COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 21
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Diciembre 2024

Agenda

01 Presentación EdS: Entregable Etapa 2

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 2

03 Consulta sobre Cambio en Finalidad – GT UX

Consideraciones para la presente sesión del GC

- La presente sesión del Grupo Consultivo tiene por propósito **comentar el entregable de la Etapa 2** elaborado por el EdS, en base a las discusiones llevadas a cabo en los respectivos Grupos Técnicos del SFA.

- De conformidad a lo solicitado por algunos miembros del GC, **se autorizó la presencia de un representante técnico** por gremio / Bco Estado, en calidad de oyente en la presente sesión.

- Al respecto, se recuerda que la participación activa en esta sesión **se limita exclusivamente a los miembros titulares y suplentes del GC,** teniendo el representante técnico un rol pasivo, destinado únicamente a facilitar el trabajo técnico a desarrollar posteriormente.

Dinámica de la reunión

- De conformidad a lo informado, el desarrollo de las presentaciones es el siguiente:
  - El **Equipo de Soporte** de la UAI realiza **presentación de entregable Etapa 2 (15 min)**
  - Se efectúan las **presentaciones por los miembros del GC**, por orden de recepción de las mismas:
    - **10 min** para presentación
    - **5 min** para preguntas
- Se hace presente que todos los temas que puedan requerir profundización podrían ser considerados y abordados en una potencial reunión del Grupo Consultivo a realizarse mañana **viernes 20 de diciembre**.

Agenda

01 Presentación EdS: Entregable Etapa 2

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 2

03 Consulta sobre Cambio en Finalidad – GT UX

Entrega Etapa 2
Sistema Finanzas Abiertas

Grupo Consultivo 19 de diciembre

Se distribuyó entregable Etapa 1 al GC

	Etapa 0 **(Fase 1)**	Flujo de solicitud de información de términos y condiciones y canales (completado)
	Etapa 1:	Flujo de consulta de información de Persona Natural* (incluye mecanismo alternativo)
	Etapa 2:	**Monitoreo + Plan de Prueba (Onboarding) + Gestión posterior al consentimiento (revocación, consultas, etc.) + Portal Web**
	Etapa 3:	Flujo de consulta de información de Persona Jurídica*
	Etapa 4:	Iniciación de pagos

(Fase 2)

* Información para Bancos, Emisores de tarjetas de pago y otros proveedores de cuenta

Se distribuyó segundo documento, correspondiente a Etapa 2

- Documento consideró: **el entregable de la Etapa 0 y 1**, la NCG, los primeros antecedentes del Directorio presentados por la CMF, **el Workshop de la Etapa 1 y 2**, **reuniones de los GT** sostenidas entre el 6 y 14 de noviembre, **retroalimentación entregable de la Etapa 0 y 1**, visión informada del Equipo de Soporte, y resultados de posiciones de los participantes de los GT a consultas del Equipo de Soporte (EdS).
- No se alcanzó a incorporar la 2da presentación de la CMF sobre el Directorio.
- El objetivo fue generar un documento consistente, basado en las visiones planteadas por los partícipes de los GT, para su discusión en el Grupo Consultivo.
- En el documento se fue cuidadoso de consignar las opiniones de los distintos gremios dentro del mismo cuerpo del entregable, con el fin de facilitar la lectura.
- Los anexos se separaron del cuerpo, incluyendo las posiciones de los participantes de los GT a consultas del EdS. Los anexos dan trazabilidad al relato del cuerpo, y permiten trazabilidad tanto de las posiciones como de las conversaciones sostenidas en el proceso.

Estructura del documento

01

Capítulos transversales con las abreviaciones, estándares y definiciones, introducción, **contribuciones proceso de discusión Etapa 2**, y la conclusion (enfocado al proceso metodológico).

02

El cuerpo con la Infraestructura, aspectos técnicos de las APIs, requerimientos de seguridad, comunicación y gestión de incidentes de Seguridad, **y experiancia de usuraio**.

03

El documento contiene todas las temáticas que el Equipo de Soporte propuso para que los GT entregaran su posición, junto con la retroalimentación que cada gremio y Banco Estado entregó respecto a sus posiciones (en anexos).

04

Finalmente, los anexos contienen las presentaciones iniciales del Workshop, las posiciones respecto a cosultas que hizo el EdS, las minutas de todas las reuniones de los GT, así como las presentaciones de cada participante.

Contribuciones proceso de discusión Etapa 2

Directorio y DCR

En esta etapa se profundizaron en aspectos técnicos del Directorio y los flujos y RFCs para el DCR y DCRM.

Finalidad

Lista inicial de finalidades y proceso de registro de nueva finalidad. Además, se propone el uso de textos diferenciados para dirigirse a distintos nichos.

Paginación

Identificar los endpoints que no requieren paginación y los que si lo requieren, tamaño máximo y default de paginación, y criterios de ordenamiento.

Infraestructura e Intercambio de Información

Portal Web Desarrolladores

Ciertas definiciones sobre la estructura y contenido que debiera tener el portal, como por ejemplo documentación técnica y recursos para desarrolladores.

Mecanismos de Monitoreo

Se propuso una matriz de monitoreo con el contenido a enviar por IPI y PSBI, además de métricas y periodicidad.

Mecanismos Alternativos

Este tema no se siguió desarrollando en los grupos técnicos a la espera de la conclusión de la discusión en el Grupo Consultivo.

Certificación

En esta sección se abordan las pruebas de Consumo y Funcionales de las APIs. Adicionalmente, esta sección detalla las pruebas de Calidad de la Información que deberán entregar periódicamente a la CMF las IPIs.

Requerimientos de Seguridad

Perfil Financiero de Seguridad FAPI 2.0

En esta etapa principalmente se profundizaron en aspectos del perfil FAPI 2.0 a utilizar en el SFA en Chile.

Consideraciones implementación FAPI 2.0

Sección que resume algunos de los acuerdos que se han tomado en la implementación del perfil FAPI 2.0 en Chile.

Ejemplo Flujo FAPI 2.0

Explicación de los flujos de consentimiento y su lineamiento con el perfil FAPI 2.0.

Experiencia de usuario

Finalidad

Lista de finalidades iniciales y proceso de incorporación de nuevas finalidades

Portal Web Usuario Final

Lineamientos generales sobre contenidos y características del diseño del portal web.

Gestión de Reclamos

Resume los aspectos de reclamo de usuarios, resolución de conflictos entre instituciones del SFA, matriz de responsabilidades y matriz de SLAs entre instituciones.

Casos Especiales

Levantamiento de casos de persona natural que requieren de algún tratamiento especial dentro de los flujos normales de intercambio de información entre los PSBI y las IPI.

Temas arrastre y consultas a CMF

Temas arrastre:

- Mecanismos alternativos: conclusión de la discusión en Grupo Consultivo

Temas con opinión CMF:

- Tratamiento de PN y PJ en información
- Modificaciones de finalidad en la PSBI

Consultas CMF:

- Convivencia de la ley de datos personales con la ley Fintec (almacenamiento, procesamiento y borrado de datos)
- Interpretación normativa para ver cómo abordar la experiencia usuaria para la selección de múltiples productos
- Borde del sistema de finanzas abiertas y finanzas embebidas

Comenzó el trabajo de la Etapa 3

- El día 12 de diciembre los distintos participantes del SFA dieron el kickoff a la Etapa 3, relacionada con PJ y todos los temas que son necesarios para comlpetar los casos de PN y PJ.
- Foco en GT de API, seguridad y Infraestructura: cerrar temas pendientes
- Para este ciclo, se ha optado por incluir otras formas de trabajo, las cuales fueron discutidas por los partícipes en el taller: división de temas entre participantes, sub-grupos que desarrollan un tema, o presentaciones.
- A medida que se ha avanzado, se ha identificado que el documento actual tiene niveles de profundidad técnica heterogéneos, pues recoge temas “normativos de segundo nivel” con otros que son más propios de un desarrollador.
    - Se propone separar en ramas paralelas estas discusiones, y generar un anexo que tenga por fin ser la base del portal del desarrollador.
    - Nuestra propuesta será generar un plan de trabajo paralelo que se haga cargo de este anexo y reunirse la próxima semana con representantes de cada gremio para recibir feedback sobre una metodología de trabajo.

Entrega Etapa 2
Sistema Finanzas Abiertas

Grupo Consultivo 19 de diciembre

Agenda

01 Presentación EdS: Entregable Etapa 2

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 2

03 Tema Finalidad

COMISIÓN
PARA EL MERCADO
FINANCIERO

Banco del Estado de Chile (BancoEstado)

Entregable Etapa 2:
Temas Transversales del SFA

Visión BancoEstado

Implementación SFA

19 de Diciembre de 2024

APIs

❑ Pruebas funcionales IPIs

- La **propuesta** sugiere que la certificación funcional para las IPIs se orienten a los **flujos** y a la correcta ejecución de los pasos definidos en dichos procesos.
  - Esto supone la ejecución de **pruebas funcionales focalizadas en interfaces *mock***, sin detallar pruebas de carácter técnico relativas al flujo FAPI, validación mTLS, flujos de borde del consentimiento, o escenarios de integración con el directorio.
- Creemos necesario **especificar** un **set de pruebas más robusto y detallado**, que **complemente** los **flujos *mock* puramente funcionales**.
- Sugerimos **incorporar** un conjunto de **pruebas en ambiente productivo** que den cuenta de la integridad de los flujos previo a dejarlos disponibles a los clientes
  - Esto sigue las **recomendaciones** del sistema **FVP en Brasil**.
  - Esto puede ser **al menos en las etapas iniciales** de la **puesta en marcha del SFA**.

APIs

❑ Pruebas de calidad de datos

- La **propuesta** basada en **criterios DAMA aplicables al SFA** requieren la **implementación de procesos adicionales** para la construcción y análisis de métricas establecidas por este criterio.
  - Entendemos que ellas **no son necesariamente vinculadas a penalidades inmediatas** a los miembros del SFA.
- Creemos conveniente **definir plazo a acordar** para que el **monitoreo de calidad de datos** pueda **utilizarse en la calibración de umbrales y métricas** que hagan sentido al ecosistema.

UX

❑ Finalidad

- ➢ **Heterogeneidad** en **requisitos de datos para una misma finalidad** genera **incompatibilidades** con el **principio de proporcionalidad del SFA.**
  - Debe existir una **relación clara entre finalidad, datos y plazo** (homogeneidad).
  - Lo anterior apunta a un **proceso más transparente** (finalidad esté asociada realmente a los datos que se requieran), y **resguardan al cliente**.
- ➢ **Finalidades** que se definen en la matriz **no deben tener adaptaciones al lenguaje aunque se mantenga el sentido**.
  - **Complicaciones** en el **análisis posterior** (subjetividad).
  - **No promueve tratamiento uniforme de datos**.

UX

❑ Gestión de reclamos

- Se sugiere que el **SLA** definido para **gestión de reclamos de usuarios** sea el que cada una de las **instituciones posee actualmente**.
  - Esto se **alinea** con los **procesos actuales** adaptados a las necesidades de los clientes.
  - **No se requiere implementar nuevos procesos** que impacten los costos.
- Para la **comunicación entre instituciones**, se sugiere utilizar una **ticketera centralizada por parte del regulador**.
  - **Correos electrónicos** (propuesta**) impiden tener un seguimiento y control**.

Gracias

BancoEstado
desde 1855

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de Empresas de Innovación Financiera de Chile A.G. (FinteChile)

Resultados Temario Etapa 2

FinteChile

Diciembre 2024

www.fintechile.org

FinteChile

Índice

GT Infraestructura

Posiciones Presentadas

Posición	Argumento
1	Existen múltiples elementos de la propuesta que no nos quedan muy claros: (1) la aplicación o no de FAPI 2.0 en el directorio; (2) el uso de Webfinger o no para información de participantes; (3) la forma de soportar multi-marca-IPI en el directorio. En el punto (1) sobre la aplicación de FAPI 2.0 en el directorio, la consideramos razonable de cara a los endpoints ofrecidos por el directorio. No así a los "webhooks" de notificación que deberán disponibilizar los participantes. Estos webhooks pueden ser un mero "ping" que fuerza a los participantes a actualizar su copia local, lo que ocurrirá utilizando los endpoints FAPI2.0 del directorio. La propuesta del EdS sobre "/message-receiver FAPI 2.0" no deja claro si se refiere a un endpoint de los directorios o de los participantes. Si fuera lo primero, estamos de acuerdo. Si fuera lo segundo, no. La propuesta del EdS sobre "/notifyUpdate" y "/notifyIncident" tampoco deja claro a qué actor se refiere. Si fueran endpoints del directorio, estamos en desacuerdo por que debiera estar cubierto por FAPI2.0. Si fueran endpoints de participantes, no parece necesario mTLS para hacer el ping (basta TLS y el posterior uso de los endpoints FAPI2.0 del directorio para obtener realmente la información). En cuanto a los "tipos de actualización", no entendemos qué significado tiene la palabra o abreviación "cs". Luego en el punto (2) no entendemos si se propone que los campos logo_uri, technical_contact_url, etc. sean parte de información que viaja vía Webfinger o si están directamente en el directorio. Ambas opciones nos parecen viables, pero la propuesta debiera ser más clara sobre cual se está recomendando (se menciona Webfinger, pero luego los campos aparecen en el payload de /participantes que entendemos es un endpoint del directorio propiamente). Además, en cuanto al punto (3) no nos parece que se haya adoptado en la propuesta del EdS el punto levantado sobre que un mismo cmf_id (participante legal) pueda tener más de una marca de cara a las personas clientes finales (ej: Bci y MACH). Eso requiere que un mismo cmf_id pueda tener múltiples entries como IPI, lo que puede requerir múltiples logos_uri y otros campos relacionados a la marca a transmitir de cara al usuario para evitar confusión.

FinteChile

Votación de Posiciones

1 **Directorio:**
No adherimos y tenemos una posición nueva

2 **DCR:**
Adherimos

3 **Monitoreo:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Infraestructura

Posiciones Presentadas

Posición	Argumento
3	Si bien estamos de acuerdo con la mayoría de lo propuesto, existe una omisión grave en el cross-check de disponibilidad. La tabla propuesta por el EdS no explica razones para dejar fuera al PSBI en los reportes de (in)disponibilidad de las API (en la primera celda vacía de la tabla propuesta). Desde Fintechile, nos parece un cross check necesario para que el regulador coteje la disponibilidad reportada por las IPIs contra las *indisponibilidades* reportadas por el PSBI. De lo contrario: Desde el punto de vista del sistema, se pierde información útil para el buen funcionamiento y monitoreo de SFA. No habría un balance en caso de que la información entregada por las IPIs tenga omisiones o errores. Desde el punto de vista de los PSBI, se les obliga a usar mecanismos de resolución de controversias u otro tipo de reclamos ante el regulador cuando a su juicio existan IPIs incumpliendo los SLAs de disponibilidad. No es deseable que ante incumplimientos de las IPIs el regulador esté recibiendo esta información o reclamos por distintas vías de manera Adhoc.

FinteChile

Votación de Posiciones

1 **Directorio:**
No adherimos y tenemos una posición nueva

2 **DCR:**
Adherimos

3 **Monitoreo:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Medios

Posiciones Presentadas

Posición	Argumento
1	Sostenemos que los PSBI solo deberían certificar su correcta implementación de FAPI, interacciones con el directorio e implementación de los paneles de control. Certificar el consumo de datos de las APIs tiene inconvenientes. Primero, porque no todas las PSBI van a necesitar consumir los mismos endpoints para proveer sus servicios. Sería un esfuerzo innecesario forzarlas a certificar el uso de datos que no necesitan. Por el contrario, si solo se certifican algunos endpoints entonces la certificación pierde sentido para los PSBI que si los consuman. Por otro lado, si una PSBI consume incorrectamente un endpoint para obtener datos esto solo afecta al servicio que puede entregar esa misma institución. La integridad del sistema, el funcionamiento de las IPIs y los servicios entregados por otros PSBIs y seguridad del SFA no se ven afectados de forma alguna por problemas de este tipo.

FinteChile

Votación de Posiciones

1. **Pruebas de “Consumo API” por parte de las PSBI:**
   No adherimos y mantenemos nuestra posición presentada en los GT

2. **Pruebas Funcionales IPIs**
   No Adherimos

3. **Ambiente de pruebas PSBI e IPIs, y Sandbox:**
   Adherimos

4. **Certificación de Consumo de APIs (PSBI) y Pruebas Funcionales APIS (IPIs):**
   Adherimos

GT Medios

Posiciones Presentadas

Posición	Argumento
5	Los PSBIs deben tener la posibilidad de reportar problemas de calidad de datos recibidos por partes de las IPIs. Hay problemas de datos que son muy difíciles de evidenciar con pruebas realizadas por las mismas IPIs. Un ejemplo de esto es la actualización de los datos (que los datos lleguen a tiempo). Para el auto reporte proponemos un mecanismo equivalente a MQD implementado en Open Finance Brasil.
7	De acuerdo con el ordenamiento por fecha de creación del recurso, pero no por el tipo de ordenamiento. Un timestamp de una fecha "más nueva" tendrá un valor mayor que el de una fecha pasada. Por eso mismo, el valor de ordenamiento debería ser descendente, de forma tal que, si se consulta un endpoint sin especificar una página, se debería obtener los registros más nuevos. O sea, los últimos registros que se han creado en la API. Mientras que los registros más antiguos deberían aparecer en las páginas posteriores.

FinteChile

Votación de Posiciones

5 **Pruebas de Calidad de Datos:**
No adherimos y mantenemos nuestra posición presentada en los GT

6 **Matriz Max Page Size:**
Adherimos

7 **Orden de Paginación:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Seguridad

Posiciones Presentadas

Posición	Argumento
1	Adhesión parcial: si el impacto está definido en base a afectación de PSBI/IPI/Directorio, las acciones deberían corresponderse con el participante que tuvo la afectación. En esta línea, para las categorías altas y críticas estos pueden darse en un PSBI o IPI particular y no requerir una sala de crisis con todos los participantes (como especifica la tabla) sino aplicación de medidas como las que se especifican para los incidentes de criticidad baja.
2	Siempre que la regulación del transporte de datos esté enfocada en FAPI 2.0, como lo entendemos).
4	Pese a que FAPI 2.0 elimina esos estándares, ambos son introducidos por Message Signing para otorgar integridad a todo el flujo.

FinteChile

Votación de Posiciones

1. **Clasificación de Incidentes de ciberseguridad:**
   Adherimos
2. **Certificación para transporte, almacenamiento, procesamiento y borrado de datos:**
   Adherimos
3. **¿Qué se implementa para el Security Profile? TLS 1.2 o 1.3:**
   Adherimos
4. **¿Qué NO se implementa para el Perfil FAPI message signing?:**
   No adherimos y mantenemos nuestra posición presentada en los GT
5. **Campos de Certificado de implementación de perfiles de seguridad de interfaces para las IPI y PSBI:**
   Adherimos
6. **Vigencia del certificado. Cada cuanto tiempo se debe certificar:**
   Adherimos

GT UX

Posiciones Presentadas

Posición	Argumento
1	Estamos de acuerdo en tener una matriz de 3 columnas (categoría, finalidad, id) para categorizar finalidades. La redacción de las finalidades será de uso interno entre participantes y la CMF. El usuario verá la redacción más apropiada según el juicio de PSBI para el servicio y nicho de mercado particular que esté abordando. La excepción propuesta para controlar el plazo en caso de verificación de identidad complica el sistema sin ninguna justificación. Las finalidades no deben estar vinculadas a plazos, ni tipos de datos, sin excepción. De acuerdo en que las finalidades se inscriban a través de un endpoint ágil, que alimente el directorio. Dado que las finalidades nuevas se incorporarán en forma ágil a través de un endpoint, el listado inicial puede partir vacío, lo que evita discusiones previas sobre las expectativas de lo que el mercado va a requerir.

FinteChile

Votación de Posiciones

1 **Finalidad:**
No adherimos y mantenemos nuestra posición presentada en los GT

2 **Gestión de reclamos**
Adherimos

COMISIÓN
PARA EL MERCADO
FINANCIERO

Cooperativas de Ahorro y Crédito Asociación Gremial - COOPERA A.G.

Entregable
Etapa 2

Posición Coopera

Entregable - Infraestructura

Servicios entregados por el Directorio

Registro dinámico de clientes

Diccionario de datos “base de datos liviana”

Portal web de desarrolladores

Estándares de seguridad y continuidad del Directorio

Mecanismo de monitoreo

Módulo de comunicaciones

Entregable - Infraestructura

Servicios entregados por el Directorio

Registro

Apoyamos que la CMF debe indicar los SLAs para el proceso de registro de un participante.

Copia local

En cuanto al payload del mensaje de notificación, no parece relevante especificar el tipo de contenido en el cuerpo del mensaje, ya que esto se gestiona a través de la cabecera HTTP "Content-Type".

```
{
    "specversion": "1.0",
    "type": "cl.sfa.participant.new",
    "source": "directorio",
    "subject": "New participant",
    "id": "xkjskk3984jcka",
    "time": "2024-08-06T17:31:00Z",
    "datacontenttype": "application/json",
    "data": {
        "participantId": "ID"
    }
}
```

Entregable - Infraestructura

Servicios entregados por el Directorio

Endpoint de los participantes

La variable "sandbox_url" genera dudas sobre si es responsabilidad de la CMF proporcionar un endpoint para el entorno de pruebas del participante, o si es el participante quien debe disponer de dicho entorno.


```
[
    {
        "cmf_id": "xyz",
        "rut": 12345,
        "dv": "x",
        "name": "example",
        "brand": "example",
        "is_psbi": true,
        "is_psip": true,
        "is_ipi": true,
        "is_ipc": true,
        "enroll_date": "2025-01-11-T17:09:17.759Z",
        "sfa_status": "ACTIVO",
        "sandbox_url": "string",
        "api_resources": [
```

Entregable - Infraestructura

Servicios entregados por el Directorio

APIs del directorio

Recomendamos seguir el principio RESTful y consolidar los endpoints "purpose-new" y "purpose-list" en un único endpoint "purpose", diferenciándose en su funcionalidad mediante el método HTTP correspondiente (POST para nuevos registros y GET para obtener la lista).

Endpoint	Tipo	Descripción
/participants	GET	Devuelve una lista completa de los participantes.
/participants/{id}	GET	Devuelve la información específica de un participante basado en el ID proporcionado.
/public-keys	GET	Devuelve una lista completa de llaves públicas de los participantes.
/public-keys/{id}	GET	Devuelve una llave pública específica de un participante según el ID proporcionado.
/last-update	GET	Devuelve la fecha de la última actualización de algún dato del directorio indicando el o los id afectados
/message-receiver	POST	La CMF recibe información de las PSBI/I-PI para actualizar directorio
/purpose-new	POST	La CMF recibe información de una nueva finalidad. Esta queda en estado ingresada
/purpose-list	GET	Devuelve la lista de finalidades activas

Entregable - Infraestructura

Servicios entregados por el Directorio

APIs del directorio

Por otra parte, no se justifica la necesidad de implementar un endpoint "message-receiver" por parte de los **participantes**, dado que ya existen los endpoints "notifyUpdate" y "notifyIncident". Esto, a menos que dicho endpoint se utilice específicamente para notificar a la CMF sobre la correcta recepción de las notificaciones.

debe tener un endpoint /message-receiver que acepte un método PUT con la información de actualización.

- Es responsabilidad de cada participante tener un endpoint /message-receiver operativo.

Entregable - Infraestructura

Registro dinámico de clientes

En términos generales, estamos de acuerdo con la propuesta del entregable. Solo sugerimos normalizar el documento cuando se haga referencia al participante, utilizando de manera consistente los parámetros "cmf_id", "participantId" e ”id" (empleando la misma variable cuando corresponda).

```
[
    {
        "cmf_id": "xyz",
        "rut": 12345,
        "dv": "x",
        "name": "example",
        "brand": "example",
        "is_psbi": true,
```

```
{
    "specversion": "1.0",
    "type": "cl.sfa.participant.new",
    "source": "directorio",
    "subject": "New participant",
    "id": "xkjskk3984jcka",
    "time": "2024-08-06T17:31:00Z",
    "datacontenttype": "application/json",
    "data": {
        "participantId": "ID"
    }
}
```

Endpoint	Tipo
/participants	GET
/participants/{id}	GET
/public-keys	GET
/public-keys/{id}	GET

Entregable - Infraestructura

Mecanismo de monitoreo

Para la matriz de monitoreo, es importante especificar los endpoints a los que aplica el TTLB.

Además, destacamos la necesidad de considerar las restricciones o límites de tamaño de los datos que se pueden enviar en una solicitud, para evitar el retorno de un error 413 "Content Too Large".

IPI	**PSBI**	**Desagregación**	**Métrica**	Periodo
Disponibilidad de las APIS		Separado por API Separado entre mantenciones y bajas no programadas.	% del tiempo disponible	Diario y mensual
TTLB entre recepción de request y envío del último byte del response)	TTLB entre envío de request y envío del último byte del response	IPI: por API y PSBI PSBI: por API y IPI	Milisegundos. mediana, máximo, mínimo, y p90	Semanal

Entregable - APIs

Diccionario de Datos

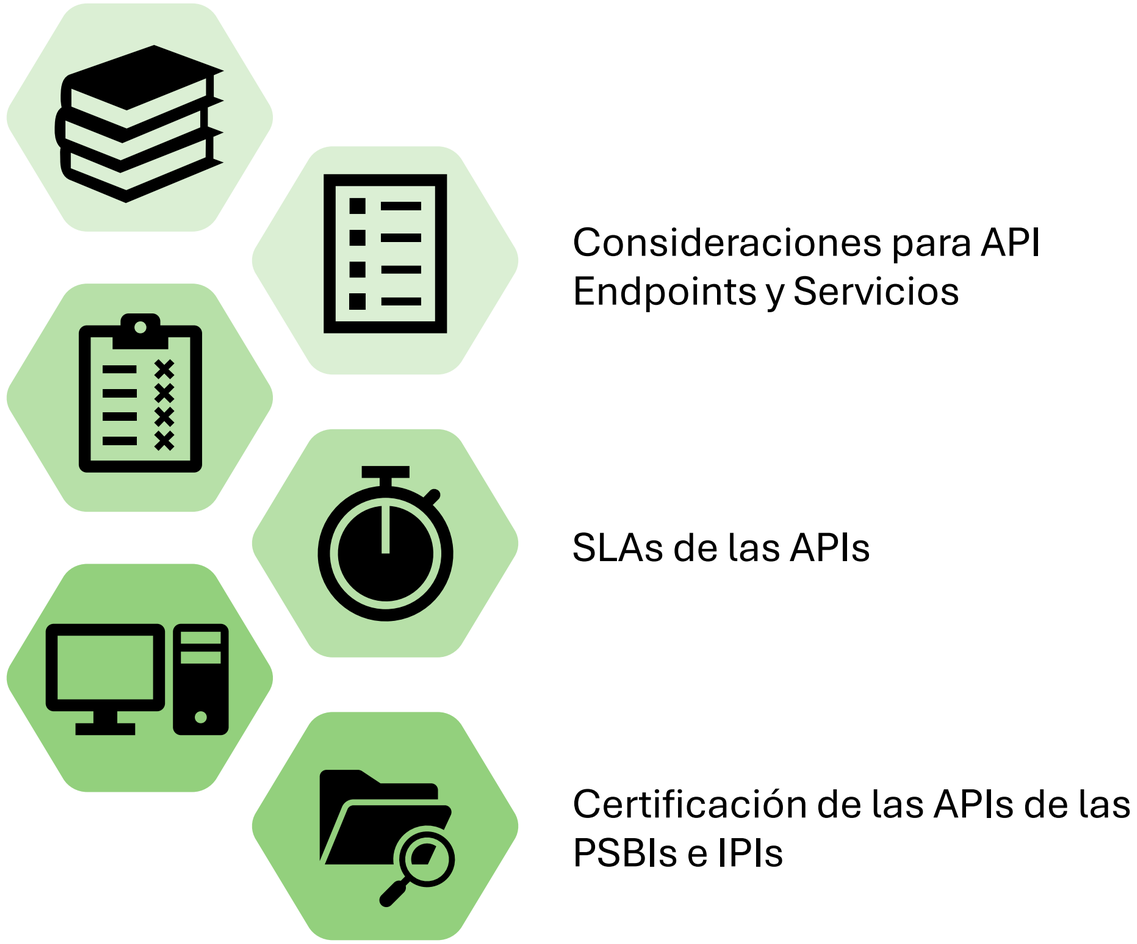
Consideraciones para API Endpoints y Servicios

Códigos de error

SLAs de las APIs

Mecanismos alternativos

Certificación de las APIs de las PSBIs e IPIs



Entregable - APIs

Consideraciones para API Endpoints y Servicios

Se propone revisar el caso de uso en el que se utilice el endpoint de "recursos", ya que creemos que podría generar mayor fricción para el usuario al tener que realizar el flujo de consentimiento por segunda vez en un mismo viaje: primero para consultar los recursos (productos) y luego para consultar un producto específico.

En cuanto a la paginación, consideramos necesario agregar una restricción en la cantidad de meses que se pueden consultar simultáneamente (misma llamada), con el fin de evitar consultas masivas de datos.

- Page: página a ser devuelta por API
- Page-size: con las opciones 25, 50, 100, y máximo pageSize, el default es según lo indicado en la columna Default Page-Size de la Tabla 13. Máximo pageSize corresponde a la columna Maz Page-Size de la Tabla 13.
- fromTransactionMonth: Mes de corte (se propone parámetro mensual para reducir los tiempos de respuesta, debido a que los sistemas actuales de las IPI están estructurados en base mensual).
- toTransactionMonth: Mes de corte (se propone parámetro mensual para reducir los tiempos de respuesta, debido a que los sistemas actuales de las IPI están estructurados en base mensual).

Entregable - APIs

Mecanismos alternativos

Mantenemos nuestra postura de que los tiempos de recuperación (15 minutos) para este mecanismo son insuficientes.

- El mecanismo secundario es activado por la IPI una vez identifica problemas en el mecanismo principal.
- Cada IPI deberá plantear el esquema a la CMF, la cual debe ser una solución homogénea y conocida para todos los PSBI. En esta propuesta se deberá especificar el tiempo de recuperación y la velocidad de respuesta de operación de este mecanismo secundario (respuestas a consultas de las PSBI), tanto para las APIs "customer present" como para el resto de las APIs (pudiendo ser igual para ambas).
- Si se propone un tiempo máximo de recuperación de 15 minutos para las APIs "customer present".
- Los token que se generan para el mecanismo principal debiesen ser compatibles con el mecanismo alternativo.

COOPERA
Cooperativas de Ahorro y Crédito Asociado

Entregable – Requerimientos de seguridad

Perfil financiero de seguridad FAPI 2.0

Consideraciones implementación FAPI 2.0 para SFA en Chile

Ejemplo de implementación de Flujo con FAPI 2.0

Certificados

Cifrado

Administración de Logs asociados al no repudio

Certificaciones

Entregable – Requerimientos de seguridad

Consideraciones implementación FAPI 2.0 para SFA en Chile

No queda claro en qué parte del flujo se debe considerar lo siguiente: "optar por DPoP y private key JWT en lugar de mTLS", ya que anteriormente se menciona que se utilizará mTLS para la autenticación del cliente.

En la iteración Etapa 2 los GTs han acordado implementar y no implementar varias medidas del Security Profile de FAPI 2.0 y del message signing. Para el Security Profile, se ha acordado implementar la Restricción del Token mediante mTLS (mutual TLS) según el RFC8705, la Autenticación del Cliente utilizando tls_client_auth (RFC8705), y el uso de TLS 1.3 por su rendimiento superior. También se ha decidido implementar el Redireccionamiento App-To-App mediante deep-link, incluir el Token Endpoint como Parte del Claim aud y utilizar el Código HTTP 303 al Redireccionar. Sin embargo, se ha acordado no implementar DPoP en los servidores de autorización, excluir el registro manual de clientes como alternativa o contingencia, y optar por DPoP y private_key_jwt en lugar de mTLS.

Entregable – Experiencia de usuario

Portal web para usuario final

Consentimiento

Gestión de reclamos

Casos especiales

Entregable – Experiencia de usuario

Consentimiento

El panel de control debería permitir ordenar y/o filtrar por fecha y por estado del consentimiento, ya que ambos son fundamentales para su revisión.

El tablero de control debe permitir el agrupamiento por glosas o familias de datos, de tal manera que el cliente pueda revisar fácilmente sus consentimientos relacionados a un tema en particular. Las glosas o familias de datos propuestas son las siguientes:

- Institución
- Finalidad

Entregable – Experiencia de usuario

Gestión de reclamos

Mantenemos nuestra postura respecto a que los SLAs propuestos para los incidentes entre instituciones, con tiempos no factibles, no son adecuados, más aún, cuando no está definido un mecanismo de comunicación entre las instituciones.

Nivel de severidad	Descripción del problema	Tiempo de respuesta	Tiempo de resolución	Escalamiento
Crítico (Nivel 1)	Interrupción total del servicio o falla que afecta a funciones críticas del negocio.Ej: Peticiones rechazadas en forma sistemática por error en la validación de la firma, falta de datos de verificación y otros.	1 hora	4 horas	Inmediato al director de soporte
Alto (Nivel 2)	Problemas significativos que afectan parcialmente el servicio o funciones importantes. Ej: Tasa de	2 horas	8 horas	Después de 4 horas sin solución

Entregable
Etapa 2

Posición Coopera

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación de Aseguradores de Chile, Asociación Gremial - Asociación de Aseguradores de Chile A.G. (AACH)

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Revisión etapa 2

19 de Diciembre 2024

Comentarios generales

Finalidad – datos – consentimiento – responsabilidad - (Ley Fintec Artículo 24 – Ley de datos personales – NCG 514)

- Consideramos pertinente que las finalidades deben estar predefinidas.
- Con respecto a la entrega de información, ésta se encuentra enmarcada en:
  - La Ley Fintec en el artículo 24 establecen obligaciones para las IPIs/PSBI/IPC/PSIP serán responsables de resguardar la integridad, disponibilidad, seguridad y **confidencialidad** de los datos involucrados **en cada transacción** y la adecuada privacidad de la información de los Clientes.
  - **La Ley de Datos Personales:**
    - **Finalidad**: “Los datos personales deben ser recolectados con fines **específicos, explícitos** y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.” (Ley de datos personales).
    - **Principio de proporcionalidad**: Los datos personales que se traten deben **limitarse estrictamente** a aquellos que resulten **necesarios, adecuados y pertinentes** en relación con los fines del tratamiento.
    - El **deber de cuidado/secreto/confidencialidad** de los responsables del dato (Ley de datos personales)
  - La posibilidad del titular de los datos, cambie la finalidad en la PSBI para el mismo conjunto de datos y con la misma temporalidad (autorización).
  - Se solicita establecer claramente los “bordes” de las responsabilidades de cada uno de los actores.

Visión general grupos técnicos etapa 2

GT Infraestructura

Se ha visto un avance en **aterrizar la infraestructura del SFA,** sin embargo, queda pendiente profundizar en temas tales como:

- Entendimiento de la gestión de **certificados** y su proceso de **validación**
- Cierre de la definición del uso de un **mecanismo alternativo** y cual será este
    - Este punto ha sido tratado en diferentes instancias, pero aún no se ha logrado **cerrar completamente**
- Detallar **los insumo a disponibilizar** en el developer portal, tales como, swaggers, diccionarios de datos, guías de usuario, entre otros, esto como una **buena práctica observada en otras geografías**

GT APIs

Se ve la necesidad de abordar un mayor detalle de **ciertos requerimientos** y colocar en discusión **buenas practicas** observadas en otras geográficas, incluyendo lo siguiente:

- Detalle de un diccionario de datos para cada **caso de uso específico**
- Se sugiere especificar las APIs de consentimiento por **tipo de caso uso**
- Profundizar en el **procedimiento de versionamiento** de APIs

GT Seguridad

Se ha hecho una revisión **detallada de los perfiles de FAPI 2.0** a nivel de seguridad, firma y modelo de atacante, sin embargo, vemos que existe algunos puntos que puede causar confusión (ej. Uso o no uso de JARM)

GT UX

Se han **observado avances** en diferentes puntos tales como; el tratamiento de casos especiales para personas naturales, pantallas mocks para el flujo de toma de consentimiento, gestión de reclamos, finalidades, entre otros temas, sin embargo vemos pendiente abordar en **mayor profundidad** los siguientes puntos:

- **Granularidad y lineamientos en la definición de las** finalidades y **procedimiento** de ingreso finalidades a la matriz
- Responsabilidad de las IPI frente a un **consentimiento con cambio de finalidad**

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Anexo - revisión etapa 2

19 de Diciembre 2024

GT Infraestrcutura: temas a pendientes o a profundizar

Infraestructura del directorio:

- La infraestructura del directorio ha sido establecida, sin embargo, queda pendiente definir en detalle **quiénes emitirán los certificados** y cuáles serán los **estándares de seguridad** para el directorio, particularmente en la comunicación entre el directorio y las IPIs
- Profundizar en el funcionamiento del directorio y el entendimiento de componentes como el servidor de certificados

Swagger en el Developer Portal:

- Se considera una buena práctica permitir la descarga de los **Swagger** correspondientes a los diferentes **casos de uso** directamente desde el portal de desarrolladores

Diagramas UML y Diccionario de Datos:

- Como buena práctica observada en otras geografías, se sugiere **disponibilizar los diagramas UML** y el **Diccionario de Datos (DD)** de los casos de uso en el portal de desarrolladores

Guías de Usuario:

- Es necesario **disponibilizar las guías de usuario** en el portal de desarrolladores para facilitar la comprensión e implementación de los servicios

Mecanismo de Monitoreo:

- Se recomienda que el mecanismo de monitoreo incluya la **visualización de métricas** relacionadas con la **adopción** y el **desempeño** del ecosistema SFA

Mecanismo Alternativo:

- Aún está pendiente definir un **mecanismo alternativo** al scraping. La posición de la **AACH** es no permitir el scraping. Se sugiere enfocarse en **garantizar la disponibilidad y continuidad de la API**, siguiendo experiencias como las implementadas en **Brasil** y el **Reino Unido**

GT APIs: temas a pendientes o a profundizar

Visualización y consulta del performance de APIs:

- Profundizar en la implementación de herramientas que permitan la visualización y consulta del desempeño de las APIs, facilitando el monitoreo de métricas clave

Diccionario de datos para casos de uso:

- Detallar un diccionario de datos para cada caso de uso específico (por ejemplo, API de saldos, API de transacciones), con el objetivo de segmentar la información y facilitar su parametrización y uso. (Ejemplo en slide 6)

API de consentimiento granular:

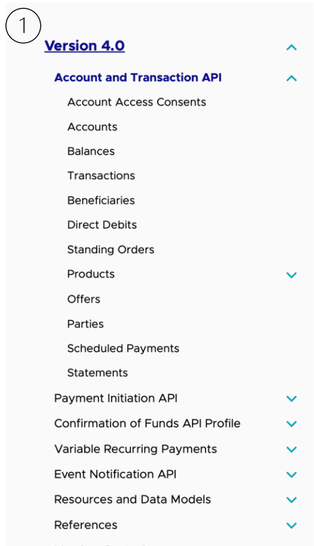
- Analizar en profundidad la API de consentimiento, proponiendo que sea granular y diferenciada por tipo de API de negocio, como cuentas, transacciones y balances, para adaptarse a las necesidades específicas del sistema. (Ejemplo en slide 6)

Procedimiento de versionamiento de APIs:

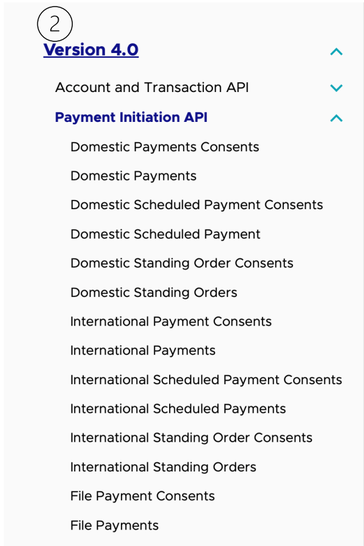
- Profundizar en el procedimiento de versionamiento de APIs, abarcando la comunicación de nuevas versiones por parte de la CMF, el desarrollo de los cambios requeridos por las entidades y los tiempos necesarios para la certificación de las nuevas versiones

GT APIs: ejemplos

1



2



- Como se detalla en la documentación del portal (imagen 1) de **Open Banking UK (OBL)**, las APIs cuentan con **especificaciones claras**, incluyendo el **diccionario de datos** para cada caso de uso, como **consentimiento**, **cuentas**, **balances** y **débito directo**, entre otros
- En el caso de las **APIs de iniciación de pagos** (imagen 2), se observa un enfoque similar. Existe documentación específica para cada caso de uso, con su respectiva **API de consentimiento** y **API de ejecución**. Por ejemplo: la **API de consentimiento para pagos domésticos** y la **API de pago doméstico**
- Por el contrario, en diccionario de datos del entregable 2 (imagen 5), la definición se **limita a solo una API genérica de consentimiento**

Diccionario de datos: API de consentimiento de cuentas

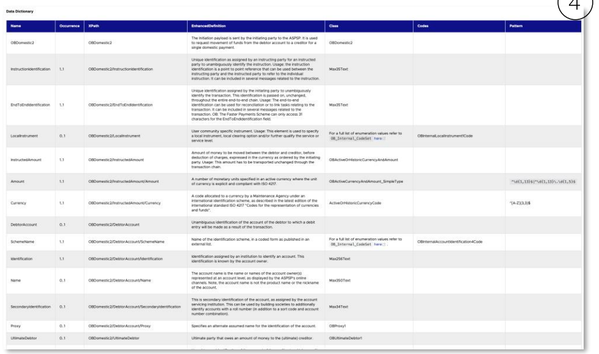
3

Data Dictionary

Name	Occurrence	XPath	EnhancedDefinition	Class	Codes
OBReadConsent1		OBReadConsent1		OBReadConsent1	
Data	1..1	OBReadConsent1/Data		OBReadData1	
Permissions	1..n	OBReadConsent1/Data/Permissions	Specifies the Open Banking account access data types. This is a list of the data clusters being consented by the PSU, and requested for authorisation with the ASPSP. For a full list of enumeration values refer to OB_External_CodeSet here	OBInternalPermissions1Code	
ExpirationDateTime	0..1	OBReadConsent1/Data/ExpirationDateTime	Specified date and time the permissions will expire. If this is not populated, the permissions will be open ended.	ISODateTime	
TransactionFromDateTime	0..1	OBReadConsent1/Data/TransactionFromDateTime	Specified start date and time for the transaction query period. If this is not populated, the start date will be open ended, and data will be returned from the earliest available transaction.	ISODateTime	
TransactionToDateTime	0..1	OBReadConsent1/Data/TransactionToDateTime	Specified end date and time for the transaction query period. If this is not populated, the end date will be open ended, and data will be returned to the latest available transaction.	ISODateTime	
Risk	1..1	OBReadConsent1/Risk	The Risk section is sent by the initiating party to the ASPSP. It is used to specify additional details for risk scoring for Account Info.	OBRisk2	

Diccionario de datos: API de consentimiento pagos domésticos

4



Diccionario de datos: consentimiento definida en entregable 2

5

Consentimiento	Creación del consentimiento	RUT cliente	String
		Finalidad	String
		Tipo de persona	Enum [PN, PJ, ambos]
		Permisos	String
		Fecha de expiración	DateString
	Consulta	ID del consentimiento	String
		RUT cliente	String
		Finalidad	String
		Tipo de persona	Enum [PN, PJ, ambos]
		Permisos	String
		Fecha de expiración	DateString
		Fecha de creación	DateString
		Fecha de actualización	DateString

GT Seguridad: temas a pendientes o a profundizar

Respuesta de autorización uso de JARM

- Es necesario clarificar el uso de este mecanismo. Si bien el punto 5.1 del documento especifica la utilización de JARM, en el punto 5.2, correspondiente a las consideraciones de implementación FAPI 2.0, se establece que no se deben implementar respuestas de autorización firmadas con JARM. Se sugiere resolver esta aparente contradicción y definir explícitamente la postura respecto a su implementación.

Servidor de Certificados CA:

- Especificar si el servidor de certificados CA constituye un componente separado del servidor de autorización o si, por el contrario, forma parte integral del mismo, y a su vez como este interactúa con el IdP que debe tener en el IPI

Creación de consentimientos

- Se requiere clarificar como se tratarán las APIs de consentimiento a nivel funcional y técnica, evitando el uso de RAR y centrándose en el método apificado

Certificados

- Detallar la especificación de los tipos de certificados requeridos, incluyendo: SSL/TLS, mTLS, Certificados de Identidad, Certificados de Infraestructura, funcionales y de seguridad. Asimismo, incluir información sobre la autoridad certificadora, la validez y cualquier otro requisito técnico relevante para la adecuada gestión de los mismos en la réplica del directorio.

Logs

- Ampliar la descripción del propósito de los logs, en particular: El objetivo de mantener registros auditables, la implementación de no repudio mediante firmas digitales, garantizando la integridad y autenticidad de la información registrada.

Controles de Seguridad del Directorio

- Se debe detallar si los controles se refieren a los servicios que provee la CMF para la sincronización del directorio o se refiere al directorio copia de la entidad. Incluyendo los informes de **pen-testing** trimestrales.

GT Seguridad: ejemplos

- Se debe precisar el uso de JARM, dado que en la imagen 1 correspondiente al capitulo 5.1 del entregable etapa 2, se considera que se debe discutir de manera profunda el **uso de JARM en próximas iteraciones** (JWT Secured Authorization Response Mode)
- Sin embargo, en la imagen 2 correspondiente al capitulo 5.2 del entregable etapa 2 se señala que **no se deberá implementar JARM** , teniendo en cuenta FAPI 2.0 para el SFA en Chile
- Se debe aclara el **uso de JARM** y para que **casos este se deberá utilizar**

(1)

Otros aspectos a considerar y discutir de manera profunda en próximas iteraciones son:

- Protección de la capa de red:
  - DNSSEC [RFC9364] para proteger contra DNS Spoofing.
  - Prohibido soportar CORS en el endpoint de autorización.
  - Uso de HTTP Strict Security Policy [RFC6797] para evitar TLS Stripping.
- Uso de Pushed Authorization Request (PAR) [RFC9126].
- Envío de client_id y request_uri al endpoint de autorización.
- Autenticación de clientes:
  - Uso de MTLS [RFC8705] o private_key_jwt [OIDC].
- Criptografía y JWT:
  - Algoritmos permitidos: PS256, ES256, EdDSA (Ed25519) [RFC8725].
  - Claves RSA de al menos 2048 bits, y claves elípticas de al menos 224 bits
- Requisitos para firmas:
  - Solicitudes de autorización: Uso de JAR [RFC9101] en el endpoint PAR [RFC9126].
  - Respuestas de autorización: Uso de JARM (JWT Secured Authorization Response Mode).
  - Respuestas de introspección: Firmadas según [draft-ietf-oauth-jwt-introspection-response-12].
  - Mensajes HTTP: Firmados con HTTP Message Signatures [RFC9421].

(2)

5.2. Consideraciones implementación FAPI 2.0 para el SFA en Chile

En la iteración E2 los GTs han acordado implementar y no implementar varias medidas del Security Profile de FAPI 2.0 y del message signing. Para el Security Profile, se ha acordado implementar la Restricción del Token mediante mTLS (mutual TLS) según el RFC8705, la Autenticación del Cliente utilizando tls_client_auth (RFC8705), y el uso de TLS 1.3 por su rendimiento superior. También se ha decidido implementar el Redireccionamiento App-To-App mediante deep-link, incluir el Token Endpoint como Parte del Claim aud, utilizar el Código HTTP 303 al Redireccionar, y emplear RAR (Rich Authorization Requests) para solicitudes de autorización más detalladas. Sin embargo, se ha acordado no implementar DPoP en los servidores de autorización, excluir el registro manual de clientes como alternativa o contingencia, y optar por DPoP y private_key_jwt en lugar de mTLS.

En cuanto al message signing, se deben implementar las Solicitudes de Autorización Firmadas (JAR), las Respuestas de Introspección Firmadas o JWT Response para la Introspección de Tokens, y la Firma de Mensajes HTTP para Solicitudes y Respuestas de Recursos. No obstante, no se deberán implementar las Respuestas de Autorización Firmadas (JARM).

Importante notar que los requerimientos del directorio establecidos durante la E0, deben ser tratados en el futuro.

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Revisión etapa 2

19 de Diciembre 2024

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de Cajas de Compensación de Asignación Familiar - Cajas de Chile A.G.

Cajas de Chile

Jueves 19 de Diciembre

Presentación Cierre Etapa 2

Foro Consultivo

Caja 18 · La Araucana más cerca · Los Héroes · Caja Los Andes

INFORMACIÓN RESERVADA Y CONFIDENCIAL

Toda información a la que se tenga acceso o se reciba en el contexto de la implementación del Sistema de Finanzas Abiertas está sujeta a la obligación de confidencialidad contenida en la Declaración de Confidencialidad del Foro de SFA firmada por todos los participantes. En consecuencia, dicha información no debe divulgarse, reproducirse ni utilizarse para fines distintos al proceso de implementación antes mencionado, salvo autorización expresa de la Secretaría Técnica o del titular de la información.

Temario

1. Mirada Temas de posición GT UX
2. Temas de posición GT Infraestructura
3. Temas de posición GT APIs
4. Temas de posición GT Seguridad

Tema de Posición GT UX

Finalidad

- **Adherimos**

Gestión de reclamos

El EdS plantea procedimientos para la gestión de reclamos de un usuario final y entre participantes.

- **Adherimos.**

Tema de Posición GT Infraestructura

Directorio

- **Adherimos.**

DCR

- **Adherimos.**

Monitoreo

- **No Adherimos.**
  - **Cajas mantiene la posición de que los auto reportes de consumo y provisión de APIs deben ser desagregados hasta cada llamada.**
  - **La ganancia en capacidad de fiscalización y entendimiento del funcionamiento del sistema es enorme.**
  - **El costo por los volúmenes de datos es bajo (ya fue demostrado por Cajas que 1TPS constante corresponde aproximadamente a 0.7GB en un mes, lo que para 2024 es despreciable).**

Tema de Posición GT API’s

Pruebas de “Consumo API” por parte de las PSBI

- **Adherimos.**

Pruebas Funcionales IPIs

- **Adherimos.**

Ambiente de pruebas PSBI e IPIs, y Sandbox

- **Adherimos.**

Certificación de Consumo de APIs(PSBI) y Pruebas Funcionales APIS (IPIs)

- **Adherimos.**

Pruebas de Calidad de Datos

- **No Adherimos.**
  - **En general adherimos con la propuesta pero creemos que los datos se deben comparar con otras instancia de despliegue de datos a usuarios, no almacenamiento. Por ejemplo, un saldo se podría almacenar con una cierta cantidad de cifras decimales y antes de desplegarla a un usuario se aplica una regla de redondeo. En la API se debe aplicar la misma regla de redondeo y se se compara contra el dato almacenado se pierde esa validación.**

Matriz Max Page Size

- **Adherimos.**

Orden de Paginación

- **Adherimos.**

Tema de Posición GT Seguridad

Clasificación de Incidentes de ciberseguridad

- **Adherimos.**

Certificación para transporte, almacenamiento, procesamiento y borrado de datos.

- **Adherimos.**

¿Qué se implementa para el Security Profile?TLS 1.2 o 1.3

- **Adherimos.**

¿Qué NO se implementa para el Perfil FAPI messagesigning?

- **Adherimos.**

Campos de Certificado de implementación de perfiles de seguridad de interfaces para las IPI y PSBI.

- **Adherimos.**

Vigencia del certificado. Cada cuanto tiempo se debe certificar.

- **Adherimos.**

Cajas de Chile

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación de Bancos e Instituciones Financieras de Chile A.G (ABIF)

Grupo Consultivo SFA

Entrega Etapa 2

19 de diciembre de 2024

banca
asociación de bancos

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

Definiciones

Ley Fintech - N°21.521 (Art. 23):

Los **Proveedores de Servicios basados en Información** y los **Proveedores de Servicio de Iniciación de pago**, en su caso, deberán adoptar mecanismos de autentificación del Cliente y **obtener su consentimiento previo y explícito** para realizar consultas de información o iniciar pagos en su nombre a través del Sistema de Finanzas Abiertas, según corresponda, a través de medios o canales electrónicos o digitales expeditos y seguros.

Para consultar información financiera a Instituciones Proveedoras de Información, a efectos de proveer servicios a los clientes basados en dicha información financiera, el **consentimiento del cliente** deberá manifestarse en forma libre, informada, expresa y **específica en cuanto al tipo de información financiera, la finalidad y el periodo máximo de validez** de esa autorización, e identificará al Proveedor de Servicios basados en Información.

Ley Datos Personales - N°21.719 (modifica N°19.628, Art. 3°):

c) **Principio de proporcionalidad.** Los **datos personales** que se traten **deben limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento.** Los datos personales pueden ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento, luego de lo cual deben ser suprimidos o anonimizados, sin perjuicio de las excepciones que establezca la ley. Un período de tiempo mayor requiere autorización legal o consentimiento del titular.

Consentimientos expresos, con finalidad específica y proporcionalidad en datos según finalidad

Posiciones Reunión 06 de Noviembre

Pregunta Temario Etapa 2:

- Proponga un listado de finalidades para los casos de uso ya discutidos.
- ¿Considera necesario que para cada finalidad definida en el punto anterior se establezcan ex-ante datos y plazos? Si su respuesta es afirmativa, proponga dicha estructura de datos y plazos

	banca asociación de bancos	BancoEstado	Asociación de Aseguradores de Chile A.G.	COOPERA Cooperativas de Ahorro y Crédito Asociadas	Cajas de Chile	FinteChile	**Propuesta** Universidad Adolfo Ibáñez
Finalidades	**Lista prestablecida:** 6 finalidades para datos (5 para PN/PJ y 1 para PJ)	**Lista prestablecida:** 6 finalidades para datos (5 para PN/PJ y 1 para PJ)	**Lista prestablecida:** 4 finalidades (3 datos + 1 pagos)	**Lista prestablecida:** 5 finalidades base para datos (las cuales pueden abrirse hasta 15 con los mismos datos y plazos)	**Lista prestablecida:** 6 finalidades para datos	**Finalidades no definidas** (texto libre). Justificación: • Claridad • Innovación • Minimalidad • Simplicidad • Evitar autotutela	**Lista prestablecida:** 11 finalidades para datos
Datos	**Tipo de datos definidos exante**	**Tipo de datos definidos exante**	**Tipo de datos definidos exante**	**Tipo de datos definidos exante**	**Sin definición de Tipo de datos exante**	**Sin definición de Tipo de datos exante**	**Sin definición de Tipo de datos exante**

Grado de alineación con la Banca: Sin definición · Convergentes · Hay divergencias · Hay divergencias críticas · Propuesta diferente

Correlacionar Finalidad y Tipo de Datos – Comparación para las Personas

	Correlación ex ante	Correlación ex post
Trasparencia	Las **personas tiene certeza de cumplimiento de proporcionalidad** los datos que se le solicitarán. Esto **aporta trasparencia** para ellos, pero también para las instituciones participantes y los reguladores	Las **personas NO tienen certeza de cumplimiento de proporcionalidad en** los datos a solicitar. Lo que podría producir **desconfianza en el sistema**, **afectando su adopción** (ej. Australia)
Proporcionalidad	La **proporcionalidad será aprobada por la CMF**, asegurando que los datos solicitados son los necesarios, adecuados y pertinentes para la finalidad establecida	La **proporcionalidad quedará a criterio de cada PSBI**, lo que también podría generar **desconfianza por parte de las personas**, afectando el alcance del SFA
Seguridad	Al ser **información establecida**, son elementos que se pueden comunicar, **mitigando potenciales fraudes o mal uso de información en general**	**Resulta complejo para las personas discernir** si la información solicitada es proporcional. Lo que **puede generar potenciales casos cuyo único objetivo sea poblar bases de datos**
Experiencia	Es posible estandarizar procesos y mejorar el modelamiento de los sistemas, **disminuyendo tiempos de respuesta**, lo que conlleva una **mejor experiencia de usuario**	Es posible estandarizar procesos y mejorar el modelamiento de los sistemas, **disminuyendo tiempos de respuesta**, lo que conlleva una **mejor experiencia de usuario**

Sin confianza por parte de las Personas, se limita el alcance del Sistema de Finanzas Abiertas

Correlacionar Finalidad y Tipo de Datos – Comparación para el Regulador e Instituciones

	Correlación ex ante	Correlación ex post
Supervisión Oportuna	**La supervisión tendría una labor preventiva**, ya que la proporcionalidad habría sido aprobada por la CMF, emulando otras industrias como los seguros con sus Condicionados Generales	**Supervisión reactiva**, **afectando la confianza de las personas** en el ecosistema
Complejidad de Supervisión	**La supervisión quedaría automatizada**, ya que se podría establecer vía sistemas la correlación Finalidad y Tipo de Datos	**Dificultad de supervisión**, generando **alta carga en los equipos** del regulador y **complejizándose la asignación de responsabilidades** de los participantes *(se estima ~200M vínculos entre instituciones)*
Riesgos para los PSBI	**Se mitigan los riesgos para las PSBI**, ya que las condiciones están establecidas y aprobadas por la CMF previamente	• **Riesgo Comercial:** Dar de baja servicios que ya se encuentran en funcionamiento • **Riesgo Reputacional:** Desconfianza por parte de los clientes en **todo el ecosistema del SFA**
Multas	**Se eliminan las posibilidades de multas por no proporcionalidad de los datos,** tanto de la CMF y la futura Agencia de Protección de Datos	**Ley Datos Personales (Art. 35.- Sanciones):** a) Infracciones leves(…) multa de hasta **5.000 UTM** b) Infracciones graves(…) multa de hasta **10.000 UTM** c) Infracciones gravísimas(…) multa de hasta **20.000 UTM** **+50%** si no se adoptan medidas para subsanar en sesenta días **X3** si hay reincidencia

Sin reglas claras, ni mitigar riesgos asociados, se limita el alcance del SFA

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

Experiencia de Usuario:
1. Cambio de finalidad (manteniendo datos y plazos)

Ley Fintech - N°21.521 (Art. 23):

Inciso primero: Los **Proveedores de Servicios basados en Información** y los **Proveedores de Servicio de Iniciación de pago**, en su caso, deberán adoptar mecanismos de autentificación del Cliente y **obtener su consentimiento previo y explícito** para realizar consultas de información o iniciar pagos en su nombre…

En el PSBI se obtiene el consentimiento

Inciso penúltimo: Las **Instituciones Proveedoras de Información** e Instituciones Proveedoras de Cuenta, en su caso, deberán **adoptar mecanismos para la autenticación de los Clientes**(…). Los medios de autenticación **y confirmación de Clientes** antes referidos deberán ajustarse a los estándares mínimos que defina la Comisión por norma de carácter general, los cuales podrán considerar reglas diferenciadas, **incluyendo mecanismos de autenticación reforzada**…

En IPI se autentican los clientes. Puede incluir mecanismos de ARC

NCG 514 (SECCIÓN III: SEGURIDAD Y RESGUARDOS DEL SISTEMA):

C.2. Autenticación del cliente financiero por parte de la IPI e IPC

Las **IPI** e IPC deberán (…) **requerir la autenticación del Cliente, lo que incluirá la autorización de acceso**(…). Esta autenticación **solo puede hacerse mediante esquemas ARC**…

La autorización de acceso a los datos se realiza mediante una ARC en la IPI

D.1. Otorgamiento del consentimiento

…**se reputará otorgado el consentimiento** por parte del titular de los datos, tanto para la IPI e IPC, como para el PSBI y PSIP, cumpliéndose con las siguientes condiciones:

a) La **voluntad haya sido manifestada de manera expresa**, en los siguientes términos:
i. *En el caso de* ***Persona Natural***: por el respectivo titular (…) para **autorizar la transmisión y tratamiento de los datos**…

La manifestación de voluntad expresa del cliente es mediante la ARC en la IPI

Experiencia de Usuario:
1. Cambio de finalidad (manteniendo datos y plazos)

Ley Fintech - N°21.521 (Art. 24):

Inciso primero: Las **Instituciones Proveedoras de Información, Instituciones Proveedoras de Cuentas, los Proveedores de Servicios basados en Información y Proveedores de Servicios de Iniciación de Pagos** participantes serán **responsables** de resguardar la **integridad, disponibilidad, seguridad y confidencialidad de los datos involucrados** en cada transacción y la adecuada privacidad de la información de los Clientes. Lo anterior, sin perjuicio del cumplimiento de las demás exigencias legales y normativas que les resulten aplicables en relación con el tratamiento de datos que cada uno de ellos realice y las disposiciones de la ley N°19.628, sobre protección de la vida privada.

Inciso final: **Las instituciones participantes serán responsables de atender las consultas y reclamos de los Clientes respecto de los datos** y servicios intercambiados a través del Sistema de Finanzas Abiertas en **que hayan tenido participación**, para lo cual deberán disponer de mecanismos de atención de Clientes, sin perjuicio de las responsabilidades que les correspondan conforme a las disposiciones de esta ley o demás leyes que les resulten aplicables conforme al ordenamiento jurídico general.

Todas las instituciones del SFA cuentan con las mismas responsabilidades en términos de seguridad y confidencialidad de datos; y atención de consultas y reclamos de clientes

Experiencia de Usuario:
1. Cambio de finalidad (manteniendo datos y plazos)

Interpretación Equipo CMF –
Escenario de que exista un cambio de finalidad, pero exista modificación de los tipos de datos, ni el plazo del consentimiento.

En conclusión, los procesos de consentimiento y autenticación, aunque relacionados, tienen funciones y actores claramente diferenciados. El consentimiento se limita a la relación entre el PSBI/PSIP y el cliente, mientras que la autenticación involucra además la responsabilidad de IPI/IPC en la verificación de identidad del cliente. Así, un cambio en la finalidad del uso de los datos que **no altere los datos ni plazos autorizados inicialmente y compartidos con el PSBI/PSIP no requiere nueva autenticación de parte de la IPI/IPC, ya que sigue siendo una relación exclusivamente bilateral entre el PSBI y el cliente.** Esta conclusión por lo demás es coherente con el principio de finalidad establecido en el proyecto de ley de protección de datos antes mencionado.

Experiencia de Usuario:
1. Cambio de finalidad (manteniendo datos y plazos)

En base a la interpretación emitida, **ABIF enviará una carta donde se sugiere complementar y aclarar los siguientes puntos:**

a) **Rol IPI e IPC**. Los bancos y, en general, las instituciones financieras, cumplen un rol garante y fiduciario con los clientes.

La interpretación emitida por el área normativa de la CMF implicará que **las IPI e IPC no podrán asumir plenamente las responsabilidades para los consentimientos que modifican finalidad sin cambio de plazos ni datos.** En particular, cabe destacar:

i. Resguardar la integridad, disponibilidad, seguridad y confidencialidad de los datos involucrados en cada transacción y la adecuada privacidad de la información de los clientes (art.24 Ley Fintec, inciso primero).

ii. Atender las consultas y reclamos de los clientes respecto de los datos y servicios intercambiados a través del SFA en que hayan tenido participación (art.24 Ley Fintec, inciso final).

b) **Rol Supervisión**. La supervisión del otorgamiento y gestión de los consentimientos requiere de un **activo rol supervisor** de las distintas etapas y roles de los distintos agentes, donde **la ARC en los consentimientos que modifican la finalidad sin alterar los plazos ni datos son responsabilidad exclusiva y directa de la PSBI o PSIP.**

Se solicita que se **complemente el documento enviado y la NCG 514, explicitando las implicancias de la interpretación legal realizada por los equipos de la CMF, precisando alcance del rol de las IPI, IPC, PSBI y PSIP.**

Esto proporcionará mayor certeza y transparencia tanto para los clientes como para los participantes del SFA.

Experiencia de Usuario:
2. Consentimiento Cerrado

Ley Fintech - N°21.521 (Art. 23):

Inciso segundo: Para consultar información financiera a Instituciones Proveedoras de Información, a efectos de proveer servicios a los clientes basados en dicha información financiera, el **consentimiento del cliente** deberá manifestarse en forma libre, informada, expresa y específica en cuanto al **tipo de información financiera**, **la finalidad** y el **periodo máximo de validez** de esa autorización, e **identificará al Proveedor de Servicios basados en Información.**

Propuesta UAI:

Existe la posibilidad de tener varios consentimientos en simultáneo. Esto quiere decir que una finalidad puede requerir múltiples consentimientos sobre varios datos, o un grupo de ítems. A esto se le llamará consentimiento cerrado.

Los ítems pertenecientes al consentimiento cerrado deben estar en concordancia con la finalidad y ligados al caso de uso. A su vez, deben aparecer agrupados.

Equipo UAI, favor explicar concepto de Consentimiento Cerrado

Experiencia de Usuario:
3. Gestión de Reclamos (Reunión 13/11)

		banca	BancoEstado	Asociación de Aseguradores de Chile A.G.	COOPERA	Cajas de Chile	FinteChile	Propuesta
Cliente → Institución	Canales	Mantener los establecidos	Mantener los establecidos	Sin propuesta definida, declaran estandarizar proceso o unificar en plataforma SFA	Mantener los establecidos	Mantener los establecidos	Mantener los establecidos	Mantener plataformas actuales, pero asegurar posibilidad de ingresos 24/7
	SLA	Mantener los establecidos	Mantener los establecidos	Comenzar con 10 días hábiles y luego ir ajustando	10 días hábiles de resolución CMF/ Sernac, 7 días hábiles	10 días hábiles para problema en misma institución +5 días si involucra a otra institución	Mantener los establecidos	10 días corridos si afecta al viaje del usuario, sino 10 días hábiles
Institución → Institución	Canales	Ticketera de la CMF Atención N1: respuesta autónoma de CMF N2: Se deriva a institución	Mediante API entre participantes	Sin propuesta definida, declaran estandarizar proceso o unificar en plataforma SFA	Define que debería existir un mecanismo de comunicación *(utilizar el modulo de comunicaciones)*	Derivación manual	Acuerdos entre participantes fuera de NCG514. Dejar copia del reclamo en plataformas de CMF	Correo entre instituciones *(Ppta Cajas)*
	SLA	5 días hábiles para dar respuesta al ticket. Luego informar tiempos de resolución	2 días hábiles para responder	• Requerimientos 10 días hábiles • Si involucran cliente CMF define el plazo • Incidentes 2,5 horas	2 días hábiles entre instituciones / 1 día hábil reguladores	5 días hábiles	Clasificación por severidad de 1 a 4, tiempos de respuesta de 1h a 8 h y resolución 4h a 7d	Clasificación por severidad de 1 a 4, tiempos de respuesta 1h a 8 h y de resolución 4h a 7d *(Ppta FinteChile)*

Grado de alineación con la Banca: Sin definición · Convergentes · Hay divergencias · Hay divergencias críticas · Propuesta diferente

Experiencia de Usuario:
3. Gestión de Reclamos – Nueva Propuesta ABIF

		Propuesta (UAI)	Nueva Propuesta (banca)	
Cliente → Institución	Canales	Mantener plataformas actuales, pero asegurar posibilidad de ingresos 24/7	Mantener los establecidos	Mantener propuesta original de: ABIF, BECH, Coopera, Cajas y FinteChile
	SLA	10 días corridos si afecta al viaje del usuario, sino 10 días hábiles	Mantener los establecidos	Mantener propuesta original de: ABIF, BECH y FinteChile
Institución → Institución	Canales	Correo entre instituciones *(Ppta Cajas)*	Correo entre instituciones	Adherimos a la propuesta de UAI, tomada desde Cajas
	SLA	Clasificación por severidad de 1 a 4, tiempos de respuesta 1h a 8 h y de resolución 4h a 7d *(Ppta FinteChile)*	5 días hábiles	Mantener propuesta original de: ABIF y Cajas. Propuesta de UAI (tomada de FinteChile) tiene problemas operacionales para el cumplimiento de esos SLA

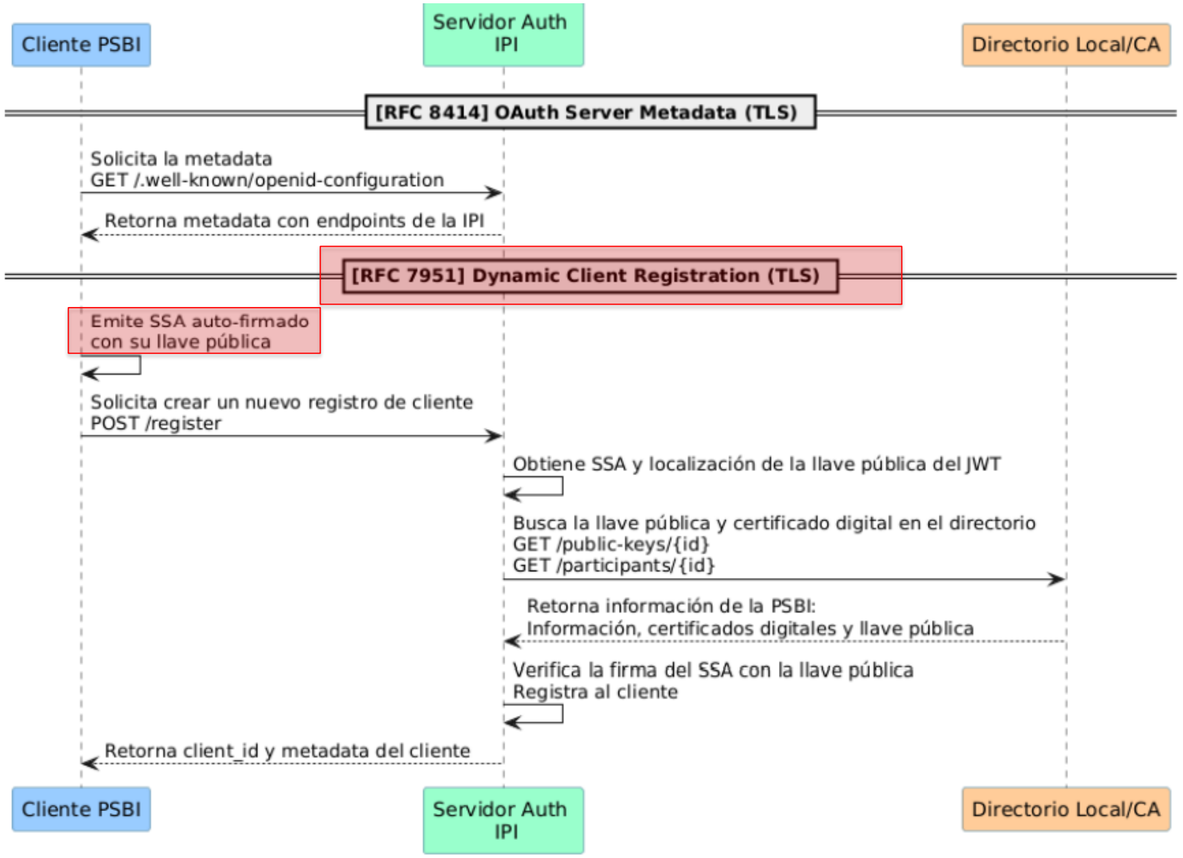
Grado de alineación con la Banca: Sin definición · Convergentes · Hay divergencias · Hay divergencias críticas · Propuesta diferente

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

Infraestructura –
DCR: Autenticación del PSBI/PSIP y Diagrama de Secuencia

Propuesta UAI:
Autenticación vía SSA auto-firmado y uso de TLS



PSC's presentarán su visión de propuesta técnica para el SFA.
Consideran pilares claves:

- Implementación **CA raíz** centralizada **(facilita mTLS en ecosistema)**
- Esquema de **firma simple robusta**
- Fortalecimiento **estándares de autenticación y custodia de claves**

Propuesta ABIF tiene un estándar de seguridad mayor y es similar a la solución de Brasil y UK:

- **Autenticación vía mTLS (propuesta inicial ABIF):** esto quedaría habilitado debido a que las PSC's contarían con una CA Raíz

- **SSA firmado por el directorio:** se indica en la presentación que este si firmaría, por lo que habilita este punto

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

API´s –
Prueba de Caludidad de Datos

Propuesta UAI:
Granularidad por dimensiones DAMA
(seis meses para establecer umbrales mínimos)

Dimensión	Descripción	Métrica
Exactitud (accuracy)	Que tan precisos son los datos en relación a otras instancias	% registros con errores % de error de los datos
Completitud (completeness)	Que tan completos son los registros en relación a otras instancias	% registros completos
Integridad (integrity)	Que tan correctas son las relaciones entre distintos datos y en el tiempo	% registros integros
Actualización (timelines)	Que tan actualizados están las APIs relativas a otras fuentes	% registros actualizados
Validez (validity)	Cumplimiento de los formatos acordados	% registros con formatos correctos
Duplicación (uniqueness)	Ausencia de registros duplicados	% registros no duplicados

Tabla 16: Matriz DAMA

Propuesta ABIF y Banco Estado:
Es consistente con tener informes al inicio del SFA que sean **simples de implementar y a la vez ricos para la toma de decisiones**. Sin perjuicio que más adelante se puedan implementar mediciones más sofisticadas como DAMA

Informe de Calidad de Información (Ejemplo)

Tamaño de la muestra: **579 consentimientos únicos**

Numero de endpoints: 2

Total de llamadas: 1158

Prueba de Comparabilidad

API XYZ	Adecuado	Inadecuado	adecuado %
Total	**940**	**218**	*81%*
Endpoint 1	**162**	**48**	*77%*
Dato x	44	26	*63%*
Dato y	58	12	*83%*
Dato z	60	10	*86%*
Endpoint n	**42**	**6**	*87%*
Dato a	16	0	*100%*
Dato b	14	2	*87%*
Dato c	12	4	*75%*

Clasificación propuesta

Excelente: > 85%
Bueno: entre 70% y 85%
Regular: entre 60% y 70%
Aceptable: entre 50% y 60%
Insatisfactorio: < 50%

Agenda

1. Finalidad y Proporcionalidad
2. Experiencia de Usuario
3. Infraestructura
4. API´s
5. Otras definiciones

Otras definiciones –
1. Temas mencionados en Entregable Etapa 2 y no definidos

Experiencia de Usuario

Selección de Productos
Definición pendiente CMF sobre entorno de selección de productos

- Definición pendiente CMF
- Definición habilitante para establecer flujos
- Reunión Consentimientos

Figura 21: Mock Entorno IPI

UAI consultó a CMF acerca de si esa selección de **detalle de producto era posible de acuerdo a su interpretación de la Ley**.

En caso de no serlo, la experiencia de cliente para autorizar compartir datos **se vería mermada,** lo que **afectaría la adopción del SFA.**

Cabe mencionar que en **Brasil, UK y Australia si se permite esa selección de detalle de producto**, como se expone en el mock

Otras definiciones –
1. Temas mencionados en Entregable Etapa 2 y no definidos

Seguridad

Control de Seguridad
Flujo de Consentimiento, *Sandbox y* Mecanismo Alternativo

MISP
Se establece como deseable, pero continuar discutiendo

Temas a establecer en Etapa 3

Propuesta ABIF:

- Enfocarnos en la utilización de RIO 2.0 (además pendiente CSIRT – Ley Ciberseguridad)
- Plataforma adicional (no intermediada por el regulador), conlleva costos y desafíos operacionales y baja expectativa de logro

Otras definiciones –
2. Definiciones CMF para la correcta implementación del SFA

Plazos de:

1. Implementación:

1. Directorio: En *roadmap* de Reunión 13/12/24, se establece “Pruebas Integrales con Instituciones” en Q1/26. Se indicó posibilidad de adelantar a Q1/25 → **ST-CMF favor confirmar**
2. Sandbox, RIO 2.0, Portal de Desarrolladores, etc. → **ST-CMF favor establecer plazos y especificaciones aún faltantes**

2. Versiones:

1. Anexo 3: Durante febrero ‘25, GT´s entregarán el 100% de flujo de datos → **Según flujo indicado en sesión del 08/08/24 del G.Consultivo, ¿ST-CMF se iniciará proceso para emitir el capitulo correspondiente? ¿Cuándo?**
2. Anexo 4: Umbrales y soluciones técnicas para cumplir con lo definido en la norma → **ST-CMF favor dar visibilidad de la versión 1 de este documento**

ST-CMF el plazo de 18 meses para el desarrollo completo del SFA es altamente exigente.
Es fundamental contar con estos plazos para planificar.

Otras definiciones –
2. Definiciones CMF para la correcta implementación del SFA

3. Servicios centralizados:

1. Posturas ya establecidas por los gremios → **Acuerdo en que el foco en Certificación Funcional y Operacional, y de Seguridad. Basada en solución de mercado, no descartando procesos de licitación acompañados por el regulador.**
2. CMF debe aprobar y supervisar a las entidades certificadoras → **ST-CMF ¿Cuándo se obtendrá respuesta de este punto?**

4. Gobierno de datos:

1. Consentimientos: Hay comprometida una reunión de parte de la CMF → **ST-CMF ¿Cuándo se realizará?**
2. Selección de productos: Consulta realizada a la CMF → **ST-CMF ¿Cuándo se tendrá respuesta?**
3. Calidad, control de finalidad, relación finalidad/datos proporcionales y especifica → **ST-CMF ¿Cuándo se tendrán definiciones?**

5. **Viabilidad financiera** iniciación de pagos → **ST-CMF ¿Existirá alguna definición para hacer viable la iniciación de pagos?**

ST-CMF estas definiciones son habilitantes para el correcto desarrollo del SFA. Es importante contar con ellas cuanto antes, para que el trabajo de los GT´s se pueda realizar correctamente.

Grupo Consultivo SFA

Entrega Etapa 2

19 de diciembre de 2024

banca
asociación de bancos

Agenda

01 Presentación EdS: Entregable Etapa 2

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 2

03 Consulta sobre Cambio en Finalidad – GT UX

Consulta sobre Cambio en Finalidad – GT UX

Consulta GT UX a CMF: Dice relación con **la interpretación de los artículos 23 y 24, específicamente en el escenario de un cambio de finalidad, que no sea plazo ni tipo de dato.** La interpretación de algunos es que este cambio de finalidad no requeriría pasar por la autenticación en la IPI nuevamente, pero para otras participantes, esto igualmente requeriría pasar por la IPI.

Para responder es relevante **distinguir entre los procesos de consentimiento y autenticación**

Consentimiento

El flujo de consentimiento ocurre **exclusivamente entre el PSBI o PSIP y el cliente, sin que la IPI o IPC intervenga en el proceso.**

Ref: Literal f) punto 1) de Sección III.D de NCG 514

Autenticación

Proceso de autenticación requiere **participación de PSBI para verificar identidad del cliente en una primera instancia.**
Posteriormente, cuando la PSBI procede a solicitar los datos a la IPI para una finalidad determinada, resulta **responsabilidad de esta última o de la IPC, por su lado, autenticar al cliente**.

Ref: Art.23 Ley Fintec

Consulta sobre Cambio en Finalidad – GT UX

Definición CMF: un cambio en la finalidad del uso de los datos que no implique una modificación en los datos ni en los plazos inicialmente consentidos **no requiere una nueva autenticación con la IPI.**

Dicha modificación **se inscribe dentro de una relación estrictamente bilateral entre la PSBI y el cliente, en la cual la IPI no tiene injerencia**, ya que no se está solicitando acceso a nuevos datos ni alterando los plazos previamente acordados, supuestos en los que en cambio sí se requeriría de una nueva autenticación para acceder a esos datos.

A contrario sensu, **si varía el tipo información cuyo intercambio, tratamiento o cesión fue consentido, o el plazo, frecuencia o período** para el que el consentimiento fue otorgado, **se requiere de una nueva autenticación**, atendido que dicho cambio incidirá en la entrega de información por parte de la IPI/IPC.

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 21
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Diciembre 2024