Boletín CIMPRA 533

30 de enero de 2023

"Strong Customer Authentication" – Identificación y autenticación fuerte de clientes

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Boletín CIMPRA Nº533

“Strong Customer Authentication” – Identificación y autenticación fuerte de clientes

I. Introducción

Con el fin de robustecer el funcionamiento del sistema nacional de pagos, en el marco de la CIMPRA se elaboró este documento que propone las bases para implementar un proceso de verificación de la identidad del cliente utilizando adecuadas medidas de seguridad y autenticación fuertes de cliente (en adelante también “Strong Customer Authentication” o SCA) en diferentes procesos.

El documento presenta a quiénes está dirigida la propuesta, la regulación vigente como marco de referencia en materia de identificación y autenticación de usuarios, ejemplos de identificación y autenticación fuerte de clientes para diferentes casos especiales considerados como buenas prácticas internacionales en su aplicación y un anexo con las reseñas normativas internacional y locales.

II. Destinatarios

Las buenas prácticas detalladas en este boletín están dirigidas a los participantes de los esquemas de transferencias inmediatas que requieran implementar un proceso de verificación de la identidad y autenticación fuerte de clientes.

III. Regulación existente sobre la identificación y autenticación de clientes

Existen diferentes normas que tratan aspectos sobre identificación y autenticación de clientes dictadas por el Banco Central de la República Argentina (BCRA) que establecen requisitos tanto a los proveedores del servicio de billetera digital como a las entidades financieras (independientemente de que brinden o no ese servicio). Esos requisitos pueden considerarse

como una buena práctica para la totalidad de los PSPCP y PSI que participan en los esquemas de transferencias inmediatas y no se encuentren alcanzados por las citadas disposiciones.

a. Normas sobre "Sistema Nacional de Pagos – Servicios de pago"

   En la Sección 5. 'Servicio de "billetera digital"' se encuentra lo requerido sobre la identificación y autenticación fuerte de los usuarios de servicios de billetera digital interoperable (ver detalle en el **punto VI.c.** de este documento) lo que implica, entre otras cuestiones, verificar la identidad de las personas que requieren la apertura de una cuenta de pago, observando a ese efecto las disposiciones para entidades financieras del punto 1.3. de las normas sobre "Depósitos de ahorro, cuenta sueldo y especiales".

b. Normas sobre "Depósitos de ahorro, cuenta sueldo y especiales"

   En el punto 1.3. de la Sección 1. "Cajas de ahorro"[1] se especifican requisitos para identificar a los clientes. Por su parte, en el punto 4.16. de la Sección 4. "Disposiciones generales" se especifican disposiciones aplicables para la apertura de cuentas de forma no presencial (ver detalle en el **punto VI.d.** de este documento).

c. Normas sobre "Reglamentación de la cuenta corriente bancaria"

   En el punto 1.3. de la Sección 1. "Funcionamiento" se especifican requisitos para identificar a los clientes.

IV. Ejemplos de identificación y autenticación fuertes. Casos especiales

Para cada uno de los casos especiales que se detallan a continuación, se presentan diferentes ejemplos, con carácter indicativo y no exhaustivo, de identificación y factores de autenticación fuerte de cliente considerados como una buena práctica en su aplicación por parte de las entidades:

a. Alta digital de cliente

   Validar la presencia del cliente mediante controles de prueba de vida y anti spoofing[2], asociar el dispositivo móvil y la aplicación al usuario de manera segura y fehaciente, validación de correo electrónico declarado con OTP (One Time Password)[3], validación del dispositivo celular asociado, creación de credenciales de acceso a la aplicación. Adicionalmente, validar la documentación presentada (identificación positiva) y los elementos biométricos asociados contra terceros (RENAPER), entre otros.

[1] Cuando no se encuentre previsto y no se oponga a la reglamentación específica de otros tipos de cuentas contempladas en esas normas, las disposiciones del punto 1.3. son también aplicables a la identificación de los clientes para la apertura de otras cuentas, como por ejemplo la cuenta sueldo.
[2] Técnica de detección de suplantación de identidad.
[3] Contraseña de único uso.

b. Enrolamiento de cuentas que pertenezcan al cliente que realizó el alta digital de acuerdo con las disposiciones del punto a.

   Autenticación fuerte del usuario, validación del dispositivo celular asociado en el alta digital del cliente que incluya la línea telefónica, entre otros.

c. Log in en la plataforma con un dispositivo ya conocido

   Acceso con autenticación fuerte.

d. Cambio de dispositivo

   Autenticación fuerte del cliente con procedimientos de verificación de que la persona propietaria del nuevo dispositivo es el titular de la cuenta.

e. Prevención para los casos de robo de dispositivo / uso no autorizado / SIM

   Con el fin de prevenir los casos de robo de dispositivo/ uso no autorizado/SIM se recomienda como mejores prácticas, entre otras alternativas posibles que pudieran aplicar algunas de las siguientes medidas: (i) instancia de recupero de la cuenta luego de 5 intentos fallidos de las credenciales de acceso; (ii) validación que el dispositivo en uso sea el asociado por el cliente que incluye la línea usada; (iii) mecanismos sencillos e inmediatos de bloqueo de cuenta para el usuario; (iv) bloqueo de pantalla automático por inactividad; u (v) otros métodos que provean adecuados niveles de seguridad.

V. Sugerencias en base a mejores prácticas internacionales

Se mencionan algunas consideraciones que, basadas en mejores prácticas internacionales, robustecen la seguridad dentro del ecosistema en un marco de prevención de fraude.

a. Incorporar segundo factor de autenticación como condición para realizar determinadas acciones, como las que se indican a continuación:
   i. Alta de persona usuaria.
   ii. Primera operación.
   iii. Operaciones que superen determinado monto de valor alto.
b. Reforzar la seguridad de las transacciones incorporando novedades técnicas para reforzar las medidas de doble autenticación del usuario.

VI. Anexo - Reseña normativa internacional y local

a. *Payment Services Directive* (PSD 2) 2015/2366

La Directiva europea incorpora dentro de su normativa los conceptos de "autenticación" y "autenticación reforzada de cliente", definiendo:

> *"(29) «autenticación»: procedimiento que permita al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario;"*
>
> *"(30) «autenticación reforzada de cliente»: la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación;"*

Por su parte, y dentro de las consideraciones iniciales a la Directiva, indica:

> *"(95) La seguridad de los pagos electrónicos es fundamental para garantizar la protección de los usuarios y el desarrollo de un entorno adecuado para el comercio electrónico. Todos los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, gracias a la adopción de tecnologías que permitan garantizar una autenticación segura del usuario y minimizar el riesgo de fraude."*
>
> *"Artículo 97 - Autenticación*
>
> *1. Los Estados miembros velarán por que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes cuando el ordenante: a) acceda a su cuenta de pago en línea; b) inicie una operación de pago electrónico; c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos."*

En lo que respecta a "responsabilidades", frente al incumplimiento en la aplicación de SCA, la Directiva determina para los PSP lo siguiente:

> *"Artículo 74*
>
> *2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante."*

b. Normas sobre “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”

Dirigidas a las entidades financieras y a las cámaras electrónicas de compensación, las normas fijan nuevos requisitos mínimos relativos a la gestión e implementación de la tecnología de la información de las entidades financieras. Específicamente del ámbito que nos compete, se introducen los siguientes términos de la Sección 6. “Canales electrónicos”:

“Autenticación Fuerte - Doble Factor. Comprende la utilización combinada de dos factores de autenticación, es decir dos elementos de las credenciales de distinto factor.

Credenciales. Comprende a todos los elementos físicos o lógicos provistos por la entidad/operador, necesarios para algunas o todas las siguientes acciones durante el uso de un Canal Electrónico específico: presentación/identificación, autenticación, solicitud, verificación, confirmación/autorización. Complementariamente, considérese lo expuesto sobre Factores de Autenticación.

Factores de Autenticación. Las credenciales utilizadas en los canales electrónicos pueden ser del siguiente tipo o factor: "algo que sabe", (Contraseña, dato personal, entre otros), "algo que tiene" (Tarjeta TC/TD, Token, entre otros), "algo que es" (Característica biométrica).”

Dado que las normas se actualizan periódicamente se recomienda consultar la última versión de los aspectos señalados en el siguiente hipervínculo: https://www.bcra.gob.ar/Pdfs/Texord/t-rmsist.pdf

c. Normas sobre “Sistema Nacional de Pagos – Servicios de pago”

La norma establece en su Sección 5. “Medidas para mitigar el fraude”, nuevas medidas de seguridad que deberán tomar las entidades financieras y los PSP para prevenir engaños a los usuarios de los servicios financieros, requiriendo lo siguiente:

“5.4.1. Las entidades financieras y los PSP que presten el servicio de billetera digital deberán:

5.4.1.1. Arbitrar mecanismos para detectar actividades sospechosas o inusuales de las personas usuarias tendientes a mitigar el riesgo de fraude.

5.4.1.2. Asociar a las “billeteras digitales” solo aquellos instrumentos de pago o cuentas –de pago o a la vista– cuyo titular (o alguno de los cotitulares) coincida con el titular de la “billetera digital”.

5.4.1.3. Arbitrar mecanismos de identificación y autenticación del usuario fuertes para acceder a la “billetera”.

5.4.1.4. Notificar a sus clientes a través de los canales de comunicación habituales acerca de lo dispuesto en los puntos 5.4.1.2. y 5.4.1.3.

5.4.2. Las entidades financieras y los PSPCP que brindan el servicio de billetera digital, deberán cumplir con los siguientes recaudos:

5.4.2.1. Verificar la identidad de las personas que requieren la apertura de una cuenta de pago, observando a ese efecto las disposiciones para entidades financieras del punto 1.3. de las normas sobre "Depósitos de ahorro, cuenta sueldo y especiales" (excepto lo requerido en su último párrafo, en relación con la declaración jurada del cliente) y concordantes –puntos 4.1., 4.2. y 4.16.1.–.

5.4.2.2. Habilitar los medios técnicos para que el cliente al momento del enrolamiento de su cuenta a la vista o de pago brinde en la entidad financiera o el PSPCP según corresponda el consentimiento de forma simple e inmediata.

5.4.2.3. Verificar en la autorización de toda instrucción de pago ordenada por el cliente a través del servicio de billetera digital, que el consentimiento brindado conforme a lo requerido en el punto 5.4.4. se encuentra vigente, manteniéndose el plazo de acreditación máximo previsto definido en las normas sobre "Sistemas Nacional de Pagos – Transferencias".

5.4.2.4. Brindar al cliente ordenante la posibilidad de establecer parámetros de uso de los servicios de billetera digital (por ejemplo: límites de montos por periodos y cantidad de operaciones).

Asimismo, deberá permitir la visualización y modificación de los parámetros establecidos y la desvinculación de su cuenta del servicio de billetera digital de manera sencilla e inmediata, especialmente ante sospecha de fraude por parte del cliente.

5.4.3. Los PSI que brinden el servicio de billetera digital deberán verificar la identidad de las personas que solicitan ese servicio, observando a ese efecto las disposiciones para entidades financieras del punto 1.3. de las normas sobre "Depósitos de ahorro, cuenta sueldo y especiales" (excepto lo requerido en su último párrafo, en relación con la declaración jurada del cliente) y concordantes –puntos 4.1., 4.2. y 4.16.1.–.

Las actividades efectuadas en los puntos 5.4.1.2., 5.4.1.3., 5.4.2.1. y 5.4.3. deben ser trazables y auditables. Se debe brindar integridad, protección y resguardo a estos registros."

Dado que las normas se actualizan periódicamente se recomienda consultar la última versión de los aspectos señalados en el siguiente hipervínculo: https://www.bcra.gob.ar/Pdfs/Texord/t-snp-spd.pdf

d. Normas sobre "Depósitos de ahorro, cuenta sueldo y especiales"

Cuando las entidades financieras admiten la apertura no presencial de cuentas a través de medios electrónicos y/o de comunicación deberán cumplir los siguientes requisitos:

"4.16.1.1. Asegurarse de que tales medios les permitan dar total cumplimiento a la normativa en materia de prevención del lavado de activos y del financiamiento

del terrorismo –especialmente en lo referido a la identificación y conocimiento del cliente– [...]

4.16.1.2. Los procedimientos, tecnologías y controles utilizados para la apertura en forma no presencial de las citadas cuentas deberán asegurar el cumplimiento de las disposiciones en materia de canales electrónicos y las relacionadas con la conservación, integridad, autenticidad y confidencialidad de las informaciones y documentos empleados.

4.16.1.3. En el caso de cuentas a nombre de personas jurídicas también deberá cumplirse lo siguiente:

i. Las entidades financieras deberán adoptar procedimientos, tecnologías y controles que permitan verificar la identidad de la persona humana que solicita la apertura en carácter de representante legal o apoderado, la autenticidad de los instrumentos que acreditan la personería invocada y los datos identificatorios de la persona jurídica [...]

ii. La persona jurídica deberá presentar en la casa en la cual esté radicada la cuenta, dentro de los 60 días corridos de realizada la solicitud de apertura, copia certificada del estatuto o contrato social con constancia de su inscripción por la autoridad de contralor societario competente en el Registro Público de la correspondiente jurisdicción [...]".

Los requisitos para la apertura de cuentas definidos en el punto 1.3. de estas normas son los siguientes:

i. Personas humanas

1. Nombres y apellidos completos.
2. Lugar y fecha de nacimiento.
3. Domicilio.
4. Ocupación.
5. Estado civil.
6. Condición de Persona Expuesta Políticamente (Declaración jurada de "PEP" o "No PEP").

Será suficiente la sola presentación de los documentos de identidad para la acreditación de los datos previstos en los puntos 1. a 3. y una declaración jurada del titular –o quien lo represente– para acreditar los datos detallados en los puntos 4. a 6.

No obstante, lo señalado precedentemente, la apertura y el posterior mantenimiento de la cuenta podrán basarse en las medidas de "Debida Diligencia Simplificada" reconocidas por la UIF (Resolución 30-E/2017), debiendo mantener la entidad financiera, en esos casos, una declaración jurada del cliente respecto de que no posee

más de una cuenta de depósito abierta en el sistema financiero y que asume el compromiso de notificar a la entidad cuando cambie esa condición.

De acuerdo con el punto 4.2.ii. de estas normas, las entidades financieras deberán obtener en forma electrónica y directa de las personas humanas titulares o a cuya orden se registre una cuenta, representantes legales, etc., la constancia del CUIL del Registro Nacional de las Personas (RENAPER) o de la ANSES. Alternativamente, podrán cumplimentar este requisito obteniendo una copia simple –en papel o medio electrónico– del dorso del documento de identidad cuando el CUIL se encuentre allí consignado.

ii. Personas jurídicas

La presentación del contrato o estatuto social deberá ajustarse a lo previsto en la normativa de la UIF. Ese requisito se considerará cumplido con la copia del instrumento constitutivo debidamente inscripto de la persona jurídica cliente que la entidad financiera obtenga –en forma electrónica o digital– directamente del Registro Público de la correspondiente jurisdicción, con resguardo de la evidencia correspondiente de tal proceso.

Según el punto 4.2.i. de estas normas las entidades financieras deberán obtener en forma electrónica y directa de las personas jurídicas o humanas titulares o a cuya orden se registre una cuenta, representantes legales, etc., de la AFIP, la constancia de CUIT o CDI.

Dado que las normas se actualizan periódicamente se recomienda consultar la última versión de los aspectos señalados en el siguiente hipervínculo: https://www.bcra.gob.ar/Pdfs/Texord/t-depaho.pdf