Capa 1 · Identidad y confianza entre participantes

Autor: Eber Bezzone | **Fecha:** 2026-11-03 | **Versión:** V 0.1

Cómo dos entidades que no se conocen prueban que son parte del sistema: el directorio, los roles, los certificados y el canal, y cómo se dan de alta y de baja.

Previo a la emisión o aceptación de cualquier consentimiento de un usuario, el sistema requiere identificar quién solicita la información, quién responderá a la solicitud y el estado operativo vigente de ambas partes.

1 · Introducción

Si desarmamos un sistema de finanzas abiertas, podemos distinguir cinco capas fuertemente relacionadas entre sí: identidad y confianza; autenticación, consentimiento y autorización; recursos; observabilidad; y gobernanza. A esas cinco se suma una capa transversal, la auditoría, que no ocupa un nivel propio, sino que atraviesa las cinco capas antes mencionadas (Figura 1).

En un escenario con dos participantes del ecosistema (una entidad transmisora y otra receptora), ambas deben demostrar su identidad y sus permisos vigentes antes de que el titular pueda otorgar su consentimiento. El objetivo de este documento es analizar esa capa inicial de **identidad y confianza entre los participantes**: el mecanismo mediante el cual dos entidades sin relación previa validan quiénes son y establecen una comunicación segura. Este proceso se enfoca exclusivamente en la identificación de las entidades, dejando la autenticación del cliente para desarrollarla en la capa 2.

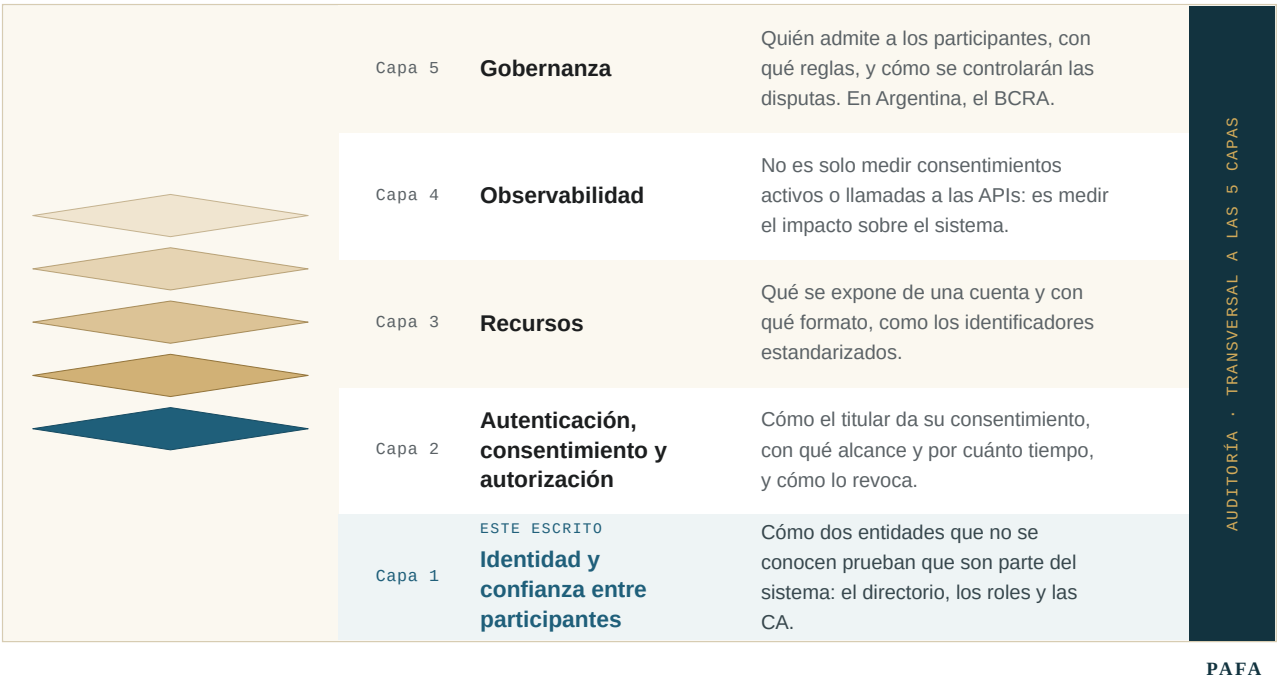


Figura 1 · Las capas del ecosistema. Capa 1: Identidad y confianza entre participantes

2 · Componentes de capa 1

Previo a la instancia en que el titular otorgue su consentimiento, la entidad transmisora debe validar cuatro aspectos fundamentales de la entidad receptora que solicita la información: verificar su validez como participante, confirmar que posea el rol adecuado, autenticar su identidad y establecer el canal de comunicación seguro a utilizar. En caso de que alguno de estos puntos no pueda verificarse, la interacción debe interrumpirse antes del consentimiento del usuario.

Con el propósito de resolver cada una de estas interrogantes, el perfil estructura la capa en cuatro componentes principales: el **directorio** de participantes, los **roles y permisos** asociados, el esquema de certificados junto con la **autoridad certificadora** y el **canal de comunicación** seguro.

2.1 · El directorio: quiénes participan y su estado

Actualmente, Argentina dispone de un padrón de participantes formal: el Banco Central de la República Argentina (BCRA) lleva el Registro de Proveedores de Servicios de Pago, habilitado por la SEFYC [3]. Para inscribirse, una entidad debe completar un trámite oficial donde presenta su CUIT, denominación social, domicilios, autoridades designadas y nómina de accionistas con participaciones iguales o superiores al 10 %. Tras validar el cumplimiento de los requisitos, el BCRA otorga un «certificado de inscripción» asignándole así la matrícula correspondiente en el Registro de Proveedores de Servicios de Pago (RPSP) [3].

No obstante, este listado posee un carácter administrativo y está orientado a la consulta humana. Por ende, esto no satisface los requerimientos de un ecosistema de finanzas abiertas, el cual exige un directorio técnico interoperable que posibilite el procesamiento automatizado e inmediato por parte de los sistemas de las diversas instituciones financieras.

El Decreto 353/2025, que crea el Sistema de Finanzas Abiertas, le encarga al BCRA fijar los requisitos que deberán cumplir “los demás organismos del Poder Ejecutivo Nacional y las entidades del sistema financiero” que participen del sistema (art. 6) [1]. Según lo anunciado, el primer caso de uso será compartir información que custodia ARCA, con un lanzamiento esperado para el primer semestre de 2027 [4], y en otras fuentes se mencionan otros organismos como ANSES [5]. Ninguno puede estarlo: el RPSP es para personas jurídicas que, sin ser entidades financieras, cumplen una función en un esquema de pago minorista, y excluye los esquemas de cobro de obligaciones con el Estado (1.2.1 y 1.2.3.2) [3]. El directorio técnico, entonces, no podrá ser una copia del registro del BCRA: deberá ser un padrón propio, que incluye a las entidades inscriptas y a esos organismos, con su rol.

Ese padrón debería exponer como mínimo:

1. la organización, con un identificador propio en el directorio y su CUIT asociado (ver abajo)
2. los roles habilitados
3. el estado (activo, suspendido, de baja) y desde cuándo
4. las claves públicas de la entidad, de transporte y de firma, publicadas por el directorio como un conjunto de claves (JWKS) por participante
5. el issuer de la entidad, si es transmisora, y la URL base de sus recursos

En cuanto al identificador, hay dos candidatos a mano: el número de inscripción en el RPSP que asigna el BCRA [3] y el CUIT, que identifica a la entidad frente a todo el Estado. El número de RPSP no alcanza: deja afuera a los organismos públicos, que no están inscriptos. El CUIT, en cambio, lo tienen todos, ARCA y ANSES incluidos, y podría hacer de identificador. El perfil decide que el directorio asigne a cada participante un identificador propio, estable, que no cambia con los roles ni con el estado: el CUIT identifica a la persona jurídica ante el Estado, no al participante del sistema. El CUIT queda asociado a ese identificador y es uno de los datos que viajarán en el certificado, sin depender del alta en el directorio (2.3). Así lo hace Chile, cuyo directorio asigna a cada participante un identificador dentro del SFA distinto del RUT (Anexo 3, I.D, Tabla 1) [2]; y en Argentina, Transferencias 3.0 ya identifica a las entidades en los tokens (`iss`, `aud`, `client_id`) con el código de entidad del BCRA, de cinco dígitos, que es un tercer candidato a tener en cuenta [13].

Que el BCRA lo regule no implica que tenga que operarlo. En los casos revisados conviven los dos modelos. En Australia, Perú, Chile y Colombia, el directorio lo opera el propio regulador: la ACCC [7], la SBS [6], la CMF [2] y la SFC, que tiene hasta abril de 2027 para ponerlo en marcha [20]. En Brasil, en cambio, desde enero de 2025 la infraestructura la gobierna una asociación del ecosistema, la Associação Open Finance, bajo las reglas del Banco Central [8]. Para esta capa, quien opera el directorio es un eje independiente del perfil: el perfil intenta describir qué tiene que poder hacer el directorio, independientemente de quién finalmente lo termine operando.

Independientemente de quién lo opere, este tiene que poder cumplir tres requisitos técnicos:

1. Publicar un cambio de estado de modo que se propague a todas las demás entidades.
2. Permitir la reconstrucción del padrón a una fecha determinada.
3. Suspender a una entidad sin darla de baja.

El directorio tiene, además, una clave propia: con ella firma los software statements (3.1) y, si notifica cambios de estado, los avisos (3.2). Esa clave es la raíz de la confianza de toda la capa: una transmisora acepta un statement porque verifica la firma del directorio, y verifica la firma porque obtuvo la clave de una dirección que conoce de antemano. El Reino Unido la publica en el keystore del directorio, con un certificado firmante de un año de vigencia [24]; Brasil, en el JWKS de su directorio [16]; Australia, en un endpoint del Register sin autenticación, pensado para distribuirse por CDN [28]; Perú exige validar el statement y los webhooks contra el JWKS público del directorio, sin fijar su dirección [6]. Ninguno fija el período de rotación ni el solapamiento. Este perfil propone lo que los casos dejan implícito: **la clave del directorio se publica en una dirección conocida, la nueva se publica antes de que la vieja deje de usarse, y la custodia es del operador del directorio.**

2.2 · Los roles: quién puede ser participante

En todo sistema de finanzas abiertas, surge, especialmente con las entidades más pequeñas, un nuevo jugador: los **proveedores** que ofrecen servicios tecnológicos a estas pequeñas entidades. Esto dispara la pregunta de quién se debe registrar en el directorio, si la entidad financiera o el operador tecnológico. El directorio registra entidades con su identificador, roles y estado. Un proveedor tecnológico puede operar la infraestructura de muchas entidades, pero no debería tener identidad propia en el padrón ni roles habilitados. De ahí salen tres consecuencias:

- **Un issuer por entidad** (el servidor que emite los tokens de esa entidad), descubierto desde el directorio y no deducido del dominio.
- **El certificado se emite a nombre de la entidad**, aunque la clave la custodie el proveedor. No se admite un certificado del proveedor que opera en nombre de varias.
- **La responsabilidad frente al ecosistema no se delega: la entidad responde por lo que su proveedor hace en su nombre**. El contrato con el proveedor reparte las tareas, y el regulador puede pedirlo y auditarlo, pero esto no quita la responsabilidad de la entidad. Eso no impide pedirle algo

> al proveedor: que acredite, con una certificación o una auditoría que presenta la entidad, que cumple lo que el perfil exige, sin tener por eso identidad propia en el padrón.

Esto no es una regla que el perfil propone: el BCRA ya la definió en dos oportunidades. Para las entidades que tercerizan tecnología, el texto ordenado de riesgos de tecnología y seguridad dice que las entidades que tercericen "no estarán liberadas de sus responsabilidades, presentes o futuras", y exige que el contrato con el tercero fije las responsabilidades de las partes, el derecho de auditoría y el acceso irrestricto de la entidad y de la SEFYC, incluso sobre los subcontratistas; y esa obligación alcanza a los PSP desde el 4 de agosto de 2026 [9]. Y el caso más parecido al de esta sección es el de los PSP que prestan cuentas de pago a través de la interfaz de un tercero. El texto ordenado de PSP dice, desde mayo de 2026, que los clientes del tercero "son clientes del PSP", que esa operatoria "no deslinda al PSP de cumplir toda la reglamentación". Además, es el PSP quien debe establecer contractualmente las exigencias con el tercero y verificar que este las cumpla [3].

2.3 · Certificados y Autoridad de Certificación (CA)

Cada participante necesita probar, en cada conexión, que es quien dice ser. Para eso existen los certificados: documentos digitales que unen una clave pública con una identidad, en este caso la de una entidad del ecosistema. Lo firma una autoridad certificadora (CA), que verifica esa identidad antes de emitir y, posteriormente, publica su estado (vigente o revocado). El conjunto de CAs que el ecosistema acepta es su ancla de confianza, y quién las opera es una elección: el ecosistema puede tener una CA propia o aceptar CAs de terceros que cumplan ciertos requisitos. En los casos revisados se observan ambos modelos: Australia [15] y el Reino Unido [10] operan una CA del ecosistema (en el Reino Unido, junto con las CAs cualificadas de eIDAS); Perú [6] y Chile [2] aceptan CAs de terceros que cumplan ciertos requisitos: Perú, las de una lista blanca; Chile, las auditadas bajo WebTrust o ETSI EN 319 411 (Anexo 3, II.A), sin que la CMF emita certificados.

En definitiva, la CA y el directorio cumplen funciones complementarias pero bien delimitadas: mientras el certificado confirma que quien realiza la llamada posee una clave vinculada a una entidad, corresponde al directorio verificar si dicha entidad cuenta con la habilitación y el rol requeridos para la solicitud en cuestión. De este modo, la autenticidad de la clave (que prueba la CA) queda claramente disociada de la autorización operativa (que valida el directorio).

Esta separación de directorio y autoridad certificadora ofrece la flexibilidad para cambiar el ancla de confianza sin reestructurar el ecosistema. Un caso de análisis se ve en el Reino Unido, que ya cambió su ancla de confianza dos veces. El open banking británico arrancó con certificados emitidos por la OBIE; con la PSD2 pasó a los certificados eIDAS; y ante el Brexit, con la revocación de los eIDAS de las entidades británicas prevista para el 31 de diciembre de 2020, evaluó volver a los certificados de Open Banking, que casi todo el ecosistema ya usaba [10]. De hecho, su especificación de registro dinámico contempla el uso de diversas anclas de forma explícita: "la especificación DCR proporciona la extensibilidad para utilizar una SSA de cualquier ancla de confianza (no solo del Directorio de Open Banking)" [11].

Brasil, por otro lado, optó por acoplar el certificado al directorio. Aunque no gestiona una CA propia, requiere certificados emitidos por autoridades de la ICP-Brasil que incluyen el código de participante junto con el identificador del software statement asignado por el directorio [21]. Esta arquitectura implica que cualquier cambio en el directorio o en el ancla de confianza afecte directamente al perfil de los certificados. En contraste, el modelo de Perú ofrece mayor flexibilidad: permite el uso de certificados de CAs de terceros incluidas en la lista blanca de su directorio (tales como entidades internacionales con auditorías WebTrust o ETSI, o nacionales pertenecientes a la Infraestructura Oficial de Firma Electrónica), evitando incluir metadatos del directorio dentro de la estructura del certificado [6].

En Argentina tenemos un precedente local, aunque no esté en el sistema financiero. Los web services de ARCA funcionan con esta separación desde hace años: el certificado X.509 "implementa la autenticación de los computadores del EE", con el CUIT en el DN (serialNumber=CUIT 30123456789), pero la autorización a cada servicio vive aparte [12]. El certificado no lleva permisos dentro; simplemente autentica y después el registro habilita. Es el mismo reparto que propone el perfil, operando a escala nacional y ya implementado por cualquiera que haya integrado facturación electrónica.

Por eso, no atar el certificado al directorio no es una elección estética: deja que cualquier CA aceptada emita el certificado sin esperar el alta en el directorio, y permite cambiar el ancla de confianza sin tocar el perfil, que es lo que Brasil resignó al poner datos del directorio en el certificado.

Aunque el certificado no contenga información del directorio, este último no lo ignora. Siguiendo el modelo adoptado por Perú [6], Brasil [16] y el Reino Unido [24], la entidad debe inscribir y mantener actualizadas en el directorio sus claves públicas (de transporte y de firma), las cuales son publicadas por el organismo. De esta forma, ante cada conexión, la entidad transmisora realiza una doble validación (Figura 2): verifica que el certificado provenga de una CA autorizada y se encuentre vigente (sin revocar), y confirma que la clave presentada coincida con alguna de las publicadas activamente en el directorio para dicha institución. Debido a que la entidad solo puede operar una vez que el directorio publica sus datos, el certificado puede tramitarse de manera previa al alta formal. Finalmente, para la firma de mensajes, únicamente se considera válida la clave registrada en el directorio, cuya validez se coteja contra el historial del padrón.

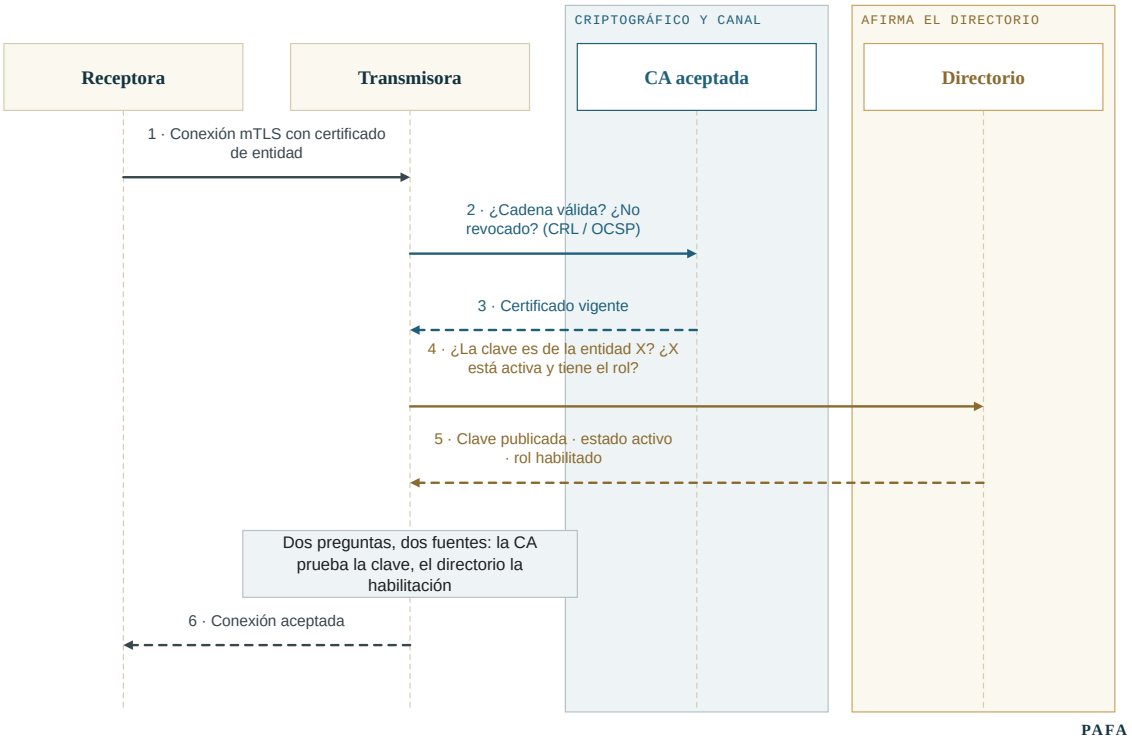


Figura 2 · Qué prueba el certificado y qué prueba el directorio

2.4 · El canal: por dónde habla, y su límite

El canal entre entidades debería ser mTLS, algo que las entidades argentinas ya operan: en Transferencias 3.0, la conexión entre los backends va siempre con mTLS [13]. No hay motivo para cambiarlo.

Lo importante del canal no es la elección sino su **límite**, y sobre él se apoya la capa 2. Cuando hay un API Gateway, un service mesh o una CDN en el borde de la red, el TLS debería terminar ahí: el certificado del cliente se valida en el borde y no llega a la aplicación. No es que falte certificado; es que su rastro no se propaga hacia adentro del ecosistema de la entidad. Mantener mTLS en cada salto interno es posible, pero el perfil opta por no exigirlo, por dos motivos. El primero es de costo: cada salto suma certificados que emitir, rotar y desplegar, y ese costo no se paga una vez sino en cada cambio de la arquitectura interna. El segundo es de alcance: el perfil fija cómo se habla entre entidades; cómo cada entidad protege su red interna es responsabilidad suya y ya está regulada, para las entidades financieras y los PSP, por el texto ordenado de riesgos de tecnología del BCRA [9]; para los organismos públicos, la exigencia tendría que venir de los requisitos que fije el BCRA según el art. 6 del decreto [1]. Lo que el perfil sí exige es el resultado: que ningún pedido llegue a los servicios internos sin que la identidad de la receptora haya sido verificada en el borde y viaje hacia adentro ya verificada. Cómo lo cumple cada entidad, con mTLS interno o pasando la identidad verificada (Figura 3), es decisión de cada organización.

La regulación peruana respalda esta segunda vía: permite que el punto donde termina mTLS (por ejemplo, el API Gateway) valide el certificado contra el token, siempre que ningún pedido llegue al backend sin verificar [6].

La capa 2 define cómo se vincula el token a esa identidad, pudiendo utilizar mTLS o DPoP, los dos mecanismos contemplados por FAPI 2.0 [22]. Asimismo, la restricción de Chile [2] y de Perú, que solo autorizan el uso de mTLS [6], es un aspecto que se aborda en dicha sección.

Dado que mTLS únicamente certifica la identidad de las partes durante el transcurso de la sesión activa, al finalizar la conexión no persiste ningún registro que un tercero pueda auditar. Ante eventuales controversias, transacciones no reconocidas o incidentes de seguridad, resulta imprescindible que cada mensaje crítico sea firmado digitalmente con una clave asociada formalmente a la entidad a través del directorio. Asimismo, se debe contar con la capacidad de verificar el registro histórico del padrón para esa institución en la fecha específica del evento, motivo por el cual el directorio mantiene su trazabilidad histórica (sección 2.1).

El estándar FAPI 2.0 Message Signing [14] determina los mensajes que requieren firma (materia detallada en la capa 2). Adicionalmente, PAFA formula en dicha capa los esquemas y formatos para la firma de solicitudes de recursos (siguiendo como referencia el uso de RFC 9421 [6] en Perú), y su primera aplicación será la revocación del consentimiento entre entidades.

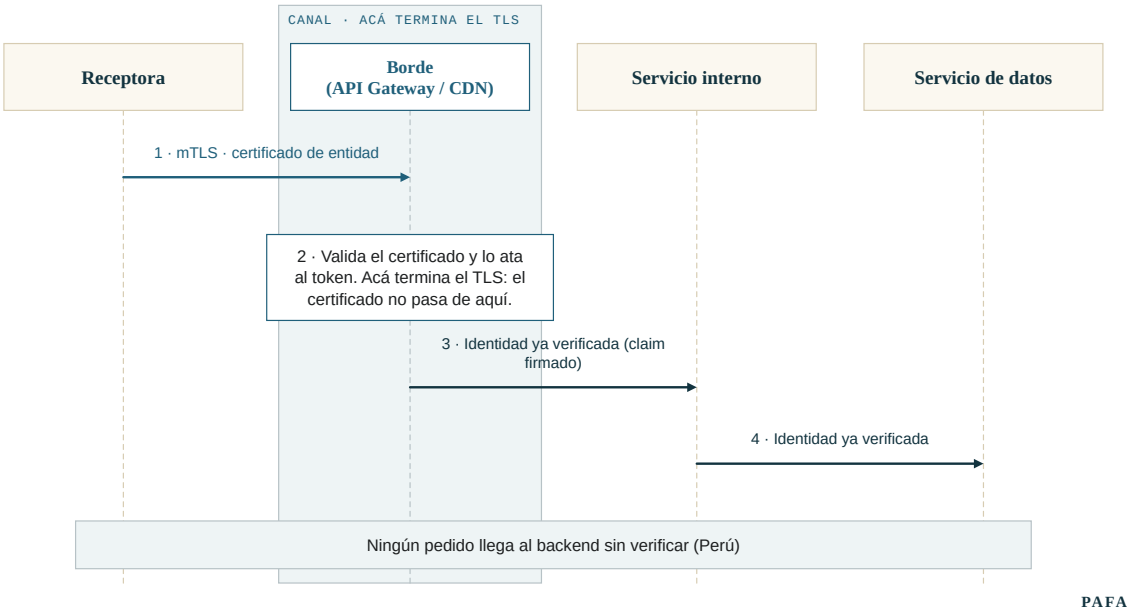


Figura 3 · Dónde termina el TLS: el borde valida el certificado y hacia adentro viaja la identidad verificada

3 · Ciclo de vida: el alta y la baja de una entidad

En esta sección se aborda la dinámica operativa con la que una entidad se integra por primera vez frente a un par desconocido, así como el impacto funcional que genera su eventual salida del ecosistema. Ambas situaciones responden a un principio central: la validez operativa reside en el estado presente de la institución participante, no en la antigüedad ni en el registro original de su alta. A modo de síntesis, la Figura 4 ilustra las tres etapas del ciclo de vida de un participante y las implicancias de cada una.

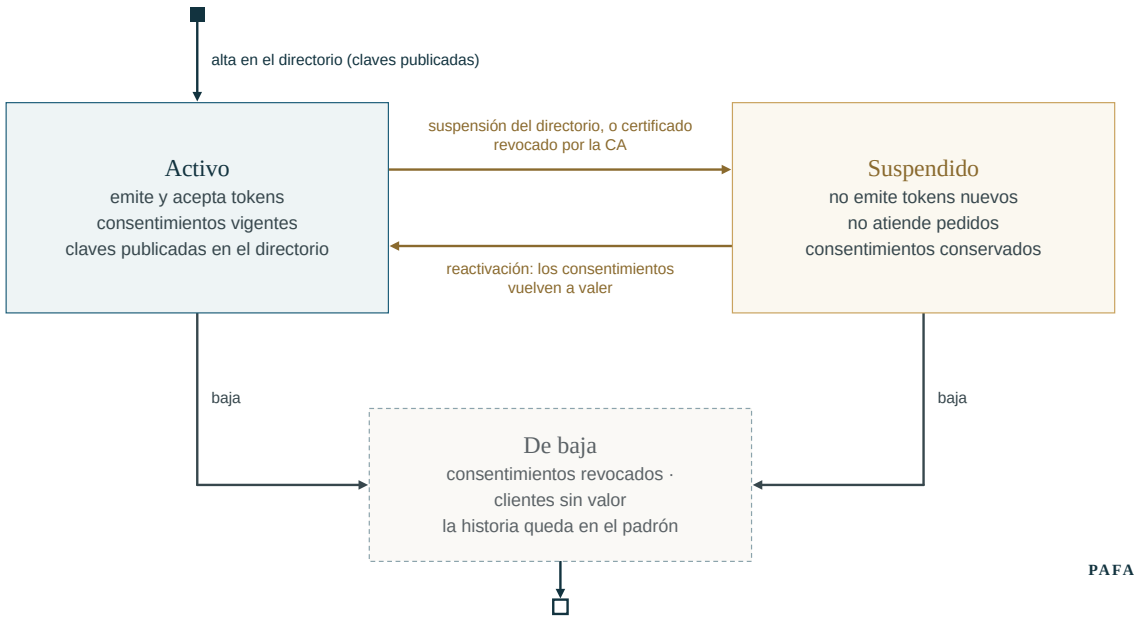


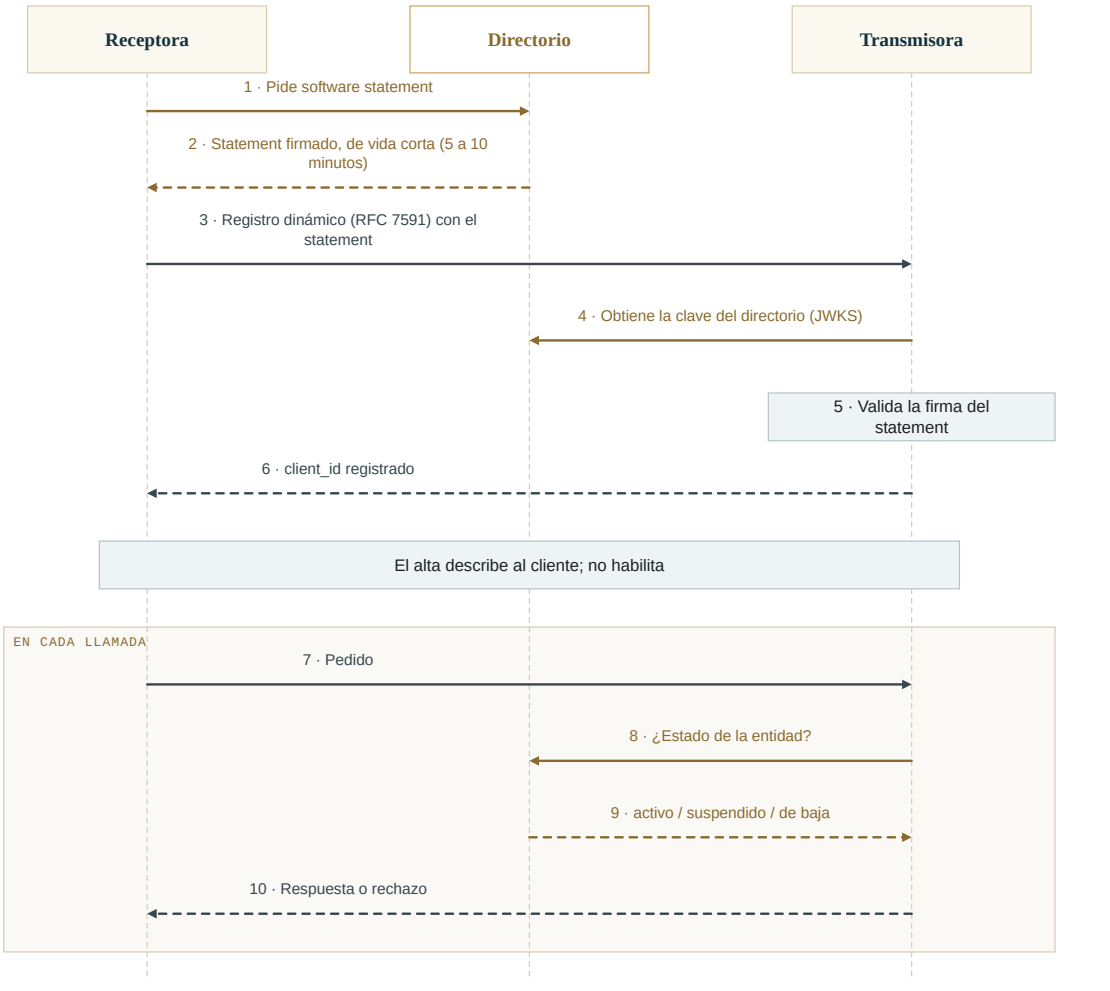
Figura 4 · Ciclo de vida del participante: activo, suspendido y de baja. La suspensión congela y se revierte; la baja extingue

3.1 · El alta: cómo una transmisora conoce a una receptora

Resueltos la gestión del directorio y los certificados, surge una interrogante operativa clave: ¿de qué manera una entidad transmisora reconoce a una receptora sin interacción previa? La regla establecida determina que **toda receptora activa en el directorio queda habilitada para operar con cualquier transmisora sin requerir un alta bilateral.** Los metadatos del cliente provienen exclusivamente del directorio (presentado por la receptora mediante un software statement firmado por dicho organismo) y no de convenios bilaterales. Este enfoque implica tres consecuencias fundamentales:

- **Carácter descriptivo del registro:** El registro únicamente acredita la identidad de la entidad cliente; la vigencia de su capacidad operativa debe revalidarse contra el padrón con *cada* transacción.
- **Dependencia del estado de la entidad:** Si la entidad es suspendida o dada de baja, sus clientes registrados pierden validez en cuanto el cambio de estado se propaga (3.2), indistintamente de la vigencia de sus certificados. Por ello, cada transmisora verifica el estado en cada interacción contra su copia del padrón.
- **Ausencia de trámites bilaterales:** Se elimina la necesidad de que la receptora gestione un alta individual ante cada transmisora, evitando la creación de una red de N×M acuerdos bilaterales entre N receptoras y M transmisoras. Transferencias 3.0 muestra el costo de ese modelo: el canje de certificados mTLS se resuelve con «ceremonias P2P» manuales entre las partes, y el propio documento lista como riesgo el uso de certificados mTLS sin control de emisión [13].

Registro dinámico mediante software statement: En este esquema, la entidad receptora efectúa su registro ante cada transmisora mediante la presentación de una declaración avalada por la firma del directorio (Figura 5). Existen diversos ejemplos representativos internacionales: en Australia, el Registro del CDR genera Declaraciones de Software específicas para cada producto activo de los Receptores de Datos Acreditados [15]; en el Reino Unido, este mecanismo automatizado facilita la inscripción de terceros como clientes de OpenID Connect prescindiendo de intervenciones manuales, fundamentándose en los certificados e instruyendo el uso de Aseveraciones de Declaración de Software (SSA) presentadas por el tercero [11]; Brasil aplica este mismo principio a través de su directorio institucional [16]; Chile también, con statements firmados por el directorio de la CMF (Anexo 3, II.D) [2]; en tanto que Perú requiere estrictamente que dicha declaración provenga en exclusiva de su directorio, siendo expedida a solicitud y con una vigencia temporal acotada [6].



PAFA

Figura 5 · Cómo la transmisora conoce a los clientes: el registro dinámico con software statement. Lo que habilita se pregunta después, en cada llamada.

Entre sus principales ventajas, el registro dinámico se fundamenta en un estándar consolidado (RFC 7591), cuenta con un amplio soporte en los servidores de autorización del mercado y dispone de un plan de conformidad formal para su certificación. No obstante, conlleva dos costos operativos: por un lado, exige que el operador del directorio emita y firme cada declaración; por otro, requiere que la entidad receptora se registre ante cada transmisora (lo que implica N×M llamadas automáticas, aunque sin trámites ni acuerdos previos). Su principal riesgo radica en que la declaración, al ser un extracto firmado de la información pública del directorio, puede quedar desactualizada; por esta razón, su vigencia es acotada.

Las regulaciones internacionales adoptan distintos criterios respecto a cuánto debería ser este plazo: Perú delega su definición en el directorio [6]; Australia impone un límite de 10 minutos [15]; Brasil rechaza statements emitidos más de 5 minutos antes del pedido [16]; y el Reino Unido no fija la vigencia del statement ni sus claims, limitándose a definir un vencimiento para la solicitud de registro [23]. En función de estos antecedentes, el perfil fija que el statement venza a los 10 minutos de emitido (`exp`) y que la transmisora rechace los emitidos hace más de 5 minutos (`iat`).

Una entidad puede tener varios statements, uno por producto o aplicación, como en Australia [15]; el estado, en cambio, es uno por entidad: si se suspende, caen todos sus clientes registrados, con el statement que sea.

3.2 · La baja: cuánto tarda en cortarse y qué queda

El retiro o desvinculación de un participante dentro del ecosistema abarca tres dimensiones esenciales: los mecanismos de interrupción del flujo ante la revocación del certificado o el cese operativo, los tiempos de respuesta requeridos para efectivizar dicho corte y la gestión de los procesos que permanecen en ejecución.

Como el padrón (2.1), la baja ya existe en la normativa: el Registro de PSP prevé el cese a pedido de la entidad, con al menos 30 días de aviso, y por decisión del BCRA ante sanciones, cambios fundamentales en las condiciones para estar inscripto, cambios en la operatoria declarada o 180 días de inactividad [3]. Y tiene la misma limitación que el padrón: es un registro que consultan personas y que cambia en días; el perfil técnico necesita que la baja llegue a las máquinas de las otras entidades en cuestión de minutos.

La baja plantea dos desafíos: **la propagación** (qué tan rápido se entera el resto del ecosistema) y **la reconstrucción** (poder verificar después cuál era el estado de una entidad en un momento dado). La propagación es un problema de latencia; sin embargo, la reconstrucción es un problema de auditoría: sin historia del padrón no se puede probar qué estado tenía una entidad cuando ocurrió un hecho. En las jurisdicciones analizadas, ningún directorio resuelve bien las dos a la vez.

En el caso de la propagación, los casos revisados siguen dos estrategias (Figura 6):

1. **Sondeo periódico (Australia):** con dos frecuencias. Pide consultar las APIs de estado a menudo, para reaccionar en 2 a 5 minutos, y sugiere consultar la API general de receptores cada 6 horas [17]. Separa así el estado (minutos) de los metadatos (horas), pero su registro sólo informa la situación actual, sin fechas de cambio ni historial [15].
2. **Notificación push (Perú y Chile):** el directorio avisa el cambio de estado a las entidades. **Perú** notifica la suspensión o la baja por webhook, en formato CloudEvents firmado y sobre mTLS, con reintentos y acuse de recibo, en un máximo de cinco minutos [6]; Chile, también por webhook con acuse de recibo, lo combina con un sondeo al menos cada 8 horas y una copia local del directorio que se usa si este no responde [2]. El Reino Unido también tiene push, la Event Notification API, pero avisa de eventos de recursos, no de cambios del padrón, y además admite el sondeo como alternativa [18].

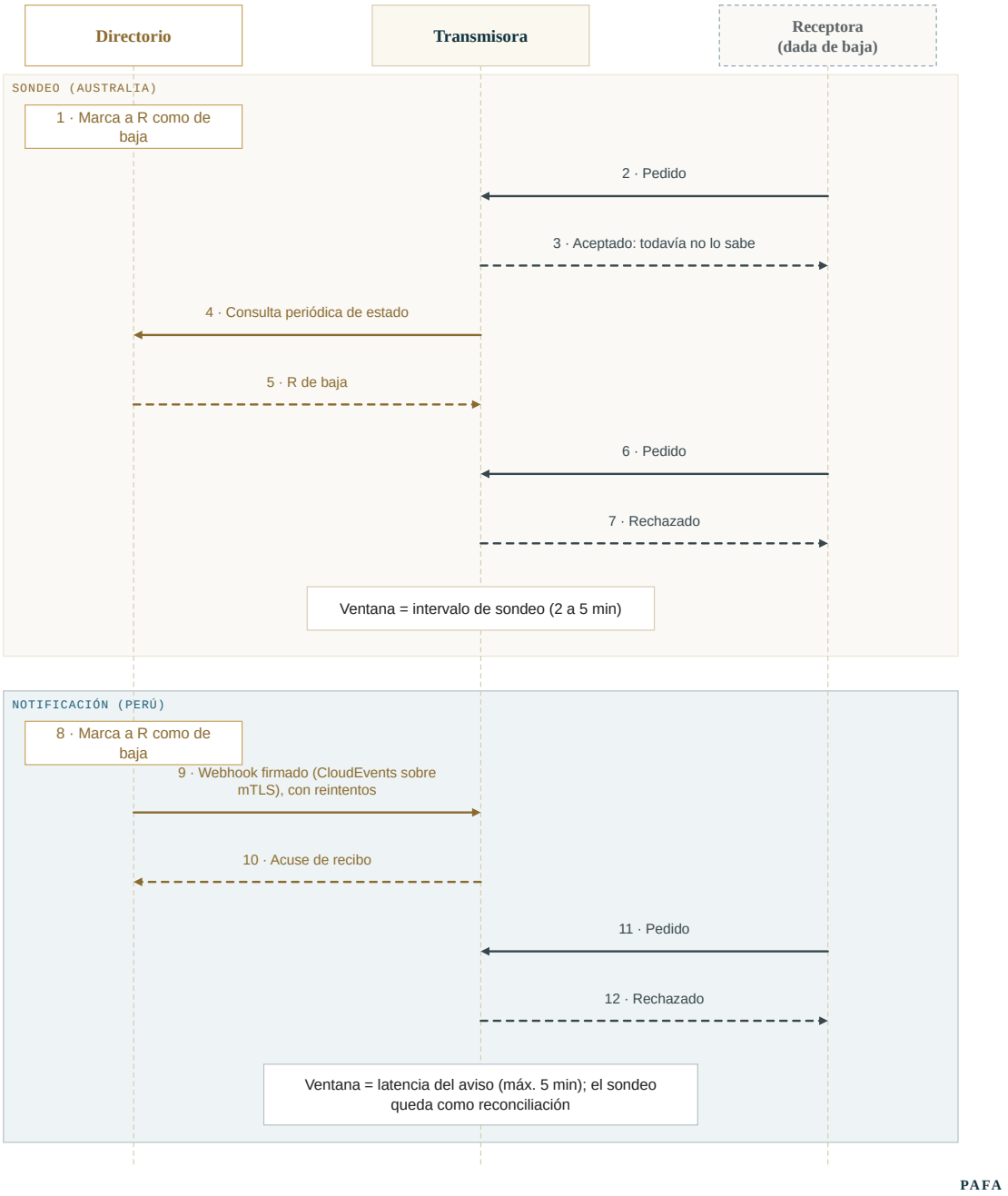


Figura 6 · La baja y su ventana de propagación: con sondeo, la ventana es el intervalo; con notificación, la latencia del aviso

Sobre la **reconstrucción**, ninguno la resuelve del todo. Australia publica sólo el estado actual, sin fechas de cambio [15], aunque los registros que llegan a un estado final se archivan y siguen consultables (`include-archived=true`) [28]. Colombia obliga a la SFC a conservar el registro histórico de las fechas de inclusión y retiro (art. 2.35.8.5.5, num. 7) [20], pero no de las suspensiones. Perú guarda los eventos de cambio de estado durante diez años [6]: la información para auditar existe y el regulador puede pedirla, pero no está a disposición de los participantes del directorio.

Existe un canal de baja independiente del directorio: la revocación del certificado emitida por la CA mediante CRL u OCSP. Resulta fundamental distinguir entre un participante activo con un certificado revocado y un participante suspendido que mantiene un certificado vigente; se trata de dos escenarios distintos que provocan de forma independiente la interrupción del servicio.

En las jurisdicciones analizadas, ambas verificaciones coexisten. En el Reino Unido, la CA de Open Banking publica el estado de sus certificados por OCSP y, como respaldo, CRL [27]; el directorio ofrece además el JWKS y SCIM para detectar bajas [27], y la baja de un participante dispara la revocación automática

de sus certificados [24]. En Australia, la CA del CDR (operada por DigiCert) utiliza OCSP como método principal y CRL como respaldo, exigiendo la verificación de revocación para compartir datos; la baja de un receptor impulsa la revocación de sus certificados en el Registrar, mientras que la suspensión solo inactiva sus productos [15] [26]. En Brasil, el Manual de Segurança obliga, desde el 3 de noviembre de 2026, a verificar la validez de los certificados ICP-Brasil con un mecanismo que cada institución elige dentro de los parámetros que fija la gobernanza (frecuencia mínima de actualización, tolerancia a fallas y una alternativa para cuando el mecanismo no esté disponible), y a poder verificarla aunque ese mecanismo esté caído (ítems 3.28 a 3.30 y 6.18) [25]. Es el mismo criterio que el perfil adopta para el directorio: ante una caída, vale la última información conocida. En Perú, se exige a las CAs de la lista blanca ofrecer OCSP o CRL bajo niveles de servicio definidos [6], mientras que en Chile el vencimiento del certificado sitúa al participante en estado «Desconectado» [2]. En consecuencia, el perfil establece que ambas validaciones son obligatorias y que la revocación del certificado no reemplaza la suspensión en el directorio, ni viceversa.

Con esto en mente, PAFA propone cuatro cosas para la baja. **Primero**, que el aviso salga del directorio: notifica la suspensión o la baja por un canal firmado, con reintentos y acuse de recibo, en una ventana máxima de cinco minutos, como en Perú [6] y Chile [2] (con un estándar como el Shared Signals Framework [19] o un webhook propio); el sondeo queda como reconciliación, y cada transmisora verifica el estado en cada llamada contra su copia del padrón (3.1), que el aviso mantiene al día; si el directorio no responde, vale la última copia, como en Chile [2]. **Segundo**, doble verificación obligatoria: la revocación del certificado por la CA y la suspensión en el directorio cortan por separado y ninguna reemplaza a la otra, como conviven en el Reino Unido [24] y Australia [15]. **Tercero**, historia del padrón: el directorio conserva cada cambio de estado, de roles y de claves con su fecha, como hace Perú durante diez años [6], para que un hecho pueda contrastarse con el estado de la entidad en ese momento; sin embargo, quién podrá consultarla queda para una definición del regulador. **En cuarto lugar**, con relación a los procesos en ejecución, PAFA diferencia conceptual y operativamente entre la suspensión y la baja (Figura 4). La suspensión congela: no se emiten tokens nuevos ni se atienden pedidos, pero los consentimientos se conservan y vuelven a valer con la reactivación de la entidad. La baja, por otro lado, es total: los consentimientos se revocan y no vuelven a ser válidos. Australia y Chile respaldan ese reparto: en Australia la suspensión deja los productos inactivos y se revierte, y la baja revoca certificados e invalida consentimientos [15] [28]; en Chile la cancelación del registro obliga a dejar sin efecto las autorizaciones vigentes [2]. Por otro lado, Perú, Brasil y el Reino Unido no definen, en las fuentes revisadas, un estado suspendido para el consentimiento: cortan la emisión de tokens [6] y la validez de las claves o certificados [16] [27].

4 · Conclusiones y preguntas abiertas

Como se dijo al principio: **para que alguien dé su consentimiento, el sistema tiene que saber antes quién pregunta y quién responde.** Las decisiones de esta capa se ordenan en torno a ese eje:

1. **El participante es la entidad, no el proveedor:** aunque compartan infraestructura, la identidad es propia y responde quien figura en el padrón.
2. **Separación entre autenticación y autorización:** el certificado únicamente valida la autenticidad de la clave, mientras que la habilitación operativa reside en el directorio, permitiendo modificar el ancla de confianza sin alterar la configuración del perfil.
3. **Identificación en tiempo real sin trazabilidad posterior:** el certificado acredita quién posee la clave durante la sesión activa; no obstante, la demostrabilidad de una transacción ante terceros con posterioridad requiere la firma explícita del mensaje (sección 2.4).
4. **Validación descriptiva en el alta:** el registro sirve para comunicar a la entidad transmisora las características y metadatos del cliente, pero la capacidad real para operar debe confirmarse contra el padrón, que cada transmisora mantiene al día, en cada interacción.

El lado positivo para Argentina es que buena parte de la infraestructura ya existe y tiene dueño: el Registro de PSP del BCRA como punto de partida del padrón (2.1), el régimen de tercerización del BCRA para los proveedores (2.2), los web services de ARCA como precedente de separar autenticación y autorización (2.3) y el mTLS de Transferencias 3.0 como canal (2.4). Para completar el esquema, restan definir el padrón técnico orientado al procesamiento automatizado y las reglas que regirán los procesos de alta y baja detallados en la sección 3.

A modo de cierre, esta primera capa plantea tres interrogantes clave que serán abordados detenidamente en la capa 2 (autenticación, consentimiento y autorización):

- **La terminación del TLS y la asociación del token** a la identidad confirmada mediante el certificado.
- **El esquema de autenticación del usuario** para cada operación y la consecuente generación de trazabilidad.
- **El alcance y las especificaciones técnicas de la firma digital**, orientados a garantizar el no repudio de las operaciones realizadas.

Asimismo, persisten interrogantes que el perfil no aborda aún, sea por la escasez de antecedentes o porque exigen una postura explícita de las propias entidades. Con el fin de evitar conclusiones prematuras, estos puntos permanecen abiertos para su examen a la luz de las experiencias internacionales de referencia y de las exigencias operativas que demande la solución.

1. **Entidades con desempeño en múltiples roles:** El Registro de PSP contempla la asignación de varias funciones para una misma entidad [3], mientras que el Decreto 353/2025 no establece regulaciones de reciprocidad [1]. La alternativa en evaluación propone registrar una única entidad en el directorio y especificar sus roles tanto en el padrón como en el software statement, omitiéndolos del certificado digital (en concordancia con la sección 2.3). Bajo este esquema, el identificador de issuer se habilita únicamente al actuar como transmisora, y el registro de clientes opera solo al desempeñarse como receptora. Este enfoque coincide con la práctica en Perú, que gestiona los roles mediante el statement [6]. Por su parte, Chile modela una única persona jurídica pero administra un estado independiente por rol, lo que permite suspender a una institución como receptora sin inhabilitar su función transmisora [2]. La resolución pendiente debe determinar si

un único par de certificados es suficiente para ambos roles, si el estado operativo debe ser global o por función, y de qué forma se explicita el rol actuante en la instancia del consentimiento.

2. **Especificaciones del certificado de entidad:** Queda definido que el certificado vincula una clave pública con una entidad determinada, incorpora el CUIT y prescinde de autorizaciones explícitas (sección 2.3). Asimismo, se establece que cada institución dispondrá de dos certificados independientes (uno de transporte mTLS y uno de firma) sin reutilización de claves, en línea con los modelos de Perú [6], Brasil [21], el Reino Unido [27] y Chile [2] (Anexo 3, IV.B, prueba I-04). Resta precisar en el anexo técnico la estructura mínima del CSR, incluyendo la ubicación del CUIT (ya sea en el campo `serialNumber`, siguiendo la práctica de ARCA en WSAA [12], o en `organizationIdentifier`, bajo el estándar ETSI), así como las definiciones relativas a `keyUsage`, SAN y algoritmos de cifrado.

Fuentes

1. Decreto 353/2025, Poder Ejecutivo Nacional (22/05/2025, BO 23/05/2025), «Trámites de inversión y adquisición de bienes – Simplificación y desregulación» — arts. 5° a 7°, Sistema de Finanzas Abiertas (los arts. 8° y 9° tratan la prevención del lavado de activos y el secreto fiscal). La única modificación que figura en el texto actualizado (Decreto 767/2025) cambia el art. 3; los arts. 5° a 7° siguen como en el original. Verificada el 04/11/2026

2. CMF (Chile) — Norma de Carácter General N° 514, Sistema de Finanzas Abiertas (03/07/2024), texto refundido con la NCG N° 569 (01/06/2026), que incorpora el Anexo Técnico N° 3. Sección I, A: la autenticación reforzada de cliente se define por dos o más elementos independientes de conocimiento, posesión e inherencia (verificada el 22/09/2026). Sección I.C.3: al cancelarse la inscripción, el PSBI debe dejar sin efecto las autorizaciones vigentes. Sección II.C y Anexo 3, I.A: directorio de participantes administrado por la CMF. Sección V.B y Anexo 3, II.E: con el certificado vencido, el participante queda en estado «Desconectado». Anexo 3, I.J: estados independientes por rol. Anexo 3, II.A: certificados de CAs que cumplan WebTrust o ETSI EN 319 411 (la CMF no emite). Copia en la biblioteca. Verificada el 04/11/2026 sobre la copia

3. BCRA — Proveedores de servicios de pago, texto ordenado (al 02/10/2026, Com. «A» 8488). Puntos 1.2.1, definición de PSP, y 1.2.3.2, exclusión de los esquemas de cobro de obligaciones con el Estado; secciones 2.1, registro habilitado por la SEFYC y más de una función registrada; 2.2, inscripción; 2.3, certificado y número de RPSP; 2.5, cese (a pedido, con 30 días de aviso; por el BCRA, por 180 días de inactividad, cambios fundamentales en las condiciones de inscripción, sanciones o cambios en la operatoria, 2.5.2); 4.5, cuentas de pago ofrecidas a través de un tercero (incorporada por la Com. «A» 8432, 30/04/2026). Verificada el 29/09/2026 sobre el texto al 14/07/2026 (Com. «A» 8454), y el 04/11/2026 sobre el texto al 02/10/2026 (puntos 1.2.1, 1.2.3.2, 2.1 y 2.5.2)

4. El Cronista (03/09/2026) — nota de P. Wolffelt sobre el lanzamiento del SFA: el primer caso de uso permitirá autorizar el acceso a información disponible en ARCA; lanzamiento esperado para el primer semestre de 2027. Fuente periodística. Verificada el 29/09/2026

5. iProUP (27/04/2026) — nota de R. Speranza sobre el plan del BCRA: según la nota, que parafrasea a P. Inchauspe (BCRA), el usuario podrá proveer datos de dependencias públicas como ARCA, ANSES o el BCRA. Fuente periodística. Verificada el 29/09/2026

6. SBS (Perú) — [ES] Financial Grade API security profile SFA Perú, versión 14 (13/10/2026), en el Confluence público de la SBS. Directorio operado por la SBS (Cap. 2); lista blanca de CAs, nacionales e internacionales (Cap. 10); sólo mTLS, sin DPoP ni private_key_jwt, y validación en el API Gateway (Cap. 6); FAPI 2.0 Message Signing con firma HTTP de las APIs (Cap. 4); registro dinámico con SSA emitido por el directorio (Cap. 9); notificación por webhook (CloudEvents firmado con JWS, sobre mTLS, con reintentos y acuse de recibo) de la revocación de grants, de los cambios de certificados y de los cambios de estado de un participante, en un máximo de 5 minutos, y retención de eventos por diez años (Cap. 11, §11.5); el AS rechaza las solicitudes de clientes cuyo participante no está habilitado (9.4); el SSA lleva el organization_id, cuya fuente autoritativa es el directorio, y su vigencia la define el directorio (9.1). Es un documento en construcción que se edita; copias de la v12 y la v14 en la biblioteca. Verificada el 28/09/2026 sobre la v12; Caps. 9 y 11, el 04/11/2026 sobre la v14 (sin cambios respecto de la v12)

7. Data Standards Body (DSB), CDR Support Portal (Australia) — Glossary. Definición de CDR Register: lo mantiene la ACCC

8. Banco Central do Brasil — Resolução BCB nº 400, de 04/07/2024. Estructura definitiva de gobernanza del Open Finance: debe empezar a funcionar a más tardar el 02/01/2025 (art. 1, § 1), y desde esa fecha queda revocada la Circular 4.032/2020 de la estructura inicial (art. 15). La operan la Associação Open Finance y la página Estrutura de governança (https://openfinancebrasil.org.br/estrutura-de-governanca/). Verificada el 26/10/2026 y el 04/11/2026

9. BCRA — Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información, texto ordenado (al 13/02/2026, Com. «A» 8401). Sección 10 (la cita textual está en 10.2), gestión de la relación con terceras partes: la entidad que terceriza no queda liberada de sus responsabilidades; contenido mínimo del contrato (10.3.1) y responsabilidad del prestador primario por sus subcontratistas (10.3.2). Alcanza a los PSP inscriptos desde el 04/08/2026. Verificada el 28/09/2026

10. OBIE — eIDAS details. El open banking británico anterior a PSD2, los OB-certs y la revocación prevista de los eIDAS el 31/12/2020 (el documento no trae fecha; es de 2020)

11. Open Banking UK — Knowledge base, Dynamic Client Registration. El SSA y la extensibilidad a cualquier ancla de confianza

12. ARCA — Especificación técnica del WSAA 1.2.2. El certificado X.509 autentica; la autorización a cada servicio vive en un registro aparte, previo trámite

13. Comisión Interbancaria para los Medios de Pago de la República Argentina (CIMPRA), publicado por el BCRA — Transferencias 3.0 · Pull · Consentimiento (2023). Las comunicaciones backend del flujo de generación de token

usan certificado de cliente (mTLS); la conexión back end a back end está siempre protegida por mTLS. Verificada el 29/09/2026

14. OpenID Foundation — FAPI 2.0 Message Signing, especificación final (fechada el 25/09/2025; anunciada el 26/09/2025). Firma de los pedidos y respuestas del flujo de autorización con el no repudio como objetivo explícito. Que la firma de las llamadas a recursos quedó en un borrador aparte surge de la página de especificaciones de la OIDF, no de este documento. Verificada el 22/09/2026
15. Data Standards Body (DSB), Australia — Consumer Data Standards, versión 1.36.0, Information Security Profile: Client Registration y Participant Statuses. SSA por producto de software activo, con vencimiento a los 10 minutos; reacción a los cambios de estado en 5 minutos, sondeando con caché de 2 a 5 minutos; estados y cascada (Suspended→Inactive, Revoked/Surrendered→Removed); los endpoints de estado dan sólo el estado actual; los registros que pasan 2 años en estado final se archivan solos; si el Register no responde, el data holder sigue con el último estado conocido. Verificada el 04/11/2026
16. Open Finance Brasil — Dynamic Client Registration v2.1.0, §7.1. El software_statement no puede haberse emitido más de 5 minutos antes del pedido de registro; §9.4, las claves de certificados revocados pasan a un keystore inactivo del directorio. Verificada el 29/09/2026 sobre la v2.0.0; el 04/11/2026, el registro de cambios de la v2.1.0 muestra un solo cambio (un alcance nuevo en §7.2), así que §7.1 y §9.4 siguen igual. Copia de la v2.1.0 en la biblioteca
17. Data Standards Body (DSB), CDR Support Portal (Australia) — Data Holder cache update periods. Estado en 2-5 minutos, metadatos de receptores cada 6 horas
18. Open Banking UK — Event Notification API Profile v3.1.8 (ya hay una v4.0.1; la cita es de la v3.1.8). Eventos de recursos, no de padrón; sondeo agregado como alternativa al push
19. OpenID Foundation — Shared Signals Framework 1.0, especificación final (publicada el 29/08/2025). Publicación y suscripción de eventos firmados entre entidades. Verificada el 22/09/2026; fecha verificada el 04/11/2026
20. Ministerio de Hacienda y Crédito Público (Colombia) — Decreto 0368 del 07/04/2026. Sistema de finanzas abiertas obligatorio; directorio de participantes administrado por la SFC (art. 2.35.8.5.1), que debe conservar el registro histórico de las fechas de inclusión y retiro (art. 2.35.8.5.5, num. 7), con hasta 12 meses desde la entrada en vigor para ponerlo en funcionamiento (art. 4, num. 2). No regula certificados: los estándares de seguridad los fija la SFC (art. 2.35.8.3.6). Verificada el 04/11/2026 sobre la copia de CETA, porque el sitio de Presidencia devuelve 403
21. Open Finance Brasil — Padrão de Certificados, versión 3.0 (publicada el 15/09/2026). Certificados de ACs de la ICP-Brasil para transporte (BRCAC) y firma (BRSeal); la 3.0 migra el BRCAC a la Família AE de la ICP-Brasil por fases, con coexistencia, y no cambia el BRSeal. Los atributos del DN que cita el texto (serialNumber = CNPJ, organizationIdentifier = OFBBR- y UID = ID del software statement) son de la versión 2.1, §5.2.2.1 (página de la 2.1 (https://openfinancebrasil.atlassian.net/wiki/spaces/OF/pages/24 Que la 3.0 los mantenga no se pudo confirmar contra el texto (el cuerpo de §5.5, §5.7 y cap. 8 no se extrae). Verificada el 26/10/2026
22. OpenID Foundation — FAPI 2.0 Security Profile, especificación final. Aprobada como especificación final en febrero de 2025 (publicada el 22/02/2025). Admite mTLS y DPoP para atar el token al cliente. Verificada el 26/10/2026
23. Open Banking UK — Dynamic Client Registration Specification v3.3 (§ Software Statement y Data Dictionary). No fija los claims del SSA (los deja al emisor); el exp obligatorio es del pedido de registro. Hay una v3.4, con copia en la biblioteca, que no cambia los claims ni el exp
24. Open Banking UK — Directory API Specification v2.2.1 (keystore del directorio en keystore.openbanking.org.uk y vigencia de un año del certificado firmante) y Open Banking Certificate Policy v1.7 (18/11/2025): §4.9.1 y §4.9.3, revocación automática de los certificados cuando el participante se retira; §4.9.6 y §4.9.10, el control de revocación por quien confía se remite al PKI Disclosure Statement; §4.9.13, sin suspensión de certificados; §5.6, cambio de la clave de la CA; §7.2.1, servicio de estado en línea obligatorio para la CA. Documentación con acceso registrado; copia de la Certificate Policy en la biblioteca. Verificada el 26/10/2026 y el 04/11/2026 sobre la copia
25. Banco Central do Brasil — Instrução Normativa BCB nº 720 (02/04/2026), publica la versión 5.0 del Manual de Segurança do Open Finance y revoca la IN 305/2022. Ítems 3.28 a 3.30 y 6.18, verificación de validez de los certificados con un mecanismo elegido según parámetros de la gobernanza (frecuencia de actualización, tolerancia a fallas y alternativa ante indisponibilidad), que debe poder hacerse aunque el mecanismo esté caído; vigentes desde el 03/11/2026. Verificada el 26/10/2026 y el 04/11/2026
26. CDR Support Portal (Australia) — Certificate Validation. La CA del CDR es DigiCert, endosada por la ACCC; OCSP es el mecanismo preferido (cada certificado trae su responder; actualización dentro de las 2 horas de notificada una revocación) y DigiCert publica CRL al menos cada 24 horas, que quien valida puede usar como respaldo; sin verificación de revocación no se comparten datos. Sin fecha. Verificada el 27/10/2026
27. Open Banking UK — Directory 2.0 Technical Overview v1.7 (16/08/2024). La CA de Open Banking ofrece OCSP y, como respaldo, CRL en CDN; el directorio da además el JWKS y SCIM para detectar bajas; al retirarse una entidad, su software statement pasa a «inactive» y sus certificados se revocan. Distingue los certificados de transporte y de firma. Verificada el 03/11/2026
28. Consumer Data Standards Australia — CDR Register Design Reference, versión 1.5.0 (archivada, 2020–2021). Se cita sólo para lo que las Consumer Data Standards vigentes [15] no traen: el JWKS del Register sin autenticación, pensado para distribuirse por CDN; los registros en estado final archivados y consultables con include-archived=true; y la reversión de la suspensión