



Regulador y Supervisor Financiero de Chile

Sesión 16

Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Agosto 2024

Agenda

01

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

02

Consideraciones para la presente sesión del Grupo Consultivo

03

Presentación EdS: Entregable Etapa 0 y avances Etapa 1

04

Presentaciones Miembros GC: posiciones sobre entregable Etapa 0

Agenda

01

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

02

Consideraciones para la presente sesión del Grupo Consultivo

03

Presentación EdS: Entregable Etapa 0 y avances Etapa 1

04

Presentaciones Miembros GC: posiciones sobre entregable Etapa 0

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

- Se informa que el **Sr. Tomás Campero renunció a su cargo** de representante titular de Cajas de Chile A.G en el Grupo Consultivo del Foro del SFA con fecha 28 de agosto de 2024.
- Por lo anterior, **los nuevos representantes de Cajas de Chile A.G en el Grupo Consultivo** corresponden a las siguientes personas:
 - Sr. **Christian Acuña**, en calidad de representante titular.
 - Sr. **Emilio Davis**, en calidad de representante suplente.
- Por otra parte, se informa que, en la presente sesión, participan los siguientes expertos técnicos:

Asociación Gremial / Entidad	Nombre	Cargo
Retail Financiero A.G.	Carlos Orellana	Ingeniero Civil Informático
BancoEstado	Eduardo Concha	Gerente de Arquitectura Tecnológica y Desarrollos CORE
COOPERA	Sergio Vergara	Subgerente de Arquitectura

Agenda

01

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

02

Consideraciones para la presente sesión del Grupo Consultivo

03

Presentación EdS: Entregable Etapa 0 y avances Etapa 1

04

Presentaciones Miembros GC: posiciones sobre entregable Etapa 0

Consideraciones para la presente sesión del GC

- La presente sesión del Grupo Consultivo tiene por propósito **comentar el entregable de la Etapa 0** 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.

Agenda

01

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

02

Consideraciones para la presente sesión del Grupo Consultivo

03


Presentación EdS: Entregable Etapa 0 y avances Etapa 1

04

Presentaciones Miembros GC: posiciones sobre entregable Etapa 0

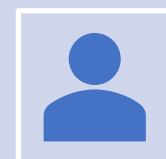
Dinámica de la reunión

- 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 0 (15 mn)**
 - Se efectúan las **presentaciones por los miembros del GC**, por orden de recepción de las mismas:
 - **10mn** para presentación
 - **5mn** 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 5 de septiembre.**



Entrega Etapa 0
Sistema Finanzas Abiertas
Grupo Consultivo 29 de agosto

Se distribuyó entregable Etapa 0 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:

Flujo de consulta de información de Persona Jurídica* + Mecanismo alternativo



Etapa 3:

Monitoreo + Plan de Prueba (Onboarding) + Gestión posterior al consentimiento (revocación, consultas, etc.) + Portal Web



Etapa 4:

Iniciación de pagos

(Fase 2)

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

Se distribuyó primer documento, correspondiente a Etapa 0

- Documento consideró: la NCG, antecedentes del Directorio presentados por la CMF, reuniones durante el período "piloto", presentaciones de los GT posteriores a la publicación de la NCG (reuniones del 25 de julio), 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. Para ello se utilizaron recuadros para señalar los puntos en los que el EdS generó propuestas, junto a las posiciones de los participantes de los GT y sus debidas argumentaciones.
- Los anexos 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 y la conclusión. Estos dos últimos enfocados en el proceso metodológico.

02

El cuerpo con con las dependencias externas al SFA, aspectos técnicos de las APIs que operarán para la información de Términos y Condiciones y Canales de Atención, y los requerimientos de Seguridad.

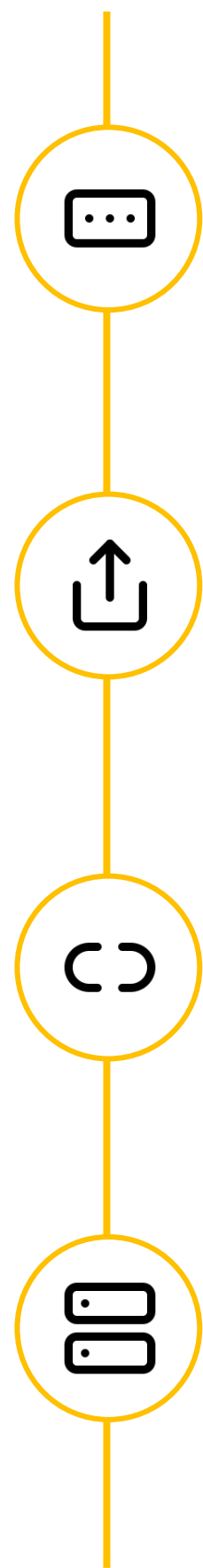
03

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.

04

Finalmente, se incluye un anexo con las minutas de todas las reuniones de los GT, así como las presentaciones de cada participante.

Dependencias Externas al SFA



Validación de Participantes

El Directorio valida a los participantes del SFA para interacciones API, asegurando la autenticidad y seguridad de las comunicaciones.

Comunicación de Cambios

Cambios en el Directorio se comunican para actualizar copias locales, manteniendo la coherencia y actualización de datos.

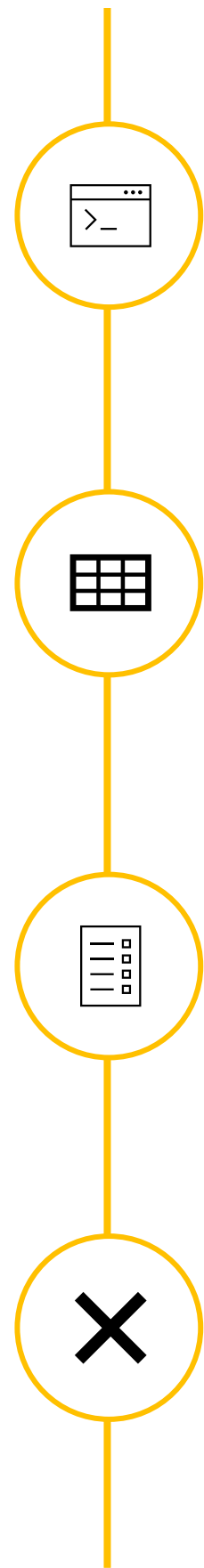
Desacoplamiento del Directorio

El desacoplamiento del Directorio es crucial para no afectar el rendimiento del sistema, permitiendo operaciones independientes.

Estándares de Seguridad y Continuidad en SFA

Se comenzó a abordar el tratamiento de incidentes operacionales y de ciberseguridad. Este es un tema que deberá completarse en la siguiente etapa.

Intercambio de Información en el SFA



Endpoints

Tres APIs sin separación de endpoints para PN y PJ, manteniendo el formato internacional de escritura de los endpoints.

Diccionario de datos

El diccionario de datos basado en estándares internacionales, lo cual facilita la interoperabilidad y el análisis de la información.

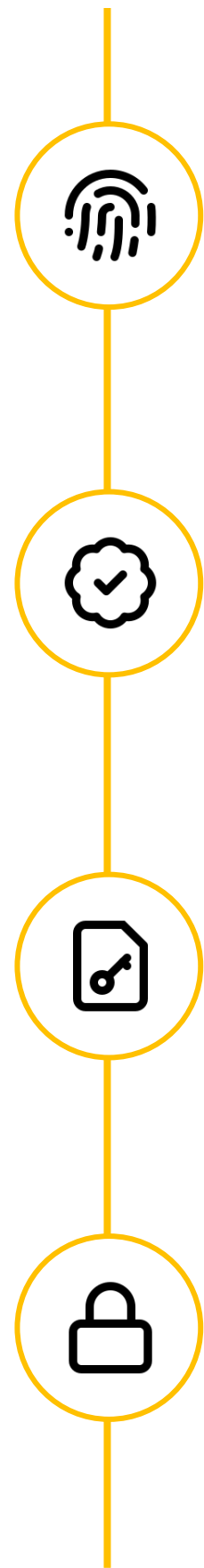
Paginación

Paginación por offset debido a los costos de la implementación por cursor. Se deber volver a visitar este tema para los casos de uso con mucha cantidad de datos.

Códigos de error

Utilización del estándar RFC2616 y se sugiere adherir en una etapa posterior al estándar RFC9457, que permite envío de más información sobre los errores.

Requerimientos de Seguridad del SFA



Perfil de Seguridad FAPI 2.0

El SFA se basa en el perfil financiero de seguridad FAPI 2.0 (NCG 514), proporcionando un marco robusto para APIs financieras.

Certificados Digitales

Uso obligatorio de certificados emitidos por una Autoridad Certificadora confiable, cumpliendo con la norma.

Cifrado de Datos en Tránsito

Se requiere una suite de cifrado de al menos 128 bits para proteger la información en tránsito.

Administración de Logs

Garantizar el no repudio registrando todas las acciones y limitando el acceso a personal autorizado.

Estado de la Etapa 0



Presentación visión general

Se realizó una reunión para revisar las propuestas consolidadas por el equipo UAI con la visión general, técnica y los temas a votar.

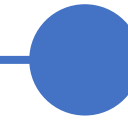
Propuesta temas a revisión de Etapa 0



Posición de Temas

Cada gremio tuvo una semana para manifestar su posición sobre los temas propuestos.

Resultados de las posiciones
Entregable Etapa 0

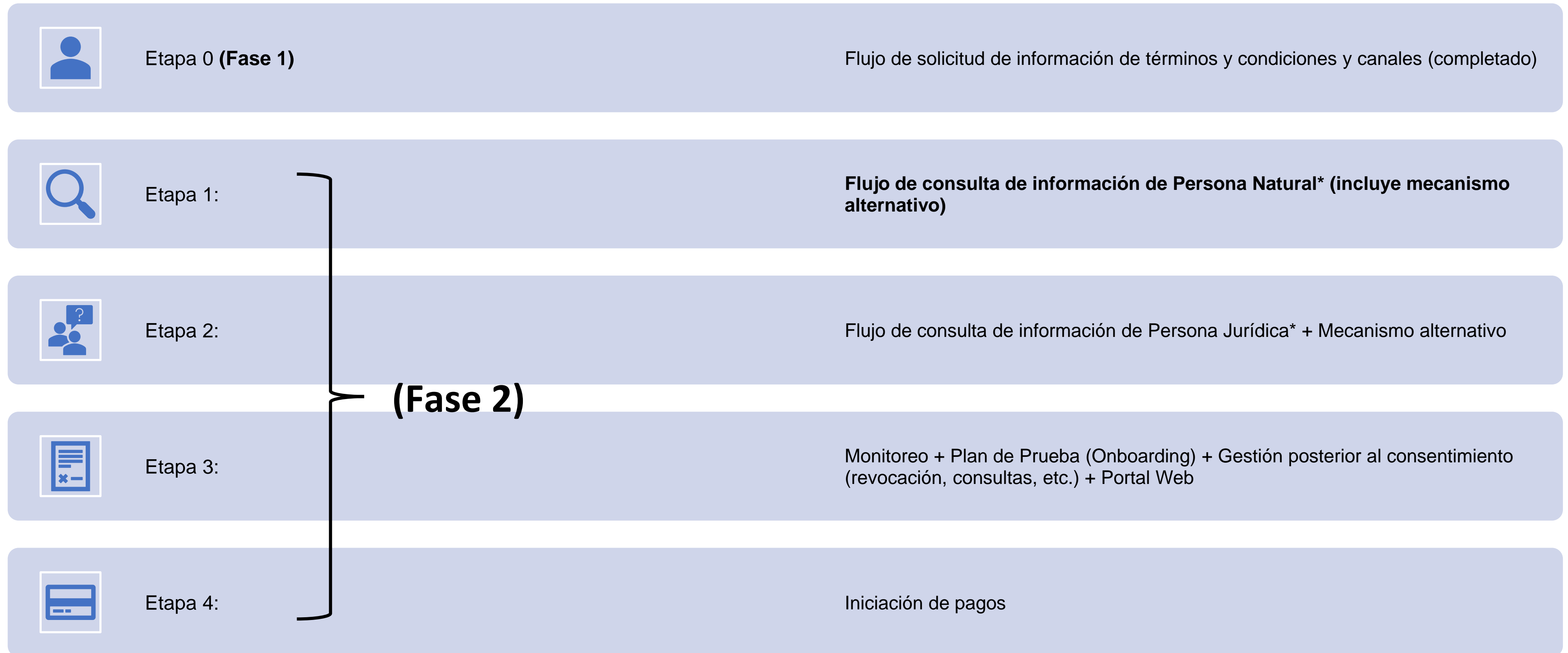


Entrega a Grupo Consultivo

Se entregó el documento de la Etapa 0, y en reunión del Grupo Consultivo se entregarán comentarios de parte de todos los participantes.

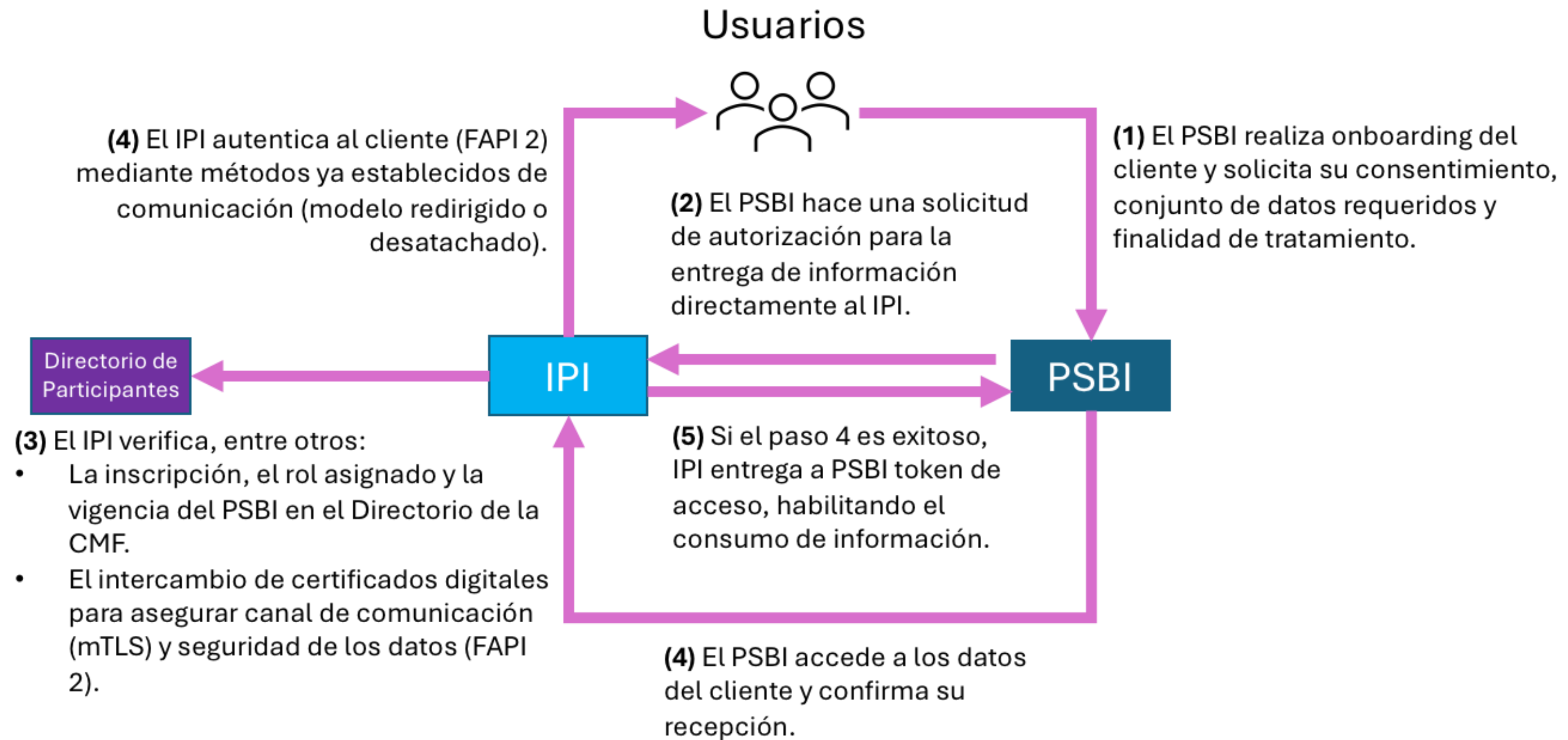
Comentarios de parte de los participantes del Grupo Consultivo

Comenzó proceso de Etapa 1 con los GT



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

Flujo de consulta persona natural



Comenzó el trabajo de la Etapa 1

- El día 22 de agosto los distintos participantes del SFA dieron el kickoff a la Etapa 1, relacionada con flujos de información para personas naturales. Se incorporaron temáticas de consentimiento y el grupo UX tuvo participación similar al resto.
- Luego de una dinámica de priorización a nivel de cada GT, se preparó un temario unificado para el ciclo completo de la Etapa 1, el que fue distribuido el 26 de agosto.
- Las reuniones comenzarán el miércoles 4 y jueves 5 de septiembre:
 - 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.

Síntesis de los temas que se tratarán en los GT

GT de Medios de Intercambio de Información (APIs)

- Revisión de la lista de APIs del caso de uso y revisión de la nomenclatura de los endpoints.
- Diagrama de Flujos de APIs para consentimiento
- Paginación
- Arquitectura de APIs
- SLAs de las APIs (Revisor: GT Infraestructura)
- Máquina de estados (APIs)
- Mecanismos alternativos (Revisor: GT Infraestructura)

GT de Seguridad, Perfiles y Autenticación

- Elementos particulares de implementación de FAPI 2.0 + Perfil de seguridad
- Flujo de autenticación y autorización del usuario+Evidencia y confirmación de autenticación del usuario
- Encriptación y firma/Certificados digitales (integración)
- Implementación de estándares de seguridad de información
- Reporte de incidentes (Revisor: GT Infraestructura)

Síntesis de los temas que se tratarán en los GT

GT de Infraestructura

- Módulo de comunicaciones.
- Registro de clientes (DCR)
- Reporte de performance (disponibilidad, tiempo de respuesta, timeouts, límites de tráfico, entre otros)
- Mecanismos alternativos (Revisor: GT APIs)
- Desarrollo gobierno directorio (Revisor GT Seguridad)
- Máquina de estados (APIs)
- Mecanismos alternativos (Revisor: GT Infraestructura)

GT de UX

- Experiencia del consentimiento (en todas las etapas)
- Usabilidad (Revisor: GT Seguridad)
- Especificaciones y Diagrama de flujo para consentimiento (Revisores GT APIs, Seguridad e Infraestructura)
- Mecanismos de agrupación de tipo de información para el consentimiento (Revisor: GT APIs)
- Reporte de incidentes (Revisor: GT Infraestructura)
- Casos de error

Agenda

01

Cambio representante GC (Cajas de Chile A.G) / Expertos técnicos

02

Consideraciones para la presente sesión del Grupo Consultivo

03

Presentación EdS: Entregable Etapa 0 y avances Etapa 1

04

Presentaciones Miembros GC: posiciones sobre entregable Etapa 0

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

Comentarios a entregables Etapa 0

29 de Agosto de 2024

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

- Temas de posición GT Infraestructura
- Temas de posición GT APIs
- Temas de posición GT Seguridad

Tema de posición GT Infraestructura

Contingencia

- **En general de acuerdo.**
- **Discordancias:**
 - **Parece razonable reemplazar cartas firmadas (CISO, Director Ejecutivo) por declaraciones hechas en un portal de la CMF con acceso controlado e identidad validada.**
 - **En el caso de una contingencia de ciberseguridad, incluir a un tercero experto accionado por la CMF podría alargar excesivamente los plazos de reincorporación. Sugerimos actuar con la declaración, respaldada por un tercero experto, del CISO o Director Ejecutivo del participante afectado de solución del problema.**
 - **El tercero experto podría salir de un registro de expertos o contar con una certificación por definir.**
 - **Validar intersecciones de estos requerimientos con la Ley Marco de Ciberseguridad.**

Funcionamiento del Directorio

- **Adherimos.**

Certificados

- **Adherimos.**
- **Observación:**
 - **En la estructura propuesta del directorio se incluyen dos campos de ocurrencia única**
 - cert_ca
 - cert_val
 - **Creemos que el sistema es más resiliente si permite que cada participante tenga más de un certificado validado, y creemos también que se puede incluir en formato X.509 con la cadena de certificación, por lo tanto sugerimos reemplazar esos campos por**
 - **certs: arreglo de certificados X.509**

Continuidad operacional

- **No Adherimos**
 - **Si bien es deseable un alto estándar de certificación de la infraestructura de los participantes, Tier III no es comúnmente utilizado por proveedores de nubes públicas como Google. Sugerimos complementar con otras certificaciones equivalentes que permitan usar nubes como GCP, AWS o Microsoft Azure.**

Tema de posición GT APIs

Diccionarios Técnicos

- **En general de acuerdo.**
- **Discordancias:**
 - **La NCG declara que la definición de las APIs debe usar el estándar ISO 20022, eso quiere decir, que para todos los campos debemos encontrar su nombre en inglés dentro de ese estándar. Los valores de cada campo podrían ser en castellano o en inglés a evaluar en cada caso (ej. Cuenta Corriente)**

Lista de APIs y nomenclatura de Endpoints

- **En general de acuerdo.**
- **Discordancias:**
 - **En el texto que antecede a las definiciones se dice que la separación entre persona natural y jurídica será con un parámetro del tipo query, pero en la tabla se incluye eso en el path de la URL. Creemos que un parámetro del tipo query es la solución correcta, incluyendo un campo que diga el tipo de persona en la respuesta (para cuando se soliciten ambos).**

Paginación

- **En general de acuerdo.**
- **Discordancias:**
 - **Creemos razonable mantener el máximo original de 100 registros por página y no subir a 1.000 como sugiere la última versión de la propuesta.**
 - **Creemos además que es razonable considerar que si una respuesta es paginada, todas las peticiones de esa paginación deben contar como una sola llamada para los efectos de límites y costos.**

Taxonomía de errores

- **Adherimos**

Tema de posición GT Seguridad

Requerimientos de seguridad para el Directorio

- **Adherimos**

Perfil FAPI 2.0

- **Adherimos**

Marco de autenticación mutua

- **Adherimos**

Certificados

- **Adherimos**
 - **Comentario: Nos parece razonable aceptar certificados EV y OV**

Autoridades Certificadoras

- **No Adherimos**
 - **No nos parece necesario que la CMF determine una lista de CAs a utilizar, la certificación del CA/Browser Forum para permitir que una CA emita certificados EV u OV es la certificación más exigente en la actualidad y sostiene los elementos más críticos de la infraestructura de Internet.**

Protección y seguridad de canal de transporte

- **Adherimos**
 - **Comentario:** En el texto que precede la posición se menciona “se propone utilizar una suite de cifrado con un mínimo de 128bits”, creemos que sin hablar de que algoritmo se está refiriendo, esa propuesta no puede ser evaluada correctamente.
 - Nos parece fundamental, desde la perspectiva de rendimiento y seguridad asegurar la utilización de algoritmos modernos (curvas elípticas sobre RSA, TLS1.3 sobre TLS 1.2, etc) con los largos de llaves apropiados para este momento del tiempo. La propuesta original del texto se hacía cargo de esto.

Estándares de Logs

- **No Adherimos**
 - **Nos parece un error la distinción “en línea” y “fuera de línea”. Lo importante es indicar un SLA de acceso rápido de máximo 4 horas durante 3 meses y un SLA de acceso lento, con tiempo máximo de 3 días durante 5 años. Esta distinción es necesaria porque los mecanismos de almacenamiento moderno son mayormente online, cambiando el tiempo de recuperación para poder implementar alternativas más baratas, contra tiempos de entrega más lentos.**

Lista blanca IPs

- **Adherimos**
 - **Comentario: Cada participante debería poder declarar conjuntos de segmentos de red en vez de una sólo IP, esto para compatibilidad con sistemas distribuidos, de alta disponibilidad y en múltiples nubes.**

Implementación RFC7636

- **Adherimos**
 - **Comentario: Si bien en la etapa 0 se utilizará el flujo client-credentials de FAPI 2.0 y por lo tanto PKCE no se utiliza, para las siguientes etapas si se utilizará.**

Cajas de Chile 

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

Resultados

Temario Etapa 0



Índice

- **Posiciones Presentadas** **Página 1..7**
- GT Infraestructura **Página 3**
- GT Medios **Página 5**
- GT Seguridad **Página 6**
- **Temas a Profundizar** **Página 8**



GT Infraestructura

Posiciones Presentadas

Posición	Argumento
1	<ul style="list-style-type: none"> ▪ Funcionamiento del directorio: Más allá de los detalles de implementación (que parecen poco definidos), el modelo corresponde a lo que hemos empujado como directorio ligero que no participa del flujo transaccional y donde cada participante mantiene su copia local.
2	<ul style="list-style-type: none"> • Continuidad Operacional: Los proveedores cloud no suelen certificar sus datacenters con el Uptime Institute. No nos parece conveniente obligar al directorio a estar fuera de dichos proveedores cloud. Nos parece solucionable este punto ampliando el requerimiento, pedir Tier III o alternativamente cloud, ya que estos proveedores alcanzan niveles equiparables de resiliencia a nivel de arquitectura e indicadores similares en la disponibilidad esperada. También podrían rescatarse elementos de la RAN 20-9 y RAN 20-7 para esta definición.
3	<ul style="list-style-type: none"> • Certificados: Adherimos a la premisa de que la información de los roles será específica en el directorio, y no se enviará a través de certificados. Asimismo, certificados enfocados en identificar participantes y certificados independientes de roles.
4	<ul style="list-style-type: none"> • Contingencia: La detención del SFA debe justificarse únicamente por un riesgo sistémico real, no por suposiciones. Se sugiere explorar mecanismos alternativos, como el uso de la plataforma MISP, para notificar incidentes de ciberseguridad si el directorio está temporalmente fuera de línea. Ya está en uso en Chile y con creciente adopción. Ofrece una solución distribuida que podría evitar riesgos asociados con el directorio. Además, se cuestiona la vinculación entre el tiempo de detención y el tiempo de refresco del sistema, sugiriendo que deberían definirse de manera independiente.

Votación de Posiciones

- 1** **Funcionamiento del Directorio:**
Adherimos
- 2** **Continuidad Operacional:**
No Adherimos y presentamos nueva posición
- 3** **Certificados:**
Adherimos
- 4** **Contingencia:**
No adherimos y tenemos una nueva posición
- 5** **Lista Blanca IPs:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Infraestructura (Cont.)

Posiciones Presentadas

Posición	Argumento
5	<ul style="list-style-type: none"> ▪ Listas Blancas IPs: No se considera que la implementación de una lista blanca de IPs aporte seguridad adicional al esquema actual, que ya utiliza mTLS y FAPI. Esta lista implicaría la introducción de nuevos procesos y un mayor riesgo de fallos, además de requerir mantenimiento adicional. Si se optara por una lista blanca, se sugiere que incluya múltiples IPs por participante en lugar de restringir a una sola, ya que esto limitaría las soluciones en la nube de alta disponibilidad que dependen de múltiples IPs para la redundancia.

Votación de Posiciones

- 1** **Funcionamiento del Directorio:**
Adherimos
- 2** **Continuidad Operacional:**
No Adherimos y presentamos nueva posición
- 3** **Certificados:**
Adherimos
- 4** **Contingencia:**
No adherimos y tenemos una nueva posición
- 5** **Lista Blanca IPs:**
No adherimos y mantenemos nuestra posición presentada en los GT

GT Medios

Posiciones Presentadas

Posición	Argumento
1	<ul style="list-style-type: none"> • Lista de APIs y nomenclatura de Endpoints: Consideramos adecuado el uso de uno solo endpoint para persona natural y jurídica evitando duplicar APIs. Se propone usar un parámetro para el tipo de cliente. También se propone otra nomenclatura.
2	<ul style="list-style-type: none"> • Diccionarios Técnicos: Adherimos a los tipos de datos y diccionarios de datos propuestos.
3	<ul style="list-style-type: none"> • Taxonomía de errores del sistema: Adherimos al estándar RFC7807 (HTTP/1.1) y RFC9457 (Problem Details for HTTP APIs) sugeridos.
4	<ul style="list-style-type: none"> • Paginación: El tamaño de página máximo propuesto era de 100 registros, sin embargo, creemos que para grandes búsquedas históricas deberían poder soportarse páginas de tamaño aun mayor y así reducir el número de peticiones. Para el tipo de paginación nuestra recomendación es el uso de cursores. • Respecto al orden de los registros no se debería de aceptar listas desordenadas para evitar inconsistencias. • Cursores: Las ventajas de usar cursores frente a OffSets es que se puede aprovechar el índice de la base de datos para obtener una página específica y permite consultar los registros más recientes en endpoints de alto flujo sin que se modifique el contenido de las páginas. Pensado para volúmenes grandes y dinámicos como datos históricos.

Votación de Posiciones

1

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

2

Diccionarios Técnicos:
Adherimos

3

Taxonomía de Errores del Sistema:
Adherimos

4

Paginación:
No adherimos y tenemos una nueva posición

GT Seguridad

Posiciones Presentadas

Posición	Argumento
1	<ul style="list-style-type: none"> ▪ Requerimientos de Seguridad para el Directorio: Se considera que OAuth es suficiente para proteger la comunicación con el directorio, y que una lista blanca de IPs no aportaría seguridad adicional. Además, su implementación añadiría complejidad innecesaria, con la introducción de nuevos procesos y un mayor riesgo de fallos. También implicaría un mantenimiento adicional que podría ser complejo y costoso para los participantes.
2	<ul style="list-style-type: none"> ▪ Perfil FAPI 2.0: Nos adherimos al perfil FAPI 2.0 junto a RFC6749 (OAuth 2.0 Authorization Framework) + RFC8414 (OAuth 2.0 Authorization Server Metadata).
3	<ul style="list-style-type: none"> • Certificados: Adherimos al uso de certificados estándar x.509. Se había propuesto el uso de certificados EV, pero por razones de costos y facilidad a nuevos participantes consideramos válido el uso de OV.
4	<ul style="list-style-type: none"> • Marco de Autenticación Mutua: Adherimos a la posición de usar autenticación mTLS. Uso de RFC8705 (OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens)
5	<ul style="list-style-type: none"> ▪ Autoridades Certificadoras: No estamos de acuerdo en limitar el uso a las certificadoras listadas por el Ministerio de Economía, ya que el resto siguen estándares similares, como los mencionados en la posición.
6	<ul style="list-style-type: none"> ▪ Protección y seguridad de canal de transporte: Adherimos en toda la dimensión presentada.

Votación de Posiciones

- 1** **Requerimientos de Seguridad para el Directorio:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 2** **Perfil FAPI 2.0:**
 Adherimos
- 3** **Certificados:**
 Adherimos
- 4** **Marco de Autenticación Mutua:**
 Adherimos
- 5** **Autoridades Certificadoras:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 6** **Protección y Seguridad de canal de transporte:**
 Adherimos
- 7** **Implementación RFC 7636:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 8** **Estándares de Logs:**
 Adherimos

GT Seguridad (Cont.)

Posiciones Presentadas

Posición	Argumento
7	<ul style="list-style-type: none"> • Implementación RFC 7636 (Proof Key for Code Exchange by OAuth Public Clients): El estándar mencionado se utiliza en un contexto de delegación, en donde hay autorización por parte de usuarios para el acceso a sus datos. Esto no es requerido en el caso de uso propuesto, por lo cual no vemos necesidad de implementación.
8	<ul style="list-style-type: none"> • Estándares: Adherimos, aunque nos surgen dudas sobre los requisitos de custodia y tiempos de recuperación.

Votación de Posiciones

- 1** **Requerimientos de Seguridad para el Directorio:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 2** **Perfil FAPI 2.0:**
 Adherimos
- 3** **Certificados:**
 Adherimos
- 4** **Marco de Autenticación única:**
 Adherimos
- 5** **Autoridades Certificadoras:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 6** **Protección y Seguridad de canal de transporte:**
 Adherimos
- 7** **Implementación RFC 7636:**
 No adherimos y mantenemos nuestra posición presentada en los GT
- 8** **Estándares de Logs:**
 Adherimos

Temas a Profundizar: Foco en Seguridad

Evaluar la lista blanca de IPs como medida de Seguridad

- Entendimiento del riesgo a mitigar que no esté cubierto en FAPI + mTLS.
- Despliegue en proveedores cloud: Base del sistema.
- En despliegues de alta disponibilidad se utilizan múltiples IPs para evitar puntos únicos de fallo (SPOF).
- Las listas blancas implican costos de mantención y demoras en actualización.

Repensar el modelo de seguridad y disponibilidad del directorio

- Revisar la indisponibilidad del SFA. La disponibilidad es parte de la seguridad
- Introducción del rol del MISIP
- Involucrar al grupo de seguridad

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

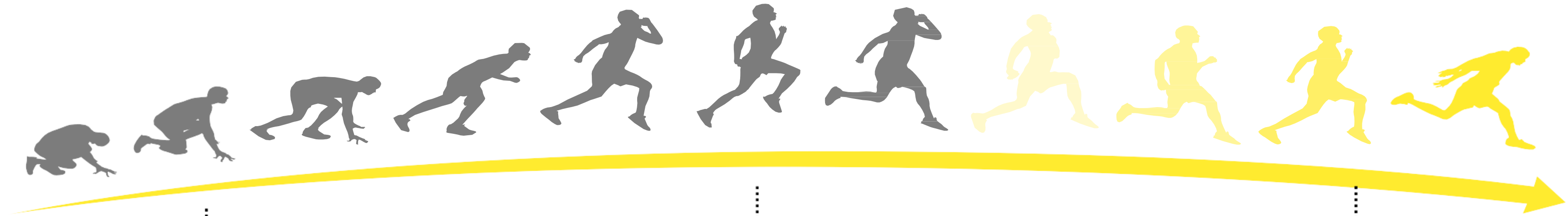


Etapa 0 Grupos técnicos



COOPERA
Cooperativas de Ahorro y Crédito Asociadas

Etapa 0



Etapa 1

Infraestructura

2 sesiones de trabajo

Temas principales

- Funcionamiento del directorio
- Continuidad operacional
- Certificados
- Contingencia
- Lista blanca IPs

Medios de Intercambio de Información

2 sesiones de trabajo

Temas principales

- Lista de APIs y nomenclatura de endpoints
- Diccionarios técnicos
- Taxonomía de errores del sistema
- Paginación

Seguridad, Perfiles y Autenticación

3 sesiones de trabajo

Temas principales

- Requerimientos de seguridad para el directorio
- Perfil FAPI 2.0
- Certificados
- Marco de autenticación mutua
- Autoridades certificadoras
- Protección y seguridad del canal de transporte
- Implementación RFC 7636
- Estándares de Logs

Directorio local

Hacemos énfasis en la propuesta entregada por la CMF en la construcción de un Directorio de participantes al ser este un punto fundamental para el buen funcionamiento del sistema de finanzas abiertas, vemos también oportuna la estrategia de que cada participante posea un directorio local el cual apunta a una mejor experiencia en términos de comunicación y verificación de las conexiones, además del rendimiento en el uso del consumo de las APIs



Aspectos positivos

Participante transversal

Nos parece correcto adicionar un participante en común para los grupos técnicos para tener una visión completa de lo que ocurre en los grupos técnicos

Cambios metodológicos

Basándonos en la experiencia de lo ocurrido en la Etapa 0, consideramos eficientes los cambios metodológicos respecto de realizar una priorización de temáticas, definición previa de los temas a discutir y apoyo transversal entre los distintos grupos, de cara a la etapa 1

Implementación FAPI 2.0

Considerando que se trata de información pública de términos y condiciones y canales de atención no se ve la necesidad de implementar una capa adicional de seguridad como FAPI 2.0, ya que complejiza el desarrollo y aumenta los costos de implementación.



Aspectos tecnológicos clave

Sistema de colaboración

Vemos que es de vital importancia tener un sistema o mecanismos de colaboración entre los participantes para compartir información ante incidentes operacionales o de ciberseguridad con el fin de prevenir y mitigar los daños colaterales.

Directorio de participantes

Creemos que el DP debería cumplir con los mismos estándares de exigencia que deben cumplir todos los participantes del sistema, en términos de disponibilidad y rendimiento.

Directorio local

No se hace mención sobre definiciones y/o lineamientos de implementación del directorio local

Proponemos que se defina lineamientos y/o directrices de implementación para el directorio local

Reportes a la CMF

No queda claro cuáles serán los medios de comunicación o métodos de consumo de los reportes a entregar a la CMF

Proponemos utilizar correo como medio de comunicación

Colaboración entre participantes

No se hace mención sobre mecanismos o plataformas para la colaboración entre los participantes

Proponemos que se utilice alguna plataforma como slack o similar para facilitar la comunicación entre participantes

Estado de las APIs

No se especifican mecanismos para identificar el estado de las APIs de un participante en línea

Proponemos implementar un Health Check de las APIs de cada participante



Aspectos clave pendientes

Costos de implementación

Es importante reducir lo más posible este valor, debido a que existe obligatoriedad de participación en este sistema para ciertas entidades financieras que tienen distintos tamaños en la industria

Monitoreo y supervisión

No queda claro la periodicidad de los procesos de supervisión y monitoreo del sistema por parte de la CMF

Proponemos que se defina la periodicidad y el mecanismo de monitoreo del sistema

Proporcionalidad del sistema

Consideramos que deberíamos tener en cuenta la posibilidad de tener una implementación proporcional a la entidad financiera que se encuentre participando en el sistema. Puede existir el caso de que una entidad financiera reciba una cantidad mínima de llamadas de pedido de información, para la cual no vemos la necesidad de cumplir con cada uno de los estándares solicitados para su ingreso

Proponemos definir estándares de disponibilidad y rendimiento proporcionales a la cantidad de usuarios que posee la institución

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

1. Etapa 0:

1. Paginación: límite de 1000 registros
2. URL Sandbox en directorio
3. Metodología entregas

2. Definiciones:

1. Certificaciones: funcional, seguridad, digital
2. Directorio: plazos para comenzar pruebas
3. Gobierno de datos: calidad, control de finalidad, relación finalidad/datos proporcionales y específica
4. Umbrales: soluciones técnicas para cumplir con lo definido en la norma
5. Servicios centralizados: rol de la CMF para supervisar y autorizar potenciales servicios a centralizar
6. Plazos de las versiones del anexo 3
7. Viabilidad financiera iniciación de pagos

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





REVISIÓN DE ARF AL DOCUMENTO

"ENTREGABLE ETAPA 0: TÉRMINOS Y CONDICIONES Y CANALES DE ATENCIÓN"

VERSIÓN 0.0.1 DEL 4/08/2024 DEL EQUIPO SOPORTE UAI

Santiago, jueves 29 de Agosto de 2024



COMENTARIO GENERAL

- De acuerdo en los principios básicos de arquitectura y funcionamiento del SFA y en particular del Directorio.
- Entendemos que la CMF deberá asignar todos los rrhh y de infraestructura necesarios, para garantizar la disponibilidad y seguridad del Directorio
 - ➔ Certeza jurídica y comercial de este mercado.
- De acuerdo con varias de las propuestas y recomendaciones
- Nos preocupan:
 - Impacto económico
 - Dimensionamiento



PUNTO 3. DEPENDENCIAS EXTERNAS AL SFA

3.1 Servicios brindados por la API del Directorio

Endpoints Críticos: Aunque hay 4 grupos de endpoint, todos muy importantes en la API del Directorio, hay 2 de ellos que permiten obtener información esencial de los participantes, como /participants y /public-keys. La ARF reconoce la importancia de estos endpoints para mantener la integridad de las comunicaciones dentro del SFA.

Recomendación ARF:

- Estos servicios de Directorio (CMF) deben tener al menos la misma disponibilidad exigida a las IPI (uptime del 99.5% o superior)
- De acuerdo con la actualización en 2 vías ante cambios en el Directorio (notificación proactiva a los participantes y Consulta periódica de estos a la CMF), aunque notificación asegurada sería mejor.
- CMF debe: Definir Casos de contingencia (grupo) y determinar el cambio de estado de un Participante.

3.2 Diccionario de datos "Base de datos liviana"

Minimización de Datos: De acuerdo con tener un "diccionario de datos liviano" para asegurar que solo la información crítica es intercambiada (mejores prácticas para reducir la superficie de ataque).

Recomendación ARF: Adherimos a la propuesta del documento, pero sugerimos:

- inicialmente que en la información crítica no sea incluido "rut", "dv" y "name" (ya existe "cmf_id").
- incluir un campo "sfa_status_date" que muestre la fecha-hora en que un Participante cambió de status.
- que CMF implemente mecanismos de auditoría regulares (asegurar que solo se almacene y transmita lo mínimo y datos "críticos").
- De acuerdo con uso de WebFinger, pero compatible con los estándares de seguridad establecidos (HTTPS para las consultas y la validación de las respuestas para prevenir ataques MITM).
- Explorar la posibilidad de agregar autenticación adicional a las consultas WebFinger (info sensible).

3.3 Estándares de Seguridad y Continuidad del Directorio

Infraestructura Resiliente: Adoptar un estándar Tier III para la infraestructura del Directorio es parcialmente adecuada para asegurar la continuidad operativa.

Recomendación ARF: Adherimos parcialmente a esta propuesta.

- Debe tener el estándar de infraestructura crítica que reglamente la ley de ciberseguridad.
- Estrategia híbrida: Aunque Tier III es robusto, se sugiere complementar con soluciones en la nube (recuperación más ágil en caso de fallas graves).
- Definir claramente el RTO (Recovery Time Objective) y RPO (Recovery Point Objective) para el Directorio, (tiempos alineados con necesidades críticas del SFA).
- De acuerdo con la ABIF en el sentido de considerar necesario definir un SLA de al menos 99,5% para los servicios y aplicaciones que serán expuestos a través del Directorio.



4

PUNTO 4. INTERCAMBIO DE INFORMACIÓN

4.1 Diccionario de Datos

Estandarización y Compatibilidad: El documento propone un diccionario de datos y sus tipos (estandarizados) para TYC y Canales de atención, para asegurar la interoperabilidad.

Recomendación ARF: Concordamos con distintas observaciones y además:

- Incorporar un campo "metadata" dentro del diccionario de datos que permita agregar información adicional sin modificar la estructura base del diccionario. Ej: contact_channel (idiomas)
- También estamos de acuerdo con la propuesta de Cajas de Chile de estandarizar todos los nombres de campos en inglés, siguiendo normas internacionales como ISO 20022.
- También creemos que el campo "Tipo" debiera permitir especificar otras plataformas comerciales (Instagram por ejemplo), basado en un principio de neutralidad.
- Usar arrays para manejar listas de productos que pueden tener varias características (product_features).

4.2 API Endpoints y Servicios

4.2.1 Definición de API Endpoints

Estamos de acuerdo con la estructura y estándares definidos para los endpoints API, el uso de mTLS, OAuth 2.0 (particularmente el flujo de credenciales del cliente, para la gestión de accesos y tokens) y OpenAPI para documentar cada endpoint e implementar un sistema de versionado

Recomendación ARF:

- Agregar un endpoint específico para la consulta de estados históricos de productos financieros. Este endpoint permitiría a los participantes acceder a versiones anteriores de los productos, útil para auditorías y para comparaciones históricas.

4.2 API Endpoints y Servicios

4.2.2 Eficiencia y Paginación

Técnica de Paginación: El documento propone varias técnicas de paginación para manejar grandes volúmenes de datos en las consultas API.

Recomendación ARF: Estamos de parcialmente de acuerdo, con algunas consideraciones:

- Control de límites de paginación: Adherimos al establecimiento inicial 100 registros por página, pero creemos que deben ser ajustables según la carga del sistema y las necesidades operativas.
- Paginación basada en cursores: Recomendamos la paginación basada en cursores sobre la "Offset y Limit". Este método es más eficiente en la gestión de grandes volúmenes de datos (particularmente para las etapas siguientes a la Etapa 0).
- Rendimiento: Recomendamos realizar pruebas de estrés y rendimiento regularmente para evaluar cómo las APIs responden bajo diferentes escenarios de carga. Trade off alta transaccionalidad vs no sobredimensionar el sistema.



5

PUNTO 5. REQUERIMIENTOS DE SEGURIDAD

5.1 Perfil financiero de Seguridad

ARF apoya en términos generales la implementación de **FAPI 2.0**, pero le preocupan los costos.

Recomendación ARF: Adherimos a la propuesta del documento, pero sugerimos acento en:

- Consideraciones de Implementación: Sugerimos que se considere ofrecer un enfoque escalonado para la implementación de FAPI 2.0. Esto permitiría a las entidades con menos recursos adoptar primero las partes críticas del estándar, como la autenticación fuerte y la gestión segura de tokens, mientras desarrollan la infraestructura necesaria para cumplir con todos los aspectos de FAPI 2.0 en etapas posteriores.
- Compatibilidad y Escalabilidad: Se establezca pautas para la integración con sistemas existentes, permitiendo a las entidades implementar FAPI 2.0 de manera progresiva y sin interrumpir sus operaciones actuales.
- De acuerdo en que el Directorio deba utilizar los protocolos: OAuth 2.0 Dynamic Client Registration Protocol y OAuth 2.0 Dynamic Client Registration Management.

5.2 Certificados

Certificados: No estamos de acuerdo en que la emisión de certificados para representar a los Participantes en el Directorio, la realicen entidades certificadoras distintas a las PSC acreditadas ante el Ministerio Economía.

Si estamos de acuerdo con el uso de certificados EV para entregar un alto nivel de autenticación (operado por una entidad legítima y confiable) a los sitios que interactúen en el SFA.

Recomendación ARF:

- Aunque estamos de acuerdo con la importancia en el uso de certificados EV (sitios web y servicios), creemos que debiera utilizarse la institucionalidad legal y técnica actualmente existente en Chile y no innovar en esta materia. El uso de Certificados de FEA para los representantes legales de los Participantes debiera ser incorporados al SFA.

5.3 Cifrado

Cifrado de Datos en Tránsito y Reposo: Se establece el uso de cifrado fuerte para proteger los datos tanto en tránsito como en reposo (suite de cifrado con un mínimo de 128bits).

Recomendación ARF: Adherimos a la propuesta de cifrado y estamos de acuerdo con la idea de la ABIF de una revisión y actualización. Evaluar AES-256 para datos muy sensibles..

5.4 Administración de Logs asociados al no repudio

Integridad de los Logs: De acuerdo con la gestión y protección de logs para garantizar el no repudio y la trazabilidad dentro del SFA.

Recomendación ARF:

- Uso de AES-256 en el cifrado de logs y se implemente sellado de tiempo y hash.
- Establecer políticas sobre la retención y eliminación segura de logs (normativas de privacidad y protección de datos).

5.5: Protección y Gestión de la Seguridad

5.5.1 Listas Blancas de Ips

Listas Blancas de IP. La implementación de listas blancas de IPs, es una buena estrategia de seguridad.

Recomendación ARF: Adherimos con algunas recomendaciones:

- Implementar una gestión centralizada para las listas blancas de IPs en el Directorio.
- Compatibles con direcciones IPv6.
- Monitoreo activo, por parte del Directorio, que detecte intentos de acceso no autorizados.

5.5: Protección y Gestión de la Seguridad

5.5.5 Comunicación y Gestión de Incidentes

Gestión de incidentes. De acuerdo con establecer protocolos para la comunicación y gestión de incidentes.

Recomendación ARF: Adherimos con algunas recomendaciones adicionales.

- Plan de comunicación de incidentes (cómo, cuándo y a quién se deben comunicar los incidentes)
- Formar un "Incident Response Team" (IRT).
- Dependiendo de los costos que ello signifique, realizar simulacros para evaluar todo.



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



Proyecto Fintec

Agosto/2024
Cierre Etapa 0
V2.0



Mercado Asegurador

- 65 Compañías de Seguros
- Agrupadas en Compañías de Vida (32), Generales(25), Garantía y Créditos (8)
- Del total de compañías, 35 son de capitales extranjeros y 30 de capitales nacionales
- Multiplicidad de sistemas-core para la operación (historia de M&A, adquisición de carteras, etc.)
- Se especializan por productos específicos, por canales de venta y por segmento: personas y empresas; personas; o empresas

Principales tipos de seguros ofrecidos

Compañía de Vida	Compañía de Generales	Compañías de Garantía y Crédito
<ul style="list-style-type: none">• Seguro de Vida• Seguros de Vida con Ahorro• Seguros con Ahorro Previsional Voluntario (APV - APVC)• Rentas Vitalicias Previsionales• Seguros de Salud• Seguros de Accidentes Personales• Seguro de Invalidez y Supervivencia	<ul style="list-style-type: none">• Seguros de Incendio y Adicionales• Seguro de Ingeniería• Seguro de Transporte• Seguros de Vehículos• SOAP• Seguro de Robo• Seguro Agrícola• Seguro de Responsabilidad Civil• Seguro de Cesantía	<ul style="list-style-type: none">• Seguro de Crédito• Seguro de Garantía (con liquidador, ejecución inmediata)

Avance del Anexo 3 de la NCG-514

Alcance de la Etapa 0

El alcance de este entregable considera la entrega el caso de uso de **consulta de información pública sobre Términos y Condiciones y Canales de Atención**. Este documento fue elaborado en conjunto por la UAI y los gremios participantes del SFA

Mesa Seguridad	Status
Requerimiento de seguridad para el Directorio	No Adhiero
Certificados	No Adhiero
Autoridades certificadoras	No Adhiero
Estándares de Logs	No Adhiero
Perfil FAPI 2.0	Adhiero
Marco de autenticación mutua	Adhiero
Protección y seguridad de canal de transporte	Adhiero
Implementación RFC	Adhiero

Mesa Infraestructura	Status
Funcionamiento del directorio	No Adhiero
Contingencias	No Adhiero
Continuidad operacional	Adhiero
Certificados	Adhiero
Lista blanca IPs	Adhiero

Mesa UX	Status
No fue convocada	N/A

17 temas de posición tratados	11 adhiero
	6 no adhiero

Mesa APIs	Status
Lista de APIs y nomenclatura de Endpoints	Adhiero
Diccionarios técnicos	Adhiero
Taxonomía de errores del sistema	Adhiero
Paginación	Adhiero

Avance del Anexo 3 de la NCG-514

Alcance de la Etapa 0 – No Adhiero

A continuación se detalla los “No Adhiero” por Mesa Técnica:

Mesa Técnica	Tema de Posición	Status
Mesa Seguridad	Requerimiento de seguridad para el Directorio	La CMF debe asegurar la alta disponibilidad del directorio de participantes. La CMF debe garantizar la seguridad perimetral del Directorio de Participantes. El Dashboard debe ser dispuesto a todos los partícipes y en tiempo real
Mesa Seguridad	Certificados	Poseer más de un certificado inscrito debe ser opcional y no una exigencia. Esto por los costos de mantenimiento que implica, y el tiempo que tardaría en efectuarse el cambio de certificado en una contingencia vs la probabilidad que ello ocurra. Cada partícipe debe tener control sobre la vigencia de sus certificados
Mesa Seguridad	Autoridades certificadoras	La ley Marco de Ciberseguridad para la Infraestructura Crítica considera los servicios digitales como servicio esencial (Art. 4 de la Ley), por lo tanto, se hace más necesario que las Autoridad Certificadora se encuentren bajo regulación chilena para efectos de emisión de los Certificados Digitales
Mesa Seguridad	Estándares de Logs	No se debe establecer roles que permitan modificar logs. Se debe asegurar inalterabilidad. Logs en “Caliente” por 90 días (RFC 5424) y Logs en “Frío” por 5 años. Si requerimiento exige log mayor a 90 días, la respuesta debiera ser en 1 mes
Mesa Infraestructura	Funcionamiento del directorio	La actualización y el riesgo de este, no puede ser responsabilidad de las instituciones participantes del sistema (IPI, PSBI), debe existir una herramienta de monitoreo del SFA
Mesa Infraestructura	Contingencias	Debe existir una herramienta de monitoreo autónomo

Preocupaciones de la industria

Comentarios Generales (1/2)

Dentro de la Asociación y habiendo conversado con las compañías queremos compartir las principales preocupaciones para lograr un buen funcionamiento del Sistema de Finanzas Abiertas desde nuestra perspectiva:

Modelo de Gobierno y Supervisión SFA: A la fecha no hay una posición de **cómo será el Modelo de Gobierno de todos los diferentes aspectos que deberán ser orquestados por el SFA en temas relacionados con la creación de las APIs**, cuando será necesario contar con una nueva versión de una API o cómo será abordado el tema cuando se deba actualizar algún standard de los que ya estén definidos.

Centralización: Si bien se ha adecuado la NCG para que los participantes se puedan organizar mejor y puedan coordinarse para plantear la Centralización de algunos servicios entendemos que el Regulador tiene un rol relevante en poder dar un marco para definir que servicios sería más oportuno tener centralizados por las futuras interacciones que tendrá el SFA en el día a día de los Servicios Financieros.

Productos Previsionales: importante tener presente que estos seguros, además de tener una naturaleza previsional y estar regulados en el Decreto Ley N°3.500, son de carácter irrevocable, razón por la cual no contribuyen a fomentar la competencia entre los actores del sistema financiero, y por ende no cumplen con el objetivo del Sistema de Finanzas Abiertas.

Gradualidad: planteada desde los productos a implementar en el SFA. Proponemos iniciar con **productos simples y de alta demanda** para luego avanzar con otros productos de Seguros. En nuestra opinión, sería beneficioso para todo el sistema considerar una incorporación gradual de los productos, comenzando con aquellos más masivos para luego ir incorporando los menos comercializados.

Personas Naturales: consideramos que para los productos relacionados con la industria aseguradora es necesario priorizar en la incorporación a las personas naturales por sobre las personas jurídicas. Esta sería otra forma de gradualidad. Una vez estabilizado Personas Naturales avanzaríamos con las Personas Jurídicas y todas las complejidades que pudieran tener la figura de los Seguros Colectivos y los Seguros Coaseguros por ejemplo.

Productos Banca Assurance: es muy importante confirmar si los productos asociados a la Banca Assurance, Seguro de Desgravamen, de Incendio, asociados a un Crédito de Consumo o Hipotecario serán parte del calendario de implementación del Grupo 1 o bien serán parte del Grupo 2 con el resto de los productos de seguros alcanzados en el Sistema de Finanzas Abiertas.

Preocupaciones de la industria

Comentarios Generales (2/2)

Directorio: se espera que el Directorio cuente con una **robustez relevante y que de confianza a todo el Sistema de Finanzas Abiertas**. Se espera que se le exija las mismas especificaciones técnicas que tendrá cada uno de los participantes que se sume al Sistema de Finanzas Abiertas

Educación financiera: no todos los actores del SFA tienen la misma situación respecto al acceso que sus clientes realizan en sus portales por lo que será muy importante contar proactivamente con un **plan de educación financiera** que permita que todos los clientes gestionen sus accesos de forma proactiva ya que será clave para que puedan otorgar los consentimientos a las PSBI que cada cliente estime oportuno



Proyecto Fintec

Agosto/2024
Cierre Etapa 0
V2.0



Banco del Estado de Chile (BancoEstado)

Entregable Etapa 0: Términos y Condiciones y Canales de Atención

Visión BancoEstado

Implementación SFA

29 de Agosto de 2024

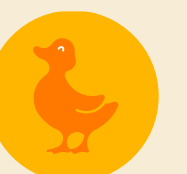
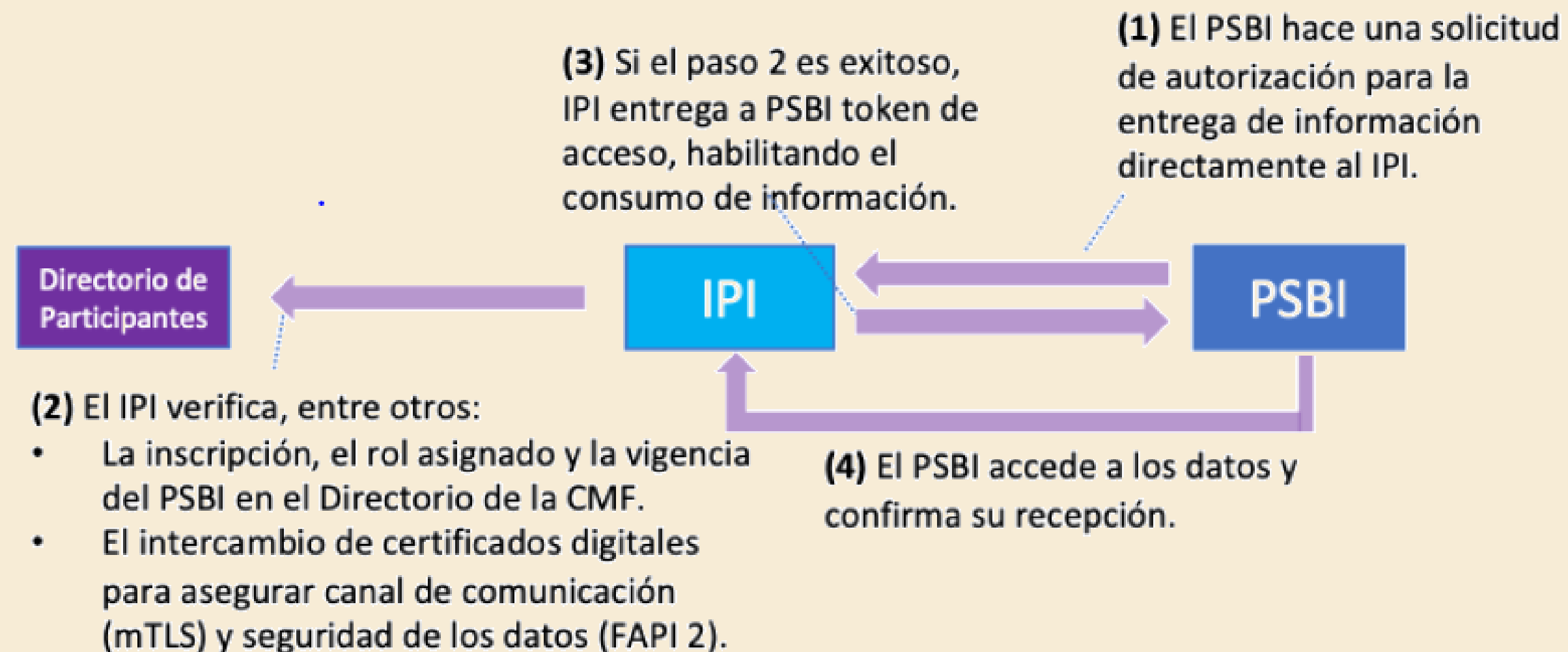


Antecedentes

Caso de uso de consulta de información pública sobre Términos y Condiciones y Canales de Atención

- Primer entregable de los GT para discusión en Grupo Consultivo
- Documento elaborado por el Equipo de Soporte UAI sobre la base de antecedentes entregados por la CMF y el trabajo de los GT en el período de piloto.

Esquema Casos de Uso de Información Pública



Dependencias Externas

Administración del Directorio y flujo de información

Casuísticas de Contingencia

- ❑ Definición por parte de la CMF, así como la definición de un protocolo de actuación.
- ❑ Lo anterior permite clarificar impacto de los posibles estados y responsabilidades.

Funcionamiento del Directorio

- ❑ Asegurar la entrega de la información para garantizar que todas las instituciones actualicen su directorio local.

Certificados

- ❑ Estandarización de la información (un certificado, un participante).

Estándares de seguridad y continuidad operacional

- ❑ Estándares de continuidad operacional y ciberseguridad robustos, y bajo estándares internacionales (Tier III)



Intercambio de información

Alcance, estandarización y formato

Diccionarios técnicos

- ❑ Definición clara del alcance de los campos para el registro de datos

Códigos de error

- ❑ Estandarización de reglas y directrices a nivel de industria

API Endpoints & Servicios

- ❑ Unificación de endpoints ("Canales de atención física" y "Canales de atención remoto")
- ❑ Dependiendo del caso de uso, tratamiento diferenciado o no para PN y PJ
- ❑ Mayor definición relacionada con la paginación



Requerimientos de Seguridad

Perfil financiero, certificados y cifrado

Requerimientos de seguridad para el Directorio

- Requerimientos de seguridad establecidos por FAPI 2.0 en casos de uso de etapas posteriores.
- Para el caso de uso de la Etapa 0, otros mecanismos (OAuth 2.0, mTLS) son suficientes para casos de uso de datos abiertos.

Certificados

- Emisión acotada a compañías certificadas por una entidad local supervisada por la CMF.

Cifrado

- Garantizar suite de encriptación (llave de largo mínimo 128bits)



Otros temas

Visión transversal

Etapa 0 ha buscado especificar APIs de información abierta

- ❑ No vemos necesidad de implementar flujo de consentimiento para datos que no son de propiedad del cliente.

Poderes Persona Natural

- ❑ Abordar con mayor profundidad el flujo de consentimiento de PN en casos especiales: cuentas con tutelaje, bipersonales y poderes.
- ❑ Proponemos un tratamiento simplificado:
 - ✓ Tutelaje, intermediarios y/o mandatarios debieran ser tratados con la misma lógica de PN con poderes operativos y datos personales sensibles no deben ser compartidos, a menos que se autorice de forma explícita
 - ✓ Cuentas bipersonales debieran tratarse con lógica de PJ
- ❑ Revocación de poder y mensajes de error ante poderes no vigentes; requiere estandarizar códigos de error a nivel del sistema.



Gracias



BancoEstado
desde 1855





Regulador y Supervisor Financiero de Chile

Sesión 16

Foro del Sistema de Finanzas Abiertas (FSFA)

Comisión para el Mercado Financiero
Agosto 2024