FAQS TECNICAS TRANXFER

ÍNDICE

FAQS TÉCNICAS

¿Como funciona vuestra plataforma?

- Se realiza la partición de los ficheros por bloques, esto nos ayuda a eliminar las limitaciones de subida de fichero existentes en los navegadores.
- Se comprueba la compatibilidad del navegador (por desgracia, Internet Explorer no da soporte con las librerías empleadas), el resto de navegadores más modernos (Chrome, Firefox, Opera, Edge y algunos más que comparten motor chromium o el de mozilla...) sí son compatibles.
- Se negocian las claves de cifrado (algoritmo ECDH P-521), para cada fichero, es decir es única por fichero.
    - Por cada bloque:
        A. Se calcula el hash del fichero (SHA384), acumulándose para obtener el hash del fichero completo.
        B. Se encripta el fichero con AES 256.
        C. Se realiza el envío al servidor.
        D. Se recibe la confirmación de llegada al servidor.
        E. Se inicia el siguiente bloque.
    - Cuando finaliza, se envía el checksum resultante.

- En el servidor, una vez subido todo el fichero se almacena en el Storage (encriptado tal cual el proceso anterior)

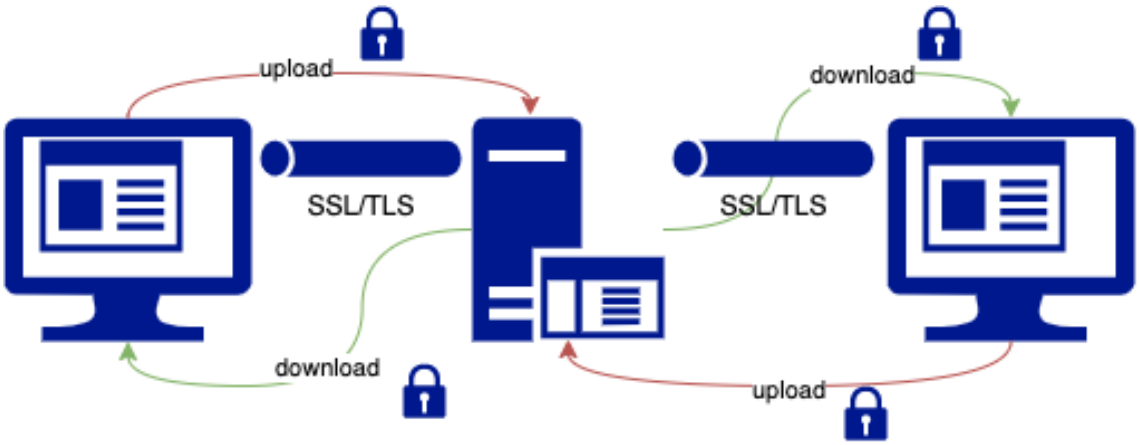
Si la compañía desea que se realicen las validaciones de seguridad oportunas

a. Se copia el fichero en un espacio temporal.
b. Se desencripta el fichero.
c. Se calcula de nuevo el checksum del fichero completo y se valida con el calculado obtenido en el lado del cliente.
    - Si no son iguales no se permite el envío del fichero.
d. Se valida el fichero con el antivirus
    - Si contiene algún tipo de malware no se permite el envío del fichero
e. Se valida el fichero con las políticas de seguridad
    - Si incumple alguna política de seguridad no se permite el envío del fichero

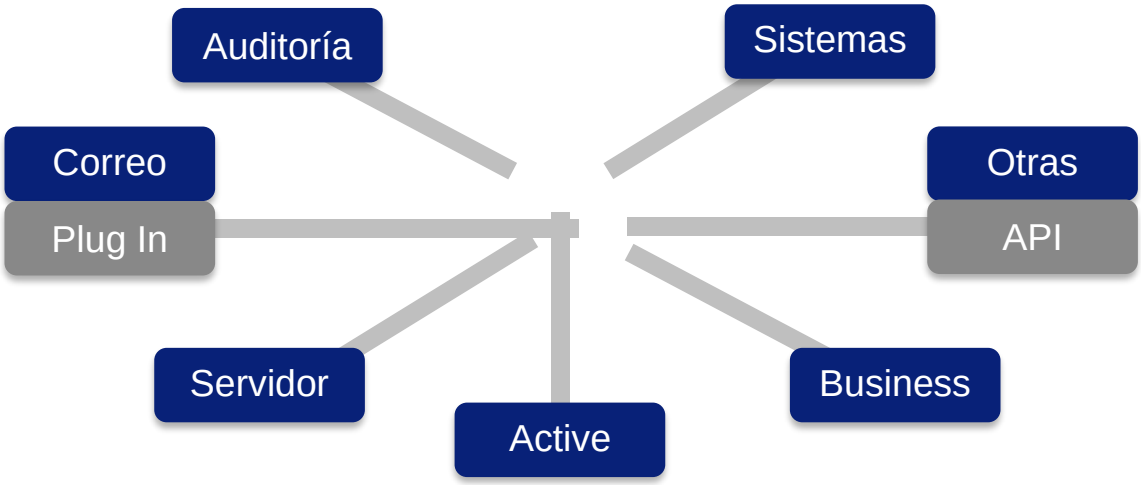
- **En el cliente Web, desde el navegador, de quién descarga el fichero**

Se negocian las claves de cifrado (SHA384), para cada fichero.

a. Se envía el fichero completo, aquí no hay problema de limitaciones
b. Se desencripta el fichero
c. Se calcula el hash del fichero (SHA384), para cerciorarse de la integridad del fichero E2E
d. Finaliza el proceso

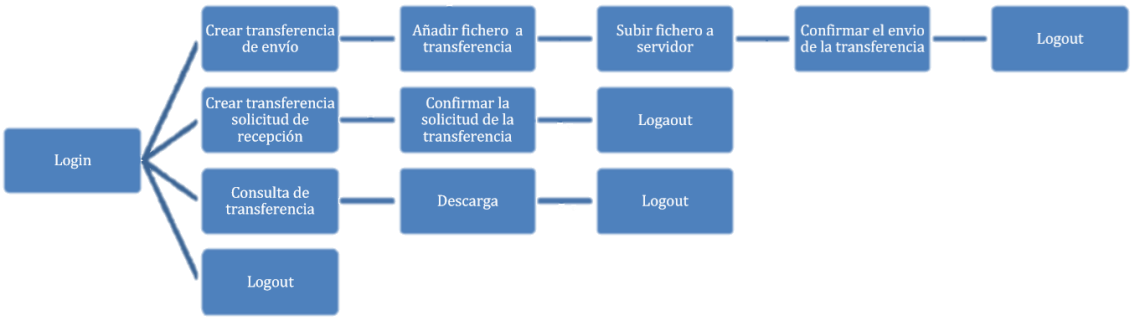


Integraciones:
Tranxfer permite una integración flexible con las distintas aplicaciones y sistemas corporativos

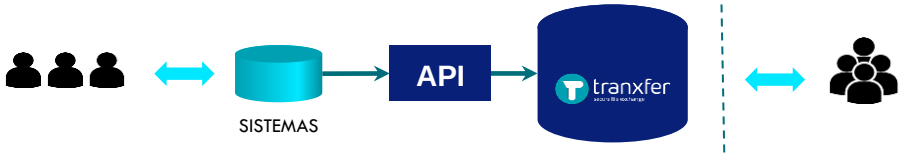


API

Tranxfer dispone de una API que permite integrar directamente el servicio de envío seguro de archivos en cualquier plataforma del cliente.
Incluyendo unas simples líneas de código de llamada a la API de Tranxfer, se podrán enviar archivos directamente desde cualquier sistema que el cliente requiera, simplificando al máximo el ecosistema de herramientas de envío de archivos para el usuario final.
En caso de ser necesario, Tranxfer podría realizar modificaciones sobre la API para facilitar la integración



Flujo de uso de la API



***En caso de ser necesario, Tranxfer podría realizar modificaciones sobre la API para facilitar la integración*

Sobre las modalidades de despliegue:

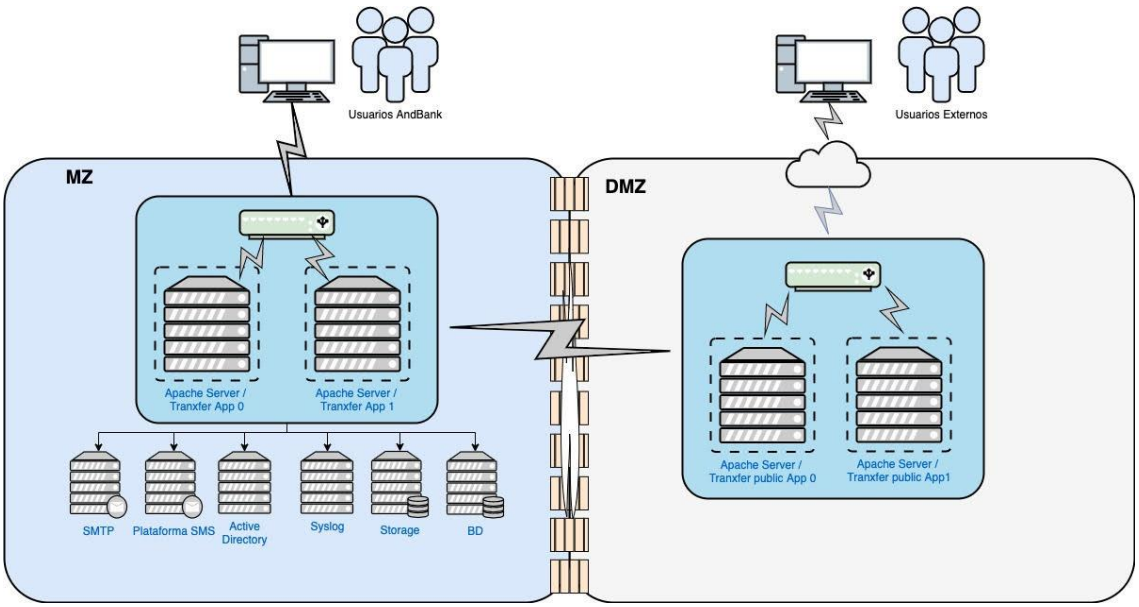
Nivel de seguridad alto y modalidades cloud ubicadas en Europa para cumplimiento estricto del GDPR.

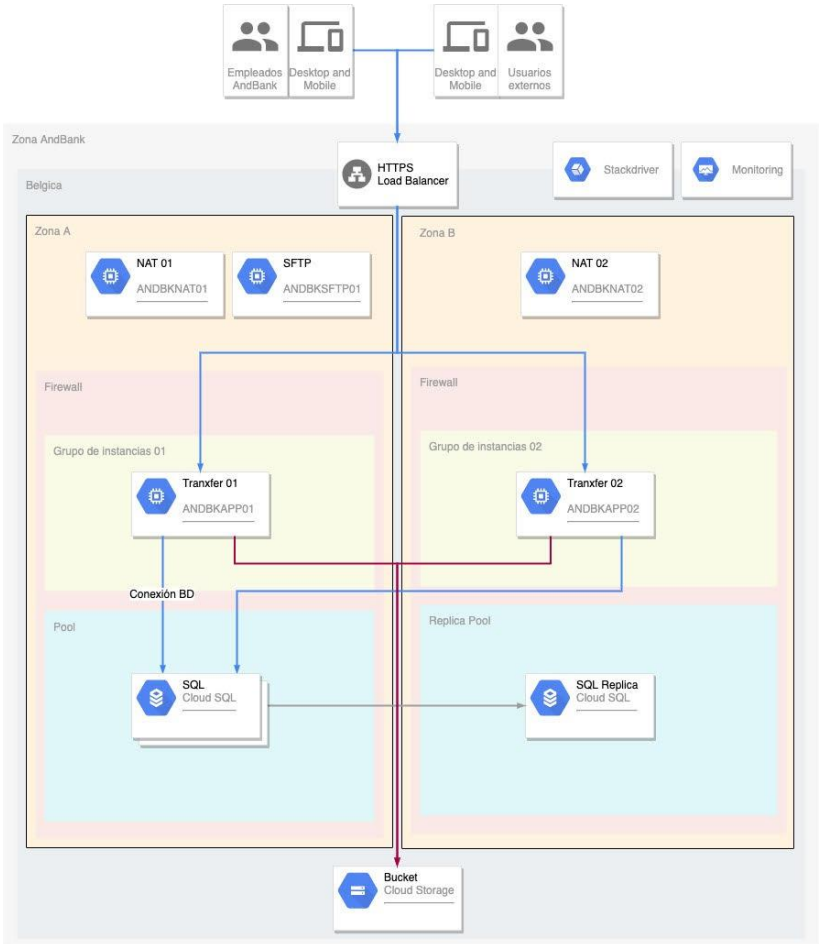
Nos podemos adaptar prácticamente a todo, por ahora tenemos nuestros servidores en el Cloud de Google (GCP) en un entorno montado con kubernetes como orquestador y todas las instancias que albergan los contenedores de los diferentes entornos, lo cual nos permite muchísima flexibilidad en cuanto a modalidades de despliegue.

Disponemos de entornos en AWS y GCP para nuestros clientes. Además, disponemos de infraestructura por código con lo que montar entornos para nuestros clientes es relativamente rápido.

También realizamos despliegues on-premise, adaptándonos a la infraestructura del cliente.

La opción que solemos montar para cloud es:





- Para on-premise (Opción HA)

La opción que solemos montar en infraestructura propia (HA) es:

¿Físicamente donde está hosteado el servicio? AWS/Azure/Google Cloud? Cuantas zonas de disponibilidad cuenta la solución?

La región de AWS que empleamos es Irlanda, las zonas son personalizables, normalmente disponemos las instancias en dos zonas, ya que para arquitecturas HA replicamos las instancias en dos zonas, podrían ser más o incluso menos, aunque el mínimo aconsejado son dos zonas para garantizar de algún modo que podemos continuar dando servicio...

¿Que garantías de seguridad ofrece vuestro Cloud / Google Cloud?

Puedes revisar las políticas de seguridad aquí, backups y recovery aquí:

https://gsuite.google.com/intl/es-419/security/?secure-by-design_activeEl=hardware

https://cloud.google.com/security/compliance/ens?hl=es-419

¿Qué tipo de seguridad se usa para la comunicación entre componentes?
Los clientes se comunican con el backend vía API-Rest, entre ambos se realiza en la propia red interna, mediante protocolo SSL/TLS v1.3

Protección de cuentas y Cifrado de BBDD ¿Qué otros mecanismos se usan para proteger la información?

En base de datos las contraseñas están encriptadas al igual que los datos en reposo en la base de datos. La encriptación en reposo, al final ayuda a que si alguien accede mediante un mecanismo no reglado a la BD los datos los verá encriptados, tendrá que realizar el ejercicio de desencriptación de los mismos.
Esta opción la controlamos desde el Cloud, adaptándonos a la configuración del cliente en despliegues on premise.

Qué significa expresamente *reposo con clave mixta AES 256?*

La clave mixta se refiere a que empleamos dos token uno fijo a nivel de compañía y otro único para cada transferencia para la encriptación de los ficheros. Además, últimamente hemos realizado alguna modificación en el

frontend que nos ha permitido que esta encriptación se realice de punto a punto, con la negociación segura de claves entre el cliente y la aplicación, con la extensión de la seguridad de encriptación desde que el usuario adjunta el fichero al navegador.

Cuántas claves de cifrado existen por cliente y usuario? Cómo funciona el ciclo de vida? Cómo se custodian dichas contraseñas?

1. Credenciales de usuario, se está trabajando en la posibilidad de 2FA en el login.
2. Claves por fichero, un usuario que realiza una transferencia con varios ficheros, dispondrá de una clave por fichero distinta, la aplicación es la que se encarga del negociado entre los clientes y el servidor.

La claves se almacenan en BD, asociadas a los ficheros, cuando las transferencias expiran, se eliminan los ficheros del servidor, con lo que la validez de las mismas finaliza.

¿Existe la posibilidad de que las claves queden del lado del cliente?

En un principio no lo contemplamos, en caso de ser requeridos entraría dentro de una personalización y por lo tanto, habría que realizar un desarrollo adicional para ello.

Se está usando autenticación OAuth2 con el Grant client credentials. ¿Es esto personalizable para realizar la autenticación con el grant de Authorization Code? ¿Podríais autenticar tokens JWT, no generados por la plataforma?

La aplicación actualmente no lo permite, se podría valorar en algún caso. No lo han pedido para poder emplearlo en integraciones con aplicaciones terceras del cliente

¿Qué mecanismos de protección contra fuerza bruta existen en la autenticación tanto para usuarios como para invitados?

A nivel de configuración es configurable, normalmente en integraciones con AD, se encarga la plataforma del cliente. En usuarios generados directamente en Tranxfer, se puede bloquear el acceso durante X minutos, si hay un número n de intentos fallidos. Además, si hay integración con SIEM, se puede generar una alerta con ello...

¿Cómo se protegen las contraseñas en la plataforma?
En integraciones con AD, no gestionamos credenciales. Las credenciales creadas para usuarios de BD, están encriptadas en BD, además de la encriptación de BD.

¿Qué solución de DLP integráis en la plataforma? Se puede integrar una solución DLP nuestra?

Por defecto, empleamos Tika, una solución de Apache. Podemos integrarlo con otros DLP, ahora mismos lo estamos con DLP Symantec mediante protocolo ICAP en on premise. Con cualquier solución API más rápida la integración

¿Qué solución antivirus/malware estáis utilizando? Se puede integrar una solución personalizada?

Por defecto, empleamos ClamaV, es una solución liberada por Cisco. Podemos integrarlo con otros AV.

¿Cómo es la integración con SIEM del cliente? ¿Qué tipos de transporte soportados y mecanismos de autenticación que soporta la solución?

Podemos integrarnos vía Syslog. En entornos oncloud lo realizamos a través de ficheros de auditorías mediante sftp, no hay una carga online, pero la generación de los mismos la podemos hacer diariamente o cada menos tiempo.

¿Cuáles son vuestras prácticas de desarrollo seguro?

Empleamos metodología BDD de desarrollo, potenciando de esta forma un producto de con la mayor calidad posible, tenemos automatizadas pruebas de regresión además de las pruebas unitarias de las mismas. Las pruebas siempre tienen en cuenta roles y permisos de los usuarios

¿Cuál es la frecuencia de los Pentestings realizados a la plataforma?

Nuestros clientes han realizado pentesting, han habido en total 4 durante los últimos 12 meses con resultado satisfactorio.

tranxfer | secure file exchange

GRACIAS