



SpanKey™

Cryptographic Key Management System
EMV Chip Card Key Management System

SpanKey Concepts and Facilities

28 July 2010

Version 3.10

Manual Ref: SPK-01-013

Span Software Consultants Limited

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the publisher.

All information contained in this document is subject to change without notice.

All trademarks acknowledged.

SpanKey Concepts and Facilities

Contents

| | | |
|-----|--|--------------------|
| 1 | Introduction. | 5 |
| 1.1 | New in SpanKey Version 3.10. | 6 |
| 1.2 | New in SpanKey Version 3.00. | 6 |
| 1.3 | New in SpanKey Version 2.30. | 7 |
| 1.4 | New in SpanKey Version 2.20. | 8 |
| 2 | Product Highlights. | 9 |
| 3 | Hardware and Software requirements. | 13 |
| 4 | SpanKey Key Management functions.. | 15 |
| 5 | SpanKey Run-time functions.. | 17 |
| 6 | EMV RSA Key Characteristics. | 19 |

1 Introduction

This document describes the main design elements of the SpanKey Cryptographic Key Management system.

SpanKey is a general-purpose Key Management system, and provides a full set of functions for generation and management of cryptographic keys.

Additionally, SpanKey provides many special functions for Chip card processing. SpanKey provides facilities to allow Financial Institutions to issue and manage Chip plastic cards conforming to the EMV standards, and supported by VISA and MasterCard.

SpanKey is designed for large-scale users of cryptography, and for issuers of credit and debit cards. All the processing is performed on an IBM System z mainframe. Many techniques available only on mainframe systems are used to ensure high performance, 100% availability, and reliability. Cryptographic processing is performed securely using the integrated cryptographic co-processors available with these IBM mainframe models.

We believe that SpanKey provides the highest performance, the highest reliability, and the lowest overall cost of ownership, of any comparable system available today.

Manuals for the SpanKey system are:

| | |
|--------|--|
| SPK-01 | SpanKey Concepts and Facilities |
| SPK-02 | SpanKey Administrator's Guide |
| SPK-03 | SpanKey Application Programmer's Guide |
| SPK-04 | SpanKey Messages and Codes |
| SPK-05 | SpanKey Special Edition Guide |
| SPK-06 | SpanKey EMV Card Data Generation Guide |

1.1 New in SpanKey Version 3.10

New features in Version 3.10 of SpanKey include the following:

- Support for 4096-bit RSA keys (on IBM hardware that supports this). Note that EMV standards currently limit EMV keys to 1984 bits.
- Support for CVV processing for card account numbers of any length from 13 to 19 digits (on IBM crypto hardware that supports this).
- It is now possible to use the APPLY option of the GENERATE DESKEY command to install keys from a specific MVS system to a new system.
- Optional tracing of ICSF cryptographic calls issued by SpanKey Application Programming Interface modules.

1.2 New in SpanKey Version 3.00

New features in Version 3.00 of SpanKey include the following:

- Comprehensive automatic EMV Card Data Generation utility. Conversion of magnetic stripe data or database extract files into EMV card production data. Creation of EMV Tag and DGI data elements.
- New SPCACEMV API for creating EMV Tag elements in application programs.
- New "MACK" option for DES key generation simplifies creation of Message Authentication Code keys.
- Support for DUKPT (Derived Unique Key Per Transaction) PIN block encryption in SpanKey APIs.
- API support for SHA-256 hashing algorithm.
- Various improvements and extensions to the TSO/ISPF panel user interface.

1.3 New in SpanKey Version 2.30

New features in Version 2.30 of SpanKey include the following:

- Expiry date support for DES keys.
- Support for customer card account numbers of greater than 16 digits in various SpanKey APIs.
- New Import facility for adding existing non-SpanKey DES keys in the ICSF CKDS to the SpanKey database.
- New COMPAT option for generating DES keys with 8-character names for compatibility with legacy systems.
- Support for creating a new DES key with the same key value as an existing DES key.
- New Report features for DES and RSA keys and certificates allow searching for expired or logically-deleted keys.
- DES keys defined with the MDK option no longer include an EXPORTER variant.
- New TSO/ISPF panel options allow setting the working SpanKey database to match the online system, and define presets for identification values.
- Key Management support for the ICSF PKDS dataset, for storing RSA key tokens.
- Support for cryptographic functionality provided with z/OS 1.6 and later.
- Various improvements and extensions to the TSO/ISPF panel user interface.
- New Dataset Encryption Utility program included with SpanKey.

1.4 New in SpanKey Version 2.20

New features in Version 2.20 of SpanKey include the following:

- RENAME command for DES and RSA keys.
- New SPCACDDG API module and associated test program for creating RSA keys and Certificate data for EMV DDA cards.
- New DDA and CRT options for the Background RSA Key Generation service, to support RSA key pairs for EMV DDA cards.
- Eight-fold increase in the capacity to generate RSA Keys in background, subject to cryptographic hardware and CPU availability.
- New Symmetric Key Import and Export commands. DES keys may be imported and exported encrypted using RSA keys.
- Optional SpanKey SMF records written to record all significant key management events.
- Many SpanKey Application Programming Interfaces may now be tested interactively using the SpanKey TSO/ISPF panel system.
- New TSO/ISPF panel displays the current status of the SpanKey Background RSA Key Generation service.
- Many usability improvements have been made to the SpanKey TSO/ISPF panel system.

2 Product Highlights

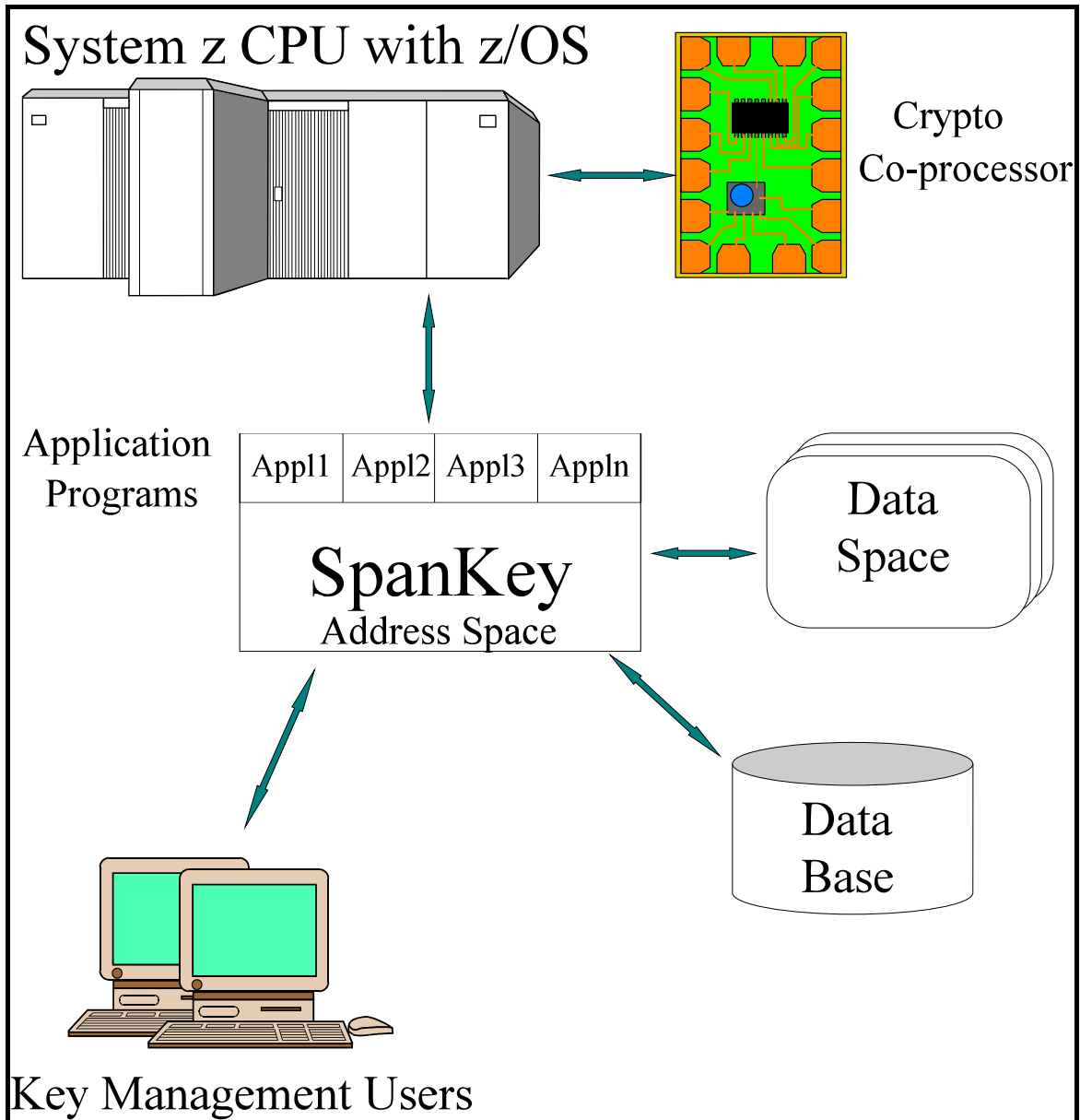
The following are some of the highlights of the features provided in SpanKey Release 3.10:

- Key Management System for all cryptographic keys. Support for symmetric encryption and asymmetric encryption.
- Key Management System for all cryptographic keys used by EMV Chip cards and other banking functions.
- Full Key Management functionality, including support for multiple MVS systems, Import and Export facilities, key database backup and restore, inclusion of existing key values, reporting, etc.
- EMV Card Data Generation system without the requirement for application programming. Fully flexible control by means of parameter statements. Includes support for DDA.
- All cryptographic processing performed in secure hardware on a System z IBM mainframe.
- Management of the contents of the ICSF CKDS and PKDS datasets.
- SpanKey/SE is also available for development and testing without the need for cryptographic hardware. SpanKey/SE can also be used for performing cryptographic processing on IBM-compatible or emulated mainframe systems. Optional emulation of ICSF is provided for systems without cryptographic hardware.
- Offline key definition and generation processes.
- Sophisticated PIN generation and management functions.
- Support for randomly-generated PINs, and PINs derived from account and other data.
- Facility to ensure that both pre-defined and particular dynamically selected PIN values are not issued as customer PINs.
- Online delivery of EMV certificates and generation of chip card data.
- Functions support EMV SDA and DDA options.

- Card issuer RSA key pairs generated, self-signed in both VISA and MasterCard formats.
- RSA Key and Certificate storage database, key management and reporting functions.
- All interchange files that are required for sending issuer keys to card schemes created.
- Interchange files from card schemes containing certified issuer keys processed.
- Certificates for issuer keys cryptographically validated.
- Interchange files containing card scheme public keys processed.
- High performance certificate management and delivery for EMV certificates.
- High volume RSA key generation facility, with instantaneous delivery of unique RSA key pairs to application programs.
- Run time APIs supplied for Digital Signature creation and verification.
- Run time APIs supplied for working key generation, data encryption and message authentication.
- Run time APIs supplied for EMV Unique Derived Key generation, and for VISA Session Key generation.
- Run time APIs supplied for creating EMV DDA RSA keys and card data.
- Run time APIs supplied for PIN generation - all PIN values are held encrypted at all times.
- Run time APIs supplied for PIN derivation and verification - all PIN values are held encrypted at all times.
- Application program support for COBOL, Language Environment and Assembler applications.
- Optional RACF protection for all commands and functions.
- Optional RACF protection of access to certificate and other data from the SpanKey data space.

- Optional RACF protection of access to RSA key generation facility and delivery of RSA key pairs.
- Optional SMF records created for all Key Management change activity.
- Fully panel-driven user interface for all key management functions.
- Interactive enquiry and reporting facilities for all data elements, such as DES and RSA keys, Certificates, PIN tables, Certification Authorities (card schemes), etc.
- Search facilities for keys and Certificates that are expired or logically deleted.
- Test programs are supplied for many encryption and other SpanKey functions.
- Interactive testing and demonstration facilities for SpanKey Application Programming Interfaces.

3 Hardware and Software requirements



SpanKey System Diagram

SpanKey is a z/OS cryptographic application, and requires some minimum levels of hardware and software in order to run.

The minimum CPU configuration is as follows:

IBM S/390 Parallel Enterprise Server Generation 5 processor, with at least one PCICC cryptographic co-processor card and the Triple-DES feature installed.

For the IBM zSeries z890, z990, System z9, System z10 or System z196, at least one PCIXCC, Crypto Express 2 or Crypto Express 3 crypto co-processor is required (as appropriate to the model of processor).

The minimum Operating System configuration is as follows:

IBM z/OS Version 1, with the ICSF (Integrated Cryptographic Service Facility) Cryptographic subsystem.

SpanKey Special Edition will run on any IBM-compatible or emulated mainframe system running z/OS, without any further hardware requirements.

4 SpanKey Key Management functions

SpanKey Key Management functions are performed using utility functions that can be run in a z/OS batch environment, or from a TSO terminal.

All major functions are available from a TSO/ISPF menu- and panel-driven user interface, and the results of user actions can be immediately displayed by using the reporting functions. Full online help is also available.

All key and certificate storage is managed in a central database, with a full set of maintenance and reporting facilities for the database contents.

Standard z/OS dataset management principles can be applied to this database, so that all of the reliability, integrity and availability advantages of using a System z implementation can be exploited.

Commands are provided to perform the following functions:

- Generate, install and manage DES keys of all types.
- Generate issuer EMV RSA public-private key pair, and format the self-signed output file appropriate for VISA or MasterCard.
- Generate a table of PIN values (eg 1234, 9999) that should not be issued as random customer PINs.
- Define a list of allowable PIN values that may be issued as customer PINs.
- Interpret and validate issuer public key certificates received from VISA and MasterCard.
- Interpret and store scheme public key files from VISA and MasterCard.
- Definition and storage of EMV Certification Authority information.
- Storage of user data or other types of RSA public and private key values.
- Import and Export key and certificate values to allow multiple systems to be managed from the same master database.
- Report on database contents.

- Add, Delete and Undelete functions for all database record types.
- Rename functions for cryptographic keys.

Full DES Key Generation and Management facilities:

- Secure generation of random DES key values
- Secure generation of random DES key components
- Application of key values to ICSF Cryptographic Key Dataset (CKDS)
- Support of multiple z/OS systems
- Import keys from other systems
- Export keys to other systems or business partners
- Import keys encrypted under a shared transport key
- Import DES keys encrypted under an RSA public key
- Import keys in component form
- Import existing keys from the ICSF CKDS into the SpanKey key database
- Create and manage keys for "legacy" system components such as VTAM and VSAM.
- All system keys are backed up in the SpanKey database
- Re-encryption of keys to permit periodic master key change
- Full reporting facilities

5 SpanKey Run-time functions

In addition to key and certificate management functions, SpanKey provides run-time support for card processing applications in the z/OS environment.

Use of z/OS features allows SpanKey to provide a highly scalable implementation, where the system capacity is limited only by the power of the hardware used, and not by any inbuilt limitations of the product architecture. For example, there is no limit to the number of parallel application jobstreams that can use SpanKey functions simultaneously.

The SpanKey EMV Certificate server runs as a z/OS Started Task, and manages a Data Space to deliver certificates and other data to running card applications with the highest possible performance. Additional Data Spaces may be created by the SpanKey Started Task in order to provide high-speed generation and delivery of unique RSA key pairs. A set of Application Programming Interfaces (APIs) is provided to allow user programs to take advantage of these system services.

Many of the APIs can be tested and demonstrated interactively, by means of the SpanKey TSO/ISPF user interface, to aid in designing applications and determining business requirements.

Functions provided by these APIs include:

- Fast retrieval of EMV keys or certificate data.
- Fast retrieval of scheme public keys.
- Fast retrieval of user data or other types of RSA public and private key data.
- Fast retrieval of tables of PIN values.
- Creation and Validation of Digital Signatures.
- Generation of random working keys.
- Generation and delivery of unique RSA key pairs.
- Generation of Derived Keys.
- Generation of Session Keys using VISA, MasterCard and EMV2000 standards.

- Generation of random PIN values.
- Derivation of PIN values based on customer account and other data.
- Calculation of PIN offsets for customer-selected PIN values.
- Randomly select customer PIN from a pre-defined list.
- Verification of PINs.
- Check customer-specified PIN against PIN exclusion list.
- Conversion of PIN block formats and re-encryption of PINs.
- Generation of all cryptographic variables for an EMV smartcard.
- Calculation and Verification of VISA CVVs (Card Verification Values) and MasterCard CVCs (Card Verification Codes).
- Calculation and Verification of American Express Card Security Codes (CSCs).
- Triple-DES Encryption and ARPC processing.
- Triple-DES Message Authentication and ARQC processing.
- Secure Hash Algorithms, SHA-1 and SHA-256..
- Creation of EMV Tag data elements.
- Creation of cryptogram for Visa PIN change EMV card script
- Creation of cryptogram for MasterCard PIN change EMV card script
- Character conversion facilities to support ASCII devices and hexadecimal data in character format.

6 EMV RSA Key Characteristics

RSA public-private key pairs used for EMV chip cards must conform to certain characteristics, as defined by the EMV standards.

Self-signed key files and certificates have a unique format, which is specific to the EMV implementation, and is, in fact, different for each card scheme. Creating and analysing these formats require special programming, and the use of cryptographic functions provided by the PCICC (or PCIXCC or CEX2C) card installed in a System z IBM mainframe (or provided in special software supplied with SpanKey/SE).

SpanKey provides all of this functionality, and also allows the definition of the technical characteristics of the RSA keys used (exponent value, modulus length, etc). Different key lengths for issuer keys require certificates built with different lengths of scheme key, and it is possible for the same issuer key to be used with multiple scheme keys to produce certificates of different lengths.

The industry trend is for the key lengths of RSA keys to increase over time, in order to ensure that the cryptographic strength of the protection provided can be maintained in the face of ever-increasing computer processing power, and the increasing sophistication of the perpetrators of credit and debit card fraud.

As standards evolve and change, SpanKey will be updated to ensure that support for changes in cryptography, and for the introduction of new card products, is always available.



For further information, please contact:

Span Software Consultants Limited
Little Moss, Peacock Lane
High Legh
Knutsford
Cheshire
WA16 6PL
England

Tel: +44/0 1565 832999
Fax: +44/0 1565 830653
Email: sales@spansoftware.com
www.spansoftware.com