BCB
DGD - VUC
19 ABR 2012 12 24
CORRESPONDENCIA
GENERAL
DESPACHADA

CIRCULAR EXTERNA DEL BANCO CENTRAL DE BOLIVIA

La Paz, 17 de abril de 2012
SGDB N° 016/2012

DE: GERENCIA GENERAL
GERENCIA DE ENTIDADES FINANCIERAS

A: ENTIDADES FINANCIERAS, ACCL S.A., EDV S.A., ATC S.A., LINKSER S.A., SERVIRED S.A., EMPRESAS PROVEEDORAS DE SERVICIOS DE PAGO

ASUNTO: REQUERIMIENTOS OPERATIVOS MÍNIMOS DE SEGURIDAD PARA INSTRUMENTOS ELECTRÓNICOS DE PAGO

Señoras y Señores:

El Banco Central de Bolivia en el marco de sus atribuciones de regulación del sistema de pagos nacional y conforme lo establecido en el Artículo 15 del Reglamento de Instrumentos Electrónicos de Pago, aprobado a través de R.D. N°126/2011 de 04.10.11 y modificado con R.D. 025/2012 de 23.02.12, remite para su aplicación y cumplimiento los requerimientos mínimos de seguridad operativa para tarjetas de pago, órdenes electrónicas de transferencia de fondos y billeteras móviles.

Los requerimientos operativos mínimos de seguridad para los citados instrumentos electrónicos de pago constituyen el marco referencial normativo para la aplicación de estándares y buenas prácticas en los sistemas de pago que operan con estos instrumentos.

Atentamente,

CRO/MMV/MAAM/PMS/AQA

Requerimientos operativos mínimos de seguridad para Órdenes Electrónicas de Transferencia de Fondos

Los siguientes requerimientos marcan las condiciones operativas mínimas de seguridad que deben cumplir las operaciones realizadas a través de OETF y deben ser aplicadas en el territorio nacional.

1. Los servicios transaccionales deben funcionar utilizando canales de comunicación encriptados sobre un servidor seguro bajo el protocolo SSL o TLS.

2. El sitio seguro (página *web*) debe indicar el nombre de la entidad que emite el certificado y un vínculo a la entidad certificadora que permita acceder a la siguiente información para verificar su validez: entidad certificante, nombre de la página web, nombre de la entidad propietaria del sitio y validez del certificado.

3. El certificado digital estará vigente hasta la fecha de expiración indicada en el mismo. En ningún caso la vigencia del certificado digital debe ser superior a la definida en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.

4. Las entidades financieras deben implementar en su operativa, a través de portales de *internet* o de banca móvil, mecanismos de autenticación robusta. Es decir, establecer al menos doble factor para la autenticación de usuarios.

5. Las transferencias de fondos deberán ser abonadas a las cuentas de los clientes en el mismo día de su procesamiento y con razón debidamente justificada a más tardar el día hábil siguiente.

6. Las OETF deben cumplir con las siguientes características:

   - Autenticidad. Deben contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago.

   - Integridad. Deben tener la cualidad de estar protegidos contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.

   - Confidencialidad. Deben contar con mecanismos de cifrado que eviten la difusión o divulgación no autorizada de la información contenida en la operación.

   - No repudio. Deben garantizar que ninguna de las partes implicadas en la transacción puedan negar su participación en la misma.

- Disponibilidad. El emisor en el ámbito de su control debe garantizar que el sistema de procesamiento esté disponible para los usuarios según lo establecido contractualmente.

7. El intercambio de información entre las entidades financieras y las empresas proveedoras de servicios externos de tecnologías deberán cumplir con las características de seguridad descritas en el punto 6.

8. El intercambio de información para el procesamiento de OETF entre las entidades financieras y la ACH deberá cumplir con lo definido en el Reglamento de Firma Digital para el Sistema de Pagos emitido por el BCB.

Abreviaturas

ACH = Cámara Electrónica de Compensación de Transferencias Electrónicas de Fondos
OETF = Órdenes Electrónicas de Transferencia de Fondos
SSL = *Secure Sockets Layer*, capa de conexión segura
TLS = *Transport Layer Security*, seguridad de la capa de transporte

Glosario

Autenticación de doble factor o mecanismo de autenticación robusta: Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

- Algo que el usuario sabe
- Algo que el usuario tiene
- Algo que el usuario es

Requerimientos operativos mínimos de seguridad para billeteras móviles

Los siguientes requerimientos marcan las condiciones operativas mínimas de seguridad que deben cumplir las operaciones realizadas a través de las billeteras móviles y deben ser aplicadas en el territorio nacional.

1. El emisor debe vincular al número de cuenta de pago el nombre completo del titular, documento de identidad, número de dispositivo móvil y mantener el registro de las operaciones procesadas por un periodo de al menos diez (10) años.

2. Las órdenes de pago deben ser procesadas a través de medios que garanticen el cumplimiento de las siguientes características de seguridad:

   - Autenticidad. Deben contar con mecanismos que permitan verificar la identidad del titular del instrumento electrónico de pago en cada transacción.

   - Integridad. Deben tener la cualidad de estar protegidos contra alteraciones accidentales o fraudulentas durante su procesamiento, transporte y almacenamiento.

   - Confidencialidad. Deben contar con mecanismos de cifrado que eviten la difusión o divulgación no autorizada de la información contenida en la operación durante toda la transacción.

   - No repudio. Deben garantizar que ninguna de las partes implicadas en la transacción puedan negar su participación en la misma.

   - Disponibilidad. El emisor debe garantizar que el sistema de procesamiento esté disponible para los usuarios según lo establecido contractualmente.

3. El usuario debe tener una contraseña para autenticarse al servicio. El emisor debe generar mecanismos para recordarle al usuario cambiar su contraseña con periodicidad, al menos cada noventa (90) días. En ningún momento esta clave deberá almacenarse en la billetera móvil.

4. Las entidades financieras y las ESP deben implementar mecanismos de autenticación robusta. Es decir, establecer al menos doble factor para la autenticación de usuarios.

5. El emisor debe prever que el tiempo máximo de inactividad en una sesión no supere los veinte (20) segundos.

6. Las entidades financieras y las ESP deben realizar campañas de información con respecto a la seguridad del uso del instrumento dirigidas a los usuarios de billeteras móviles que además incluyan:

    a) Descripción de las operaciones
    b) Uso del servicio
    c) Cambios en la operativa
    d) Sistema de atención de reclamos y consultas de clientes

Abreviaturas

ESP = Empresas Proveedoras de Servicios de Pago

Glosario

Autenticación de doble factor o mecanismo de autenticación robusta: Es una forma de verificar la identidad de los usuarios basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

- Algo que el usuario sabe
- Algo que el usuario tiene
- Algo que el usuario es

Requerimientos operativos mínimos de seguridad para tarjetas de pago

Los siguientes requerimientos marcan las condiciones operativas mínimas de seguridad que deben cumplir las operaciones realizadas a través de tarjetas de pago y deben ser aplicadas en el territorio nacional.

1. Las tarjetas de pago deben contener en forma impresa, grabada o embozada según corresponda los siguientes datos: nombre del emisor, número de tarjeta, valor de verificación de la tarjeta y cuando corresponda, nombre, logo y holograma de la marca internacional. La tarjeta de crédito debe incluir fecha de vencimiento.

2. Los últimos cuatro dígitos embozados, grabados o impresos en la tarjeta deben concordar con los dígitos que figuran en el recibo generado por la terminal al momento de realizar retiros o compras presenciales.

3. Cuando se trate de tarjetas de débito o prepagadas, concluido el proceso de migración al estándar EMV el emisor debe ofrecer al titular la opción de impresión del nombre del tarjetahabiente en el plástico explicando las ventajas y desventajas de la selección. En caso de que el cliente no desee incluir este dato el emisor debe registrar y guardar la selección realizada con la firma del titular.

4. La banda magnética de las tarjetas de pago debe contener la información siguiente: número de cuenta principal (PAN), fecha de vencimiento, valor de verificación del PIN, valor de verificación de la tarjeta (CVV) y código de servicio. Esta información debe ser validada por el emisor al momento de procesarse las transacciones.

5. El código de validación de la tarjeta (CAV2, CID, CVC2, CVV2) o los datos de validación del PIN no podrán almacenarse en sistemas o bases de datos.

6. Los mensajes que se intercambien entre las terminales deben generarse bajo el estándar ISO 8583, que podrá ser adaptado a las necesidades particulares para facilitar la interoperabilidad de las plataformas involucradas.

7. Las Entidades de Servicios de Compensación y Liquidación de transacciones con tarjetas de pago deberán comunicar con una anticipación de 30 días calendario a sus participantes, al BCB y la ASFI las actualizaciones que se realicen al estándar ISO 8583.

8. Como factor de autenticación, para tarjetas solamente con banda magnética, el titular o usuario del instrumento al momento de realizar una compra presencial en un comercio deberá;

   Para el caso de las tarjetas de débito o prepagadas:

- introducir el PIN y firmar los comprobantes de la transacción.

Para el caso de las tarjetas de crédito:

- presentar su documento de identificación y firmar los comprobantes de la transacción.

9. Una vez finalizado el proceso de migración al estándar EMV, los adquirentes deben instruir a los comercios procesar las transacciones siempre utilizando la lectura del chip.

10. Una vez cumplido el plazo para migración al estándar EMV, que será establecido entre el BCB y la ASFI, las disputas o reclamos por el procesamiento de transacciones recaerán sobre las entidades emisoras o adquirentes que no operen con tarjeta chip bajo el estándar EMV de la siguiente manera:

    - La responsabilidad por transacciones procesadas con banda magnética en terminales que no tengan la capacidad de procesar tarjetas con chip, será del adquirente.

    - La responsabilidad por transacciones procesadas con tarjetas solamente de banda magnética en una terminal que tenga habilitada la lectura de chip, será del emisor que no opere bajo el estándar EMV.

11. Se deben aplicar algoritmos de cifrado para autenticar la tarjeta con chip y los datos de la operación.

12. Como mecanismo de autenticación robusta para tarjetas con chip el titular o usuario del instrumento, para realizar compras presenciales en comercios con tarjetas de pago, deberá introducir el PIN y firmar los comprobantes de la transacción. En este sentido, los emisores deben prever en el diseño del instrumento que el código de servicio requiera la introducción del PIN para realizar transacciones.

13. Para verificar la identidad del tarjetahabiente también se pueden utilizar sistemas biométricos de autenticación.

14. En caso de que el emisor autorice la realización de operaciones fuera de línea, las tarjetas de pago deberán utilizar un mecanismo de autenticación de la tarjeta (CAM) dinámico de tipo DDA o CDA que permita recalcular el valor de la firma digital en cada transacción para lo que deben estar equipadas con un criptoprocesador.

15. El sistema operativo de las tarjetas podrá ser de plataforma nativa o abierta pero deberá tener la capacidad de manejar DDA o CDA, en caso de que el emisor acepte el procesamiento de transacciones fuera de línea.

Abreviaturas

CAM = *Card Authentication Method*, método de autenticación de la tarjeta
CVV = *Card Verification Value*, valor de verificación de la tarjeta
CDA = *Combined Data Authentication*, autenticación combinada
DDA = *Dynamic Data Authentication*, autenticación dinámica
EMV = Europay, MasterCard y Visa
PAN = *Primary Account Number*
CAV2 = *Card Security Code*, código de validación de la tarjeta para *Japan Credit Bureau*
CID = *Card Security Code*, código de validación de la tarjeta para *American Express*
CVC2 = *Card Security Code*, código de validación de la tarjeta para MasterCard
CVV2 = *Card Security Code*, código de validación de la tarjeta para VISA
PIN = *Personal Identification Number*, número de identificación personal