Layer 1 · Identity and trust between participants

Author: Eber Bezzone | **Date:** 2026-11-03 | **Version:** V 0.1

How two entities that do not know each other prove they belong to the system: the directory, roles, certificates and the channel, and how they are onboarded and removed.

Before any user consent is issued or accepted, the system needs to identify who is requesting the information, who will answer the request, and the current operational status of both parties.

1 · Introduction

If we take an open finance system apart, we can distinguish five closely related layers: identity and trust; authentication, consent and authorisation; resources; observability; and governance. To those five we add a cross-cutting layer, audit, which does not occupy a level of its own but runs through all five layers above (Figure 1).

In a scenario with two participants of the ecosystem (a transmitting entity and a receiving entity), both must prove their identity and their current permissions before the account holder can give consent. The aim of this paper is to analyse that first layer of **identity and trust between participants**: the mechanism by which two entities with no prior relationship validate who they are and establish secure communication. This process focuses exclusively on identifying the entities, leaving customer authentication to be developed in layer 2.

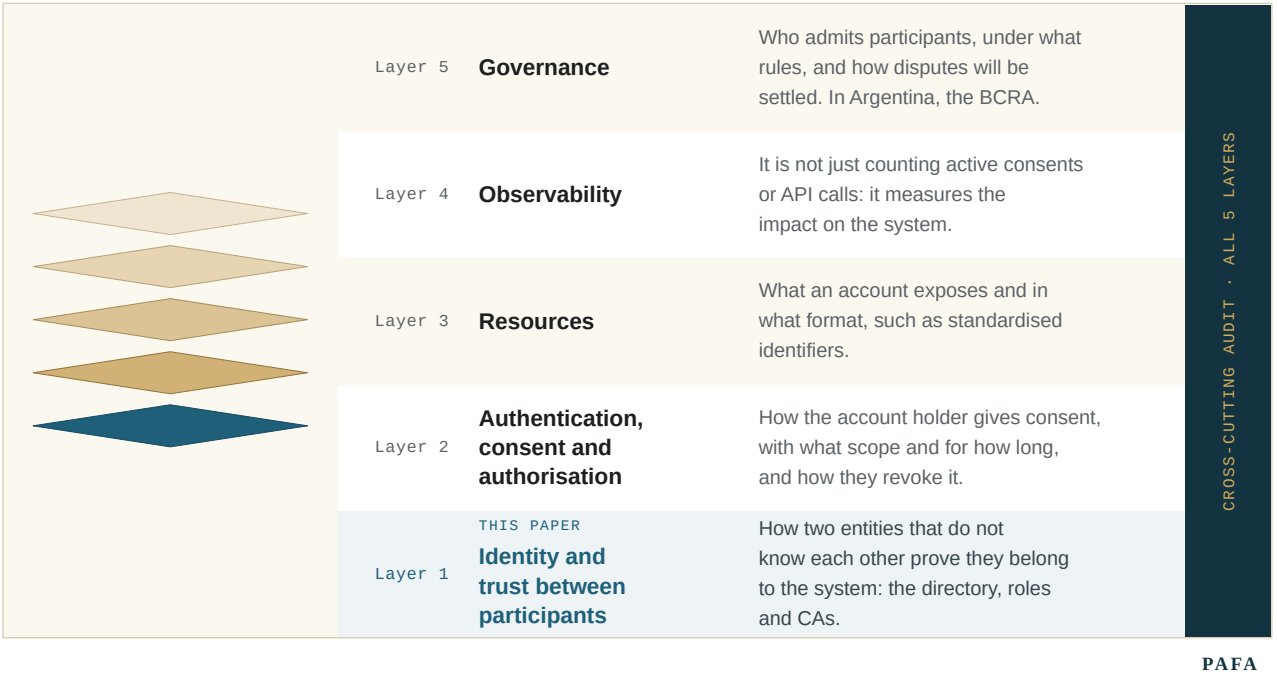


Figure 1 · The layers of the ecosystem. Layer 1: Identity and trust between participants

2 · Components of layer 1

Before the account holder gives consent, the transmitting entity must validate four fundamental aspects of the receiving entity requesting the information: check that it is a valid participant, confirm that it holds the right role, authenticate its identity and establish the secure communication channel to be used. If any of these points cannot be verified, the interaction must stop before the user's consent.

To answer each of these questions, the profile structures the layer into four main components: the participant **directory**, the associated **roles and permissions**, the certificate scheme together with the **certification authority**, and the secure **communication channel**.

2.1 · The directory: who takes part and their status

Argentina currently has a formal participant register: the Central Bank of the Argentine Republic (BCRA) keeps the Register of Payment Service Providers, enabled by the SEFYC [3]. To register, an entity must complete an official procedure in which it submits its CUIT (tax ID), corporate name, addresses, appointed officers and the list of shareholders holding 10 % or more. Once compliance with the requirements has been validated, the BCRA grants a «registration certificate», thereby assigning the corresponding entry in the Register of Payment Service Providers (RPSP) [3].

However, this list is administrative in nature and meant to be consulted by people. It therefore does not meet the needs of an open finance ecosystem, which requires an interoperable technical directory that the systems of the various financial institutions can process automatically and immediately.

Decree 353/2025, which creates the Open Finance System, tasks the BCRA with setting the requirements to be met by “the other bodies of the National Executive Branch and the entities of the financial system” that take part in the system (art. 6) [1]. According to what has been announced, the first use case will be sharing information held by ARCA (the tax authority), with a launch expected for the first half of 2027 [4], and other sources mention further bodies such as ANSES (the social security administration) [5]. None of them can be registered: the RPSP is for legal persons that, without being financial entities, perform a function in a retail payment scheme, and it excludes schemes for collecting obligations owed to the State (1.2.1 and 1.2.3.2) [3]. The technical directory, then, cannot be a copy of the BCRA's register: it will have to be a register of its own, including the registered entities and those bodies, with their role.

At a minimum, that register should expose:

1. the organisation, with an identifier of its own in the directory and its associated CUIT (see below)
2. the enabled roles
3. the status (active, suspended, removed) and since when
4. the entity's public keys, for transport and for signing, published by the directory as a key set (JWKS) per participant
5. the entity's issuer, if it is a transmitting entity, and the base URL of its resources

As for the identifier, there are two candidates at hand: the RPSP registration number assigned by the BCRA [3] and the CUIT, which identifies the entity before the whole State. The RPSP number is not enough: it leaves out public bodies, which are not registered. The CUIT, on the other hand, is held by all of them, ARCA and ANSES included, and could serve as the identifier. The profile decides that the directory assigns each participant an identifier of its own, stable, that does not change with roles or status: the CUIT identifies the legal person before the State, not the participant in the system. The CUIT stays associated with that identifier and is one of the data items that will travel in the certificate, without depending on onboarding in the directory (2.3). This is what Chile does: its directory assigns each participant an identifier within the open finance system that is different from the RUT (Annex 3, I.D, Table 1) [2]; and in Argentina, Transferencias 3.0 already identifies entities in its tokens (`iss`, `aud`, `client_id`) with the BCRA's five-digit entity code, a third candidate to bear in mind [13].

That the BCRA regulates it does not mean it has to operate it. Both models coexist in the cases reviewed. In Australia, Peru, Chile and Colombia, the directory is operated by the regulator itself: the ACCC [7], the SBS [6], the CMF [2] and the SFC, which has until April 2027 to put it in place [20]. In Brazil, by contrast, since January 2025 the infrastructure has been governed by an ecosystem association, the Associação Open Finance, under the Central Bank's rules [8]. For this layer, who operates the directory is an axis independent of the profile: the profile tries to describe what the directory must be able to do, regardless of who ends up operating it.

Whoever operates it, it must be able to meet three technical requirements:

1. Publish a status change so that it propagates to every other entity.
2. Allow the register to be reconstructed as of a given date.
3. Suspend an entity without removing it.

The directory also has a key of its own: with it, it signs software statements (3.1) and, if it notifies status changes, the notices (3.2). That key is the root of trust for the whole layer: a transmitting entity accepts a statement because it verifies the directory's signature, and it can verify the signature because it obtained the key from an address it knows in advance. The United Kingdom publishes it in the directory keystore, with a signing certificate valid for one year [24]; Brazil, in its directory's JWKS [16]; Australia, at an unauthenticated Register endpoint meant to be distributed through a CDN [28]; Peru requires statements and webhooks to be validated against the directory's public JWKS, without fixing its address [6]. None of them sets the rotation period or the overlap. This profile proposes what the cases leave implicit: **the directory's key is published at a well-known address, the new key is published before the old one stops being used, and custody belongs to the directory operator.**

2.2 · Roles: who can be a participant

In every open finance system a new player appears, especially with smaller entities: the **providers** offering technology services to those small entities. This raises the question of who should be registered in the directory, the financial entity or the technology operator. The directory registers entities with their identifier, roles and status. A technology provider may operate the infrastructure of many entities, but it should not have an identity of its own in the register, nor enabled roles. Three consequences follow:

- **One issuer per entity** (the server that issues that entity's tokens), discovered from the directory and not inferred from the domain.
- **The certificate is issued in the entity's name**, even if the provider holds the key. A provider certificate operating on behalf of several entities is not allowed.
- **Accountability towards the ecosystem is not delegated: the entity answers for what its provider does on its behalf**. The contract with the provider splits the tasks, and the regulator can request and audit it, but this does not remove the entity's responsibility. That does not prevent asking something of the provider: that it shows, through a certification or an audit submitted by the entity, that it meets what the profile requires, without thereby having an identity of its own in the register.

This is not a rule the profile proposes: the BCRA has already set it twice. For entities that outsource technology, the consolidated text on technology and information security risks says that entities that outsource “shall not be released from their responsibilities, present or future”, and requires the contract with the third party to set out the parties' responsibilities, the right to audit and unrestricted access for the entity and the SEFYC, including over subcontractors; and that obligation has applied to PSPs since 4 August 2026 [9]. And the case closest to this section is that of PSPs that provide payment accounts through a third party's interface. Since May 2026, the consolidated text on PSPs says that the third party's customers “are customers of the PSP”, and that this arrangement “does not release the PSP from complying with all the regulations”. Moreover, it is the PSP that must set the requirements for the third party by contract and verify that it meets them [3].

2.3 · Certificates and Certification Authority (CA)

Every participant needs to prove, on every connection, that it is who it claims to be. That is what certificates are for: digital documents that bind a public key to an identity, in this case that of an entity of the ecosystem. They are signed by a certification authority (CA), which verifies that identity before issuing and then publishes its status (valid or revoked). The set of CAs the ecosystem accepts is its trust anchor, and who operates them is a choice: the ecosystem can have a CA of its own or accept third-party CAs that meet certain requirements. Both models appear in the cases reviewed: Australia [15] and the United Kingdom [10] operate an ecosystem CA (in the United Kingdom, alongside eIDAS qualified CAs); Peru [6] and Chile [2] accept third-party CAs that meet certain requirements: Peru, those on an allow-list; Chile, those audited under WebTrust or ETSI EN 319 411 (Annex 3, II.A), without the CMF issuing certificates.

In short, the CA and the directory play complementary but clearly bounded roles: while the certificate

confirms that the caller holds a key bound to an entity, it is up to the directory to check whether that entity holds the enablement and the role required for the request at hand. In this way, the authenticity of the key (which the CA proves) is clearly decoupled from operational authorisation (which the directory validates).

This separation of directory and certification authority gives the flexibility to change the trust anchor without restructuring the ecosystem. A case in point is the United Kingdom, which has already changed its trust anchor twice. British open banking started with certificates issued by the OBIE; with PSD2 it moved to eIDAS certificates; and faced with Brexit, with the revocation of British entities' eIDAS certificates scheduled for 31 December 2020, it considered going back to Open Banking certificates, which almost the whole ecosystem was already using [10]. In fact, its dynamic registration specification explicitly provides for several anchors: “the DCR specification provides the extensibility to use an SSA from any trust anchor (not just the Open Banking Directory)” [11].

Brazil, on the other hand, chose to couple the certificate to the directory. Although it does not run a CA of its own, it requires certificates issued by ICP-Brasil authorities that include the participant code together with the software statement identifier assigned by the directory [21]. This architecture means that any change in the directory or in the trust anchor directly affects the certificate profile. In contrast, Peru's model offers more flexibility: it allows certificates from third-party CAs on its directory's allow-list (such as international entities with WebTrust or ETSI audits, or national ones belonging to the Official Electronic Signature Infrastructure), avoiding directory metadata inside the certificate structure [6].

In Argentina we have a local precedent, even if it is outside the financial system. ARCA's web services have worked with this separation for years: the X.509 certificate “implements the authentication of the external entity's computers”, with the CUIT in the DN (serialNumber=CUIT 30123456789), but the authorisation for each service lives separately [12]. The certificate carries no permissions; it simply authenticates, and then the register enables. It is the same split the profile proposes, running at national scale and already implemented by anyone who has integrated electronic invoicing.

That is why not tying the certificate to the directory is not an aesthetic choice: it lets any accepted CA issue the certificate without waiting for onboarding in the directory, and it allows the trust anchor to change without touching the profile, which is what Brazil gave up by putting directory data in the certificate.

Although the certificate contains no directory information, the directory does not ignore it. Following the model adopted by Peru [6], Brazil [16] and the United Kingdom [24], the entity must register its public keys (transport and signing) in the directory and keep them up to date, and the directory publishes them. In this way, on every connection, the transmitting entity performs a double validation (Figure 2): it checks that the certificate comes from an authorised CA and is valid (not revoked), and it confirms that the key presented matches one of those actively published in the directory for that institution. Because the entity can only operate once the directory publishes its data, the certificate can be obtained before formal onboarding. Finally, for message signing, only the key registered in the directory is considered valid, and its validity is checked against the register's history.

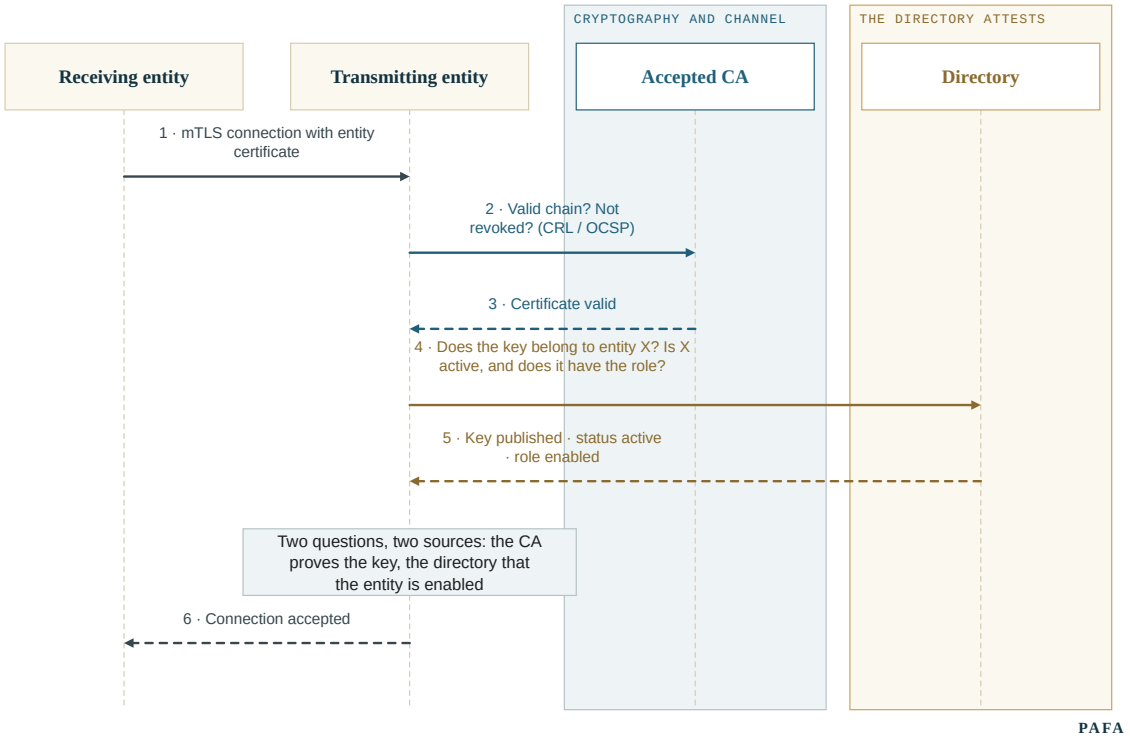


Figure 2 · What the certificate proves and what the directory proves

2.4 · The channel: how entities talk, and its boundary

The channel between entities should be mTLS, something Argentine entities already run: in Transferencias 3.0, the connection between back ends always uses mTLS [13]. There is no reason to change it.

What matters about the channel is not the choice but its **boundary**, and layer 2 builds on it. When there is an API gateway, a service mesh or a CDN at the edge of the network, TLS should terminate there: the client certificate is validated at the edge and does not reach the application. It is not that the certificate is missing; it is that its trace does not propagate inwards into the entity's own environment. Keeping mTLS on every internal hop is possible, but the profile chooses not to require it, for two reasons. The first is cost: every hop adds certificates to issue, rotate and deploy, and that cost is not paid once but on every change to the internal architecture. The second is scope: the profile sets how entities talk to each other; how each entity protects its internal network is its own responsibility and is already regulated, for financial entities and PSPs, by the BCRA's consolidated text on technology risks [9]; for public bodies, the requirement would have to come from the requirements the BCRA sets under art. 6 of the decree [1]. What the profile does require is the outcome: that no request reaches internal services unless the receiving entity's identity has been verified at the edge and travels inwards already verified. How each entity achieves this, with internal mTLS or by passing on the verified identity (Figure 3), is each organisation's decision.

Peruvian regulation supports this second route: it allows the point where mTLS terminates (for example, the API gateway) to validate the certificate against the token, as long as no request reaches the back end unverified [6].

Layer 2 defines how the token is bound to that identity, using either mTLS or DPoP, the two mechanisms provided for by FAPI 2.0 [22]. The restriction in Chile [2] and Peru, which only allow mTLS [6], is also addressed in that layer.

Since mTLS only attests the parties' identity for the duration of the active session, once the connection ends no record remains that a third party could audit. In the event of disputes, unrecognised transactions or security incidents, every critical message must be digitally signed with a key formally bound to the

entity through the directory. It must also be possible to check the register's history for that institution on the specific date of the event, which is why the directory keeps its history (section 2.1).

The FAPI 2.0 Message Signing standard [14] determines which messages must be signed (a matter detailed in layer 2). In addition, PAFA sets out in that layer the schemes and formats for signing resource requests (taking as reference Peru's use of RFC 9421 [6]), and its first application will be the revocation of consent between entities.

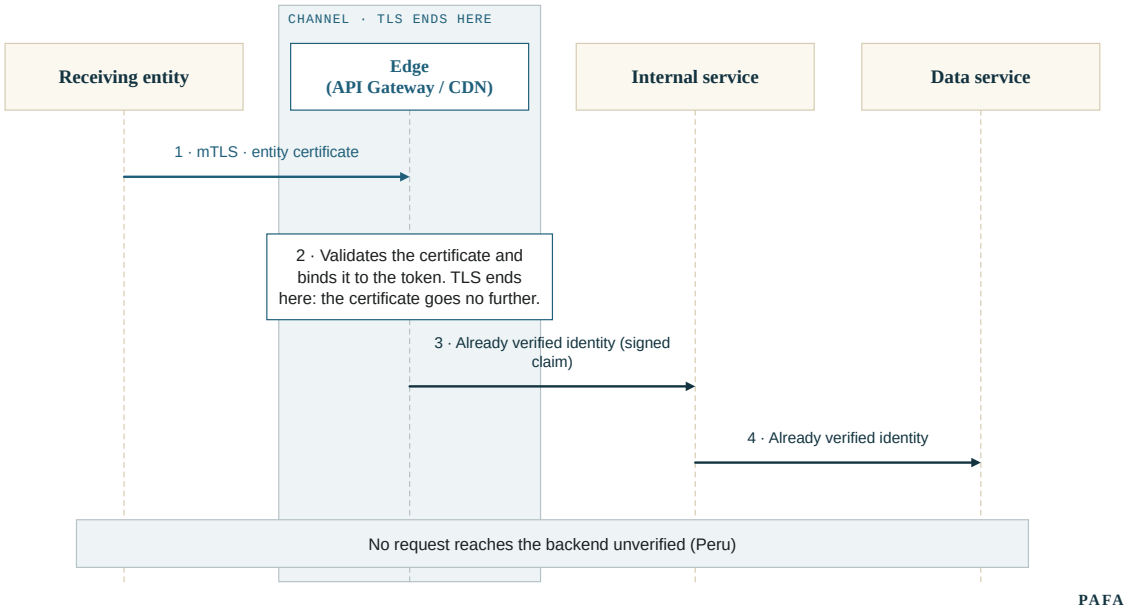


Figure 3 · Where TLS terminates: the edge validates the certificate and the verified identity travels inwards

3 · Lifecycle: onboarding and removal of an entity

This section covers how an entity first connects with an unknown counterpart, and the functional impact of its eventual exit from the ecosystem. Both situations follow one central principle: operational validity lies in the participant's present status, not in its seniority or in the original record of its onboarding. As a summary, Figure 4 shows the three stages of a participant's lifecycle and what each one implies.

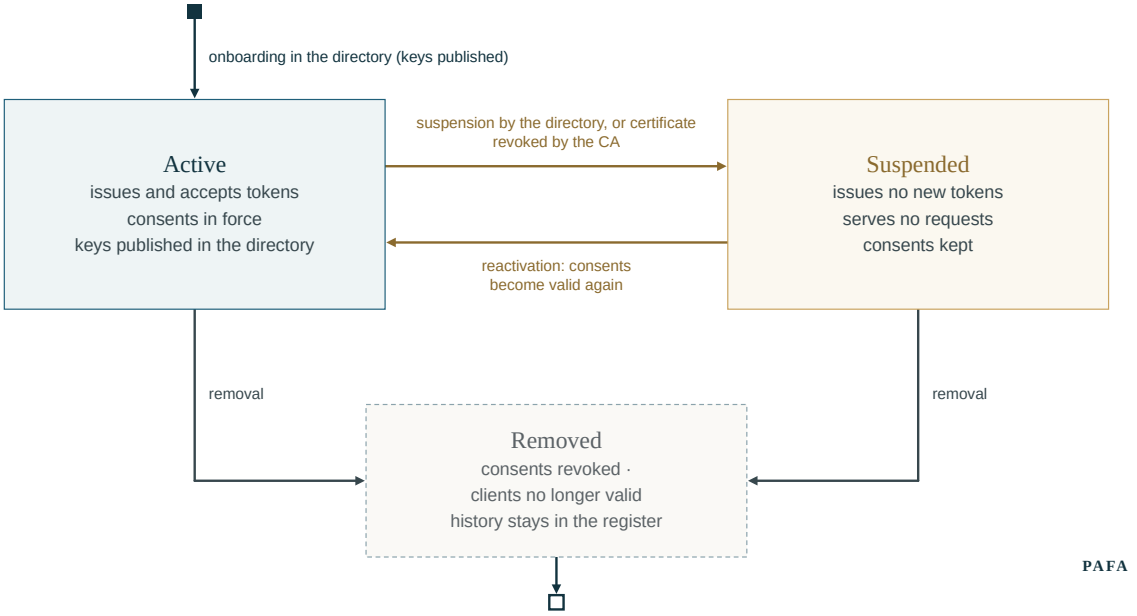


Figure 4 · Participant lifecycle: active, suspended and removed. Suspension freezes and can be reversed; removal ends everything

3.1 · Onboarding: how a transmitting entity gets to know a receiving entity

With directory management and certificates settled, a key operational question arises: how does a transmitting entity recognise a receiving entity with no prior interaction? The rule is that **every receiving entity active in the directory is enabled to operate with any transmitting entity, without bilateral onboarding.** The client metadata comes exclusively from the directory (presented by the receiving entity through a software statement signed by the directory) and not from bilateral agreements. This approach has three fundamental consequences:

- **Registration is descriptive:** Registration only attests the identity of the client entity; whether it can still operate must be revalidated against the register on *every* transaction.
- **Dependence on the entity's status:** If the entity is suspended or removed, its registered clients lose validity as soon as the status change propagates (3.2), regardless of whether its certificates are still valid. That is why each transmitting entity checks the status on every interaction against its copy of the register.
- **No bilateral procedures:** The receiving entity no longer needs to go through individual onboarding with each transmitting entity, avoiding a web of N×M bilateral agreements between N receiving and M transmitting entities. Transferencias 3.0 shows the cost of that model: the exchange of mTLS certificates is handled through manual «P2P ceremonies» between the parties, and the document itself lists the use of mTLS certificates without issuance control as a risk [13].

Dynamic registration with a software statement: In this scheme, the receiving entity registers with each transmitting entity by presenting a statement backed by the directory's signature (Figure 5). There are several representative international examples: in Australia, the CDR Register issues software statements for each active product of Accredited Data Recipients [15]; in the United Kingdom, this automated mechanism lets third parties register as OpenID Connect clients without manual intervention, based on certificates and on Software Statement Assertions (SSAs) presented by the third party [11]; Brazil applies the same principle through its institutional directory [16]; Chile does too, with statements signed by the CMF's directory (Annex 3, II.D) [2]; while Peru strictly requires the statement to come only from its directory, issued on request and with a limited validity [6].

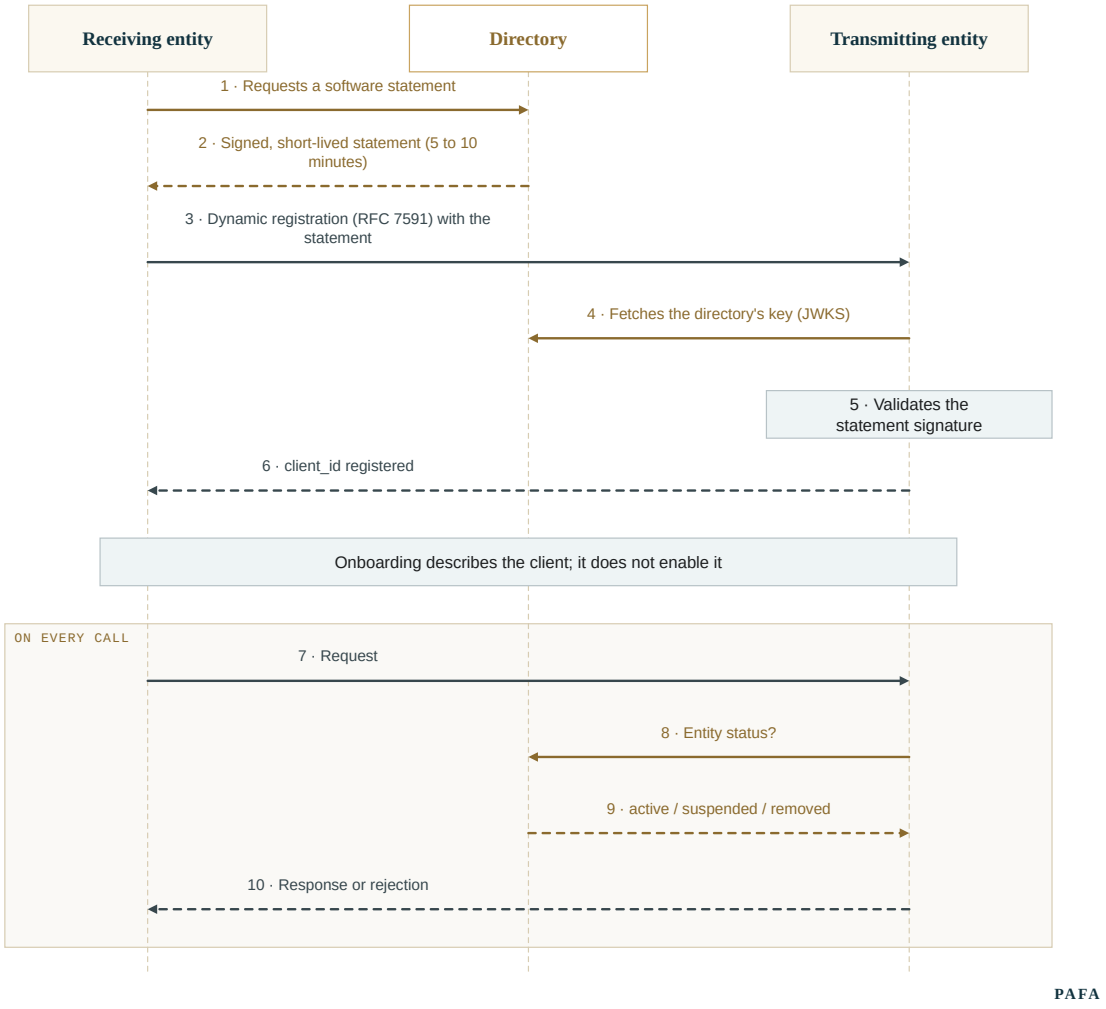


Figure 5 · How the transmitting entity gets to know its clients: dynamic registration with a software statement. What it is enabled to do is asked afterwards, on every call.

Among its main advantages, dynamic registration rests on an established standard (RFC 7591), is widely supported by authorisation servers on the market and has a formal conformance programme for certification. However, it carries two operational costs: on the one hand, the directory operator must issue and sign every statement; on the other, the receiving entity must register with each transmitting entity (which means N×M automated calls, though without paperwork or prior agreements). Its main risk is that the statement, being a signed extract of the directory's public information, can become outdated; that is why its validity is short.

International regulations take different views on how long that should be: Peru leaves it to the directory [6]; Australia sets a 10-minute limit [15]; Brazil rejects statements issued more than 5 minutes before the request [16]; and the United Kingdom sets neither the statement's validity nor its claims, only an expiry for the registration request [23]. Based on these precedents, the profile sets that the statement expires 10 minutes after issuance (`exp`) and that the transmitting entity rejects statements issued more than 5 minutes earlier (`iat`).

An entity may have several statements, one per product or application, as in Australia [15]; status, on the other hand, is one per entity: if it is suspended, all its registered clients fall, whatever the statement.

3.2 · Removal: how long it takes to cut off and what remains

The withdrawal of a participant from the ecosystem has three essential dimensions: the mechanisms that stop the flow when the certificate is revoked or operations cease, the response times needed to make that cut effective, and the handling of processes still running.

Like the register (2.1), removal already exists in regulation: the PSP Register provides for exit at the entity's request, with at least 30 days' notice, and by decision of the BCRA in the event of sanctions, fundamental changes in the conditions for being registered, changes in the declared operations or 180 days of inactivity [3]. And it has the same limitation as the register: it is a record consulted by people that changes over days; the technical profile needs removal to reach the other entities' machines within minutes.

Removal poses two challenges: **propagation** (how quickly the rest of the ecosystem finds out) and **reconstruction** (being able to check afterwards what an entity's status was at a given moment). Propagation is a latency problem; reconstruction, however, is an audit problem: without the register's history it cannot be proven what status an entity had when something happened. In the jurisdictions analysed, no directory solves both well at once.

For propagation, the cases reviewed follow two strategies (Figure 6):

1. **Periodic polling (Australia):** with two frequencies. It asks for the status APIs to be checked often, to react within 2 to 5 minutes, and suggests checking the general recipients API every 6 hours [17]. It thus separates status (minutes) from metadata (hours), but its register only reports the current situation, with no change dates or history [15].
2. **Push notification (Peru and Chile):** the directory notifies entities of the status change. **Peru** notifies suspension or removal by webhook, as signed CloudEvents over mTLS, with retries and acknowledgement, within five minutes at most [6]; Chile, also by webhook with acknowledgement, combines it with polling at least every 8 hours and a local copy of the directory used if the directory does not respond [2]. The United Kingdom also has push, the Event Notification API, but it reports resource events, not register changes, and also allows polling as an alternative [18].

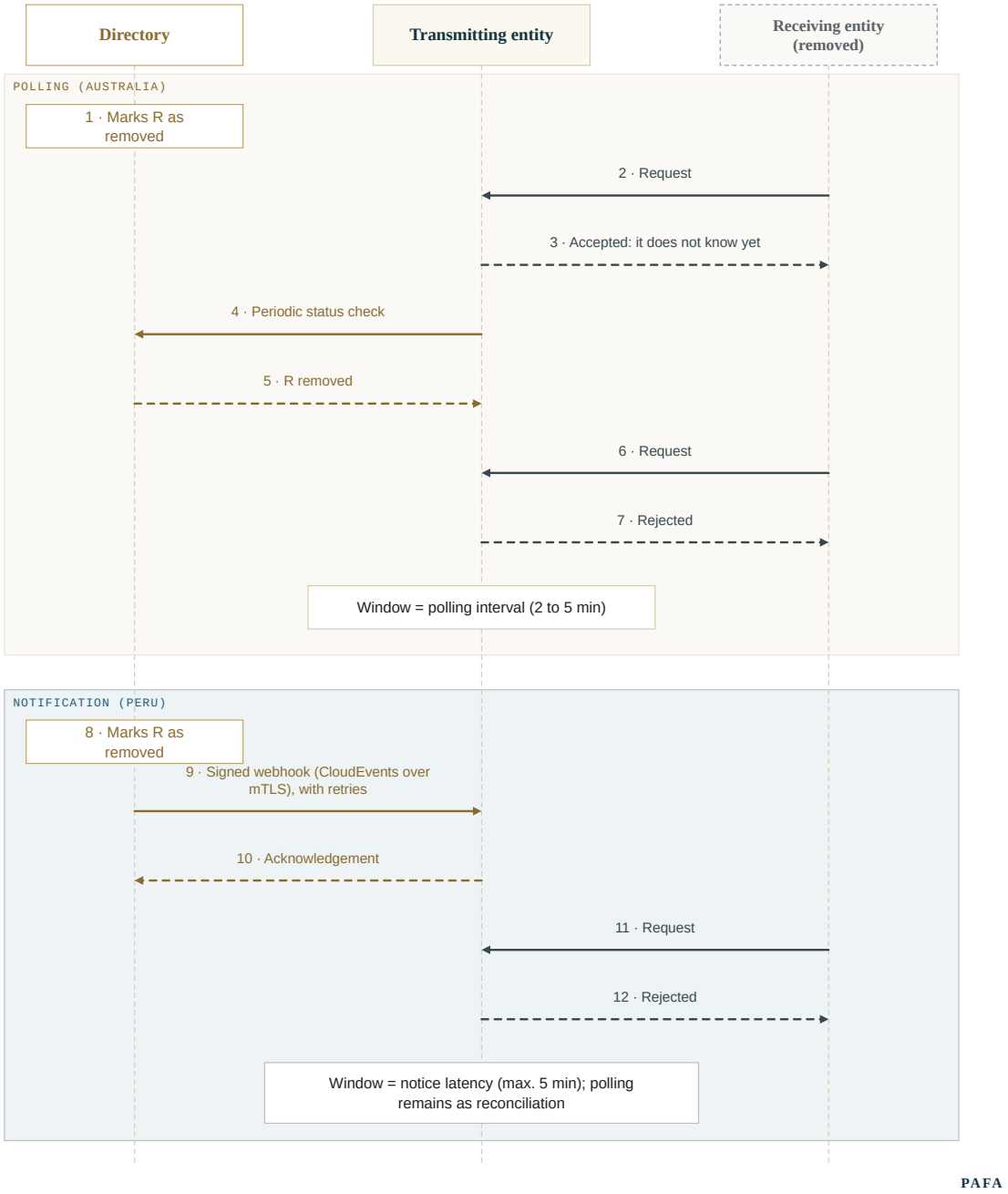


Figure 6 · Removal and its propagation window: with polling, the window is the interval; with notification, the latency of the notice

As for **reconstruction**, none solves it fully. Australia publishes only the current status, with no change dates [15], although records that reach a final status are archived and remain queryable (`include-archived=true`) [28]. Colombia requires the SFC to keep the historical record of inclusion and withdrawal dates (art. 2.35.8.5.5, item 7) [20], but not of suspensions. Peru keeps status-change events for ten years [6]: the information for auditing exists and the regulator can request it, but it is not available to the directory's participants.

There is a removal channel independent of the directory: certificate revocation issued by the CA through CRL or OCSP. It is essential to distinguish between an active participant with a revoked certificate and a suspended participant that still holds a

valid certificate; these are two different scenarios that each, independently, interrupt the service.

In the jurisdictions analysed, both checks coexist. In the United Kingdom, the Open Banking CA publishes the status of its certificates through OCSP and, as a fallback, CRL [27]; the directory also offers the JWKS and SCIM to detect removals [27], and the removal of a participant automatically triggers the revocation of its certificates [24]. In Australia, the CDR CA (operated by DigiCert) uses OCSP as its main method and CRL as a fallback, and requires revocation checking in order to share data; the removal of a recipient triggers the revocation of its certificates in the Register, while suspension only makes its products inactive [15] [26]. In Brazil, since 3 November 2026 the Manual de Segurança requires the validity of ICP-Brasil certificates to be checked with a mechanism each institution chooses within the parameters set by governance (minimum update frequency, fault tolerance and an alternative for when the mechanism is unavailable), and requires that it can be checked even if that mechanism is down (items 3.28 to 3.30 and 6.18) [25]. It is the same criterion the profile adopts for the directory: in an outage, the last known information applies. In Peru, CAs on the allow-list must offer OCSP or CRL under defined service levels [6], while in Chile certificate expiry places the participant in «Disconnected» status [2]. Accordingly, the profile establishes that both checks are mandatory and that certificate revocation does not replace suspension in the directory, nor the other way round.

With this in mind, PAFA proposes four things for removal. **First**, that the notice comes from the directory: it notifies suspension or removal over a signed channel, with retries and acknowledgement, within a maximum window of five minutes, as in Peru [6] and Chile [2] (with a standard such as the Shared Signals Framework [19] or a webhook of its own); polling remains for reconciliation, and each transmitting entity checks the status on every call against its copy of the register (3.1), which the notice keeps up to date; if the directory does not respond, the last copy applies, as in Chile [2]. **Second**, mandatory double checking: certificate revocation by the CA and suspension in the directory each cut off separately and neither replaces the other, as they coexist in the United Kingdom [24] and Australia [15]. **Third**, register history: the directory keeps every change of status, roles and keys with its date, as Peru does for ten years [6], so that an event can be checked against the entity's status at that moment; who will be able to consult it, however, is left for the regulator to define. **Fourth**, regarding processes still running, PAFA distinguishes conceptually and operationally between suspension and removal (Figure 4). Suspension freezes: no new tokens are issued and no requests are served, but consents are kept and become valid again when the entity is reactivated. Removal, on the other hand, is final: consents are revoked and never become valid again. Australia and Chile support that split: in Australia suspension makes products inactive and can be reversed, while removal revokes certificates and invalidates consents [15] [28]; in Chile cancellation of the registration requires current authorisations to be voided [2]. Peru, Brazil and the United Kingdom, on the other hand, do not define, in the sources reviewed, a suspended status for consent: they stop token issuance [6] and the validity of keys or certificates [16] [27].

4 · Conclusions and open questions

As stated at the beginning: **for someone to give consent, the system must first know who is asking and who is answering.** The decisions of this layer are organised around that axis:

1. **The participant is the entity, not the provider:** even if they share infrastructure, the identity is the entity's own, and whoever appears in the register is accountable.
2. **Separation of authentication and authorisation:** the certificate only validates the authenticity of the key, while operational enablement lives in the directory, which allows the trust anchor to change without altering the profile.
3. **Real-time identification without later traceability:** the certificate attests who holds the key during the active session; proving a transaction to third parties afterwards, however, requires an explicit message signature (section 2.4).
4. **Descriptive validation at onboarding:** registration tells the transmitting entity the client's characteristics and metadata, but the actual ability to operate must be confirmed on every interaction against the register, which each transmitting entity keeps up to date.

The good news for Argentina is that much of the infrastructure already exists and has an owner: the BCRA's PSP Register as the starting point for the

register (2.1), the BCRA's outsourcing regime for providers (2.2), ARCA's web services as a precedent for separating authentication and authorisation (2.3) and the mTLS of Transferencias 3.0 as the channel (2.4). To complete the scheme, what remains is to define the technical register for automated processing and the rules for the onboarding and removal processes detailed in section 3.

To close, this first layer raises three key questions that will be addressed in detail in layer 2 (authentication, consent and authorisation):

- **TLS termination and binding the token** to the identity confirmed through the certificate.
- **The user authentication scheme** for each operation and the resulting traceability.
- **The scope and technical specifications of the digital signature**, aimed at guaranteeing non-repudiation of the operations performed.

There are also questions the profile does not yet address, either because precedents are scarce or because they require an explicit position from the entities themselves. To avoid premature conclusions, these points remain open for examination in the light of the international reference experiences and of the operational demands of the solution.

1. **Entities acting in more than one role:** The PSP Register allows several functions to be assigned to the same entity [3], while Decree 353/2025 sets no reciprocity rules [1]. The option under evaluation is to register a single entity in the directory and specify its roles both in the register and in the software statement, leaving them out of the digital certificate (consistent with section 2.3). Under this scheme, the issuer identifier is enabled only when acting as a transmitting entity, and client registration only works when acting as a receiving entity. This approach matches practice in Peru, which handles roles through the statement [6]. Chile, for its part, models a single legal person but keeps an independent status per role, which allows an institution to be suspended as a receiving entity without disabling its transmitting function [2]. What remains to be decided is whether a single pair of certificates is enough for both roles, whether operational status should be global or per function, and how the acting role is made explicit at the time of consent.
2. **Specifications of the entity certificate:** It is settled that the certificate binds a public key to a given entity, includes the CUIT and carries no explicit authorisations (section 2.3). It is also established that each institution will have two independent certificates (one for mTLS transport and one for signing) without key reuse, in line with the models of Peru [6], Brazil [21], the United Kingdom [27] and Chile [2] (Annex 3, IV.B, test I-04). What remains to be specified in the technical annex is the minimum CSR structure, including where the CUIT goes (either in the `serialNumber` field, following ARCA's practice in WSAA [12], or in `organizationIdentifier`, under the ETSI standard), as well as the definitions for `keyUsage`, SAN and cryptographic algorithms.

Sources

1. Decree 353/2025, National Executive Branch (22/05/2025, Official Gazette 23/05/2025), «Trámites de inversión y adquisición de bienes – Simplificación y desregulación» — arts. 5 to 7, Open Finance System (arts. 8 and 9 deal with anti-money-laundering and tax secrecy). The only amendment in the updated text (Decree 767/2025) changes art. 3; arts. 5 to 7 remain as in the original. Checked 04/11/2026
2. CMF (Chile) — General Rule No. 514, Open Finance System (03/07/2024), consolidated with General Rule No. 569 (01/06/2026), which adds Technical Annex No. 3. Section I, A: strong customer authentication is defined by two or more independent elements of knowledge, possession and inherence (checked 22/09/2026). Section I.C.3: when a registration is cancelled, the PSBI must void current authorisations. Section II.C and Annex 3, I.A: participant directory run by the CMF. Section V.B and Annex 3, II.E: with an expired certificate, the participant goes into «Disconnected» status. Annex 3, I.J: independent statuses per role. Annex 3, II.A: certificates from CAs meeting WebTrust or ETSI EN 319 411 (the CMF does not issue). Copy in the library. Checked 04/11/2026 on the copy
3. BCRA — Payment service providers, consolidated text (as of 02/10/2026, Communication «A» 8488). Points 1.2.1, definition of PSP, and 1.2.3.2, exclusion of schemes for collecting obligations owed to the State; sections 2.1, register enabled by

the SEFYC and more than one registered function; 2.2, registration; 2.3, certificate and RPSP number; 2.5, exit (on request, with 30 days' notice; by the BCRA, for 180 days of inactivity, fundamental changes in the registration conditions, sanctions or changes in operations, 2.5.2); 4.5, payment accounts offered through a third party (added by Communication «A» 8432, 30/04/2026). Checked 29/09/2026 on the text as of 14/07/2026 (Communication «A» 8454), and 04/11/2026 on the text as of 02/10/2026 (points 1.2.1, 1.2.3.2, 2.1 and 2.5.2)

4. El Cronista (03/09/2026) — article by P. Wolffelt on the launch of the Open Finance System: the first use case will allow authorising access to information held by ARCA; launch expected for the first half of 2027. Press source. Checked 29/09/2026

5. iProUP (27/04/2026) — article by R. Speranza on the BCRA's plan: according to the article, which paraphrases P. Inchauspe (BCRA), users will be able to provide data from public bodies such as ARCA, ANSES or the BCRA. Press source. Checked 29/09/2026

6. SBS (Peru) — [ES] Financial Grade API security profile SFA Perú, version 14 (13/10/2026), on the SBS's public Confluence. Directory run by the SBS (Ch. 2); allow-list of national and international CAs (Ch. 10); mTLS only, no DPoP or private key jwt, and validation at the API gateway (Ch. 6); FAPI 2.0 Message Signing with HTTP signatures on the APIs (Ch. 4); dynamic registration with an SSA issued by the directory (Ch. 9); webhook notification (CloudEvents signed with JWS, over mTLS, with retries and acknowledgement) of grant revocations, certificate changes and participant status changes, within 5 minutes at most, and event retention for ten years (Ch. 11, §11.5); the AS rejects requests from clients whose participant is not enabled (9.4); the SSA carries the organization id, whose authoritative source is the directory, and its validity is set by the directory (9.1). It is a document under construction that keeps being edited; copies of v12 and v14 in the library. Checked 28/09/2026 on v12; Chs. 9 and 11, 04/11/2026 on v14 (unchanged from v12)

7. Data Standards Body (DSB), CDR Support Portal (Australia) — Glossary. Definition of the CDR Register: maintained by the ACCC

8. Banco Central do Brasil — Resolução BCB nº 400, of 04/07/2024. Definitive governance structure of Open Finance: it must start operating by 02/01/2025 at the latest (art. 1, § 1), and from that date Circular 4.032/2020 on the initial structure is revoked (art. 15). It is run by the Associação Open Finance; see the Estrutura de governança page (https://openfinancebrasil.org.br/estrutura-de-governanca/). Checked 26/10/2026 and 04/11/2026

9. BCRA — Minimum requirements for managing and controlling technology and information security risks, consolidated text (as of 13/02/2026, Communication «A» 8401). Section 10 (the quotation is in 10.2), management of third-party relationships: an entity that outsources is not released from its responsibilities; minimum contract content (10.3.1) and the primary provider's responsibility for its subcontractors (10.3.2). Applies to registered PSPs from 04/08/2026. Checked 28/09/2026

10. OBIE — eIDAS details. British open banking before PSD2, the OB certificates and the planned revocation of eIDAS certificates on 31/12/2020 (the document is undated; it is from 2020)

11. Open Banking UK — Knowledge base, Dynamic Client Registration. The SSA and extensibility to any trust anchor

12. ARCA — WSAA technical specification 1.2.2. The X.509 certificate authenticates; authorisation for each service lives in a separate register, after a procedure

13. Interbank Commission for Means of Payment of the Argentine Republic (CIMPRA), published by the BCRA — Transferencias 3.0 · Pull · Consentimiento (2023). Back-end communications in the token generation flow use a client certificate (mTLS); the back-end to back-end connection is always protected by mTLS. Checked 29/09/2026

14. OpenID Foundation — FAPI 2.0 Message Signing, final specification (dated 25/09/2025; announced 26/09/2025). Signing of authorisation-flow requests and responses with non-repudiation as an explicit goal. That signing of resource calls was left to a separate draft comes from the OIDF specifications page, not from this document. Checked 22/09/2026

15. Data Standards Body (DSB), Australia — Consumer Data Standards, version 1.36.0, Information Security Profile: Client Registration and Participant Statuses. SSA per active software product, expiring after 10 minutes; reacting to status changes within 5 minutes, polling with a 2 to 5 minute cache; statuses and cascade (Suspended → Inactive, Revoked/Surrendered → Removed); the status endpoints give only the current status; records that

spend 2 years in a final status are archived automatically; if the Register does not respond, the data holder carries on with the last known status. Checked 04/11/2026

16. Open Finance Brasil — Dynamic Client Registration v2.1.0, §7.1. The software statement cannot have been issued more than 5 minutes before the registration request; §9.4, keys of revoked certificates move to an inactive keystore in the directory. Checked 29/09/2026 on v2.0.0; on 04/11/2026, the v2.1.0 changelog shows a single change (a new scope in §7.2), so §7.1 and §9.4 are unchanged. Copy of v2.1.0 in the library
17. Data Standards Body (DSB), CDR Support Portal (Australia) — Data Holder cache update periods. Status within 2-5 minutes, recipient metadata every 6 hours
18. Open Banking UK — Event Notification API Profile v3.1.8 (v4.0.1 now exists; the citation is from v3.1.8). Resource events, not register events; polling added as an alternative to push
19. OpenID Foundation — Shared Signals Framework 1.0, final specification (published 29/08/2025). Publishing and subscribing to signed events between entities. Checked 22/09/2026; date checked 04/11/2026
20. Ministry of Finance and Public Credit (Colombia) — Decree 0368 of 07/04/2026. Mandatory open finance system; participant directory run by the SFC (art. 2.35.8.5.1), which must keep the historical record of inclusion and withdrawal dates (art. 2.35.8.5.5, item 7), with up to 12 months from entry into force to put it into operation (art. 4, item 2). It does not regulate certificates: security standards are set by the SFC (art. 2.35.8.3.6). Checked 04/11/2026 on the CETA copy, because the Presidency's site returns 403
21. Open Finance Brasil — Padrão de Certificados, version 3.0 (published 15/09/2026). Certificates from ICP-Brasil CAs for transport (BRCAC) and signing (BRSeal); 3.0 migrates the BRCAC to ICP-Brasil's Família AE in phases, with coexistence, and does not change the BRSeal. The DN attributes cited in the text (serialNumber = CNPJ, organizationIdentifier = OFBBR- and UID = software statement ID) are from version 2.1, §5.2.2.1 (version 2.1 page (https://openfinancebrasil.atlassian.net/wiki/spaces/OF/pages/246054913)). Whether 3.0 keeps them could not be confirmed against the text (the body of §5.5, §5.7 and ch. 8 cannot be extracted). Checked 26/10/2026
22. OpenID Foundation — FAPI 2.0 Security Profile, final specification. Approved as a final specification in February 2025 (published 22/02/2025). Allows mTLS and DPoP to bind the token to the client. Checked 26/10/2026
23. Open Banking UK — Dynamic Client Registration Specification v3.3 (§ Software Statement and Data Dictionary). It does not fix the SSA claims (it leaves them to the issuer); the mandatory exp belongs to the registration request. There is a v3.4, with a copy in the library, that changes neither the claims nor the exp
24. Open Banking UK — Directory API Specification v2.2.1 (directory keystore at keystore.openbanking.org.uk and one-year validity of the signing certificate) and Open Banking Certificate Policy v1.7 (18/11/2025): §4.9.1 and §4.9.3, automatic revocation of certificates when the participant withdraws; §4.9.6 and §4.9.10, revocation checking by relying parties is referred to the PKI Disclosure Statement; §4.9.13, no certificate suspension; §5.6, CA key changeover; §7.2.1, online status service mandatory for the CA. Documentation with registered access; copy of the Certificate Policy in the library. Checked 26/10/2026 and 04/11/2026 on the copy
25. Banco Central do Brasil — Instrução Normativa BCB nº 720 (02/04/2026), publishes version 5.0 of the Open Finance Manual de Segurança and revokes IN 305/2022. Items 3.28 to 3.30 and 6.18, checking certificate validity with a mechanism chosen within governance parameters (update frequency, fault tolerance and an alternative when unavailable), which must be possible even if the mechanism is down; in force from 03/11/2026. Checked 26/10/2026 and 04/11/2026
26. CDR Support Portal (Australia) — Certificate Validation. The CDR CA is DigiCert, endorsed by the ACCC; OCSP is the preferred mechanism (each certificate carries its responder; updated within 2 hours of a revocation being notified) and DigiCert publishes a CRL at least every 24 hours, which relying parties may use as a fallback; without revocation checking no data is shared. Undated. Checked 27/10/2026
27. Open Banking UK — Directory 2.0 Technical Overview v1.7 (16/08/2024). The Open Banking CA offers OCSP and, as a fallback, a CRL on a CDN; the directory also provides the JWKS and SCIM, to detect removals; when an entity withdraws, its software statement becomes «inactive» and its certificates are revoked. It distinguishes transport and signing certificates. Checked 03/11/2026
28. Consumer Data Standards Australia — CDR Register Design Reference, version 1.5.0

(archived, 2020–2021). Cited only for what the current Consumer Data Standards [15] do not cover: the unauthenticated Register JWKS, meant to be distributed through a CDN; records in a final status archived and queryable with include-archived=true; and the reversal of suspension