z/OS

Cryptographic Services Integrated Cryptographic Service Facility UDX Simplification and Reduction (PKT UDX) APAR OA43816

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product from integrating an existing User Defined Extension (UDX) into the CCA base. Three new *rule_array* keywords are added to the ICSF CSNDPKT callable service enabling CSNDPKT to translate RSA CRT tokens to EMV DDA, EMV DDAE, and EMV CRT formats.

These changes are available through the application of the PTF for APAR OA43816 and apply to FMID HCR77A1, HCR77A0, and HCR7790. This document contains alterations to information previously presented in *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-00.

The technical changes made to the ICSF product by the application of the PTF for APAR OA43816 are indicated in this document by a vertical line to the left of the change.

Chapter 2. Update of z/OS Cryptographic Services ICSF Application Programmer's Guide, SC14-7508-00, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-00, for the UDX Simplification and Reduction (PKT UDX) support provided by the PTF for APAR OA43816. Refer to this source document if background information is needed.

PKA Key Translate (CSNDPKT and CSNFPKT)

The PKA key translate callable service is used to do the following:

- Translation - Translate a CCA RSA key token into an external key token. The format of the external key token is specified by the output format keyword of the *rule_array* parameter.

  The source CCA RSA key token must be wrapped with a transport key-encrypting key (KEK). The XLATE bit must also be turned on in the key usage byte of the source token. The source token is unwrapped using the specified source transport KEK. The target key token will be wrapped with the specified target transport KEK. Existing information in the target token is overwritten. There are restrictions on which type key can be used for the source and target transport key tokens. These restrictions are enforced by access control points.
- Conversion - Convert the object protection key (OPK) in an CCA RSA private key token from a DES key to an AES key.

  The service will convert an existing internal or external RSA private key token. The modulus-exponent and Chinese Remainder Theorem forms are supported. Private key section identifiers 0x06, 0x08, and 0x09 can be converted.

The callable service name for AMODE(64) invocation is CSNFPKT.

Format

```
CALL CSNDPKT(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             source_key_identifier_length,
             source_key_identifier,
             source_transport_key_identifier_length,
             source_transport_key_identifier,
             target_transport_key_identifier_length,
             target_transport_key_identifier,
             target_key_token_length,
             target_key_token)
```

Parameters

return_code

Direction	Type
Output	Integer

The return code specifies the general result of the callable service.

reason_code

Direction	Type
Output	Integer

The reason code specifies the result of the callable service that is returned to the application program. Each return code has different reason codes assigned to it that indicate specific processing problems.

exit_data_length

Direction	Type
Input/Output	Integer

The length of the data that is passed to the installation exit. The length can be from X'00000000' to X'7FFFFFFF' (2 gigabytes). The data is identified in the *exit_data* parameter.

exit_data

Direction	Type
Input/Output	String

The data that is passed to the installation exit.

rule_array_count

Direction	Type
Input	Integer

The number of keywords you supplied in the *rule_array* parameter. Value must be 1.

rule_array

Direction	Type
Input	String

A keyword that provides control information to the callable service. See Table 1 for a list. A keyword is left-justified in an 8-byte field and padded on the right with blanks.

Table 1. Keywords for PKA Key Translate Rule Array

Keyword	Meaning
Output format, one required	
Output formats for conversion	
EXTDWAKW	Specifies that the source key is an external DES wrapped token to be converted to an AESKW wrapped token.
INTDWAKW	Specifies that the source key is an internal DES wrapped token to be converted to an AESKW wrapped token.
Output formats for translation	

Table 1. Keywords for PKA Key Translate Rule Array (continued)

Keyword	Meaning
EMVCRT	This keyword indicates translating an external RSA CRT key into EMV CRT format and wrapped using TDES-ECB. The XLATE bit (bit 22) must be set in the *target_transport_key_identifier* control vector.
EMVDDA	This keyword indicates translating an external RSA CRT key into EMV DDA format and wrapped using TDES-CBC. The XLATE bit (bit 22) must be set in the *target_transport_key_identifier* control vector.
EMVDDAE	This keyword indicates translating an external RSA CRT key into EMV DDAE format and wrapped using TDES-ECB. The XLATE bit (bit 22) must be set in the *target_transport_key_identifier* control vector.
SCCOMCRT	This keyword indicates translating the key into the smart card Chinese Remainder Theorem format.
SCCOMME	This keyword indicates translating the key into the smart card Modulus-Exponent format.
SCVISA	This keyword indicates translating the key into the smart card Visa proprietary format.

source_key_identifier_length

Direction	Type
Input	Integer

Length in bytes of the *source_key_identifier* variable. The maximum length is 3500 bytes.

source_key_identifier

Direction	Type
Input	String

This field contains either a key label identifying an RSA private key token or an RSA public-private key token. For smart card processing, the key must be in an external key token. For OPK conversion, the token may be internal or external. External tokens are wrapped with a DES key encrypting key. When an internal token is specified, the transport keys are not used.

source_transport_key_identifier_length

Direction	Type
Input	Integer

Length in bytes of the *source_transport_key_identifier* parameter. This value must be 64. For format rule INTDWAKW, the length must be zero.

source_transport_key_identifier

Direction	Type
Input/Output	String

This field contains an internal token or label of a DES key-encrypting key. This key is used to unwrap the input RSA key token specified with parameter *source_key_identifier*. See "Access Control Points" on page 7 for details on the type of transport key that can be used

target_transport_key_identifier_length

Direction	Type
Input	Integer

Length in bytes of the *target_transport_key_identifier* parameter. When a DES key-encrypting is used, this value must be 64. When an AES key-encrypting key is used, this value is the length of the token. The maximum length is 725. For INTDWAKW, the length must be zero.

target_transport_key_identifier

Direction	Type
Input/Output	String

This field contains an internal token or label of a DES key-encrypting key. This key is used to wrap the output RSA key returned with parameter target_key_token. See "Access Control Points" on page 7 for details on the type of transport key that can be used.

target_key_token_length

Direction	Type
Input/Output	Integer

Length in bytes of the *target_key_token* parameter. On output, the value in this variable is updated to contain the actual length of the *target_key_token* produced by the callable service. The maximum length is 3500 bytes.

target_key_token

Direction	Type
Output	String

This field contains the RSA key in the smartcard format specified in the rule array and is protected by the key-encrypting key specified in the *target_transport_key* parameter. This is not a CCA token, and cannot be stored in the PKDS.

Restrictions

CCA RSA ME tokens will not be translated to the SCCOMCRT, EMV DDA, EMV DDAE, or the EMV CRT formats. CCA RSA CRT tokens will not be translated to the SCCOMME format. SCVISA only supports Modulus-Exponent (ME) keys.

The maximum modulus size of CCA RSA CRT tokens for the EMVDDA, EMVDDAE, or the EMVCRT formats is 2040 bits.

Only CCA RSA CRT tokens with a private section of X'08' are supported by the EMVDDA, EMVDDAE, or the EMVCRT rule array keywords.

Access Control Points

There are access control points that control use of the format rule array keywords and the type of transport keys that can be used.

Table 2. Required access control points for PKA Key Translate

Rule array keyword	Access control point
INTDWAKW	PKA Key Translate – Translate internal key token
EXTDWAKW	PKA Key Translate – Translate external key token
SCVISA	PKA Key Translate - from CCA RSA to SC Visa Format
SCCOMME	PKA Key Translate - from CCA RSA to SC ME Format
SCCOMCRT	PKA Key Translate - from CCA RSA to SC CRT Format
EMVDDA	PKA Key Translate - from CCA RSA CRT to EMV DDA Format
EMVDDAE	PKA Key Translate - from CCA RSA CRT to EMV DDAE Format
EMVCRT	PKA Key Translate - from CCA RSA CRT to EMV CRT Format

These access control points control the key type combination shown in this table. One of these access control points must be enabled.

Table 3. Required access control points for source/target transport key combinations

Source transport key type	Target transport key type	Access control point
EXPORTER	EXPORTER	PKA Key Translate - from source EXP KEK to target EXP KEK
IMPORTER	EXPORTER	PKA Key Translate - from source IMP KEK to target EXP KEK
IMPORTER	IMPORTER	PKA Key Translate - from source IMP KEK to target IMP KEK
EXPORTER	IMPORTER	(Not allowed)

Required Hardware

This table lists the required cryptographic hardware for each server type and describes restrictions for this callable service.

Table 4. PKA key translate required hardware

Server	Required Cryptographic hardware	Restrictions
IBM eServer zSeries 990 IBM eServer zSeries 890		This callable service is not supported.

Table 4. PKA key translate required hardware (continued)

Server	Required Cryptographic hardware	Restrictions
IBM System z9 EC IBM System z9 BC	Crypto Express2 Coprocessor	Requires the Apr. 2009 or later licensed internal code (LIC). The *rule_array* keywords EMVDDA, EMVDDAE, and EMVCRT are not supported.
IBM System z10 EC IBM System z10 BC	Crypto Express2 Coprocessor Crypto Express3 Coprocessor	Requires the Apr. 2009 or later licensed internal code (LIC). The *rule_array* keywords EMVDDA, EMVDDAE, and EMVCRT are not supported.
IBM zEnterprise 196 IBM zEnterprise 114	Crypto Express3 Coprocessor	Support for the *rule_array* keywords EMVDDA, EMVDDAE, and EMVCRT requires the March 2014 or later licensed internal code (LIC).
IBM zEnterprise EC12 IBM zEnterprise BC12	Crypto Express3 Coprocessor Crypto Express4 Coprocessor	Support for the *rule_array* keywords EMVDDA, EMVDDAE, and EMVCRT requires the March 2014 or later licensed internal code (LIC).

Access Control Points and Callable Services

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

- The Allow weak DES wrap of RSA access control point is only checked if the Prohibit weak wrap – Transport keys access control point is enabled.
- The ANSI X9.8 PIN - Allow modification of PAN and ANSI X9.8 PIN - Allow only ANSI PIN blocks access control points can only be enable when the ANSI X9.8 PIN - Enforce PIN block restrictions access control point is enabled.

This following table lists access control points that affect specific services indicated in the access control point name. There is a description of the usage of the access control point in the Usage Notes section of the callable service description.

Note: If the domain role has been changed via the TKE workstation, all new access control points are disabled by default.

Table 5. Access control points – Callable Services

Name	Callable Service	Usage
Authentication Parameter Generate	CSNBAPG / CSNEAPG	ED
Authentication Parameter Generate - Clear	CSNBAPG / CSNEAPG	DD
Cipher Text translate2	CSNBCTT2 / CSNECTT2 and CSNBCTT3 / CSNECTT3	ED
Cipher Text translate2 – Allow translate from AES to TDES	CSNBCTT2 / CSNECTT2 and CSNBCTT3 / CSNECTT3	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Cipher Text translate2 – Allow translate to weaker AES	CSNBCTT2 / CSNECTT2 and CSNBCTT3 / CSNECTT3	ED
Cipher Text translate2 – Allow translate to weaker DES	CSNBCTT2 / CSNECTT2 and CSNBCTT3 / CSNECTT3	ED
Cipher Text translate2 – Allow only cipher text translate types	CSNBCTT2 / CSNECTT2 and CSNBCTT3 / CSNECTT3	DD
Clear Key Import / Multiple Clear Key Import - DES	CSNBCKI / CSNECKI and CSNBCKM / CSNECKM	ED
Clear PIN Encrypt	CSNBCPE / CSNECPE	ED
Clear PIN Generate - 3624	CSNBPGN / CSNEPGN	ED
Clear PIN Generate - GBP	CSNBPGN / CSNEPGN	ED
Clear PIN Generate - VISA PVV	CSNBPGN / CSNEPGN	ED
Clear PIN Generate - Interbank	CSNBPGN / CSNEPGN	ED
Clear Pin Generate Alternate - 3624 Offset	CSNBCPA / CSNECPA	ED
Clear PIN Generate Alternate - VISA PVV	CSNBCPA / CSNECPA	ED
Control Vector Translate	CSNBCVT / CSNECVT	ED
Cryptographic Variable Encipher	CSNBCVE / CSNECVE	ED
CVV Key Combine	CSNBCKC / CSNECKC	ED
CVV Key Combine - Allow wrapping override keywords	CSNBCKC / CSNECKC	ED
CVV Key Combine - Permit mixed key types	CSNBCKC / CSNECKC	ED
Data Key Export	CSNBDKX / CSNEDKX	ED
Data Key Export - Unrestricted	CSNBDKX / CSNEDKX	ED
Data Key Import	CSNBDKM / CSNEDKM	ED
Data Key Import - Unrestricted	CSNBDKM / CSNEDKM	ED
Decipher - DES	CSNBDEC / CSNEDEC	ED
Digital Signature Generate	CSNDDSG / CSNFDSG	ED
DSG - ZERO-PAD restriction lifted	CSNDDSG / CSNFDSG	ED
Digital Signature Verify	CSNDDSV / CSNFDSV	ED
Diversified Key Generate - CLR8–ENC	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - SESS-XOR	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - TDES-ENC	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - TDES-CBC	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - TDES-DEC	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - TDES-XOR	CSNBDKG / CSNEDKG	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Diversified Key Generate - TDESEMV2/TDESEMV4	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - Allow wrapping override keywords	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - single length or same halves	CSNBDKG / CSNEDKG	ED
Diversified Key Generate - DKYGENKY - DALL	CSNBDKG / CSNEDKG	DD, SC
ECC Diffie-Hellman	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow Prime Curve 192	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow Prime Curve 224	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow Prime Curve 256	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow Prime Curve 384	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow Prime Curve 521	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 160	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 192	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 224	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 256	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 320	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 384	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow BP Curve 512	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow PASSTHRU	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Allow key wrap override	CSNDEDH / CSNFEDH	ED
ECC Diffie-Hellman – Prohibit weak key generate	CSNDEDH / CSNFEDH	DD, SC
Encipher - DES	CSNBENC / CSNEENC	ED
Encrypted PIN Generate - 3624	CSNBEPG / CSNEEPG	ED
Encrypted PIN Generate - GBP	CSNBEPG / CSNEEPG	ED
Encrypted PIN Generate - Interbank	CSNBEPG / CSNEEPG	ED
Encrypted PIN Translate - Translate	CSNBPTR / CSNEPTR	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Encrypted PIN Translate - Reformat	CSNBPTR / CSNEPTR	ED
Encrypted PIN Verify - 3624	CSNBPVR / CSNEPVR	ED
Encrypted PIN Verify - GPB	CSNBPVR / CSNEPVR	ED
Encrypted PIN Verify - VISA PVV	CSNBPVR / CSNEPVR	ED
Encrypted PIN Verify - Interbank	CSNBPVR / CSNEPVR	ED
HMAC Generate – SHA-1	CSNBHMG / CSNBHMG1 and CSNEHMG / CSNEHMG1	ED
HMAC Generate – SHA-224	CSNBHMG / CSNBHMG1 and CSNEHMG / CSNEHMG1	ED
HMAC Generate – SHA-256	CSNBHMG / CSNBHMG1 and CSNEHMG / CSNEHMG1	ED
HMAC Generate – SHA-384	CSNBHMG / CSNBHMG1 and CSNEHMG / CSNEHMG1	ED
HMAC Generate – SHA-512	CSNBHMG / CSNBHMG1 and CSNEHMG / CSNEHMG1	ED
HMAC Verify – SHA-1	CSNBHMV / CSNBHMV1 and CSNEHMV / CSNEHMV1	ED
HMAC Verify – SHA-224	CSNBHMV / CSNBHMV1 and CSNEHMV / CSNEHMV1	ED
HMAC Verify – SHA-256	CSNBHMV / CSNBHMV1 and CSNEHMV / CSNEHMV1	ED
HMAC Verify – SHA-384	CSNBHMV / CSNBHMV1 and CSNEHMV / CSNEHMV1	ED
HMAC Verify – SHA-512	CSNBHMV / CSNBHMV1 and CSNEHMV / CSNEHMV1	ED
Key Export	CSNBKEX / CSNEKEX	ED
Key Export - Unrestricted	CSNBKEX / CSNEKEX	ED
Key Generate – OP	CSNBKGN / CSNEKGN	ED
Key Generate – Key set	CSNBKGN / CSNEKGN	ED
Key Generate – Key set extended	CSNBKGN / CSNEKGN	ED
Key Generate - SINGLE-R	CSNBKGN / CSNEKGN	ED
Key Generate2 – OP	CSNBKGN2 / CSNEKGN2	ED
Key Generate2 – Key set	CSNBKGN2 / CSNEKGN2	ED
Key Generate2 – Key set extended	CSNBKGN2 / CSNEKGN2	ED
Key Import	CSNBKIM / CSNEKIM	ED
Key Import - Unrestricted	CSNBKIM / CSNEKIM	ED
Key Part Import - First key part	CSNBKPI / CSNEKPI	ED
Key Part Import - Middle and final	CSNBKPI / CSNEKPI	ED
Key Part Import - ADD-PART	CSNBKPI / CSNEKPI	ED
Key Part Import - COMPLETE	CSNBKPI / CSNEKPI	ED
Key Part Import - Allow wrapping override keywords	CSNBKPI / CSNEKPI	ED
Key Part Import - Unrestricted	CSNBKPI / CSNEKPI	ED
Key Part Import2 – Load first key part, require 3 key parts	CSNBKPI2 / CSNEKPI2	ED
Key Part Import2 – Load first key part, require 2 key parts	CSNBKPI2 / CSNEKPI2	ED
Key Part Import2 - Load first key part, require 1 key parts	CSNBKPI2 / CSNEKPI2	ED
Key Part Import2 - Add second of 3 or more key parts	CSNBKPI2 / CSNEKPI2	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Key Part Import2 - Add last required key part	CSNBKPI2 / CSNEKPI2	ED
Key Part Import2 - Add optional key part	CSNBKPI2 / CSNEKPI2	ED
Key Part Import2 – Complete key	CSNBKPI2 / CSNEKPI2	ED
Key Test and Key Test2	CSNBKYT / CSNEKYT and CSNBKYT2 / CSNEKYT2	AE
Key Test2 – AES, ENC-ZERO	CSNBKYT2 / CSNEKYT2	AE
Key Test - Warn when keyword inconsistent with key length	CSNBKYTX / CSNFKYTX	DD
Key Translate	CSNBKTR / CSNEKTR	ED
Key Translate2	CSNBKTR2 / CSNEKTR2	ED
Key Translate2 - Allow use of REFORMAT	CSNBKTR2 / CSNEKTR2	ED
Key Translate2 - Allow wrapping override keywords	CSNBKTR2 / CSNEKTR2	ED
Key Translate2 - Disallow AES ver 5 to ver 4 conversion	CSNBKTR2 / CSNEKTR2	DD
Key Translate2 – Translate fixed to variable payload	CSNBKTR2 / CSNEKTR2	DD
MAC Generate	CSNBMGN / CSNEMGN	ED
MAC Verify	CSNBMVR / CSNEMVR	ED
Multiple Clear Key Import / Multiple Secure Key Import - AES	CSNBCKM / CSNECKM and CSNBSKM / CSNESKM	ED
Multiple Clear Key Import - Allow wrapping override keywords	CSNBCKM / CSNECKM	ED
Multiple Secure Key Import - Allow wrapping override keywords	CSNBSKM / CSNESKM	ED
Operational Key Load	CSNBOKL / CSNEOKL	ED
Operational Key Load - Variable-Length Tokens	CSNBOKL / CSNEOKL	ED
PIN Change/Unblock - change EMV PIN with OPINENC	CSNBPCU / CSNEPCU	ED
PIN Change/Unblock - change EMV PIN with IPINENC	CSNBPCU / CSNEPCU	ED
PKA Decrypt	CSNDPKD / CSNFPKD	ED
PKA Encrypt	CSNDPKE / CSNFPKE	ED
PKA Key Generate	CSNDPKG / CSNFPKG	ED
PKA Key Generate – Clear RSA keys	CSNDPKG / CSNFPKG	ED
PKA Key Generate – Clear ECC keys	CSNDPKG / CSNFPKG	ED
PKA Key Generate - Clone	CSNDPKG / CSNFPKG	ED
PKA Key Generate - Permit Regeneration Data	CSNDPKG / CSNFPKG	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
PKA Key Generate - Permit Regeneration Data Retain	CSNDPKG / CSNFPKG	ED
PKA Key Import	CSNDPKI / CSNFPKI	ED
PKA Key Import - Import an External Trusted Key Block to internal form	CSNDPKI / CSNFPKI	ED
PKA Key Token Change RTCMK	CSNDKTC / CSNFKTC	ED
PKA Key Translate - from CCA RSA to SC Visa format	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from CCA RSA to SC ME format	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from CCA RSA to SC CRT format	CSNDPKT / CSNFPKT	ED
PKA Key Translate – Translate internal key token	CSNDPKT / CSNFPKT	ED
PKA Key Translate – Translate external key token	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from source EXP KEK to target EXP KEK	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from source IMP KEK to target EXP KEK	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from source IMP KEK to target IMP KEK	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from CCA RSA CRT to EMVDDA format	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from CCA RSA CRT to EMVDDAE format	CSNDPKT / CSNFPKT	ED
PKA Key Translate - from CCA RSA CRT to EMVCRT format	CSNDPKT / CSNFPKT	ED
Prohibit Export	CSNBPEX / CSNEPEX	ED
Prohibit Export Extended	CSNBPEXX /CSNEPEXX	ED
Recover PIN From Offset	CSNBPFO / CSNEPFO	ED
Remote Key Export - Generate or export a key for use by a non-CCA node	CSNDRKX / CSNFRKX	ED
Remote Key Export – Include RKX in Default Key-Wrapping Configuration	CSNDRKX / CSNFRKX	DD
Remote Key Export - Allow wrapping override keywords	CSNDRKX / CSNFRKX	DD
RKX/TBC – Disallow triple-length MAC key	CSNDRKX / CSNFRKX and CSNDTBC / CSNFTBC	DD, SC
Restrict Key Attribute – Export Control	CSNBRKA / CSNERKA	ED
Restrict Key Attribute - Permit setting the TR-31 export bit	CSNBRKA / CSNERKA	ED
Retained Key Delete	CSNDRKD / CSNFRKD	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Retained Key List	CSNDRKL / CSNFRKL	ED
Secure Key Import – DES, IM	CSNBSKI / CSNESKI and CSNBSKM / CSNESKM	ED
Secure Key Import – DES, OP	CSNBSKI / CSNESKI and CSNBSKM / CSNESKM	ED
Secure Key Import2 - OP	CSNBSKI2 / CSNESKI2	ED
Secure Key Import2 - IM	CSNBSKI2 / CSNESKI2	ED
Secure Messaging for Keys	CSNBSKY / CSNESKY	ED
Secure Messaging for PINs	CSNBSPN / CSNESPN	ED
SET Block Compose	CSNDSBC / CSNFSBC	ED
SET Block Decompose	CSNDSBD / CSNFSBD	ED
SET Block Decompose - PIN ext IPINENC	CSNDSBD / CSNFSBD	ED
SET Block Decompose - PIN ext OPINENC	CSNDSBD / CSNFSBD	ED
Symmetric Algorithm Decipher - Secure AES	CSNBSAD / CSNESAD and CSNBSAD1 / CSNESAD1	ED
Symmetric Algorithm Encipher - Secure AES	CSNBSAE / CSNESAE and CSNBSAE1 / CSNESAE1	ED
Symmetric Key Encipher/Decipher - Encrypted DES keys	CSNBSYD / CSNBSYE and CSNBSYD1 / CSNESYD1	ED
Symmetric Key Encipher/Decipher - Encrypted AES keys	CSNBSYD / CSNBSYE and CSNBSYD1 / CSNESYD1	ED
Symmetric Key Export with Data	CSNDSXD / CSNFSXD	DD
Symmetric Key Export with Data - Special	CSNDSXD / CSNFSXD	DD
Symmetric Key Export - AES, PKCSOAEP, PKCS-1.2	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - AES, PKOAEP2	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - AES, ZERO-PAD	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - AESKW	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - AESKWCV	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - DES, PKCS-1.2	CSNDSYX / CSNFSYX	ED
Symmetric Key Export - DES, ZERO-PAD	CSNDSYX / CSNFSYX	ED
Symmetric Key Export – HMAC,PKOAEP2	CSNDSYX / CSNFSYX	ED
Symmetric Key Generate - AES, PKCSOAEP, PKCS-1.2	CSNDSYG / CSNFSYG	ED
Symmetric Key Generate - AES, ZERO-PAD	CSNDSYG / CSNFSYG	ED
Symmetric Key Generate - DES, PKCS-1.2	CSNDSYG / CSNFSYG	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Symmetric Key Generate - DES, ZERO-PAD	CSNDSYG / CSNFSYG	ED
Symmetric Key Generate - DES, PKA92	CSNDSYG / CSNFSYG	ED
Symmetric Key Generate - Allow wrapping override keywords	CSNDSYG / CSNFSYG	ED
Symmetric Key Import - AES, PKCSOAEP, PKCS-1.2	CSNDSYI / CSNFSYI	ED
Symmetric Key Import - AES, ZERO-PAD	CSNDSYI / CSNFSYI	ED
Symmetric Key Import - DES, PKCS-1.2	CSNDSYI / CSNFSYI	ED
Symmetric Key Import - DES, ZERO-PAD	CSNDSYI / CSNFSYI	ED
Symmetric Key Import - DES, PKA92 KEK	CSNDSYI / CSNFSYI	ED
Symmetric Key Import - Allow wrapping override keywords	CSNDSYI / CSNFSYI	ED
Symmetric Key Import2 – AES,PKOAEP2	CSNDSYI2 / CSNFSYI2	ED
Symmetric Key Import2 - AESKW	CSNDSYI2 / CSNFSYI2	ED
Symmetric Key Import2 - AESKWCV	CSNDSYI2 / CSNFSYI2	ED
Symmetric Key Import2 - Allow wrapping override keywords	CSNDSYI2 / CSNFSYI2	ED
Symmetric Key Import2 - disallow weak import	CSNDSYI2 / CSNFSYI2	DD, SC
Symmetric Key Import2 – HMAC,PKOAEP2	CSNDSYI2 / CSNFSYI2	ED
TR31 Export – Permit version A TR-31 key blocks	CSNBT31X / CSNET31X	ED
TR31 Export – Permit version B TR-31 key blocks	CSNBT31X / CSNET31X	ED
TR31 Export – Permit version C TR-31 key blocks	CSNBT31X / CSNET31X	ED
TR31 Export – Permit any CCA key if INCL-CV is specified	CSNBT31X / CSNET31X	ED
TR31 Export – Permit KEYGENKY:UKPT to B0	CSNBT31X / CSNET31X	ED
TR31 Export – Permit MAC/MACVER:AMEXCSC to C0:G/C/V	CSNBT31X / CSNET31X	DD
TR31 Export – Permit MAC/MACVER:CVVKEYA to C0:G/C/V	CSNBT31X / CSNET31X	DD
TR31 Export – Permit MAC/MACVER:ANYMAC to C0:G/C/V	CSNBT31X / CSNET31X	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
TR31 Export – Permit DATA to C0:G/C	CSNBT31X / CSNET31X	ED
TR31 Export – Permit ENCIPHER/DECIPHER/CIPHER to D0:E/D/B	CSNBT31X / CSNET31X	ED
TR31 Export – Permit DATA to D0:B	CSNBT31X / CSNET31X	ED
TR31 Export – Permit EXPORTER/OKEYXLAT to K0:E	CSNBT31X / CSNET31X	DD
TR31 Export – Permit IMPORTER/IKEYXLAT to K0:D	CSNBT31X / CSNET31X	DD
TR31 Export – Permit EXPORTER/OKEYXLAT to K1:E	CSNBT31X / CSNET31X	DD
TR31 Export – Permit IMPORTER/IKEYXLAT to K1:D	CSNBT31X / CSNET31X	DD
TR31 Export – Permit MAC/DATA/DATAM to M0:G/C	CSNBT31X / CSNET31X	DD
TR31 Export – Permit MACVER/DATAMV to M0:V	CSNBT31X / CSNET31X	ED
TR31 Export – Permit MAC/DATA/DATAM to M1:G/C	CSNBT31X / CSNET31X	ED
TR31 Export – Permit MACVER/DATAMV to M1:V	CSNBT31X / CSNET31X	ED
TR31 Export – Permit MAC/DATA/DATAM to M3:G/C	CSNBT31X / CSNET31X	ED
TR31 Export – Permit MACVER/DATAMV to M3:V	CSNBT31X / CSNET31X	ED
TR31 Export – Permit OPINENC to P0/E	CSNBT31X / CSNET31X	ED
TR31 Export – Permit IPINENC to P0/D	CSNBT31X / CSNET31X	ED
TR31 Export – Permit PINVER:NO-SPEC to V0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit PINGEN:NO-SPEC to V0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit PINVER:NO-SPEC/IBM-PIN/IBM-PINO to V1	CSNBT31X / CSNET31X	ED
TR31 Export – Permit PINGEN:NO-SPEC/IBM-PIN/ IBM-PINO to V1	CSNBT31X / CSNET31X	ED
TR31 Export – Permit PINVER:NO-SPEC/VISA-PVV to V2	CSNBT31X / CSNET31X	ED
TR31 Export – Permit PINGEN:NO-SPEC/VISA-PVV to V2	CSNBT31X / CSNET31X	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DMV to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DALL to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DMAC to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DMV to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DALL to E0	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DMPIN to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DALL to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DDATA to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DMPIN to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DALL to E1	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E2	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DALL to E2	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DMAC to E2	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL1+DALL to E2	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DATA/MAC/CIPHER/ENCIPHER to E3	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E4	CSNBT31X / CSNET31X	ED
TR31 Export – Permit DKYGENKY:DKYL0+DALL to E4	CSNBT31X / CSNET31X	ED
TR31 Export – Permit DKYGENKY:DKYL0+DEXP to E5	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DMAC to E5	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DDATA to E5	CSNBT31X / CSNET31X	DD
TR31 Export – Permit DKYGENKY:DKYL0+DALL to E5	CSNBT31X / CSNET31X	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
TR31 Export – Permit PINGEN/PINVER to V0/V1/V2:N	CSNBT31X / CSNET31X	DD
TR31 Import – Permit version A TR-31 key blocks	CSNBT31I / CSNET31I	ED
TR31 Import – Permit version B TR-31 key blocks	CSNBT31I / CSNET31I	ED
TR31 Import – Permit version C TR-31 key blocks	CSNBT31I / CSNET31I	ED
TR31 Import – Permit override of default wrapping method	CSNBT31I / CSNET31I	ED
TR31 Import – Permit C0 to MAC/MACVER:CVVKEY-A	CSNBT31I / CSNET31I	DD
TR31 Import – Permit C0 to MAC/MACVER:AMEX-CSC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K0:E to EXPORTER/OKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K0:D to IMPORTER/IKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K0:B to EXPORTER/OKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K0:B to IMPORTER/IKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K1:E to EXPORTER/OKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K1:D to IMPORTER/IKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K1:B to EXPORTER/OKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit K1:B to IMPORTER/IKEYXLAT	CSNBT31I / CSNET31I	DD
TR31 Import – Permit M0/M1/M3 to MAC/MACVER:ANY-MAC	CSNBT31I / CSNET31I	ED
TR31 Import – Permit P0:E to OPINENC	CSNBT31I / CSNET31I	ED
TR31 Import – Permit P0:D to IPINENC	CSNBT31I / CSNET31I	ED
TR31 Import – Permit V0 to PINGEN:NO-SPEC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit V0 to PINVER:NO-SPEC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit V1 to PINGEN:IBM-PIN/IBM-PINO	CSNBT31I / CSNET31I	ED
TR31 Import – Permit V1 to PINVER:IBM-PIN/IBM-PINO	CSNBT31I / CSNET31I	ED
TR31 Import – Permit V2 to PINGEN:VISA-PVV	CSNBT31I / CSNET31I	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
TR31 Import – Permit V2 to PINVER:VISA-PVV	CSNBT31I / CSNET31I	ED
TR31 Import – Permit E0 to DKYGENKY:DKYL0+DMAC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E0 to DKYGENKY:DKYL0+DMV	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E0 to DKYGENKY:DKYL1+DMAC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E0 to DKYGENKY:DKYL1+DMV	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E1 to DKYGENKY:DKYL0+DMPIN	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E1 to DKYGENKY:DKYL0+DDATA	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E1 to DKYGENKY:DKYL1+DMPIN	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E1 to DKYGENKY:DKYL1+DDATA	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E2 to DKYGENKY:DKYL0+DMAC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E2 to DKYGENKY:DKYL1+DMAC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E3 to ENCIPHER	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E4 to DKYGENKY:DKYL0+DDATA	CSNBT31I / CSNET31I	ED
TR31 Import – Permit E5 to DKYGENKY:DKYL0+DMAC	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E5 to DKYGENKY:DKYL0+DDATA	CSNBT31I / CSNET31I	DD
TR31 Import – Permit E5 to DKYGENKY:DKYL0+DEXP	CSNBT31I / CSNET31I	DD
TR31 Import – Permit V0/V1/V2:N to PINGEN/PINVER	CSNBT31I / CSNET31I	DD
Transaction Validation – Generate	CSNBTRV / CSNETRV	ED
Transaction Validation - Verify CSC-3	CSNBTRV / CSNETRV	ED
Transaction Validation - Verify CSC-4	CSNBTRV / CSNETRV	ED
Transaction Validation - Verify CSC-5	CSNBTRV / CSNETRV	ED
Trusted Block Create - Activate an Inactive Trusted Key Block	CSNDTBC / CSNFTBC	ED
Trusted Block Create - Create Trusted Key Block in Inactive Form	CSNDTBC / CSNFTBC	ED
Unique Key Derive	CSNBUKD / CSNEUKD	ED

Table 5. Access control points – Callable Services (continued)

Name	Callable Service	Usage
Unique Key Derive - Allow PIN-DATA processing	CSNBUKD / CSNEUKD	DD
Unique Key Derive - K3IPEK	CSNBUKD / CSNEUKD	DD
Unique Key Derive - Override default wrapping	CSNBUKD / CSNEUKD	ED
VISA CVV Generate	CSNBCSG / CSNECSG	ED
VISA CVV Verify	CSNBCSV / CSNECSV	ED

Printed in USA