Alternativas tecnológicas en seguridad desde la Red

iRed - Servicio de gestión de identidad

ACELERAR PARA SER MÁS LÍDERES

Telefónica

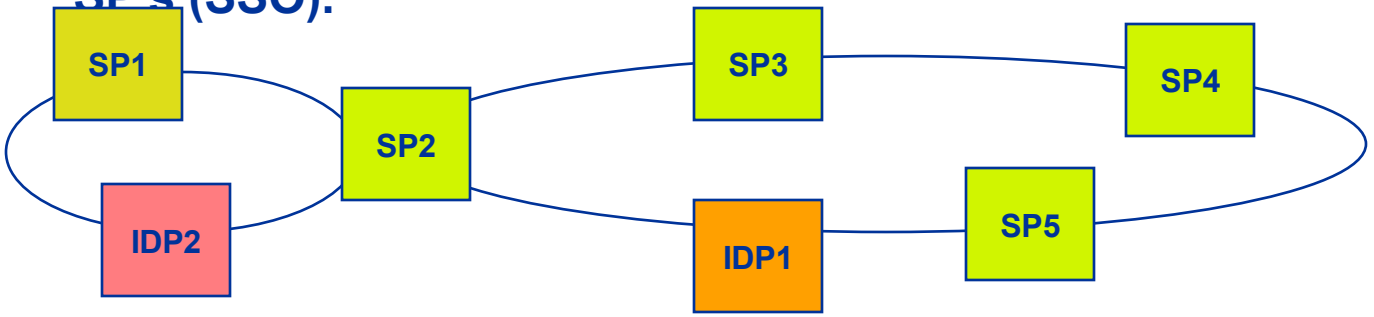
Noviembre 2007

ACELERAR PARA SER MÁS LÍDERES

01 Federación de identidad

La Federación de Identidad **está descrita en el protocolo Liberty, que constituye un estándar. Se basa en la existencia de un círculo de confianza establecido entre proveedores de servicios (SP's) y un proveedor de identidad (IDP).**

- **Los SP's confían en "la gestión de usuarios" que hace el IDP y "mancomunan" esta tarea.**
- **El usuario, siempre que se mueva en el circulo de confianza, sólo se autentica una vez y no necesita recordar las credenciales para acceder a los distintos SP's (SSO).**



La Federación de Identidad se utiliza para poder implementar la autenticación en red, utilizando un protocolo estándar. Este proyecto es un proyecto de autenticación, no de provisión de identidad.

ACELERAR PARA SER MÁS LÍDERES

01 Federación de identidad

La identidad federada tiene las siguientes ventajas, dentro del círculo de confianza:

El cliente maneja un único juego de credenciales para acceder a múltiples servicios: No necesita recordar un montón de identificadores y contraseñas.

El cliente sólo deposita sus atributos de identidad en un único proveedor, el Proveedor de Identidad, y define qué datos puede darse a los distintos Proveedores de Servicio. No necesita proporcionar sus atributos cada vez que se da de alta en un nuevo servicio.

La privacidad del cliente queda garantizada en todo momento y gestionada por él mismo.

El proveedor de servicio no necesita mantener atributos del cliente (aparte de los relacionados con su propio negocio), la consistencia de la información se mantiene a lo largo del tiempo puesto que se consume en el momento de necesitarse.

ACELERAR PARA SER MÁS LÍDERES

01 Federación de identidad

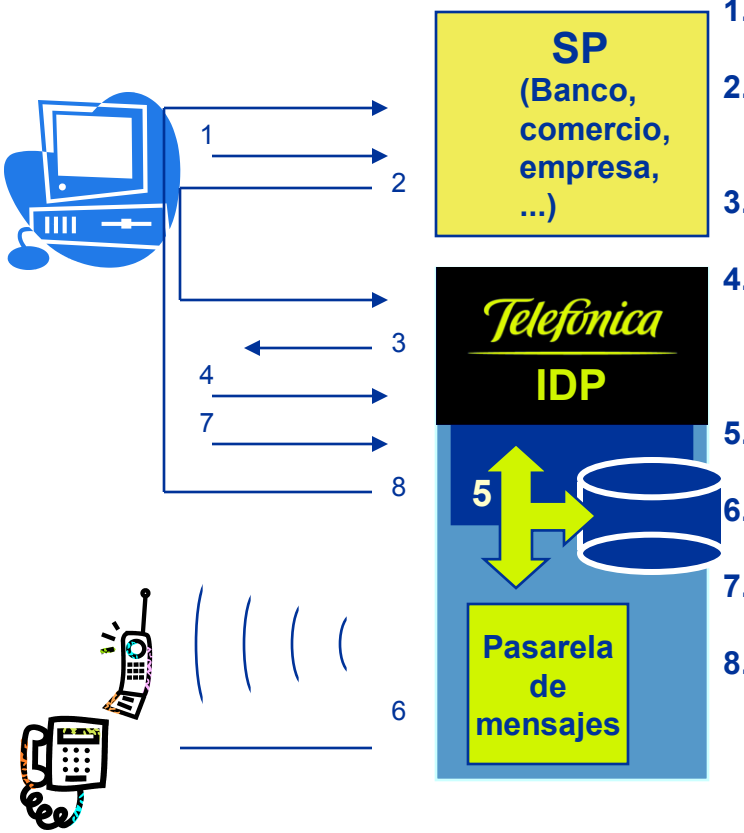
Mediante protocolo XML (web services), el proveedor de servicio y el proveedor de identidad intercambian la información necesaria para completar los procesos entre cliente y proveedor de servicio.

En el círculo de confianza se amplía enormemente los mecanismos de comercialización.

La identidad está mejor fundada porque el esfuerzo de gestión se centraliza y al mismo tiempo existe un gran despliegue geográfico, en función de las entidades que participan en el círculo de confianza.

ACELERAR PARA SER MÁS LÍDERES

02 Acceso con identidad segura



1. El cliente del proveedor de servicios (SP) intenta acceder a su banco, empresa, etc.
2. Como el cliente no tiene credencial de acceso, el SP redirige al cliente a Telefónica (Proveedor de Identidad – IDP).
3. Telefónica pide al cliente que se autentique (usuario y contraseña)
4. El cliente proporciona su usuario, contraseña y especifica en qué teléfono quiere su mensaje, de las opciones que están cargadas previamente, o no indica nada y se toma la opción por defecto.
5. Telefónica extrae el nº de teléfono adecuado, genera una contraseña aleatoria de un solo uso ...
6. y envía un SMS al cliente que contiene esta contraseña.
7. El cliente introduce en el formulario de autenticación la contraseña adicional.
8. Telefónica verifica la contraseña proporcionada por el cliente y la generada anteriormente. Si coinciden la autenticación es correcta, genera la credencial de acceso para el SP y redirige al cliente ya autenticado a su proveedor de servicios.

A partir de aquí el SP controla la sesión de su cliente.

ACELERAR PARA SER MÁS LÍDERES

02 Acceso con identidad segura

Si mediante phishing o pharming se hubieran capturado las contraseñas, aún habría sido necesario intervenir un canal de comunicación adicional para recibir el SMS.

Si un troyano o un keylogger captura toda la secuencia de conexión, como la contraseña adicional es de un solo uso no puede reutilizar esta información para suplantar al cliente.

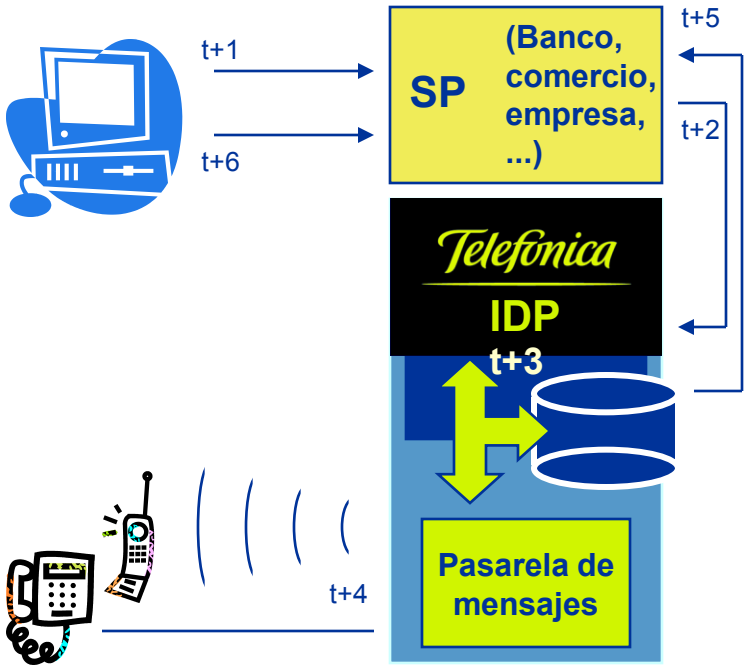
Una vez que un cliente se ha autenticado no es necesario que se vuelva a autenticar para acceder a otros servicios del círculo de confianza (SSO). Aunque los procesos de autenticación se siguen produciendo de forma transparente para el cliente.

Para que el proceso pueda ejecutarse, el SP debe tener un cliente liberty y el proveedor de identidad debe tener un servidor liberty.

ACELERAR PARA SER MÁS LÍDERES

02 ¿Habría sido posible que el phisher que atacó a citibank pudiera usurpar la identidad del cliente con nuestra "Identidad Segura"?

- El atacante habría tenido que suplantar a 2 entidades (SP e IDP) y el cliente habría tenido que caer en la trampa 2 veces. La complejidad del phishing aumenta exponencialmente.
- El cliente tendría que habernos indicado que aceptáramos peticiones suyas procedentes de Rusia (control de IP del cliente).
- Además tendría que superar el control adicional de clave de firma.



t+1. En un momento de la navegación el SP propone una verificación de control de sesión al cliente (porque se va a realizar una transferencia, por ejemplo)

t+2 El SP manda un mensaje al IDP con texto libre y solicitando una "clave de firma".

t+3 El IDP genera una clave de firma.

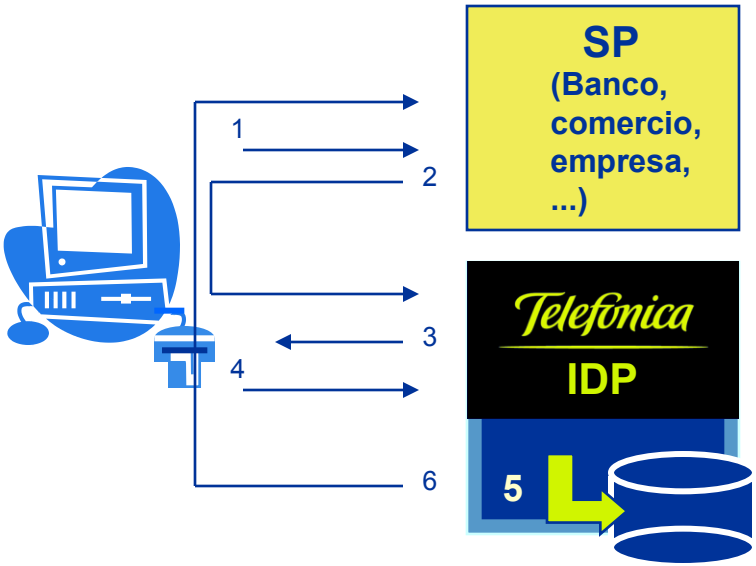
t+4 El IDP manda al cliente el mensaje propuesto por el SP ('verifique la transferencia al nº de cuenta xxxx-xxxx-xxxx-xxxx') y la clave de firma.

t+5 El IDP envía la clave generada al SP. El SP puede marcar un umbral de tiempo para aceptar la respuesta.

t+6 Si el cliente está de acuerdo con la transferencia, tecleará la clave de firma en el formulario del SP y la operación continuará. De lo contrario finalizará la sesión del cliente.

ACELERAR PARA SER MÁS LÍDERES

02 Acceso con DNI electrónico



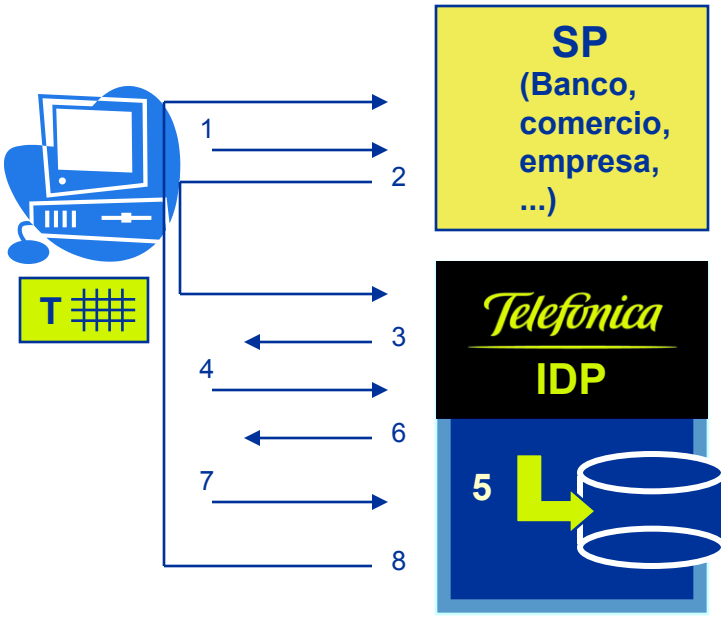
Si utilizáramos el DNI digital como TOKEN, la autenticación sería más sencilla:
...
3. Telefónica solicita la credencial al cliente, 4. El cliente entrega la credencial firmada con su clave privada
5. Telefónica verifica la firma con la clave pública
6. Si el resultado es correcto, redirige al cliente a su proveedor de servicio.

Para emplear este token tampoco necesitamos ninguna inversión en logística.

Como el empleo de certificados no es totalmente seguro. Sería conveniente combinarlo con alguno de los otros sistemas de aseguramiento de la identidad (SMS o tarjeta)

ACELERAR PARA SER MÁS LÍDERES

02 Acceso con tarjeta de coordenadas



En este caso sí empleamos logística.

Podemos utilizar tarjetas de coordenadas:

...

3. Telefónica pide al cliente que se autentique (usuario y contraseña)

4. El cliente proporciona su usuario y contraseña.

5. Telefónica identifica la tarjeta del cliente, genera una combinación aleatoria de coordenadas

6. e indica al cliente que introduzca los valores resultantes.

7. El cliente introduce en el formulario de autenticación esta contraseña adicional.

8. Telefónica verifica la contraseña proporcionada por el cliente y la generada anteriormente. Si coinciden la autenticación es correcta, genera la credencial de acceso para el SP y redirige al cliente ya autenticado a su proveedor de servicio.

ACELERAR PARA SER MÁS LÍDERES

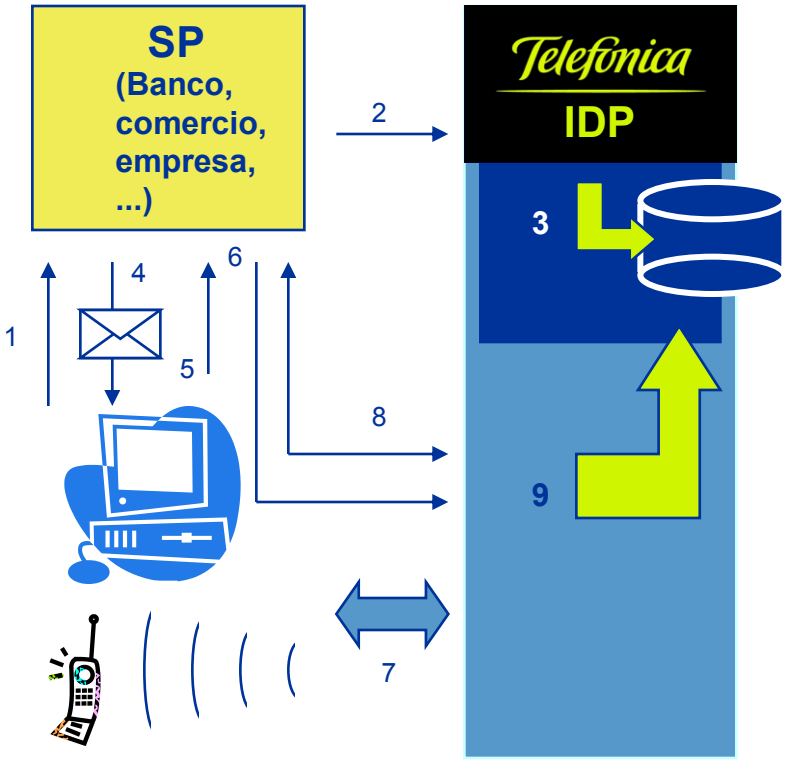
02 Acceso con tarjeta inteligente proporcionada por Telefónica

Disponemos de una PKI y podemos utilizar certificados sobre tarjeta inteligente o sobre TOKEN-USB emitidos por nosotros para realizar la autenticación de empleados de empresas o clientes VIP.

Hoy podemos emitir certificados pero a un coste demasiado elevado. En cualquier caso habría que adaptar las aplicaciones actuales de gestión y emisión de certificados así como las prácticas de autoridad de registro.

ACELERAR PARA SER MÁS LÍDERES

02 Registro con pseudónimo

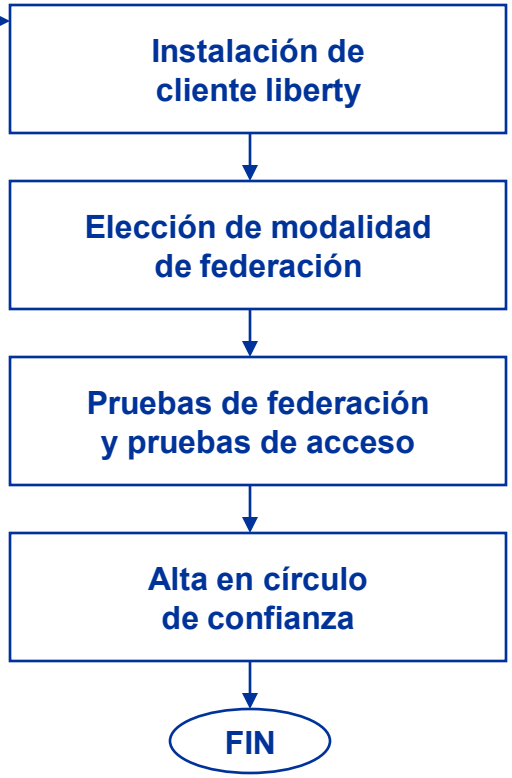


1. El cliente accede al SP. El SP le propone la federación y le solicita el nº de teléfono para recibir SMS.
   y le indica al cliente el uid en el IDP.
2. 3 . El SP registra:
   - pseudónimo en el SP
   - uid en IDP
   - contraseña en IDP
   - nº teléfono
4. El SP manda la contraseña al cliente.
5. 6, 7. Cuando el cliente accede al SP, le redirige al IDP,
   que realiza el proceso de autenticación.
8. El IDP redirige al cliente para que autentique en el
   SP y éste redirige al cliente para verificar la cuenta
   de acceso.
9. El IDP confirma la asociación de UID y pseudónimo.

No registramos datos personales del cliente, por lo que no se puede hablar en sentido estricto de federación.

ACELERAR PARA SER MÁS LÍDERES

3 Proceso operacional

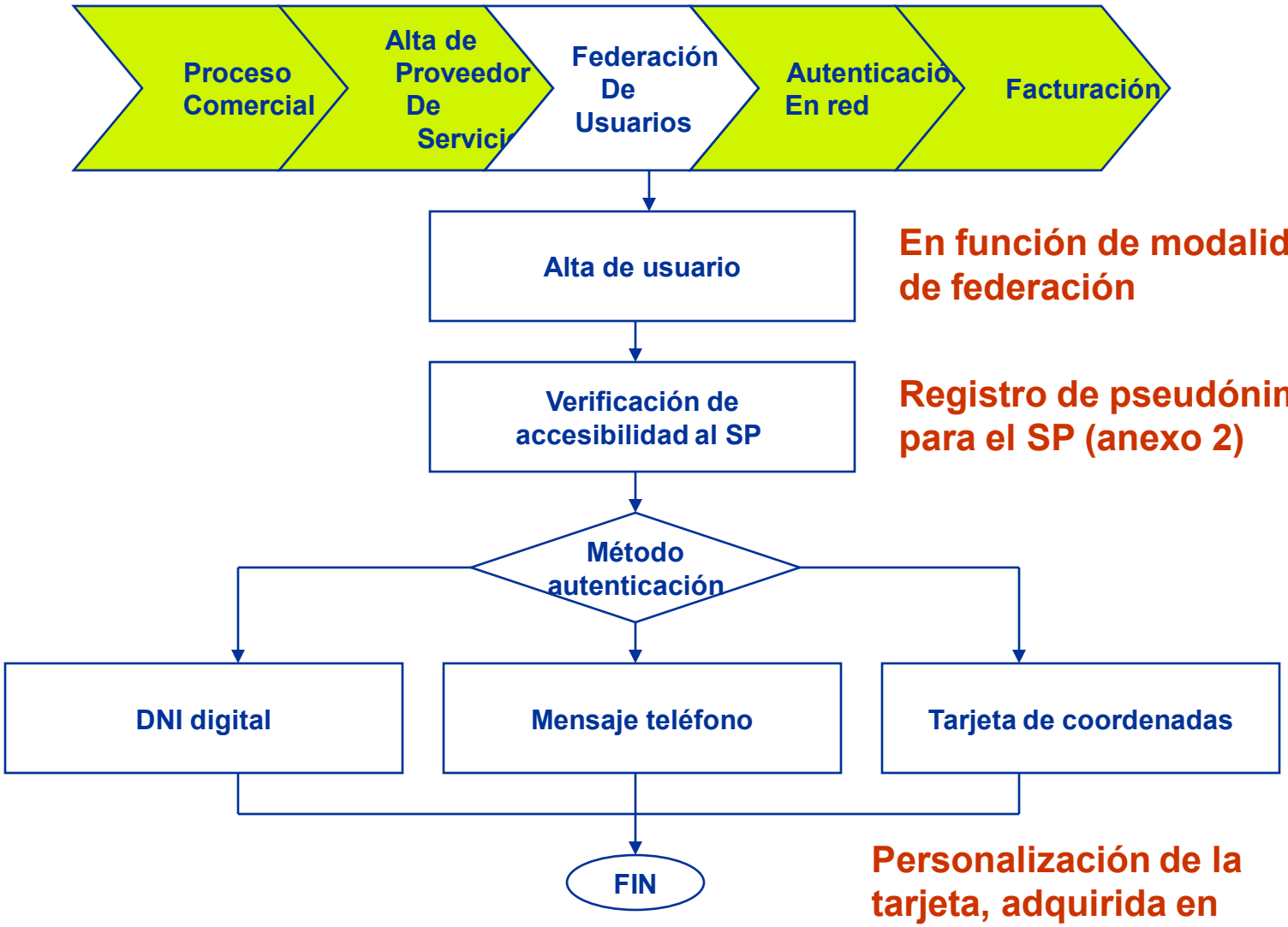


Kit autoinstalable con soporte remoto

Dos modalidades de federación: a instancia del cliente y a instancia del SP:
1) Alta débil. El cliente se da de alta en el IDP y verifica la posesión del usuario en el SP.
2) Alta fuerte. El SP proporciona las claves de alta del cliente en el IDP. El cliente accede al IDP y verifica la posesión del usuario en el SP.
En este último caso es importante si existe control presencial del cliente.

ACELERAR PARA SER MÁS LÍDERES

3 Proceso operacional



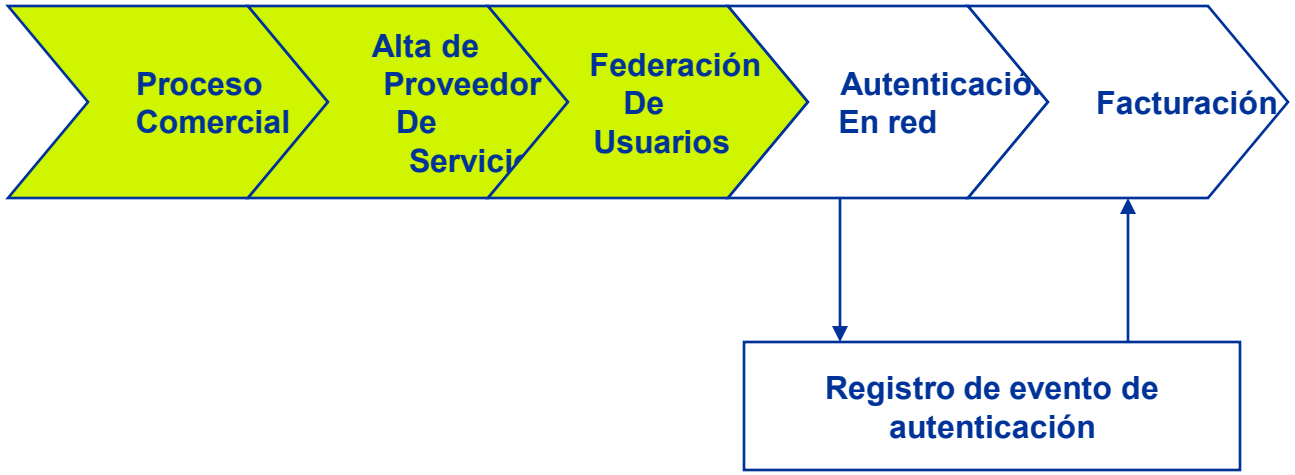
En función de modalidad de federación

Registro de pseudónimo para el SP (anexo 2)

Personalización de la tarjeta, adquirida en tiendas y puntos de distribución

ACELERAR PARA SER MÁS LÍDERES

3 Proceso operacional



Por cada evento de autenticación se registrará el SP para que pueda alimentar los procesos de facturación


Telefonica