BIS CGIDE

Reporte

API para el Intercambio de Datos (Data-Sharing)-Agregación de Cuentas.

Diciembre 2022

Informe sobre APIs para el intercambio de datos

- **El presente informe es la tercera publicación de la serie sobre open finance y APIs, dirigida por el BCRP,** en el marco del grupo de trabajo técnico de expertos en bancos centrales de las Américas formado por el BIS en febrero del 2020 (CGIDE).

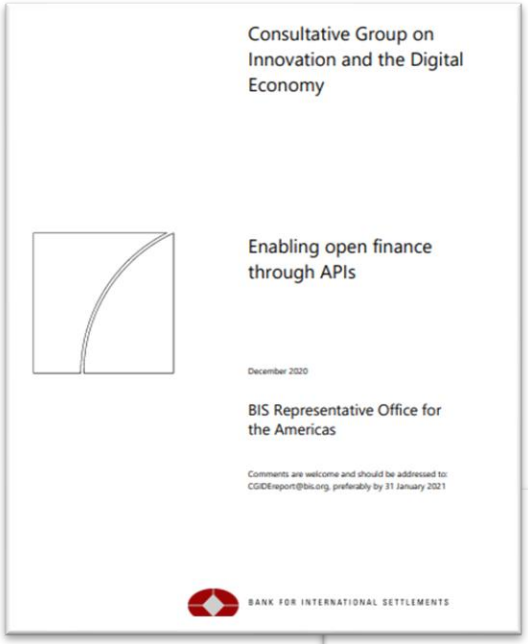
Los informes previos fueron:

- "**Enabling open finance through APIs**" (Dic. 2020)

  Explora los problemas técnicos que rodean el desarrollo de una API de identificación y autenticación que podría usarse para implementar soluciones de open finance administradas de forma privada y pública con alta escalabilidad.

- "**Report on payment initiation**" (Sep. 2021)

  Analiza dos arquitecturas de API alternativas para la iniciación de pagos, ambas basadas en una aplicación de autenticación para teléfonos móviles desarrollada y mantenida por un validador central (CV).



https://www.bis.org/publ/othp36.pdf

https://www.bis.org/publ/othp41.pdf

Contenido

- Introducción
- Conceptos claves
- Modelos de data-sharing
- Interacción y flujos de datos
- Consideraciones tecnológicas
- Lecciones aprendidas de iniciativas de otros países
- Conclusiones

https://www.bis.org/publ/othp56.pdf

Introducción

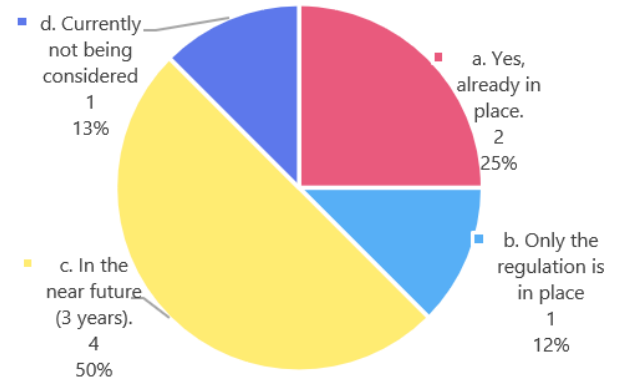
Se realizó una encuesta dirigida a los ocho bancos centrales que participan del grupo técnico del CGIDE

- Los datos de la encuesta mostraron que **la mayoría de los participantes ya han implementado el intercambio de datos como parte de sus iniciativas de open finance o planean implementarlo dentro de los próximos tres años** (Figura A).

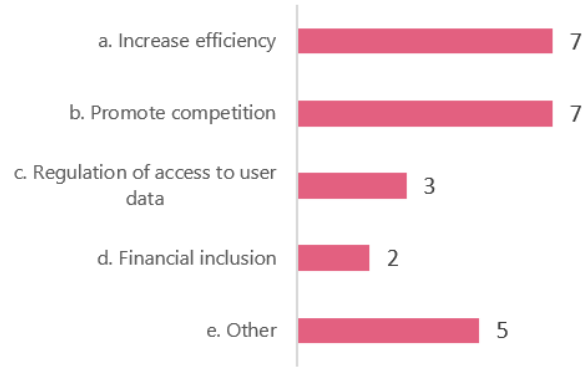
- Los factores principales para adoptar e implementar el intercambio de datos (Figura B) son:
  - Fomentar la eficiencia
  - Promover la competencia.

- Otros factores que resultaron importantes para algunos participantes:
  - Necesidad de regular el acceso a los datos
  - Mejorar la inclusión financiera
  - Promover la innovación
  - Mejorar la seguridad y privacidad de los datos, entre otros.

A. Is your country considering data-sharing as part of open finance initiatives?



B. What would be the key drivers for data-sharing adoption/implementation?



Conceptos claves

API (Interfaz de Programación de Aplicaciones)

- Una API es un conjunto de funciones utilizadas por un programa de software para proporcionar una interfaz que permite que otros programas de consumo (terceros) se conecten e interactúen con él.

- Una API contiene:
  - Protocolos de comunicación
  - Requisitos de intercambio de datos
  - Políticas de acceso y consumo
  - Integridad y gestión confidencial

- Para implementar soluciones de intercambio de datos basadas en API se necesitan normas internacionales y aceptadas por el sector. Los estándares más comunes son:
  - OpenAPI, para la especificación de las APIs que permite documentarlas y diseñarlas de manera consistente;
  - REST o SOAP, como estilo de arquitectura;
  - JSON o XML, como formato de mensajería;
  - OAuth, como estándar de autorización;
  - entre otros.

Conceptos claves

El intercambio de datos o data-sharing

- El intercambio de datos es uno de los principales pilares de las iniciativas de open banking.
- Es la práctica que facilita a los proveedores externos (terceros) el acceso a los datos bancarios de los usuarios, previo su consentimiento.
- El intercambio de datos promueve la transparencia en una sociedad digital y respalda altos niveles de reciprocidad y cooperación dentro del ecosistema financiero.

Algunos beneficios del intercambio de datos:

- Promover una sociedad digital transparente.
- Lograr la reciprocidad y la cooperación en el ecosistema financiero.
- Combinar datos de diversas fuentes para mejorar el rendimiento y el valor de los servicios.
- Permite una mejor toma de decisiones y la entrega de mejores productos.
- Empoderar la propiedad de los datos de los ciudadanos.

Modelos regulatorios de data-sharing

Market-Driven

- **Este modelo es impulsado por la propia industria.**
- En este tipo de modelo, los marcos regulatorios no existen o son fluidos, sin requisitos en cuanto al intercambio de datos.
- Los proveedores terceros (TPP) no tienen que lidiar con marcos de privacidad complejos o reglas de cumplimiento costosas.
- El open banking en esta versión de libre mercado permite que los TPP accedan a las API de los bancos para brindar nuevos servicios a los clientes.

Regulatory-Driven

- **Impulsado por la regulación y puede ser de forma obligatoria. Este enfoque es aplicable cuando se identifican problemas de competencia en el mercado bancario.**
- En ese contexto, la regulación es obligatoria para abrir el mercado, por lo que los TPP y las pequeñas instituciones financieras pueden acceder a las API de los bancos con el consentimiento del propietario de los datos.
- Este modelo busca la reciprocidad de los grandes bancos, con mayores volúmenes de datos, con entidades más pequeñas

https://www2.deloitte.com/ie/en/pages/financial-services/articles/Creating_an_Open_Banking_data_sharing_ecosystem.html

Conceptos claves

Proveedores de datos (DP)

- **Son las entidades que tienen los datos financieros de los usuarios finales**
- Los DP se pueden ver como repositorios externos de datos financieros.
- La estandarización y armonización de dichos repositorios y servicios asociados, es un punto de partida relevante para cualquier iniciativa de open banking y data-sharing ya que cada DP puede maneja su propio estándar.

DP: Pueden ser bancos, compañías de seguros, fondos mutuos, corredores de bolsa e incluso agencias gubernamentales.

Consumidores de datos (DC)

- **Los consumidores de datos pueden ser proveedores terceros de servicios financieros que requieren constantemente acceso a datos granulares y precisos sobre los clientes actuales y potenciales para brindarles servicios más personalizados.**
- La entrega de valor es una constante de estas organizaciones; por lo tanto, acceder a los datos de sus clientes alojados por los proveedores de datos es crucial para ser más precisos en la oferta de sus productos financieros.

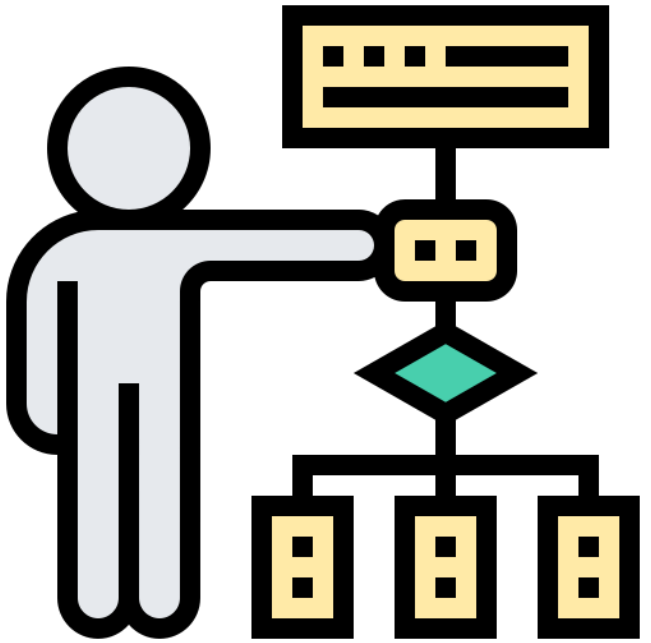
DC: fintech de préstamos, los administradores de finanzas personales, los bots de asesoría, los bancos y otras organizaciones financieras

Conceptos claves

Arquitectura de consentimiento

- En el contexto del open banking, los bancos tienen el desafío de compartir datos confidenciales de los clientes.
- Una arquitectura de consentimiento basada en APIs permite promover una mayor confianza entre los participantes.

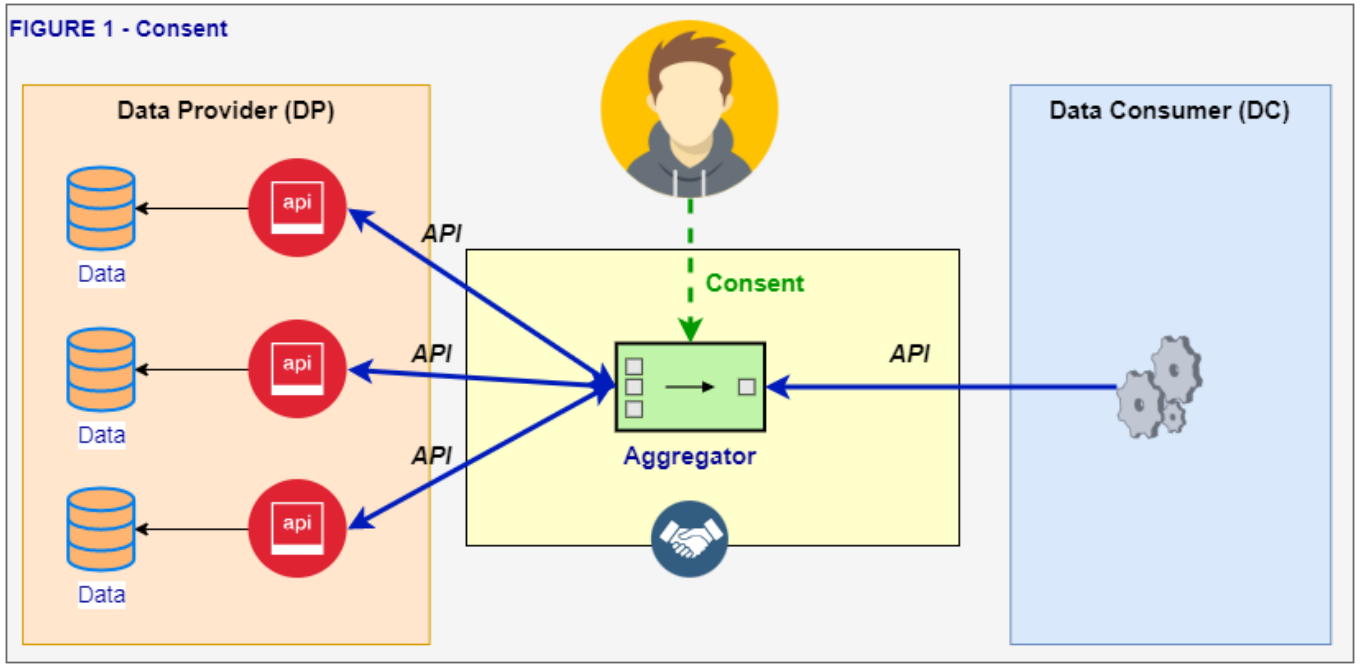
- El esquema de consentimiento consiste en:
  - **Consentimiento**: Se refiere a la aceptación por parte del usuario de compartir sus datos. Se muestra al usuario la información que requiere el DC, sus datos y por cuanto tiempo da el consentimiento.
  - **Autenticación**: Se refiere a verificar la identidad del usuario. los mecanismos de seguridad y autenticación son responsabilidad de los bancos participantes.
  - **Autorización:** Cómo se gestiona los permisos para acceder a los datos. El usuario recibe los detalles del consentimiento solicitado y se le pide aprobarlo o negarlo.



Conceptos claves

Agregador de cuentas (AA)

- Un agregador de cuentas (AA) es comúnmente una plataforma tecnológica intermedia responsable de administrar y transferir flujos de datos entre los proveedores de datos (DP) y los consumidores de datos (DC).
- Los AA desarrollan la interoperabilidad entre los participantes.
- Son mecanismos importantes para la implementación del data-sharing en el esquema de open banking.
- Un AA o centralizador es un punto de concentración de flujos de información, debidamente estandarizado y regulado.
- Estos agregadores son solo intermediarios, que no pueden almacenar los datos ni redirigirlos a entidades no autorizadas.
- Una característica importante de los AA es que desarrollan mecanismos para obtener el consentimiento de los flujos de datos de y para los usuarios finales.



Modelos de data-sharing

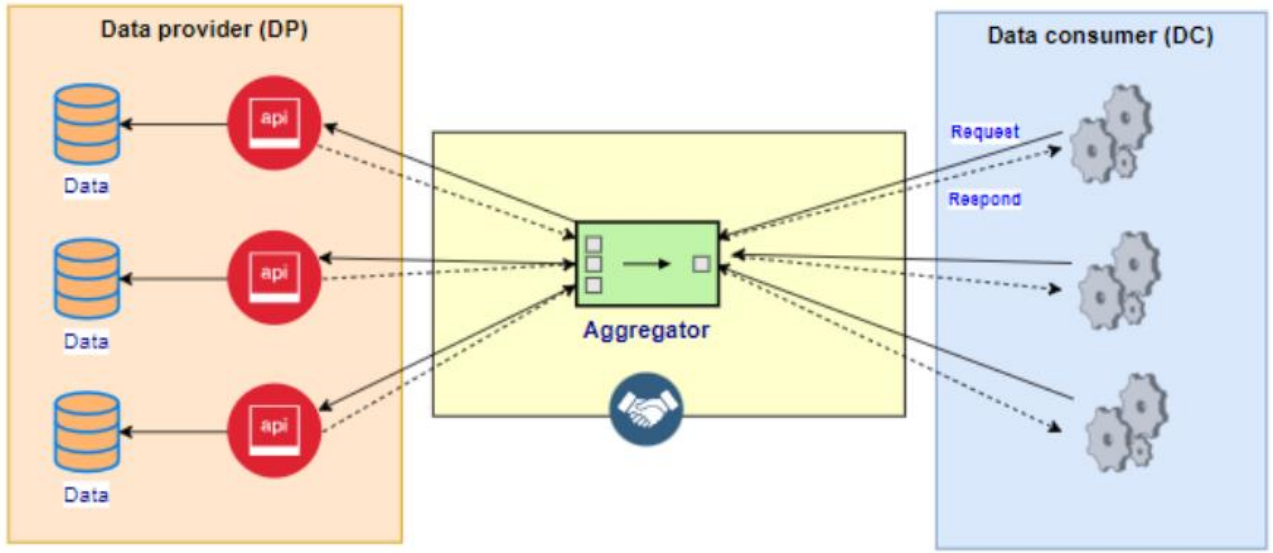
- El esquema para el intercambio de datos se basa en un conjunto de decisiones:
  - Dónde se almacenarán los datos
  - Quiénes son los consumidores
  - Qué interfaces de comunicación se utilizarán.
- Las responsabilidades de las partes involucradas, así como el consentimiento obligatorio de los usuarios, juegan un papel importante en el establecimiento de un modelo adecuado.
- Además, las tecnologías de comunicación, los protocolos, los mensajes estandarizados, las infraestructuras y los mecanismos de seguridad deben decidirse antes de cualquier tipo de implementación.

- **Describiremos tres alternativas de modelo de data-sharing:**
  - Modelo centralizado
  - Modelo descentralizado
  - Modelo de ecosistema de confianza

Modelos de data-sharing

Modelo centralizado

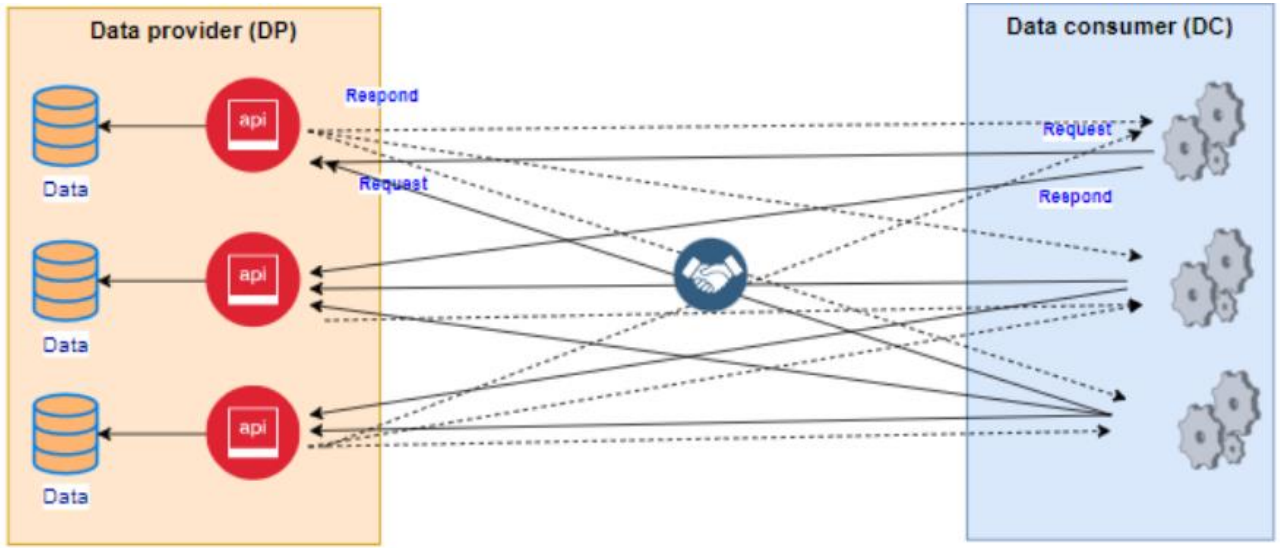
- **Los datos se recopilan de un agregador, quien tiene control sobre el intercambio de datos.**
- Esto incluye el control sobre el proceso de autorización y autenticación para acceder a los datos a través del agregador.
- El corto tiempo de respuesta para las devoluciones de datos es uno de los beneficios clave de este modelo, ya que es más rápido obtener datos de un agregador central (es decir, una fuente consolidada) que de múltiples fuentes.



Modelos de flujo de data-sharing

Modelo descentralizado

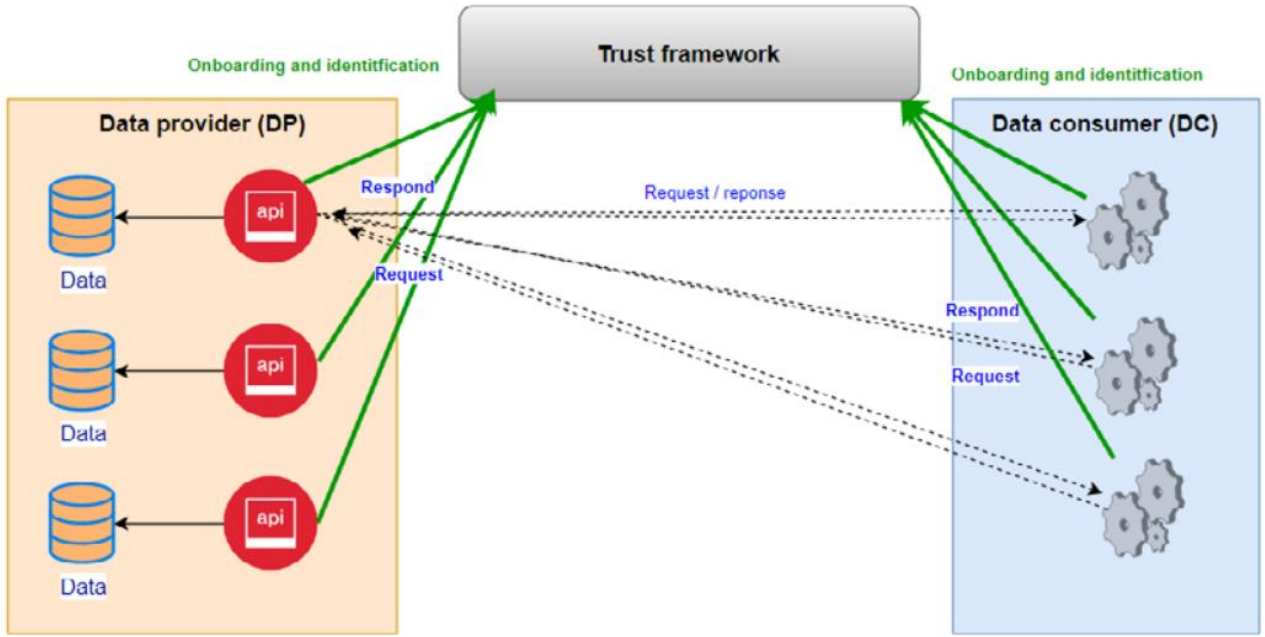
- **Los datos también permanecen en la fuente o punto de servicio. Los miembros participantes aceptan compartir sus datos con otros participantes, individualmente.**
- Cada participante mantiene el control de los datos dentro de sus bases de datos de origen.
- Uno de los principales beneficios es que se garantiza el acceso a datos actualizados y cada participante puede negociar la lista de datos a compartir.
- Sin embargo, dado que existen transferencias punto a punto entre diferentes participantes, no es necesariamente posible seguir un estándar preciso para el intercambio de datos.



Modelos de data-sharing

Modelo de ecosistema de confianza

- **El agregador de cuentas no es necesario, siempre que los estándares estén muy bien definidos. Por lo tanto, no hay un centralizador.**
- **La estandarización, las pruebas y un proceso de certificación preciso son los pilares clave de este modelo, que está descentralizado para compartir datos y centralizado para la gestión de identidades.**
- La propuesta se basa en un marco de confianza que registra dinámicamente tanto a los proveedores de datos como a los consumidores, por ejemplo, una plataforma central que permite el registro inicial, pero el intercambio de datos se mantiene distribuido. Dado que las implementaciones individuales de los estándares a menudo varían, aunque sea levemente, el modelo establece que es necesario un proceso de re-certificación, que debe ser gestionado por las autoridades certificadoras.

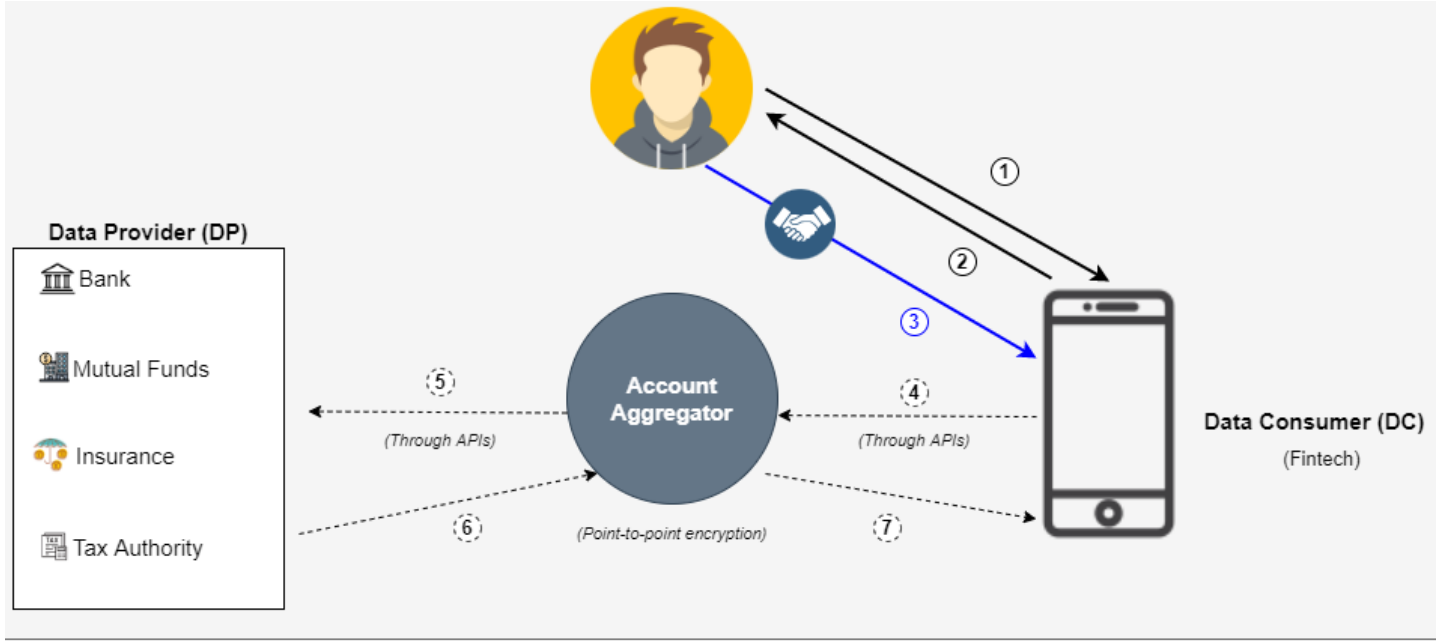


Interacción y flujos de datos

- En el reporte anterior "Report on Payment Initiation" (Sep, 2021), se desarrollaron dos esquemas para la implementación de un Validador Central (Central Validator o CV):
  - **Auth-app scheme:** Se requiere la instalación de una aplicación de un proveedor externo, que es responsable de la autenticación de las credenciales y la confirmación de la transacción de pago
  - **In-app scheme:** El CV se integra de forma nativa dentro de la aplicación, sin necesidad de instalar una aplicación adicional.

- **Para la agregación de cuentas en el contexto del intercambio de datos se desarrollan alternativas similares para las interacciones de usuario y flujos de datos:**
  - Modelo totalmente centralizado a través de API
  - Modelo centralizado con una aplicación de consentimiento de terceros
  - Modelo de confianza sin centralizador

Modelo totalmente centralizado a través de APIs



Condiciones previas:

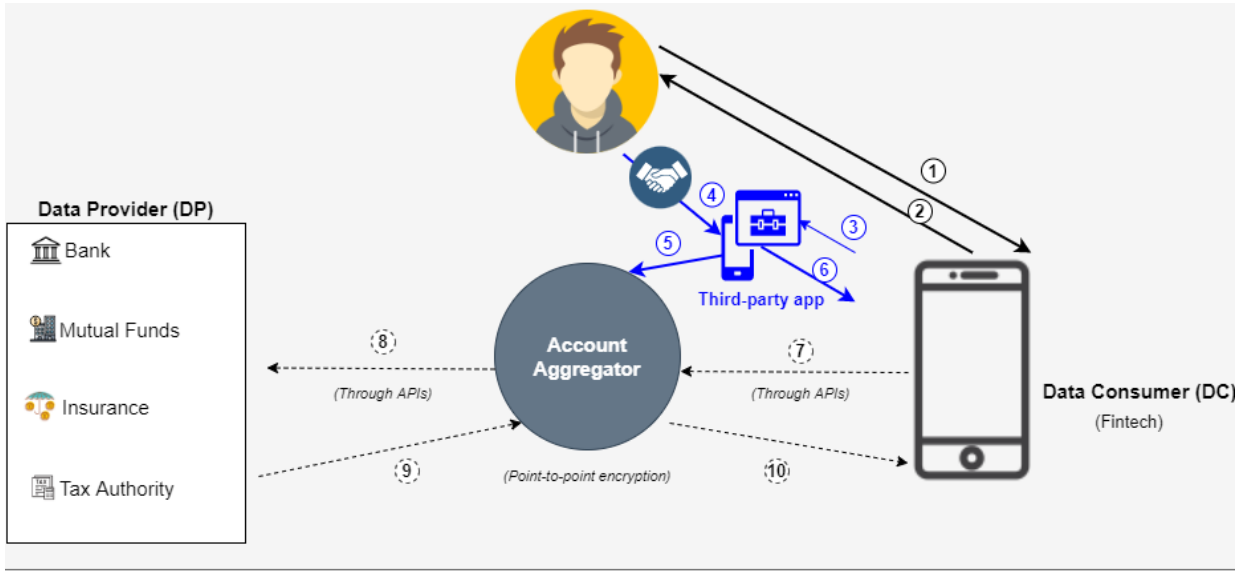
- El usuario ya ha instalado la app Fintech (sólo una app).
- El usuario ha creado un PIN o credenciales con la aplicación Fintech. Ya se ha realizado el proceso de onboarding.

Flujo de datos e interacción:

1. El usuario solicita algún servicio financiero a una Fintech (DC).
2. El DC procesa la solicitud, y dentro de su flujo, requiere acceso a unos datos de terceros donde el usuario tiene información. El DC muestra al usuario la lista de fuentes de información (bancos, seguros, organismos públicos y otros).
3. El usuario da su consentimiento para acceder a los datos de las fuentes solicitadas.
4. El DC se conecta a su servidor back-end, que tiene una conexión segura, privada y encriptada con el AA. El servidor back-end envía la solicitud de consulta al AA, al que proporciona metadatos que garantizan que se ha dado el consentimiento del usuario.
5. El AA valida los datos recibidos. A continuación, proceda a consumir las API de todos los DPs implicados.
6. Los DPs responden al AA. El AA procede a consolidar los datos recibidos.
7. El AA responde al servidor back-end de la Fintech con los resultados obtenidos.

Por último, la Fintech ya puede procesar el servicio financiero ofrecido al cliente.

Modelo centralizado con una aplicación de consentimiento de terceros



Condiciones previas:

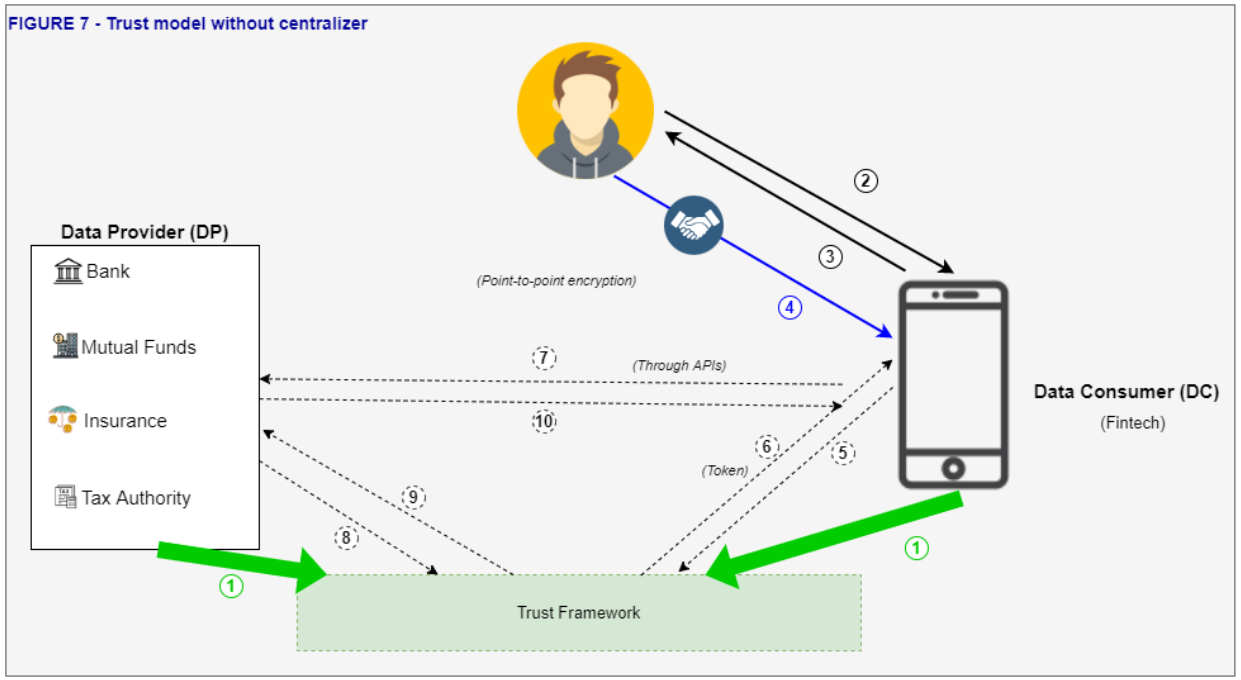
- El usuario ya instaló la aplicación Fintech.
- El usuario ya ha instalado la aplicación de consentimiento (aplicación de terceros)
- El usuario ha creado un PIN o credenciales para la aplicación Fintech y la aplicación de consentimiento. El proceso de onboarding ya se realizó en ambos entornos.

Flujo de datos e interacción:

1. El usuario solicita algún servicio financiero de Fintech (DC).
2. El DC procesa la solicitud, y dentro de su flujo requiere acceso a datos de terceros donde el usuario tiene información. La Fintech muestra al usuario la lista de fuentes de información (bancos, seguros, agencias gubernamentales y otros).
3. El DC también invoca a la aplicación de terceros para que se muestre con la interfaz de consentimiento.
4. El usuario da su consentimiento para acceder a los datos de las fuentes solicitadas.
5. La aplicación de terceros notifica al AA.
6. La aplicación de terceros notifica a la aplicación del DC. Se ha prestado el consentimiento y se ha invocado a las partes.
7. El DC se conecta a su servidor de back-end, que tiene una conexión segura, privada y encriptada con el agregador de cuentas. El servidor back-end envía la solicitud de consulta al AA.
8. El AA valida los datos recibidos. Luego procede a consumir las API de todos los DPs involucrados.
9. Los DPs responden al AA. El AA procede a consolidar los datos recibidos.
10. El AA responde al servidor back-end del DC con los resultados obtenidos.

Finalmente, la fintech ahora puede procesar el servicio financiero ofrecido al cliente.

Modelo de ecosistema de confianza



Condiciones previas:

- El usuario ya instaló la aplicación Fintech.
- Tanto el proveedor de datos (PD) como el consumidor de datos (DC) ya han realizado el proceso de onboarding (paso 1) en el Trust Framework

Flujo de datos e interacción:

1. El DP y el DC realizan un proceso de onboarding.
2. El usuario solicita algún servicio financiero a una Fintech (DC), por ejemplo, un préstamo.
3. El DC procesa la solicitud y, dentro de su flujo, requiere acceso a un DP que tiene información del usuario. El DC muestra al usuario la lista de fuentes de las que necesita agregar información (bancos, compañías de seguros, agencias gubernamentales y otros).
4. El usuario da su consentimiento para acceder a los datos de las fuentes solicitadas.
5. El DC se conecta a su servidor de back-end, que tiene una conexión segura, privada y encriptada con Trust Framework. El servidor back-end envía la solicitud de token a Trust Framework.
6. Trust Framework autentica y valida el servidor back-end del DC y genera un token. El token se envía al DC.
7. El servidor back-end del DC realiza una conexión directa, a través de la API, con el DP utilizando el token proporcionado.
8. El DP se conecta al Trust Framework para validar el token.
9. Trust Framework responde a la validación del token.
10. Si el token es válido, el DP devuelve los datos solicitados por el DC.

El token se puede permanecer válido durante un largo período de tiempo (caducidad). Por lo tanto, se podrían crear mecanismos como sellos de tiempo y criptografía para que los pasos 8 y 9 no sean redundantes.

Modelos alternativos podrían mejorar este ejercicio.

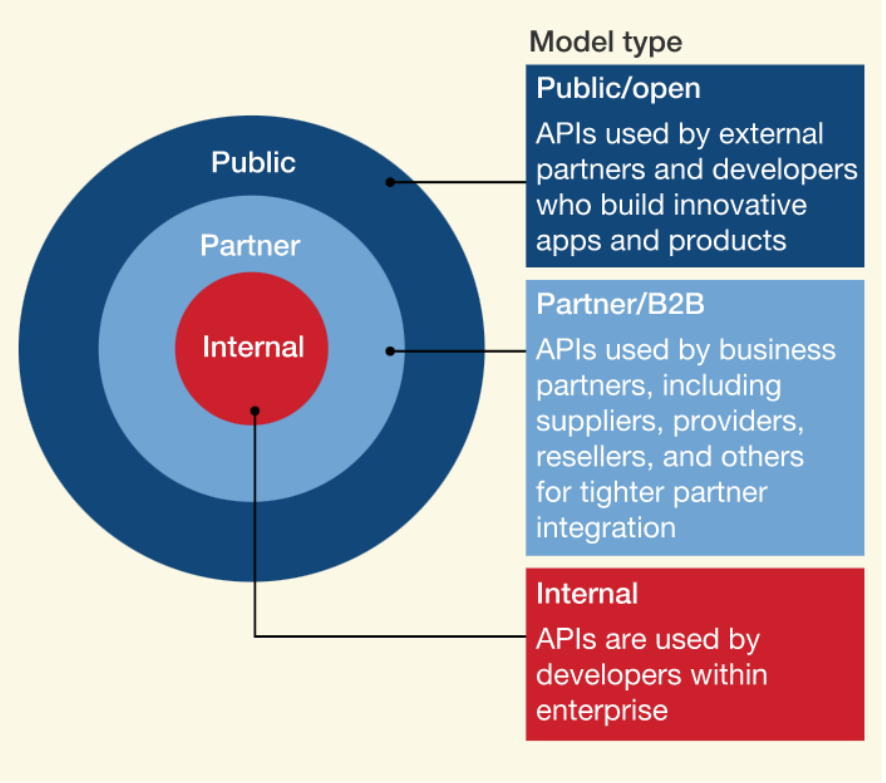
Consideraciones tecnológicas

- En un **esquema centralizado**, los encargados de implementar y publicar las APIs son los DP y los AA.
- En un **ecosistema de confianza**, tanto los DP como los DC están obligados a implementar y publicar servicios de API, en un contexto de reciprocidad.

- Hay diferentes alternativas de diseño disponibles para las implementaciones de API. El informe proporciona una serie de patrones básicos de diseño con los que lograr interfaces y tecnologías sólidas para compartir datos.

- **Estilos de arquitectura para APIs**
  - El estilo predominante es REST, sin embargo hay un considerable numero de sistemas legados basados en SOAP.
  - Otro estilos de arquitectura son: RPC, gRPC, GraphQL

- **Niveles de acceso de las API**
  - Privado
  - Socios
  - Público



McKinsey&Company | Source: McKinsey Payments Practice

Consideraciones tecnológicas

- En cuanto a los mecanismos de seguridad de las API, estos se pueden definir en términos de:

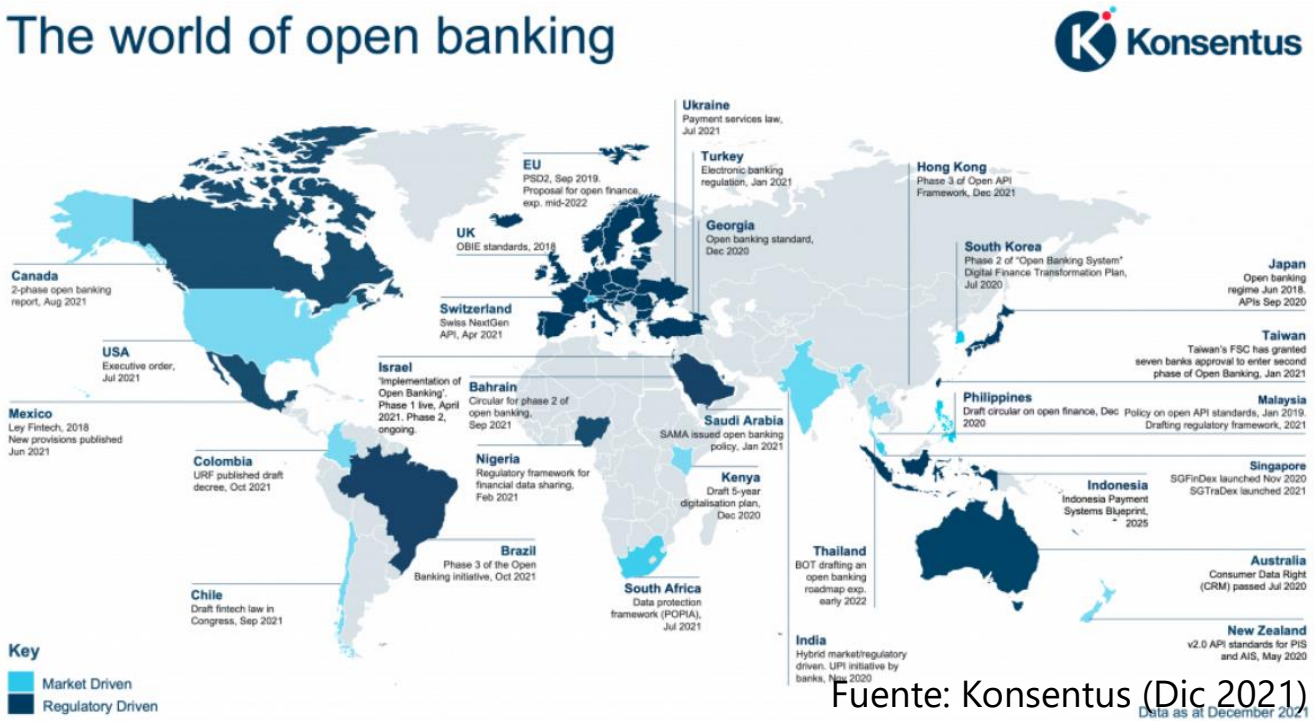
  - **Autenticación:** Este es el proceso de identificar si los clientes y usuarios son quienes dicen ser. Es el primer paso en la implementación y ejecución segura de la API.
  - **Control de Acceso:** Una vez superada la etapa de autenticación, es necesario establecer mecanismos de control para limitar las acciones de los usuarios. El control de acceso debe ocurrir después de la autenticación, en respuesta a las acciones del consumidor de la API. Además de validar y otorgar los accesos que se estimen convenientes.
  - **Cifrado**: Para el cifrado es necesario el uso de tokens, que son estructuras de datos simples esenciales para la funcionalidad de las API. Los tokens encriptados almacenan información importante, como el nombre de usuario y la contraseña. Estos tokens deben caducar después de un cierto tiempo, dando mayor solidez a la seguridad de la API.
  - **Registros de auditoría:** nos permite almacenar las acciones o llamadas que se han realizado a la API, lo que permite la auditoría. Tras la autenticación y el control, se almacenan así en los registros las actividades clave, tanto las positivas como las fallidas o caídas.

Lecciones aprendidas de iniciativas de otros países

- De acuerdo con esta investigación, el TTF de CGIDE realizó seminarios web con oradores de varias jurisdicciones sobre sus iniciativas de intercambio de datos.

- El objetivo fue conocer el modelo implementado, las consideraciones tomadas para la elección del modelo, las lecciones aprendidas de las implementaciones, el ambiente en el que fueron desarrolladas y tener discusión entre los integrantes del CGIDE TTF y las organizaciones a cargo. de las iniciativas de las distintas jurisdicciones invitadas.

- **Los invitados fueron NPCI de India, la empresa Raidiam y los responsables de las iniciativas en Reino Unido, Corea, Brasil y Australia.**



Fuente: Konsentus (Dic 2021)

Conclusiones

- El intercambio de datos o data-sharing es uno de los principales pilares de las iniciativas de open banking que surgen en los servicios financieros. Las innovaciones incluyen proveedores externos, que facilitan el acceso a registros bancarios con el consentimiento del usuario, o proveedores de servicios de pago. El intercambio de datos promueve la transparencia en una sociedad digital y respalda altos niveles de reciprocidad y cooperación en el ecosistema financiero.

- A partir de una encuesta aplicada a los bancos centrales miembros del grupo, existe un interés común en implementar el intercambio de datos para la agregación de cuentas, con el objetivo de aumentar la eficiencia y promover la competencia del ecosistema. Los principales desafíos son la coordinación entre los participantes, la estandarización y la infraestructura tecnológica.

- El esquema para el intercambio de datos se basa en una decisión sobre qué marco regulatorio es preferible. Establecer dónde se almacenarán los datos, quiénes son los consumidores y qué interfaces de comunicación se utilizarán son los mayores desafíos para seleccionar un modelo adecuado.

- Este informe presenta tres modelos: centralizado, descentralizado y de confianza; y desarrolla las interacciones de los usuarios y los flujos de datos para ellos.

Conclusiones

- Además, el informe presenta la funcionalidad del agregador de cuentas (AA) y los posibles arreglos para implementarlo en el ecosistema de open finance. Una demostración basada en una arquitectura de microservicios que promueve alta disponibilidad, escalabilidad y resiliencia es parte del informe. El caso de uso se basó en la recuperación de saldos personales por parte de los consumidores de datos (DC), que fueron puestos a disposición por tres bancos (también simulados en la demostración).

- Otros bancos centrales participaron a través de presentaciones: Corea del Sur (KFTC), India (NPCI), Reino Unido (OBIE), Brasil (BCB) y Australia (CDR). Raidiam Services Limited presentó sus experiencias y perspectivas como proveedor privado de tecnología para iniciativas open banking y data-sharing.

- Finalmente, este es el último informe relacionado con las API en el contexto de la implementación de open finance que realiza el CGIDE, ya que se han cubierto los principales temas relacionados con esa área de interés de los bancos centrales.

BIS

¡Gracias!