ICSF

PKDS Key Management Panels- OA15156

Contents

Chapter 1. Introduction

Overview

This document enhances the ICSF utilities panel to provide PKDS key management capability. This new function gives customers the ability to:

- Generate an RSA key pair PKDS record
- Delete an existing PKDS record
- Export an existing public key to an x.509 certificate stored in an MVS physically sequential data set
- Import a public key from an x.509 certificate stored in an MVS physically sequential data set.

These functions are intended for use with the Encryption Facility, but may be used for other purposes. The releases supported are:

- HCR770A
- HCR770B
- HCR7720
- HCR7730.

Chapter 2. ICSF Utilities Panel

PKDS Key Management

Coprocessor Requirements for using the ICSF PKDS Key Management Panels

To use the full function of the ICSF PKDS Key Management panels, you must have a PCICC, PCIXCC, or CEX2C cryptographic coprocessor. If you do not have one of these coprocessors, you cannot generate key pairs using the panels.

Modified Panels

The ICSF utilities panel (CSFUTL00) has a new option 6 PKDSKEYS:

```
CSFUTL00 ---------------- ICSF - Utilities --------------------------
OPTION ===>


Enter the number of the desired option.

  1  ENCODE        -  Encode data
  2  DECODE        -  Decode data
  3  RANDOM        -  Generate a random number
  4  CHECKSUM      -  Generate a checksum and verification and
                      hash pattern
  5  PPKEYS        -  Generate master key values from a pass phrase
  6  PKDSKEYS      -  Manage keys in the PKDS









Press ENTER to go to the selected option.
Press END to exit to the previous menu.

OPTION ===>
```

Figure 1. ICSF Utilities Panel

The ICSF Utilities help panel (CSFUHL00) has also been updated.

New Panels

If option 6 is selected on the utilities panel, a new panel ICSF - PKDS Keys (CSFPKY00) is presented:

```
CSFPKY00 ---------------- ICSF - PKDS Keys -------------------------

    Enter the PKDS record's label for the actions below
     ==>


    Select one of the following actions then press ENTER to process:

    -  Generate a new PKDS key pair record
       Enter the key length  ===>          512, 1024, or 2048
       Enter Private Key Name (optional)
        ==>

    -  Delete the existing public key or key pair PKDS record

    -  Export the PKDS record's public key to a certificate data set
       Enter the DSN  ===>
       Enter desired subject's common name (optional)
        CN=

    -  Create a PKDS public key record from an input certificate.
       Enter the DSN  ===>


COMMAND ===>
```

Figure 2. ICSF (CSFPKY00) PKDS Keys Panel

The (CSFPKY00) PKDS Keys Panel has a new scrollable help panel (CSFPHY00).

From this panel you can manage key entries in the PKDS. To create a new record or manage an existing PKDS record, supply the PKDS key label and then select an action.

Supported actions:

- Generate a new PKDS key pair record
  - The key length in bits must be specified (512, 1024, or 2048).
  - The private key name may also be specified. To learn more see private_key_name in *z/OS Cryptographic Services ICSF Application Programmer's Guide*.
- Delete an existing key record
  - If Delete is selected, a new popup panel Delete PKDS Key Confirmation (CSFPKY0P) is displayed forcing the user to confirm the delete.

  Note: If a PKDS key record, which contains both a public and private key, is deleted, any data encrypted with the private key will no longer be recoverable.
- Export a public key to an X'509' certificate for importation elsewhere
  - The certificate created will be stored in an MVS physical sequential data set.
  - You must supply the data set name where the certificate is to be stored.
  - The data set should not exist prior to export.
    - If the data set exists prior to export, its contents will be destroyed and the data set reallocated new.
  - The data set can not be a PDS or PDS member.

  - You may specify a value for the subject's common name in the certificate, if desired. This can help others identify the owner of the certificate and key.
    - If no value is specified, the PKDS record's label will be used as the common name.
  - The PKDS key record, which contains both a public and private key, must support signing.
  - The certificate created will be self-signed and DER encoded (binary).
- Import a public key from an X'509' certificate received from elsewhere
  - The data set name supplied must contain the certificate
  - The certificate must be a single DER encoded X'509' certificate.
  - Base64 encoded certificates are not supported.
  - The data set containing the certificate must be physical sequential with RECFM(V B).
  - The data set can not be a PDS or PDS member.

  Note: No signature check is performed on the certificate.

When these options are specified and the function is successful, the following panels are generated:

- Generate or Delete - PKDS Key Request Successful Panel (CSFPKY01)
- Export - PKDS Public Key Export Successful Panel (CSFPKY03)
- Import - Public Key Import Successful Panel (CSFPKY05)

RACF Protecting ICSF Services used by the New Panels

ICSF uses the following ICSF callable services to create or delete PKDS records and export or import RSA keys to x.509 certificates:

CSNDKRR
: Ensures that the specified PKDS label does not already exist.

CSNDPKB
: Builds the skeleton key token.

CSNDKRC
: Creates the PKDS record.

CSNKRD
: Deletes the PKDS record.

CSNDKRR
: Reads the record from the PKDS.

CSNDPKX
: Extracts only the public key from the record.

CSNBOWH
: Hashes the to-be-signed portion of the generated certificate.

CSNDDSG
: Signs the hash.

If you are using RACF or a similar security product, ensure that the security administrator authorizes ICSF to use these services and any cryptographic keys that are input. For information about ICSF callable services, see *z/OS Cryptographic Services ICSF Application Programmer's Guide*.

Errors

For the various functions, the following expected errors will generate an error message without presenting a new panel:

1. Panel input errors (e.g., not specifying a PKDS label to work with)
2. ICSF not active
3. Authorization failures (all functions)
4. Incorrect label syntax (all functions)
5. PKDS label already exists (Generate and Import only)
6. PKDS label not found (Delete and Export only)
7. Specifying a PDS member (Import and Export only)
8. Can't export a public key only PKDS record (Export only)

Unexpected ICSF callable service errors from any function, cause the PKDS Key Request Failed Panel (CSFPKY02) to appear.

Non-ICSF related errors for Export cause the PKDS Public Key Export Failure Panel (CSFPKY04) to appear.

Non-ICSF related errors for Import cause the PKDS Public Key Import Failure Panel (CSFPKY06) to appear.

Glossary

This glossary defines terms and abbreviations used in Integrated Cryptographic Service Facility (ICSF). If you do not find the term you are looking for, refer to the index of the appropriate Integrated Cryptographic Service Facility document or view *IBM Glossary of Computing Terms* located at:

`http://www.ibm.com/ibm/terminology`

This glossary includes terms and definitions from:

- *IBM Glossary of Computing Terms*. Definitions are identified by the symbol (D) after the definition.
- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

Definitions specific to the Integrated Cryptographic Services Facility are labeled “In ICSF.”

C

callable service. A predefined sequence of instructions invoked from an application program, using a CALL instruction. In ICSF, callable services perform cryptographic functions and utilities.

cryptography. (1) The transformation of data to conceal its meaning. (2) In computer security, the principles, means, and methods for encrypting plaintext and decrypting ciphertext. (D) (3) In ICSF, the use of cryptography is extended to include the generation and verification of MACs, the generation of MDCs and other one-way hashes, the generation and verification of PINs, and the generation and verification of digital signatures.

D

data set. The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access. (D)

E

encode. (1) To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T) (2) In computer security, to convert plaintext into an unintelligible form by means of a code system. (D) (3) In ICSF, to encipher data by use of a clear key.

exit. (1) To execute an instruction within a portion of a computer program in order to terminate the execution of that portion. Such portions of computer programs include loops, subroutines, modules, and so on. (T) (2) In ICSF, a user-written routine that receives control from the system during a certain point in processing—for example, after an operator issues the START command.

I

ICSF. Integrated Cryptographic Service Facility.

Integrated Cryptographic Service Facility (ICSF). A licensed program that runs under MVS/System Product 3.1.3, or higher, or OS/390 Release 1, or higher, or z/OS, and provides access to the hardware cryptographic feature for programming applications. The combination of the hardware cryptographic feature and ICSF provides secure high-speed cryptographic services.

M

master key. (1) In computer security, the top-level key in a hierarchy of key-encrypting keys. (2) In ICSF, there are three types of master keys on the Cryptographic Coprocessor Feature: the 128-bit DES master key, the 192-bit signature master key, and the 192-bit key management master key. On the PCI Cryptographic Coprocessor there are two types of master keys: the 192-bit Symmetric master key and the 192-bit Asymmetric master key. Master keys are known only to the ICSF hardware and maintained in the cryptographic enclosure in a secure fashion. All keys in operational form in the system are enciphered under a master key. Master keys are used only to encrypt other keys.

P

partitioned data set (PDS). A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. (D)

PCI Cryptographic Coprocessor. The 4758 model 2 standard PCI-bus card supported on the field upgraded IBM S/390 Parallel Enterprise Server - Generation 5, the IBM S/390 Parallel Enterprise Server - Generation 6 and the IBM @server zSeries.

PKDS. Public key data set (PKA cryptographic key data set).

private key. In computer security, a key that is known only to the owner and used with a public key algorithm to decrypt data or generate digital signatures. The data is encrypted and the digital signature is verified using the related public key.

public key. In computer security, a key made available to anyone who wants to encrypt information using the public key algorithm or verify a digital signature generated with the related private key. The encrypted data can be decrypted only by use of the related private key.

R

RSA. Rivest-Shamir-Adleman.

V

verification pattern. An 8-byte pattern that ICSF calculates from the key parts you enter when you enter a master key or clear key. You can use the verification pattern to verify that you have entered the key parts correctly and specified a certain type of key.