z/OS

Cryptographic Services
Integrated Cryptographic Service Facility
DK AES PIN Migrate Support -
APAR OA44444

Contents

Chapter 1. Overview

This document describes changes to the Integrated Cryptographic Service Facility (ICSF) product in support of the German Banking Industry Committee (DK) PIN methods. A new callable service, DK Migrate PIN (CSNBDMP and CSNEDMP), is added which converts existing ISO-1 format PIN blocks to DK PIN blocks.

Note: All crypto coprocessors must be loaded with the same level of code. There have been several licensed internal code (LIC) released in support of the DK PIN methods. Ensure that all of the coprocessors have the same LIC level to support the function you want to use.

These changes are available through the application of the PTF for APAR OA44444 and apply to FMID HCR77A1 and HCR77A0. Note: APAR OA42246 (DK AES PIN Support) and APAR OA43906 (DK AES PIN Part 2 Support) are required prerequisites for this function.

This document contains alterations to information previously presented in the following books:

- *z/OS Cryptographic Services ICSF Application Programmer's Guide*, SC14-7508-00
- *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-00
- *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-00
- *z/OS Cryptographic Services ICSF Overview*, SC14-7505-00

The technical changes made to the ICSF product by the application of the PTF for APAR OA44444 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 DK AES PIN Migrate support provided by this APAR. Refer to this source document if background information is needed.

Introducing Symmetric Key Cryptography and Using Symmetric Key Callable Services

The German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) designed methods of creating, processing, and verifying PINs for its members. The methods use a PIN reference value (PRW) which is generated when a PIN is created or changed and used to verify the PIN supplied in a transaction. The methods are not dependent on a specific cryptographic algorithm, but DK has chosen the AES algorithm for its implementation.

AES Key Types

The following AES key types are added for the DK PIN methods. These key types can only be used with the DK PIN services. The symmetric key management services can be used to generate these key types. The Diversified Key Generate2 service can be used to derive these key types.

DKYGENKY
These keys are used to derive the other key types in this list.

MAC These keys are used to generate and verify message authentication codes. The CMAC algorithm is supported.

PINCALC
These keys are used to generate PINs.

PINPROT
These keys are used to encrypt and decrypt PIN blocks.

PINPRW
These keys are used to generate and verify PIN reference values.

Table 1. Descriptions of AES Key Types and service usage

AES Key Type	Usable with services
Fixed-length AES key-token, version X'04'	
DATA	Symmetric Algorithm Decipher, Symmetric Algorithm Encipher
Variable-length AES key-token, version X'05' *Cipher class (data operation keys)* These keys are used to cipher text.	
CIPHER	Symmetric Algorithm Decipher, Symmetric Algorithm Encipher, Ciphertext Translate2
Key-encrypting key class These keys are used to cipher other keys.	
EXPORTER	Key Generate2, Key Translate2, PKA Key Generate, Symmetric Key Export

Table 1. Descriptions of AES Key Types and service usage (continued)

AES Key Type	Usable with services
IMPORTER	Key Generate2, PKA Key Generate, Key Test2, Key Translate2, Restrict Key Attribute, Secure Key Import2, Symmetric Key Import2
MAC class These keys are used to generate and verify a message authentication code (MAC).	
MAC	DK Deterministic PIN Generate, DK Migrate PIN, DK PIN Change, DK PAN Modify in Transaction, DK PAN Translate, DK PRW Card Number Update, DK PRW CMAC Generate, DK Random PIN Generate, DK Regenerate PRW, MAC Generate2, MAC Verify2
PIN class These keys are used in various financial-PIN processing services.	
PINCALC	DK Deterministic PIN Generate
PINPROT	DK Deterministic PIN Generate, DK Migrate PIN, DK PAN Translate, DK PIN Change, DK PRW Card Number Update, DK Random PIN Generate, DK Regenerate PRW
PINPRW	DK Deterministic PIN Generate, DK Migrate PIN, DK PAN Modify in Transaction, DK PAN Translate, DK PIN Change, DK PIN Verify, DK PRW Card Number Update, DK Random PIN Generate, DK Regenerate PRW
Key generating class These keys are used to derive operational keys.	
DKYGENKY	Diversified Key Generate2

DK PIN methods support

This topic describes the financial services that are based on the PIN methods of and meet the requirements specified by the German Banking Industry Committee, *Die Deutsche Kreditwirtschaft*, also known as DK. The intellectual property rights regarding the methods and specification belongs to the German Banking Industry Committee.

The callable service that supports the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN methods is:

- “DK Migrate PIN (CSNBDMP and CSNEDMP)”

DK Migrate PIN (CSNBDMP and CSNEDMP)

The DK Migrate PIN service is used to generate a PIN reference value (PRW) for an existing ISO-1 formatted PIN block. The PIN reference value is used to verify the PIN in other services.

Financial Services for DK PIN Methods

This section provides information on financial services that are based on the PIN methods of and meet the requirements specified by the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)). DK is an association of the German banking industry. The intellectual property rights regarding the methods and specification belongs to the German Banking Industry Committee.

Note: All crypto coprocessors must be loaded with the same level of code. There have been several licensed internal code (LIC) released in support of the DK PIN methods. Ensure that all of the coprocessors have the same LIC level to support the function you want to use.

The callable service that supports the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN methods is:

- "DK Migrate PIN (CSNBDMP and CSNEDMP)"

DK PIN methods

The DK PIN methods use a PIN Reference Value (PRW) to verify PINs rather than regenerating the PIN from customer account data. The PRW is generated by concatenating the customer PAN data, the issuer card data, the PIN length, the PIN, and a 4-byte random number and encrypting using a PRW key with the GENONLY key usage. The PRW and random number are the output of the generation. The PIN is verified by generating the PRW using a PRW key with the VERIFY key usage and comparing it against the supplied PRW and random number.

DK Migrate PIN (CSNBDMP and CSNEDMP)

Use the DK Migrate PIN callable service to generate the PIN reference value (PRW) for a specified user account. An ISO-1 formatted PIN block is input to determine the value of the PIN for the account. The PIN is reformatted into a DK-defined PIN block and the PIN reference value is calculated using a PRW random value and other account information. The PIN reference value and associated PRW random value are returned to be used as input by other PIN processes to verify the PIN.

If validation of the PIN is desired to personalize smart cards, specify the EPB PIN block output selection rule-array keyword. This keyword causes an output encrypted PIN block to be returned along with a PIN block MAC. The MAC is calculated over the output PIN block and additional card data using the block cipher-based MAC algorithm called CMAC (NIST SP 800-38B).

Note: Regarding weak PINs, this service does not test for weak PINs.

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

Format

```
CALL CSNBDMP(
             return_code,
             reason_code,
             exit_data_length,
             exit_data,
             rule_array_count,
             rule_array,
             PAN_data_length,
             PAN_data,
             card_p_data_length,
             card_p_data,
             card_t_data_length,
             card_t_data,
             ISO1_PIN_block_length,
             ISO1_PIN_block,
             IPIN_encryption_key_identifier_length,
             IPIN_encryption_key_identifier,
             PRW_key_identifier_length,
             PRW_key_identifier,
OPIN_encryption_key_identifier_length,
OPIN_encryption_key_identifier,
OEPB_MAC_key_identifier_length,
OEPB_MAC_key_identifier,
PIN_reference_value_length,
PIN_reference_value,
PRW_random_number_length,
PRW_random_number,
encrypted_PIN_block_length,
encrypted_PIN_block,
PIN_block_MAC_length,
PIN_block_MAC)
```

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. The value must be 0 or 1.

rule_array

Direction	Type
Input	String

Keywords that provide control information to the callable service. The keywords must be in contiguous storage with each of the keywords left-justified in its own 8-byte location and padded on the right with blanks. There are no keywords for this service.

Table 2. Rule array keywords for the DK Migrate PIN service

Keyword	Meaning
PIN Block output selection keyword (One, optional)	
NOEPB	Do not return an encrypted PIN block (EPB). This is the default value.
EPB	Return an encrypted PIN block and a MAC of the encrypted PIN block.

PAN_data_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *PAN_data* parameter. The value must be between 10 and 19, inclusive.

PAN_data

Direction	Type
Input	String

The personal account number in character form which the PIN will be associated. The primary account number, including check digit, should be included.

card_p_data_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *card_p_data* parameter. The value must be between 2 and 256, inclusive.

card_p_data

Direction	Type
Input	String

The time-invariant card data (CDp), determined by the card issuer, which is used to differentiate between multiple cards for one account.

card_t_data_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *card_t_data* parameter. The value must be between 2 and 256, inclusive.

card_t_data

Direction	Type
Input	String

The time-sensitive card data, determined by the card issuer, which, together with the account number and the card_p_data, specifies an individual card.

ISO1_PIN_block_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *ISO1_PIN_block* parameter. This value must be 8.

ISO1_PIN_block

Direction	Type
Input	String

The 8-byte encrypted PIN block with the current PIN in ISO-1 format with the customer chosen PIN. This PIN is used to generate the PIN reference value.

IPIN_encryption_key_identifier_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *IPIN_encryption_key_identifier* parameter. If the *IPIN_encryption_key_identifier* contains a label, the length must be 64. Otherwise, the value must be between the actual length of the token and 725.

IPIN_encryption_key_identifier

Direction	Type
Input/Output	String

The identifier of the key to decrypt the PIN_block containing the IOS-1 PIN. The key identifier is an operational token or the key label of an operational token in key storage. The key algorithm of this key must be DES and the key type must be IPINENC.

If the token supplied was encrypted under the old master key, the token will be returned encrypted under the current master key.

PRW_key_identifier_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *PRW_key_identifier* parameter. If the *PRW_key_identifier* parameter contains a label, the length must be 64. Otherwise, the value must be between the actual length of the token and 725.

PRW_key_identifier

Direction	Type
Input/Output	String

The identifier of the PRW generating key. The key identifier is an operational token or the key label of an operational token in key storage. The key algorithm of this key must be AES, the key type must be PINPRW, and the key usage fields must indicate GENONLY, CMAC, and DKPINOP.

If the token supplied was encrypted under the old master key, the token will be returned encrypted under the current master key.

OPIN_encryption_key_identifier_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *OPIN_encryption_key_identifier* parameter. If the rule array indicates that no encrypted PIN block is to be returned, this value must be 0. If the *OPIN_encryption_key_identifier* parameter contains a label, the length must be 64. Otherwise, the value must be between the actual length of the token and 725.

OPIN_encryption_key_identifier

Direction	Type
Input/Output	String

The identifier of the key to wrap the PIN block. The key identifier is an operational token or the key label of an operational token in key storage. If the rule array indicates that no encrypted PIN block is to be returned, this parameter is ignored. The key algorithm of this key must be AES, the key type must be PINPROT, and the key usage fields must indicate ENCRYPT, CBC, and DKPINOP.

If the token supplied was encrypted under the old master key, the token will be returned encrypted under the current master key.

OEPB_MAC_key_identifier_length

Direction	Type
Input	Integer

Specifies the length in bytes of the *OEPB_MAC_key_identifier* parameter. If the rule array indicates that no encrypted PIN block MAC is to be returned, this value must be 0. If the *OEPB_MAC_key_identifier* parameter contains a label, the length must be 64. Otherwise, the value must be between the actual length of the token and 725.

OEPB_MAC_key_identifier

Direction	Type
Input/Output	String

The identifier of the key to generate the MAC of PIN block. The key identifier is an operational token or the key label of an operational token in key storage. If the rule array indicates that no encrypted PIN block is to be returned, this parameter is ignored. The key algorithm of this key must be AES, the key type must be MAC, and the key usage fields must indicate GENONLY, CMAC, and DKPINOP.

If the token supplied was encrypted under the old master key, the token will be returned encrypted under the current master key.

PIN_reference_value_length

Direction	Type
Input/Output	Integer

Specifies the length in bytes of the *PIN_reference_value* parameter. This value must be 16. On output, *PIN_reference_value_length* will be set to 16.

PIN_reference_value

Direction	Type
Output	String

The 16-byte calculated PIN reference value.

PRW_random_number_length

Direction	Type
Input/Output	Integer

Specifies the length in bytes of the *PRW_random_number* parameter. The value must be 4. On output, *PRW_random_number_length* will be set to 4.

PRW_random_number

Direction	Type
Output	String

The 4-byte random number associated with the PIN reference value.

encrypted_PIN_block_length

Direction	Type
Input/Output	Integer

Specifies the length in bytes of the *encrypted_PIN_block* parameter. If the rule array indicates that no encrypted PIN block should be returned, this value must be 0. Otherwise, it should be at least 32.

encrypted_PIN_block

Direction	Type
Output	String

The 32-byte encrypted PIN block in PBF-1 format. This parameter is ignored if no encrypted PIN block is returned.

PIN_block_MAC_length

Direction	Type
Input/Output	Integer

Specifies the length in bytes of the *PIN_block_MAC* parameter. If the rule_array indicates that no PIN block MAC should be returned, this value must be 0. Otherwise, it must be at least 8.

PIN_block_MAC

Direction	Type
Output	String

The 8-byte CMAC of the encrypted PIN block. This parameter is ignored if no encrypted PIN block is returned.

Usage Notes

SAF may be invoked to verify the caller is authorized to use this callable service, the key label, or internal secure key tokens that are stored in the CKDS.

Access Control Points

The **DK Migrate PIN** access control point in the domain role controls the function of this service.

Required Hardware

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

Table 3. DK Migrate PIN required hardware

Server	Required cryptographic hardware	Restrictions
IBM eServer zSeries 990 IBM eServer zSeries 890		This service is not supported.
IBM System z9 EC IBM System z9 BC		This service is not supported.
IBM System z10 EC IBM System z10 BC		This service is not supported.
IBM zEnterprise 196 IBM zEnterprise 114	Crypto Express3 Coprocessor	DK AES PIN key support requires the June 2014 or later licensed internal code (LIC).
IBM zEnterprise EC12 IBM zEnterprise BC12	Crypto Express3 Coprocessor Crypto Express4 Coprocessor	DK AES PIN key support requires the June 2014 or later licensed internal code (LIC).

Access Control Points and Callable Services

Access to callable services that are executed on a coprocessor is through Access Control Points in the domain role. To execute services on the coprocessor, access control points must be enabled for each service in the domain role. The access control points available depend on the coprocessor you are using.

The TKE workstation allows you to enable or disable access control points. For systems that do not use the optional TKE Workstation, most access control points (current and new) are enabled in the domain role with the appropriate licensed internal code on the coprocessor. The table of access control points lists the default setting of each access control point.

New TKE users and non-TKE users have the default set of access control points enabled. For existing TKE users who have changed the setting of any access control point, any new access control points will not be enabled.

Note: Access control points for ICSF utilities are listed in *z/OS Cryptographic Services ICSF Administrator's Guide*.

If an access control point is disabled, the corresponding ICSF callable service will fail during execution with an access denied error.

The following tables list usage information using the following abbreviations:

AE Always enabled, can not be disabled.

ED Enabled by default.

DD Disabled by default.

SC Usage of this access control point requires special consideration.

Table 4. Access control points – Callable Services

Name	Callable Service	Usage
DK Migrate PIN	CSNBDMP / CSNEDMP	DD

Chapter 3. Update of z/OS Cryptographic Services ICSF Administrator's Guide, SC14-7506-00, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Administrator's Guide*, SC14-7506-00, for the DK AES PIN Migrate support provided by this APAR. Refer to this source document if background information is needed.

Setting up profiles in the CSFSERV general resource class

This topic provides the resource names for the new callable services that support the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN methods:

Table 5. Resource names for ICSF Callable Services

Resource Name	Callable Service Name(s)	Callable Service Description
CSFDMP	CSNBDMP CSNEDMP	DK Migrate PIN

Callable services affected by key store policy

This table provides application programmers guidance on parameters covered by the key store policy controls.

Only the names of the 31-bit versions of the callable services are listed. However, 64-bit versions of the callable services and the ALET qualified versions of the services are also covered by the key store policy. The callable services that are affected by the TOKEN_CHECK key store policy controls are in the table below.

Table 6. Callable services and parameters affected by key store policy

ICSF callable service	31-bit name	Parameter checked
DK Migrate PIN	CSNBDMP	IPINENC_key_identifier PRW_key_identifier OPIN_encryption_key_identifier OEPB_MAC_key_identifier

Chapter 4. Update of z/OS Cryptographic Services ICSF System Programmer's Guide, SC14-7507-00, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF System Programmer's Guide*, SC14-7507-00, for the DK AES PIN Migrate support provided by this APAR. Refer to this source document if background information is needed.

Installation, Initialization, and Customization

This topic provides the updates that support the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN methods.

Parameters in the installation options data set

Table 7. Exit identifiers and exit invocations

Exit identifiers	Exit invocations
CSFDMP	Gets control during the DK Migrate PIN callable service.

Migration

This topic provides the updates that support the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN methods.

Migrating from earlier software releases

These topics describe common activities and considerations that should be considered when you migrate from an earlier release of ICSF to FMID HCR77A1 or HCR77A0.

Callable Services

The following table summarizes the new and changed callable services for ICSF FMID HCR77A1 and HCR77A0. For complete reference information on these callable services, refer to *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Table 8. Summary of new and changed ICSF callable services

Callable service	Release	Description
DK Migrate PIN	HCR77A0	**New:** Generate a PIN reference value (PRW) for an existing IOS-1 PIN block.

CICS Attachment Facility

If you have the CICS Attachment Facility installed and you specify your own CICS wait list data set, you need to modify the wait list data set to include the new callable services.

Modify and include:

- ICSF FMID HCR77A1 only:
  - HCR77A1: CSFAPG, CSFPFO, CSFSXD

- ICSF FMID HCR77A1 and HCR77A0:
  - HCR77A0: CSFCTT2, CSFCTT3, CSFUDK, CSFDPV, CSFDPC, CSFDPMT, CSFDRPG, CSFDKG2, CSFDDPG, CSFDPCG, CSFDPNU, CSFDPT, CSFDRP, CSFMGN2, CSFMGN3, CSFMVR2, CSFMVR3, CSFDMP
  - HCR7790: CSFEDH, CSFT31X, CSFT31I, CSFCKC
  - HCR7780: CSFHMG, CSFHMG1, CSFHMV, CSFHMV1, CSFKGN2, CSFKPI2, CSFKTR2, CSFKYT2, CSFRKA, CSFSKI2, CSFSYI2, CSFKRC2, CSFKRW2
  - HCR7770: CSNBSYD, CSNBSYD1, CSNBSYE, CSNBSYE1, CSFPKT, CSF1DMK, CSF1DVK, CSF1SKD, CSF1SKE, CSF1HMG, CSF1HMV, CSF1OWH, CSF1PRF, CSNBSAD, CSNBSAD1, CSNBSAE, CSNBSAE1, CSFRNGL, CSF1GKP, CSF1GSK, CSF1PKS, CSF1PKV, CSF1SAV, CSF1TRC, CSF1TRD, CSF1UWK, CSF1WPK, CSFTBC, CSFRKX
  - HCR7751: CSNBSAD, CSNBSAD1, CSNBSAE, CSNBSAE1, CSFRNGL, CSF1GKP, CSF1GSK, CSF1PKS, CSF1PKV, CSF1SAV, CSF1TRC, CSF1TRD, CSF1UWK, CSF1WPK, CSFTBC, CSFRKX

Note: If no Wait List is specified, the default wait list will be used. See sample CSFWTL01 for the contents of the default wait list.

Chapter 5. Update of z/OS Cryptographic Services ICSF Overview, SC14-7505-00, information

This topic contains updates to the document *z/OS Cryptographic Services ICSF Overview*, SC14-7505-00, for the DK AES PIN Migrate support provided by this APAR. Refer to this source document if background information is needed.

Standards

The Cryptographic Coprocessor Feature, PCI Cryptographic Coprocessor, and ICSF provide support for these International and USA standards (at least in part):

NIST SP 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

Glossary

Central Credit Committee
The official English name for *Zentraler Kreditausschuss*, also known as ZKA. ZKA was founded in 1932 and was renamed in August 2011 to *Die Deutsche Kreditwirtschaft*, also known as DK. DK is an association of the German banking industry. The hybrid term in English for DK is 'German Banking Industry Committee'.

DK *Die Deutsche Kreditwirtschaft* (German Banking Industry Committee). Formerly known as ZKA.

German Banking Industry Committee
A hybrid term in English for *Die Deutsche Kreditwirtschaft*, also known as DK, an association of the German banking industry. Prior to August 2011, DK was named ZKA for *Zentraler Kreditausschuss*, or Central Credit Committee. ZKA was founded in 1932.

Printed in USA