EVM: estándar de interoperabilidad de tarjetas IC

(Europay Mastercard Visa)

TPV: Terminal punto venta (postnet)

Define la interaccion a nivel físico,eléctrico de datos y aplicación.

Dos ventajas, SEGURIDAD, APROBACION DE TRANSACCIONES SIN CONEXIÓN

CIFRADO: DES, TRIPLE DES, RSA, SHA

Son mas lentos debido a esto.

Toda transacción sin EMV no responsabiliza a los bancos.

Todas la terminales requieren un NIP (Numero de identificación personal)

Nivel 1 : interfaces físicas, eléctricas y d transporte

Nivel 2: seleccion de aplicación de pago y procesamiento de transacciones financieras

COMANDOS EMV:

* BLOQUEAR APLICACIÓN
* DESBLOQUEAR PALICACION
* BLOQUEAR TARJETA
* AUTENTIFICACION EXTERNA (7816-4)
* GENERAR CRIPTOGRAMA APLICACIÓN
* OBETENER DATOS (7816-14)
* OBTENER OPCIONES DE PROCESAMIENTO
* AUTENTIFICACION INTERNA (7816-14)
* CAMBIO DE PIN/DESBLOQUEAR
* LEER REGISTRO (7816-14)
* SELECCIONAR (7816-14)
* VERIFICAR (7816-14)

FLUJO DE TRANSACCIONES EMV:

1. SELECCIÓN DE APLICACIONES
2. INICIAR EL PROCESO DE APLICACIÓN
3. LEER DATOS DE APLICACIÓN
4. RESTRICCIONES DE PROCESAMIENTO
5. AUTENTIFICACION DE DATOS SIN CONEXIÓN
6. VERIFICACION DEL TITULAR DE LA TARJETA
7. GESTION DE RIESGO DEL TERMINAL
8. ANALISIS DE LA ACCION TERMINAL
9. ANALISIS PRIMERA ACCION TARJETA
10. AUTORIZACION DE TRANSACCION EN LINEA (OBLIGATORIO CAJEROS AUTOMATICOS)
11. SEGUNDA ACCION DE ANALISIS DE TARJETA
12. PROCESAMIENTO DEL EMISOR

**SELECCION DE APLICACION**

Todos los emisores deben tener su propia aplicación.

AID: Identificador de aplicación, identificar la aplicación en la tarjeta

RID: registro de proveedores de aplicaciones (5 bytes)

PIX: Identificador de aplicación

EL AID debe imprimirse en todos los recibos EMV.

**INICIAR PROCESO DE APLICACIÓN**

COMANDO “Obtener opciones de procesamiento”

Devuelve lista de objetos (PDOL)

PDOL: Lista de etiquetas y las longitudes de los elementos de datos, opcionalmente provisto por la tarjeta al terminal durante la Selección de aplicación.

Responde con AIP (intecambio de aplicación)

También envía AFL (Localizador de expediente de solicitud)

**LEER DATOS DE APLICACIÓN**

AFL Contiene los archivos que contienen datos EMV.

Los datos se leen con el comando REGISTRO LEIDO.

EMV no especifica en que archivos están los datos, todo debe ser leído.

Se almacenan según las BEER, y el formato TLV (tag,length,value)

**RESTRICCIONES DE PROCESAMIENTO**

Comprueba si la tarjeta se debe utilizar

Tres elementos a comprobar:

* Numero de versión de la aplicación
* El control de la utilizacion de aplicaciones
* Las fechas de aplicación efectiva/caducidad

Si alguna falla no necesariamente es rechazado.

El terminal establece el bit apropiado en los resultado de la verificación de terminal(TVR)

**AUTENTICACION DE DATOS SIN CONEXIÓN**

Se pretende validar la autenticidad de la tarjeta empleando criptografía de clave publica.

* Autentificacion de datos estatica(SDA)
* Autentificacion de datos dinámica(DDA)
* Autentificacion de datos combinada(CDA)

**VERIFICACION DEL TITULAR DE LA TARJETA**

**Metodos CVM**

* Firma
* Plaintext PIN offline
* PIN cifrado offline
* Planitext PIN y firma offline
* PIN y firma cifrada offline
* PIN Online
* No se requiere CVM
* Procesamiento de Falla CVM

**GESTION DE RIESGOS DEL TERMINAL**

La gestión de riesgos Terminal sólo se realiza en los dispositivos donde hay una decisión que debe tomarse si una operación debe ser autorizada en línea o fuera de línea.

**ANALISIS DE LA ACCION TERMINAL**

Se determina si la transacción fue aprobada, utilizando una combinación de códigos de acción de terminales (TAC) y códigos de acción Emisor (AIC).

**ANALISIS PRIMERA ACCION TARJETA**

Los datos leidos de la tarjeta en la Leer datos de aplicación es CDOL1. Es una lista de etiquetas. Solicita criptograma con el comando.

Tipo de criptogramas

* Certificado de transacción(TC) - Desconectado
* Autorizacion de solicitud de autorización de criptograma (ARQC) – Online
* Aplicación de autentificación criptograma (AAC) Desconectado