monetae

Políticas de Custodia de Activos Digitales

Introducción

El presente documento describe en detalle la plataforma de custodia y supervisión de activos digitales de Fintech Americas, S.A. de C.V. (en adelante "Fintech Americas"), así como las políticas relacionadas con la seguridad, la infraestructura, la auditoría y el cumplimiento normativo y financiero. El objetivo principal es garantizar la protección y disponibilidad de los activos digitales, asegurando su resguardo en entornos de máxima seguridad.

Fintech Americas utiliza a Fireblocks como proveedor de infraestructura de custodia, una plataforma de autocustodia que elimina riesgos de contraparte y proporciona seguridad multicapa. A través de Fireblocks, se almacenan y transfieren activos digitales desde billeteras MPC-CMP (siglas de Computación Multipartita) y entornos con enclaves SGX.

El sistema de custodia y supervisión de Fintech Americas permite:

- Almacenar, gestionar y supervisar diversos activos digitales (criptomonedas, tokens, etc.).
- Aplicar múltiples métodos de seguridad (cifrado, autenticación de dos factores, monitoreo de actividad) para proteger a inversores y usuarios.
- Garantizar la disponibilidad de los activos digitales cuando se requieran.

Infraestructura de Custodia:

Fintech Americas ha implementado un sistema de seguridad robusto que combina defensas de software y hardware. Este sistema de custodia se organiza en cuatro pilares fundamentales:

1. **Infraestructura de billetera MPC-CMP** con almacenamiento en caliente y templado.
2. **Enclaves seguros Intel SGX:** Aislamiento a nivel de hardware del software sensible y material criptográfico en entornos de nube segregados.
3. **Motor de Políticas Automatizado** para configurar y aplicar reglas que afectan cómo se manejan y aprueban las transacciones. Protegido por SGX para evitar que tanto hackers como personas internas manipulen las políticas o aprobaciones.
4. **Sistema de respaldo y recuperación** de claves privadas para asegurar la continuidad del negocio.

Infraestructura de billetera MPC-CMP

La Computación Multipartita (MPC) es una tecnología criptográfica que permite a varias partes utilizar su información secreta para resolver un problema de cálculo sin compartir sus secretos con los demás participantes. Fireblocks desarrolló el protocolo MPC-CMP que aplica este concepto a las firmas ECDSA y EdDSA basadas en blockchain, utilizadas por todas las blockchains. MPC-CMP elimina el concepto de una clave privada única.

A través de fireblocks, Fintech Americas ofrece billeteras basadas en la computación multipartita segura (MPC) que evita que una clave privada sea un punto único de falla al firmar transacciones. Las billeteras MPC-CMP dividen las claves privadas en múltiples partes, que se almacenan en un dispositivo móvil y en enclaves de hardware en dos centros de datos en la nube de primer nivel, geográficamente dispersos.

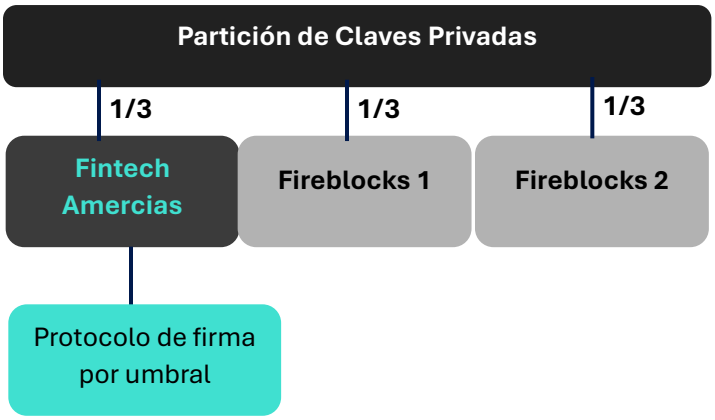
Esta clave nunca se reúne como un todo, ni durante la creación inicial de la billetera ni durante la firma de la transacción. MPC-CMP sigue un conjunto de pasos para garantizar que nunca haya un único punto de vulnerabilidad de la clave privada:

- Los secretos individuales son aleatorizados por cada uno de los tres puntos de contacto, ya sea servidores o dispositivos móviles. Esos secretos nunca se comparten entre ellos.
- Los puntos de contacto participan en un protocolo descentralizado de creación de billeteras, en el cual calculan la clave pública (dirección de la billetera) que corresponde al conjunto de acciones privadas individuales.
- Cuando se solicita una firma en una transacción de blockchain, los tres puntos de contacto participan en un proceso de firma distribuida. Durante este proceso, cada uno de los puntos valida individualmente la transacción y la política antes de firmarla.

El protocolo MPC-CMP es abierto y está disponible en repositorios públicos. Ha sido revisado académicamente en varias ocasiones y fue presentado en las conferencias NIST 2020 y ACM CCS 2020.

Las claves privadas se dividen en tres fragmentos los cuales se generan y resguardan por separado. Estos nunca se combinan ni se exponen, ni siquiera cuando se firman transacciones.

- Para firmar transacciones, cada fragmento de clave crea una firma sin revelar la clave privada a las otras partes, y las firmas de cada fragmento de clave se combinan entre sí



Este proceso garantiza que la clave privada extendida nunca se construya en un único entorno. Por lo tanto, la clave privada extendida no se almacena en ningún lugar, ya que ninguna parte debe tener acceso a la clave privada completa ni se genera en un solo punto. La única excepción es la copia de seguridad y recuperación de la clave del espacio de trabajo, donde los fragmentos de la clave se encriptan y se guardan en un paquete de recuperación para situaciones de emergencia.

Protocolos de firma por umbral

Una firma por umbral es un tipo de firma digital en la que el material secreto subyacente, como una clave privada, se divide en varias partes. Cada parte es mantenida por un miembro diferente del grupo, y para crear una firma válida, se deben combinar el número requerido de partes.

En estos casos, un mínimo de participantes debe estar de acuerdo para firmar un mensaje, lo cual es útil en escenarios donde es importante que varias personas aprueben una acción.

Este tipo de protocolos permite a Fintech Americas proveer una capa adicional de seguridad, debido a que ciertas operaciones y transacciones predefinidas requieren la firma de varios participantes.

Compartición Aditiva de Secretos

La Compartición Aditiva de Secretos es un método más sofisticado que divide un secreto en múltiples partes únicas. A diferencia de la compartición de secretos ingenua, este método garantiza que un atacante no gane ventaja alguna al obtener uno o dos fragmentos del secreto, ya que no puede usar esos fragmentos para calcular el resto del secreto.

Con la implementación de la Compartición Aditiva de Secretos en MPC-CMP, el secreto nunca existe como un todo, ni siquiera durante la ceremonia de generación de claves.

MPC-CMP vs. Multi-Sig

Al igual que las billeteras Multi-Signature (Multi-Sig), la protección de la clave privada en MPC-CMP elimina el riesgo de un único punto de vulnerabilidad tanto para atacantes externos como para personas internas, ya que la clave privada nunca se concentra en un solo dispositivo. Además, la naturaleza distribuida de MPC permite a los miembros del equipo requerir múltiples autorizadores para firmar una transacción, sin necesidad de estar en la misma ubicación.

Operacionalmente, MPC representa un avance significativo sobre Multi-Sig debido a su flexibilidad inherente, permitiendo la modificación y mantenimiento continuo del esquema de aprobadores, algo crucial para las nuevas demandas del ecosistema de activos digitales.

El protocolo MPC-CMP garantiza propiedades de seguridad fuertes y es compatible con la composición universal, lo que significa que sigue siendo seguro incluso cuando se combina con otros protocolos.

MPC-CMP también permite la firma completamente desconectada (air-gapped), lo que añade un nivel extra de seguridad en transacciones.

Enclaves Seguras Intel SGX

Las billeteras en la plataforma son billeteras de múltiples firmantes. Por lo tanto, requieren un conjunto de cofirmantes independientes, cada uno con un fragmento de la clave privada, para participar en el proceso de firma.

Estos segmentos se almacenan independientemente y son controlados por entidades diferentes. Específicamente, un fragmento es controlado por Fintech Americas y dos fragmentos son almacenados por Fireblocks en enclaves de hardware en dos centros de datos en la nube de primer nivel, geográficamente dispersos

Para firmar transacciones, se requiere la participación de un umbral de cofirmantes pertenecientes a Fireblocks y otro umbral de cofirmantes pertenecientes a Fintech Americas. Ninguna de las partes, ni Fireblocks ni Fintech Americas, puede firmar una transacción por sí sola.

Fireblocks utiliza un conjunto de cofirmantes en servidores seguros (SGX). Estos cofirmantes actúan como medidas de seguridad en caso de que las claves de los clientes se vean comprometidas.

- Protegen la billetera al aplicar de manera lógica una política de seguridad, como establecer un límite en el monto de las transacciones o asegurar la integridad de la dirección de destino.

Intel SGX es un enclave a nivel de hardware que aísla código y datos seleccionados dentro de un sistema, similar a un módulo de seguridad de hardware (HSM), separándolos del sistema operativo. Está diseñado para proteger el material criptográfico, el algoritmo criptográfico y la ejecución de partes sensibles del software, tanto de hackers

como de insiders, como administradores malintencionados. En comparación con un HSM, Intel SGX ofrece varios beneficios, como:

- Protección de algoritmos criptográficos de nueva generación, como MPC y pruebas de conocimiento cero.
- Capacidad para aislar y proteger motores de políticas, bases de datos de listas blancas y flujos de trabajo contra insiders y hackers.
- Autenticación de usuarios robusta, aislada por hardware, mediante la certificación de enclaves seguros (ARM TrustZone) en dispositivos móviles y tokens de hardware como Yubikey.
- Alta escalabilidad en nubes públicas y despliegues locales, lo que aumenta la seguridad, disponibilidad y redundancia.

En general, SGX ofrece gran flexibilidad operativa mientras brinda la seguridad asociada con un HSM tradicional. Para empresas de activos digitales que requieren el más alto nivel de seguridad basada en hardware junto con velocidad y flexibilidad, SGX es una opción muy sólida.

Fireblocks utiliza enclaves SGX en un mínimo de tres a cinco máquinas (cada una en una red segregada) para distribuir claves privadas con un alto nivel de seguridad. Las claves están almacenadas en el enclave SGX, que encripta su espacio de memoria y datos, lo que impide que las claves sean extraídas incluso si malware o un hacker toma control del sistema operativo del servidor. Además, Fireblocks emplea SGX para asegurar las claves API en entornos de ejecución confiables (TEEs), protegiendo estas credenciales de posibles ataques o accesos internos, e incluso del propio personal de Fireblocks.

Manejo de Fragmento de Clave Privada de Fintech Americas

Fintech Americas utiliza un conjunto de dispositivos móviles o servidores SGX, cada uno operado y gestionado por diferentes miembros del equipo. El dispositivo móvil almacena los fragmentos de la clave en un almacenamiento seguro y de manera encriptada. Por ejemplo, en iOS, se almacenan en el Keychain. La extracción de las claves requiere múltiples factores utilizados en combinación para la autenticación y el descifrado:

- Autenticación por medio de PIN
- Autenticación por medio de Face ID
- Autenticación por medio de Frase de Seguridad

La aplicación móvil de Fireblocks transfiere datos con encriptación TLS (Seguridad de la Capa de Transporte), incluyendo TLS bidireccional, con soporte para fijación de certificados. Esto garantiza el nivel más alto de seguridad, previene ataques de intermediarios (man-in-the-middle) y evita que los datos sean manipulados o reproducidos.

Motor de Políticas Automatizado

La plataforma permite establecer un conjunto de reglas para gobernar las transacciones entre billeteras y entre partes externas. Además, permite controlar qué usuarios del espacio de trabajo de Fintech Americas pueden crear, firmar o aprobar transacciones mediante la creación de reglas basadas en un conjunto de parámetros personalizables.

Esta funcionalidad permite definir reglas en un orden lógico predeterminado. Al efectuarse una transacción, automáticamente se aplican las reglas y parámetros definidos para cada transacción.

Las reglas tienen dos componentes definidos por Fintech Americas. Los Parámetros determinan cómo una transacción puede coincidir con la regla, y luego las Acciones indican al Motor de Políticas qué hacer a continuación.

- Parámetros: Definen qué características debe "coincidir" una transacción para que la regla se aplique.
    - Quien inicia la transacción
    - Tipo de transacción: envío, recepción, minting, burning, contract call, etc.
    - Origen de la transacción (Whitelist)
    - Destino (Whitelist)
    - Montos mínimos y máximos
    - Periodos de tiempo
- Acciones: Definen qué sucederá a continuación, con las siguientes opciones:
    - Permitir: El Motor de Políticas aprueba automáticamente y reenvía a un firmante designado (manual o automático).
    - Aprobado por: Otros usuarios firmantes o grupos de usuarios deben aprobar o denegar la transacción permitida. Todos ellos deben tener roles de usuario autorizados para ser aprobadores.
    - Bloquear: El Motor de Políticas bloquea automáticamente la transacción.

Adicionalmente, Fintech Americas define diferentes umbrales de aprobación y firmantes designados para diferentes combinaciones de parámetros con el fin de resguardar los activos digitales de los clientes.

Las reglas del motor de políticas serán definidas por la dirección de Fintech Americas y aprobadas por el Representante Legal. Estas políticas serán revisadas anualmente o en un plazo menor de ser requerido.

Sistema de Respaldo y Recuperación

Fintech Américas implementó un proceso de respaldo y recuperación de las claves privadas a través de un servicio de Station 70. Esto permite tener control total sobre la clave privada completa, permitiendo recuperar los activos digitales en caso haya una falla o disrupción en los sistemas de Fireblocks.

Modelo de segurida

Las copias de seguridad de Fintech Americas, utilizan un modelo de seguridad de varias capas para lograr una serie de propiedades de seguridad. Hay tres propiedades principales:

1. Cumplimiento criptográfico
2. Cumplimiento de la política de recuperación
3. Copias de seguridad verificables (registros)

Las medidas criptográficas brindan políticas de seguridad rígidas, pero protegen contra amenazas internas y ataques a todo el sistema. La división de claves en 3 dominios garantiza que Fintech Americas, operadores y todos los sistemas en la nube participen para poder recuperar una copia de seguridad.

La aplicación de políticas de recuperación garantiza que Fintech Americas controle a los usuarios que deben aprobar una recuperación antes de que comience cualquier recuperación. Esto brinda los controles para equilibrar la seguridad.

Las copias de seguridad verificables utilizan registros periódicos de los dispositivos, así como escaneos y verificaciones automáticas del material almacenado, para demostrar a los clientes y a terceros que las copias de seguridad pueden:

- Recuperarse cuando sea necesario
- Los dispositivos del cliente están disponibles (sin dispositivos perdidos o PINs olvidados)
- y el personal está disponible (sin cuentas inaccesibles debido a la rotación de empleados).

Además, el diseño de seguridad en el Station70 garantiza que:

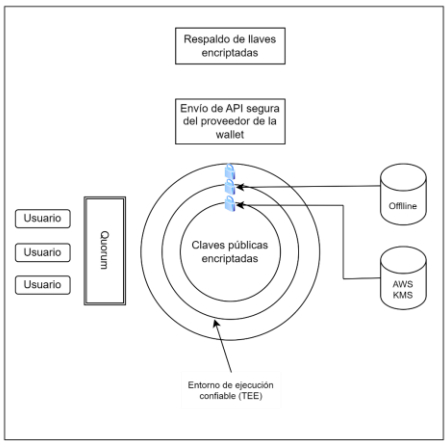
- Station70 nunca tiene en su posesión suficiente material criptográfico para acceder a las copias de seguridad de Fintech Americas y sus clientes.
- Los tres dominios de seguridad (cliente-nube-operador) deben ser activados para realizar una recuperación confiable.
- La redundancia dentro de cada dominio garantiza una alta durabilidad del material de las claves de respaldo.
- Cada dominio de seguridad utiliza módulos de seguridad de hardware (HSM) para gestionar el material criptográfico. Dos de los dominios de seguridad almacenan el material de las claves de forma offline hasta que se inicie la recuperación.
- Los dispositivos HSM perdidos o comprometidos pueden ser anulados individualmente mediante el borrado de texto cifrado.
- Fintech Americas tiene control sobre las políticas de recuperación: por ejemplo, umbral de aprobación de 2 de 5 personas.

Descripción general del servicio "Bunker" de Station70

Bunker es, en términos criptográficos y funcionales:

- Un servicio de gestión de texto cifrado de alta durabilidad
- Un motor de políticas y aprobaciones impulsado por el cliente
- Una API de copias de seguridad segura
- Un entorno de ejecución confiable (TEE por sus siglas en inglés) que genera una clave de cifrado de respaldo, divide la clave de respaldo en tres partes y cifra cada una de ellas con claves públicas de distintos dominios de seguridad (un proceso llamado enrolamiento del paquete de respaldo.
- Una serie de sitios de descifrado para recuperación:

    - Fintech Americas descifra un recurso compartido de recuperación mediante un navegador y un token de hardware (Yubikey) en un recurso compartido que sólo Station70 de custodia puede usar.
    - Los operadores ejecutan un software local que descifra un recurso compartido de recuperación del operador mediante un YubiHSM en un recurso compartido que sólo Station70 de custodia puede usar.
    - TEE que descifra los paquetes de respaldo almacenados y los vuelve a cifrar en una clave pública en recuperación.



Gestión de texto cifrado

La durabilidad e integridad del texto cifrado son, sin duda, el aspecto más importante de un servicio de recuperación confiable. La mayoría de las claves criptográficas se pierden por una mala administración (normalmente, como resultado de fallos de durabilidad, como perder un teléfono, cambiar de teléfono, colocar incorrectamente los tokens de hardware o eliminarlos accidentalmente).

La recuperación confiable de nuestra tecnología utiliza al menos dos técnicas para garantizar la durabilidad del texto cifrado: 1) almacenamiento en la nube de alta durabilidad y 2) escaneo periódico. De manera similar, se utilizan dos técnicas para probar la integridad del texto cifrado: 1) listas de texto cifrado firmadas y 2) escaneo periódico.

Los textos cifrados necesarios para la recuperación son:

- Paquete de copia de seguridad encriptado.
- Fintech Americas comparte al Proveedor de forma encriptada, la clave de encriptación de la copia de seguridad. Un texto cifrado para cada uno de los dispositivos encriptados.
- Recursos compartidos cifrados del operador (un texto cifrado para cada dispositivo del operador).
- Nube compartida cifrada (sólo puede haber una).

Durabilidad

Para garantizar una alta durabilidad, Station70 almacena las copias de seguridad y los textos cifrados relacionados en sistemas de almacenamiento que son multizona y multiregión.

Integridad

Para cada copia de seguridad cifrada, Station70 almacena la huella digital SHA256 de todas las copias de seguridad cifradas y los textos cifrados relacionados en sistemas de almacenamiento separados (las huellas digitales se almacenan en una base de datos relacional y los textos cifrados se almacenan en un almacenamiento S3 de alta durabilidad).

Verificación

Station70 analiza de forma asincrónica el sistema de gestión de texto cifrado periódicamente (por ejemplo, trimestralmente) y verifica que el contenido de cada paquete de copia de seguridad coincida con las huellas digitales de la base de datos. Asimismo, informan de los resultados de estos análisis como parte del informe de registro de copias de seguridad que son proveídos a Fintech Americas. Estos análisis detectan cualquier componente faltante o alterado antes de que sea necesaria una recuperación. Cualquier falla en el proceso de escaneo genera alertas que se comunican al equipo de ingeniería de nuestro Proveedor.

Proceso para recuperar una copia de seguridad

Para obtener una copia de seguridad a través de nuestro Proveedor, es necesario cumplir con condiciones previas que son:

1. Fintech Americas solicita una recuperación al Proveedor.
2. Se ha cumplido la política de aprobación de recuperación.
3. Fintech Americas publica una participación que puede ser descifrada por el TEE.
4. El operador ha aprobado la recuperación y ha publicado una participación de operador que puede ser descifrada por el TEE.
5. El TEE ha sido implementado.

Procedimiento

1. El TEE recibe las siguientes entradas: textos cifrados de respaldo, participación en la nube cifrada, participación de Fintech Americas cifrada, participación del operador cifrada.
2. El TEE utiliza KMS para descifrar cada uno de: la participación de Fintech Americas; la participación en la nube; y la participación del operador.
3. El TEE utiliza la **interpolación de LaGrange** para reconstruir la clave de cifrado de respaldo (BEK), que es una clave simétrica AES-GCM-256.
4. El TEE descifra la clave privada de cifrado de respaldo y utiliza esto para descifrar el respaldo.
5. El TEE cifra el respaldo con la clave pública de recuperación designada de Fintech Americas.
6. El TEE emite el respaldo recifrado, que se almacena a la espera de ser descargado.

Auditoria y Monitoreo

- Fireblocks ofrece herramientas de auditoria y monitoreo en tiempo real que permite a Fintech Américas, S.A. de C.V. rastrear y verificar todas las transacciones y actividades relacionadas con los activos digitales.
- Se deberán realizar pruebas de penetración de forma anual con el objetivo de identificar y mitigar cualquier vulnerabilidad en los sistemas de custodia de Fintech Americas. Los hallazgos derivados de estas pruebas deberán ser abordados de manera inmediata mediante la implementación de medidas correctivas y mejoras en la infraestructura de seguridad, garantizando así la máxima protección de los activos digitales.

monetae

Políticas Financieras y Contables Relacionadas a la Custodia de Activos Digitales

El objetivo de esta política es establecer principios contables y financieros que regulen la custodia de activos digitales en Fintech Americas, asegurando transparencia, cumplimiento normativo y una gestión adecuada del riesgo. Estas políticas son aplicables a todas las operaciones relacionadas con la custodia de activos digitales, incluyendo registro contable, valoración, reporte financiero, auditoría y cumplimiento normativo.

Principios Generales

- Cumplir con las Normas Internacionales de Información Financiera (NIIF/IFRS) y regulaciones locales.
- Implementar controles internos robustos para mitigar riesgos operacionales, financieros y de cumplimiento.
- Mantener una segregación clara entre los activos propios de Fintech Americas y los activos custodiados de clientes.

Reconocimiento y Clasificación

- Los activos digitales custodiados estarán en todo momento resguardados en billeteras a nombres del cliente y segregadas de los activos y fondos de Fintech Americas.
- Se mantienen registros detallados de cada activo digital custodiado, identificando titularidad y movimientos.

Contabilización de Tarifas y Comisiones

- Las comisiones por custodia y transacciones de activos digitales se reconocen como ingresos operativos en el periodo en que se prestan los servicios.
- Se deben desglosar ingresos por tipo de activo y servicio en los reportes financieros.

Valoración de Activos Digitales

- Se utilizará un método de valoración basado en precios de mercado detallados por Fireblocks u otras fuentes de información confiables.

Controles Financieros y Auditoría

- Se implementan sistemas de monitoreo en tiempo real de las posiciones custodiadas.
- Se deberá de hacer reconciliaciones de registros internos y balances en blockchain de forma recurrente.
- Fintech Americas, deberá de restringir el acceso a los fundos custodiados y deberá establecer multifirma para transacciones significativas.

Auditorías

- Se realizarán auditorías externas por una firma independiente al menos una vez al año.
- La firma de auditoria será definida por el organismo de administración de Fintech Americas.

Reportes y acceso a la información

- Los clientes podrán, en todo momento, solicitar informes sobre sus activos en custodia, asegurando transparencia en saldos y movimientos.
- Fintech Americas deberá cumplir con todos los reportes regulatorios conforme a las exigencias de la Ley de Emisión de Activos Digitales, Ley de Proveedor de Servicios Bitcoin, y cualquier otra regulación aplicable.

Cumplimiento Normativo y Regulatorio

- Cumplimiento con regulaciones de activos digitales, incluyendo normativas AML/CFT y de protección al inversionista.
- Reporte de operaciones sospechosas según marcos regulatorios aplicables.
- Cooperación con entidades regulatorias para garantizar la legalidad y solidez del negocio de custodia.

Revisión y Actualización

- Estas políticas serán revisadas anualmente para adaptarlas a cambios regulatorios, contables y de mejores prácticas del sector.