT31I		0161	DD	4.2
T31I - Permit K1/K4:B to DES EXPORTER/OKEYXLAT	CSNBT31I		0162	DD	4.2
T31I - Permit K1/K4:B to DES IMPORTER/IKEYXLAT	CSNBT31I		0163	DD	4.2
T31I - Permit M0/M1/M3:G/C/V to DES MAC/MACVER:ANY-MAC	CSNBT31I		0164	ED	4.2
T31I - Permit P0:E to DES OPINENC	CSNBT31I		0165	ED	4.2
T31I - Permit P0:D to DES IPINENC	CSNBT31I		0166	ED	4.2
T31I - Permit V0:N/G/C to DES PINGEN:NO-SPEC NOOFFSET	CSNBT31I		0167	DD	4.2
T31I - Permit V0:N/V to DES PINVER:NO-SPEC NOOFFSET	CSNBT31I		0168	DD	4.2
T31I - Permit V1:N/G/C to DES PINGEN:IBM-PIN/IBM-PINO NOOFFSET	CSNBT31I		0169	ED	4.2
T31I - Permit V1:N/V to DES PINVER:IBM-PIN/IBM-PINO NOOFFSET	CSNBT31I		016A	ED	4.2
T31I - Permit V2:N/G/C to DES PINGEN:VISA-PVV	CSNBT31I		016B	ED	4.2
T31I - Permit V2:N/V to DES PINVER:VISA-PVV	CSNBT31I		016C	ED	4.2
T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		016D	DD	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMV	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	016E	DD	4.2
T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMAC	CSNBT31I		016F	DD	4.2
T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMV	CSNBT31I		0170	DD	4.2
T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DMPIN	CSNBT31I		0171	DD	4.2
T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		0172	DD	4.2
T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DMPIN	CSNBT31I		0173	DD	4.2
T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DDATA	CSNBT31I		0174	DD	4.2
T31I - Permit E2:N/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		0175	DD	4.2
T31I - Permit E2:N/X to DES DKYGENKY:DKYL1+DMAC	CSNBT31I		0176	DD	4.2
T31I - Permit E3:N/E/D/B/G/X to DES ENCIPHER	CSNBT31I		0177	DD	4.2
T31I - Permit E4:N/B/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		0178	DD	4.2
T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		0179	DD	4.2
T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		017A	DD	4.2
T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DEXP	CSNBT31I		017B	DD	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31I - Permit V0/V1/V2:N to DES PINGEN/PINVER	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *V TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	017C	DD	4.2
T31I - Permit D0:E/D/B to AES CIPHER:ENC/DEC/ENC+DEC	CSNBT31I		01E0	ED	4.5
T31I - Permit M6:G/C/V to AES MAC:CMAC+GENONLY/GEN/VER	CSNBT31I		01E1	ED	4.5
T31I - Permit P0:E/D to AES PINPROT:ENC/DEC+CBC+ISO-4	CSNBT31I		01E2	ED	4.5
T31I - Permit K0:E to AES EXPORTER	CSNBT31I		01E3	ED	4.5
T31I - Permit K0:D to AES IMPORTER	CSNBT31I		01E4	ED	4.5
T31I - Permit K1/K4:E to AES EXPORTER:EXPTT31D+VARDRV-D	CSNBT31I		01E5	ED	4.5
T31I - Permit AES K1/K4:D to AES IMPORTER:IMPTT31D+VARDRV-D	CSNBT31I		01E6	ED	4.5
T31I - Permit E0:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	CSNBT31I		01E7	ED	4.5
T31I - Permit E1:X to AES DKYGENKY:DKYL0/L1/L2+D-SECMSG+SMPIN	CSNBT31I		01E8	ED	4.5
T31I - Permit E2:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	CSNBT31I		01E9	ED	4.5
T31I - Permit E3:X to AES DKYGENKY:D-CIPHER+ENC+DEC+CBC	CSNBT31I		01EA	ED	4.5

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31I - Permit E3:E/B to AES CIPHER:ENCRYPT/ENC+DEC	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *V TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	01EB	ED	4.5
T31I - Permit E4:X to AES DKYGENKY:DKYL0/L1/L2+D-CIPHER+ENC+DEC	CSNBT31I		01EC	ED	4.5
T31I - Permit E5:X to AES DKYGENKY:DKYL0/L1/L2/D-MAC+GEN+CMAC	CSNBT31I		01ED	ED	4.5
T31X - Permit version A TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARXOR-A is allowed.	014D	ED	4.2
T31X - Permit version B TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARDRV-B is allowed.	014E	ED	4.2
T31X - Permit version C TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARXOR-C is allowed.	014F	ED	4.2
T31X - Permit version D TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARDRV-D is allowed.	0382	DD	4.5
T31X - Permit any CCA DES key if INCL-CV is specified	CSNBT31X	The key identifier supplied in the source_key_identifier parameter may be any key type when the Control vector transport control *rule_array* keyword is INCL-CV.	0158	ED	4.2
T31X - Permit DES KEYGENKY: DUKPT to B0:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	0180	ED	4.2
T31X - Permit DES MAC/MACVER:AMEX-CSC to C0:G/C/V	CSNBT31X		0181	DD	4.2
T31X - Permit DES MAC/MACVER: CVV-KEYA to C0:G/C/V	CSNBT31X		0182	DD	4.2
T31X - Permit DES MAC/MACVER: ANY-MAC to C0:G/C/V	CSNBT31X		0183	ED	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31X - Permit DES DATA/DATAM/DATAMV to C0:G/C/V	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	0184	ED	4.2
T31X - Permit DES ENCIPHER/DECIPHER/CIPHER to D0:E/D/B	CSNBT31X		0185	ED	4.2
T31X - Permit DES DATA to D0:E/D/B	CSNBT31X		0186	ED	4.2
T31X - Permit DES EXPORTER/OKEYXLAT to K0:E	CSNBT31X		0187	DD	4.2
T31X - Permit DES IMPORTER/IKEYXLAT to K0:D	CSNBT31X		0188	DD	4.2
T31X - Permit DES EXPORTER/OKEYXLAT to K1/K4:E	CSNBT31X		0189	DD	4.2
T31X - Permit DES IMPORTER/IKEYXLAT to K1/K4:D	CSNBT31X		018A	DD	4.2
T31X - Permit DES MAC/DATA/DATAM to M0:G/C	CSNBT31X		018B	DD	4.2
T31X - Permit DES MACVER/DATA/DATAMV to M0:V	CSNBT31X		018C	ED	4.2
T31X - Permit DES MAC/DATA/DATAM to M1:G/C	CSNBT31X		018D	ED	4.2
T31X - Permit DES MACVER/DATA/DATAMV to M1:V	CSNBT31X		018E	ED	4.2
T31X - Permit DES MAC/DATA/DATAM to M3:G/C	CSNBT31X		018F	ED	4.2
T31X - Permit DES MACVER/DATA/DATAMV to M3:V	CSNBT31X		0190	ED	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31X - Permit DES OPINENC to P0:E	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	0191	ED	4.2
T31X - Permit DES IPINENC to P0:D	CSNBT31X		0192	ED	4.2
T31X - Permit DES PINVER: NO-SPEC to V0:N/V	CSNBT31X		0193	DD	4.2
T31X - Permit DES PINGEN: NO-SPEC to V0:N/C	CSNBT31X		0194	DD	4.2
T31X - Permit DES PINVER: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V	CSNBT31X		0195	ED	4.2
T31X - Permit DES PINGEN: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V	CSNBT31X		0196	ED	4.2
T31X - Permit DES PINVER: NO-SPEC/VISA-PVV to V2:N/V	CSNBT31X		0197	ED	4.2
T31X - Permit DES PINGEN: NO-SPEC/VISA-PVV to V2:N/C	CSNBT31X		0198	ED	4.2
T31X - Permit DES DKYGENKY: DKYL0+DMAC to E0:N/X	CSNBT31X		0199	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DMV to E0:N/X	CSNBT31X		019A	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DALL to E0:N/X	CSNBT31X		019B	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DMAC to E0:N/X	CSNBT31X		019C	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DMV to E0:N/X	CSNBT31X		019D	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DALL to E0:N/X	CSNBT31X		019E	DD	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31X - Permit DES DKYGENKY: DKYL0+DDATA to E1:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	019F	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DMPIN to E1:N/X	CSNBT31X		01A0	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DALL to E1:N/X	CSNBT31X		01A1	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DDATA to E1:N/X	CSNBT31X		01A2	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DMPIN to E1:N/X	CSNBT31X		01A3	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DALL to E1:N/X	CSNBT31X		01A4	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DMAC to E2:N/X	CSNBT31X		01A5	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DALL to E2:N/X	CSNBT31X		01A6	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DMAC to E2:N/X	CSNBT31X		01A7	DD	4.2
T31X - Permit DES DKYGENKY: DKYL1+DALL to E2:N/X	CSNBT31X		01A8	DD	4.2
T31X - Permit DES DATA/DATAM/CIPHER/MAC/ENCIPHER to E3:N/G/E/X	CSNBT31X		01A9	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DDATA to E4:N/X	CSNBT31X		01AA	ED	4.2
T31X - Permit DES DKYGENKY: DKYL0+DALL to E4:N/X	CSNBT31X		01AB	ED	4.2
T31X - Permit DES DKYGENKY: DKYL0+DEXP to E5:N/X	CSNBT31X		01AC	DD	4.2

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31X - Permit DES DKYGENKY: DKYL0+DMAC to E5:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	01AD	DD	4.2
T31X - Permit DES DKYGENKY: DKYL0+DDATA to E5:N/X	CSNBT31X		01AE	DD	4.2
T31X - Permit DES DKYGENKY:DKYL0+DALL to E5:N/X	CSNBT31X		01AF	ED	4.2
T31X - Permit DES PINGEN to V0:N and DES PINVER to V1/V2:N	CSNBT31X		01B0	DD	4.2
T31X - Permit AES CIPHER to D0:E/D/B	CSNBT31X		01D0	ED	5.4
T31X - Permit AES MAC: CMAC to M6:G/C/V	CSNBT31X		01D1	ED	5.4
T31X - Permit AES PINPROT to P0:E/D	CSNBT31X		01D2	ED	5.4
T31X - Permit AES EXPORTER to K0:E	CSNBT31X		01D3	ED	5.4
T31X - Permit AES EXPORTER to K1:E	CSNBT31X		01D4	ED	5.4
T31X - Permit AES EXPORTER to K4:E	CSNBT31X		01D5	ED	5.4
T31X - Permit AES IMPORTER to K0:D	CSNBT31X		01D6	ED	5.4
T31X - Permit AES IMPORTER to K1:D	CSNBT31X		01D7	ED	5.4
T31X - Permit AES IMPORTER to K4:D	CSNBT31X		01D8	ED	5.4
T31X - Permit AES DKYGENKY:D-ALL/DMAC to E0:X	CSNBT31X		01D9	ED	5.4

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
T31X - Permit AES DKYGENKY:D-ALL/DCIPHER to E1:X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	01DA	ED	5.4
T31X - Permit AES DKYGENKY:D-ALL/D-MAC to E2:X	CSNBT31X		01DB	ED	5.4
T31X - Permit AES CIPHER to E3/E/B,DKYGENKY:D-ALL/DCIP to E3:X	CSNBT31X		01DC	ED	5.4
T31X - Permit AES DKYGENKY:D-ALL/D-CIPHER to E4:X	CSNBT31X		01DD	ED	5.4
T31X - Permit AES DKYGENKY:D-MAC to E5:X	CSNBT31X		01DE	ED	5.4
T31X - Permit DES DKYGENKY: DKYL0:DMPIN to 12:X	CSNBT31X		0385	DD	5.4
T31X - Permit AES KDKGENKY: KDKTYPEA to 11:X	CSNBT31X		0383	DD	5.4
T31X - Permit AES KDKGENKY: KDKTYPEB to 10:X	CSNBT31X		0384	DD	5.4
TR-34 Bind-Begin	CSNDT34B		01F0	ED	6.3
TR-34 Bind-Begin - allow BINDCR	CSNDT34B	Requested action *rule_array* keyword BINDCR is allowed.	01F1	ED	6.3
TR-34 Bind-Begin - allow UNBINDCR	CSNDT34B	Requested action *rule_array* keyword UNBINDCR is allowed.	01F2	ED	6.3
TR-34 Bind-Begin - allow REBINDCR	CSNDT34B	Requested action *rule_array* keyword REBINDCR is allowed.	01F3	ED	6.3
TR-34 Bind-Complete	CSNDT34C		01F4	ED	6.3
TR-34 Bind-Complete - allow BINDKRDC	CSNDT34C	Requested action *rule_array* keyword BINDKRDC is allowed.	01F5	ED	6.3
TR-34 Bind-Complete - allow BINDRV	CSNDT34C	Requested action *rule_array* keyword BINDRV is allowed.	01F6	ED	6.3

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
TR-34 Bind-Complete - allow UNBINDRV	CSNDT34C	Requested action *rule_array* keyword UNBINDRV is allowed.	01F7	ED	6.3
TR-34 Bind-Complete - allow REBINDRV	CSNDT34C	Requested action *rule_array* keyword REBINDRV is allowed.	01F8	ED	6.3
TR-34 Key Distribution	CSNDT34D		01F9	ED	6.3
TR-34 Key Distribution – Allow 2PASSCRE	CSNDT34D	Requested action *rule_array* keyword 2PASSCRE is allowed.	01FA	ED	6.3
TR-34 Key Distribution – Allow 1PASSCRE	CSNDT34D	Requested action *rule_array* keyword 1PASSCRE is allowed.	01FB	ED	6.3
TR-34 Key Distribution - Permit DES EXPORTER to K0 or K1	CSNDT34D	Permits the export of a DES EXPORTER with TR-31 key usage K0 or K1.	0242	ED	6.3
TR-34 Key Distribution - Permit DES IMPORTER to K0 or K1	CSNDT34D	Permits the export of a DES IMPORTER with TR-31 key usage K0 or K1.	0243	ED	6.3
TR-34 Key Distribution - Permit AES EXPORTER to K0	CSNDT34D	Permits the export of a AES EXPORTER with TR-31 key usage K0.	0244	ED	6.3
TR-34 Key Distribution - Permit AES EXPORTER to K1	CSNDT34D	Permits the export of a AES EXPORTER with TR-31 key usage K1.	0245	ED	6.3
TR-34 Key Distribution - Permit AES IMPORTER to K0	CSNDT34D	Permits the export of a AES IMPORTER with TR-31 key usage K0.	0246	ED	6.3
TR-34 Key Distribution - Permit AES IMPORTER to K1	CSNDT34D	Permits the export of a AES IMPORTER with TR-31 key usage K1.	0247	ED	6.3
TR-34 Key Receive	CSNDT34R		01FC	ED	6.3
TR-34 Key Receive – Allow 2PASSRCV	CSNDT34R	Requested action *rule_array* keyword 2PASSRCV is allowed.	01FD	ED	6.3
TR-34 Key Receive – Allow 1PASSRCV	CSNDT34R	Requested action *rule_array* keyword 1PASSRCV is allowed.	01FE	ED	6.3
TR-34 Key Receive – Allow wrapping override keywords	CSNDT34R	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	01DF	ED	6.3

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
TR-34 Key Receive – Permit DES EXPORTER	CSNDT34R	Permits the import of a DES EXPORTER.	0248	ED	6.3
R-34 Key Receive – Permit DES IMPORTER	CSNDT34R	Permits the import of a DES IMPORTER.	0249	ED	6.3
TR-34 Key Receive – Permit AES EXPORTER	CSNDT34R	Permits the import of a AES EXPORTER.	024A	ED	6.3
TR-34 Key Receive – Permit AES IMPORTER	CSNDT34R	Permits the import of a AES IMPORTER.	024B	ED	6.3
TR-34 Key Receive – Permit AES EXPORTER with EXPTT31D	CSNDT34R	Permits the import of a AES EXPORTER with key usage EXPTT31D.	024C	ED	6.3
TR-34 Key Receive – Permit AES IMPORTER with IMPTT31D	CSNDT34R	Permits the import of a AES IMPORTER with key usage IMPTT31D.	024D	ED	6.3
Transaction Validation – Generate	CSNBTRV	The combination of the Operation *rule_array* keyword being GENERATE and the Security code keyword being CSC-345 is allowed.	0291	ED	
Transaction Validation – Verify CSC-3	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-3 is allowed.	0292	ED	
Transaction Validation – Verify CSC-4	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-4 is allowed.	0293	ED	
Transaction Validation – Verify CSC-5	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-5 is allowed.	0294	ED	
Trusted Block Create - Create Block in inactive form	CSNDTBC	Operational *rule_array* keyword INACTIVE is allowed.	030F	ED	
Trusted Block Create - Activate an inactive block	CSNDTBC	Operational *rule_array* keyword ACTIVATE is allowed.	0310	ED	
Trusted Block Create – Disallow triple-length MAC key	CSNDTBC	The MAC key in the trusted block may not be a triple-length key.	032E	DD, SC	4.3
Unique Key Derive	CSNBUKD		01C8	ED	4.3
Unique Key Derive – Allow PIN-DATA processing	CSNBUKD	Output Key Selection *rule_array* keyword PIN-DATA is allowed.	01C9	DD	4.3

Name	Callable services	Parameters affected when enabled	Offset (Hex)	Usage	Release
Unique Key Derive - K3IPEK	CSNBUKD	Output Key Selection *rule_array* keyword K3IPEK is allowed.	0335	DD	4.3
Unique Key Derive – Override default wrapping	CSNBUKD	The key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	01CA	ED	4.3
Visa CVV Generate	CSNBCSG		00DF	ED	
Visa CVV Verify	CSNBCSV		00E0	ED	

There are relationships between certain access controls. A controlling access control is required to be enabled before subordinate access controls can enabled. The TKE workstation will enable the controlling access control when a subordinate access control is enabled.

- To use **Data Key Export - Unrestricted**, the **Data Key Export** access control must be enabled.
- To use **Data Key Import - Unrestricted**, the **Data Key Import** access control must be enabled.
- **Diversified Key Generate - single length or same halves** requires either **Diversified Key Generate - TDES-ENC** or **Diversified Key Generate – TDES-DEC** be enabled.
- To use **Key Export - Unrestricted**, the **Key Export** access control must be enabled.
- To use **Key Import - Unrestricted**, the **Key Import** access control must be enabled.
- To use **Key Part Import – Unrestricted**, the **Key Part Import - First key part** and **Key Part Import - Middle and final** access controls must be enabled.
- To use **TR31 Export - Permit PINGEN/PINVER to V0/V1/V2:N**, the **TR31 Export - Permit version A TR-31 key blocks** access control must be enabled.
- To use **Unique Key Derive - Allow PIN-DATA** processing or **Unique Key Derive - Override default wrapping access control points**, **Unique Key Derive** access control must be enabled.
- To use **SET Block Decompose - PIN ext IPINENC or PIN ex OPINENC**, the **SET Block Decompose** access control must be enabled.
- To use **PKA Key Generate - Permit Regeneration Data**, the **PKA Key Generate** access control must be enabled.
- To use **PKA Key Generate - Permit Regeneration Data Retain**, the **PKA Key Generate** and **PKA Key Generate – Clone** access controls must be enabled.
- To use **PKA Key Generate - Clear** or **PKA Key Generate - Clone,** the **PKA Key Generate** access control must be enabled.
- To use **PKA Key Generate - Allow weak DES wrap of RSA** access control, the **Prohibit weak wrap – Transport keys** access control must be enabled.
- To use any of the following access control points, the **ECC Diffie-Hellman** access control must be enabled:
    - **ECC Diffie-Hellman - Allow PASSTHRU**
    - **ECC Diffie-Hellman - Allow DERIV02**
    - **ECC Diffie-Hellman - Allow key wrap override**
    - **ECC Diffie-Hellman - Allow Prime Curve 192**
    - **ECC Diffie-Hellman - Allow Prime Curve 224**

- **ECC Diffie-Hellman - Allow Prime Curve 256**
- **ECC Diffie-Hellman - Allow Prime Curve 384**
- **ECC Diffie-Hellman - Allow Prime Curve 521**
- **ECC Diffie-Hellman - Allow BP Curve 160**
- **ECC Diffie-Hellman - Allow BP Curve 192**
- **ECC Diffie-Hellman - Allow BP Curve 224**
- **ECC Diffie-Hellman - Allow BP Curve 256**
- **ECC Diffie-Hellman - Allow BP Curve 320**
- **ECC Diffie-Hellman - Allow BP Curve 384**
- **ECC Diffie-Hellman - Allow BP Curve 512**
- **ECC Diffie-Hellman - Prohibit weak key generate**

Table 2. Access controls – callable services ordered by offset

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
000E	Encipher - DES	CSNBENC		ED	
		CSNBESC	Action *rule_array* keywords SMCON and SMCONINT are allowed.		
		CSNBEVF	The action *rule_array* keyword is DACVER and DYNVER are allowed.		
000F	Decipher - DES	CSNBDEC		ED	
		CSNBEVF	Action *rule_array* keyword DECCNT is allowed.		
0010	MAC Generate	CSNBEAC	Action *rule_array* keyword GENARPC and VERGEN are allowed.	ED	
		CSNBESC	Action *rule_array* keywords SMINT, SMCONINT, and SMCIPIN are allowed.		
		CSNBMGN			
0011	MAC Verify	CSNBEAC	Action *rule_array* keywords VERARQC and VERGEN is allowed.	ED	
		CSNBMVR			
0012	Key Import	CSNBKIM		ED	
		CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.		
0013	Key Export	CSNBKEX		ED	
		CSNBDCM	Key encryption *rule_array* keyword XPORT is allowed.		
		CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.		
001B	Key Part Import - First key part	CSNBKPI	Key part *rule_array* keyword FIRST is allowed.	ED	
001C	Key Part Import - Middle and final	CSNBKPI	Key part *rule_array* keywords MIDDLE and FINAL are allowed.	ED	
001D	Key Test and Key Test2	CSNBKYT CSNBKYTX CSNBKYT2		AE	
001F	Key Translate	CSNBKTR		ED	
0021	Key Test2 – AES, ENC-ZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword AES and Verification pattern calculation algorithm *rule_array* keyword ENC-ZERO is allowed.	AE	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0022	Key Test2 – AES, CMACZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword AES and the *Verification pattern calculation algorithm rule_array* keyword CMACZERO is allowed.	ED	5.2
0023	Key Test2 – DES, CMACZERO	CSNBKYT2	The combination of token algorithm *rule_array* keyword DES and the *Verification pattern calculation algorithm rule_array* keyword CMACZERO is allowed.	ED	5.2
0024	DK Random PIN Generate2	CSNBDRG2		DD	5.5
0025	DK PRW Card Number Update2	CSNBDCU2		DD	5.5
003A	PKA Key Import – Disallow clear key import	CSNDPKI	The key token supplied in the *source_key_token* parameter can not contain a clear key.	DD	5.2
0040	Diversified Key Generate - CLR8–ENC	CSNBDKG	Processing method *rule_array* keyword CLR8-ENC is allowed.	ED	
0041	Diversified Key Generate - TDES-ENC	CSNBDKG	Processing method *rule_array* keyword TDES-ENC is allowed.	ED	
		CSNBDSK	Key mode *rule_array* keyword MC and VISA are allowed.		
		CSNBEAC	Key mode *rule_array* keyword MC and VISA are allowed.		
		CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed.		
		CSNBEVF	Action *rule_array* keywords DECCNT are DYNVER are allowed.		
0042	Diversified Key Generate - TDES-DEC	CSNBDKG	Processing method *rule_array* keyword TDES-DEC is allowed.	ED	
0043	Diversified Key Generate - SESS-XOR	CSNBDKG	Processing method *rule_array* keyword SESS-XOR is allowed.	ED	
		CSNBEAC	Key mode *rule_array* keyword VISA is allowed.		
		CSNBESC	Action *rule_array* keywords SMINT, SMCON, and SMCONPIN are allowed.		
		CSNBEVF	Action *rule_array* keywords DECCNT and DYNVER are allowed.		
0044	Diversified Key Generate – single length or same halves	CSNBDKG	When the processing method *rule_array* keyword is TDES-ENC or TDES-DEC, the *generated_key_identifier* parameter may specify a single-length key or a double-length key with equal key-halves.	ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0045	Diversified Key Generate - TDES-XOR	CSNBDKG	Processing method *rule_array* keyword TDES-XOR is allowed.	ED	
		CSNBDSK	Key mode *rule_array* keyword VISA is allowed.		
		CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed.		
0046	Diversified Key Generate - TDESEMV2/TDESEMV4	CSNBDKG	Processing method *rule_array* keywords TDESEMV2 and TDESEMV4 are allowed.	ED	
		CSNBDSK	Key mode *rule_array* keyword EMV is allowed.		
		CSNBEAC	Key mode *rule_array* keyword EMV is allowed.		
		CSNBESC	Action *rule_array* keywords SMINT, SMCON, SMCONPIN, SMCONINT, and SMCIPIN are allowed.		
		CSNBEVF	Action *rule_array* keyword DECCNT is allowed.		
0070	Public Infrastructure Certificate	CSNDPIC		ED	6.0
007C	Public Infrastructure Certificate - PK10SNRQ	CSNDPIC		ED	6.0
0080	Diversify Directed Key	CSNBDDK		ED	5.4
0081	Diversify Directed Key – Allow KDFFM DERIVE	CSNBDDK	Function rule_array keyword DERIVE is allowed.	DD	5.4
0082	Diversify Directed Key – Allow KDFFM GENERATE	CSNBDDK	Function rule_array keyword GENERATE is allowed.	DD	5.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
008C	Key Generate – Key set	CSNBKGN	These combinations are allowed: • The value of the *key_form* parameter is EX and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the EX column. • The value of the *key_form* parameter is IM and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the IM column. • The value in the *key_form* parameter is OPEX, EXEX, OPIM, OPOP, IMIM, or IMEX and the key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key Generate Valid Key Types and Key Forms for a Key Pair* table in the column matching the key form.	ED	
008E	Key Generate – OP	CSNBKGN	This combination is allowed: the value of the *key_form* parameter OP and the key type specified in the *key_type_1* parameter is one of the key types listed in the *Key Generate Valid Key Types and Key Forms for a Single Key* table in the OP column.	ED	
		CSNBGIM	Key encryption *rule_array* keyword XPORT is allowed.		
		CSNBRNG			
00A0	Clear PIN Generate - 3624	CSNBPGN	The Process rule *rule_array* keywords IBM-PIN and IBM-PINO are allowed.	ED	
00A1	Clear PIN Generate - GBP	CSNBPGN	The Process rule *rule_array* keyword GBP-PIN is allowed.	ED	
00A2	Clear PIN Generate - VISA PVV	CSNBPGN	The Process rule *rule_array* keyword VISA-PVV is allowed.	ED	
00A3	Clear PIN Generate - Interbank	CSNBPGN	The Process rule *rule_array* keyword INBK-PIN is allowed.	ED	
00A4	Clear Pin Generate Alternate – 3624 Offset	CSNBCPA	The PIN calculation method *rule_array* keyword IBM-PINO is allowed.	ED	
00AB	Encrypted PIN Verify - 3624	CSNBPVR	Algorithm value rule *rule_array* keywords IBM-PIN and IBM-PINO are allowed.	ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
00AC	Encrypted PIN Verify - GPB	CSNBPVR	Algorithm value rule *rule_array* keyword GBP-PIN is allowed.	ED	
00AD	Encrypted PIN Verify - VISA PVV	CSNBPVR	Algorithm value rule *rule_array* keyword VISA-PVV is allowed.	ED	
00AE	Encrypted PIN Verify - Interbank	CSNBPVR	Algorithm value rule *rule_array* keyword INBK-PIN is allowed.	ED	
00AF	Clear PIN Encrypt	CSNBCPE		ED	
00B0	Encrypted PIN Generate - 3624	CSNBEPG	Process rule *rule_array* keyword IBM-PIN is allowed.	ED	
00B1	Encrypted PIN Generate - GBP	CSNBEPG	Process rule *rule_array* keyword GBP-PIN is allowed.	ED	
00B2	Encrypted PIN Generate - Interbank	CSNBEPG	Process rule *rule_array* keyword INBK-PIN is allowed.	ED	
00B3	Encrypted PIN Translate - Translate	CSNBPTR CSNBPTRE	Process rule *rule_array* keyword TRANSLATE is allowed.	ED	
00B7	Encrypted PIN Translate - Reformat	CSNBPTR CSNBPTRE CSNBPTR2	Process rule *rule_array* keyword REFORMAT is allowed.	ED	
00BB	Clear PIN Generate Alternate - VISA PVV	CSNBCPA	The PIN calculation method *rule_array* keyword VISA-PVV is allowed.	ED	
00BC	PIN Change/Unblock – change EMV PIN with OPINENC	CSNBESC	Action *rule_array* keyword VISAPIN is allowed.	ED	
		CSNBPCU	The key type of the PIN block encrypting key may be OPINENC.		
00BD	PIN Change/Unblock – change EMV PIN with IPINENC	CSNBESC	Action *rule_array* keyword VISAPIN is allowed.	ED	
		CSNBPCU	The key type of the PIN block encrypting key may be IPINENC.		
00C3	Clear Key Import/Multiple Clear Key Import - DES	CSNBCKI		ED	
		CSNBCKM	The Algorithm *rule_array* keyword DES is allowed.		
00C4	Secure Key Import – DES, OP	CSNBSKI	The value of the *key_form* parameter may be OP.	ED	
		CSNBSKM	The combination of the Algorithm *rule_array* keyword being DES and the value of the *key_form* parameter being OP is allowed.		
00CD	Prohibit Export	CSNBPEX		ED	
00D6	Control Vector Translate	CSNBCVT		ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
00D7	Key Generate – Key set extended	CSNBKGN	This combination is allowed: the value of the *key_form* parameter is OPEX, OPIM, OPOP, IMIM, or IMEX and the key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key Generate Valid Key Types and Key Forms for a Key Pair* table in the column matching the key form.	ED	
00DA	Cryptographic Variable Encipher	CSNBCVE		ED	
00DB	Key Generate - SINGLE-R	CSNBKGN	A value of SINGLE-R is allowed in the *key_length* parameter.	ED	
		CSNBRKX	A single-length source key will be replicated when the following conditions are met: 1. The key token returned using the *sym_encrypted_key_identifier* parameter is a fixed-length DES key token, as defined in the rule section identified by the *rule_id* parameter 2. The rule section identified by the *rule_id* parameter has a common export key parameters subsection defined, and the control vector in the subsection is 16 bytes in length with key-form bits of B'010' for the left half and B'001' for the right half. 3. The token identified by the *source_key_identifier* parameter is single length, either a fixed-length DES token or an RKX token.		
00DC	Secure Key Import – DES, IM	CSNBSKI	The value of the *key_form* parameter may be IM.	ED	
		CSNBSKM	The combination of the Algorithm *rule_array* keyword being DES and the value of the *key_form* parameter being IM is allowed.		
00DF	Visa CVV Generate	CSNBCSG		ED	
00E0	Visa CVV Verify	CSNBCSV		ED	
00E4	HMAC Generate – SHA-1	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-1 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-1 is allowed.		
00E5	HMAC Generate – SHA-224	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-224 is allowed.	ED	4.1

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-224 is allowed.		
00E6	HMAC Generate – SHA-256	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-256 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-256 is allowed.		
00E7	HMAC Generate – SHA-384	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-384 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-384 is allowed.		
00E8	HMAC Generate – SHA-512	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-512 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-512 is allowed.		
00E9	Restrict Key Attribute – Export Control	CSNBRKA	Token type *rule_array* keywords AES and HMAC are allowed.	ED	4.1
00EA	Key Generate2 – OP	CSNBKGN2	Key form *rule_array* keywords OP, IM, and EX are allowed.	ED	4.1
00EB	Key Generate2 – Key set	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX, EXEX, OPIM, OPOP, IMIM, or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key Generate2 Valid key type and key forms for two AES or HMAC keys* table or the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	ED	4.1
00EC	Key Generate2 – Key set extended	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key Generate2 Valid key type and key forms for two AES or HMAC keys* table in the column matching the key form.	ED	4.3
00F2	Secure Key Import2 - OP	CSNBSKI2	Key form *rule_array* keyword OP is allowed.	ED	4.1
00F3	Secure Key Import2 - IM	CSNBSKI2	Key form *rule_array* keyword IM is allowed.	ED	4.1

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
00F4	Symmetric Key Import2 – HMAC, PKOAEP2	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being HMAC and recovery method *rule_array* keyword being PKOAEP2 is allowed.	ED	4.1
00F5	Symmetric Key Export – HMAC, PKOAEP2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being HMAC and and Key formatting method *rule_array* keyword being PKOAEP2 is allowed.	ED	4.1
00F7	HMAC Verify – SHA-1	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-1 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-1 is allowed.		
00F8	HMAC Verify – SHA-224	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-224 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-224 is allowed.		
00F9	HMAC Verify – SHA-256	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-256 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-256 is allowed.		
00FA	HMAC Verify – SHA-384	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-384 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-384 is allowed.		
00FB	HMAC Verify – SHA-512	CSNBHMG CSNBHMG1	Hash method *rule_array* keyword SHA-512 is allowed.	ED	4.1
		CSNBMGN2 CSNBMGN3	When the token algorithm keyword is HMAC, the hash method *rule_array* keyword SHA-512 is allowed.		
00FC	Symmetric Key Export – AES, PKOAEP2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being PKOAEP2 is allowed.	ED	4.1

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
00FD	Symmetric Key Import2 – AES, PKOAEP2	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being PKOAEP2 is allowed.	ED	4.2
00FE	PKA Key Translate – Translate internal key token	CSNDPKT	Output format *rule_array* keyword INTDWAKW is allowed.	ED	4.3
00FF	PKA Key Translate – Translate external key token	CSNDPKT	Output format *rule_array* keyword EXTDWAKW is allowed.	ED	4.3
0100	Digital Signature Generate	CSNDDSG		ED	
0101	Digital Signature Verify	CSNDDSV		ED	
0102	PKA Key Token Change RTCMK	CSNDKTC		ED	
0103	PKA Key Generate	CSNDPKG		ED	
0104	PKA Key Import	CSNDPKI		ED	
0105	Symmetric Key Export – DES, PKCS-1.2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and and Key formatting method *rule_array* keyword being PKCS-1.2 is allowed.	ED	
		CSNDSXD	The combination of the *rule_array* keywords being DES and PKCS-EXT is allowed		
0106	Symmetric Key Import – DES, PKCS-1.2	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and and Recovery method *rule_array* keyword being PKCS-1.2 is allowed.	ED	
0109	Data Key Import	CSNBDKM		ED	
010A	Data Key Export	CSNBDKX		ED	
010B	SET Block Compose	CSNDSBC		ED	
010C	SET Block Decompose	CSNDSBD		ED	
010D	Symmetric Key Generate – DES, PKA92	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being PKA92 is allowed.	ED	
011E	PKA Encrypt	CSNDPKE		ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
011F	PKA Decrypt	CSNDPKD		ED	
0121	SET Block Decompose - PIN ext IPINENC	CSNDSBD	The combination of the Formatting information *rule_array* keyword being PINBLOCK and the key type of the PIN block encrypting key being IPINENC is allowed.	ED	
0122	SET Block Decompose - PIN ext OPINENC	CSNDSBD	The combination of the Formatting information *rule_array* keyword being PINBLOCK and the key type of the PIN block encrypting key being OPINENC is allowed.	ED	
0129	Multiple Clear Key Import/Multiple Secure Key Import - AES	CSNBCKM	Algorithm *rule_array* keyword AES is allowed.	ED	3.30
		CSNBSKM	The combination of algorithm *rule_array* keyword AES and the value of OP specified in the *key_form* parameter is allowed.		
012A	Symmetric Algorithm Encipher - Secure AES keys	CSNBSAE CSNBSAE1		ED	3.30
012B	Symmetric Algorithm Decipher - Secure AES keys	CSNBSAD CSNBSAD1		ED	3.30
012C	Symmetric Key Generate - AES, PKCSOAEP, PKCS-1.2	CSNDSYG	The combination of the Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	ED	3.30
012D	Symmetric Key Generate - AES, ZERO-PAD	CSNDSYG	The combination of the Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	ED	3.30
012E	Symmetric Key Import – AES, PKCSOAEP, PKCS-1.2	CSNDSYI	The combination of the Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	ED	3.30
012F	Symmetric Key Import – AES, ZERO-PAD	CSNDSYI	The combination of the Algorithm *rule_array* keyword being AES and Recovery method *rule_array* keyword being ZEROPAD is allowed.	ED	3.30
0130	Symmetric Key Export – AES, PKCSOAEP, PKCS-1.2	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and the Key formatting method *rule_array* keyword being PKCSOAEP or PKCS-1.2 is allowed.	ED	3.30
		CSNDSXD	The combination of the *rule_array* keywords being AES and PKCS-EXT is allowed		

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0131	Symmetric Key Export – AES, ZERO-PAD	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	ED	3.30
013D	Diversified Key Generate - Allow wrapping override keywords	CSNBDKG	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	ED	4.1
013E	Symmetric Key Generate - Allow wrapping override keywords	CSNDSYG	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.1
013F	Remote Key Export - include RKX in default wrap config	CSNDRKX	Key wrapping method *rule_array* keywords USECONFG, WRAP-ECB, WRAP-ENH, and ENH-ONLY are allowed.	DD	4.4
0140	Key Part Import - Allow wrapping override keywords	CSNBKPI	Key wrapping method *rule_array* keywords WRAP-ECB or WRAP-ENH are allowed.	ED	4.1
0141	Multiple Clear Key Import - Allow wrapping override keywords	CSNBCKM	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.1
0142	Multiple Secure Key Import - Allow wrapping override keywords	CSNBSKM	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.1
0144	Symmetric Key Import - Allow wrapping override keywords	CSNDSYI	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.1
0149	Key Translate2 – Translate	CSNBKTR2		ED	4.2
014A	Key Translate2 - Allow wrapping override keywords	CSNBKTR2	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.1
014B	Key Translate2 - Allow use of REFORMAT	CSNBKTR2	Encipherment *rule_array* keyword REFORMAT is allowed.	ED	4.1
014D	T31X - Permit version A TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARXOR-A is allowed.	ED	4.2
014E	T31X - Permit version B TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARDRV-B is allowed.	ED	4.2
014F	T31X - Permit version C TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARXOR-C is allowed.	ED	4.2
0150	T31I - Permit version A TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID A.	ED	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0151	T31I - Permit version B TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID B.	ED	4.2
0152	T31I - Permit version C TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID C.	ED	4.2
0153	T31I - Permit override of default wrapping method	CSNBT31I	The key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.2
0154	Restrict Key Attribute – Permit setting the TR-31 export bit	CSNBRKA	Token type *rule_array* keyword DES is allowed and Export control keyword NOT31XPT is allowed.	ED	4.2
0155	CVV Key Combine	CSNBCKC		ED	4.2
0156	CVV Key Combine – Allow wrapping override keywords	CSNBCKC	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	ED	4.2
0157	CVV Key Combine - Permit mixed key types	CSNBCKC	The key supplied by *key_a_identifier* parameter and the key supplied by *key_b_identifier* parameter need not be the same key type.	ED	4.2
0158	T31X - Permit any CCA DES key if INCL-CV is specified	CSNBT31X	The key identifier supplied in the source_key_identifier parameter may be any key type when the Control vector transport control *rule_array* keyword is INCL-CV.	ED	4.2
015A	T31I - Permit C0:G/C/V to DES MAC/MACVER:CVVKEY-A	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	DD	4.2
015B	T31I - C0:G/C/V to DES MAC/MACVER:AMEX-CSC	CSNBT31I		DD	4.2
015C	T31I - K0:E to DES EXPORTER/OKEYXLAT	CSNBT31I		DD	4.2
015D	T31I - K0:D to DES IMPORTER/IKEYXLAT	CSNBT31I		DD	4.2
015E	T31I - K0:B to DES EXPORTER/OKEYXLAT	CSNBT31I		DD	4.2
015F	T31I - K0:B to DES IMPORTER/IKEYXLAT	CSNBT31I		DD	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0160	T31I - Permit K1/K4:E to DES EXPORTER/OKEYXLAT	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	DD	4.2
0161	T31I - Permit K1/K4:D to DES IMPORTER/IKEYXLAT	CSNBT31I		DD	4.2
0162	T31I - Permit K1/K4:B to DES EXPORTER/OKEYXLAT	CSNBT31I		DD	4.2
0163	T31I - Permit K1/K4:B to DES IMPORTER/IKEYXLAT	CSNBT31I		DD	4.2
0164	T31I - Permit M0/M1/M3:G/C/V to DES MAC/MACVER:ANY-MAC	CSNBT31I		ED	4.2
0165	T31I - Permit P0:E to DES OPINENC	CSNBT31I		ED	4.2
0166	T31I - Permit P0:D to DES IPINENC	CSNBT31I		ED	4.2
0167	T31I - Permit V0:N/G/C to DES PINGEN:NO-SPEC NOOFFSET	CSNBT31I		DD	4.2
0168	T31I - Permit V0:N/V to DES PINVER:NO-SPEC NOOFFSET	CSNBT31I		DD	4.2
0169	T31I - Permit V1:N/G/C to DES PINGEN:IBM-PIN/IBM-PINO NOOFFSET	CSNBT31I		ED	4.2
016A	T31I - Permit V1:N/V to DES PINVER:IBM-PIN/IBM-PINO NOOFFSET	CSNBT31I		ED	4.2
016B	T31I - Permit V2:N/G/C to DES PINGEN:VISA-PVV	CSNBT31I		ED	4.2
016C	T31I - Permit V2:N/V to DES PINVER:VISA-PVV	CSNBT31I		ED	4.2
016D	T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		DD	4.2
016E	T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMV	CSNBT31I		DD	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
016F	T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMAC	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	DD	4.2
0170	T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMV	CSNBT31I		DD	4.2
0171	T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DMPIN	CSNBT31I		DD	4.2
0172	T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		DD	4.2
0173	T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DMPIN	CSNBT31I		DD	4.2
0174	T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DDATA	CSNBT31I		DD	4.2
0175	T31I - Permit E2:N/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		DD	4.2
0176	T31I - Permit E2:N/X to DES DKYGENKY:DKYL1+DMAC	CSNBT31I		DD	4.2
0177	T31I - Permit E3:N/E/D/B/G/X to DES ENCIPHER	CSNBT31I		DD	4.2
0178	T31I - Permit E4:N/B/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		DD	4.2
0179	T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DMAC	CSNBT31I		DD	4.2
017A	T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DDATA	CSNBT31I		DD	4.2
017B	T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DEXP	CSNBT31I		DD	4.2
017C	T31I - Permit V0/V1/V2:N to DES PINGEN/PINVER	CSNBT31I		DD	4.2
0180	T31X - Permit DES KEYGENKY: DUKPT to B0:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the	ED	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0181	T31X - Permit DES MAC/MACVER:AMEX-CSC to C0:G/C/V	CSNBT31X	attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	DD	4.2
0182	T31X - Permit DES MAC/MACVER: CVV-KEYA to C0:G/C/V	CSNBT31X		DD	4.2
0183	T31X - Permit DES MAC/MACVER: ANY-MAC to C0:G/C/V	CSNBT31X		ED	4.2
0184	T31X - Permit DES DATA/DATAM/DATAMV to C0:G/C/V	CSNBT31X		ED	4.2
0185	T31X - Permit DES ENCIPHER/DECIPHER/CIPHER to D0:E/D/B	CSNBT31X		ED	4.2
0186	T31X - Permit DES DATA to D0:E/D/B	CSNBT31X		ED	4.2
0187	T31X - Permit DES EXPORTER/OKEYXLAT to K0:E	CSNBT31X		DD	4.2
0188	T31X - Permit DES IMPORTER/IKEYXLAT to K0:D	CSNBT31X		DD	4.2
0189	T31X - Permit DES EXPORTER/OKEYXLAT to K1/K4:E	CSNBT31X		DD	4.2
018A	T31X - Permit DES IMPORTER/IKEYXLAT to K1/K4:D	CSNBT31X		DD	4.2
018B	T31X - Permit DES MAC/DATA/DATAM to M0:G/C	CSNBT31X		DD	4.2
018C	T31X - Permit DES MACVER/DATA/DATAMV to M0:V	CSNBT31X		ED	4.2
018D	T31X - Permit DES MAC/DATA/DATAM to M1:G/C	CSNBT31X		ED	4.2
018E	T31X - Permit DES MACVER/DATA/DATAMV to M1:V	CSNBT31X		ED	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
018F	T31X - Permit DES MAC/DATA/DATAM to M3:G/C	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	ED	4.2
0190	T31X - Permit DES MACVER/DATA/DATAMV to M3:V	CSNBT31X		ED	4.2
0191	T31X - Permit DES OPINENC to P0:E	CSNBT31X		ED	4.2
0192	T31X - Permit DES IPINENC to P0:D	CSNBT31X		ED	4.2
0193	T31X - Permit DES PINVER: NO-SPEC to V0:N/V	CSNBT31X		DD	4.2
0194	T31X - Permit DES PINGEN: NO-SPEC to V0:N/C	CSNBT31X		DD	4.2
0195	T31X - Permit DES PINVER: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V	CSNBT31X		ED	4.2
0196	T31X - Permit DES PINGEN: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V	CSNBT31X		ED	4.2
0197	T31X - Permit DES PINVER: NO-SPEC/VISA-PVV to V2:N/V	CSNBT31X		ED	4.2
0198	T31X - Permit DES PINGEN: NO-SPEC/VISA-PVV to V2:N/C	CSNBT31X		ED	4.2
0199	T31X - Permit DES DKYGENKY: DKYL0+DMAC to E0:N/X	CSNBT31X		DD	4.2
019A	T31X - Permit DES DKYGENKY: DKYL0+DMV to E0:N/X	CSNBT31X		DD	4.2
019B	T31X - Permit DES DKYGENKY: DKYL0+DALL to E0:N/X	CSNBT31X		DD	4.2
019C	T31X - Permit DES DKYGENKY: DKYL1+DMAC to E0:N/X	CSNBT31X		DD	4.2
019D	T31X - Permit DES DKYGENKY: DKYL1+DMV to E0:N/X	CSNBT31X		DD	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
019E	T31X - Permit DES DKYGENKY: DKYL1+DALL to E0:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	DD	4.2
019F	T31X - Permit DES DKYGENKY: DKYL0+DDATA to E1:N/X	CSNBT31X		DD	4.2
01A0	T31X - Permit DES DKYGENKY: DKYL0+DMPIN to E1:N/X	CSNBT31X		DD	4.2
01A1	T31X - Permit DES DKYGENKY: DKYL0+DALL to E1:N/X	CSNBT31X		DD	4.2
01A2	T31X - Permit DES DKYGENKY: DKYL1+DDATA to E1:N/X	CSNBT31X		DD	4.2
01A3	T31X - Permit DES DKYGENKY: DKYL1+DMPIN to E1:N/X	CSNBT31X		DD	4.2
01A4	T31X - Permit DES DKYGENKY: DKYL1+DALL to E1:N/X	CSNBT31X		DD	4.2
01A5	T31X - Permit DES DKYGENKY: DKYL0+DMAC to E2:N/X	CSNBT31X		DD	4.2
01A6	T31X - Permit DES DKYGENKY: DKYL0+DALL to E2:N/X	CSNBT31X		DD	4.2
01A7	T31X - Permit DES DKYGENKY: DKYL1+DMAC to E2:N/X	CSNBT31X		DD	4.2
01A8	T31X - Permit DES DKYGENKY: DKYL1+DALL to E2:N/X	CSNBT31X		DD	4.2
01A9	T31X - Permit DES DATA/DATAM/CIPHER/MAC/ENCIPHER to E3:N/G/E/X	CSNBT31X		DD	4.2
01AA	T31X - Permit DES DKYGENKY: DKYL0+DDATA to E4:N/X	CSNBT31X		ED	4.2
01AB	T31X - Permit DES DKYGENKY: DKYL0+DALL to E4:N/X	CSNBT31X		ED	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
01AC	T31X - Permit DES DKYGENKY: DKYL0+DEXP to E5:N/X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	DD	4.2
01AD	T31X - Permit DES DKYGENKY: DKYL0+DMAC to E5:N/X	CSNBT31X		DD	4.2
01AE	T31X - Permit DES DKYGENKY: DKYL0+DDATA to E5:N/X	CSNBT31X		DD	4.2
01AF	T31X - Permit DES DKYGENKY:DKYL0+DALL to E5:N/X	CSNBT31X		ED	4.2
01B0	T31X - Permit DES PINGEN to V0:N and DES PINVER to V1/V2:N	CSNBT31X		DD	4.2
01C0	Cipher Text Translate2	CSNBCTT2 CSNBCTT3		ED	4.3
01C1	Cipher Text Translate2 – Allow translate from AES to TDES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be a DES key when the key supplied in the *key_identifier_in* parameter is an AES key.	ED	4.3
01C2	Cipher Text Translate2 – Allow translate to weaker AES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be weaker AES key than the AES key supplied in the *key_identifier_in* parameter.	ED	4.3
01C3	Cipher Text Translate2 – Allow translate to weaker DES	CSNBCTT2 CSNBCTT3	The key supplied in the *key_identifier_out* parameter is allowed to be weaker DES key than the DES key supplied in the *key_identifier_in* parameter.	ED	4.3
01C4	Cipher Text Translate2 – Allow only cipher text translate types	CSNBCTT2 CSNBCTT3	The *key_identifier_in* and *key_identifier_out* parameters must be a key with key type CIPHERXI, CIPHERXL, or CIPHERXO for DES and key type CIPHER with the C-XLATE key usage bit on for AES.	DD	4.3
01C8	Unique Key Derive	CSNBUKD		ED	4.3
01C9	Unique Key Derive – Allow PIN-DATA processing	CSNBUKD	Output Key Selection *rule_array* keyword PIN-DATA is allowed	DD	4.3
01CA	Unique Key Derive – Override default wrapping	CSNBUKD	The key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	4.3

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
01CB	Key Test - Warn when keyword inconsistent with key length	CSNBKYT CSNBKYTX	The key rule *rule_array* keyword specified does not match the DES encrypted key token in the *key_identifier* parameter.	DD	4.4
01CD	Symmetric Algorithm Encipher - GCM/Counter mode AES	CSNBSAE CSNBSAE1	Processing rule *rule_array* keyword GCM is allowed.	ED	5.2
01CE	Symmetric Algorithm Decipher - GCM/Counter mode AES	CSNBSAD CSNBSAD1	Processing rule *rule_array* keyword GCM is allowed.	ED	5.2
01D0	T31X - Permit AES CIPHER to D0:E/D/B	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Control Points (ACPs)* table in the CSNBT31X service description.	ED	4.5
01D1	T31X - Permit AES MAC: CMAC to M6:G/C/V	CSNBT31X		ED	4.5
01D2	T31X - Permit AES PINPROT to P0:E/D	CSNBT31X		ED	4.5
01D3	T31X - Permit AES EXPORTER to K0:E	CSNBT31X		ED	4.5
01D4	T31X - Permit AES EXPORTER to K1:E	CSNBT31X		ED	4.5
01D5	T31X - Permit AES EXPORTER to K4:E	CSNBT31X		ED	4.5
01D6	T31X - Permit AES IMPORTER to K0:D	CSNBT31X		ED	4.5
01D7	T31X - Permit AES IMPORTER to K1:D	CSNBT31X		ED	4.5
01D8	T31X - Permit AES IMPORTER to K4:D	CSNBT31X		ED	4.5
01D9	T31X - Permit AES DKYGENKY:D-ALL/DMAC to E0:X	CSNBT31X		ED	4.5
01DA	T31X - Permit AES DKYGENKY:D-ALL/DCIPHER to E1:X	CSNBT31X		ED	4.5
01DB	T31X - Permit AES DKYGENKY:D-ALL/D-MAC to E2:X	CSNBT31X		ED	4.5

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
01DC	T31X - Permit AES CIPHER to E3/E/B,DKYGENKY:D-ALL/DCIP to E3:X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Controls* table in the CSNBT31X service description.	ED	4.5
01DD	T31X - Permit AES DKYGENKY:D-ALL/D-CIPHER to E4:X	CSNBT31X		ED	4.5
01DE	T31X - Permit AES DKYGENKY:D-MAC to E5:X	CSNBT31X		ED	4.5
01DF	TR-34 Key Receive – Allow wrapping override keywords	CSNDT34R	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	ED	6.3
01E0	T31I - Permit D0:E/D/B to AES CIPHER:ENC/DEC/ENC+DEC	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	ED	4.5
01E1	T31I - Permit M6:G/C/V to AES MAC:CMAC+GENONLY/GEN/VER	CSNBT31I		ED	4.5
01E2	T31I - Permit P0:E/D to AES PINPROT:ENC/DEC+CBC+ISO-4	CSNBT31I		ED	4.5
01E3	T31I - Permit K0:E to AES EXPORTER	CSNBT31I		ED	4.5
01E4	T31I - Permit K0:D to AES IMPORTER	CSNBT31I		ED	4.5
01E5	T31I - Permit K1/K4:E to AES EXPORTER:EXPTT31D+VARDRV-D	CSNBT31I		ED	4.5
01E6	T31I - Permit AES K1/K4:D to AES IMPORTER:IMPTT31D+VARDRV-D	CSNBT31I		ED	4.5
01E7	T31I - Permit E0:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	CSNBT31I		ED	4.5
01E8	T31I - Permit E1:X to AES DKYGENKY:DKYL0/L1/L2+D-SECMSG+SMPIN	CSNBT31I		ED	4.5

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
01E9	T31I - Permit E2:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	CSNBT31I	The CCA Output Key Usage Subgroups and Key Derivation Level *rule_array* keywords and the attributes of the key block and optional blocks supplied in the *TR31_key_block* parameter determine which access control is required. All of this information is listed in the *TR-31 to CCA Import required access controls* table in the CSNBT31I service description.	ED	4.5
01EA	T31I - Permit E3:X to AES DKYGENKY:D-CIPHER+ENC+DEC+CBC	CSNBT31I		ED	4.5
01EB	T31I - Permit E3:E/B to AES CIPHER:ENCRYPT/ENC+DEC	CSNBT31I		ED	4.5
01EC	T31I - Permit E4:X to AES DKYGENKY:DKYL0/L1/L2+D-CIPHER+ENC+DEC	CSNBT31I		ED	4.5
01ED	T31I - Permit E5:X to AES DKYGENKY:DKYL0/L1/L2/D-MAC+GEN+CMAC	CSNBT31I		ED	4.5
01EE	PKA Key Translate – allow COMP-TAG	CSNDPKT	Conversion service rule_array keyword COMP-TAG is allowed.	ED	6.3
01EF	PKA Key Translate – allow COMP-CHK	CSNDPKT	Conversion service rule_array keyword COMP-CHK is allowed.	ED	6.3
01F0	TR-34 Bind-Begin	CSNDT34B		ED	6.3
01F1	TR-34 Bind-Begin - allow BINDCR	CSNDT34B	Requested action *rule_array* keyword BINDCR is allowed.	ED	6.3
01F2	TR-34 Bind-Begin - allow UNBINDCR	CSNDT34B	Requested action *rule_array* keyword UNBINDCR is allowed.	ED	6.3
01F3	TR-34 Bind-Begin - allow REBINDCR	CSNDT34B	Requested action *rule_array* keyword REBINDCR is allowed.	ED	6.3
01F4	TR-34 Bind-Complete	CSNDT34C		ED	6.3
01F5	TR-34 Bind-Complete - allow BINDKRDC	CSNDT34C	Requested action *rule_array* keyword BINDKRDC is allowed.	ED	6.3
01F6	TR-34 Bind-Complete - allow BINDRV	CSNDT34C	Requested action *rule_array* keyword BINDRV is allowed.	ED	6.3
01F7	TR-34 Bind-Complete - allow UNBINDRV	CSNDT34C	Requested action *rule_array* keyword UNBINDRV is allowed.		

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
01F8	TR-34 Bind-Complete - allow REBINDRV	CSNDT34C	Requested action *rule_array* keyword REBINDRV is allowed.	ED	6.3
01F9	TR-34 Key Distribution	CSNDT34D		ED	6.3
01FA	TR-34 Key Distribution – Allow 2PASSCRE	CSNDT34D	Requested action *rule_array* keyword 2PASSCRE is allowed.	ED	6.3
01FB	TR-34 Key Distribution – Allow 1PASSCRE	CSNDT34D	Requested action *rule_array* keyword 1PASSCRE is allowed.	ED	6.3
01FC	TR-34 Key Receive	CSNDT34R		ED	6.3
01FD	TR-34 Key Receive – Allow 2PASSRCV	CSNDT34R	Requested action *rule_array* keyword 2PASSRCV is allowed.	ED	6.3
01FE	TR-34 Key Receive – Allow 1PASSRCV	CSNDT34R	Requested action *rule_array* keyword 1PASSRCV is allowed.	ED	6.3
01FF	Permit X.509 without PKI root validation	CSNDDSV CSNDPKE CSNDSYX CSNDSYG CSNDT34B CSNDT34C CSNDT34D CSNDT34R	Public Key Infrastructure Usage *rule_array* keyword PKI-NONE is allowed.	ED	6.3
0203	Retained Key Delete	CSNDRKD		ED	
0204	PKA Key Generate – Clone	CSNDPKG	Private Key Encryption *rule_array* keyword CLONE is allowed.	ED	
0205	PKA Key Generate – Clear RSA keys	CSNDPKG	The combination of Private Key Encryption *rule_array* keyword CLEAR and the algorithm of the skeleton key supplied in the *skeleton_key_identifier* parameter being RSA is allowed.	ED	
0206	PKA Encrypt – Disallow PKCS-1.2	CSNDPKE	Recovery Method *rule_array* keyword can not be PKCS-1.2.	DD	4.4.5
0207	PKA Encrypt – Disallow ZEROPAD	CSNDPKE	Recovery Method *rule_array* keyword can not be ZEROPAD.	DD	4.4.5
0208	PKA Encrypt – Disallow MRP	CSNDPKE	Recovery Method *rule_array* keyword can not be MRP.	DD	4.4.5
0209	PKA Encrypt – Disallow PKCSOAEP	CSNDPKE	Recovery Method *rule_array* keyword can not be PKCSOAEP.	DD	4.4.5

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
020A	PKA Decrypt – Disallow PKCS-1.2	CSNDPKD	Recovery Method *rule_array* keyword can not be PKCS-1.2.	DD	4.4.5
020B	PKA Decrypt – Disallow ZEROPAD	CSNDPKD	Recovery Method *rule_array* keyword can not be ZEROPAD.	DD	4.4.5
0208	PKA Decrypt – Disallow PKCSOAEP	CSNDPKD	Recovery Method *rule_array* keyword can not be PKCSOAEP.	DD	4.4.5
0230	Retained Key List	CSNDRKL		ED	
0235	Symmetric Key Import – DES, PKA92 KEK	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword being PKA92 is allowed.	ED	
023C	Symmetric Key Generate - DES, ZERO-PAD	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	ED	
023D	Symmetric Key Import – DES, ZERO-PAD	CSNDSYI	The combination of the Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword being ZEROPAD is allowed.	ED	
023E	Symmetric Key Export – DES, ZERO-PAD	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being ZEROPAD is allowed.	ED	
023F	Symmetric Key Generate - DES, PKCS-1.2	CSNDSYG	The combination of the Algorithm *rule_array* keyword being DES and and Key formatting method *rule_array* keyword being PKCS-1.2 is allowed.	ED	
0242	TR-34 Key Distribution - Permit DES EXPORTER to K0 or K1	CSNDT34D	Permits the export of a DES EXPORTER with TR-31 key usage K0 or K1.	ED	6.3
0243	TR-34 Key Distribution - Permit DES IMPORTER to K0 or K1	CSNDT34D	Permits the export of a DES IMPORTER with TR-31 key usage K0 or K1.	ED	6.3
0244	TR-34 Key Distribution - Permit AES EXPORTER to K0	CSNDT34D	Permits the export of a AES EXPORTER with TR-31 key usage K0.	ED	6.3
0245	TR-34 Key Distribution - Permit AES EXPORTER to K1	CSNDT34D	Permits the export of a AES EXPORTER with TR-31 key usage K1.	ED	6.3
0246	TR-34 Key Distribution - Permit AES IMPORTER to K0	CSNDT34D	Permits the export of a AES IMPORTER with TR-31 key usage K0.	ED	6.3
0247	TR-34 Key Distribution - Permit AES IMPORTER to K1	CSNDT34D	Permits the export of a AES IMPORTER with TR-31 key usage K1.	ED	6.3

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0248	TR-34 Key Receive – Permit DES EXPORTER	CSNDT34R	Permits the import of a DES EXPORTER.	ED	6.3
0249	TR-34 Key Receive – Permit DES IMPORTER	CSNDT34R	Permits the import of a DES IMPORTER.	ED	6.3
024A	TR-34 Key Receive – Permit AES EXPORTER	CSNDT34R	Permits the import of a AES EXPORTER.	ED	6.3
024B	TR-34 Key Receive – Permit AES IMPORTER	CSNDT34R	Permits the import of a AES IMPORTER.	ED	6.3
024C	TR-34 Key Receive – Permit AES EXPORTER with EXPTT31D	CSNDT34R	Permits the import of a AES EXPORTER with key usage EXPTT31D.	ED	6.3
024D	TR-34 Key Receive – Permit AES IMPORTER with IMPTT31D	CSNDT34R	Permits the import of a AES IMPORTER with key usage IMPTT31D.	ED	6.3
0273	Secure Messaging for Keys	CSNBSKY		ED	
0274	Secure Messaging for PINs	CSNBESC	Action *rule_array* keyword SMCIPIN is allowed.	ED	
		CSNBSPN			
0276	Key Export - Unrestricted	CSNBKEX	The key identifier specified in the *exporter_key_identifier* parameter may be an exporter with equal key halves.	ED	
0277	Data Key Export - Unrestricted	CSNBDKX	The key-encrypting key identified by the *exporter_key_identifier* parameter may have equal key halves.	ED	
0278	Key Part Import - ADD-PART	CSNBKPI	Key part *rule_array* keyword ADD-PART is allowed.	ED	
0279	Key Part Import - COMPLETE	CSNBKPI	Key part *rule_array* keyword COMPLETE is allowed.	ED	
027A	Key Part Import - Unrestricted	CSNBKPI	The key identifier specified in the *key_identifier* parameter may be a key with equal key halves.	ED	
027B	Key Import - Unrestricted	CSNBKIM	The key identifier specified in the *importer_key_identifier* parameter may be an importer with equal key halves.	ED	
027C	Data Key Import - Unrestricted	CSNBDKM	The key-encrypting key identified by the *importer_key_identifier* parameter may have equal key halves.	ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
027D	PKA Key Generate - Permit Regeneration Data	CSNDPKG	The use of the *regeneration_data* parameter is allowed with the Private Key Encryption *rule_array* keywords MASTER, XPORT, and CLEAR.	ED	
027E	PKA Key Generate - Permit Regeneration Data Retain	CSNDPKG	The use of the *regeneration_data* parameter is allowed with the Private Key Encryption *rule_array* keyword RETAIN.	ED	
0290	Diversified Key Generate - DKYGENKY - DALL	CSNBDKG CSNBPCU	When the key-generating key is a DKYGENKY key type, the control vector bits (19 – 22) may be B'1111'.	DD, SC	
0291	Transaction Validation – Generate	CSNBTRV	The combination of the Operation *rule_array* keyword being GENERATE and the Security code keyword being CSC-345 is allowed.	ED	
0292	Transaction Validation – Verify CSC-3	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-3 is allowed.	ED	
0293	Transaction Validation – Verify CSC-4	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-4 is allowed.	ED	
0294	Transaction Validation – Verify CSC-5	CSNBTRV	The combination of the Operation *rule_array* keyword being VERIFY and security code keyword being CSC-5 is allowed.	ED	
0297	Key Part Import2 – Load first key part, require 3 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN3PART is allowed.	ED	4.1
0298	Key Part Import2 – Load first key part, require 2 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN2PART is allowed.	ED	4.1
0299	Key Part Import2 - Load first key part, require 1 key parts	CSNBKPI2	The combination of key part *rule_array* keyword FIRST and split knowledge keyword MIN1PART is allowed.	ED	4.1
029A	Key Part Import2 - Add second of 3 or more key parts	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	ED	4.1
029B	Key Part Import2 - Add last required key part	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	ED	4.1
029C	Key Part Import2 - Add optional key part	CSNBKPI2	Key part *rule_array* keyword ADD-PART is allowed.	ED	4.1
029D	Key Part Import2 – Complete key	CSNBKPI2	Key part *rule_array* keyword COMPLETE is allowed.	ED	4.1
02B0	Recover PIN From Offset	CSNBPFO		ED	4.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
02B1	Authentication Parameter Generate	CSNBAPG		ED	4.4
02B2	Authentication Parameter Generate - Clear	CSNBAPG	The AP Protection Method *rule_array* keyword CLEAR is allowed.	DD	4.4
02B3	Symmetric Key Export - AESKWCV	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being DES and Key formatting method *rule_array* keyword being AESKWCV is allowed.	ED	4.4
02B4	Symmetric Key Import2 - AESKWCV	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being DES and Recovery method *rule_array* keyword i being s AESKWCV is allowed.	ED	4.4
02B5	Symmetric Key Export with Data	CSNDSXD		ED	4.4
02B6	Symmetric Key Export with Data - Special	CSNDSXD	The key identifier supplied in the *source_key_identifier* parameter need not be key type DATAC or key type DKYGENKY with subtype DKYL0.	DD	4.4
02B8	Diversified Key Generate - TDES-CBC	CSNBDKG	Processing method *rule_array* keyword TDES-CBC is allowed.	ED	4.4
02B9	Symmetric Key Import2 - Allow wrapping override keywords	CSNDSYI2	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH is allowed.	ED	4.4
02BA	Remote Key Export – Allow wrapping override keywords	CSNDRKX	Key wrapping method *rule_array* keywords WRAP-ECB and WRAP-ENH are allowed.	DD	4.4
02BB	Key Generate2 – DK PIN key set	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPIM, OPOP, or IMIM and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	DD	4.4
02BC	Key Generate2 – DK PIN print key	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	DD	4.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
02BE	Key Generate2 – DK PIN admin1 key MAC	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX, OPIM, OPOP, IMIM, or IMEX and key types specified in the *key_type_1* and *key_type_2* parameters is one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	DD	4.4
02BD	Key Generate2 – DK PIN admin1 key PINPROT	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword specified is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	DD	4.4
02BF	Key Generate2 – DK PIN admin2 key MAC	CSNBKGN2	This combination is allowed: The key form *rule_array* keyword is OPEX or IMEX and *key_type_1* and *key_type_2* parameters are one of the valid key type pairs listed in the *Key type and key form keywords for AES keys - DK PIN methods* table in the column matching the key form.	DD	4.4
02C0	DK Random PIN Generate	CSNBDRPG		DD	4.4
02C1	DK PIN Verify	CSNBDPV		DD	4.4
02C2	DK PIN Change	CSNBDPC		DD	4.4
02C3	DK PRW Card Number Update	CSNBPNU		DD	4.4
02C4	DK PRW CMAC Generate	CSNBDPCG		DD	4.4
02C5	DK PAN Modify in Transaction	CSNBDPMT		DD	4.4
02C6	DK Deterministic PIN Generate	CSNBDDPG		DD	4.4
02C7	DK PAN Translate	CSNBDPT		DD	4.4
02C8	DK Regenerate PRW	CSNBDRP		DD	4.4
02CC	Diversified Key Generate2 – SESS-ENC	CSNBDKG2	Diversification process *rule_array* keyword SESS-ENC is allowed.	ED	4.4
02CD	Diversified Key Generate2 - DALL	CSNBDKG2	The key-generating key specified may have key-usage fields indicate that all key types may be derived.	DD, SC	4.4
02CE	DK Migrate PIN	CSNBDMP		DD	4.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
02CF	FPE Encrypt	CSNBFPEE		ED	5.0
02D0	FPE Decrypt	CSNBFPED		ED	5.0
02D1	FPE Translate	CSNBFPET		ED	5.0
02D2	Diversified Key Generate2 - MK-OPTC	CSNBDKG2	Diversification process *rule_array* keyword MK-OPTC is allowed.	ED	4.4.5
02D3	Diversified Key Generate2 – KDFFM-DK	CSNBDKG2	Diversification process *rule_array* keyword KDFFM-DK is allowed.	ED	4.4.5
02D5	Encrypted PIN Translate Enhanced	CSNBPTRE		ED	5.2
02D4	Diversified Key Generate2 - Allow length option with KDFFM-DK	CSNBDKG2	When the Diversification process *rule_array* keyword is KDFFM-DK, the bit length *rule_array* keyword may be KLEN192 or KLEN256.	DD	4.4.5
02EE	PKA Key Translate – allow INTUSCHG	CSNDPKT	Conversion service rule_array keyword INTUSCHG is allowed.	ED	6.3
02F8	Key Translate2 - COMP-CHK	CSNBKTR2	Encipherment *rule_array* keyword COMP-CHK is allowed.	ED	6.0
02F9	Key Translate2 - COMP-TAG	CSNBKTR2	Encipherment *rule_array* keyword COMP-TAG is allowed.	ED	6.0
0301	Prohibit Export Extended	CSNBPEXX		ED	
030C	DSG - ZERO-PAD restriction lifted	CSNDDSG	The value of the *hash_length* parameter may be greater than 36 when the data input type keyword is HASH.	DD	
030D	Key Encryption Translate – CBC to ECB	CSNBKET	Key translation *rule_array* keyword CBCTOECB is allowed.	DD ED on z13 and later server	
030E	Key Encryption Translate – ECB to CBC	CSNBKET	Key translation *rule_array* keyword ECBTOCBC is allowed.	DD ED on z13 and later server	
0310	Trusted Block Create - Activate an inactive block	CSNDTBC	Operational *rule_array* keyword ACTIVATE is allowed.	ED	

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
030F	Trusted Block Create - Create Block in inactive form	CSNDTBC	Operational *rule_array* keyword INACTIVE is allowed.	ED	
0311	PKA Key Import - Import an external trusted block	CSNDPKI	the token supplied in the *source_key_token* parameter may be a trusted block.	ED	
0312	Remote Key Export - Gen or export a non-CCA node key	CSNDRKX		ED	
0318	PKA Key Translate - from CCA RSA to SC Visa format	CSNDPKT	Output format *rule_array* keyword SCVISA is allowed.	ED	3.60
0319	PKA Key Translate - from CCA RSA to SC ME format	CSNDPKT	Output format *rule_array* keyword SCCOMME is allowed.	ED	3.60
031A	PKA Key Translate - from CCA RSA to SC CRT format	CSNDPKT	Output format *rule_array* keyword SCCOMCRT is allowed.	ED	3.60
031B	PKA Key Translate - from source EXP KEK to target EXP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an EXPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an EXPORTER key-encrypting key is allowed.	ED	3.60
031C	PKA Key Translate - from source IMP KEK to target EXP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an IMPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an EXPORTER key-encrypting key is allowed.	ED	3.60
031D	PKA Key Translate - from source IMP KEK to target IMP KEK	CSNDPKT	The combination of the key identifier supplied in the *source_key_identifier* parameter being an IMPORTER key-encrypting key and the key identifier supplied in the *target_key_identifier* parameter being an IMPORTER key-encrypting key is allowed.	ED	3.60
0326	PKA Key Generate – Clear ECC keys	CSNDPKG	The combination of Private Key Encryption *rule_array* keyword CLEAR and the algorithm of the skeleton key supplied in the *skeleton_key_identifier* parameter being ECC is allowed.	ED	4.0

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0327	Symmetric Key Export - AESKW	CSNDSYX	The combination of the Token Algorithm *rule_array* keyword being AES or HMAC and and Key formatting method *rule_array* keyword being AESKW is allowed.	ED	4.2
0329	Symmetric Key Import2 - AESKW	CSNDSYI2	The combination of the Token Algorithm *rule_array* keyword being AES or HMAC and Recovery method *rule_array* keyword being AESKW is allowed.	ED	4.2
032A	Key Translate2 - Disallow AES ver 5 to ver 4 conversion	CSNBKTR2	When the key token supplied in the *input_key_token* parameter is a version 5 AES key token, the token cannot be converted to a version 4 token.	DD	4.2
032B	Symmetric Key Import2 – disallow weak import	CSNDSYI	The key identifier supplied in the *RSA_private_key_identifier* parameter may not be weaker than the key being imported in the *RSA_enciphered_key* parameter.	DD, SC	4.2
		CSNDSYI2	The key identifier supplied in the *transport_key_identifier* parameter may not be weaker than the key being imported in the *encipher_key* parameter.		
		CSNBUKD	The key identifier supplied in the *transport_key_identifier* parameter may not be weaker than the keys being derived and returned in the *generated_key_identifier1*, *generated_key_identifier2*, and *generated_key_identifier3* parameters.		
032E	Trusted Block Create – Disallow triple-length MAC key	CSNDTBC	The MAC key in the trusted block may not be a triple-length key.	DD, SC	4.3
0334	Key Translate2 – Translate fixed to variable payload	CSNBKTR2	The key token supplied in the *input_key_token* parameter with a fixed-length payload will be re-enciphered with a variable-length payload.	DD, SC	4.4
0335	Unique Key Derive - K3IPEK	CSNBUKD	Output Key Selection *rule_array* keyword K3IPEK is allowed.	DD	4.4
0336	MAC Generate2 – AES CMAC	CSNBMGN2 CSNBMGN3	Token algorithm *rule_array* keyword AES is allowed.	ED	4.4
0337	MAC Verify2 – AES CMAC	CSNBMVR2 CSNBMVR3	Token algorithm *rule_array* keyword AES is allowed.	ED	4.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0338	PKA Key Translate - from CCA RSA CRT to EMVDDA format	CSNDPKT	Output format *rule_array* keyword EMVDDA is allowed.	ED	4.4
0339	PKA Key Translate - from CCA RSA CRT to EMVDDAE format	CSNDPKT	Output format *rule_array* keyword EMVDDAE is allowed.	ED	4.4
033A	PKA Key Translate - from CCA RSA CRT to EMVCRT format	CSNDPKT	Output format *rule_array* keyword EMVCRT is allowed.	ED	4.4
033B	Digital Signature Generate – PKCS-PSS allow small salt	CSNDDSG	For the PKCS-PSS formatting method, the salt length specified in the *data* parameter is required to be zero, the length of the hash specified, or longer. When the access control is enabled, the salt length may be less than the length of the hash.	DD	5.3
033C	Digital Signature Verify – PKCS-PSS allow not exact salt length	CSNDDSV	For the PKCS-PSS formatting method, the salt length derived from the signature must be an exact match for the salt length specified in the *data* parameter. When the access control is enabled, the NEXMATCH keyword may be specified in the *rule_array* parameter. When the NEXMATCH keyword is specified, the salt length derived from the signature need not be an exact match for the salt length specified with the *data* parameter.	DD	5.3
035F	ECC Diffie-Hellman – Allow DERIV02	CSNDEDH	The key agreement *rule_array* keyword DERIVE02 is allowed	ED	5.2
0360	ECC Diffie-Hellman	CSNDEDH		ED	4.2
0361	ECC Diffie-Hellman – Allow PASSTHRU	CSNDEDH	Key agreement *rule_array* keyword PASSTHRU is allowed.	ED	4.2
0362	ECC Diffie-Hellman – Allow key wrap override	CSNDEDH	Key wrapping method *rule_array* keywords WRAP-ENH and WRAP-ECB are allowed.	ED	4.2
0363	ECC Diffie-Hellman – Allow Prime Curve 192	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 192.	ED	4.2
0364	ECC Diffie-Hellman – Allow Prime Curve 224	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 224.	ED	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0365	ECC Diffie-Hellman – Allow Prime Curve 256	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 256.	ED	4.2
0366	ECC Diffie-Hellman – Allow Prime Curve 384	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 384.	ED	4.2
0367	ECC Diffie-Hellman – Allow Prime Curve 521	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a NIST Prime curve with a curve length of 521.	ED	4.2
0368	ECC Diffie-Hellman – Allow BP Curve 160	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 160.	ED	4.2
0369	ECC Diffie-Hellman – Allow BP Curve 192	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 192.	ED	4.2
036A	ECC Diffie-Hellman – Allow BP Curve 224	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 224.	ED	4.2
036B	ECC Diffie-Hellman – Allow BP Curve 256	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 256.	ED	4.2
036C	ECC Diffie-Hellman – Allow BP Curve 320	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 320.	ED	4.2
036D	ECC Diffie-Hellman – Allow BP Curve 384	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 384.	ED	4.2
036E	ECC Diffie-Hellman – Allow BP Curve 512	CSNDEDH	The EC keys specified in the *private_key_identifier* and *public_key_identifier* parameters may have attributes of a Brainpool curve with a curve length of 512.	ED	4.2
036F	ECC Diffie-Hellman – Prohibit weak key generate	CSNDEDH	The *output_key_identifier* parameter may specify a key that is stronger than the generating key.	DD, SC	4.2

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0382	T31X - Permit version D TR-31 key blocks	CSNBT31X	TR-31 key block protection method *rule_array* keyword VARDRV-D is allowed.	DD	5.4
0383	T31X - Permit AES KDKGENKY: KDKTYPEA to 11:X	CSNBT31X	The TR-31 key block protection method, TR-31 key usage values, and TR-31 modes of key use *rule_array* keywords and the attributes of the CCA key supplied in the *source_key_identifier* parameter determine which access control is required. All of this information is listed in the *Valid CCA to TR-31 Export Translations and Required Access Control Points (ACPs)* table in the CSNBT31X service description.	DD	5.4
0384	T31X - Permit AES KDKGENKY: KDKTYPEB to 10:X	CSNBT31X		DD	5.4
0385	T31X - Permit DES DKYGENKY: DKYL0:DMPIN to 12:X	CSNBT31X		DD	5.4
0386	T31I - Permit version D TR-31 key blocks	CSNBT31I	The key block supplied in the *TR31_key_block* parameter may have version ID D.	DD	5.4
038A	Encrypted PIN Translate2 – Permit ISO-4 to ISO-4 Translate	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword TRANSLAT is allowed.	ED	5.4
038B	Encrypted PIN Translate2 – Permit ISO-4 Reformat w/ PAN Chg	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT and the PAN change keyword PAN-CHG is allowed.	DD	5.4
038C	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-1, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed.	ED	5.4
038D	Encrypted PIN Translate2 – Permit ISO-4 to ISO-1 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-1, and the the *rule_array* mode keyword REFORMAT is allowed.	ED	5.4
038E	Encrypted PIN Translate2 – Permit ISO-0 to ISO-4 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-0, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed.	ED	5.4
038F	Encrypted PIN Translate2 – Permit ISO-4 to ISO-0 Reformat	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-0, and the the *rule_array* mode keyword REFORMAT is allowed.	ED	5.4
0391	Encrypted PIN Translate2 – REFORMAT with AES token	CSNBPTR2	Process rule *rule_array* keyword REFORMAT is allowed.	ED	5.4

Offset (Hex)	Name	Callable services	Parameters affected when enabled	Usage	Release
0392	Encrypted PIN Translate2 – TRANSLAT with AES token	CSNBPTR2	Process rule *rule_array* keyword TRANSLAT is allowed.	ED	5.4
0393	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 RFMT1TO4.	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-1, the *output_PIN_profile* PIN block format being ISO-4, and the the *rule_array* mode keyword REFORMAT is allowed. The output_PIN_encrypting_key_identifier must have key attribute RFMT1TO4 enabled.	DD	5.4
0395	Encrypted PIN Translate2 - Permit ISO-4 to ISO-4 PTR2AUTH	CSNBPTR2	The combination of the *input_PIN_profile* PIN block format being ISO-4, the *output_PIN_profile* PIN block format being ISO-4, and the the rule_array mode keyword REFORMAT and the PAN change keyword PAN-CHG is allowed. In addition, the AES MAC key identified by the *authentication_key_identifier* must have the PTR2AUTH key usage attribute enabled.	DD	5.5

Access controls affecting multiple services

The **Name** column contains the control name as it appears on the TKE workstation and ICSF Domain Role panels

The **Callable services** column contains the service name of all services affected by the control or a description of the services.

The **Parameters affected when enabled** column contains the service parameters that are affected when the control is enabled. The control may restrict the value of the a parameter or allow a value to be used. When the field is blank, the access control applies to the service in general. That is, the access control must be enabled to use the service regardless of any other controls for the service.

The **Notes** column contains additional comments or references to the ICSF books for additional information.

The **Offset** column contains the hexadecimal offset of the access control point in the domain role.

The **Usage** column contains the default value of the access control point. See the introduction for a discussion of the values.

The **Release** column contains the coprocessor code level the access control first became available. When the field is blank, the access control is available for all servers and coprocessors. See table 5 for CCA code levels.

Table 3. Access controls affecting multiple services or requiring special consideration

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
Allow weak wrapping of compliance-tagged keys by DES MK	Services that use DES key tokens		Applies to domains in imprint or compliance mode. Applies to all secure DES keys (non-compliant-tagged and compliant-tagged)	02EB	DD, SC	6.0
Allow weak DES wrap of RSA	CSNDPKG CSNDPKI CSNDPKT	Any DES key-encrypting keys and RSA private key tokens.	A weaker DES key-encrypting key is allowed to wrap an RSA private key token. The Prohibit weak wrap – Transport keys access control must be enabled and this access control will override the restriction.	0331	DD,SC	4.3
ANSI X9.8 PIN –	CSNBPTR	The value in the PAN data parameters	See “ANSI X9.8 PIN Restrictions” in the	0351	DD, SC	4.1

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
Allow modification of PAN	CSNBPTR2 CSNBPTRE CSNBSPN	(CSNBPTR: *PAN_data_in*, *PAN_data_out*, CSNBSPN: *input_PAN_data*, *output_PAN_data*) are affected.	"Financial Services" chapter of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*			
ANSI X9.8 PIN - Allow only ANSI PIN blocks	CSNBPTR CSNBPTR2 CSNBPTRE CSNBSPN	The PIN block format is restricted to ANSI formats. The PIN block profile parameters are affected.	See "ANSI X9.8 PIN Restrictions" in the "Financial Services" chapter of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*	0352	DD, SC	4.1
ANSI X9.8 PIN - Enforce PIN block restrictions	CSNBCPA	When the PIN calculation method *rule_array* keyword is VISA-PVV, the *PIN_profile* must specify ISO-0 or ISO-3 formats.	See "ANSI X9.8 PIN Restrictions" in the "Financial Services" chapter of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*	0350	DD, SC	4.1
	CSNBPFO	Only a PIN-block format keyword of ISO-0 or ISO-3 is allowed in the input PIN_profile parameter.				
	CSNBPTR	• The *output_PIN_profile* parameter can not specify the IBM 3624 PIN format when the *input_PIN_profile* parameter doesn't specify IBM 3624. • The *input_PIN_profile* can not specify ISO-0 or ISO-3 formats unless the *output_PIN_profile* specifies ISO-0 or ISO-3. • The *output_PIN_profile* parameter can not specify ISO-1 or ISO-2 formats when the *input_PIN_profile* parameter specifies ISO-0, ISO-3, or VISA4. • When the *input_PIN_profile* parameter specifies either ISO-0 or ISO-3 formats, the decrypted PIN block will be examined to ensure that the PAN within the PIN block is the same as the PAN which was supplied as the *input_PAN_data* parameter, and that this is the same as the PAN which was supplied as the *output_PAN_data* parameter. • The *input_PAN_data* and *output_PAN_data* parameters of must be equivalent.	*See "ANSI X9.8 PIN Restrictions" in the "Financial Services" chapter of the z/OS Cryptographic Services ICSF Application Programmer's Guide*			

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
	CSNBPTR2	• The *output_PIN_profile* parameter can not specify the IBM 3624 PIN format when the *input_PIN_profile* parameter doesn't specify IBM 3624. • The *input_PIN_profile* can not specify ISO-0, ISO-3, or ISO-4 formats unless the *output_PIN_profile* specifies ISO-0, ISO-3 or ISO-4. • The *output_PIN_profile* parameter can not specify ISO-1 or ISO-2 formats when the *input_PIN_profile* parameter specifies ISO-0, ISO-3, ISO-4, or VISA4. • When the *input_PIN_profile* parameter specifies either ISO-0 or ISO-3 formats, the decrypted PIN block will be examined to ensure that the PAN within the PIN block is the same as the PAN which was supplied as the *input_PAN_data* parameter, and that this is the same as the PAN which was supplied as the *output_PAN_data* parameter.				
	CSNBPTRE	• The *output_PIN_profile* parameter can not specify the IBM 3624 PIN format when the *input_PIN_profile* parameter doesn't specify IBM 3624. • The *input_PIN_profile* can not specify ISO-0 or ISO-3 formats unless the *output_PIN_profile* specifies ISO-0 or ISO-3. • The *output_PIN_profile* parameter can not specify ISO-1 or ISO-2 formats when the *input_PIN_profile* parameter specifies ISO-0, ISO-3, or VISA4. • When the *input_PIN_profile* parameter specifies either ISO-0 or ISO-3 formats, the decrypted PIN block will be examined to ensure that the PAN within the PIN block is the same as the PAN which was supplied as				

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
		the *input_PAN_data* parameter, and that this is the same as the PAN which was supplied as the *output_PAN_data* parameter.				
	CSNBSPN	• The *output_PIN_profile* parameter can not specify the IBM 3624 PIN format when the *input_PIN_profile* parameter doesn't specify IBM 3624. • The *output_PIN_profile* parameter can not specify ISO-1 or ISO-2 formats when the *input_PIN_profile* parameter specifies ISO-0, ISO-3, or VISA4. • When the *input_PIN_profile* parameter specifies either ISO-0 or ISO-3 formats, the decrypted PIN block will be examined to ensure that the PAN within the PIN block is the same as the PAN which was supplied as the *input_PAN_data* parameter, and that this is the same as the PAN which was supplied as the *output_PAN_data* parameter. • The *input_PAN_data* and *output_PAN_data* parameters of must be equivalent.				
ANSI X9.8 PIN – Use stored decimalization tables only	CSNBCPE CSNBPGN CSNBCPA CSNBEPG CSNBPVR CSNBPF0	The decimalization_table in the *data_array* parameter must match one of the active decimalization tables in the coprocessors.	See “ANSI X9.8 PIN Restrictions” in the “Financial Services” chapter of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*	0356	DD, SC	4.2
Authenticated Key Export - DRVTXKEY	CSNBSYD CSNBSYD1 CSNBSYE CSNBSYE1 CSNBFLD CSNBFLE CSNBKRR2	Required in order to establish a secure communication channel between the coprocessor and CPACF.		02F6	AE	6.0

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
Authenticated Key Export - EXPTSK	CSNBSYD CSNBSYD1 CSNBSYE CSNBSYE1 CSNBFLD CSNBFLE CSNBKRR2	Required in order to export secure key tokens to CPACF protected key format.	APAR OA54264 changed the Usage from enable by default to always enabled.	02F7	AE	6.0
Authenticated Key Export - SETSNKEY	CSNBSYD CSNBSYD1 CSNBSYE CSNBSYE1 CSNBFLD CSNBFLE CSNBKRR2	Required in order to establish a secure communication channel between the coprocessor and CPACF.		02F5	AE	6.0
DATAM Key Management Control	CSNBKGN CSNBKIM CSNBKEX CSNBDKG	When enabled, the DATAM and DATAMV key types can be used or generated. When disabled, the key types are not allowed.		0275	ED	
Disallow 24-byte DATA wrapped with 16-byte Key	CSNBCKI CSNBDKM CSNBDKG CSNDEDH CSNBKEX CSNBKGN CSNBKIM CSNBKTR CSNBKTR2 CSNBCKM CSNBSKM CSNBSKI CSNDSYG CSNDSYI	When enabled, a triple-length DATA keys cannot be wrapped by a 16-byte DES Key, either the master key or a key-encrypting key. See “Key strength and wrapping of key” in the *z/OS Cryptographic Services ICSF Application Programmer's Guide* for more information.		032D	DD, SC	4.1
Disallow translation from AES wrapping to	CSNBKTR2 CSNDPKT	Disallows the input key from being wrapped an AES key-encrypting key to being wrapped by a DES key-encrypting key.		01C5	DD	5.4

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
DES wrapping	CSNBPTR2	Disallows the input PIN block from being wrapped an AES PIN-encrypting key to being wrapped by a DES PIN-encrypting key.				
Disallow translation from AES wrapping to weaker AES wrapping	CSNBKTR2 CSNDPKT	Disallows the input key from being wrapped an AES key-encrypting key to being wrapped by a weaker AES key-encrypting key.		01C6	DD	5.4
	CSNBPTR2	Disallows the input PIN block from being wrapped an AES PIN-encrypting key to being wrapped by a weaker AES PIN-encrypting key.				
Disallow translation from DES wrapping to weaker DES wrapping	CSNBEPG CSNBPFO	Disallows the PIN from being generated a DES PIN-generating key and being wrapped by a weaker DES PIN-encrypting key.		01C7	DD	5.4
	CSNBAPG CSNBPTR CSNBPTR2 CSNBPTRE	Disallows the input PIN block from being wrapped an DES PIN-encrypting key to being wrapped by a weaker DES PIN-encrypting key.				
	CSNBKTR CSNBKTR2 CSNDPKT	Disallows the input key from being wrapped an DES key-encrypting key to being wrapped by a weaker DES key-encrypting key.				
	CSNBSKY	Disallows the input key from being wrapped an DES key-encrypting key to being wrapped by a weaker DES secure-messaging key.				
DUKPT - PIN Verify, PIN Translate	CSNBPTR CSNBPTR2 CSNBPTRE CSNBPVR	When enabled, the key identifier parameters for the PIN block encrypting keys must specify key-generating keys to be used to derive the PIN block encrypting keys. Rule array keywords define which key identifier parameters are affected.		00E1	ED	5.2
Enhanced PIN Security	CSNBCPA CSNBCPE CSNBEPG CSNBPCU CSNBPFO	When enabled, this control affects callable services that extract or format a PIN using a PIN-block format of 3621 or 3624 with a PIN-extraction method of PADDIGIT.	See “Enhanced PIN Security Mode” in the “Financial Services” chapter of the *z/OS Cryptographic Services ICSF Application Programmer's Guide*	0313	DD, SC	

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
	CSNBPTR CSNBPTR2 CSNBPTRE CSNBPVR					
High-performance secure AES keys	CSNBSYD CSNBSYD1 CSNBSYE CSNBSYE1	The combination of the Algorithm *rule_array* keyword being AES and the identifier supplied in the *key_identifier* parameter being the CKDS label of operational AES DATA key encrypted under the master key is allowed		0296	ED	4.0
	CSNBFLD CSNBFLE	The combination of the Algorithm *rule_array* keyword being AESVFPE and the identifier supplied in the *key_identifier* parameter being the CKDS label of operational AES DATA key encrypted under the master key is allowed				
	CSNBKRR2 CSNEKRR2	The PROTKEY *rule_array* keyword can be used and the *key_label* parameter identifies a record with a AES DATA key.				
	CSFWRP CSFWRP6	The access control must be enable for operation.				
High-performance secure DES keys	CSNBSYD CSNBSYD1 CSNBSYE CSNBSYE1	The combination of the Algorithm *rule_array* keyword being DES and the identifier supplied in the *key_identifier* parameter being the CKDS label of operational DES DATA key encrypted under the master key is allowed		0295	ED	4.0
	CSNBFLD CSNBFLE	The combination of the Algorithm *rule_array* keyword being TDESVFPE and the identifier supplied in the *key_identifier* parameter being the CKDS label of operational DES DATA key encrypted under the master key is allowed				
	CSNBKRR2 CSNEKRR2	The PROTKEY *rule_array* keyword can be used and the *key_label* parameter identifies a record with a DES DATA key.				

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
	CSFWRP CSFWRP6	The access control must be enable for operation.				
NOCV KEK usage for export-related functions	CSNBDKX CSNBDCM CSNBGIM CSNBKEX CSNBKGN CSNDRKX	A NOCV EXPORTER may be specified in the key identifier parameter for the key-encrypting key		0300	ED, SC	
NOCV KEK usage for import-related functions	CSNBDKM CSNBGIM CSNBKGN CSNBKIM CSNBSKM CSNDRKX CSNBSKI	A NOCV IMPORTER may be specified in the key identifier parameter for the key-encrypting key		030A	ED, SC	
Prohibit weak wrap – Master keys	CSNBCKI CSNBCKM CSNBDKM CSNBDKG CSNBKGN CSNBKGN2 CSNBKIM CSNBKPI CSNBKPI2 CSNBMKP CSNBPEX CSNBRKA CSNBSKI CSNBSKM CSNBT31I CSNBUKD CSNDEDH CSNDKTC CSNDPKG CSNDPKI	When enabled, an attempt to wrap a stronger key with a weaker master key will not be permitted. Also, when loading the last part into the new DES or RSA master key register using the Master Key Entry utility, if the complete master key is weak, the key part will be rejected.	Both symmetric and asymmetric keys are affected	0333	DD, SC	4.2

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
	CSNDSYG CSNDSYI CSNDSYI2					
Prohibit weak wrap – Transport keys	CSNBKGN2 CSNDEDH CSNDPKG CSNDSYI CSNDSYX	When enabled, an attempt to wrap a stronger key with a weaker transport key will not be permitted.	Both symmetric and asymmetric keys are affected	0328	DD, SC	4.2
Symmetric Key Token Change – RTCMK	Services that use operational fixed-length symmetric key tokens	When enabled, this control allows symmetric key tokens under the old master key to be reenciphered under the current master key. These reenciphered tokens are returned from all callable service that use symmetric tokens.		0090	AE	
Symmetric Key Token Change2 – RTCMK	Services that use operational variable-length symmetric key tokens	When enabled, this control allows symmetric key tokens under the old master key to be reenciphered under the current master key. These reenciphered tokens are returned from all callable service that use symmetric tokens.		00F1	AE	4.1
Symmetric token wrapping - internal enhanced method	Services that wrap internal symmetric key tokens	Allows the value for internal wrapping method for the DEFAULTWRAP parameter in the installation options data set to be set to ENHANCED. When enabled, this control allow ICSF to change the default wrapping setting for internal tokens to be the enhanced method.	When wrapping method is ENHANCED, all generated or imported keys to be wrapped with the enhanced method. This wrapping can be overridden by rule array keywords for certain services. Each service has an access control that must be enabled to allow the wrapping to be overridden.	0139	AE	4.1
Symmetric token wrapping - internal original	Services that wrap internal	Allows the value for internal wrapping method for the DEFAULTWRAP parameter in the installation options data set to be set to	When wrapping method is ORIGINAL, all generated or imported keys to be wrapped with the original method.	013A	AE	4.1

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
method	symmetric key tokens	ORIGINAL. When enabled, this control allow ICSF to change the default wrapping setting for internal tokens to be the original method.	 This wrapping can be overridden by rule array keywords for certain services. Each service has an access control that must be enabled to allow the wrapping to be overridden.			
Symmetric token wrapping - external enhanced method	Services that wrap external symmetric key tokens	Allows the value for external wrapping method for the DEFAULTWRAP parameter in the installation options data set to be set to ENHANCED. When enabled, this control allow ICSF to change the default wrapping setting for external tokens to be the enhanced method.	When wrapping method is ENHANCED, all generated or exported keys to be wrapped with the enhanced method. This wrapping can be overridden by rule array keywords for certain services. Each service has an access control that must be enabled to allow the wrapping to be overridden.	013B	AE	4.1
Symmetric token wrapping - external original method	Services that wrap external symmetric key tokens	Allows the value for external wrapping method for the DEFAULTWRAP parameter in the installation options data set to be set to ORIGINAL. When enabled, this control allow ICSF to change the default wrapping setting for external tokens to be the original method.	When wrapping method is ORIGINAL, all generated or exported keys to be wrapped with the original method. This wrapping can be overridden by rule array keywords for certain services. Each service has an access control that must be enabled to allow the wrapping to be overridden.	013C	AE	4.1
Warn when weak wrap – Master keys	CSNBCKI CSNBCKM CSNBDKM CSNBDKG CSNBKGN CSNBKGN2 CSNBKIM CSNBKPI CSNBKPI2 CSNBPEX CSNBRKA	When enabled, an informational return code will be returned when attempting to wrap a stronger key with a master key that is weaker. Also, a warning will be returned when the last part is loaded into the DES or RSA new master key register, if the master key is weak.	Both symmetric and asymmetric keys are affected	0332	DD. SC	4.2

Name	Callable services	Parameters affected when enabled	Notes	Offset (hex)	Usage	Release
	CSNBSKI CSNBSKM CSNBT31I CSNBUKD CSNDEDH CSNDKTC CSNDPKG CSNDPKI CSNDSYG CSNDSYI CSNDSYI2					
Warn when weak wrap – Transport keys	CSNBKGN2 CSNDEDH CSNDPKG CSNDPKT CSNDSYX CSNDSY1	When enabled, an informational return code will be returned when attempting to wrap a stronger key with a weaker key or when attempting to import a key token that has previously been wrapped with a weaker key, as indicated by its security history field.	Both symmetric and asymmetric keys are affected	032C	DD. SC	4.2

There are relationships between certain access controls. A controlling access control is required to be enabled before subordinate access controls can enabled. The TKE workstation will enable the controlling access control when a subordinate access control is enabled.

- The **ANSI X9.8 PIN - Allow modification of PAN** and **ANSI X9.8 PIN – Allow only ANSI PIN blocks** access controls can only be enable when the **ANSI X9.8 PIN - Enforce PIN block restrictions** access control is enabled.

Access controls for ICSF utilities

Access to utilities that are executed on the CCA coprocessor is through access controls in the domain role. To execute utilities on the coprocessor, access controls must be enabled for the utility.

The **Name** column contains the control name as it appears on the TKE workstation and ICSF Domain Role panels

The **Utilities** column contains the ICSF ISPF panel utilities that require the access control to be enabled in order to use the utility.

The **Offset** column contains the hexadecimal offset of the access control point in the domain role.

The **Usage** column contains the default value of the access control. See the introduction for a discussion of the values.

The **Release** column contains the coprocessor code level the access control first became available. When the field is blank, the access control is available for all servers and coprocessors. See table 5 for CCA code levels.

Table 4. Access controls and associated utilities

Name	Utilities	Offset (Hex)	Usage	Release
AES Master Key - Clear new master key register	Master Key Entry, Pass Phrase Initialization	0124	ED	3.30
AES Master Key - Combine key parts	Master Key Entry, Pass Phrase Initialization	0126	ED	3.30
AES Master Key - Load first key part	Master Key Entry, Pass Phrase Initialization	0125	ED	3.30
AES Master Key - Set master key	Set Master Key, Pass Phrase Initialization	0128	AE	3.30
CKDS Conversion2 - Allow use of REFORMAT	CKDS Conversion 2	014C	ED	4.1
CKDS Conversion2 - Allow wrapping override keywords	CKDS Conversion 2	0146	AE	4.1
CKDS Conversion2 - Convert from enhanced to original	CKDS Conversion 2	0147	ED	4.1
DES Master Key - Clear new master key register	Master Key Entry, Pass Phrase Initialization	0032	ED	
DES Master Key - Combine key parts	Master Key Entry, Pass Phrase Initialization	0019	ED	
DES Master Key - Load first key part	Master Key Entry, Pass Phrase Initialization	0018	ED	
DES master key – 24-byte key	Master Key Entry, Pass Phrase Initialization	0330	DD, SC	4.3
DES Master Key - Set master key	Set Master Key, Pass Phrase Initialization	001A	AE	
ECC Master Key - Clear new master key register	Master Key Entry, Pass Phrase Initialization	031F	ED	4.0

Name	Utilities	Offset (Hex)	Usage	Release
ECC Master Key - Combine key parts	Master Key Entry, Pass Phrase Initialization	0321	ED	4.0
ECC Master Key - Load first key part	Master Key Entry, Pass Phrase Initialization	0320	ED	4.0
ECC Master Key - Set master key	Set Master Key, Pass Phrase Initialization	0322	AE	4.0
Operational Key Load	Operational Key Load, KGUP	0309	ED	
Operational Key Load - Variable-Length Tokens	Operational Key Load, KGUP	029E	ED	4.1
PCF CKDS Conversion - Allow wrapping override keywords	PCF CKDS Conversion	0148	ED	
PCF CKDS Conversion Program	PCF CKDS Conversion	0303	ED	
Reencipher CKDS	Reencipher CKDS	001E	AE	
Reencipher CKDS2	Reencipher CKDS	00F0	AE	4.1
Reencipher PKDS	Reencipher PKDS	0241	AE	
RSA Master Key - Clear new master key register	Master Key Entry, Pass Phrase Initialization	0060	ED	
RSA Master Key - Combine key parts	Master Key Entry, Pass Phrase Initialization	0054	ED	
RSA Master Key - Load first key part	Master Key Entry, Pass Phrase Initialization	0053	ED	
RSA Master Key - Set master key	Set Master Key, Pass Phrase Initialization	0057	AE	

The key generator utility program (KGUP), which is used to manage keys in the CKDS, requires these access controls be enabled to use the utility.

Key Generate – OP
Key Generate – Key set
Key Generate – Key set extended
Key Generate – SINGLE-R
Key Generate2 – Key set
Key Generate2 – Key set extended
Key Generate2 – OP
Key Import
Multiple Clear Key Import /Multiple Secure Key Import - AES
Secure Key Import2 - OP
Secure Key Import2 – IM

The PKDS keys utility, which is used to manage keys in the PKDS, requires these access controls be enabled to use the utility.

Digital Signature Generate
PKA Key Generate

CCA code level cross reference

Table 5 lists the CCA code level used in the previous tables and the ICSF release, licensed internal code release, Crypto Express feature and z server.

The **Code level** column lists the short designation of the release of the licensed internal code. This designation is used in the access control table. It is the same as the release level used by the IBM 4765/4767/4768 coprocessors.

The **ICSF release** column lists the release where the support for the code was introduced.

The **z server** column lists the system z servers that supports the Crypto Express feature for which the code is available.

The **Crypto Express coprocessor** column lists the feature for which the code is available.

The **Licensed internal code release** column lists the date the code was made available.

The **Notes** column lists addition information about the code level.

Table 5. CCA code levels

Code level	ICSF release	z server	Crypto Express coprocessor	Licensed internal code release	Notes
6.3	HCR77D0 OA57089 OA57088	IBM z14	CEX6C	July, 2019	CCA SPE
6.2	HCR77D0	IBM z14	CEX6C	December, 2018	z14 GA2
6.0	HCR77C1	IBM z14	CEX6C	September, 2017	z14 GA1
5.5	HCR77D0 OA57089 OA57088	IBM z14	CEX5C	July, 2019	CCA SPE
5.5	HCR77D0 OA57089 OA57088	IBM z13	CEX5C	July, 2019	CCA SPE
5.4	HCR77C1 OA55184	IBM z14	CEX5C	November, 2018	CCA SPE
5.3	HCR77C0	IBM z13	CEX5C	October, 2016	

		IBM z13S			
5.2	HCR77B1	IBM z13 IBM z13S	CEX5C	March, 2016	z13 GA2, CCA Algorithm part B SPE
5.1		IBM z13 IBM z13S	CEX5C	July, 2015	CCA Algorithm part A SPE
5.0	HCR77B0	IBM z13 IBM z13S	CEX5C	February, 2015	z13 GA1
4.50		IBM zEnterprise EC12 IBM zEnterprise BC12	CEX4C	September, 2013	DK AES PIN SPEs
4.4.5		IBM zEnterprise EC12 IBM zEnterprise BC12	CEX4C	July, 2015	CCA Algorithm part A SPE
4.4	HCR77A1	IBM zEnterprise EC12 IBM zEnterprise BC12	CEX4C	September, 2013	zEC12 GA2
4.3	HCR77A0	IBM zEnterprise EC12 IBM zEnterprise BC12	CEX4C	September 2012	zEC12 GA1
4.2	HCR7790	IBM zEnterprise 196 IBM zEnterprise 114	CEX3C	September 2011	z196 GA2
4.1	HCR7780	IBM zEnterprise 196 IBM zEnterprise 114	CEX3C	September 2010	z196 GA1
4.0	HCR7770	IBM System z10 EC IBM System z10 BC	CEX3C	November, 2009	
3.40/3.60	HCR7751	IBM System z10 EC IBM System z10 BC	CEX2C	November, 2008	
3.30	HCR7750	IBM System z9 EC IBM System z9 BC	CEX2C	November, 2007	

ICSF – IBM 4764/4765/4767 Cryptographic Coprocessor cross reference

Table 5 lists the ICSF access control name and the equivalent command name for the IBM 4764 PCI-X and IBM 4765 and IBM 4767 PCIe Cryptographic Coprocessors. The table is ordered by the offset.

Those access controls for the 4764/4765/4767 coprocessor which are not used by ICSF are not listed. N/A in the 4767 command name column indicates that the access control is not used by the 4764/4765/4767 coprocessor.

The Offset column contains the hexadecimal offset of the access control point in the domain role.

Table 5. Cross reference - ICSF access control names and IBM 4767 command names

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
000E	Encipher - DES	Encipher	CSNBENC
000F	Decipher - DES	Decipher	CSNBDEC
0010	MAC Generate	Generate MAC	CSNBMGN
0011	MAC Verify	Verify MAC	CSNBMVR
0012	Key Import	Reencipher to Master Key	CSNBKIM
0013	Key Export	Reencipher from Master Key	CSNBKEX
0018	DES Master Key - Load first key part	Load First Master Key Part	CSNBMKP
0019	DES Master Key - Combine key parts	Combine Master Key Parts	CSNBMKP
001A	DES Master Key - Set master key	Set Master Key	CSNBMKP
001B	Key Part Import - First key part	Load First Key Part	CSNBKPI
001C	Key Part Import - Middle and final	Combine Key Parts	CSNBKPI
001D	Key Test and Key Test2	Compute Verification Pattern	CSNBKYT CSNBKYTX CSNBKYT2
001F	Key Translate	Translate Key	CSNBKTR
0021	Key Test2 – AES, ENC-ZERO	Compute ENC-ZERO Verification Pattern for AES	CSNBKYT2
0022	Key Test2 – AES, CMACZERO	Compute CMACZERO Verification Pattern for AES	CSNBKYT2

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0023	Key Test2 – DES, CMACZERO	Compute CMAC Verification Pattern for DES	CSNBKYT2
0024	DK Random PIN Generate2	Allow DK Random PIN Generate2	CSNBDRG2
0025	DK PRW Card Number Update2	Allow DK PRW Card Number Update2	CSNBDCU2
0032	DES Master Key - Clear new master key register	Clear New Master Key Register	CSNBMKP
003A	PKA Key Import – Disallow clear key import	PKI: Disallow Clear Key Import	CSNBPKI
0040	Diversified Key Generate - CLR8–ENC	Generate Diversified Key (CLR8-ENC)	CSNBDKG
0041	Diversified Key Generate - TDES-ENC	Generate Diversified Key (TDES-ENC)	CSNBDKG
0042	Diversified Key Generate - TDES-DEC	Generate Diversified Key (TDES-DEC)	CSNBDKG
0043	Diversified Key Generate - SESS-XOR	Generate Diversified Key (SESS-XOR)	CSNBDKG
0044	Diversified Key Generate – single length or same halves	Enable DKG Single Length Keys and Equal Halves for TDES-ENC, TDES-DEC	CSNBDKG
0045	Diversified Key Generate - TDES-XOR	Generate Diversified Key (TDES-XOR)	CSNBDKG
0046	Diversified Key Generate - TDESEMV2/TDESEMV4	Generate Diversified Key (TDESEMV*n*)	CSNBDKG
0053	RSA Master Key - Load first key part	Load First Asymmetric Master Key Part	CSNBMKP
0054	RSA Master Key - Combine key parts	Combine Asymmetric Master Key	CSNBMKP
0057	RSA Master Key - Set master key	Set Asymmetric Master Key	CSNBMKP
0060	RSA Master Key - Clear new master key register	Clear New Asymmetric Master Key Buffer	CSNBMKP
0070	Public Infrastructure Certificate	Public Infrastructure Certificate	CSNDPIC
007C	Public Infrastructure Certificate - PK10SNRQ	PIC: Create PKCS#10 Certification Request	CSNDPIC
0080	Diversify Directed Key	Diversify Directed Key	CSNBDDK
0081	Diversify Directed Key – Allow KDFFM DERIVE	Diversify Directed Key (KDFFM DERIVE)	CSNBDDK
0082	Diversify Directed Key – Allow KDFFM GENERATE	Diversify Directed Key (KDFFM GENERATE)	CSNBDDK
008C	Key Generate – Key set	Generate Key Set	CSNBKGN
008E	Key Generate – OP	Generate Key	CSNBKGN CSNBRNG
0090	Symmetric Key Token Change - RTCMK	Reencipher to Current Master Key	CSNBKTC

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
00A0	Clear PIN Generate - 3624	Generate Clear 3624 PIN	CSNBPGN
00A1	Clear PIN Generate - GBP	N/A	
00A2	Clear PIN Generate - VISA PVV	N/A	
00A3	Clear PIN Generate - Interbank	N/A	
00A4	Clear Pin Generate Alternate – 3624 Offset	Generate Clear 3624 PIN Offset	CSNBCPA
00AB	Encrypted PIN Verify - 3624	Verify Encrypted 3624 PIN	CSNBPVR
00AC	Encrypted PIN Verify - GPB	Verify Encrypted German Bank Pool PIN	CSNBPVR
00AD	Encrypted PIN Verify - VISA PVV	Verify Encrypted Visa PVV	CSNBPVR
00AE	Encrypted PIN Verify - Interbank	Verify Encrypted InterBank PIN	CSNBPVR
00AF	Clear PIN Encrypt	Format and Encrypt PIN	CSNBCPE
00B0	Encrypted PIN Generate - 3624	Generate Formatted and Encrypted 3624	CSNBEPG
00B1	Encrypted PIN Generate - GBP	Generate Formatted and Encrypted German Bank Pool PIN	CSNBEPG
00B2	Encrypted PIN Generate - Interbank	Generate Formatted and Encrypted InterBank PIN	CSNBEPG
00B3	Encrypted PIN Translate - Translate	Encrypted PIN Translate - TRANSLAT	CSNBPTR
00B7	Encrypted PIN Translate - Reformat	Encrypted PIN Translate - REFORMAT	CSNBPTR CSNBPTRE CSNBPTR2
00BB	Clear PIN Generate Alternate - VISA PVV	Generate Clear Visa PVV Alternate	CSNBCPA
00BC	PIN Change/Unblock – change EMV PIN with OPINENC	Generate PIN Change Using OPINENC	CSNBPCU
00BD	PIN Change/Unblock – change EMV PIN with IPINENC	Generate PIN Change Using IPINENC	CSNBPCU
00C3	Clear Key Import / Multiple Clear Key Import - DES	Encipher Under Master Key	CSNBCKI CSNBCKM
00C4	Secure Key Import – DES, OP	N/A	
00CD	Prohibit Export	Lower Export Authority	CSNBPEX
00D6	Control Vector Translate	Translate Control Vector	CSNBCVT
00D7	Key Generate – Key set extended	Generate Key Set Extended	CSNBKGN

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
00DA	Cryptographic Variable Encipher	Encipher Cryptovariable	CSNBCVE
00DB	Key Generate - SINGLE-R	Replicate Key	CSNBKGN CSNDRKX
00DC	Secure Key Import – DES, IM	N/A	
00DF	Visa CVV Generate	Generate CVV	CSNBCSG
00E0	Visa CVV Verify	Verify CVV	CSNBCSV
00E1	DUKPT - PIN Verify, PIN Translate	Derived Unique Key Per Transaction, ANS X9.24	CSNBPTR CSNBPVR
00E4	HMAC Generate – SHA-1	Generate SHA-1 HMAC	CSNBHMG CSNBMGN2
00E5	HMAC Generate – SHA-224	Generate SHA-224	CSNBHMG CSNBMGN2
00E6	HMAC Generate – SHA-256	Generate SHA-256	CSNBHMG CSNBMGN2
00E7	HMAC Generate – SHA-384	Generate SHA-384	CSNBHMG CSNBMGN2
00E8	HMAC Generate – SHA-512	Generate SHA-512	CSNBHMG CSNBMGN2
00E9	Restrict Key Attribute – Export Control	Lower Export Authority2	CSNBRKA
00EA	Key Generate2 – OP	Generate2 Key	CSNBKGN2
00EB	Key Generate2 – Key set	Generate2 Key	CSNBKGN2
00EC	Key Generate2 – Key set extended	Generate2 Key Set Extended	CSNBKGN2
00F0	Reencipher CKDS2	N/A	
00F1	Symmetric Key Token Change2 – RTCMK	Reencipher to Current Master	CSNBKTC2
00F2	Secure Key Import2 - OP	N/A	
00F3	Secure Key Import2 - IM	N/A	
00F4	Symmetric Key Import2 – HMAC,PKOAEP2	Import HMAC Key (PKOAEP2)	CSNDSYI2

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
00F5	Symmetric Key Export – HMAC,PKOAEP2	Export HMAC Key (PKOAEP2)	CSNDSYX
00F7	HMAC Verify – SHA-1	Verify SHA-1 HMAC	CSNBHMV CSNBMVR2
00F8	HMAC Verify – SHA-224	Verify SHA-224 HMAC	CSNBHMV CSNBMVR2
00F9	HMAC Verify – SHA-256	Verify SHA-256 HMAC	CSNBHMV CSNBMVR2
00FA	HMAC Verify – SHA-384	Verify SHA-384 HMAC	CSNBHMV CSNBMVR2
00FB	HMAC Verify – SHA-512	Verify SHA-512 HMAC	CSNBHMV CSNBMVR2
00FC	Symmetric Key Export – AES, PKOAEP2	Export AES Key (PKOAEP2)	CSNDSYX
00FD	Symmetric Key Import2 – AES, PKOAEP2	Import AES Key (PKOAEP2)	CSNDSYI2
00FE	PKA Key Translate – Translate internal key token	PKT from Old to New Format - Internal	CSNDPKT
00FF	PKA Key Translate – Translate external key token	PKT from Old to New Format - External	CSNDPKT
0100	Digital Signature Generate	PKA96 Digital Signature Generate	CSNDDSG
0101	Digital Signature Verify	PKA96 Digital Signature Verify	CSNDDSV
0102	PKA Key Token Change RTCMK	PKA96 Reencipher to Current Master Key	CSNDKTC
0103	PKA Key Generate	PKA96 PKA Key Generate	CSNDPKG
0104	PKA Key Import	PKA96 PKA Key Import	CSNDPKI
0105	Symmetric Key Export – DES, PKCS-1.2	Symmetric Key Export PKCS-1.2/OAEP	CSNDSYX CSNDSXD
0106	Symmetric Key Import – DES, PKCS-1.2	Symmetric Key Import PKCS-1.2/OAEP	CSNDSYI
0109	Data Key Import	Data Key Import	CSNBDKM
010A	Data Key Export	Data Key Export	CSNBDKX
010B	SET Block Compose	Compose SET Block	CSNDSBC
010C	SET Block Decompose	Decompose SET Block	CSNDSBD

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
010D	Symmetric Key Generate – DES, PKA92	PKA96 Symmetric Key Generate	CSNDSYG
011E	PKA Encrypt	PKA Encipher Clear Key	CSNDPKE
011F	PKA Decrypt	PKA Decipher Key Data	CSNDPKD
0121	SET Block Decompose - PIN ext IPINENC	SET PIN Encrypt with IPINENC	CSNDSBD
0122	SET Block Decompose - PIN ext OPINENC	SET PIN Encrypt with OPINENC	CSNDSBD
0124	AES Master Key - Clear new master key register	Clear AES NMK Register (CLEAR)	CSNBMKP
0125	AES Master Key - Load first key part	Load First AES Master Key Part	CSNBMKP
0126	AES Master Key - Combine key parts	Combine Intermediate AES Master Key Parts	CSNBMKP
0128	AES Master Key - Set master key	Activate New AES Master Key (SET)	CSNBMKP
0129	Multiple Clear Key Import/Multiple Secure Key Import - AES	Encipher Under AES Master Key	CSNBCKM
012A	Symmetric Algorithm Encipher - Secure AES keys	Encipher Data Using AES	CSNBSAE
012B	Symmetric Algorithm Decipher - Secure AES keys	Decipher Data Using AES	CSNBSAD
012C	Symmetric Key Generate – AES, PKCSOAEP, PKCS-1.2	Generate AES DATA Key (PKCSOAEP or PKCS-1.2)	CSNDSYG
012D	Symmetric Key Generate – AES, ZERO-PAD	Generate AES DATA Key (ZERO-PAD)	CSNDSYG
012E	Symmetric Key Import – AES, PKCSOAEP, PKCS-1.2	Import AES Key (PKCSOAEP or PKCS-1.2)	CSNDSYI
012F	Symmetric Key Import – AES, ZERO-PAD	Import AES Key (ZERO-PAD)	CSNDSYI
0130	Symmetric Key Export – AES, PKCSOAEP, PKCS-1.2	Export AES Key (PKCSOAEP or PKCS-1.2)	CSNDSYX CSNDSXD
0131	Symmetric Key Export – AES, ZERO-PAD	Export AES Key (ZERO-PAD)	CSNDSYX
0139	Symmetric token wrapping - internal original method	N/A	
013A	Symmetric token wrapping - internal enhanced method	N/A	
013B	Symmetric token wrapping - external original method	N/A	
013C	Symmetric token wrapping - external enhanced method	N/A	
013D	Diversified Key Generate – Allow wrapping override keywords	Allow Configuration Override with Keyword in DKG	CSNBDKG

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
013E	Symmetric Key Generate – Allow wrapping override keywords	Allow Configuration Override with Keyword in SYG	CSNDSYG
013F	Remote Key Export - include RKX in default wrap config	Include RKX in Default Key-Wrapping Configuration	CSNDRKX
0140	Key Part Import - Allow wrapping override keywords	Allow Configuration Override with Keyword in KPI	CSNBKPI
0141	Multiple Clear Key Import – Allow wrapping override keywords	Allow Configuration Override with Keyword in CKM	CSNBCKM
0142	Multiple Secure Key Import - Allow wrapping override keywords	N/A	
0144	Symmetric Key Import – Allow wrapping override keywords	Allow Configuration Override with Keyword in SYI	CSNDSYI
0146	CKDS Conversion2 - Allow wrapping override keywords	Allow Configuration Override with Keyword in KTC	CSNBKTC
0147	CKDS Conversion2 - Convert from enhanced to original	Enable Translation from New to Old Format in KTC and KTR2	CSNBKTC CSNBKTR2
0148	PCF CKDS Conversion - Allow wrapping override keywords	N/A	
0149	Key Translate2	Translate Key2	CSNBKTR2
014A	Key Translate2 - Allow wrapping override keywords	Allow Configuration Override with Keyword in KTR2	CSNBKTR2
014B	Key Translate2 - Allow use of REFORMAT	Translate Key2 (REFORMAT)	CSNBKTR2
014C	CKDS Conversion2 - Allow use of REFORMAT	Key Token Change (REFORMAT)	CSNBKTC
014D	TR31 Export – Permit version A TR-31 key blocks T31X Permit Version A TR-31 Key Blocks (5.4/6.2 and later)	TR31 Export - Permit Version A TR-31 Key Blocks T31X Permit Version A TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31X
014E	TR31 Export – Permit version B TR-31 key blocks T31X Permit Version B TR-31 Key Blocks (5.4/6.2 and later)	TR31 Export - Permit Version B TR-31 Key Blocks T31X Permit Version B TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31X
014F	TR31 Export – Permit version C TR-31 key blocks T31X Permit Version C TR-31 Key Blocks (5.4/6.2 and later)	TR31 Export - Permit Version C TR-31 Key Blocks T31X Permit Version C TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31X
0150	TR31 Import – Permit version A TR-31 key blocks T31I Permit Version A TR-31 Key Blocks (5.4/6.2 and later)	TR31 Import - Permit Version A TR-31 Key Blocks T31I Permit Version A TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31I
0151	TR31 Import – Permit version B TR-31 key blocks T31I Permit Version B TR-31 Key Blocks (5.4/6.2 and later)	TR31 Import - Permit Version B TR-31 Key Blocks T31I Permit Version B TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0152	TR31 Import – Permit version C TR-31 key blocks T31I Permit Version C TR-31 Key Blocks (5.4/6.2 and later)	TR31 Import - Permit Version C TR-31 Key Blocks T31I Permit Version C TR-31 Key Blocks (5.4/6.2 and later)	CSNBT31I
0153	TR31 Import – Permit override of default wrapping method T31I Permit Override of Default Wrapping Method (5.4/6.2 and later)	TR31 Import - Permit Override of Default Wrapping Method T31I Permit Override of Default Wrapping Method (5.4/6.2 and later)	CSNBT31I
0154	Restrict Key Attribute – Permit setting the TR-31 export bit	Restrict Key Attribute - Permit Setting the TR-31 Export Bit	CSNBRKA
0155	CVV Key Combine	CVV Key Combine	CSNBCKC
0156	CVV Key Combine – Allow wrapping override keywords	CVV Key Combine - Allow Wrapping Override Keywords	CSNBCKC
0157	CVV Key Combine - Permit mixed key types	CVV Key Combine - Permit Mixed Key Types	CSNBCKC
0158	TR31 Export – Permit any CCA key if INCL-CV is specified T31X Permit Any CCA DES Key if INCL-CV Is Specified (5.4/6.2 and later)	TR31 Export - Permit Any CCA Key if INCL-CV Is Specified T31X Permit Any CCA DES Key if INCL-CV Is Specified (5.4/6.2 and later)	CSNBT31X
015A	TR31 Import – Permit C0 to MAC/MACVER:CVVKEY-A T31I - Permit C0:G/C/V to DES MAC/MACVER:CVVKEY-A (5.4/6.2 and later)	TR31 Import - Permit C0 to MAC/MACVER:CVVKEY-A T31I Permit C0:G/C/V to TDES MAC/MACVER: CVVKEY-A (5.4/6.2 and later)	CSNBT31I
015B	TR31 Import – Permit C0 to MAC/MACVER:AMEX-CSC T31I - C0:G/C/V to DES MAC/MACVER:AMEX-CSC (5.4/6.2 and later)	TR31 Import - Permit C0 to MAC/MACVER:AMEX-CSC T31I Permit C0:G/C/V to DES/TDES MAC/MACVER: AMEX-CSC (5.4/6.2 and later)	CSNBT31I
015C	TR31 Import – Permit K0:E to EXPORTER/OKEYXLAT T31I - K0:E to DES EXPORTER/OKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K0:E to EXPORTER/OKEYXLAT T31I Permit K0:E to TDES EXPORTER/OKEYXLAT (5.4/6.2 and later)	CSNBT31I
015D	TR31 Import – Permit K0:D to EXPORTER/OKEYXLAT T31I - K0:D to DES IMPORTER/IKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K0:D to IMPORTER/IKEYXLAT T31I Permit K0:D to TDES IMPORTER/IKEYXLAT (5.4/6.2 and later)	CSNBT31I
015E	TR31 Import – Permit K0:B to IMPORTER/IKEYXLAT T31I - K0:B to DES EXPORTER/OKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K0:B to EXPORTER/OKEYXLAT T31I Permit K0:B to TDES EXPORTER/OKEYXLAT (5.4/6.2 and later)	CSNBT31I
015F	TR31 Import – Permit K0:B to IMPORTER/IKEYXLAT T31I - K0:B to DES IMPORTER/IKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K0:B to IMPORTER/IKEYXLAT T31I Permit K0:B to TDES IMPORTER/IKEYXLAT (5.4/6.2 and later)	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0160	TR31 Import – Permit K1:E to EXPORTER/OKEYXLAT T31I - Permit K1/K4:E to DES EXPORTER/OKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K1:E to EXPORTER/OKEYXLAT T31I Permit K1/K4:E to TDES EXPORTER/OKEYXLAT (5.4/6.2 and later)	CSNBT31I
0161	TR31 Import – Permit K1:D to IMPORTER/IKEYXLAT T31I - Permit K1/K4:D to DES IMPORTER/IKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K1:D to IMPORTER/IKEYXLAT T31I Permit K1/K4:D to TDES IMPORTER/IKEYXLAT (5.4/6.2 and later)	CSNBT31I
0162	TR31 Import – Permit K1:B to EXPORTER/OKEYXLAT T31I - Permit K1/K4:B to DES EXPORTER/OKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K1:B to EXPORTER/OKEYXLAT T31I Permit K1/K4:B to TDES EXPORTER/OKEYXLAT (5.4/6.2 and later)	CSNBT31I
0163	TR31 Import – Permit K1:B to IMPORTER/IKEYXLAT T31I - Permit K1/K4:B to DES IMPORTER/IKEYXLAT (5.4/6.2 and later)	TR31 Import - Permit K1:B to IMPORTER/IKEYXLAT T31I Permit K1/K4:B to TDES IMPORTER/IKEYXLAT (5.4/6.2 and later)	CSNBT31I
0164	TR31 Import – Permit M0/M1/M3 to MAC/MACVER:ANY-MAC T31I - Permit M0/M1/M3:G/C/V to DES MAC/MACVER:ANY-MAC (5.4/6.2 and later)	TR31 Import - Permit M0/M1/M3 to MAC/MACVER:ANY-MAC T31I Permit M0/M1/M3:G/C/V to DES/TDES MAC/MACVER: ANY-MAC (5.4/6.2 and later)	CSNBT31I
0165	TR31 Import – Permit P0:E to OPINENC T31I - Permit P0:E to DES OPINENC (5.4/6.2 and later)	TR31 Import - Permit P0:E to OPINENC T31I Permit P0:E to TDES OPINENC (5.4/6.2 and later)	CSNBT31I
0166	TR31 Import – Permit P0:D to IPINENC T31I - Permit P0:D to DES IPINENC (5.4/6.2 and later)	TR31 Import - Permit P0:D to IPINENC T31I Permit P0:D to TDES IPINENC (5.4/6.2 and later)	CSNBT31I
0167	TR31 Import – Permit V0 to PINGEN:NO-SPEC T31I - Permit V0:N/G/C to DES PINGEN:NO-SPEC NOOFFSET (5.4/6.2 and later)	TR31 Import - Permit V0 to PINGEN:NO-SPEC T31I Permit V0:N/G/C to TDES PINGEN: NO-SPEC+optional NOOFFSET (5.4/6.2 and later)	CSNBT31I
0168	TR31 Import – Permit V0 to PINVER:NO-SPEC T31I - Permit V0:N/V to DES PINVER:NO-SPEC NOOFFSET (5.4/6.2 and later)	TR31 Import - Permit V0 to PINVER:NO-SPEC T31I Permit V0:N/V to TDES PINVER: NO-SPEC+optional NOOFFSET (5.4/6.2 and later)	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0169	TR31 Import – Permit V1 to PINGEN:IBM-PIN/IBM-PINO T31I - Permit V1:N/G/C to DES PINGEN:IBM-PIN/IBM-PINO NOOFFSET (5.4/6.2 and later)	TR31 Import - Permit V1 to PINGEN:IBM-PIN/IBM-PINO T31I Permit V1:N/G/C to TDES PINGEN: IBM-PIN/IBM-PINO+optional NOOFFSET (5.4/6.2 and later)	CSNBT31I
016A	TR31 Import – Permit V1 to PINVER:IBM-PIN/IBM-PINO T31I - Permit V1:N/V to DES PINVER:IBM-PIN/IBM-PINO NOOFFSET (5.4/6.2 and later)	TR31 Import - Permit V1 to PINVER:IBM-PIN/IBMPINO T31I Permit V1:N/V to TDES PINVER: IBM-PIN/IBM-PINO+optional NOOFFSET (5.4/6.2 and later)	CSNBT31I
016B	TR31 Import – Permit V2 to PINGEN:VISA-PVV T31I - Permit V2:N/G/C to DES PINGEN:VISA-PVV (5.4/6.2 and later)	TR31 Import - Permit V2 to PINGEN:VISA-PVV T31I Permit V2:N/G/C to TDES PINGEN: VISA-PVV (5.4/6.2 and later)	CSNBT31I
016C	TR31 Import – Permit V2 to PINVER:VISA-PVV T31I - Permit V2:N/V to DES PINVER:VISA-PVV (5.4/6.2 and later)	TR31 Import - Permit V2 to PINVER:VISA-PVV T31I Permit V2:N/V to TDES PINVER: VISA-PVV (5.4/6.2 and later)	CSNBT31I
016D	TR31 Import – Permit E0 to DKYGENKY:DKYL0+DMAC T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMAC (5.4/6.2 and later)	TR31 Import - Permit E0 to DKYGENKY:DKYL0+DMAC T31I Permit E0:N/X to TDES DKYGENKY: DKYL0+DMAC (5.4/6.2 and later)	CSNBT31I
016E	TR31 Import – Permit E0 to DKYGENKY:DKYL0+DMV T31I - Permit E0:N/X to DES DKYGENKY:DKYL0+DMV (5.4/6.2 and later)	TR31 Import - Permit E0 to DKYGENKY:DKYL0+DMV T31I Permit E0:N/X to TDES DKYGENKY: DKYL0+DMV (5.4/6.2 and later)	CSNBT31I
016F	TR31 Import – Permit E0 to DKYGENKY:DKYL1+DMAC T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMAC (5.4/6.2 and later)	TR31 Import - Permit E0 to DKYGENKY:DKYL1+DMAC T31I Permit E0:N/X to TDES DKYGENKY: DKYL1+DMAC (5.4/6.2 and later)	CSNBT31I
0170	TR31 Import – Permit E0 to DKYGENKY:DKYL1+DMV T31I - Permit E0:N/X to DES DKYGENKY:DKYL1+DMV (5.4/6.2 and later)	TR31 Import - Permit E0 to DKYGENKY:DKYL1+DMV T31I Permit E0:N/X to TDES DKYGENKY: DKYL1+DMV (5.4/6.2 and later)	CSNBT31I
0171	TR31 Import – Permit E1 to DKYGENKY:DKYL0+DMPIN T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DMPIN (5.4/6.2 and later)	TR31 Import - Permit E1 to DKYGENKY:DKYL0+DMPIN T31I Permit E1:N/E/D/B/X to TDES DKYGENKY: DKYL0+DMPIN (5.4/6.2 and later)	CSNBT31I
0172	TR31 Import – Permit E1 to DKYGENKY:DKYL0+DDATA T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL0+DDATA (5.4/6.2 and later)	TR31 Import - Permit E1 to DKYGENKY:DKYL0+DDATA T31I Permit E1:N/E/D/B/X to TDES DKYGENKY: DKYL0+DDATA (5.4/6.2 and later)	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0173	TR31 Import – Permit E1 to DKYGENKY:DKYL1+DMPIN T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DMPIN (5.4/6.2 and later)	TR31 Import - Permit E1 to DKYGENKY:DKYL1+DMPIN T31I Permit E1:N/E/D/B/X to TDES DKYGENKY: DKYL1+DMPIN (5.4/6.2 and later)	CSNBT31I
0174	TR31 Import – Permit E1 to DKYGENKY:DKYL1+DDATA T31I - Permit E1:N/E/D/B/X to DES DKYGENKY:DKYL1+DDATA (5.4/6.2 and later)	TR31 Import - Permit E1 to DKYGENKY:DKYL1+DDATA T31I Permit E1:N/E/D/B/X to TDES DKYGENKY: DKYL1+DDATA (5.4/6.2 and later)	CSNBT31I
0175	TR31 Import – Permit E2 to DKYGENKY:DKYL0+DMAC T31I - Permit E2:N/X to DES DKYGENKY:DKYL0+DMAC (5.4/6.2 and later)	TR31 Import - Permit E2 to DKYGENKY:DKYL0+DMAC T31I Permit E2:N/X to TDES DKYGENKY: DKYL0+DMAC (5.4/6.2 and later)	CSNBT31I
0176	TR31 Import – Permit E2 to DKYGENKY:DKYL1+DMAC T31I - Permit E2:N/X to DES DKYGENKY:DKYL1+DMAC (5.4/6.2 and later)	TR31 Import - Permit E2 to DKYGENKY:DKYL1+DMAC T31I Permit E2:N/X to TDES DKYGENKY: DKYL1+DMAC (5.4/6.2 and later)	CSNBT31I
0177	TR31 Import – Permit E3 to ENCIPHER T31I - Permit E3:N/E/D/B/G/X to DES ENCIPHER (5.4/6.2 and later)	TR31 Import - Permit E3 to ENCIPHER T31I Permit E3:N/E/D/B/G/X to TDES ENCIPHER (5.4/6.2 and later)	CSNBT31I
0178	TR31 Import – Permit E4 to DKYGENKY:DKYL0+DDATA T31I - Permit E4:N/B/X to DES DKYGENKY:DKYL0+DDATA (5.4/6.2 and later)	TR31 Import - Permit E4 to DKYGENKY:DKYL0+DDATA T31I Permit E4:N/B/X to TDES DKYGENKY: DKYL0+DDATA (5.4/6.2 and later)	CSNBT31I
0179	TR31 Import – Permit E5 to DKYGENKY:DKYL0+DMAC T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DMAC (5.4/6.2 and later)	TR31 Import - Permit E5 to DKYGENKY:DKYL0+DMAC T31I Permit E5:N/G/C/V/E/D/G/X to TDES DKYGENKY: DKYL0+DMAC (5.4/6.2 and later)	CSNBT31I
017A	TR31 Import – Permit E5 to DKYGENKY:DKYL0+DDATA T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DDATA (5.4/6.2 and later)	TR31 Import - Permit E5 to DKYGENKY:DKYL0+DDATA T31I Permit E5:N/G/C/V/E/D/G/X to TDES DKYGENKY: DKYL0+DDATA (5.4/6.2 and later)	CSNBT31I
017B	TR31 Import – Permit E5 to DKYGENKY:DKYL0+DEXP T31I - Permit E5:N/G/C/V/E/D/G/X to DES DKYGENKY:DKYL0+DEXP (5.4/6.2 and later)	TR31 Import - Permit E5 to DKYGENKY:DKYL0+DEXP T31I Permit E5:N/G/C/V/E/D/G/X to TDES DKYGENKY: DKYL0+DEXP (5.4/6.2 and later)	CSNBT31I
017C	TR31 Import – Permit V0/V1/V2:N to PINGEN/PINVER T31I - Permit V0/V1/V2:N to DES PINGEN/PINVER (5.4/6.2 and later)	TR31 Import - Permit V0/V1/V2:N to PINGEN/PINVER T31I Permit V0/V1/V2:N to TDES PINGEN/PINVER (5.4/6.2 and later)	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0180	TR31 Export – Permit KEYGENKY:DUKPT to B0 T31X - Permit DES KEYGENKY: DUKPT to B0:N/X (5.4/6.2 and later)	TR31 Export - Permit KEYGENKY:DUKPT to B0 T31X Permit TDES KEYGENKY: DUKPT to B0:N/X (5.4/6.2 and later)	CSNBT31X
0181	TR31 Export – Permit MAC/MACVER:AMEXCSC to C0:G/C/V T31X - Permit DES MAC/MACVER:AMEX-CSC to C0:G/C/V (5.4/6.2 and later)	TR31 Export - Permit MAC/MACVER:AMEX-CSC to C0:G/C/V T31X Permit DES/TDES MAC/MACVER: AMEX-CSC to C0:G/C/V (5.4/6.2 and later)	CSNBT31X
0182	TR31 Export – Permit MAC/MACVER:CVVKEYA to C0:G/C/V T31X - Permit DES MAC/MACVER: CVV-KEYA to C0:G/C/V (5.4/6.2 and later)	TR31 Export - Permit MAC/MACVER:CVV-KEYA to C0:G/C/V T31X Permit TDES MAC/MACVER: CVV-KEYA to C0:G/C/V (5.4/6.2 and later)	CSNBT31X
0183	TR31 Export – Permit MAC/MACVER:ANYMAC to C0:G/C/V T31X - Permit DES MAC/MACVER: ANY-MAC to C0:G/C/V (5.4/6.2 and later)	TR31 Export - Permit MAC/MACVER:ANY-MAC to C0:G/C/V T31X Permit TDES MAC/MACVER: ANY-MAC to C0:G/C/V (5.4/6.2 and later)	CSNBT31X
0184	TR31 Export – Permit DATA to C0:G/C T31X - Permit DES DATA/DATAM/DATAMV to C0:G/C/V (5.4/6.2 and later)	TR31 Export - Permit DATA to C0:G/C T31X Permit TDES DATA/DATAM/DATAMV to C0:G/C/V (5.4/6.2 and later)	CSNBT31X
0185	TR31 Export – Permit ENCIPHER/DECIPHER/CIPHER to D0:E/D/B T31X - Permit DES ENCIPHER/DECIPHER/CIPHER to D0:E/D/B (5.4/6.2 and later)	TR31 Export - Permit ENCIPHER/DECIPHER/CIPHER to D0:E/D/B T31X Permit DES/TDES ENCIPHER/DECIPHER/CIPHER to D0:E/D/B (5.4/6.2 and later)	CSNBT31X
0186	TR31 Export – Permit DATA to D0:B T31X - Permit DES DATA to D0:E/D/B (5.4/6.2 and later)	TR31 Export - Permit DATA to D0:B T31X Permit DES/TDES DATA/DATAC to D0:E/D/B (5.4/6.2 and later)	CSNBT31X
0187	TR31 Export – Permit EXPORTER/OKEYXLAT to K0:E T31X - Permit DES EXPORTER/OKEYXLAT to K0:E (5.4/6.2 and later)	TR31 Export - Permit EXPORTER/OKEYXLAT to K0:E T31X Permit TDES EXPORTER/OKEYXLAT to K0:E (5.4/6.2 and later)	CSNBT31X
0188	TR31 Export – Permit IMPORTER/IKEYXLAT to K0:D T31X - Permit DES IMPORTER/IKEYXLAT to K0:D (5.4/6.2 and later)	TR31 Export - Permit IMPORTER/IKEYXLAT to K0:D T31X Permit TDES IMPORTER/IKEYXLAT to K0:D (5.4/6.2 and later)	CSNBT31X

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0189	TR31 Export – Permit EXPORTER/OKEYXLAT to K1:E T31X - Permit DES EXPORTER/OKEYXLAT to K1/K4:E (5.4/6.2 and later)	TR31 Export - Permit EXPORTER/OKEYXLAT to K1:E T31X Permit TDES EXPORTER/OKEYXLAT to K1/K4:E (5.4/6.2 and later)	CSNBT31X
018A	TR31 Export – Permit IMPORTER/IKEYXLAT to K1:D T31X - Permit DES IMPORTER/IKEYXLAT to K1/K4:D (5.4/6.2 and later)	TR31 Export - Permit IMPORTER/IKEYXLAT to K1:D T31X Permit TDES IMPORTER/IKEYXLAT to K1/K4:D (5.4/6.2 and later)	CSNBT31X
018B	TR31 Export – Permit MAC/DATA/DATAM to M0:G/C T31X - Permit DES MAC/DATA/DATAM to M0:G/C (5.4/6.2 and later)	TR31 Export - Permit MAC/DATA/DATAM to M0:G/C T31X Permit TDES MAC/DATA/DATAM to M0:G/C (5.4/6.2)	CSNBT31X
018C	TR31 Export – Permit MACVER/DATAMV to M0:V T31X - Permit DES MACVER/DATA/DATAMV to M0:V (5.4/6.2 and later)	TR31 Export - Permit MACVER/DATAMV to M0:V T31X Permit TDES MACVER/DATA/DATAMV to M0:V (5.4/6.2 and later)	CSNBT31X
018D	TR31 Export – Permit MAC/DATA/DATAM to M1:G/C T31X - Permit DES MAC/DATA/DATAM to M1:G/C (5.4/6.2 and later)	TR31 Export - Permit MAC/DATA/DATAM to M1:G/C T31X Permit DES/TDES MAC/DATA/DATAM to M1:G/C (5.4/6.2 and later)	CSNBT31X
018E	TR31 Export – Permit MACVER/DATAMV to M1:V T31X - Permit DES MACVER/DATA/DATAMV to M1:V (5.4/6.2 and later)	TR31 Export - Permit MACVER/DATAMV to M1:V T31X Permit DES/TDES MACVER/DATA/DATAMV to M1:V (5.4/6.2 and later)	CSNBT31X
018F	TR31 Export – Permit MAC/DATA/DATAM to M3:G/C T31X - Permit DES MAC/DATA/DATAM to M3:G/C (5.4/6.2 and later)	TR31 Export - Permit MAC/DATA/DATAM to M3:G/C T31X Permit DES/TDES MAC/DATA/DATAM to M3:G/C (5.4/6.2 and later)	CSNBT31X
0190	TR31 Export – Permit MACVER/DATAMV to M3:V T31X - Permit DES MACVER/DATA/DATAMV to M3:V (5.4/6.2 and later)	TR31 Export - Permit MACVER/DATAMV to M3:V T31X Permit DES/TDES MACVER/DATA/DATAMV to M3:V (5.4/6.2 and later)	CSNBT31X
0191	TR31 Export – Permit OPINENC to P0/E T31X - Permit DES OPINENC to P0:E (5.4/6.2 and later)	TR31 Export - Permit OPINENC to P0:E T31X Permit TDES OPINENC to P0:E (5.4/6.2 and later)	CSNBT31X
0192	TR31 Export – Permit IPINENC to P0/D T31X - Permit DES IPINENC to P0:D (5.4/6.2 and later)	TR31 Export - Permit IPINENC to P0:D T31X Permit TDES IPINENC to P0:D (5.4/6.2 and later)	CSNBT31X
0193	TR31 Export – Permit PINVER:NO-SPEC to V0 T31X - Permit DES PINVER: NO-SPEC to V0:N/V (5.4/6.2 and later)	TR31 Export - Permit PINVER:NO-SPEC to V0 T31X Permit DES/TDES PINVER: NO-SPEC to V0:N/V (5.4/6.2 and later)	CSNBT31X

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0194	TR31 Export – Permit PINGEN:NO-SPEC to V0 T31X - Permit DES PINGEN: NO-SPEC to V0:N/C (5.4/6.2 and later)	TR31 Export - Permit PINGEN:NO-SPEC to V0 T31X Permit DES/TDES PINGEN: NO-SPEC to V0:N/C (5.4/6.2 and later)	CSNBT31X
0195	TR31 Export – Permit PINVER:NO-SPEC/IBM-PIN/IBMPINO to V1 T31X - Permit DES PINVER: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V (5.4/6.2 and later)	TR31 Export - Permit PINVER:NO-SPEC/IBM-PIN/IBM-PINO to V1 T31X Permit DES/TDES PINVER: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V (5.4/6.2 and later)	CSNBT31X
0196	TR31 Export – Permit PINGEN:NO-SPEC/IBM-PIN/IBM-PINO to V1 T31X - Permit DES PINGEN: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V (5.4/6.2 and later)	TR31 Export - Permit PINGEN:NO-SPEC/IBM-PIN/IBM-PINO to V1 T31X Permit DES/TDES PINGEN: NO-SPEC/IBM-PIN/IBM-PINO to V1:N/V (5.4/6.2 and later)	CSNBT31X
0197	TR31 Export – Permit PINVER:NO-SPEC/VISA-PVV to V2 T31X - Permit DES PINVER: NO-SPEC/VISA-PVV to V2:N/V (5.4/6.2 and later)	TR31 Export - Permit PINVER:NO-SPEC/VISA-PVV to V2 T31X Permit DES/TDES PINVER: NO-SPEC/VISA-PVV to V2:N/V (5.4/6.2 and later)	CSNBT31X
0198	TR31 Export – Permit PINGEN:NO-SPEC/VISA-PVV to V2 T31X - Permit DES PINGEN: NO-SPEC/VISA-PVV to V2:N/C (5.4/6.2 and later)	TR31 Export - Permit PINGEN:NO-SPEC/VISAPVV to V2 T31X Permit DES/TDES PINGEN: NO-SPEC/VISA-PVV to V2:N/C (5.4/6.2 and later)	CSNBT31X
0199	TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E0 T31X - Permit DES DKYGENKY: DKYL0+DMAC to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DMAC to E0 T31X Permit TDES DKYGENKY: DKYL0+DMAC to E0:N/X (5.4/6.2 and later)	CSNBT31X
019A	TR31 Export – Permit DKYGENKY:DKYL0+DMV to E0 T31X - Permit DES DKYGENKY: DKYL0+DMV to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DMV to E0 T31X Permit TDES DKYGENKY: DKYL0+DMV to E0:N/X (5.4/6.2 and later)	CSNBT31X
019B	TR31 Export – Permit DKYGENKY:DKYL0+DALL to E0 T31X - Permit DES DKYGENKY: DKYL0+DALL to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DALL to E0 T31X Permit TDES DKYGENKY: DKYL0+DALL to E0:N/X (5.4/6.2 and later)	CSNBT31X
019C	TR31 Export – Permit DKYGENKY:DKYL1+DMAC to E0 T31X - Permit DES DKYGENKY: DKYL1+DMAC to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DMAC to E0 T31X Permit TDES DKYGENKY: DKYL1+DMAC to E0:N/X (5.4/6.2 and later)	CSNBT31X
019D	TR31 Export – Permit DKYGENKY:DKYL1+DMV to E0 T31X - Permit DES DKYGENKY: DKYL1+DMV to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DMV to E0 T31X Permit TDES DKYGENKY: DKYL1+DMV to E0:N/X (5.4/6.2 and later)	CSNBT31X

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
019E	TR31 Export – Permit DKYGENKY:DKYL1+DALL to E0 T31X - Permit DES DKYGENKY: DKYL1+DALL to E0:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DALL to E0 T31X Permit TDES DKYGENKY: DKYL1+DALL to E0:N/X (5.4/6.2 and later)	CSNBT31X
019F	TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E1 T31X - Permit DES DKYGENKY: DKYL0+DDATA to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DDATA to E1 T31X Permit TDES DKYGENKY: DKYL0+DDATA to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A0	TR31 Export – Permit DKYGENKY:DKYL0+DMPIN to E1 T31X - Permit DES DKYGENKY: DKYL0+DMPIN to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DMPIN to E1 T31X Permit TDES DKYGENKY: DKYL0+DMPIN to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A1	TR31 Export – Permit DKYGENKY:DKYL0+DALL to E1 T31X - Permit DES DKYGENKY: DKYL0+DALL to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DALL to E1 T31X Permit TDES DKYGENKY: DKYL0+DALL to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A2	TR31 Export – Permit DKYGENKY:DKYL1+DDATA to E1 T31X - Permit DES DKYGENKY: DKYL1+DDATA to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DDATA to E1 T31X Permit TDES DKYGENKY: DKYL1+DDATA to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A3	TR31 Export – Permit DKYGENKY:DKYL1+DMPIN to E1 T31X - Permit DES DKYGENKY: DKYL1+DMPIN to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DMPIN to E1 T31X Permit TDES DKYGENKY: DKYL1+DMPIN to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A4	TR31 Export – Permit DKYGENKY:DKYL1+DALL to E1 T31X - Permit DES DKYGENKY: DKYL1+DALL to E1:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DALL to E1 T31X Permit TDES DKYGENKY: DKYL1+DALL to E1:N/X (5.4/6.2 and later)	CSNBT31X
01A5	TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E2 T31X - Permit DES DKYGENKY: DKYL0+DMAC to E2:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DMAC to E2 T31X Permit TDES DKYGENKY: DKYL0+DMAC to E2:N/X (5.4/6.2 and later)	CSNBT31X
01A6	TR31 Export – Permit DKYGENKY:DKYL0+DALL to E2 T31X - Permit DES DKYGENKY: DKYL0+DALL to E2:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DALL to E2 T31X Permit TDES DKYGENKY: DKYL0+DALL to E2:N/X (5.4/6.2 and later)	CSNBT31X
01A7	TR31 Export – Permit DKYGENKY:DKYL1+DMAC to E2 T31X - Permit DES DKYGENKY: DKYL1+DMAC to E2:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DMAC to E2 T31X Permit TDES DKYGENKY: DKYL1+DMAC to E2:N/X (5.4/6.2 and later)	CSNBT31X

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
01A8	TR31 Export – Permit DKYGENKY:DKYL1+DALL to E2 T31X - Permit DES DKYGENKY: DKYL1+DALL to E2:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL1+DALL to E2 T31X Permit TDES DKYGENKY: DKYL1+DALL to E2:N/X (5.4/6.2 and later)	CSNBT31X
01A9	TR31 Export – Permit DATA/MAC/CIPHER/ENCIPHER to E3 T31X - Permit DES DATA/DATAM/CIPHER/MAC/ENCIPHER to E3:N/G/E/X (5.4/6.2 and later)	TR31 Export - Permit DATA/MAC/CIPHER/ENCIPHER to E3 T31X Permit TDES DATA/DATAC/DATAM/CIPHER/MAC/ENCIPHER to E3:N/G/E/X (5.4/6.2 and later)	CSNBT31X
01AA	TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E4 T31X - Permit DES DKYGENKY: DKYL0+DDATA to E4:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DDATA to E4 T31X Permit TDES DKYGENKY: DKYL0+DDATA to E4:N/X (5.4/6.2 and later)	CSNBT31X
01AB	TR31 Export – Permit DKYGENKY:DKYL0+DALL to E4 T31X - Permit DES DKYGENKY: DKYL0+DALL to E4:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DALL to E4 T31X Permit TDES DKYGENKY: DKYL0+DALL to E4:N/X (5.4/6.2 and later)	CSNBT31X
01AC	TR31 Export – Permit DKYGENKY:DKYL0+DEXP to E5 T31X - Permit DES DKYGENKY: DKYL0+DEXP to E5:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DEXP to E5 T31X Permit TDES DKYGENKY: DKYL0+DEXP to E5:N/X (5.4/6.2 and later)	CSNBT31X
01AD	TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E5 T31X - Permit DES DKYGENKY: DKYL0+DMAC to E5:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DMAC to E5 T31X Permit TDES DKYGENKY: DKYL0+DMAC to E5:N/X (5.4/6.2 and later)	CSNBT31X
01AE	TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E5 T31X - Permit DES DKYGENKY: DKYL0+DDATA to E5:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DDATA to E5 T31X Permit TDES DKYGENKY: DKYL0+DDATA to E5:N/X (5.4/6.2 and later)	CSNBT31X
01AF	TR31 Export – Permit DKYGENKY:DKYL0+DALL to E5 T31X - Permit DES DKYGENKY:DKYL0+DALL to E5:N/X (5.4/6.2 and later)	TR31 Export - Permit DKYGENKY:DKYL0+DALL to E5 T31X Permit TDES DKYGENKY:DKYL0+DALL to E5:N/X (5.4/6.2 and later)	CSNBT31X
01B0	TR31 Export – Permit PINGEN/PINVER to V0/V1/V2:N T31X - Permit DES PINGEN to V0:N and DES PINVER to V1/V2:N (5.4/6.2 and later)	TR31 Export - Permit PINGEN/PINVER to V0/V1/V2:N T31X Permit TDES PINGEN to V0:N and DES PINVER to V1/V2:N (5.4/6.2 and later)	CSNBT31X
01C0	Cipher Text Translate2	Cipher Text Translate2	CSNBCTT2
01C1	Cipher Text Translate2 – Allow translate from AES to TDES	CTT2 from AES Key to Weaker DES Key	CSNBCTT2
01C2	Cipher Text Translate2 – Allow translate to weaker AES	CTT2 from AES Key to Weaker AES Key	CSNBCTT2

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
01C3	Cipher Text Translate2 – Allow translate to weaker DES	N/A	
01C4	Cipher Text Translate2 – Allow only cipher text translate types	Allow Only Cipher Text Translate Key Types	CSNBCTT2
01C5	Disallow translation from AES wrapping to DES wrapping	Disallow Translation from an AES KEK to DES KEK	CSNBKTR2 CSNBPTR2 CSNDPKT
01C6	Disallow translation from AES wrapping to weaker AES wrapping	Disallow Translation from an AES KEK to a Weaker AES KEK	CSNBKTR2 CSNBPTR2 CSNDPKT
01C7	Disallow translation from DES wrapping to weaker DES wrapping	Disallow Translation from a DES KEK to a Weaker DES KEK	CSNBAPG CSNBEPG CSNBKTR CSNBKTR2 CSNBPFO CSNBPTR CSNBPTRE CSNBPTR2 CSNBSKY CSNDPKT
01C8	Unique Key Derive	DUKPT Key Derive	CSNBUKD
01C9	Unique Key Derive – Allow PIN-DATA processing	DUKPT PIN-DATA	CSNBUKD
01CA	Unique Key Derive – Override default wrapping	Allow Configuration Override with Keyword in UKD	CSNBUKD
01CB	Key Test - Warn when keyword inconsistent with key length	N/A	CSNBKYT
01CD	Symmetric Algorithm Encipher - GCM/Counter mode AES	GCM Encipher Data with AES	CSNBSAE
01CE	Symmetric Algorithm Decipher - GCM/Counter mode AES	GCM Decipher Data with AES	CSNBSAD
01D0	T31X - Permit AES CIPHER to D0:E/D/B	T31X Permit AES CIPHER to D0:E/D/B	CSNBT31X
01D1	T31X - Permit AES MAC: CMAC to M6:G/C/V	T31X Permit AES MAC: CMAC to M6:G/C/V	CSNBT31X
01D2	T31X - Permit AES PINPROT to P0:E/D	T31X Permit AES PINPROT to P0:E/D	CSNBT31X
01D3	T31X - Permit AES EXPORTER to K0:E	T31X Permit AES EXPORTER to K0:E	CSNBT31X

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
01D4	T31X - Permit AES EXPORTER to K1:E	T31X Permit AES EXPORTER to K1:E	CSNBT31X
01D5	T31X - Permit AES EXPORTER to K4:E	T31X Permit AES EXPORTER to K4:E	CSNBT31X
01D6	T31X - Permit AES IMPORTER to K0:D	T31X Permit AES IMPORTER to K0:D	CSNBT31X
01D7	T31X - Permit AES IMPORTER to K1:D	T31X Permit AES IMPORTER to K1:D	CSNBT31X
01D8	T31X - Permit AES IMPORTER to K4:D	T31X Permit AES IMPORTER to K4:D	CSNBT31X
01D9	T31X - Permit AES DKYGENKY:D-ALL/DMAC to E0:X	T31X Permit AES DKYGENKY:D-ALL/DMAC to E0:X	CSNBT31X
01DA	T31X - Permit AES DKYGENKY:D-ALL/DCIPHER to E1:X	T31X Permit AES DKYGENKY:D-ALL/DCIPHER to E1:X	CSNBT31X
01DB	T31X - Permit AES DKYGENKY:D-ALL/D-MAC to E2:X	T31X Permit AES DKYGENKY:D-ALL/D-MAC to E2:X	CSNBT31X
01DC	T31X - Permit AES CIPHER to E3/E/B,DKYGENKY:D-ALL/DCIP to E3:X	T31X Permit AES CIPHER to E3/E/B and AES DKYGENKY: D-ALL/DCIPHER to E3:X	CSNBT31X
01DD	T31X - Permit AES DKYGENKY:D-ALL/D-CIPHER to E4:X	T31X Permit AES DKYGENKY:D-ALL/D-CIPHER to E4:X	CSNBT31X
01DE	T31X - Permit AES DKYGENKY:D-MAC to E5:X	T31X Permit AES DKYGENKY:D-MAC to E5:X	CSNBT31X
01DF	TR-34 Key Receive – Allow wrapping override keywords	CFG_OVERRIDE_KW_T34R	CSNDT34R
01E0	T31I - Permit D0:E/D/B to AES CIPHER:ENC/DEC/ENC+DEC	T31I Permit D0:E/D/B to AES CIPHER: ENCRYPT/DECRYPT/ENCRYPT+DECRYPT	CSNBT31I
01E1	T31I - Permit M6:G/C/V to AES MAC:CMAC+GENONLY/GEN/VER	T31I Permit M6:G/C/V to AES MAC: CMAC+GENONLY/GENERATE/VERIFY	CSNBT31I
01E2	T31I - Permit P0:E/D to AES PINPROT:ENC/DEC+CBC+ISO-4	T31I Permit P0:E/D to AES PINPROT: ENC/DEC+CBC+PINXLATE+REFORMAT+ISO-4	CSNBT31I
01E3	T31I - Permit K0:E to AES EXPORTER	T31I Permit K0:E to AES EXPORTER	CSNBT31I
01E4	T31I - Permit K0:D to AES IMPORTER	T31I Permit K0:D to AES IMPORTER	CSNBT31I
01E5	T31I - Permit K1/K4:E to AES EXPORTER:EXPTT31D+VARDRV-D	T31I Permit K1/K4:E to AES EXPORTER: EXPTT31D+VARDRV-D	CSNBT31I
01E6	T31I - Permit AES K1/K4:D to AES IMPORTER:IMPTT31D+VARDRV-D	T31I Permit AES K1/K4:D to AES IMPORTER: IMPTT31D+VARDRV-D	CSNBT31I
01E7	T31I - Permit E0:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	T31I Permit E0:X to AES DKYGENKY: DKYL0/L1/L2+D-MAC+GENERATE+CMAC	CSNBT31I

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
01E8	T31I - Permit E1:X to AES DKYGENKY:DKYL0/L1/L2+D-SECMSG+SMPIN	T31I Permit E1:X to AES DKYGENKY: DKYL0/L1/L2+D-SECMSG+SMPIN+ANY-USE	CSNBT31I
01E9	T31I - Permit E2:X to AES DKYGENKY:DKYL0/L1/L2+D-MAC+GEN+CMAC	T31I Permit E2:X to AES DKYGENKY: DKYL0/L1/L2+D-MAC+GENERATE+CMAC	CSNBT31I
01EA	T31I - Permit E3:X to AES DKYGENKY:D-CIPHER+ENC+DEC+CBC	T31I Permit E3:X to AES DKYGENKY: D-CIPHER+ENCRYPT+DECRYPT+CBC	CSNBT31I
01EB	T31I - Permit E3:E/B to AES CIPHER:ENCRYPT/ENC+DEC	T31I Permit E3:E/B to AES CIPHER: ENCRYPT/ENCRYPT+DECRYPT	CSNBT31I
01EC	T31I - Permit E4:X to AES DKYGENKY:DKYL0/L1/L2+D-CIPHER+ENC+DEC	T31I Permit E4:X to AES DKYGENKY: DKYL0/L1/L2+D-CIPHER+ENCRYPT+DECRYPT+CBC	CSNBT31I
01ED	T31I - Permit E5:X to AES DKYGENKY:DKYL0/L1/L2/D-MAC+GEN+CMAC	T31I Permit E5:X to AES DKYGENKY: DKYL0/L1/L2/D-MAC+GENERATE+CMAC	CSNBT31I
01EE	PKA Key Translate – allow COMP-TAG	CMD_PKT_ALLOW_COMPTAG	CSNDPKT
01EF	PKA Key Translate – allow COMP-CHK	CMD_PKT_ALLOW_COMPCHK	CSNDPKT
01F0	TR-34 Bind-Begin	CMP_T34B_ALLOW_VERB	CSNDT34B
01F1	TR-34 Bind-Begin - allow BINDCR	CMP_T34B_ALLOW_BINDCR	CSNDT34B
01F2	TR-34 Bind-Begin - allow UNBINDCR	CMP_T34B_ALLOW_UNBINDCR	CSNDT34B
01F3	TR-34 Bind-Begin - allow REBINDCR	CMP_T34B_ALLOW_REBINDCR	CSNDT34B
01F4	TR-34 Bind-Complete	CMP_T34C_ALLOW_VERB	CSNDT34C
01F5	TR-34 Bind-Complete - allow BINDKRDC	CMP_T34C_ALLOW_BINDKRDC	CSNDT34C
01F6	TR-34 Bind-Complete - allow BINDRV	CMP_T34C_ALLOW_BINDRV	CSNDT34C
01F7	TR-34 Bind-Complete - allow UNBINDRV	CMP_T34C_ALLOW_UNBINDRV	CSNDT34C
01F8	TR-34 Bind-Complete - allow REBINDRV	CMP_T34C_ALLOW_REBINDRV	CSNDT34C
01F9	TR-34 Key Distribution	CMP_T34D_ALLOW_VERB	CSNDT34D
01FA	TR-34 Key Distribution – Allow 2PASSCRE	CMP_T34D_ALLOW_2PASSCRE	CSNDT34D
01FB	TR-34 Key Distribution – Allow 1PASSCRE	CMP_T34D_ALLOW_1PASSCRE	CSNDT34D
01FC	TR-34 Key Receive	CMP_T34R_ALLOW_VERB	CSNDT34R

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
01FD	TR-34 Key Receive – Allow 2PASSRCV	CMP_T34R_ALLOW_2PASSRCV	CSNDT34R
01FE	TR-34 Key Receive – Allow 1PASSRCV	CMP_T34R_ALLOW_1PASSRCV	CSNDT34R
01FF	Permit X.509 without PKI root validation	CMD_IGNORE_PKI	CSNDT34B CSNDT34C CSNDT34D CSNDT34R
0203	Retained Key Delete	Delete Retained Key	CSNDKRD
0204	PKA Key Generate - Clone	PKA Clone Key	CSNDPKG
0205	PKA Key Generate – Clear RSA keys	PKA Clear Key Generate	CSNDPKG
0206	PKA Encrypt – Disallow PKCS-1.2	PKA Encipher Clear Key Disallow PKCS-1.2	CSNDPKE
0207	PKA Encrypt – Disallow ZEROPAD	PKA Encipher Clear Key Disallow ZEROPAD	CSNDPKE
0208	PKA Encrypt – Disallow MRP	PKA Encipher Clear Key Disallow MRP	CSNDPKE
0209	PKA Encrypt – Disallow PKCSOAEP	PKA Encipher Clear Key Disallow PKCSOAEP	CSNDPKE
020A	PKA Decrypt – Disallow PKCS-1.2	PKA Decipher Key Data Disallow PKCS-1.2	CSNDPKD
020B	PKA Decrypt – Disallow ZEROPAD	PKA Decipher Key Data Disallow ZEROPAD	CSNDPKD
020C	PKA Decrypt – Disallow PKCSOAEP	PKA Decipher Key Data Disallow PKCSOAEP	CSNDPKD
0230	Retained Key List	List Retained Key	CSNDRKL
0235	Symmetric Key Import – DES, PKA92 KEK	PKA96 Symmetric Key Import	CSNDSYI
023C	Symmetric Key Generate – DES, ZERO-PAD	ZERO-PAD Symmetric Key Generate	CSNDSYG
023D	Symmetric Key Import – DES, ZERO-PAD	ZERO-PAD Symmetric Key Import	CSNDSYI
023E	Symmetric Key Export – DES, ZERO-PAD	ZERO-PAD Symmetric Key Export	CSNDSYX
023F	Symmetric Key Generate – DES, PKCS-1.2	Symmetric Key Generate PKCS-1.2/OAEP	CSNDSYG
0240	Authorize UDX	N/A	
0241	Reencipher PKDS	N/A	
0242	TR-34 Key Distribution - Permit DES EXPORTER to K0 or K1	CMP_T34D_DES_EXP_KX	CSNDT34D

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0243	TR-34 Key Distribution - Permit DES IMPORTER to K0 or K1	CMP_T34D_DES_IMP_KX	CSNDT34D
0244	TR-34 Key Distribution - Permit AES EXPORTER to K0	CMP_T34D_AES_EXP_K0	CSNDT34D
0245	TR-34 Key Distribution - Permit AES EXPORTER to K1	CMP_T34D_AES_EXP_K1	CSNDT34D
0246	TR-34 Key Distribution - Permit AES IMPORTER to K0	CMP_T34D_AES_IMP_K0	CSNDT34D
0247	TR-34 Key Distribution - Permit AES IMPORTER to K1	CMP_T34D_AES_IMP_K1	CSNDT34D
0248	TR-34 Key Receive – Permit DES EXPORTER	CMP_T34R_DES_KX_EXP	CSNDT34R
0249	TR-34 Key Receive – Permit DES IMPORTER	CMP_T34R_DES_KX_IMP	CSNDT34R
024A	TR-34 Key Receive – Permit AES EXPORTER	CMP_T34R_AES_K0_EXP	CSNDT34R
024B	TR-34 Key Receive – Permit AES IMPORTER	CMP_T34R_AES_K0_IMP	CSNDT34R
024C	TR-34 Key Receive – Permit AES EXPORTER with EXPTT31D	CMP_T34R_AES_K1_EXP	CSNDT34R
024D	TR-34 Key Receive – Permit AES IMPORTER with IMPTT31D	CMP_T34R_AES_K1_IMP	CSNDT34R
0273	Secure Messaging for Keys	Secure Messaging for Keys	CSNBSKY
0274	Secure Messaging for PINs	Secure Messaging for PINs	CSNBSPN
0275	DATAM Key Management Control	N/A	
0276	Key Export - Unrestricted	Unrestrict Reencipher from Master Key	CSNBKEX
0277	Data Key Export - Unrestricted	Unrestrict Data Key Export	CSNBDKX
0278	Key Part Import - ADD-PART	Add Key Part	CSNBKPI
0279	Key Part Import - COMPLETE	Complete Key Part	CSNBKPI
027A	Key Part Import - Unrestricted	Unrestrict Combine Key	CSNBKPI
027B	Key Import - Unrestricted	Unrestrict Reencipher to Master Key	CSNBKIM
027C	Data Key Import - Unrestricted	Unrestrict Data Key Import	CSNBDKM
027D	PKA Key Generate – Permit Regeneration Data	Permit Regeneration Data	CSNDPKG
027E	PKA Key Generate – Permit Regeneration Data Retain	Permit Regeneration Data for Retained Keys	CSNDPKG

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0290	Diversified Key Generate - DKYGENKY - DALL	Generate Diversified Key (DALL with DKYGENKY Key Type)	CSNBDKG CSNBPCU
0291	Transaction Validation – Generate	Generate CSC 3, 4 and 5 Values	CSNBTRV
0292	Transaction Validation – Verify CSC-3	Verify CSC 3 Values	CSNBTRV
0293	Transaction Validation – Verify CSC-4	Verify CSC 4 Values	CSNBTRV
0294	Transaction Validation – Verify CSC-5	Verify CSC 5 Values	CSNBTRV
0295	Symmetric Key Encipher/Decipher - Encrypted DES keys	N/A	
0296	Symmetric Key Encipher/Decipher - Encrypted AES keys	N/A	
0297	Key Part Import2 – Load first key part, require 3 key parts	Import Minimum Three Parts	CSNBKPI2
0298	Key Part Import2 – Load first key part, require 2 key parts	Import Minimum Two Parts	CSNBKPI2
0299	Key Part Import2 - Load first key part, require 1 key parts	Import Minimum One Part	CSNBKPI2
029A	Key Part Import2 - Add second of 3 or more key parts	Import Second of Three or More Parts	CSNBKPI2
029B	Key Part Import2 - Add last required key part	Import Last Minimum Required Part	CSNBKPI2
029C	Key Part Import2 - Add optional key part	Import Optional Part	CSNBKPI2
029D	Key Part Import2 – Complete key	Complete Import of Key Parts	CSNBKPI2
029E	Operational Key Load - Variable-Length Tokens	N/A	
02B0	Recover PIN From Offset	Recover PIN from Offset	CSNBPFO
02B1	Authentication Parameter Generate	Allow Authentication Parameter	CSNBAPG
02B2	Authentication Parameter Generate - Clear	Allow Authentication Parameter Value in Clear	CSNBAPG
02B3	Symmetric Key Export - AESKWCV	Export DES Key (AESKWCV)	CSNDSYX
02B4	Symmetric Key Import2 - AESKWCV	Import DES Key (AESKWCV)	CSNDSYI2
02B5	Symmetric Key Export with Data	Symmetric Key Export with Data	CSNBSXD
02B6	Symmetric Key Export with Data - Special	SXD Special Export	CSNBSXD
02B8	Diversified Key Generate - TDES-CBC	Generate Diversified Key (TDES-CBC)	CSNBDKG2
02B9	Symmetric Key Import2 – Allow wrapping override keywords	Allow Configuration Override with Keyword in SYI2	CSNDSYI2

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
02BA	Remote Key Export – Allow wrapping override keywords	Allow Configuration Override with Keyword in RKX	CSNDRKX
02BB	Key Generate2 – DK PIN key set	Generate DK Key Set Extended for AES	CSNBKGN2
02BC	Key Generate2 – DK PIN print key	Generate DK PIN Print Pair	CSNBKGN2
02BD	Key Generate2 – DK PIN admin1 key PINPROT	Generate DK PIN Admin 1 PINPROT Pair	CSNBKGN2
02BE	Key Generate2 – DK PIN admin1 key MAC	Generate DK PIN Admin 1 MAC Pair	CSNBKGN2
02BF	Key Generate2 – DK PIN admin2 key MAC	Generate DK PIN Admin 2 MAC Pair	CSNBKGN2
02C0	DK Random PIN Generate	Allow DK Random PIN Generate	CSNBDRPG
02C1	DK PIN Verify	Allow DK PIN Verify	CSNBDPV
02C2	DK PIN Change	Allow DK PIN Change	CSNBDPC
02C3	DK PRW Card Number Update	Allow DK PRW Card Number Update	CSNBDPNU
02C4	DK PRW CMAC Generate	Allow DK PRW CMAC Generate	CSNBDPCG
02C5	DK PAN Modify in Transaction	Allow DK PAN Modify in Transaction	CSNBDPMT
02C6	DK PAN Translate	Allow DK Deterministic PIN	CSNBDDPG
02C7	DK Deterministic PIN Generate	Allow DK PAN Translate	CSNBDPT
02C8	DK Regenerate PRW	Allow DK Regenerate	CSNBDRP
02CC	Diversified Key Generate2 – SESS-ENC	Diversified Key Generate2 (SESS-ENC)	CSNBDKG2
02CD	Diversified Key Generate2 - DALL	Derive Any Key Type	CSNBDKG2
02CE	DK Migrate PIN	Allow DK Migrate PIN	CSNBDMP
02CF	FPE Encrypt	FPE Encipher	
02D0	FPE Decrypt	FPE Decipher	
02D1	FPE Translate	FPE Translate	
02D2	Diversified Key Generate2 - MK-OPTC	Diversified Key Generate2 (MK-OPTC)	CSNBDKG2
02D3	Diversified Key Generate2 – KDFFM-DK	Diversified Key Generate2 (KDFFM-DK)	CSNBDKG2
02D4	Diversified Key Generate2 – Allow length option with KDFFM-DK	Allow Generated Key Length Option with KDFFM-DK Keyword	CSNBDKG2

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
02D5	Encrypted PIN Translate Enhanced	Encrypted PIN Translate Enhanced	CSNBPTRE
02EB	Allow weak wrapping of compliance-tagged keys by DES MK	N/A	
02EE	PKA Key Translate – allow INTUSCHG	SCA_CMD_PKT_INTUSCHG	CSNDPKT
02F5	Authenticated Key Export - SETSNKEY	N/A	
02F6	Authenticated Key Export - DRVTXKEY	N/A	
02F7	Authenticated Key Export - EXPTSK	N/A	
02F8	Key Translate2 - COMP-CHK	CMD_KTR2_ALLOW_COMPTAG	CSBNKTR2
02F9	Key Translate2 - COMP-TAG	CMD_KTR2_ALLOW_COMPCHK	CSBNKTR2
0300	NOCV KEK usage for export-related functions	N/A	
0301	Prohibit Export Extended	Lower Export Authority, Extended	CSNBPEXX
0303	PCF CKDS Conversion Program	N/A	
0309	Operational Key Load	N/A	
030A	NOCV KEK usage for import-related functions	N/A	
030C	DSG - ZERO-PAD restriction lifted	Override DSG ZERO-PAD Length Restriction	CSNDDSG
030D	Key Encryption Translate – CBC to ECB	Translate Key from CBC to ECB	CSNBKET
030E	Key Encryption Translate – ECB to CBC	Translate Key from ECB to CBC	CSNBKET
0310	Trusted Block Create - Activate an inactive block	Create a Trusted Block in Inactive Form	CSNDTBC
030F	Trusted Block Create - Create Block in inactive form	Activate an Inactive Trusted Block	CSNDTBC
0311	PKA Key Import - Import an external trusted block	Convert Trusted Block from External to Internal Form	CSNDPKI
0312	Remote Key Export - Gen or export a non-CCA node key	Generate or Export a Key for Use by a Non-CCA Node	CSNDRKX
0313	Enhanced PIN Security	Enhanced PIN Security Mode	CSNBCPA CSNBCPE CSNBEPG CSNBPTR CSNBPVR CSNBPCU
0318	PKA Key Translate - from CCA RSA to SC Visa format	Translate from CCA RSA to SC Visa Format	CSNDPKT

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0319	PKA Key Translate - from CCA RSA to SC ME format	Translate from CCA RSA to SC M-E Format	CSNDPKT
031A	PKA Key Translate - from CCA RSA to SC CRT format	Translate from CCA RSA to SC CRT Format	CSNDPKT
031B	PKA Key Translate - from source EXP KEK to target EXP KEK	XLATE from Encryption Under Source EXP KEK to Target EXP KEK	CSNDPKT
031C	PKA Key Translate - from source IMP KEK to target EXP KEK	XLATE from Encryption Under Source IMP KEK to Target EXP KEK	CSNDPKT
031D	PKA Key Translate - from source IMP KEK to target IMP KEK	XLATE from Encryption Under Source IMP KEK to Target IMP KEK	CSNDPKT
031F	ECC Master Key - Clear new master key register	Clear APKA NMK Register (CLEAR)	CSNBMKP
0320	ECC Master Key - Load first key part	Load First APKA Master Key Part	CSNBMKP
0321	ECC Master Key - Combine key parts	Combine Intermediate APKA Master Key Parts	CSNBMKP
0322	ECC Master Key - Set master key	Activate New APKA Master Key (SET)	CSNBMKP
0326	PKA Key Generate – Clear ECC keys	Generate ECC Keys in the Clear	CSNDPKG
0327	Symmetric Key Export - AESKW	Export AES Key (AESKW)	CSNDSYX
0328	Prohibit weak wrap – Transport keys	Disallow Weak Transport Key	CSNDEDH CSNBKGN2 CSNDPKG CSNDSYX
0329	Symmetric Key Import2 - AESKW	Import AES Key (AESKW)	CSNDSYI2
032A	Key Translate2 - Disallow AES ver 5 to ver 4 conversion	Disallow Translation from an AES X'05' to an AES X'04' Token	CSNBKTR2
032B	Symmetric Key Import2 – disallow weak import	Disallow Import of Key Wrapped with Weaker Transport Key	CSNDSYI CSNDSYI2 CDNBUKD
032C	Warn when weak wrap – Transport keys	Warn When Transport Key Is Weak	CSNDEDH CSNBKGN2 CSNDPKG CSNDSYX
032D	Disallow 24-byte DATA wrapped with 16-byte Key	N/A	

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
032E	Trusted Block Create – Disallow triple-length MAC key	Disallow Import of Triple-Length MAC Key Under Double-Length TDES KEK	CSNBTBC
0330	DES master key – 24-byte key	N/A	
0331	Allow weak DES wrap of RSA	Allow weak DES wrap of RSA	CSNBKET CSNDPKG CSNDPKI CSNDPKT CSNDSXD CSNDSYG CSNDSYI CSNDSYX
0332	Warn when weak wrap – Master keys	Warn When Wrapping Key with Weaker Master Key	CSNBCKI CSNBDKM CSNBDKG CSNDEDH CSNBKGN CSNBKGN2 CSNBKIM CSNBKPI CSNBKPI2 CSNBKTC CSNBKTC2 CSNBMKP CSNBCKM CSNDPKG CSNDPKI CSNDKTC CSNBPEX CSNBRKA CSNDSYG CSNDSYI CSNDSYI2 CSNBT31I CSNBUKD

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
0333	Prohibit weak wrap – Master keys	Disallow Wrapping Key with Weaker Master Key	CSNBCKI CSNBDKM CSNBDKG CSNDEDH CSNBKGN CSNBKGN2 CSNBKIM CSNBKPI CSNBKPI2 CSNBKTC CSNBKTC2 CSNBMKP CSNBCKM CSNDPKG CSNDPKI CSNDKTC CSNBPEX CSNBRKA CSNDSYG CSNDSYI CSNDSYI2 CSNBT31I CSNBUKD
0334	Key Translate2 – Translate fixed to variable payload	Allow Translation from Version 1 Payload to Version 0 Payload	CSNBKTR2
0335	Unique Key Derive - K3IPEK	DUKPT K3IPEK	CSNBUKD
0336	MAC Generate2 – AES CMAC	Generate AES CMAC	CSNBMGN2
0337	MAC Verify2 – AES CMAC	Verify AES CMAC	CSNBMVR2
0338	PKA Key Translate - from CCA RSA CRT to EMVDDA format	Translate from CCA RSA CRT to EMVDDA Format	CSNDPKT
0339	PKA Key Translate - from CCA RSA CRT to EMVDDAE format	Translate from CCA RSA CRT to EMVDDAE Format	CSNDPKT
033A	PKA Key Translate - from CCA RSA CRT to EMVCRT format	Translate from CCA RSA CRT to EMVCRT Format	CSNDPKT
033B	Digital Signature Generate – PKCS-PSS allow small salt	Allow Not Exact Salt Length	CSNDDSG

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
033C	Digital Signature Verify – PKCS-PSS allow not exact salt length	Allow Small Salt	CSNDDSV
0350	ANSI X9.8 PIN - Enforce PIN block restrictions	Enforce ANS X9.8 PIN Rules	CSNBCPA CSNBPTR CSNBSPN
0351	ANSI X9.8 PIN – Allow modification of PAN	Allow Change of PAN with ANS X9.8 PIN Rules	CSNBPTR CSNBSPN
0352	ANSI X9.8 PIN - Allow only ANSI PIN blocks	Enforce ANS X9.8 PIN Rules and Disallow Use of Non-ISO PINs	CSNBPTR CSNBSPN
0356	ANSI X9.8 PIN – Use stored decimalization tables only	Use Only Valid Decimalization Tables	CSNBPGN CSNBCPA CSNBEPG CSNBPVR
0360	ECC Diffie-Hellman	Elliptic Curve Diffie-Hellman	CSNDEDH
0361	ECC Diffie-Hellman – Allow PASSTHRU	N/A	CSNDEDH
0362	ECC Diffie-Hellman – Allow key wrap override	Allow Configuration Override with Keyword in EDH	CSNDEDH
0363	ECC Diffie-Hellman – Allow Prime Curve 192	Allow Prime Curve 192	CSNDEDH
0364	ECC Diffie-Hellman – Allow Prime Curve 224	Allow Prime Curve 224	CSNDEDH
0365	ECC Diffie-Hellman – Allow Prime Curve 256	Allow Prime Curve 256	CSNDEDH
0366	ECC Diffie-Hellman – Allow Prime Curve 384	Allow Prime Curve 384	CSNDEDH
0367	ECC Diffie-Hellman – Allow Prime Curve 521	Allow Prime Curve 521	CSNDEDH
0368	ECC Diffie-Hellman – Allow BP Curve 160	Allow Brainpool Curve 160	CSNDEDH
0369	ECC Diffie-Hellman – Allow BP Curve 192	Allow Brainpool Curve 192	CSNDEDH
036A	ECC Diffie-Hellman – Allow BP Curve 224	Allow Brainpool Curve 224	CSNDEDH
036B	ECC Diffie-Hellman – Allow BP Curve 256	Allow Brainpool Curve 256	CSNDEDH
036C	ECC Diffie-Hellman – Allow BP Curve 320	Allow Brainpool Curve 320	CSNDEDH
036D	ECC Diffie-Hellman – Allow BP Curve 384	Allow Brainpool Curve 384	CSNDEDH

Offset (Hex)	ICSF access control name	IBM 4767 command name	IBM 4767 verbs affected
036E	ECC Diffie-Hellman – Allow BP Curve 512	Allow Brainpool Curve 512	CSNDEDH
036F	ECC Diffie-Hellman – Prohibit weak key generate	Prevent Weaker Key from Being Used to Generate Stronger Key	CSNDEDH
0382	T31X - Permit version D TR-31 key blocks	T31X Permit Version D TR-31 Key Blocks	CSNBT31X
0383	T31X - Permit AES KDKGENKY: KDKTYPEA to 11:X	T31X Permit AES KDKGENKY: KDKTYPEA to 11:X	CSNBT31X
0384	T31X - Permit AES KDKGENKY: KDKTYPEB to 10:X	T31X Permit AES KDKGENKY: KDKTYPEB to 10:X	CSNBT31X
0385	T31X - Permit DES DKYGENKY: DKYL0:DMPIN to 12:X	T31X Permit DES DKYGENKY: DKYL0:DMPIN to 12:X	CSNBT31X
0386	T31I - Permit version D TR-31 key blocks	T31I Permit Version D TR-31 Key Blocks	CSNBT31I
038A	Encrypted PIN Translate2 – Permit ISO-4 to ISO-4 Translate	Encrypted PIN Translate2 – Permit ISO-4 to ISO-4 Translate	CSNBPTR2
038B	Encrypted PIN Translate2 – Permit ISO-4 Reformat w/ PAN Chg	Encrypted PIN Translate2 – Permit ISO-4 to ISO-4 Reformat with PAN Change	CSNBPTR2
038C	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 Reformat	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 Reformat	CSNBPTR2
038D	Encrypted PIN Translate2 – Permit ISO-4 to ISO-1 Reformat	Encrypted PIN Translate2 – Permit ISO-4 to ISO-1 Reformat	CSNBPTR2
038E	Encrypted PIN Translate2 – Permit ISO-0 to ISO-4 Reformat	Encrypted PIN Translate2 – Permit ISO-0 to ISO-4 Reformat	CSNBPTR2
038F	Encrypted PIN Translate2 – Permit ISO-4 to ISO-0 Reformat	Encrypted PIN Translate2 – Permit ISO-4 to ISO-0 Reformat	CSNBPTR2
0391	Encrypted PIN Translate2 – REFORMAT with AES token	Encrypted PIN Translate2 – REFORMAT with AES Token	CSNBPTR2
0392	Encrypted PIN Translate2 – TRANSLAT with AES token	Encrypted PIN Translate2 – TRANSLATE with AES Token	CSNBPTR2
0393	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 RFMT1TO4.	Encrypted PIN Translate2 – Permit ISO-1 to ISO-4 only with RFMT1TO4	CSNBPTR2
0395	Encrypted PIN Translate2 - Permit ISO-4 to ISO-4 PTR2AUTH	PTR2 Permit ISO-4 to ISO-4 Reformat with PAN Change	CSNBPTR2