COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 18
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Octubre 2024

Agenda

01 Presentación EdS: Entregable Etapa 1

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 1

Consideraciones para la presente sesión del GC

- La presente sesión del Grupo Consultivo tiene por propósito **comentar el entregable de la Etapa 1** 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 1 (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 requieran profundización serán considerados y abordados en la próxima reunión del Grupo Consultivo a realizarse **el jueves 7 de noviembre**.

COMISIÓN PARA EL MERCADO FINANCIERO

Agenda

01 Presentación EdS: Entregable Etapa 1

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 1

Entrega Etapa 1
Sistema Finanzas Abiertas

Grupo Consultivo 25 de octubre

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 1

- Documento consideró: **el entregable de la Etapa 0**, la NCG, antecedentes del Directorio presentados por la CMF, **el Workshop de la Etapa 1** (realizado el 2 de agosto), **reuniones de los GT** sostenidas entre el 4 y 26 de septiembre, **retroalimentación entregable de la Etapa 0**, visión informada del Equipo de Soporte, y resultados de posiciones de los participantes de los GT a consultas del Equipo de Soporte (EdS).

- 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 1**, y la conclusion (enfocado al proceso metodológico).

02

El cuerpo con el **directorio y módulo de comunicaciones**, aspectos técnicos de las APIs, requerimientos de Seguridad, **comunicación y gestión de incidentes de Seguridad, y consentimiento**.

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 1

Estándares para el Directorio

Se realizaron cambios a la seguridad y contingencias del directorio, proponiendo un Marco Integral de Gestión de Riesgos y uptime de 99%.

Módulo de comunicación

Funcionamiento del modulo de Comunicaciones, incluyendo las APIs, los estados y cómo actualizar esta información.

Paginación

Se revisita la paginación tomando en cuenta comentarios posteriores a la Etapa 0, y las discusiones de la Etapa 1 con la inclusión de nuevos elementos (matriz de máximo pageSize).

Directorio y Módulo de Comunicaciones

Servicios API y Módulo de Comunicaciones

Incorporación de endpoints para comunicación de Participantes con el Directorio, con propuesta de estados de los participantes en el Directorio.

Diccionario de datos “base de base liviana”

Separación de los datos críticos y no críticos, identificando el responsable de la actualización de cada uno de los datos.

Estándares de Seguridad y Continuidad

Se propone que la CMF tome como base en el diseño del Directorio los criterios que resulten aplicables de su propia NCG 489, en particular se consideran importante los criterios establecidos para un Marco Integral de Gestión de Riesgos, Marco de Gestión de Riesgo Operacional, Continuidad Operacional y Seguridad de la Información y Ciberseguridad

Registro Dinámico de Clientes

Si bien hay aristas que quedaron pendientes para discusión en la Etapa 2, se propone la utilización del estándar RFC 7591 para el registro de aplicaciones PSBI con un servidor IPI.

Intercambio de Información en el SFA

Endpoints

Minimizar la cantidad de endpoints separados para Persona Natural y Jurídica.

Paginación

Paginación por offset debido a los costos de la implementación por cursor, pero incoporando algunos parámetros complementarios, con posibilidad de consultar por mes de corte.

SLAs

Se propone la utilización de una matriz de TPM y TPS, diferenciando estos valores por tamaño de institución y por endpoint.

Mecanismos alternativos

Activado por la IPI, con un esquema aprobado por la CMF. Se propone un tiempo máximo de recuperación de 15 minutos para las APIs “customer present”.

Requerimientos de Seguridad del SFA

Perfil de Seguridad FAPI 2.0

Autenticación mutua mediante mTLS. Obliga al uso de certificados EV para todas las entidades y cumpliendo con los estándares de claves públicas (PKI).

Cifrado

Se deben discutir en próximas etapas los algoritmos permitidos, claves RCA (al menos 2048 bits) y las claves de curva elíptica (al menos 224 bits).

FAPI Message Signing

Puede garantizar el no repudio mediante el uso de firmas digitales en las transacciones, pero deben estudiarse las implicancias con mayor detalle.

Comunicación y Gestión de Incidentes de Seguridad

Suspensión de participantes del SFA

La CMF es quien debe decidir la suspensión de una entidad participante del SFA.

Reporte de incidencias

Reporte a través del Sistema RIO en menos de 30 minutos, con actualización (por parte de la CMF) del estado en el Directorio.

Uso de MISP

Utilización de una Plataforma MISP pcomo herramienta para intercambio de amenazas, siendo un mecanismo separado de la CMF.

Consentimiento

Selección multiple de productos

Se debe minimizar la fricción al usuario, siempre bajo el cumplimiento de la NCG, por lo que se envió una consulta a la CMF para clarificar la interpretación legal.

Finalidad

Si bien no hay una convergencia absoluta en cuanto a si la finalidad debe ser texto libre o texto fijo, si hubo mayoría que piensa que debe existir un listado de finalidades estándar que sea regulado por la CMF, con distintas formas de escribir la finalidad según el nicho, y con un proceso para incorporar nuevas finalidades.

Usabilidad

Principios de Nielsen y pauta WCGA 2.1 con un nivel de conformidad de A, en su etapa inicial, y evolucionando gradualmente a AA.

Finanzas embebidas

Una parte importante de la discusión se centró en torno a si se debiera permitir a empresas que no son parte del perímetro del SFA el solicitar, guardar y procesar datos. La interpretación del perímetro del SFA le corresponde a la CMF, por lo que se envió la consulta.

Temas arrastre y consultas abiertas a CMF

Temas arrastre:

- En seguridad: caracterización de incidentes de ciberseguridad y respuestas
- En infraestructura: detalles implementación del DCR
- En UX: listado preliminar de finalidades y detalle mecanismo actualización
- En comunicaciones: matriz de máximo *pageSize*.

Consultas CMF:

- ¿Es posible que PSBI cambie finalidad manteniendo plazos y datos?
- Interpretación normativa para ver cómo resolver la experiencia usuaria para la selección de múltiples productos
- Borde del sistema de finanzas abiertas y finanzas embebidas

Comenzó el trabajo de la Etapa 2

- El día 24 de octubre los distintos participantes del SFA dieron el kickoff a la Etapa 2, relacionada con temas transversales.
- Luego de una dinámica de priorización a nivel de cada GT, se está trabajando en un temario unificado para el ciclo completo de la Etapa 2, que será distribuido a principios de la próxima semana.
- Las reuniones comenzarán el miércoles 6 y jueves 7 de noviembre:
  - GT UX: miércoles de 14:00 a 16:00
  - GT Infraestructura: miércoles de 16:30 a 18:30
  - GT Seguridad: jueves de 14:00 a 16:00
  - GT APIs: jueves de 16:30 a 18:30
- Debido a la relevancia de temas comunes a distintos GT, la metodología de trabajo incluye el rol de **revisores** de algunos grupos para que participen de otros GT.

Avances en Etapa 2 Sistema Finanzas Abiertas

Grupo Consultivo 25 de octubre

Agenda

01 Presentación EdS: Entregable Etapa 1

02 Presentaciones miembros GC: posiciones sobre entregable Etapa 1

COMISIÓN
PARA EL MERCADO
FINANCIERO

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

Cajas de Chile

Viernes 25 de Octubre

Presentación Cierre Etapa 1

Foro Consultivo

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

Finanzas Embebidas

“La opinión del EdS es que en la situación actual del proyecto los costos pueden ser superiores a los beneficios por lo que se propone dejar fuera de esta etapa las Finanzas Embebidas, y re visitarlo cuando el SFA ya esté implementado”

- **No adherimos.**
  - **Desde Cajas consideramos deseable un sistema de finanzas embebidas en que una organización pueda contratar una PSBI para obtener datos en el SFA sin que la organización esté necesariamente inscrita como otro PSBI.**
  - **Durante los trabajos del Foro Cajas propuso formas para incluir dentro de la UX del consentimiento a las tres partes (empresa contratante, PSBI e IPI) para que el usuario final pueda dar un consentimiento con todas las características descritas en la Ley.**
  - **Además, por la vía del mandato, creemos imposible evitar las finanzas embebidas y no reconocerlas dentro de la normativa solo provoca que sea más difícil de regular.**
  - **Creemos que es deseable incluir, dentro del trabajo del Foro llegar a un acuerdo en recomendaciones para la CMF en cómo abordar este caso de uso incluyendo la UX y una matriz de asignación de responsabilidades que comprenda la existencia de esa tercera parte.**

Selección de Productos

El EdS plantea dos escenarios y se inclina por el escenario 1

- **No adherimos.**
  - **Desde cajas reconocemos casos de uso en datos en los que es deseable que el usuario escoja los productos a compartir (ej. Finanzas personales) y otros en que es necesario que el usuario comparta todos sus productos (ej. Evaluación de riesgo crediticio).**
  - **Por lo tanto creemos que el PSBI debe, al momento de solicitar el consentimiento, indicar si necesita que el usuario comparta todos los productos (y así se indique en la UI) o si puede seleccionar productos a compartir.**

Autenticación reforzada en PSBI

- **Adherimos.**

Finalidad

- **Adherimos.**

Cambios de Finalidad

“El EdS propone que si hay cambio de finalidad, se cree un nuevo consentimiento con el flujo ya conocido, y se invalide el anterior.”

- **No Adherimos.**
  - **El encargado de gestionar el consentimiento con el usuario final es el PSBI y la IPI aparece como un mecanismo para esto. Una vez que la PSBI cuenta con la validación de identidad (derivada del consentimiento), puede acordar cambios al consentimiento con el usuario final sin pasar previamente por la IPI pero sí informando de las modificaciones para la correcta gestión del consentimiento en el panel de control de la IPI.**

Tema de Posición GT Infraestructura

Incidencias, comunicaciones y disponibilidad del Directorio

- **Adherimos.**

Mecanismos alternativos

- **No Adherimos.**
  - **En general adherimos, pero creemos que como el espíritu de la ley era que el mecanismo alternativo fuera WebScrapping dependiendo del canal de atención online principal de los IPI, no era necesario definir SLAs, pero si se van a utilizar mecanismos alternativos distintos a WebScrapping, estos deberían estar sujetos a exigencias de SLAs, sin duda, más bajos que el mecanismo principal.**

Registro dinámico de clientes

- **No Adherimos.**
  - **Creemos que cada participante debe tener sólo una aplicación cliente en el directorio por lo tanto no requiere un registro dinámico.**
  - **Pero cada PSBI debe poder tener N aplicaciones clientes registrado en cada IPI (por ambiente, por caso de usos que tengan diferentes términos y condiciones o políticas de privacidad, para permitir finanzas embebidas, etc).**
  - **Creemos que el registro de esas aplicaciones cliente debe hacerse usando el estándar DCR de OpenId Connect usando un Software Statement firmado usando el certificado del participante inscrito en el directorio.**
  - **La contraseña generada por DCR más el certificado del participante inscrito en el directorio conforman las dos pruebas de identidad necesarias para FAPI para cada llamada posterior.**

Tema de Posición GT API’s

Lista de APIs y nomenclatura de Endpoints

- **Adherimos.**

Paginación

- **No Adherimos.**
  - **En general adherimos pero creemos fundamental especificar que el orden de los datos que utilizarán los endpoints es el timestamp de creación del registro de manera ascendente, esto para evitar que la creación de un nuevo elemento mientras ocurre una paginación rompa la integridad de la respuesta.**

SLAs (TPM/TPS)

- **Adherimos.**

Medición del tiempo de respuesta de requests

- **No Adherimos.**
  - **Creemos que el tiempo a medir en los SLAs es el tiempo desde que la IPI recibe la petición hasta que envía el último byte de la respuesta.**
  - **Creemos interesante correlacionar esto con el tiempo medido desde el PSBI pero la IPI no puede ser responsable por la latencia de red involucrada y sobre la que no tiene control.**

Tema de Posición GT Seguridad

FAPI message signing

- **Adherimos.**

RFCs a utilizar

- **No Adherimos.**
  - **Aparte de todos los RFC obligatorios de FAPI 2.0 creemos necesario**
    - **Rich Authorization Requests (RAR) es el RFC 9396**
      - **Las peticiones de consentimientos son complejos, la solución de la OpenId foundation para esto es RAR**
    - **Oauth 2.0 Dynamic Client Registration Protocol (RFC7591 y RFC7592)**
      - **En el grupo de Infraestructura sostuvimos que era necesario DCR**
    - **HTTP Strict Transport Security (HSTS) (RFC 6797)**
      - **Todas las llamadas del sistema deben ser TLS**
    - **HTTP Message Signatures (RFC 9421)**
      - **Creemos necesario el firmado de mensajes para obtener “no repudio”**

Uso de mTLS y DPoP

- **Adherimos.**

No uso de rotación de refresh token

- **Adherimos.**

Reporte de incidentes

- **No Adherimos.**
  - **En general adherimos a la propuesta pero consideramos que los flujos 1a y 1b en el caso de contingencia de ciberseguridad propuestos por Banca para los PSBI también aplican para los IPI.**

COMISIÓN
PARA EL MERCADO
FINANCIERO

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

Etapa 1

Posición Coopera

Experiencia de Usuario

Tema 1 de posición: Finanzas Embebidas

Adherimos

La opinión del EdS es que en la situación actual del proyecto los costos pueden ser superiores a los beneficios por lo que se propone dejar fuera de esta etapa las Finanzas Embebidas, y revisitarlo cuando el SFA ya esté implementado.

Tal como planteamos en su momento, no consideramos que es el momento de hablar de finanzas embebidas en esta etapa de implementación

Tema 2 de posición: Selección de productos

No adherimos

El EdS propone el escenario 1, con el doble consentimiento

Consideramos que se debe utilizar el escenario 2 debido a que por medio de esta se tiene una mejor experiencia para el usuario. Siempre y cuando se cumpla que los productos que se le muestran al usuario para compartir estén ligados a la finalidad empleada. Esto significa que, en el listado de finalidades autorizado por la CMF, también deberá tener su listado de productos correspondientes a cada finalidad.

Tema 3 de posición: Autenticación reforzada en PSBI

Adherimos

- La norma habla de autenticación reforzada sólo en la IPI, no mencionando a la PSBI
- Esto da a entender que no es obligación de la PSBI implementar autenticación reforzada.

Como gremio Coopera, vamos por la reducción de costos y obligar a un PSBI a implementar autenticación reforzada es un costo adicional

Experiencia de Usuario

Tema 4 de posición: Finalidad

Adherimos

- Se propone como paso inicial un listado de finalidades estándar que sea regulado por la CMF. Este listado contiene todas las finalidades existentes inicialmente, junto a los datos que serán compartidos para tales finalidades.
- Resulta evidente que no todas las finalidades posibles estarán dentro de este listado, por lo cual se propone un mecanismo de agregación de finalidades asociado a casos de uso específicos, los cuales deben ser presentados a la CMF.
- Toda vez que la CMF aprueba la nueva finalidad, es compartida a todos los participantes del SFA y se incluye en el listado.

Tal como propusimos durante las sesiones de los grupos técnicos, estamos de acuerdo con tener un listado estándar inicial que pueda ser modificado en favor de la innovación. Queremos mencionar que se debe dejar muy claro el método de aprobación de una nueva finalidad por parte de la CMF. Esto implica definir tiempos límite para aprobar, forma de comunicación, etc.

Tema 5 de posición: Cambios de finalidad

Adherimos

El EdS propone que si hay cambio de finalidad, se cree un nuevo consentimiento con el flujo ya conocido, y se invalide el anterior

Vamos del lado de que un cambio de consentimiento implica uno nuevo

Medios de intercambio de información

Tema 1 de posición: Lista de APIs y nomenclatura de Endpoints

No adherimos

No queda claro que es lo que retorna el endpoint de resources.
Encontramos que existen errores tipográficos en la nomenclatura de los endpoints (ej: paymentcards debiese ser payment-cards).

API	Endpoint	Path
Operaciones de Crédito	Lista de Operaciones	GET /loans
	Información de la operación de crédito	GET /loans/{loanID}
	Saldo a Fin de Mes	GET /loans/{loanID}/balance
	Saldo Actual	GET /loans/{loanID}/current-balance
	Movimientos	GET /loans/{loanID}/transactions
Pólizas de Seguro	Lista de Seguros	GET /insurances
	Información de Póliza de Seguro	GET /insurances/{insurancesID}
	Movimientos	GET /insurances/{insurancesID}/transactions
Instrumentos de Ahorro o Inversión	Lista de Instrumentos	GET /investments
	Información del Instrumento	GET /investments/{investmentsID}
	Saldo a Fin de Mes	GET /investments/{investmentsID}/balance
	Saldo Actual	GET /investments/{investmentsID}/current-balance
	Movimientos	GET /investments/{investmentsID}/transactions

API	Endpoint	Path
Servicios de Operación de Tarjetas de Pago	Lista de Tarjetas de Pago	GET /paymentcards
	Información de Tarjeta de Pago	GET /paymentcards/{paymentcardsID}
	Movimientos	GET /paymentcards/{paymentcardsID}/transactions
Consentimiento	Creación	POST /consents
	Consulta	GET /consents/{consentsID}
	Actualizar	PUT /consents/{consentsID}
	Revocar	DELETE /consents/{consentsID}
Recursos	Consulta Recurso	GET /resources

Tema 2 de posición: Paginación

No adherimos

Específicamente no estamos de acuerdo en que el orden de los registros entregados por el IPI sea a opción del IPI, si no que vemos la necesidad de que estos estén ordenados por fecha de creación/modificación ascendente, esto quiere decir que el ultimo registro en ingresar es el último en retornarse

Utilización de Offset, debido a costos de desarrollo debido a cambio a cursor.

- Incorporación de los siguientes parámetros (moviéndose hacia un parecido a cursor):
  - Page: página a ser devuelta por API
  - Page-size: con las opciones 25, 50, 100, y máximo pageSize, el default es 100.
  - fromTransactionDate: Fecha de corte
  - toTransactionDate: Fecha de corte
- Máximo pageSize se calcula en base a parámetro a definir para cada producto (en base al cálculo de registros que minimice la necesidad de paginación).
- Ordenamiento de responsabilidad del consumidor de la API (para este caso de uso). Independiente de eso, el proveedor de la información debe acompañar la respuesta con un parámetro que indique el tipo de ordenamiento utilizado: unsorted, alpha, numeric. Además, el campo sobre el cual se ordenaron los registros.
- Seguir estructura https://jsonapi.org/format/
- Matriz de máximo pageSize. Se propone que los valores de esta matriz se calculen en base a la experiencia de los primeros meses de funcionamiento del SFA

Medios de intercambio de información

Tema 3 de posición: SLAs (TPM/TPS)

Adherimos

Se propone la implementación de una matriz de TPM y TPS, diferenciando estos valores por tamaño de institución y por endpoint.

- Como valor default: 10 TPS (de una IPI a todos los PSBI) y 60 TPM (de una IPI a cada PSBI)
- Para las siguientes etapas queda pendiente ajustar estos valores iniciales según:
  - Tamaño de institución, para lo que se deberá acordar la variable que defina esto.
  - Cálculo de TPM y TPS ajustada por endpoint.

Implementación de un sistema de revisión de los TPM/TPS que permita actualizar estos parámetros según el dinamismo del SFA. Se propone:

- Revisión de la matriz de TPM y TPS para cada institución de manera mensual durante los primeros 6 meses, y de manera trimestral posteriormente.
- Los datos para esta revisión deberán ser los informados en el auto reporte de cada IPI (los auto reportes están en revisión).

Queremos poner foco en determinar de manera detallada el reajuste de los parámetros de acuerdo con el tamaño de la institución.

Tema 4 de posición: Medición del tiempo de respuesta de requests

Adherimos

Tiempo desde cuando PSBI hacer request a endpoint hasta la respuesta de la IPI (menor a 4.000 milisegundos. Si son más de 100 registros, la medición se aplica a 100 registros).

Infraestructura

Tema 1 de posición: Incidencias, comunicaciones y disponibilidad del directorio

Adherimos

Estándar para el directorio, contingencia/monitoreo/desconexión, estados / transiciones y módulo comunicaciones

Tema 2 de posición: Mecanismos alternativos

No adherimos

Propuesta EdS

- Dado alto uptime, parece razonable postura 1
- Cada IPI deberán plantear en el esquema a CMF: respuesta, velocidad => homogéneo y conocido
- Tiempo máximo de recuperación 15 minutos. Priorizar APIs “customer present”!

A pesar de estar de acuerdo con prácticamente toda la propuesta sobre el mecanismo alternativo, no nos adherimos por la condición de los 15 minutos de tiempo de recuperación, observamos que posiblemente este valor no sea suficiente. Por otra parte, recalcamos que no consideramos necesaria la conversación de un mecanismo alternativo considerando las exigencias y estándares que debe cumplir el mecanismo principal. Además, debemos tener en cuenta los costos que está implicando la definición de este mecanismo alternativo y lo perjudicial que puede llegar a ser para ciertas entidades financieras.

Tema 3 de posición: Registro dinámico de clientes

No adherimos

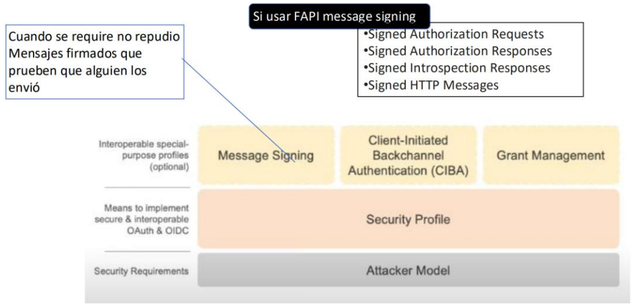
- Se considera importante poder ingresar las aplicaciones de los PSBI
- Dado el volumen de cambio, se sugiere ingresar via MC, con actualización automática al Directorio.

Creemos que no hay necesidad de implementar una solución customizada sobre el registro dinámico de clientes, por lo que no nos adherimos y proponemos utilizar el estándar RFC7591

Seguridad, Perfiles y Autenticación

Tema 1 de posición: FAPI message signing

Adherimos



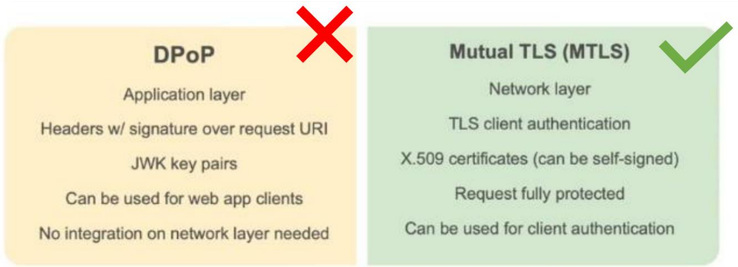
Tema 2 de posición: RFCs a utilizar

No adherimos

Vemos la necesidad de implementar el estándar **RFC7591** para resolver el registro dinámico de clientes, dado que un PSBI puede tener más de una aplicación para consumir los recursos de la IPI. Además, recomendamos utilizar el estándar **RFC6797**.

Tema 3 de posición: Uso de mTLS y DPoP

Adherimos



Seguridad, Perfiles y Autenticación

Tema 4 de posición: Uso de rotación de refresh token

Adherimos

Acorde a Banca los refresh tokens solo pueden ser utilizados por el client_id que los obtuvo y este client_id estará vinculado a un certificado digital de una organización específica.

- Los PSBIs deben almacenar sus refresh tokens en bases de datos enriptadas y con estricto control de acceso
- Genera problemas operativos más que adicionar seguridad en sí

No usar rotación de refresh tokens

Tema 5 de posición: Reporte de incidentes

Adherimos

Estructura de reporte : información básica/descripción/cronología del incidente – sistemas o datos afectados – respecta al incidente – investigación técnica – impacto y consecuencias

- Estándares ISO 27.035 Y NIST 800-6 para estructurar respuesta a incidentes.
- Plataforma (alternativas):
- RIO 2.0 con workflow de reporte y respuesta para eventos operacionales y de ciberseguridad + MISP para eventos de ciberseguridad (que no esté en la CMF y se utilice como medio de intercambio de amenazas potenciales, intentos de ataques, impacto en infraestructura, etc.).
- La norma NCG 514 ya aborda este tema.
- Existen leyes para tratar el tema de fraudes y AML (ley 20009)

Usar Propuesta Banca

Etapa 1

Posición Coopera

COMISIÓN
PARA EL MERCADO
FINANCIERO

Banco del Estado de Chile (BancoEstado)

Entregable Etapa 1:
Información Persona Natural e Información Pública

Visión BancoEstado

Implementación SFA

25 de Octubre de 2024

APIs

❑ Paginación

- **Limitar paginación** a aquellos *endpoints* que retornen resultados de gran tamaño (por ejemplo, listas de productos y transacciones) para **optimizar su eficiencia y escalabilidad**.
- Sugerimos **límites** de **hasta 500 registros por página**

❑ SLAs (TPM/TPS)

- **Tema complejo** de abordar pues es extrapolación de experiencia internacional no necesariamente es aplicable en Chile.
- **Gradualidad** en adopción de valores permite ir ajustando estas métricas a la realidad local.
- **De acuerdo** con iniciar con **valores default** (10 TPS y 60 TPM), pero **no estamos de acuerdo** con incorporar **valores diferenciados por tamaño de la IPI en las etapas iniciales**

Seguridad

❑ RFCs a utilizar

- Utilizar el **registro dinámico de clientes** (DCR) como **mecanismo opcional de autenticación**.
- De este modo, sugerimos **incluir estándares técnicos relativos a DCR y DCM** (gestión dinámica de clientes).

❑ Reporte de incidentes

- **De acuerdo** con implementar una **plataforma MISP** para facilitar **intercambio de información sobre amenazas de seguridad**.
- Relevamos la **importancia** de **no depender exclusivamente de este sistema** para **gestión y reportería de incidentes o vulnerabilidades** dentro del SFA.

UX

❑ Finanzas embebidas

- ➢ De acuerdo con **postergar la discusión** de este tema
  - Bajo este esquema, **no hay control de los datos de clientes manejados por terceros**.
- ➢ **Revisitar** el tema **luego de la implementación del SFA**.

❑ Selección de productos

- ➢ Selección múltiple de productos con **doble consentimiento** ofrece una **experiencia de usuario inferior** respecto de una con un **único consentimiento**.
- ➢ **Nuestra visión** respecto de este punto:
  - **Selección de productos** se define al escoger **finalidades establecidas**.
  - **Detalle de los productos** seleccionados por el cliente en la **IPI.**

Infraestructura

❑ Incidencias, comunicaciones y disponibilidad del Directorio

- ➢ **Estándar NCG 489** (cámaras de bajo valor) es **adecuado para regular al Directorio**.
- ➢ Sugerimos que Directorio debiera extender **normas similares al OBIE** (*Open Banking Implementation Entity*) de UK:
  - **Servicios de emisión** participant id/client id
  - **Validación de certificados** utilizados por las IPI/PSBI/PSIP
  - **Portal de gestión de cambios** en el Directorio
  - **Enrolamiento automatizado de instituciones**

❑ Mecanismos alternativos

- ➢ **Plazo máximo** de **30 minutos** para **informar eventos de seguridad/incidentes operacionales**, de acuerdo con la RAN 20-8.
- ➢ Sugerimos **evaluar la pertinencia del uso de web scrapping**
  - ➢ **Complejidades** asociadas a **garantizar** que **servicios de consentimiento y autorización se implementen**.

Gracias

BancoEstado
desde 1855

COMISIÓN
PARA EL MERCADO
FINANCIERO

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

Grupo Consultivo

Entrega Etapa 1

25 de octubre de 2024

banca
asociación de bancos

Etapa 1

Experiencia de Usuario - UX	
Pauta WCAG	**Infactible:** Pauta WCAG implica **modificaciones en HTML y CCS**. Existen flujos digitales vigentes que **no es posible adaptarlos** en el 100% de esta pauta (Ej. gestores contenidos seguros, 2FA-NCG514) La propuesta del EdS, en nuestro conocimiento, no es respaldado por ningún miembro del Foro.

Etapa 1

Infraestructura	
Directorio	**Incompleto:** Faltan definiciones de **procesos**, definiciones **técnicas**, **protocolos** y ***payloads*** (No Exhaustivo) Debe existir **catálogo de incidentes** y respectivos **marcos de actuación**
Mecanismo Alternativo	**Inconsistente:** Uso **exclusivo** de **réplicas de API o sus instancias** ya que entregará **mayor seguridad y mejor calidad** de datos al SFA en casos de contingencia **(no webscrapping)**

Etapa 1

API	
Flujos de Consentimiento	**Incorrecto:** Flujos con **detalles incorrectos** en la propuesta (se hará llegar documento a EdS)
Reporte de Performance	**Infactible:** Reporte **granular** genera problema de procesamiento en **altos volúmenes** de transacciones
Diccionario de Datos	**Incompleto:** Se requiere detalle sobre estructura de los *payloads* y reglas de campo **(bloqueante para desarrollo)**

Etapa 1

Seguridad	
FAPI *Message Signing*	**Incompleto:** EdS establece necesidad de revisar uso del protocolo de manera transversal. **Se requiere una definición**, para esto debe existir una **evaluación de impacto de las alternativas**

Definiciones

1. **Supervisión y Certificación de seguridad**
    1. Validar la seguridad en **Transporte, Procesamiento, Almacenamiento y Borrado de Información** (incluido **Directorio**)
    2. **Servicios centralizados:** rol de la CMF para supervisar y autorizar potenciales servicios a centralizar
2. **Plazos de Implementación:** Directorio, Sandbox, RIO 2.0, Portal de Desarrolladores, etc.
3. **Gobierno de datos:** calidad, control de finalidad, relación finalidad/datos proporcionales y especifica
4. **Umbrales:** soluciones técnicas para cumplir con lo definido en la norma (Anexo 4)
5. **Plazos de las versiones** del Anexo 3 y Anexo 4
6. **Viabilidad financiera** iniciación de pagos

Grupo Consultivo

Entrega Etapa 1

25 de octubre de 2024

banca
asociación de bancos

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.

Comentarios Post Entregable Etapa 1

Octubre / 2024

Revisión Posición AACH Etapa 1

Directorio

Estamos de acuerdo con los puntos planteados, incorporaron nuestras consideramos tales como: uso del DCR, gobernanza del directorio (CMF), gestión de estados, entre otros. Sin embargo, consideramos que el uptime debe ser igual al del sistema en atención a que es una pieza clave en el sistema.

Intercambio de Información

Estamos de acuerdo con los puntos planteados, se utilizó la lista de errores que propusimos como Asociación y los tiempos de respuesta van en línea con lo que propusimos en los GT.
Respecto al mecanismo alternativo a nivel de API nos parece suficiente para una primera etapa, en particular para mantener todos los beneficios en cuanto a seguridad que plantea FAPI 2.0.

Requerimientos de Seguridad

Estamos de acuerdo con la mayoría de los puntos planteados, sin embargo, nosotros sí consideramos que **debemos utilizar FAPI Message Signing**, pues es parte del estándar.

Gestión de Incidentes de Seguridad

Como Asociación consideramos que se debe **diferenciar** entre **incidentes de ciberseguridad de los operacionales.**

- **Ciberseguridad:** proponemos que la CMF con SCIRT definan el mecanismo a aplicar
- **Operacionales:** proponemos que continúen siendo canalizados por RIO (Canal definido x CMF)

Consentimiento

Como Asociación estamos de acuerdo con la mayoría de los puntos, sin embargo, **faltan profundizar aspectos tales como 2FA, confirmar que tanto la IPI y la PSBI deben autenticar al cliente y definir cómo abordar las finanzas embebidas**

Comentarios Generales Avanzado a la fecha

A continuación, se hace referencia a aspectos relevantes sobre el avance del SFA, sin ser necesariamente relativos al entregable de la Etapa 1:

1. **Riesgos y mitigadores:** Dado los grandes desafíos que impone la implementación del Sistema de Finanzas Abiertas, debemos comenzar a implementar una matriz clara de riesgo en los grupos técnicos y que los riesgos más relevantes sean escalados por el equipo de soporte al Grupo Consultivo*
2. **Ley de Ciberseguridad/Reglamentos - Ley de Datos Personales:** Proponemos revisitar la norma y el trabajo en los grupos técnicos desde la perspectiva de estas leyes que están avanzando en su proceso de implementación.
3. **Anexo 3**: Entendemos que el trabajo propuesto para desarrollar el Anexo 3 es un trabajo que irá evolucionando a medida que se desarrollen las etapas planificadas por el regulador y el equipo de soporte, pero habiendo terminado la Etapa 1 de la Fase 2 sería oportuno contar con la 1ra versión de este anexo.
4. **Preocupaciones Industria**: Actualización de listado de productos: rentas vitalicias, SOAP, ¿coaseguros?, entre otros, junto con el intercambio de información sensible, por ejemplo, los datos de salud de los clientes (referenciado en el registro del documento fase 1).
5. **Gradualidad:** Seguimos considerando que es muy importante tener en cuenta la posibilidad de avanzar con el criterio de gradualidad en los **productos/Casos de Usos**, apuntando a comenzar con los más masivos; gradualidad en lo funcional, comenzar con persona natural para que luego de un período de madurez y estabilidad del SFA avanzar con persona jurídica si se estima oportuno.
6. **Roadmap:** proponemos que en conjunto, el Foro Consultivo comience a definir un roadpmap a alto nivel con fechas tentativas para conocer los hitos relevantes en el contexto de la implementación del SFA. Es importante otorgar visibilidad a todos los participantes del SFA a partir de este roadmap.

** Referencia del documento Entregable Etapa 1: "el Directorio debiese contar con un Marco Integral de Gestión de Riesgos que asegure la continuidad de sus servicios, así como la integridad y oportunidad de la información contenido"*

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

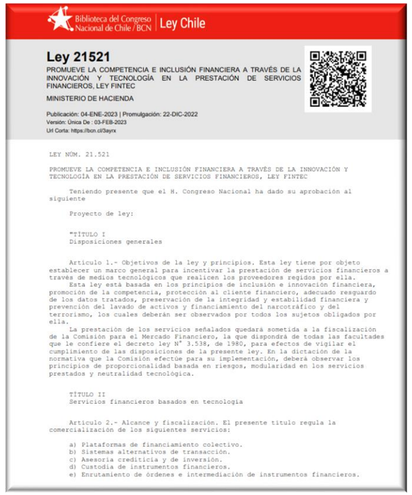
Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

Los GT se encuentran trabajando la elaboración de los manuales técnicos

Ley Fintec


Biblioteca del Congreso Nacional de Chile / BCN | Ley Chile

Ley 21521

PROMUEVE LA COMPETENCIA E INCLUSIÓN FINANCIERA A TRAVÉS DE LA INNOVACIÓN Y TECNOLOGÍA EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS. LEY FINTEC

MINISTERIO DE HACIENDA

Publicación: 04-ENE-2023 | Promulgación: 22-DIC-2022
Versión: Única De - 03-FEB-2023
Url Corta: https://bcn.cl/3eyrx

LEY NÚM. 21.521

PROMUEVE LA COMPETENCIA E INCLUSIÓN FINANCIERA A TRAVÉS DE LA INNOVACIÓN Y TECNOLOGÍA EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS, LEY FINTEC

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

"TÍTULO I
Disposiciones generales

Artículo 1.- Objetivos de la ley y principios. Esta ley tiene por objeto establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos que realicen los proveedores regidos por ella.
Esta ley está basada en los principios de inclusión e innovación financiera, promoción de la competencia, protección al cliente financiero, adecuado resguardo de los datos tratados, preservación de la integridad y estabilidad financiera y prevención del lavado de activos y financiamiento del narcotráfico y del terrorismo, los cuales deberán ser observados por todos los sujetos obligados por ella.
La prestación de los servicios señalados quedará sometida a la fiscalización de la Comisión para el Mercado Financiero, la que dispondrá de todas las facultades que le confiere el decreto ley N° 3.538, de 1980, para efectos de vigilar el cumplimiento de las disposiciones de la presente ley. En la dictación de la normativa que la Comisión efectúe para su implementación, deberá observar los principios de proporcionalidad basada en riesgos, modularidad en los servicios prestados y neutralidad tecnológica.

TÍTULO II
Servicios financieros basados en tecnología

Artículo 2.- Alcance y fiscalización. El presente título regula la comercialización de los siguientes servicios:

a) Plataformas de financiamiento colectivo.
b) Sistemas alternativos de transacción.
c) Asesoría crediticia y de inversión.
d) Custodia de instrumentos financieros.
e) Enrutamiento de órdenes e intermediación de instrumentos financieros.

Regula a las Fintechs y establece la creación del Sistema de Finanzas Abiertas (SFA), definiendo objetivos y principales consideraciones

Normativas

Define los requisitos para la inscripción de las Fintechs

Define las reglas que rigen el SFA a nivel de lineamientos y definiciones técnicas

Manuales Técnicos

Profundiza y detalla los aspectos más técnicos para el funcionamiento del SFA

Actualmente estamos trabajando en la etapa 2, sin embargo, es acumulativo a medida que avanzan las etapas

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Mar – Julio /24	Jul – Oct /24	Oct – Nov /24	Nov – Ene /25	Ene – Mar /25
0	1	2	3	4
Etapa 0 Fase 1	**Etapa 1 Fase 2**	**Etapa 2 Fase 2**	**Etapa 3 Fase 2**	**Etapa 4 Fase 2**
▶ En la fase 0 se trabaja el flujo de solicitud de información de términos y condicione y canales	▶ Flujo de consulta de información de Persona Natural (incluye mecanismo alternativo)	▶ Flujo de consulta de información de Persona Jurídica + mecanismo alternativo.	▶ Revisaremos las posiciones finales, y seleccionaremos un responsable que debe enviar el documento antes de cada sesión.	▶ Iniciación de pagos.

Estamos acá

Los puntos revisados en las etapas 0 y 1 fueron los siguientes:

Fase 0: Información pública

- ✓ Realización de esquema de información
- ✓ Dependencias del SFA, directorio y máquina de estado
- ✓ Diccionario de datos
- ✓ Certificados
- ✓ Estándares de seguridad y continuidad del directorio
- ✓ Diccionario técnico
- ✓ Endpoints y servicios
- ✓ Definición de los endpoints de las APIs
- ✓ Paginación
- ✓ Perfil de seguridad
- ✓ MTLS
- ✓ Autoridades certificadoras
- ✓ Administración de Logs
- ✓ Controles de seguridad
- ✓ Dashboard
- ✓ Monitoreo
- ✓ Gestión de incidentes

Por cada semana se realizaron 4 reuniones semanales de trabajo, llevamos postura como Asociación y participamos de workshops

Fase 1: Información privada

- ✓ Lista y SLAs de APIs y nomenclatura de Endpoints
- ✓ Diagrama de flujo de consentimiento (A nivel de APIs y UX)
- ✓ Paginación, arquitectura de APIs, máquina de estado, mecanismos alternativos
- ✓ Perfil FAPI 2.0
- ✓ Flujos de autenticación y firma (encriptación)
- ✓ Flujos de información
- ✓ Registro de clientes
- ✓ Reportes y directorio
- ✓ UX, usabilidad, directrices,
- ✓ Gestión de consentimiento
- ✓ Agrupación de datos, casos de error

Desde el 4 al 26 de septiembre, con 4 sesiones a la semana de trabajo + presentaciones de la AACHH

La metodología de trabajo es la siguiente

Envían un temario con los temas a discutir en cada grupo técnico, consultando por las posturas de los gremios por cada tema

Reciben el material enviado por la Universidad Adolfo Ibáñez, y envían a AACHH e EY

Reciben el temario y la propuesta para analizarlo internamente, EY prepara respuestas en base a experiencia internacional y lleva reuniones de trabajo con GTs

Centro de Innovación Financiera de la CMF

UNIVERSIDAD ADOLFO IBÁÑEZ

Participantes de los Grupos Técnicos

ASOCIACION DE ASEGURADORES DE CHILE A.G.

EY Building a better working world

Los representantes de cada Asociación envían sus posturas a la CMF, estableciendo así la definición final como industria

Revisan posturas, realizan cambios o comentarios, en caso de existir y presentan entre todos los gremios participantes del SFA

Asociadas, junto con la AACH consensuan una postura como gremio

Consideración

Existen temas y/o posturas revisadas tanto en la Etapa 0, como en la Etapa 1, esto debido a que el objetivo es ir avanzando en la profundización y conocimientos del tema en mayor nivel de detalle a medida que avanzan las etapas de los Grupos Técnicos. Lo anterior también implica que al estar en la etapa 2, los temas revisados a continuación pueden sufrir modificaciones.

A su vez, se debe considerar que los temas expuestos en este documento son un resumen del documento de entregable de la Etapa 1, siendo una propuesta creada por la Universidad Adolfo Ibáñez, que considera la postura de los gremios del grupo consultivo y que no tienen una validez regulatoria, pues es la CMF la encargada de tomar la decisión final de lo expuesto en el anexo 3 de la normativa NCG 514.

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

Directorio y Módulo de Comunicaciones

El **Directorio**, es un componente que permite a los participantes del SFA ser validados para i**nteractuar** entre ellos a través de APIS. Este componente **será administrado por la CMF**. Recordar que en la NCG 514 se mencionan los atributos necesarios para inscribirse al SFA y, por ende, registrarse en el directorio

Propuesta UAI

- ✓ Tendrá dos **mecanismos de actualización**:
  - ✓ El primero son cambios que produce la **CMF** al directorio para reflejar cambios en los registros y nómina de participantes que mantiene la CMF
  - ✓ El segundo son cambios efectuados por los mismos **participantes,** (en caso por ejemplo de incidente operacional y/o de ciberseguridad)
- ✓ Usará un **mecanismo de webfinger** para la entrega de información no crítica a los participantes.
- ✓ Cada participante del directorio puede estar en los siguientes estados: **activo, en alternativo, inactivo, vigente o suspendido,** y la transición de los primeros 3 será reportada por el partícipe al directorio a través de una API
- ✓ Cada participante debe contar con una **copia local** y que es su responsabilidad consultar periódicamente la actualización de este
- ✓ El Directorio por su lado, debe avisar en caso de ocurrir cambios y mantenerlo actualizado
- ✓ El diccionario de datos del directorio se encuentra en las páginas 27 y 28
- ✓ El directorio debe seguir los **estándares de seguridad de la NCG 489** (Cámaras de bajo valor)
- ✓ Se considera que el directorio puede tener un **uptime menor al sistema** (99%), sin tener impacto
- ✓ El reporte de cada PSBI /IPI debe ser mensual y contener, tasas de éxito de las APIs, tiempos de respuesta y tasas de abandono / rechazo
- ✓ La comunicación será **por APIs,** para más detalle de la taxonomía ver página 30
- ✓ Se usarán los **RFC 7591 y 7592 para el DCR**

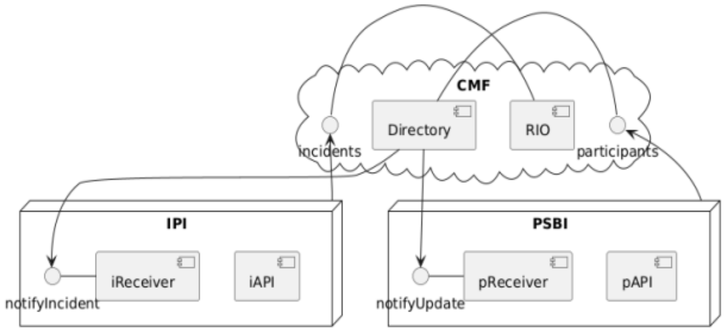


Ilustración 2: Dependencia entre SFA y Directorio

Postura AACH

Estamos de acuerdo con los puntos planteados, incorporaron nuestras consideramos tales como: uso del DCR, gobernanza del directorio (CMF), estados, entre otros. **La única discrepancia es que nosotros propusimos que el uptime debe ser igual al del sistema**

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

Intercambio de Información

El **Intercambio de Información** en el Sistema de Finanzas Abiertas (SFA) hace referencia a los mecanismos y estándares necesarios para compartir la información entre instituciones participantes del sistema. En la Ley y en la Normativa, queda establecido que esta comunicación **debe ser por APIs**, sin embargo, ahora se están construyendo los detalles del funcionamiento de éstas

Propuesta UAI

- ✓ La UAI propone el **diccionario de datos**, la descripción y el tipo de datos (ver página 32)
- ✓ La UAI propone la **lista de endpoints de las APIs**, estos serán escritos en inglés para mantener formato internacional. Durante las sesiones hubo consenso en tratar de minimizar la necesidad de separar endpoints por (ver página 44**) PN (Persona natural) y PJ (Persona jurídica),** por lo que se propone separar **solo la información del enrolamiento** por la diferencia de campos, el resto de los campos serán separados y serán diferenciados a través de querys
- ✓ Uso de API de recurso que **permite a los PSBI verificar los recursos disponibles asociados a un consentimiento**
- ✓ Paginación: se paginará solo los endpoints que retornen de gran tamaño
- ✓ Agregar parámetros: Page, Page-size con las opciones 24,50,100 y máximo pagesize
- ✓ Ordenamiento: timestamp de creación de registro **de manera ascendente**
- ✓ Códigos de error: Se propone la lista utilizada comúnmente (ver página 45)
- ✓ Usar una matriz de TPM y TPM, diferenciado por tamaño de la institución y endpoint, (TPS:10 Y 60 TPM). La matriz se revisará de manera trimestral en el auto-reporte
- ✓ Rendimiento: request, la normativa comenta un tiempo máximo de 4.000 milisegundos, considerando el tiempo entre que se realiza la consulta de la API y el tiempo TTLB transcurrido, midiendo por endpoint utilizando el percentil 95
- ✓ Mecanismo alternativo:
  - ✓ Debe ser transparente para PSBI. Si una IPI opera en mecanismo alternativo debe avisar a la CMF
  - ✓ Cada IPI deberá resolverlo por lo que la forma del mecanismo alternativo lo debe aprobar la CMF
  - ✓ Lo debe activar la IPI una vez que identifique problemas con el mecanismo principal, se propone un tiempo de recuperación de 15 minutos
- ✓ Auto reporte: se proponen el contenido (p.50) y la CMF será la responsable de recibir la información

Postura AACH

Estamos de acuerdo con los puntos planteados, se utilizó la lista de errores que propusimos como Asociación y los tiempos de respuesta van en línea con lo que propusimos en los GT. Respecto al mecanismo alternativo a nivel de API nos parece suficiente para una primera etapa, en particular para mantener todos los beneficios en cuanto a seguridad que plantea FAPI 2.0.

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

Requerimientos de Seguridad

El **SFA es un ecosistema de intercambio de datos** entre clientes de instituciones financieras y proveedores de servicios financieros. Para asegurar que la comunicación y el **intercambio de datos entre los PSBI y las API sean seguros y eficientes** se aplica el perfil de seguridad FAPI 2.0 en cumplimiento con la norma

Propuesta UAI

- ✓ Perfil de seguridad FAPI 2.0, junto con su modelo del atacante
  - ✓ Firmado de mensajes de FAPI 2.0
  - ✓ Implementación de autorización y autenticación segura
  - ✓ Cumplimiento estricto del uso de PKI de FAPI 2.0
- ✓ Uso de mTLS, con certificado EV
- ✓ Certificados:
  - ✓ Deben ser criptográficos, emitidos por una autoridad certificadora o Prestador de Servicios de Certificación
  - ✓ Usaremos certificados de Validación extendida (VE), pues ofrece mayor nivel de seguridad, el certificado es otorgado por la Autoridad certificadora (CA)
  - ✓ Las CA deben ser respaldada por una entidad de raíz chilena y la lista debe ser administrada por la CMF, estando homologadas por el Ministerio de Economía
- ✓ Cifrado: Algoritmos permitidos: FAPI 2.0 permite uso de algoritmos como PS256 ES256 y Ed25519 para JWT, RSA debe tener al menos 2048 bits, y clave de curva elíptica al menso 225 bits
- ✓ Administración de logs asociados a no repudio: Si bien no se tomaron acuerdos sobre el Message Signing, se quiere discutir en próximas etapas pues el uso del Message Signing ayuda a garantizar el no repudio
- ✓ Requerimientos generales
  - ✓ Controles de seguridad del directorio: (Tema no tratado explícitamente en los GT), se deben implementar controles se seguridad al directorio tales como: Seguridad perimetral, control de amenazas, WAF, y seguridad del directorio
  - ✓ Se deben seguir las normativas y especificaciones tales como: ISO 27001, ISO 22301, ISO 27002 e ISO 27032
  - ✓ Debe existir un dashboard de monitoreo en tiempo real para los participantes

Postura AACH

Estamos de acuerdo con la mayoría de los puntos planteados, sin embargo, nosotros si consideramos que debemos utilizar FAPI Message Signing, pues es parte del estándar.

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

Comunicación y Gestión de Incidentes de Seguridad

Es crucial establecer **protocolos de acción y canales de comunicación simples y expeditos** ante la ocurrencia de incidentes operacionales y se seguridad

Propuesta UAI

- ✓ Un partícipe **deberá informar la ocurrencia de un evento operacional** (incluyendo de seguridad)a la CMF en **no más de 30 minutos** por el canal de reporte de incidentes operacionales (RIO). La CMF decidirá las acciones a seguir, incluyendo la suspensión temporal del partícipe, gatillando en forma automática la actualización del directorio. El fin de **la suspensión será una decisión de la CMF**
- ✓ Acuerdo sobre implementar una plataforma de intercambio de información sobre Malware (Malware information sharing platform MSIP), la UAI considera que si bien es valioso no debe ser el mecanismo de reporte.
- ✓ En casos donde la CMF estime que la naturaleza del incidente en uno o más partícipes o del propio directorio podrían poner en riesgo la seguridad del SFA
- ✓ **Se siguiere seguir discutiendo el MISP en la siguiente etapa**

Postura AACH

Como Asociación consideramos que se debe diferenciar entre incidentes de ciberseguridad de los operacionales, los primeros debiesen informarse al CSIRT y a la CMF (para actualizar en el Directorio si así lo estima oportuno) y los operacionales por RIO

Estado de Situación: Entregable Etapa 1

Contexto: Metodología de Trabajo

Tema 1: Directorio y Módulo de Comunicación

Tema 2: Intercambio de Información

Tema 3: Requerimientos de Seguridad

Tema 4: Comunicación y Gestión de Incidentes de Seguridad

Tema 5: Consentimiento

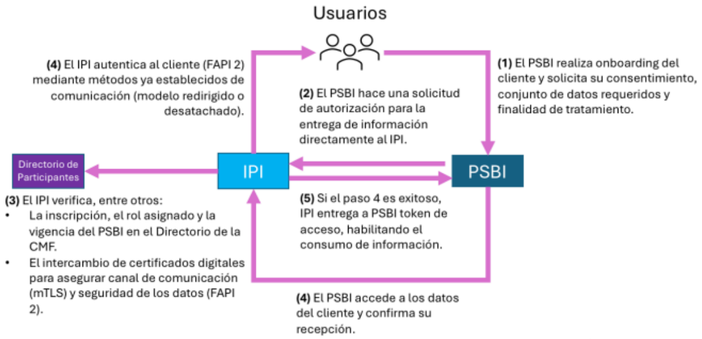
Consentimiento

A partir del **Consentimiento otorgado por el Cliente** tanto a la PSBI como a la IPI es que se establecerá una **comunicación entre la PSBI y la IPI** por donde la **información será compartida**

Propuesta UAI

- ✓ El consentimiento es **generado en la PSB, y queda en la IPI o IPC en modo readonly**
- ✓ 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
- ✓ En términos de plazos y vigencia de los consentimientos, estos **deben estar ligados a la finalidad**. Se proponen plazos fijos que no pueden ser modificados por el usuario, pero si renovarse (única vez, 7 días, 1 mes, 3 meses, 6 meses 12 meses
- ✓ **No se utilizará el refresh token**
- ✓ Se proponen **los principios de usabilidad de Nielsen** y los lineamientos para una experiencia inclusiva son los entregados por las pautas de accesibilidad para el contenido web (WCGA)
- ✓ Se propone un listado de finalidades estándar que sea regulado por la CMF
- ✓ Debe existir un tablero de control con la lista del consentimiento
- ✓ Los errores entregados deben tener su transcripción a lenguaje natural (ver página 71)
- ✓ Finanzas embebidas (servicios financieros que pueden ser presentados por empresas que no se encuentren dentro del SFA) (Pendiente)
- ✓ Mock up flujo de consentimiento

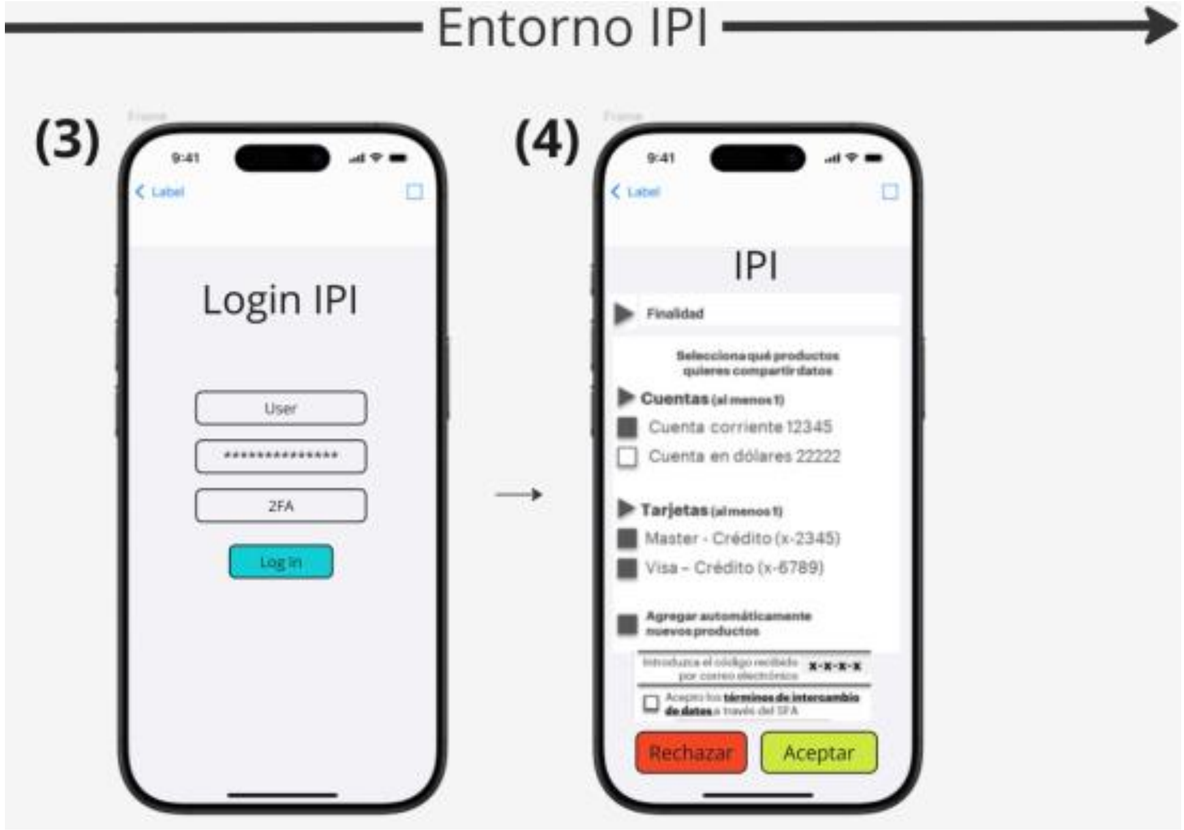
8.1 Flujo y consistencia/cumplimiento FAPI 2.0



Postura AACH

Como Asociación estamos de acuerdo con la mayoría de los puntos, sin embargo, faltan los puntos de segundo factor de autorización y finanzas embebidas

Consentimiento



1 El usuario se autentica en el PSBI
2 PSBI solicita consentimiento mediante onboarding

3 Usuario se autentica en la IPI
4 Usuario selecciona los productos y autoriza el uso de estos

ASOCIACION DE ASEGURADORES DE CHILE A.G.

Comentarios Post Entregable Etapa 1

Octubre / 2024

COMISIÓN
PARA EL MERCADO
FINANCIERO

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

Resultados Temario Etapa 1

FinteChile

Octubre 2024

www.fintechile.org

GT Infraestructura

Posiciones Presentadas

Posición	Argumento
1	• Consideramos que comparar el Directorio con una cámara de pago **en cuanto a continuidad operacional** es inapropiado, ya que el Directorio no forma parte de los flujos transaccionales. • Expresamos nuestro **desacuerdo con la idea de detener el SFA ante una "falla del API + web-hook y mecanismo de contingencia"**. **Faltan definiciones claras** sobre qué constituye una falla y cómo se gestionaría. • Por último, **también solicitamos más detalles sobre las experiencias locales y regionales que sugieren que el uso de MISP es ineficaz para compartir información sobre incidentes.**
2	• Supone un grave error entender que uptime exigido al mecanismo principal implique que el **mecanismo alternativo tenga alcance "acotado".** Primero porque no hay garantías que al comienzo del sistema se cumpla el uptime exigido. Segundo, porque en la industria la disponibilidad se juzga por su complemento (la indisponibilidad). Ejemplo: 99.5% es el doble de exigente que 99% (0.5% es la mitad de 1%, en cuanto a indisponibilidad). • A nuestro juicio, la propuesta del EdS de **esperar hasta 15 minutos para que el mecanismo alternativo opere merma severamente capacidad del mecanismo alternativo de complementar al mecanismo principal**. Especialmente bajo el entendido (expresado también por representantes de otros gremios) de que en un comienzo es improbable que el mecanismo principal alcance el uptime exigido por la CMF en dicho mecanismo principal

FinteChile

Posiciones

1 **Incidencias, comunicaciones y disponibilidad del Directorio:**
No adherimos y mantenemos nuestra posición presentada en los GT

2 **Mecanismos alternativos:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Medios

Posiciones Presentadas

Posición	Argumento
1	• Mantenemos la posición de **unificar los endpoints para Persona Natural y Persona Jurídica, siempre que sea posible.** • Para el caso del enrolamiento, si bien hay algunos campos que solo existen para cierto tipo de cliente, no son muchos como para hacer una separación PN y PJ. • La lista de APIs propuestas es: customers (enrolamiento), accounts (cuentas), credit-cards (tarjeta de crédito), loans (créditos), insurances (seguros) y consents (consentimientos).
2	• **Tipo de páginación:** Cambiamos de opinión y nos adherimos a la utilización de Offsets siempre y cuando los recursos vengan ordenados y que existan filtros de fecha en las APIs que permitan hacer búsquedas eficientes (before_date, after_date). • **Tamaño de página**: Page-size debería ser un rango entre 1 y el tamaño máximo de página. No existe una mejora en rendimiento en tener opciones fijas (25, 50 y 100) y agrega lógica innecesaria a la especificación de la API. Además, el tamaño máximo de página debe ser mayor a 100. • **Sistema de ordenación:** Se debe respetar el orden de creación de los recursos en la API (registros inmutables). Si se insertan registros nuevos entremedio, la paginación se volverá impredecible. Si no se sigue esta práctica, se tendrá que recorrer el end-point completo más de una vez por cada registro nuevo que recibido, lo que hará el intercambio de información ineficiente tanto para las IPIs como PSBI. Esto se vuelve más crítico conforme el N de recursos que retorna un end-points aumenta (ej: cartolas de movimientos bancarios).

FinteChile

Posiciones

1 **Lista de APIs y nomenclatura de Endpoints:**
No adherimos y mantenemos nuestra posición presentada en los GT

2 **Paginación (se actualizaría la propuesta Etapa 0):**
No adherimos y tenemos una posición nueva

3 **SLAs (TPM/TPS):**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Medios

Posiciones Presentadas

Posición	Argumento
3	• Para TPM/TPS parece razonable implementación de una matriz de TPM y TPS, **diferenciando estos valores por tamaño de institución (n de usuarios) y por endpoint**. • El TPM y TPS inicial es de relevancia, pero lo que realmente asegurará la estabilidad del sistema es contar con **un mecanismo adecuado y claro para las IPIs de ajuste de límites**. Tomando la experiencia comparada de Brasil y ajustando sus TPS y TPM, se propone una capacidad mínima inicial de 25 TPS por IPI y 180 TPM, con un mecanismo automático de ajuste que incrementa el TPS en bloques de 25 cuando se supere el 80% del límite vigente durante más del 10% del tiempo semanal.

FinteChile

Posiciones

1 **Lista de APIs y nomenclatura de Endpoints:**
No adherimos y mantenemos nuestra posición presentada en los GT

2 **Paginación (se actualizaría la propuesta Etapa 0):**
No adherimos y tenemos una posición nueva

3 **SLAs (TPM/TPS):**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Seguridad

Posiciones Presentadas

Posición	Argumento
1	· Adherimos al uso de **Message Signing** cuando se require no repudio que pruebe que alguien los envió.
2	· Celebramos la **flexibilidad del equipo de soporte** para retomar el trabajo sobre **7591 y RFC 7592**, que describen los protocolos de **Dynamic Client Registration** y Dynamic Client Registration Management Protocol. Adoptar estos estándares públicos evitará demoras y costos adicionales, mientras que desarrollar un protocolo ad-hoc introduce riesgos. Además, estos estándares están alineados con las normativas de FAPI 2.0 y su análisis de seguridad, lo que los hace cruciales para futuras implementaciones sin requerir trabajos adicionales de adaptación.
3	· Adherimos al uso exclusivo de mTLS.
4	· Nos preocupa que **refresh tokens** no deberian rotar ya que esto generaría más problemas operativos que beneficios en términos de seguridad.Eso de acuerdo a lo recomendado por FAPI 2.0.
5	· Adherimos a que la estructura del **reporte de incidentes** siga los estándares de ISO 27.035 y NIST 800-6, abarcando información básica, cronología, sistemas afectados, y el impacto. Además, se sugiere utilizar plataformas como RIO 2.0 con workflow de reporte y MISP para eventos de ciberseguridad, como una herramienta de intercambio de información sobre amenazas y ataques, sin depender de la CMF.

FinteChile

Posiciones

1. **FAPI message signing:** Adherimos
2. **RFCs a utilizar:** Retomemos DCR
3. **Uso de mTLS y DPoP:** Adherimos
4. **Uso de rotación de refresh token:** Ojo con recomendaciones FAPI 2
5. **Reporte de incidentes:** Adherimos

GT Seguridad

Posiciones Presentadas

Posición	Argumento
1	· Adherimos al uso de **Message Signing** cuando se require no repudio que pruebe que alguien los envió.
	· Celebramos la **flexibilidad del equipo de soporte** para retomar el trabajo sobre **7591 y RFC 7592**, que describen los protocolos de **Dynamic Client Registration** y Dynamic Client Registration Management Protocol. Adoptar estos estándares públicos evitará

FinteChile

Posiciones

1. **FAPI message signing:** Adherimos
2. **RFCs a utilizar:** Retomemos DCR
3. **Uso de mTLS y DPoP:** Adherimos
4. **Uso de rotación de refresh token:** Ojo con recomendaciones FAPI 2

NOTE 2: The use of refresh token rotation does not provide security benefits when used with confidential clients and sender-constrained access tokens. This specification prohibits the use of refresh token rotation for security reasons as it causes user experience degradation and operational issues whenever the client fails to store or receive the new refresh token and has no option to retry.

However, as refresh token rotation may be required from time to time for infrastructure migration or similar extraordinary circumstances, this specification allows it, provided that authorization servers offer clients the time-limited option to retry with the old refresh token in case of failure. Implementers need to consider a secure mechanism for clients to recover from a loss of a new refresh token on issue. The details of this

GT UX

Posiciones Presentadas

Posición	Argumento
1	• **Las finanzas embebidas no están prohibidas explícitamente y por lo tanto, están permitidas**. Al no ser consideradas en los manuales técnicos, están pasan a ser reguladas por medio de la **ley 19.628 de protección de datos** por ejemplo. • Si las finanzas embebidas fueran incluidas en los manuales técnicos se podría, con poco esfuerzo, mejorar mucho la experiencia de usuario.
2	• La **selección de productos <u>(granularidad de cuentas) debiera ser opcional</u>, provista por el PSBI** (que de manera clara debe informar al usuario por qué se solicita acceso granular a cuentas o, al contrario, se solicita de manera <u>no granular</u>)
3	• Habríamos sido el primer país en pedir ARC en dos flujos consecutivos (4 elementos de autenticación desde la perspectiva del usuario). Ya nos parece poco justificado usar ARC en flujos no relacionados en pagos (en Europa, donde nace el concepto de SCA/ARC, **existen waivers que eximen de SCA incluso para flujos de pagos, sujeto al apropiado análisis de riesgos**). Para datos no se debiera exigir ARC. Al exigirlo no se está respetando la paridad en entre canales.
4	• **La Ley no delega en las IPIs la tutela de que sus eventuales competidores estén cumpliendo adecuadamente con las finalidades consentidas por las personas.** La propuesta del EdS nos parece que va en contra de la letra o al menos el sentido de la norma. **Establecer un listado finito de finalidades implica una limitación al derecho a emprender** y al objetivo de innovación que se persigue con la Ley.
5	• Dado que la Ley encarga a los PSBIs la autenticación y consentimiento en cada autorización y que las IPIs no deben hacer validaciones sobre las finalidades, no hace sentido que al tratarse de un nuevo consentimiento que sólo cambia la finalidad, el PSBI esté obligado a elegir como mecanismo el paso por la PSBI.

FinteChile

Posiciones

1. **Finanzas Embebidas:**
   No adherimos y tenemos una posición nueva
2. **Selección de Productos (IPI o PSBI):**
   Valoramos ajustes pero hay que seguir con mucho foco en la UX
3. **Autenticación reforzada en PSBI:**
   Habría sido escandaloso incluirla. Ya es un exceso ARC en datos.
4. **Finalidad:**
   No adherimos y tenemos una posición nueva
5. **Cambios de Finalidad:**
   No adherimos y tenemos una posición nueva

“Que los datos sobre los que versa el consentimiento y vigencia de éste sean los estrictamente necesarios para la finalidad respectiva, circunstancia que <u>el PSBI o PSIP deberá acreditar cuando ello sea requerido por la Comisión</u> en el marco de sus procesos de fiscalización, <u>no correspondiendo a la IPI o IPC pronunciarse a ese respecto</u>”
— NCG 514

Temas a Profundizar: Énfasis en temas de la etapa 1

- **UX:**
  Mockups para evaluar fricción: Es esencial traducir las propuestas a mockups para evaluar la fricción que podrían introducir en la experiencia del usuario, asegurando la comparabilidad y coherencia en los flujos de interacción.

- **Seguridad:**
  Definir parámetros de seguridad específicos: Es necesario detallar parámetros como la duración de los tokens, los scopes, y los mecanismos de cifrado y firmado, para garantizar la seguridad del sistema y la protección de los datos.

- **Infraestructura:**
  Desarrollo del Mecanismo Alternativo:
  Profundizar en la implementación técnica de un Mecanismo Alternativo eficiente, que funcione de manera robusta y esté alineado con el modelo europeo (PSD2).

- **APIs:**
  Consistencia en el uso de offsets: Afinar la descripción técnica de los offsets es clave para garantizar la consistencia en el intercambio de datos y evitar problemas de integridad en el sistema.

Temas Estratégicos

- **Consentimiento:**

Nos estamos alejando en los GTs de lo descrito en la ley y en la norma, a juicio nuestro y también de nuestro equipo legal. El encasillamiento de la finalidades y el intento de limitar conjunto de datos a dichas finalidades son el ejemplo más evidente, más no el único.

- **Adopción del Sistema:**

Invitamos a todos los miembros del Foro, CMF y del EdS a **recordar que la participación de PSBIs en el sistema es opcional**.

Es decir, si creamos un SFA que en el aspecto datos no cumpla con métricas comparables con otros mecanismos (sujetos exclusivamente a ley de protección de datos) en cuanto a **conversión, experiencia de usuario y completitud/calidad de datos**, habremos invertido cuantiosos recursos en un sistema que tendrá limitado uso.

Esto lo conectamos muy fuertemente con nuestras apreciaciones en UX y en Finanzas Embebidas, en los que **queremos aportar para crear un SFA exitoso en su uso.**

COMISIÓN
PARA EL MERCADO
FINANCIERO

Asociación Gremial de la Industria del Retail Financiero A.G. - Retail Financiero A.G.

Asociación
Retail
Financiero

REVISIÓN DE ARF AL DOCUMENTO

"Entregable Etapa 1: Información Persona Natural e información pública"

VERSIÓN 0.1.1 DEL EQUIPO SOPORTE UAI

Santiago, viernes 25 de Octubre de 2024

Comentario General

De acuerdo con la mayoría de las propuestas y recomendaciones

- Impacto económico de las exigencias tecnologícas.

Asociación Retail Financiero

Punto 4. Directorio y Módulo de Comunicaciones

4.4 Módulo de Comunicaciones.

De acuerdo con los 3 components: APIs del Directorio; Webfinger para difundir información no crítica y Canal de comunicación alternativa.

4.5 Registro Dinámico de Clientes.

De acuerdo con su implementación, pero expectante de cómo se realizaría éste.

Punto 5. Intercambio de Información

5.2.2 Definición de API endpoints para información persona natural

- De acuerdo en términos generales, pero con la misma alerta sobre manejo de información transaccional (movimientos) con excesivo detalle (GET /accounts/{accountID}/transactions; GET /creditcard-accounts/{creditcardaccountID}/transactions).

5.2.3 Paginación

- Proponíamos usar "Cursor", pero estamos de acuerdo en una primera fase usar Offset. (ojo con el volumen de datos)
- También es fundamental registros ordenados por timestamp.

5.4 SLAs de las APIs

- Estamos de acuerdo con utilizar una "*matriz de **TPM y TPS**, diferenciando estos valores **por tamaño de institución** y por endpoint*". Realizaremos una revisión interna si los parámetros iniciales definidos son adecuados en nuestro gremio (valor default: 10 TPS (de una IPI a todos los PSBI) y 60 TPM (de una IPI a cada PSBI)).

Punto 5. Intercambio de Información

5.5 Mecanismos alternativos

- De acuerdo en que el mecanismo alternativo (por replica u otro) debe resolverlo cada IPI, con aprobación de la CMF. Esto porque tienen importantes implicancias en costos de implementación y operación.

- No al auto webscraping.

Artículo 16.- Objetivos y Principios del Sistema de Finanzas Abiertas. Con el objetivo de promover la competencia, innovación e inclusión en el sistema financiero, el presente título establece las reglas y principios básicos para la implementación de un sistema de finanzas abiertas, en adelante, "Sistema de Finanzas Abiertas" o "Sistema", que permita el intercambio entre distintos prestadores de servicios de información de clientes financieros que hayan consentido expresamente en ello y otros tipos de datos señalados en el artículo siguiente, a través de interfaces de acceso remoto y automatizado que permitan una interconexión y comunicación directa entre las instituciones participantes del Sistema, bajo adecuados estándares de seguridad y sujeto al cumplimiento de las exigencias y condiciones establecidas en esta ley y la normativa que dicte la Comisión, en las materias que se señalan al efecto.

El Sistema de Finanzas Abiertas resultará aplicable a las instituciones, productos y servicios financieros, tipos de datos y servicios que se indican en los artículos siguientes y en los términos y condiciones que determine la normativa que dicte al efecto la Comisión.

En el cumplimiento de sus deberes y obligaciones, las instituciones que participen en el Sistema de Finanzas Abiertas deberán observar los principios de proporcionalidad, calidad, transparencia e información al cliente, seguridad y privacidad de los datos, trato no discriminatorio e interoperabilidad entre instituciones participantes.

Asociación Retail Financiero

Punto 6. Requerimientos de Seguridad

6.1 Perfil Financiero de Seguridad

- De acuerdo con el requisito perfil de seguridad FAPI 2.0, aunque volvemos a adv
- Entendiendo que en la Etapa 1 no se volvió a discutir si este requisito aplica también al Directorio, creemos que si debiera serle exigible.

6.2 Certificados

- Aunque proponíamos se debiera utilizarse la institucionalidad legal y técnica actualmente existente en Chile y no innovar en esta materia (Certificados de FEA para los representantes legales de los Participantes), aceptamos el uso de Certificados EV en los términos descritos en el documento.

Punto 7. Comunicación y Gestión de Incidentes de Seguridad

- De acuerdo en utilizar una Plataforma de Intercambio de Información sobre Malware (MISP) para facilitar el intercambio de información sobre amenazas de seguridad.

Asociación Retail Financiero

COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Sesión 18
Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Octubre 2024