



## Revisión del cumplimiento de los requerimientos de seguridad estándares en el tratamiento de los PIN

Seguridad de las tarjetas de banda magnética

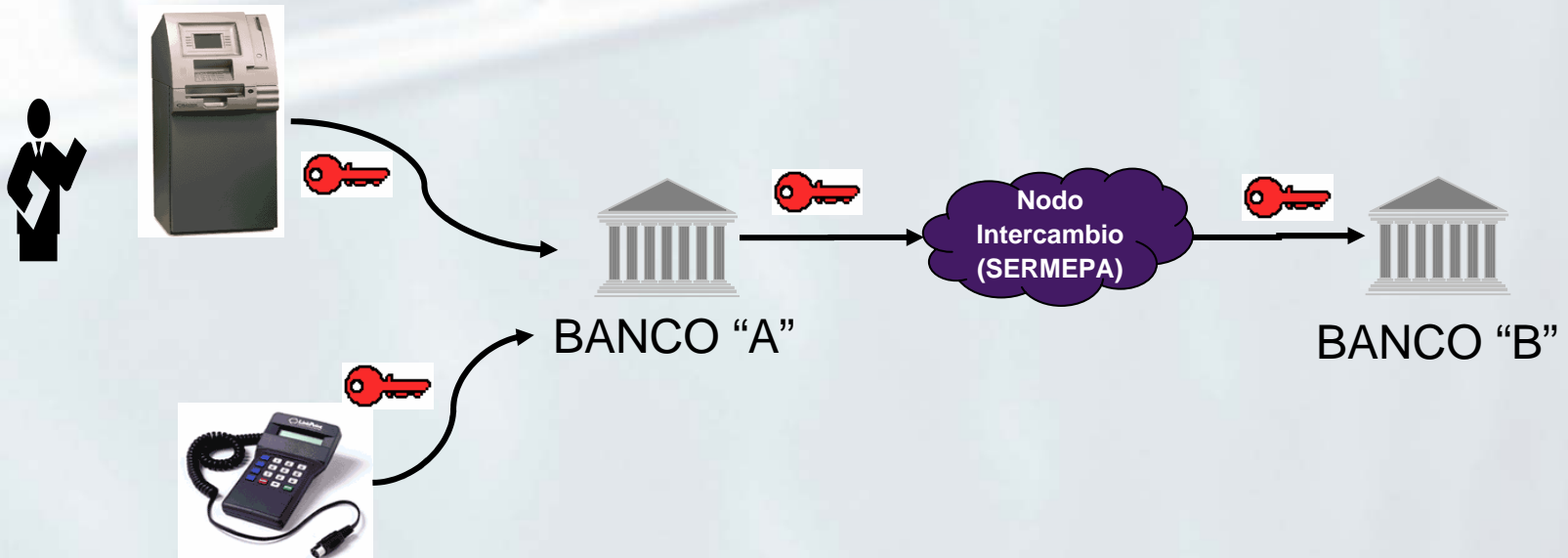


+

9 0 5 9

✓ Visa Internacional y Mastercard han establecido unos **requerimientos de seguridad** para garantizar la confidencialidad del PIN durante todo el ciclo de intercambio.

✓ Para asegurar su cumplimiento: **AUDITORÍAS PERIÓDICAS + INSPECCIONES**



- Basados en los estándares ANSI e ISO
- Se organizan en:
  - ✓ **4 Áreas de revisión**
    - ✓ **7 Objetivos de control**
      - ✓ **28 Requerimientos de seguridad**
        - ✓ Utilización de mecanismos criptográficos
        - ✓ Implantación de controles específicos

### PROCEDIMIENTOS Y CONTROLES GENERALES DE SEGURIDAD

9 0 5 9

#### Procesos de:

- Generación
- Verificación
- Traducción
- Cambio
- Consulta

### GESTIÓN DE CLAVES



#### Procesos de:

- Generación
- Carga
- Custodia
- Mantenimiento

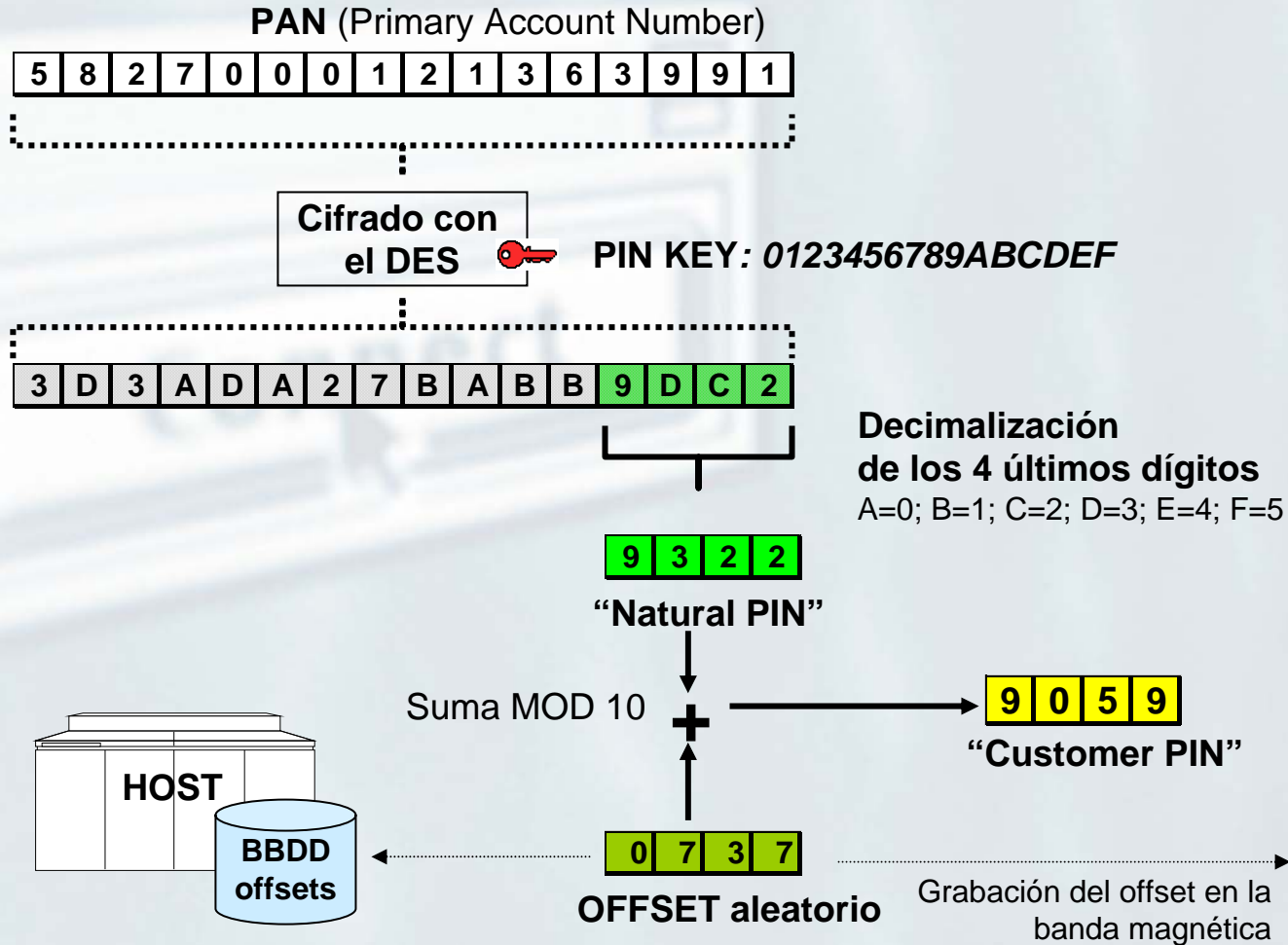
### SEGURIDAD Y CONTROL DEL EQUIPO



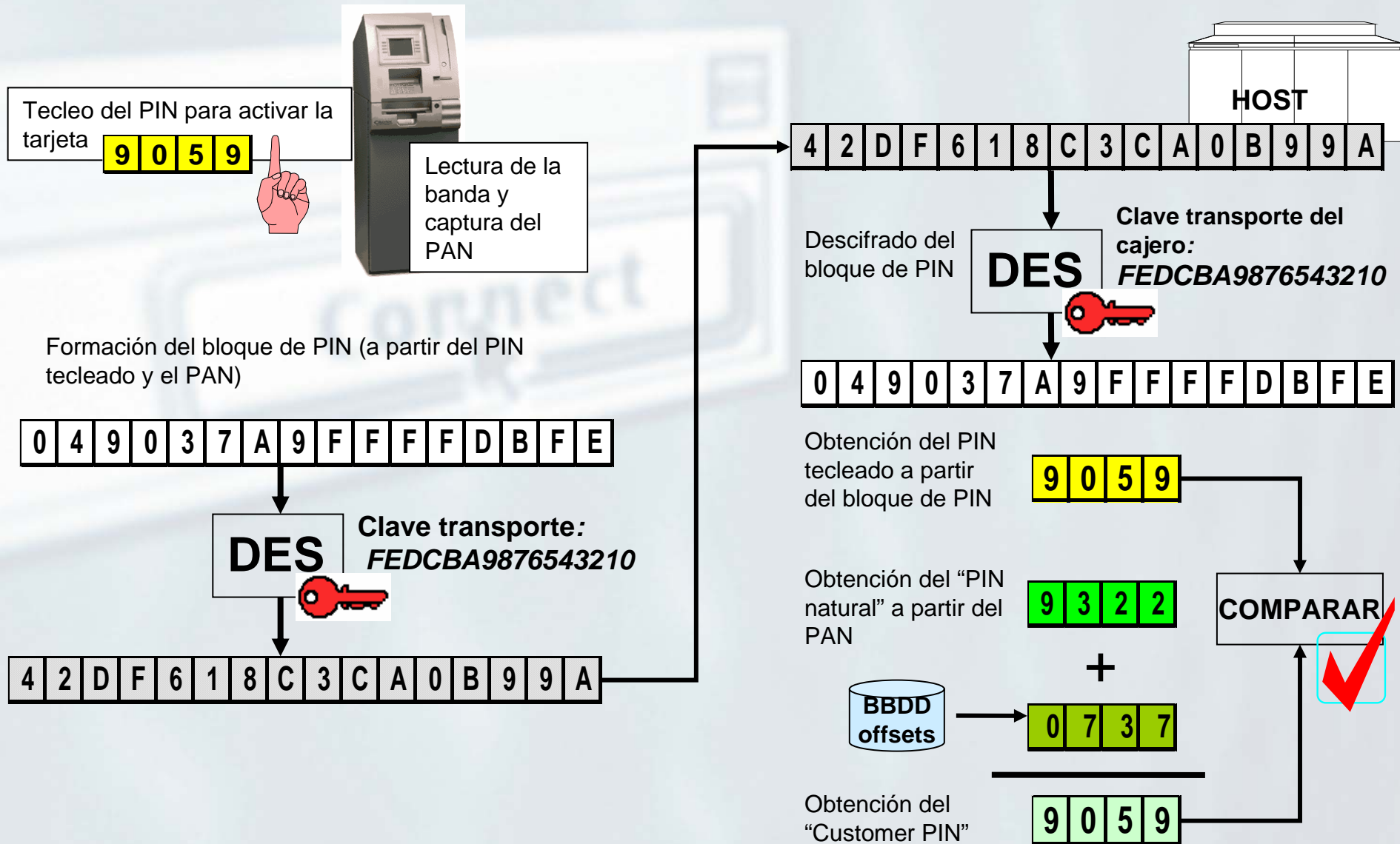
#### Especificaciones Mantenimiento

### DOCUMENTACIÓN DE LOS PROCEDIMIENTOS

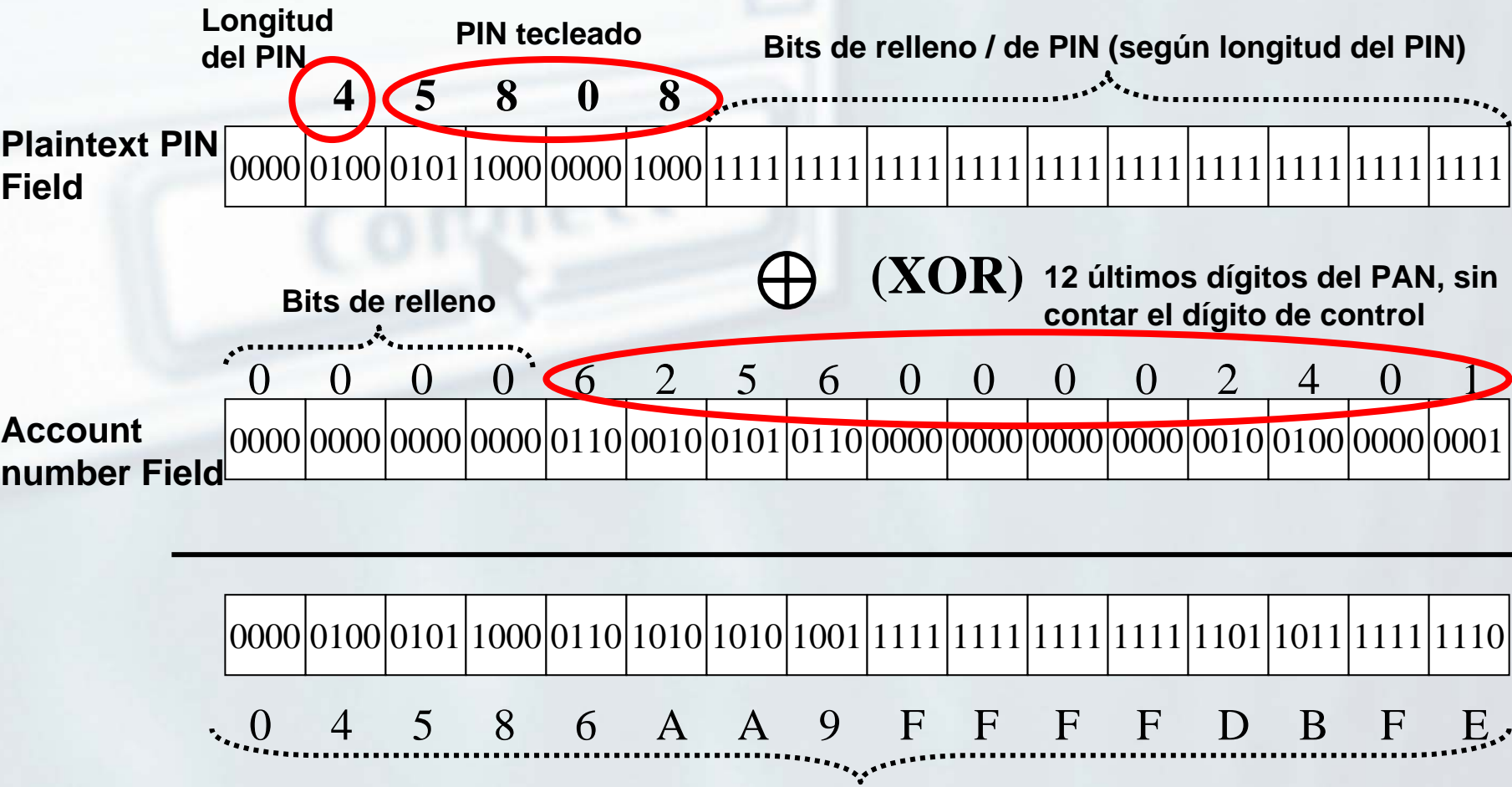
#### Existencia Exactitud



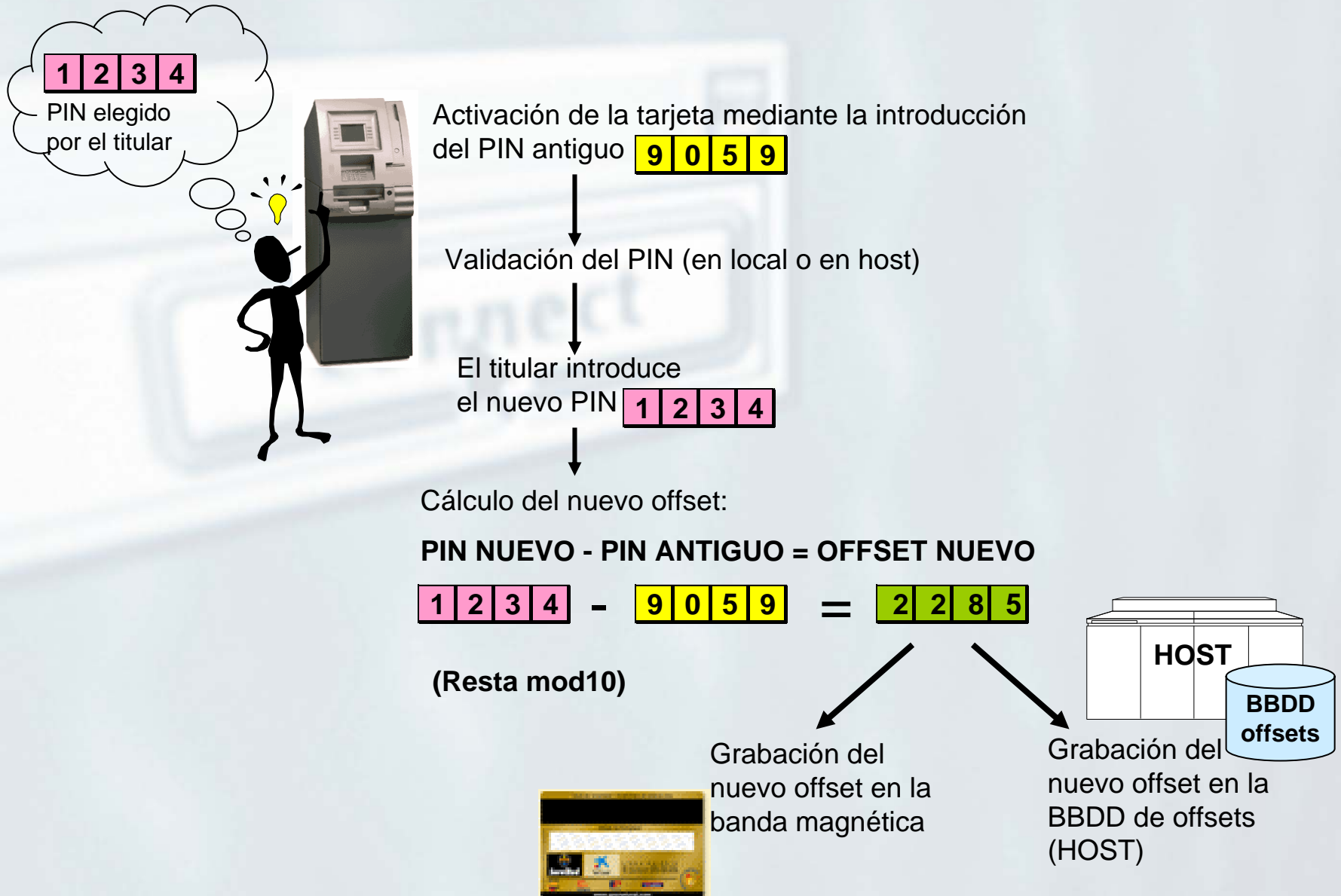
**El PIN nunca debe almacenarse en claro.**



Sirve para garantizar que el **mismo PIN**, cifrado con la **misma clave de transporte**, pero asociado a **diferentes tarjetas**, no da el mismo bloque de PIN cifrado







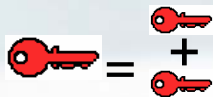
Para cada una de las claves que intervienen en el ciclo de intercambio:

- **Identificación**
- **Localización**
- **Función**
- **Gestión (generación, carga, custodia, destrucción)**

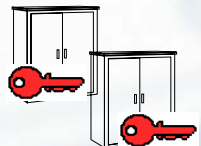
**Ejemplo:**



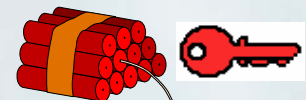




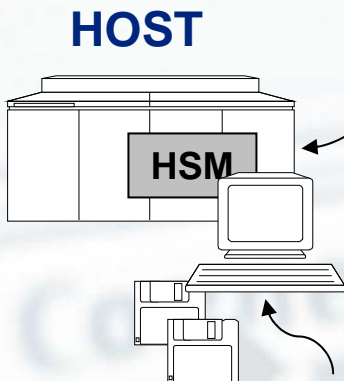
Las claves deben estar formadas por un mínimo de dos componentes, que deben combinarse de forma que no pueda determinarse la clave final sin conocer todos los componentes.



Las copias físicas de las claves deben almacenarse separando cada componente en una caja fuerte independiente



La destrucción de las claves que no se utilizan o que han sido comprometidas debe realizarse siguiendo los procedimientos especificados en la normativa

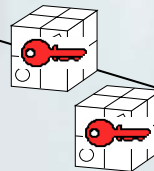


La introducción de las claves en los dispositivos debe realizarse bajo control dual y conocimiento parcial

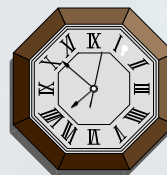
Las claves nunca deben estar fuera de los dispositivos físicamente seguros, a no ser que estén cifradas



Las claves que se transmiten electrónicamente deben viajar cifradas



Las claves que se transmiten físicamente deben ser separadas en componentes y cada uno de ellos debe ser enviado por un canal de comunicaciones distinto



Algunas entidades, como MasterCard recomiendan que las claves se renueven periódicamente (actualmente no es un requisito de VISA)

### IBM PCI Cryptographic Coprocessor

Top  
security  
rating



Los **Módulos de Seguridad** deben estar **certificados**, para garantizar que cumplen con los estándares de seguridad exigidos por la normativa.



### Certificación FIPS 140-1

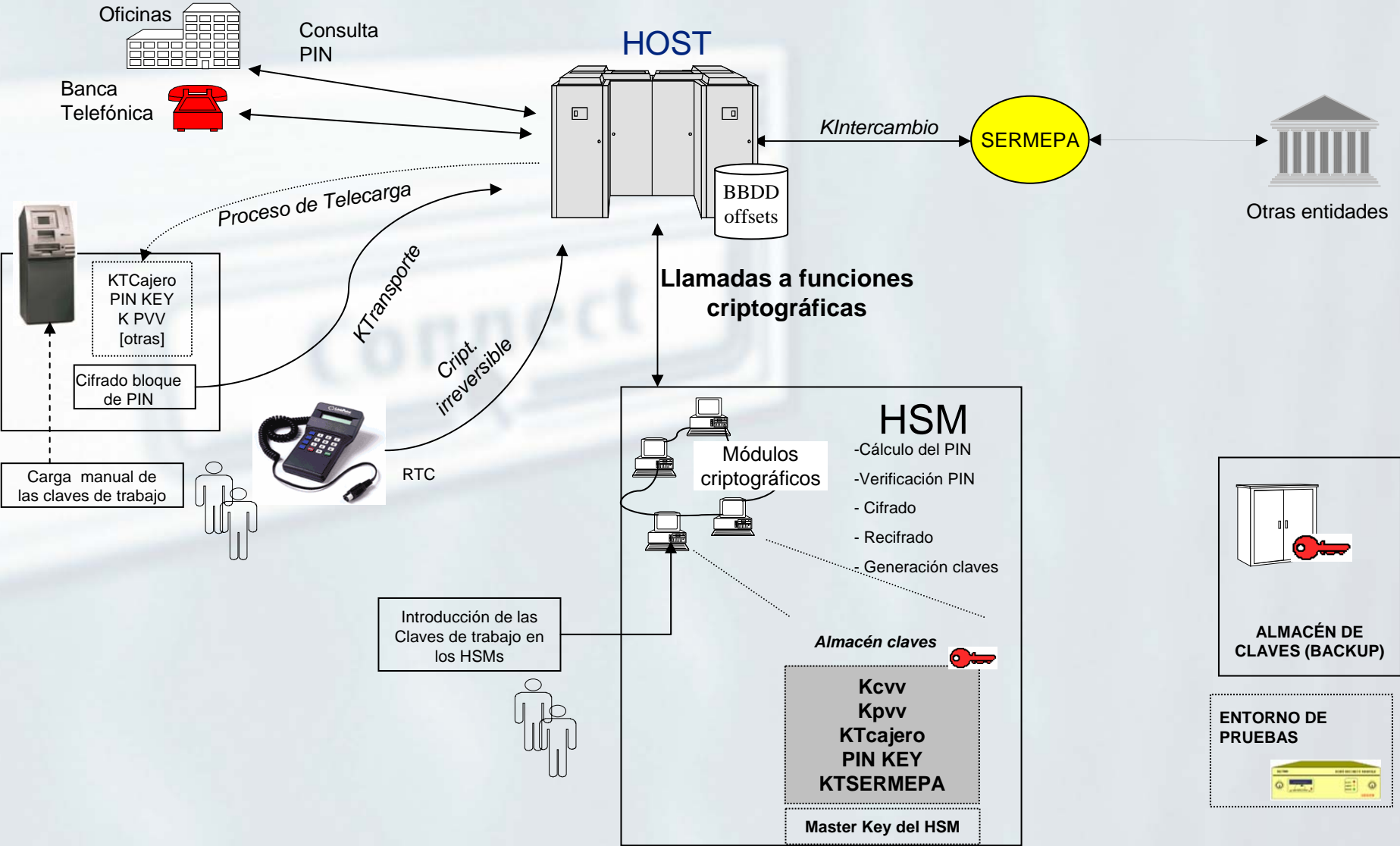
- Publicado por el NIST (National Institute of standards and technology)
- Estándar que especifica los **requerimientos de seguridad que deben cumplir los módulos criptográficos** utilizados en los sistemas de seguridad.
- Establece **4 niveles de seguridad**, destinados a cubrir todo el espectro de aplicaciones y entornos potenciales donde estos módulos criptográficos pueden ser utilizados.
- Los dispositivos en los niveles 3 y 4 se consideran suficientemente seguros.

Existencia de **cláusulas en los contratos con los proveedores de los equipos** (cajeros, TPVs) que garanticen que no han sido sometidos a intrusiones o modificaciones no autorizadas e:



- El proceso de fabricación
- La puesta en funcionamiento
- El mantenimiento del HW/SW

En las **especificaciones de los equipos** suministrados por el fabricante debe constar que **cumplen con los estándares** de seguridad exigidos por la normativa, incluyendo los mecanismos para procesar los PIN



# Deloitte.