IBM Software Group

IBM Data Encryption for IMS and DB2

Sonia Márquez Paz
sonia_marquez@es.ibm.com

Information Management
software

Agenda

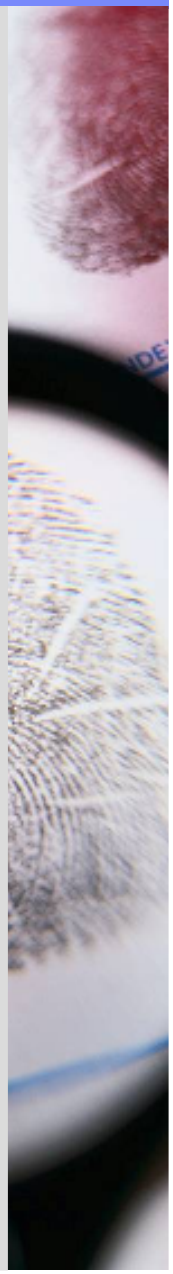
- Introducción:
  - La importancia y necesidad de Cifrado
- IBM Data Encryption for IMS and DB2 Databases
- Secure Keys vs Clear Keys
- Un ejemplo actual: PCI
- Enlaces de interés

Introducción: La importancia y necesidad de cifrado

- Actualmente, existen múltiples normas y regulaciones que requieren que se cifren ciertos datos.
  - **PCI Data Security Standards**, de la industria de tarjetas de pago.
    - https://www.pcisecuritystandards.org/
  - **Regulaciones Gubernamentales**
    - Sarbanes-Oxley, HIPAA y otras
  - **European Union Privacy Directive**
  - Posibles nuevas regulaciones de UK a consecuencia de incidentes de pérdida de datos
  - **ISO 27001, ISO 27002**
- Con frecuencia se requiere que los datos estén cifrados, pero no se indica cómo se debe realizar o cuáles son las amenazas más habituales.
- Los entornos con sistemas z (particularmente z/OS) disponen de muchos mecanismos para proporcionar cifrado.

¿Cuáles son las principales amenazas?

- ***Revelación***
  - Los datos pueden estar disponibles para ser examinados por personal no autorizado.
  - Los datos cambiados pueden volver a su valor original, pero no hay manera de deshacer el hecho de “ver” datos.
  - El examen de los datos no muestra qué ha sido visto, ni quién los vio (a no ser que se disponga de mecanismos de **auditoría**).
- ***Modificación Deliberada***
  - Los datos pueden ser cambiados de manera consciente por personal no autorizado.
  - Se incluyen los cambios deliberados para sustraer información, etc.
- ***Corrupción Accidental***
  - Los datos pueden ser modificados accidentalmente por personal no autorizado.
  - Una vez corrompidos los datos, pueden perder su utilidad.
- ***Destrucción***
  - Los datos pueden destruirse físicamente o ser sobreescritos.



Cifrado de Datos

Un imperativo de negocio

- Las empresas se están centrando, de manera proactiva, en asegurar y proteger los datos de clientes y de negocio:
  - Aumenta el número de regulaciones que solicitan la protección y seguridad de datos para auditoría y cumplimiento de normativas.
  - Numerosos eventos recientes demuestran el impacto de la pérdida/sustracción de datos.
  - Los requisitos para una seguridad más estricta dan lugar a la necesidad de cifrar datos.

Data Governance

Impactos potenciales de una exposición o ataque a los datos

- **Tendencias en brechas de Seguridad**
  - El porcentaje de incidencia ha disminuido
  - La severidad de los ataques ha aumentado
  - El porcentaje del presupuesto dedicado a seguridad ha aumentado
- **Confianza de clientes e inversores**
  - 77% de un total de 2.750 clientes dejarían de hacer negocio con compañías que hayan sufrido ataques a sus datos **
- **Disminución de la ventaja competitiva**
- **Pérdida de negocio**
  - 1/3 de las compañías podrían quedarse sin negocio como resultado de un incidente de seguridad severo *

Year	Major Security Breaches *(1000 companies)*	Severity of Security Breaches *(Scale 1-10)*	% of Budget on Security
2006	34%	4.8	20%
2005	38%	2.6	15%
2004	58%	2.3	12%

Otras tendencias clave

- 44% considera los accesos por usuarios autorizados como el mayor reto de seguridad
- El coste medio de un incidente de seguridad en 2006 fue de 369.388 $

Computing Technology Industry Association (CompTIA) study

** McAfee Survey*
***Javelin Strategy & Research*

Principales Normativas relacionadas con la Privacidad

Sarbanes-Oxley (SEC)	Publicly traded companies	Integrity of financial data/Confidentiality of forward looking financial data/Protect valuable assets
HIPAA (CMS)	Organizations that handle patient health information	Confidentiality, integrity and availability of patient health information
Data Breach Disclosure (30+ States) SB 1386	Collect information about US Residents	Notifications and investigations of security breach of Personally Identifiable Information
FISMA (OMB)	Federal Agencies	Complete security program based on NIST (National Institute of Standards and Technology) guidelines
NERC/FERC (NERC)	Power Companies	Protection of US power systems
Gramm-Leach-Bliley (SEC, FTC, FDIC…)	Credit card issuers All financial services.	Protection of consumer information
PCI (Visa, MC, Discover, AMEX)	Major retailers and processors	Protection of credit card data

¿Por qué cifrar datos DB2?

- El DB2 proporciona mecanismos de seguridad tales como autorización nativa DB2 (grant/revoke), autorizaciones Secundarias DB2, e interfaz DB2/RACF.
- Las Aplicaciones que pueden acceder a los datos a través de varios mecanismos (attach) también están protegidos, habitualmente a través de la autenticación RACF (signon).
- El Acceso a los datases VSAM lineales que están por debajo, y a los datos de las Image Copies, suele estar controlado mediante RACF (dataset access control).
- Pero …

Se elude la protección RACF

...hay gente que puede entrar en el Sistema Operativo y ver los datos en los almacenamientos DASD

- Personal (proveedor de almacenamiento) que soporta el hardware del subsistema DASD (p.ej. IBM, EMC o Hitachi)
- ¿Qué sucede con soportes expirados tales como CTAPE?
- ¿Qué sucede cuando hardware DASD se actualiza y reemplaza?
- Cada vez que se que se envían datos fuera de la instalación para archivado o para propósitos de backup/recovery, hay un riesgo…
- Ataques internos por parte del personal que dispone de todos los permisos para poder acceder a los datos (usuarios privilegiados)

IBM Data Encryption for IMS and DB2 Databases

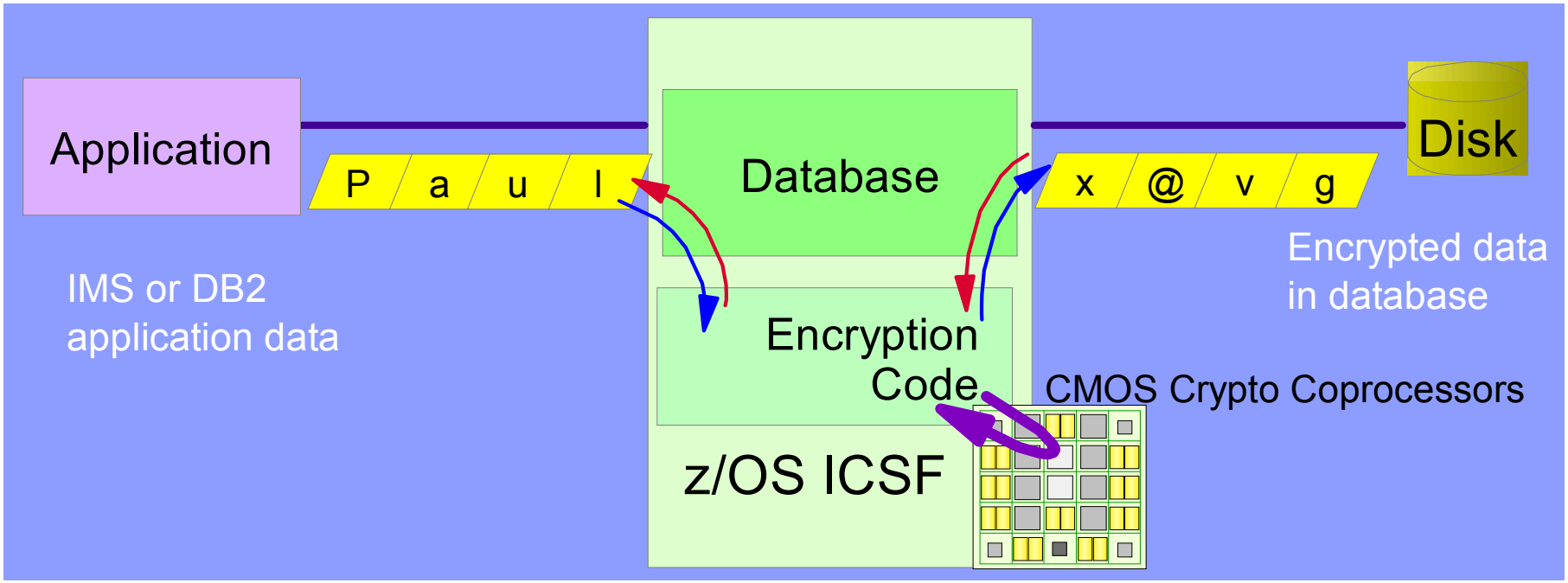
Qué ofrece

- Cifra la información de tablas y backups offline de las bases de datos sin penalizar el rendimiento.

Beneficios

- Ayuda a mantener el cumplimiento de normativas gubernamentales y de protección de datos en diversos ámbitos de negocio (como el estándar PCI).
- Protege los datos frente a la exposición en el caso de una brecha de seguridad.
- Minimiza el riesgo de seguridad que supone la exposición indeseada de los datos de backup y replicados si se pierden o son sustraídos.

Cifrado de Datos



Durante el cifrado, los datos de aplicación IMS o DB2 ("paul") se convierten en otros en la base de datos, que son ininteligibles ("x@vg") excepto para la persona que tiene la clave de cifrado y puede, por lo tanto, descifrar los datos. Esta clave la asigna el administrador de seguridad.

IBM Data Encryption for IMS and DB2 Databases

Características

- **Cifrado a nivel de tabla DB2 o segmento IMS**
- **Soporta todas las versiones de DB2**
- **No necesita cambios en la aplicación**
  - Las aplicaciones no necesitan conocer las claves
- **Soporta cifrado de tipo *secure key* y *clear key***
- **Compatible con utilidades DB2 Load/Unload y DB2 Tools**
- **El rendimiento es similar a la compresión de datos a nivel de fila**
- **El acceso a índices no se ve afectado por el cifrado**

IBM Encryption for IMS and DB2 Databases

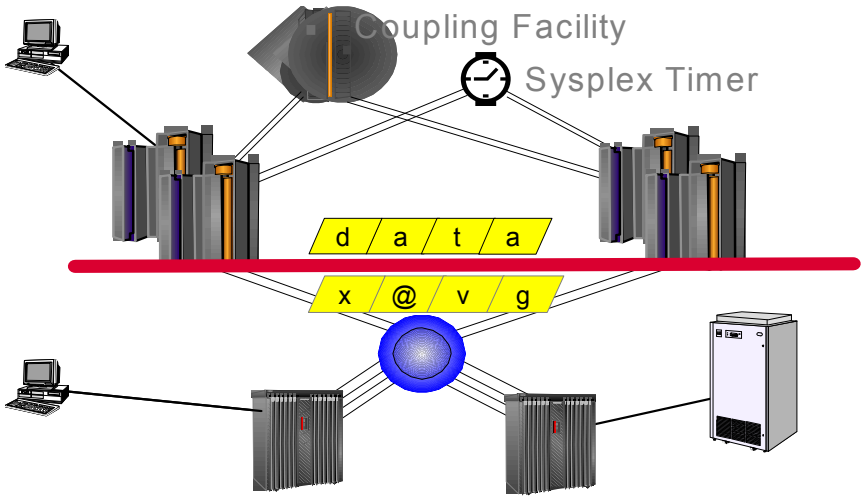
Características

- **Utiliza exits customizadas pre-codificadas**
  - Segmento IMS
  - Tabla DB2
- **Explota las características Criptográficas de zSeries (ICSF), que se traducen en un proceso de cifrado/descifrado de bajo overhead.**
- **Utiliza el ANSI Data Encryption Algorithm (DEA), también conocido como el algoritmo Data Encryption Standard (DES) del U.S. National Institute of Science and Technology (NIST). También permite cifrar con algoritmos AES.**
- **Posibilidad de Cifrado con soporte Crypto Express3 (CPACF Protected Key)**

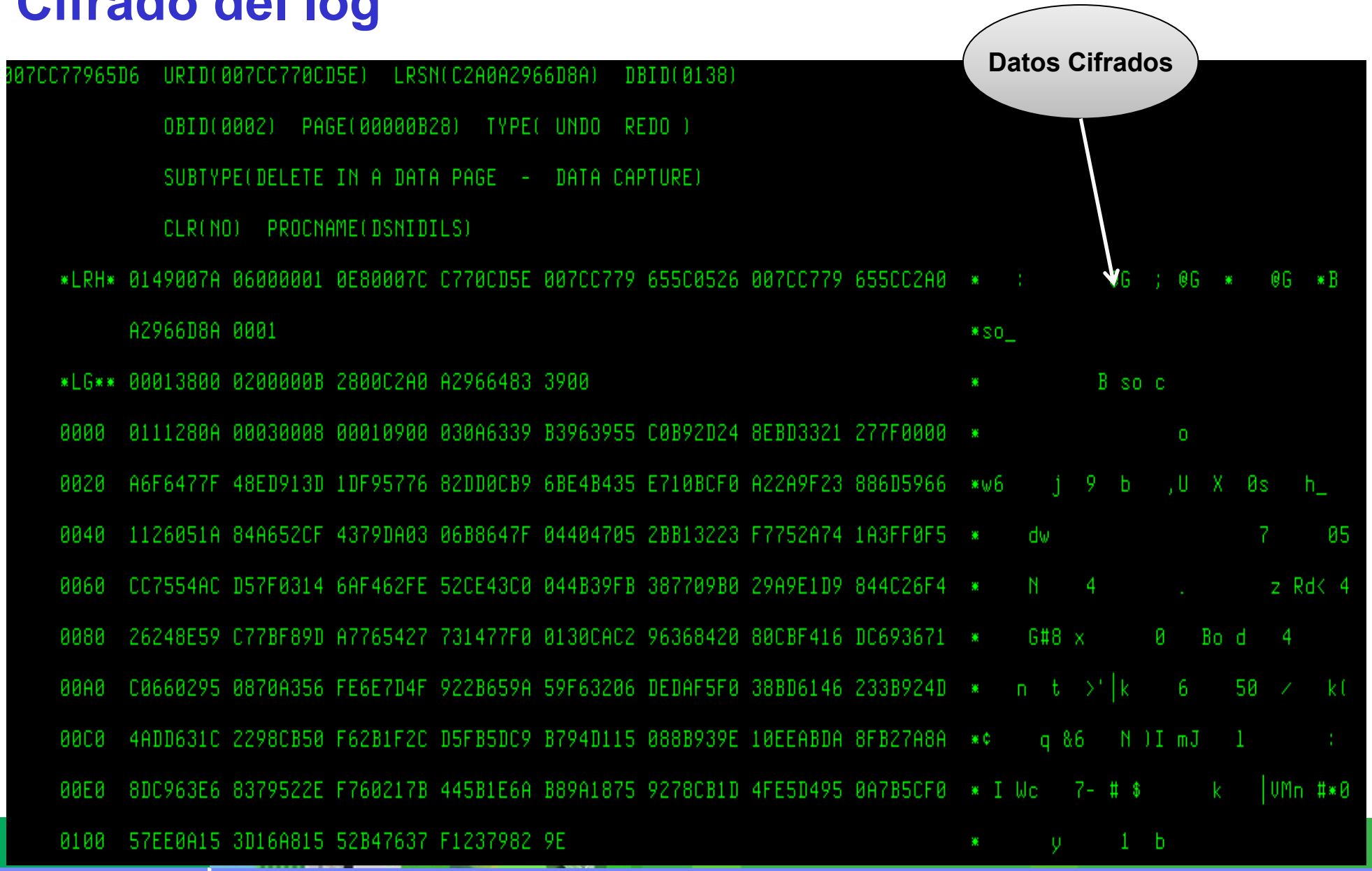
IBM Data Encryption for IMS and DB2 Databases

Protección proporcionada

- **Datos cifrados en disco**
  - Datos en el canal cifrados (protege contra los sniffers de canal/red)
  - Datos en buffers no cifrados
- **Los controles de autorizaciones existentes que acceden a estos datos no se ven afectados.**
- **Se asume que el acceso se realiza a través del Gestor de Base de Datos, o mediante acceso directo que invoca las exits de datos del Gestor.**



Cifrado del log



Retos relacionados con el cifrado de datos

- **Overhead en Rendimiento**
  - El menor overhead por cifrado posible.
  - Usa cifrado hardware on-board.
  - Mucho más rápido que el software de cifrado.
  - Más rápido que el cifrado hardware off-board (PCI card).
  - Posibilidad de seguir usando zIIPs cuando proceda.
- **Gestión de Claves**
  - No se requiere gran inversión para su aprendizaje.
  - Utiliza los servicios criptográficos existentes (ICSF) para gestionar las claves de encriptación en un repositorio central.
- **Cambios en las Aplicaciones**
  - No se requieren cambios en las aplicaciones - no hay intercambio de passwords.
  - Cambios de administración de sistemas que afectan sólo a la definición de la tabla o segmento.

IBM Data Encryption Tool for DB2 and IMS

Interfaz ISPF – Panel de entrada

```
*************************************************************
DECPMAIN     DATA ENCRYPTION FOR IMS AND DB2 DATABASES - PK69786

Command ===>

Select an OPTION to continue or END to exit

OPTION . .  2

     1  Build a standalone encryption DB2 EDITPROC or IMS exit

     2  Build a DB2 compression/encryption EDITPROC

     3  Build an IMS compression/encryption exit

*************************************************************
```

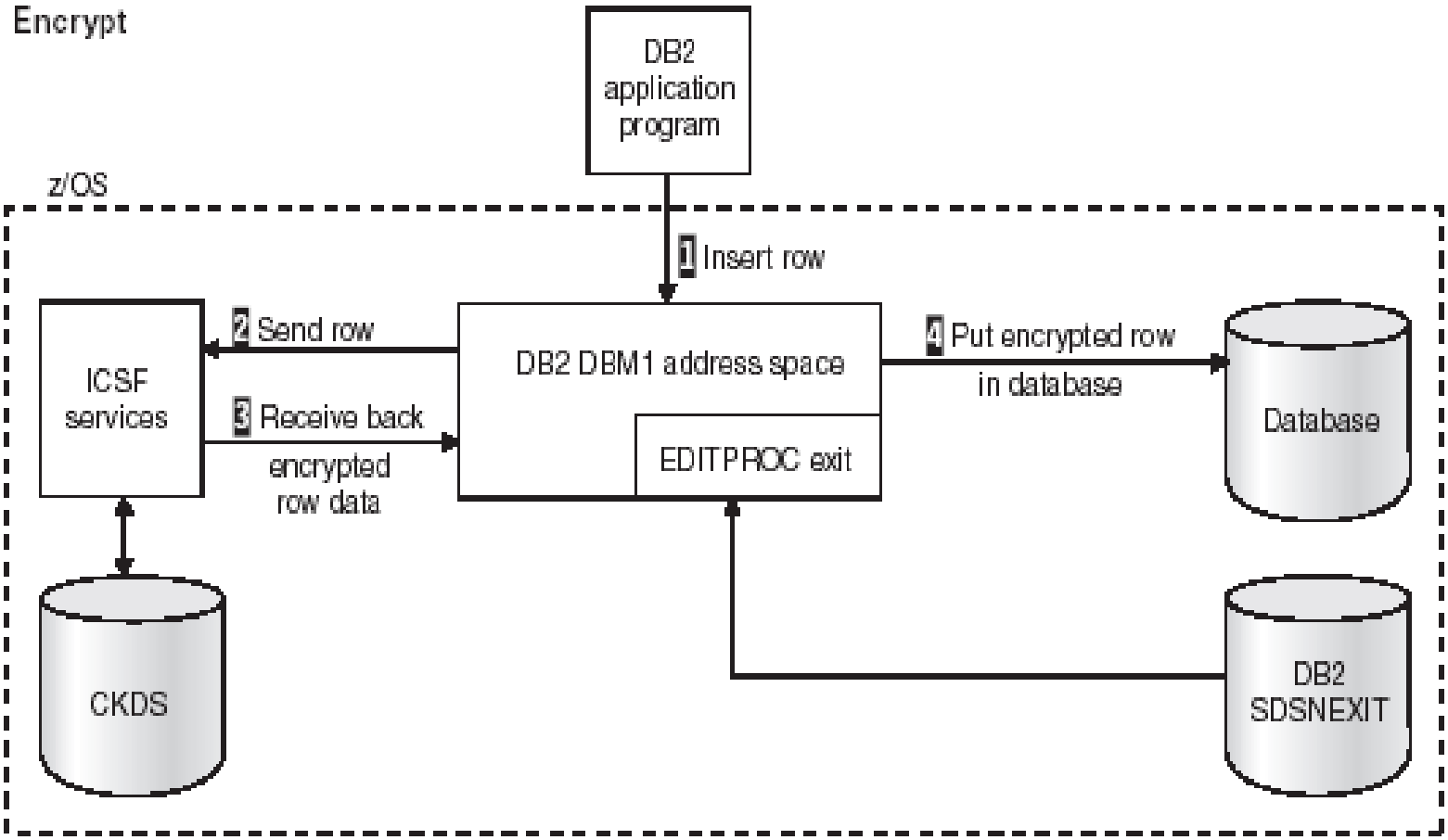
IBM Data Encryption Tool for DB2 and IMS

Interfaz *ISPF – Panel de cifrado*

```
              DATA ENCRYPTION FOR IMS AND DB2 DATABASES

 Command ===>

 Press ENTER to continue or END to exit

 Specify ICSF encryption key to be implemented.
 Key label . . DB2ICSFKEY

Specify 1 - IMS or DB2 SECURE KEY  3 - IMS DES CLEAR KEY
        2 - DB2 CLEAR KEY non-CPK  4 - IMS AES SECURE KEY
        5 - DB2 SECURE KEY CPK                          . .
Database management system                             . .       (IMS or DB2)
 Specify encryption JCL parameters.
Jobcard   . . //BILDDECX JOB (userid),
          . . //'user',REGION=0M,TIME=5,MSGCLASS=H,
          . . // NOTIFY=userid,CLASS=A
          . .
          . .
 CSF lib   . . SYS1.LINKLIB
 ZAP lib   . . SYS1.MIGLIB
 SMP lib   . . HCO.DEC.ADECLMD0
 Exit lib  . . HCO.DEC.SDECLMD0
 Exit name . . AIMSEXIT
```

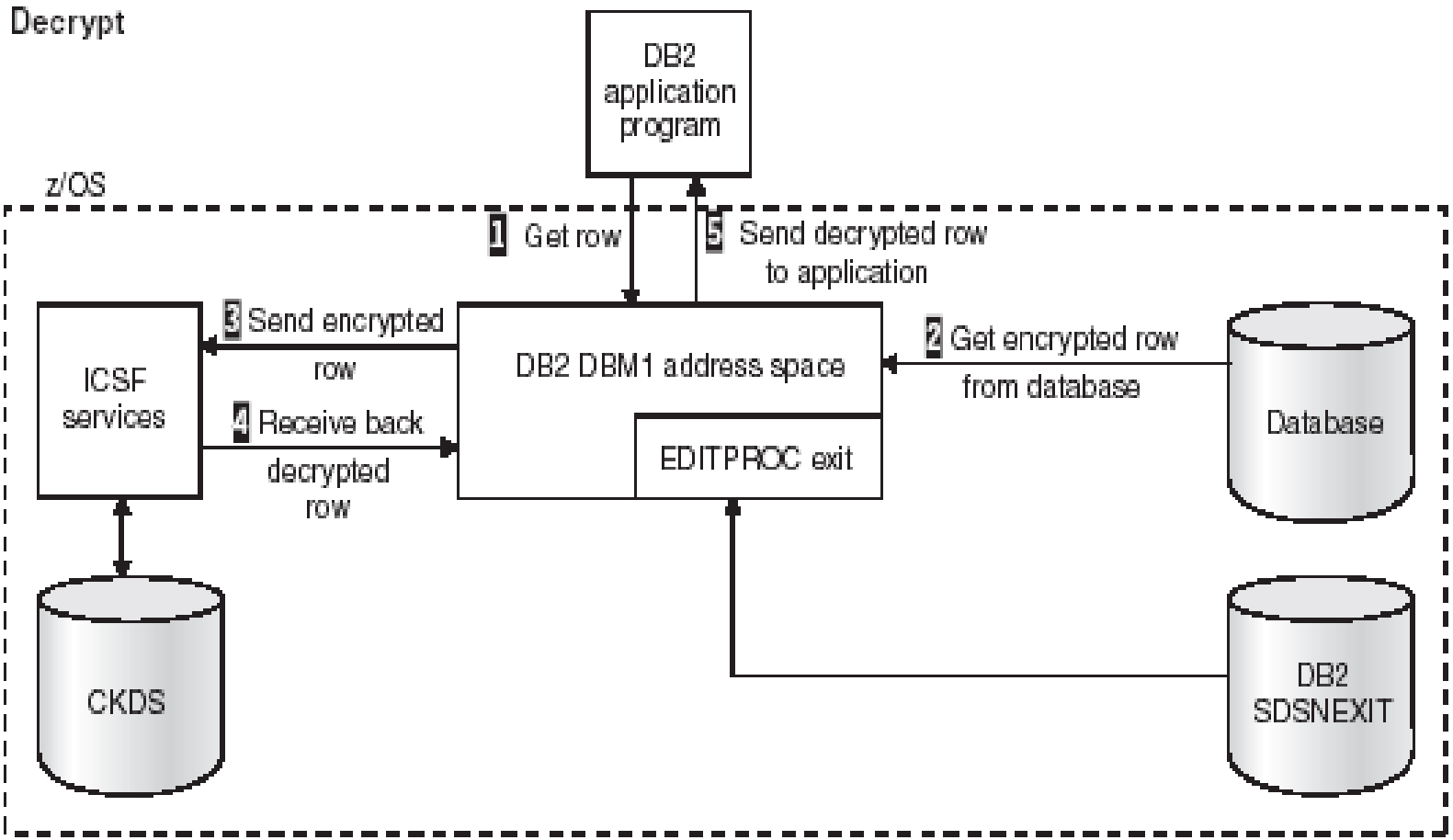
IBM Data Encryption Tool for DB2 and IMS Databases

Proceso de Cifrado con Secure Key



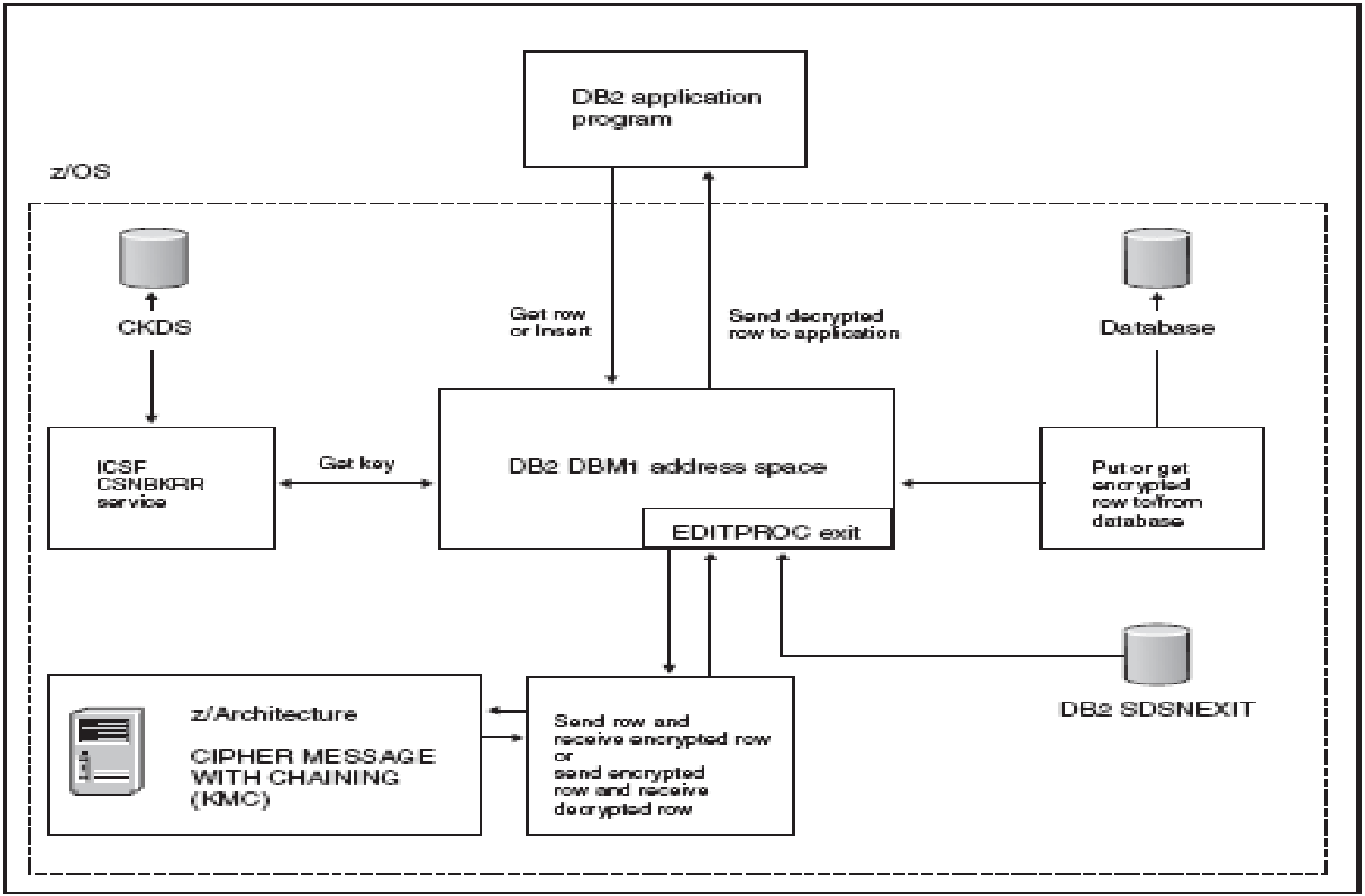
IBM Data Encryption for IMS and DB2 Databases

Proceso de Descifrado con Secure Key



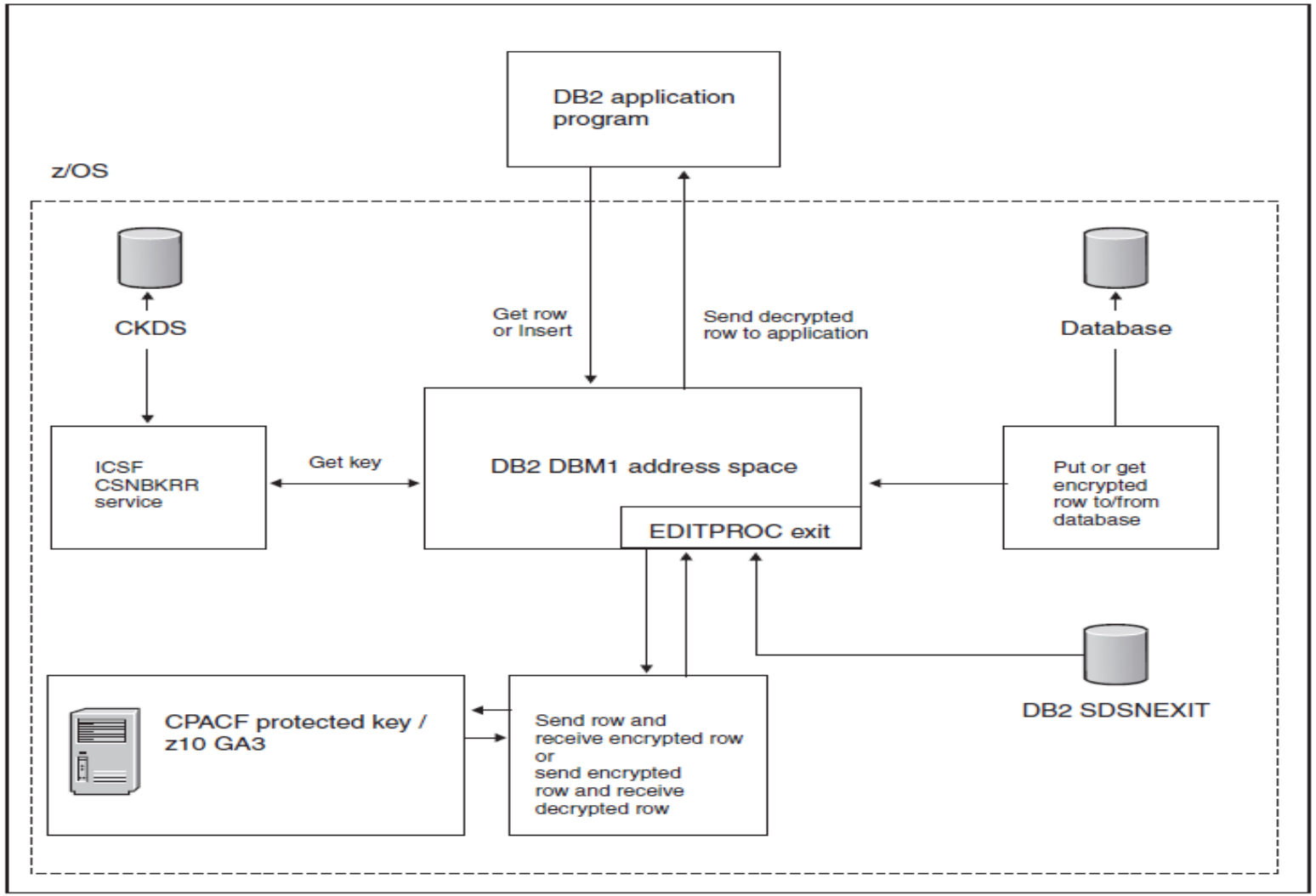
IBM Data Encryption Tool for DB2 and IMS Databases

Proceso de Cifrado con Clear Key



IBM Data Encryption Tool for DB2 and IMS Databases

Proceso de Cifrado con soporte Crypto Express3 (CPACF Protected Key)



DB2 for z/OS y la explotación del cifrado

- IBM Data Server Drivers a partir de V9.5 soportan protocolo SSL y cifrado AES.
- Desde el Fix Pack 2, los clientes no-Java soportan el protocolo Secure Sockets Layer (SSL). Todos los clientes de DB2 Versión 9.5 soportan ahora SSL. Además, los clientes Java y CLI soportan ahora el cifrado AES de 256-bits.
- La conectividad SSL y el cifrado AES de usuario y password requieren que se configure AT-TLS de la Comunicación y se arranquen los ICSFs. El soporte AES requiere que se aplique la PTF PK56287 al DB2.
- A partir de DB2 for z/OS V8, se proporciona la capacidad de cifrado a nivel de *columna* a través de SQL.
- El cifrado a nivel de *fila* se puede implantar en DB2 for z/OS a través de IBM Encryption Tool for IMS and DB2 databases.

Secure Key versus Clear Key

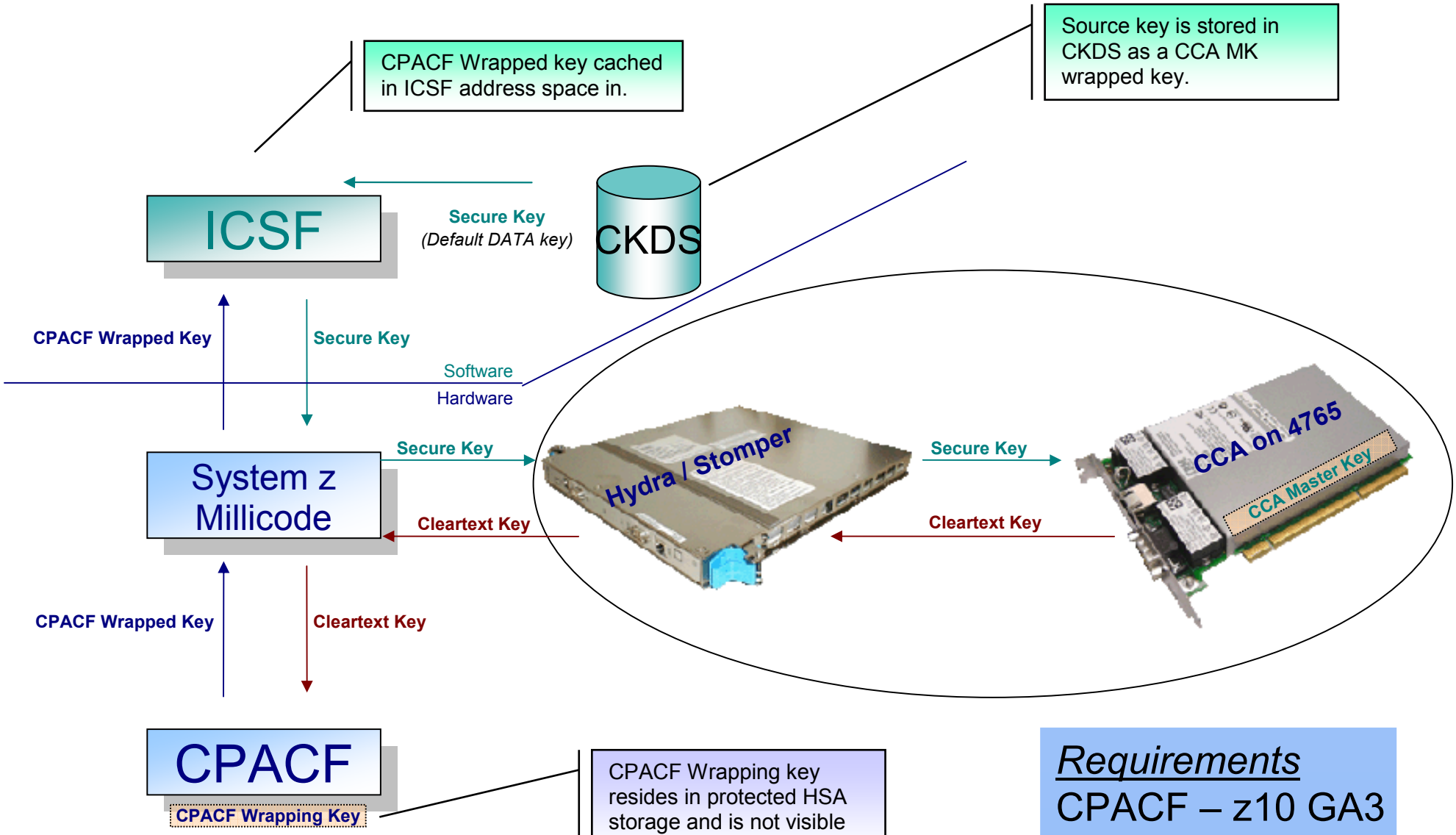
Secure Key (Muy Segura – Elevado Overhead)

- Las claves se cifran fuera de la tarjeta CEX2C.
- Una interrupción no expone valores de claves desprotegidos.
- Las claves de cifrado se cifran en el CKDS con la clave maestra.
- El cifrado/descifrado de datos se realiza dentro de la tarjeta CEX2C.
- AES se puede usar también para cifrado con clave segura (con HCR7751).

Clear Key (Menos Segura – Bajo Overhead)

- Las claves de cifrado de los datos se almacenan como texto en claro en el CKDS (para mejorar el rendimiento).
- La EDITPROC contiene la key label que se pasa al servicio ICSF que realiza una búsqueda en el CKDS y recupera la clave de cifrado asociada con la key label.
- Una vez que se ha obtenido la clave, el DB2 la conserva en memoria, donde se usa para las peticiones de cifrado/descifrado de la EDITPROC.
- No se utiliza la tarjeta CEX2C para realizar peticiones de cifrado/descifrado con clear key. Con el HCR7751, no se necesita una tarjeta CEX2Cpara cifrado con clear key. Antes del HCR7751, se necesitaba una CEX2C para la creación de un CKDS funcional.

CPACF Protected Key - Key Wrapping



Requirements

CPACF – z10 GA3

CEX3C – CLT

ICSF - HCR7770

Un ejemplo de Cifrado
Payment Card Industry (PCI)

- **PCI Data Security Standards (PCI DSS)**
  - Iniciativa dirigida por las compañías de tarjetas más importantes (Visa Inc, MasterCard Worldwide, AMEX, Discover Financial Services y JCB International) para asegurar el uso de un estándar por parte de las compañías que trabajen con datos de tarjetas de pago y luchar contra el fraude (entre otros objetivos).
  - PCI DSS intenta asegurar los datos de los titulares de tarjetas que **almacenan, procesan o transmiten** los comercios y otras organizaciones.
  - El cumplimiento de estas normativas es un requisito **obligatorio** para **todas** las empresas que almacenen, procesen o transmitan datos de titulares de tarjetas.
  - En caso de no cumplimiento, se aplican penalizaciones severas.
  - Están **sincronizadas** con otras iniciativas de cumplimiento de normas.
  - Se suele presentar el cumplimiento de los estándares como ventaja competitiva.

PCI – Áreas específicas de cumplimiento

Requirement 3 *Protect Stored Data*	*Encryption is the ultimate protection mechanism (if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption)*
Requirement 6.3.4 *Production data (live PANs) are not used for testing or development*	*Develop software applications based on industry best practices and incorporate information security throughout the software development lifecycle. Production data (live PANs) are not used for testing or development [PANs - personal account numbers]*
Requirement 7 *Restrict access to data by business "need to know"*	*Limit access to computing resources and cardholder information to only those individuals whose job requires such access*
Requirement 10 *Track and monitor all access to network resources and cardholder data*	*Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong*
Requirement 10.7 *Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations*	*An audit history usually covers a period of at least one year, with a minimum of 3 months available online*

PCI – Áreas específicas de cumplimiento

Requirement 3 *Protect Stored Data*	***Data Encryption for IMS and DB2 Databases***
Requirement 6.3.4 *Production data (live PANs) are not used for testing or development*	***Optim Data Privacy*** ***Optim Test Data Management***
Requirement 7 *Restrict access to data by business "need to know"*	***DB2 for z/OS Multi-Level Security via RACF*** ***Tivoli zSecure Admin***
Requirement 10 *Track and monitor all access to network resources and cardholder data*	***DB2 Audit Management Expert*** ***Guardium*** ***Tivoli zSecure Audit***
Requirement 10.7 *Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations*	***Optim Data Growth Solution***

PCI: Tratamiento de datos de titulares de tarjetas

Guidelines for Cardholder Data Elements

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name[1]	Yes	Yes[1]	No
	Service Code[1]	Yes	Yes[1]	No
	Expiration Date[1]	Yes	Yes[1]	No
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2 / CVC2 / CVV2 / CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

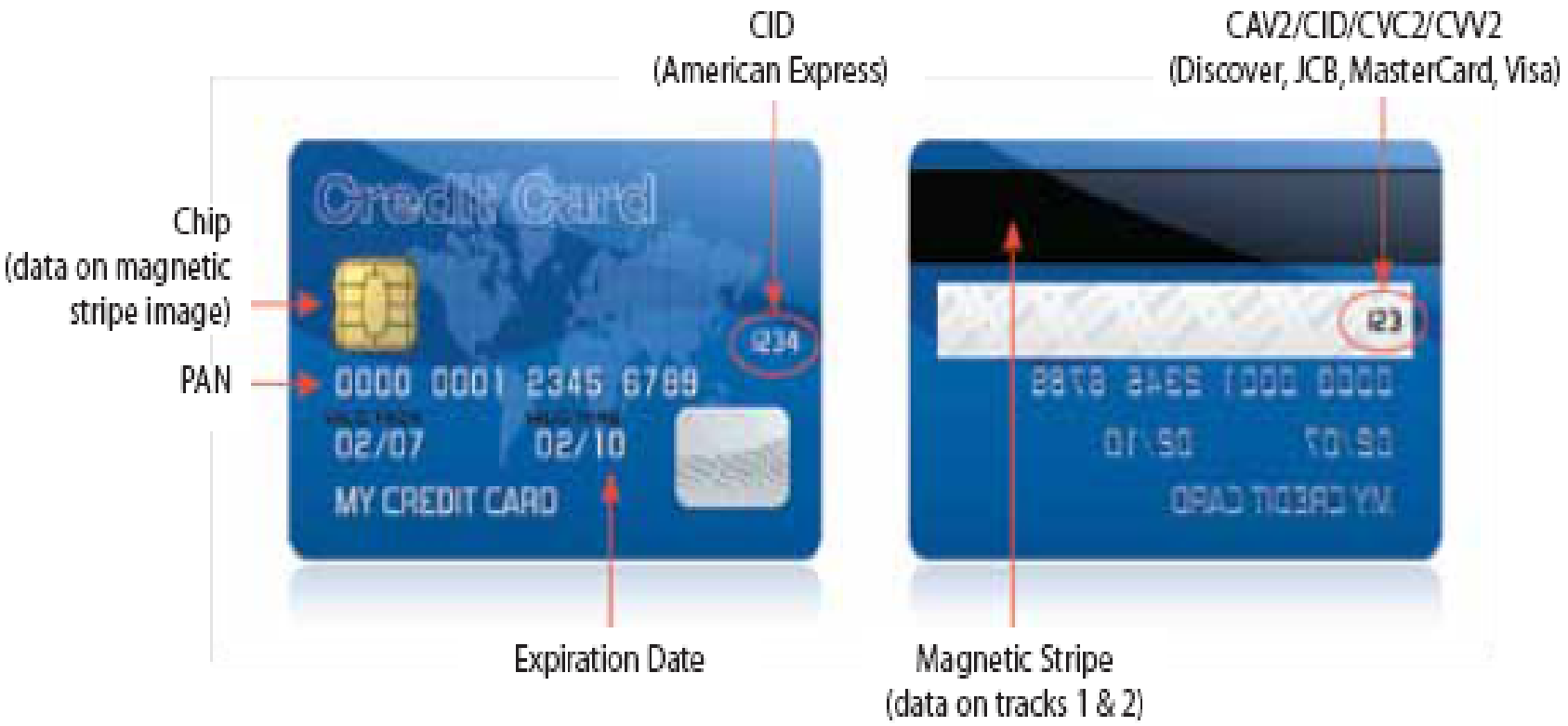
[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

Fuente: PCI Security Standards Council (www.pcisecuritystandards.org)

Tipos de datos en una tarjeta de pago



Fuente: PCI Security Standards Council (www.pcisecuritystandards.org)

PCI: Comportamientos peligrosos

- Una reciente encuesta a empresas en EEUU y Europa refleja actividades que pueden comprometer la seguridad de los titulares de tarjetas:
  - 81 % almacenan números de tarjetas de pago
  - 73% almacenan fechas de expiración de tarjetas de pago
  - 71% guardan los códigos de verificación de tarjetas de pago
  - 57% almacenan datos de los clientes obtenidos de la banda magnética de las tarjetas de pago
  - 16% almacenan otros datos personales

Fuente: Forrester Consulting: The State of PCI Compliance (commissioned by RSA/EMC)

Terminología relacionada con Cifrado

- **Clear Key** - Describe el valor desprotegido de una clave en el momento que se realiza una petición de criptografía. El valor real está disponible en la memoria del sistema operativo, pero no fácilmente localizable.
- **Secure Key** – Hace referencia a una clave criptográfica que debido a las políticas de seguridad debe tener su valor protegido de tal manera que nunca se exponga en la memoria del sistema operativo.
- **DES** – Data Encryption Standard (existen dos versiones, single DES y Triple DES).
- **ICSF** (Integrated Cryptographic Services Feature) – Componente del Sistema Operativo que se utiliza para gestionar las claves empleadas en el cifrado DB2.

Enlaces de interés

- www.ibm.com/software/data/db2imstools/db2tools-library.html#ibmencrypt-lib
- www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt/
- www.ibm.com/software/data/db2imstools/solutions/compliance.html
- www.pcisecuritystandards.org
- www.privacyrights.org/

Information Management
software