Span Software

SpanKey™ & SpanKey/SE™

Cryptographic Key Management System

EMV Chip Card Key Management System

PIN Processing System

www.spansoftware.com

Span Software

SpanKey

Topics

- Introduction
- Overview
- Span Software
- SpanKey Features
- Future direction
- Discussion
- Live Demonstration

Span Software

SpanKey

Product Components

- DES Key Management System
- RSA Key Management System
- EMV Key Management System
- EMV Card Data Generation System
- Debit and Credit card PIN Processing
- High-performance Application Programming Interfaces for all cryptographic functions
- High-performance Application Programming Interfaces for all EMV functions

Span Software

SpanKey

Mainframe-based commercial-quality software product
by Span Software Consultants Limited

- Pure System z product (z/OS)
- High performance
- High reliability
- High availability
- Security via RACF
- All Crypto performed in internal IBM hardware via ICSF with PCIXCC or CEX2C
- Installation and maintenance via SMP/E

or... SpanKey/SE

Span Software

Mainframe-based commercial-quality software product
by Span Software Consultants Limited

- Pure System z product (z/OS)
- High performance
- High reliability
- High availability
- Security via RACF
- Crypto in software - no hardware needed
- Installation and maintenance via SMP/E

Span Software

SpanKey

Mainframe-based commercial-quality software product

- All cryptographic keys are generated, stored and managed on the mainframe – keys and customer data never need leave the z/OS environment
- All SpanKey software is written in assembler for maximum performance and compatibility with all environments
- All cryptographic processing uses IBM hardware internal to the CPU
- No assumptions made about customer applications - SpanKey does not require any external database software and retrieves its data with typical access times of well under a millisecond (including RACF checks)
- SpanKey works within customers' existing standards for data backup, naming conventions, access control, etc
- SpanKey is designed for 100% system availability

Span Software

Span Software Consultants Limited

Profile

- Suppliers of consultancy services and MVS system software
- Established in 1976
- More than 30 years of experience in developing and supporting MVS software products

Span Software Consultants

Commercial software products - 1

- **SPANEX** program and job execution services, development tools
  - Job scheduling and automatic job restart
  - Many development and run-time execution tools
- **SPICE/DLI** automated restart and recovery for database applications
  - IMS version of well-established program development and automatic restart tool
  - Used by major corporations world-wide
- **SPICE/SQL** automated restart and recovery for database applications
  - DB2 version of program automatic restart tool
  - Used world-wide by major corporations and banks
- **BEARS/IMS** IMS performance and usage monitor
  - Performance measurement for the largest IMS systems
  - Also used for cross-charging of IMS transactions

Span Software Consultants

Commercial software products - 2

- **EMV Issuer's Companion** toolkit for card issuers and those working with EMV
  - DES Debugger (Data Encryption Standard Testing Tool)
  - Big Maths (Multiple Precision Arithmetic)
  - Cert Auth (Dummy Certification Authority for EMV Issuer RSA Keys)
  - List File (Browse, Print and Compare files)
  - Test PIN (Perform PIN Processing operations)
  - Session Key (Compute EMV 2000 Session Keys)
  - Generate RSA Keys in Chinese Remainder Theorem (CRT) format

SpanKey Features

Span Software

Hardware and Software Requirements for SpanKey

- IBM System z processor
- At least one cryptographic co-processor
- zSeries z890, z990, System z9 or z10 requires PCIXCC or CEX2C crypto adapter, as appropriate
- Triple-DES feature
- z/OS
- ICSF
- RACF or equivalent

SpanKey Features

Span Software

Hardware and Software Requirements for SpanKey/SE

- Any IBM, IBM-compatible or emulated mainframe processor
- z/OS
- RACF or equivalent

SpanKey Features

Span Software

Facilities Provided

- Key and Certificate database
- MVS Data Space provides instantaneous access to keys, RSA Certificates, PIN tables, etc
- RSA Key Generation and Management
- Data interchange with VISA and MasterCard
- High-performance Run-time APIs for all crypto, PIN and EMV functions
- Provides all functions for card issuing and transaction processing
- Automatic creation of EMV card production data
- Dataset encryption utility

SpanKey Features

Span Software

EMV Features

- Installs and stores Card Scheme public keys
- Generates issuer RSA keys, ICC and PIN Encipherment RSA keys
- Formats self-signed public key files for Card Schemes
- Formats hash files for Card Schemes
- Cryptographically verifies public key certificates signed by Card Schemes
- Installs and stores issuer certificates
- Provides application interfaces to cryptographic functions
- Creates EMV card production data from input file (database extract or magnetic stripe data) and user-specified parameters
- Infinitely scalable
- Supports all environments (eg batch, TSO, IMS, IMSFP, CICS)

SpanKey Features

Span Software

Other Features - 1

- DES and RSA Key Management System
  - Generates and stores DES keys and definitions
  - Generates DES key components
  - Installs DES keys in ICSF CKDS
  - Supports multiple MVS systems and CKDSs
  - Generates and manages RSA keys and certificates
  - Exports keys for other systems
  - Imports keys from other systems
  - Imports keys in component form (dual-control supported)
  - Imports existing DES keys from CKDS
- Stores and delivers user-defined data
- Comprehensive reporting facilities
- Database export/import facilities
- Re-encrypt facility for database contents

SpanKey Features

Span Software

Other Features - 2

- PIN Processing
  - Random customer PIN generation in hardware
  - PINs and offset values derived from account and other data
  - PVVs generated and verified
  - PINs never revealed in clear
  - Supports PIN lengths from 4 to 12 digits
  - Supports PIN encryption with DUKPT key
- PIN Exclusion table (for random PINs)
  - Generated offline, loaded into SpanKey Data Space
  - Contains undesirable customer PIN values (eg 1234, 9999)
  - Can include “wild card” characters
  - Accessed at run-time to eliminate easily guessed PINs
  - Additional card-specific PINs can be excluded at run-time
  - Can be used to reject customer-selected PINs
  - All processing performed on encrypted PIN values

SpanKey Features

Span Software

Other Features - 3

- ISPF/TSO Panel-driven user interface
  - Very easy to use and to understand
  - Minimal training required for users
  - All standard key management functions can be performed interactively
  - Results of actions can be displayed immediately
  - Key changes can be applied to the system instantly
  - Full RACF control of user functions
  - Full interactive Help system
  - Interactive testing and demonstration facilities for many SpanKey APIs

SpanKey Features

Span Software

Primary Option Menu Screen-shot

```
----------------- SpanKey Cryptographic Key Management System ----------------
  Command ===>

  Select option from the list below:

      1    Define new SpanKey key or resource
      2    Delete existing SpanKey key or resource
      3    Generate a cryptographic key or DES key PIN table
      4    Validate an EMV RSA key
      5    Install Certification Authority Public Key
      6    Import commands
      7    Export commands
      8    Report SpanKey resources
      9    Test SpanKey Application Programming Interfaces

      M    More SpanKey facilities

      X    Exit SpanKey menu

      Specify SpanKey Database name:
              SPANKEY.DATABASE

              Copyright (c) 2008 Span Software Consultants Limited
```

SpanKey Features

Span Software

Application Program Interfaces - 1

- Card Verification Value (CVV, CVC) Calculations
- Card Security Code (AmEx CSC) Calculations
- Triple DES Encryption and ARPC
- Triple DES Message Authentication and ARQC
- Secure Hash Algorithms
- Read data from SpanKey Data Space (eg RSA Certificates, User data, PIN Exclusion tables, etc)

Span Software

SpanKey Features

Application Program Interfaces - 2

- PIN processing:
  - Generate random PIN
  - Derive PIN from account and other data
  - Calculate PIN offset for customer-selected PIN
  - Verify PIN from account, offset and other data
  - Select PIN from PIN List
  - Validate customer-selected PIN against PIN Exclusion List
  - PIN block translate or reformat
  - Generate PVV
  - Verify PVV

SpanKey Features

Span Software

Application Program Interfaces - 3

- EMV API facilities:
  - Generate Digital Signature
  - Verify Digital Signature
  - Generate EMV Card Keys
  - Create EMV Unique Derived Key (UDK)
  - Create EMV Tag Element
  - Create VISA session key for card script processing
  - Create MasterCard session key for card script processing
  - Generate script cryptogram for VISA PIN change
  - Generate script cryptogram for MasterCard PIN change
  - Generate script cryptogram for EMV2000 PIN change
  - Generate DDA data (ICC RSA key and certificate, ICC PIN Encipherment key and certificate)
- Ultra-high speed RSA key generation/delivery (eg for DDA)
- Character conversions

SpanKey Features

Span Software

API Testing Menu Screen-shot

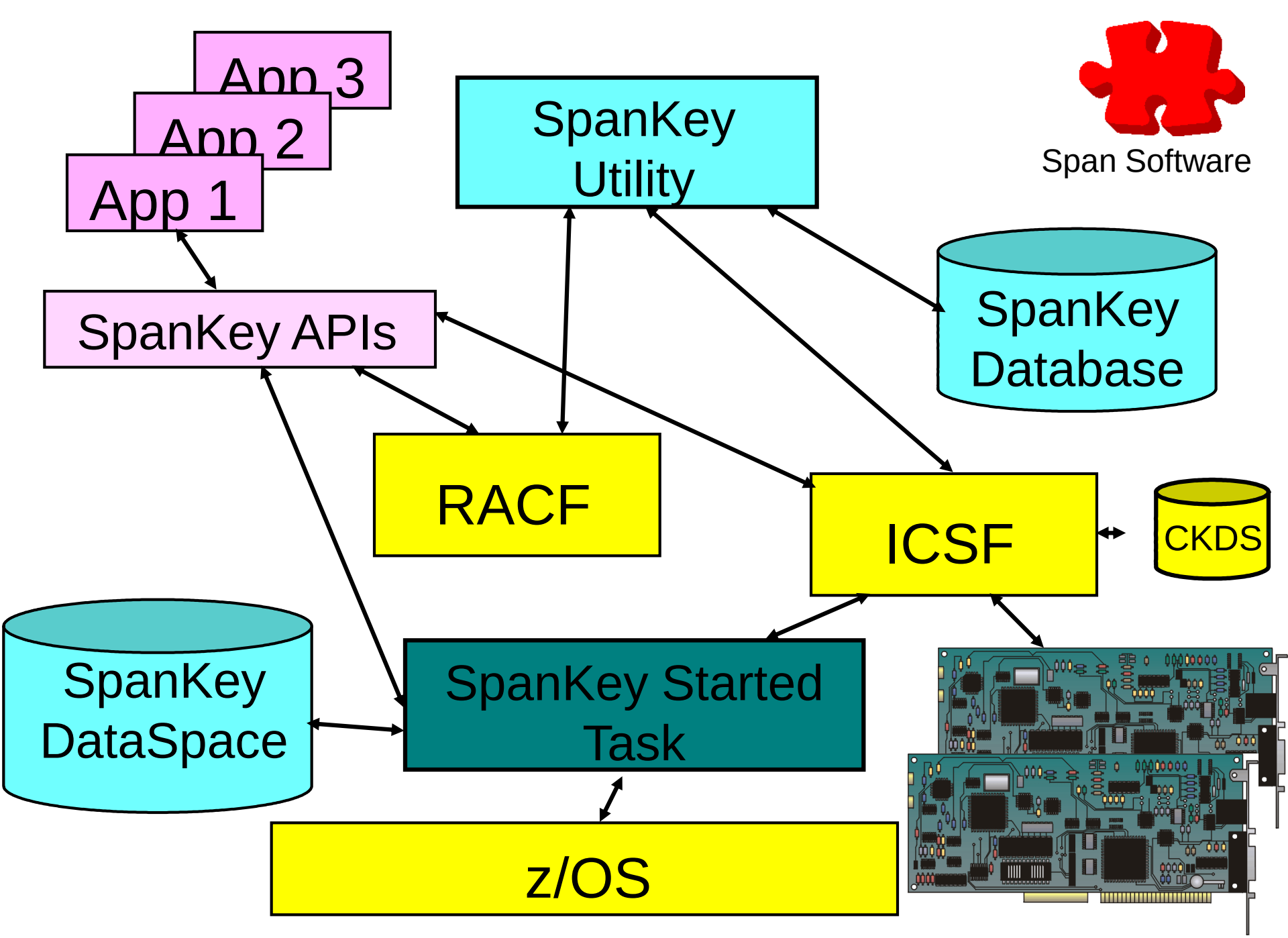
```
----------------- SpanKey Cryptographic Key Management System -----------------
--------------- Test SpanKey Application Programming Interfaces ---------------
 Command ===>

 Select option from the list below:

     0    Test SPCACDRD API (Read data from SpanKey Data Space)

     1    Test SPCACCSC API (American Express Card Security Codes)
     2    Test SPCACCVV API (VISA and MasterCard Verification Values)
     3    Test SPCACDDG API (DDA Data Generation)
     4    Test SPCACDES API (DES Encryption and Decryption, and ARPC)
     5    Test SPCACDPN API (Generate Derived PIN)
     6    Test SPCACDPN API (Generate PIN Verification Value)
     7    Test SPCACEMV API (EMV Tag Creation)
     8    Test SPCACFRG API (Fast RSA Key Generation)
     9    Test SPCACGWK API (Generate Working DES Key)
    10    Test SPCACMAC API (Triple DES MAC and ARQC)
    11    Test SPCACSPL API (Select PIN from List)
    12    Test SPCACSSR API (Special Script functions)
    13    Test SPCACUDK API (Unique Derived Key)
    14    Test SPCACVSK API (VISA or MasterCard Session Key)

     X    Return to SpanKey Primary Option Menu
```


App 3
App 2
App 1
SpanKey Utility
Span Software
SpanKey APIs
SpanKey Database
RACF
ICSF
CKDS
SpanKey DataSpace
SpanKey Started Task
z/OS

Span Software

SpanKey

Sample Commands
(Commands can also be performed interactively)

To create a VISA Master Derivation Key:

```
GENERATE DESKEY NAME(FRED) MDK
```

To add all DES keys to a new MVS system:

```
GENERATE DESKEY APPLY NAME(ALL)
```

To create a PIN Exclusion Table:

```
GENERATE PINTABLE NAME(BERT)
         TYPE(STANDARD 7283 911*)
```

SpanKey/SE

Span Software

Further Information

- SpanKey/SE has all the functionality of SpanKey, but does not use ICSF or its CKDS
  - Encrypted keys are stored in the SpanKey/SE database
  - Keys can be transferred between products using Import/Export features
- Other security and Access Control is as for SpanKey
- Optional ICSF Emulation for use of ICSF APIs
- SpanKey/SE is ideal for:
  - Evaluating the SpanKey product range
  - Evaluating the use of the mainframe
  - Application development and testing
  - Minimising hardware costs

Span Software

EMV Card Data Generation

- Automatic generation of EMV chip card data
  - Input: Magnetic-stripe card production file

    or
  - Input: Customer/cardholder database extract file containing relevant details – any file format
  - Output: EMV chip card production file
  - No Application Programming required
  - Completely flexible EMV tag and data creation
  - Pure z/OS mainframe implementation
  - Very fast!

Span Software

SpanKey

Questions and Discussion

Span Software

New features

New features in the current Version 3.1 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.
- Automatically add new data to existing EMV card production files (eg convert from SDA to DDA).
- New SPCACEMV API for creating EMV Tag elements in application programs.
- New support for DUKPT PIN block encryption in SpanKey PIN APIs
- New “MACK” option for DES key generation simplifies creation of Message Authentication Code keys.
- API support for SHA-256 hashing algorithm.
- Support for dual-control of DES key components
- Support for RSA keys up to 4096 bits
- Various improvements and extensions to the TSO/ISPF panel user interface.