FORTKNOXSTER

WHITEPAPER

La Encriptación como servicio.
Versión 1.2 • 17 Octubre 2017

FORT
KNOXSTER

Si gasta más en café que en seguridad,
este seguro que será pirateado

Nota: *Richard Clarke. Experto en ciberseguridad del gobierno de EE. UU.*

Renuncia de Derechos.

La información proporcionada en este documento se entrega "tal cual", sin garantía de ningún tipo. En ningún caso nuestra empresa o nuestros asesores serán responsables de daño alguno directos, indirectos, incidentales, o consecuentes, o por la pérdida de beneficios comerciales o daños especiales, incluso si nuestra empresa o nuestros asesores han sido informados respecto a la posibilidad de tales daños.

Documento Definitivo

Ocasionalmente, podemos actualizar la documentación en línea entre lanzamientos y lanzamientos de software y relacionados. En consecuencia, si este documento no se descargó recientemente, es posible que no contenga la información más actualizada. Para ello, consulte nuestro website www.FortKnoxster.com para obtener la información más reciente.

Información del producto:

Para documentación, notas de la versión, actualizaciones de software o para obtener información sobre productos, licencias y servicios. Por favor, consulte nuestro sitio web www.FortKnoxster.com

Soporte técnico:

Para obtener asistencia técnica, ingrese en www.FortKnoxster.com y seleccione la opción “Soporte”. En la página de Soporte, verá varias opciones, incluida una que le permite realizar una solicitud de asistencia.

Comentarios

Sus sugerencias nos ayudarán a seguir mejorando la precisión, la organización y la calidad general de las publicaciones para los usuarios. Envíe su opinión sobre este documento a: hello@FortKnoxster.com.

Si tiene comentarios o preguntas sobre información o procedimientos específicos, incluya el título y, si está disponible, la revisión, los números de página y cualquier otro detalle que nos ayude a ubicar el tema al que se refiere.

Marcas registradas

FortKnoxster *es una marca comercial en proceso de registro, propiedad de FortKnoxster Ltd.*

Índice de Contenidos

Resumen Ejecutivo

Nuestro mundo está cambiando más rápido que nunca y es difícil mantenerse al día con las nuevas tendencias, las palabras de moda y las tecnologías emergentes. El uso de la tecnología blockchain está en su punto más alto. La cantidad de diferentes monedas criptográficas ahora se cuentan por miles, cuando se trata de diferentes tokens, monedas, activos digitales o lo que uno elija para llamarlos.

Desafortunadamente, la tasa de crímenes cibernéticos también está en su punto más alto y estar en línea nunca ha sido tan inseguro como hasta ahora. Jaqueos, espionaje de vigilancia masiva, virus, malware, espionaje, phishing, extorsión ... la lista de ataques es larga y sigue creciendo día a día, a medida que los atacantes se vuelven más sofisticados, agresivos y creativos.

El FBI afirma que hemos entrado en una epidemia de cibercrimen y que los ciberdelitos han superado los crímenes "normales" de la vieja escuela, tanto en la intensidad como en el daño.

El equipo detrás de **FortKnoxster**, está conformado por experimentados Ingenieros ciberseguridad y de seguridad cibernética experimentados, ha pasado más de 3 años desarrollando "Fort Knox" como una plataforma de comunicación encriptada para usuarios finales tipo Punto a Punto.(P2P)

"FortKnoxster ha aprovechado el uso de blockchain y sofisticadas técnicas de encriptación de punto a punto en una plataforma de comunicación todo en uno, amigable para el usuario, donde los usuarios pueden comunicarse de forma privada y segura, ya sea a través de bandeja de entrada, chat, llamadas de teléfono y video, almacenamiento de archivos, etc. FortKnoxster elimina el riesgo de piratería, amenazas cibernéticas y vigilancia gubernamental centralizada ".

FortKnoxster es la primera plataforma de comunicación encriptada punto a punto, llave en mano del mundo y, en resumen, se puede describir como:

"Telegram con esteroides"

cita: Telegram, aplicación de comunicacion y chat

FortKnoxster es todo lo que necesita para comunicarse, interactuar y trabajar de forma segura en un mundo en línea dominado por crímenes cibernéticos en aumento..

FortKnoxster, es una de las pocas ventas de tokens respaldadas por un producto funcional.

Introducción

FortKnoxster es una compañía de seguridad cibernética, especializada en el desarrollo de soluciones de comunicación seguras y encriptadas. La compañía ha desarrollado una plataforma de cifrado única, que está principalmente dirigida al mercado B2C.

La plataforma viene como una solución EaaS (Encriptación como servicio).

FortKnoxster ha sido diseñado con una arquitectura y características únicas, lo que permite a todos utilizar nuestra plataforma para todas sus necesidades de comunicaciones y almacenamiento de datos.

FortKnoxster aborda uno de los mayores desafíos en nuestra sociedad moderna; para proteger las comunicaciones y sus datos de los ciberdelincuentes, y al mismo tiempo mantener un alto nivel de privacidad.

Nuevas regulaciones complejas: La creciente adopción de nuevas tecnologías (IoT, BYOD, servicios en la nube, etc.). Han impulsado la necesidad de una seguridad y encriptación mejoradas más que nunca. Las nuevas leyes y regulaciones son muy estrictas, y FortKnoxster ofrece una de las mejores soluciones "plug-and-play" para cumplir con la mayoría de estas nuevas leyes.

FortKnoxster puede ser utilizado por cualquier persona, en cualquier momento, independientemente si se encuentra en una computadora portátil / escritorio o con su teléfono inteligente o tableta.

La plataforma FortKnoxster ha sido probada contra el jaqueo, por una variedad de hackers éticos y "cypherpunks" en todo el mundo, y ha "superado su examen", con creces, ya que nadie ha logrado comprometer nuestra plataforma de ninguna manera, como así, tampoco acceder a ningún sector, cuentas cifradas o contenido.

"El cifrado debe estar disponible para todos y de manera predeterminada, no es una función que requiera solo si está haciendo algo que considera que vale la pena proteger. El cifrado es la tecnología de preservación de privacidad más importante que tenemos"

cita: Bruce Schneier, criptógrafo estadounidense, profesional de la seguridad informática, especialista en privacidad y escritor.

Desafio

La conexión en línea ahora es esencial para casi todos, creando nuevas oportunidades para la innovación, la interacción con amigos y socios comerciales, y el crecimiento global.

El cibercrimen, los ciberdelincuentes y sus herramientas son cada vez más diversas y sofisticadas. El delito cibernético ahora se presenta en una variedad de formas, y a menos que los consumidores, las empresas y los gobiernos actúen inmediatamente, los ciberdelitos podrían amenazar el fundamento de nuestra sociedad de muchas maneras devastadoras.

En el futuro cercano, y a medida que la tecnología de computación sea más predominante en nuestras vidas, estas amenazas tendrán más impacto. Las interfaces intuitivas que valoramos cada vez más, y de las que dependemos, son a menudo donde surgen todos los problemas.

Usar Internet y comunicarse en línea nunca ha sido tan inseguro como ahora, y empeora cada día. Los piratas informáticos representan una gran amenaza, ya que el pronóstico indica que el cibercrimen costará más de $ 3 billones de dólares en el 2019, según *Juniper Research*.

"El Cibercrimen es la mayor amenaza para todas las empresas del mundo".

cita: Ginni Rometty - CEO de IBM

Los ciberdelincuentes de hoy, son a menudo profesionales altamente motivados, bien financiados por empresas competidoras, organizaciones criminales o estados nacionales, que persisten en sus esfuerzos por penetrar y dañar al oponente tanto como le sea posible.

Según una encuesta reciente de **PWC**, tanto las pequeñas como las grandes empresas han experimentado un fuerte aumento en las infracciones de seguridad en línea, informando que más del 80% de las empresas y pymes sufrieron una violación de seguridad el año pasado.

La mayoría de los ejecutivos encuestados esperan que haya más incidentes de seguridad por delante y que no haya "buenas noticias" cuando se habla de seguridad cibernética (o falta de seguridad) en el futuro.

Además, el costo de las brechas reales continúa aumentando y se ha más que duplicado en un año. Una empresa promedio, con 500 empleados, que experimentan una brecha de seguridad en línea, termina con una factura neta de más de 3.5 millones de USD en ventas perdidas, interrupción del negocio, recuperación de activos, pérdida de clientes, multas y compensaciones, etc. Y además de esto su imagen es dañada y sufrirá la humillación.

En los últimos años, hemos escuchado mucho sobre el poder de Big Data, que permite a las empresas ofrecer productos y servicios más personalizados. El beneficio de esto para el

consumidor puede ser obvio, pero plantea muchas preguntas éticas, y no solo cuando los datos personales están en manos de negocios inescrupulosos.
Ha quedado claro por un tiempo que las leyes de datos (o la falta de ellas) dañaron a los consumidores y su privacidad . Esto ha dado como resultado la aplicación de la ley GDPR. (Reglamento general de protección de datos).

La ley tiene como objetivo dar a los ciudadanos un mayor control sobre sus datos y crear una uniformidad de las normas para hacer cumplir en todo el continente.

Los grandes desafíos para la mayoría de las empresas ahora son, cómo cumplir con esta estricta nueva ley, que se inicia el 25 de mayo de 2018.

Algunas de las compañías más grandes de nuestro tiempo, como Google y Facebook, se han creado recopilando y crecido, usando datos de usuarios de sus usuarios para publicitar a terceros. Todo lo que hace o dice dentro de estas plataformas se graba, almacena, analiza y el principal objetivo de tenerlo allí es ganar dinero en su perfil y ubicación.

Agregue a esto la vigilancia masiva general de la mayoría de los gobiernos que rastrea y registra todo lo que se hace en línea las 24 horas, los 7 días de la semana, y lo almacena para siempre. Y aún más intimidante: Estos servidores del gobierno son pirateados todo el tiempo, por lo que sus datos pueden terminar en manos de criminales.

No hace falta decir que hay muchos peligros potenciales (y cuestiones éticas) asociadas con la proliferación de perfiles digitales, desde la piratería, a la discriminación, a un estado de vigilancia tipo “Orwelliana”. Hay una gran diferencia entre lo que las empresas pueden y deben saber.

cita: Orwelliana. Adjetivo creado por George Orwell para indicar actividades que atentan contra el bienestar de una sociedad libre.

La actividad en línea siempre deja huellas: Archivos de registro, links de acceso o datos que se crean en los sistemas al utilizarlos. Una vez que se eliminen estos controles de privacidad, los proveedores de servicios de Internet podrán vender la información que capturen sobre cómo usted y sus usuarios usan Internet (que visita, que lee, etc)..

La pérdida de la privacidad en línea hace que sea mucho más fácil para los delincuentes acceder a sus datos, ya que esas inmensas empresas son pirateadas regularmente y todos sus datos están ahora en manos de posibles organizaciones deshonestas o personas que buscan sacar lucro con sus datos.

Aunque todos podemos encontrar formas de protegernos, la única forma real de evitar el rastreo y "robo" de nuestros datos es dejar de utilizar estos servicios gratuitos y proteger nuestras comunicaciones con encriptación de punto a punto, como FortKnoxster.

Qué es FortKnoxter ?

FortKnoxster es una plataforma integral de comunicación, colaboración y almacenamiento seguro de archivos.

"Piense en ella como una combinación de todas sus aplicaciones diarias favoritas (no seguras) como Skype, Slack, Telegram, Dropbox, Facetime, Gmail, etc., Todas reunidas en una sola plataforma segura y superior con la mayor privacidad que se pueda lograr."

Las aplicaciones convencionales mencionadas anteriormente son excelentes, pero a menudo, presentan muchos fallas de seguridad. En primer lugar, como estos servicios son gratuitos, "**usted es el producto**", es decir, todos sus datos y comunicaciones se están leyendo, almacenando, vendiendo y, a menudo, pirateando desde el mismo lugar donde se almacenan.

No existe absolutamente ninguna privacidad, ya que la mayoría de los modelos de negocios de estas compañías generan la mayor cantidad de ingresos posible al vender sus datos a terceras partes

FortKnoxster es su alternativa más segura, ya que no podemos nosotros, ni nadie más, leer sus datos o comunicaciones en absoluto, porque está encriptada de punto a punto. Incluso si pudiéramos, nuestro modelo comercial es exactamente el opuesto a la mayoría de los demás, estamos en el negocio de proteger sus datos, no vendiéndolos al mejor postor.

FortKnoxster es extremadamente fácil de usar, ya que no requiere instalaciones adicionales o plug-in.Los usuarios están literalmente activos en cuestión de minutos y pueden comenzar a disfrutar de un nivel extremo de seguridad , siendo su interfaz muy intuitiva.

Es muy fácil, invitar a amigos, familiares o socios comerciales a unirse a la plataforma.

FortKnoxster fue diseñado para ser utilizado por todos y, por lo tanto, no hay necesidad de conocimientos técnicos para su utilización.

Si desea probar o experimentar una demostración gratuita de FortKnoxster, haga clic aquí.

Principales características de FortKnoxster

• **Bandeja de entrada**

Los mensajes están encriptados de punto a punto y tan seguros como sea posible. Envíe mensajes a colegas, clientes y socios comerciales con total tranquilidad.

• **Almacenamiento distribuidos de archivos**

Almacene sus datos valiosos encriptados, y asegúrese de que permanezcan como suyos. Es muy fácil compartir y administrar archivos y carpetas sin problemas.

• **Chat**

Chat seguro en tiempo real para comunicaciones rápidas e instantáneas. Viene con mensajes de voz, chat en grupo y mucho más.

• **Llamadas**

Llamadas seguras sin intromisión de competidores o vigilancia externa. La llamada más privada que puede obtener tanto en la web como en dispositivos móviles.

• **Llamadas grupales y/o conferencias**

Colabore de forma segura chateando, llamando, compartiendo archivos, etc., mediante la función de conferencia en grupo: trabaje de forma más inteligente y segura.

• **Compartir pantalla**

Hemos desarrollado el uso compartido de pantalla cifrada, como una herramienta valiosa adicional para colaborar de forma segura con socios y otros terceros.

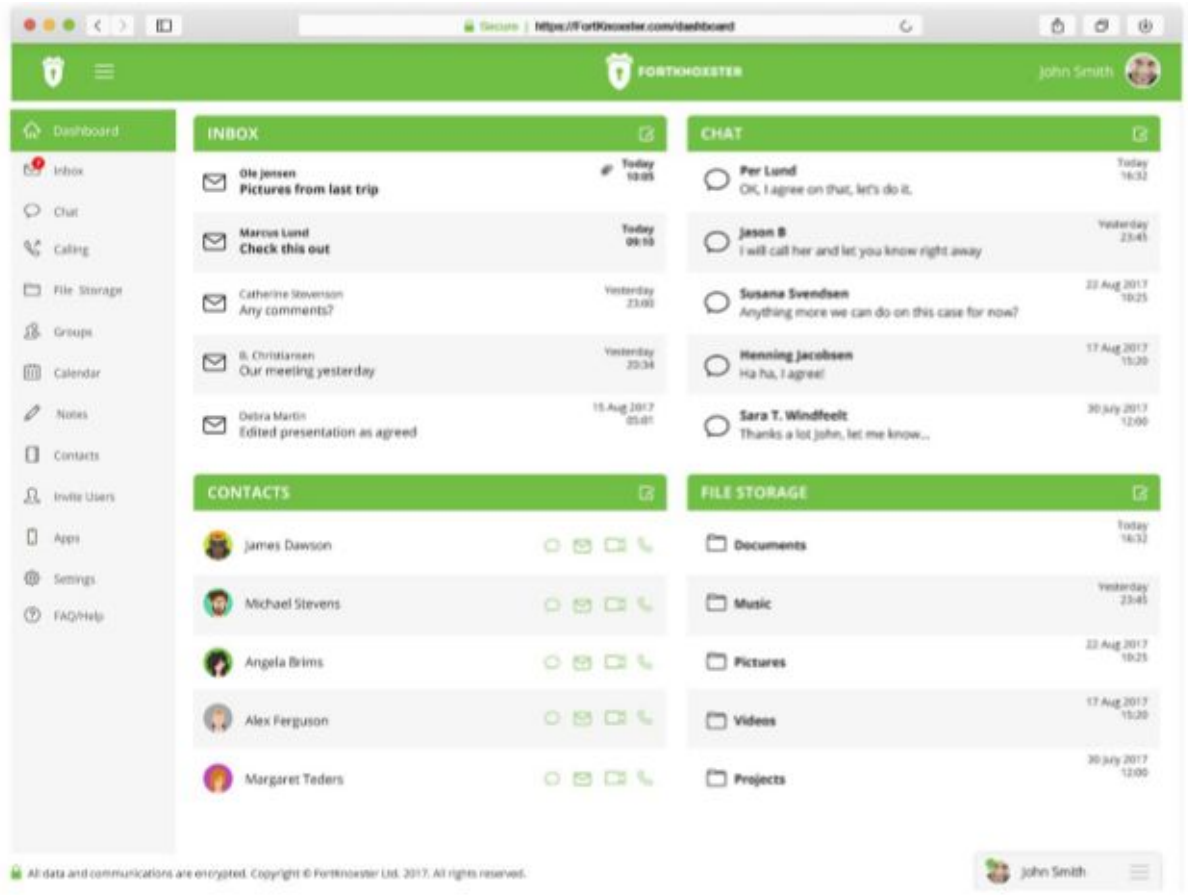
• **Mensajes de voz**

Envía mensajes de voz rápidos sin llamar. Ahorre tiempo y la función está disponible tanto en la plataforma web como en la de aplicaciones móviles.

• **Panel de control, intuitivo**

El panel de control, brinda a los usuarios una visión general de todas las comunicaciones y datos.

Consulte la página siguiente para ver las imágenes de la consola y el tablero.



Aplicación móvil FortKnoxster

Our iOS and Android apps will be launched January 2018.

Nuestra Misión/Objetivos

"FortKnoxster será la plataforma de comunicación y almacenamiento de datos más segura jamás construida ...

y, finalmente, será la pesadilla de cualquier pirata informático, espía o delincuente informático"

¿Por qué utilizar el cifrado?

La palabra encriptación proviene de la palabra griega "**kryptos**", que significa "**oculto**" o "**secreto**". El cifrado se usa para mejorar los niveles de seguridad al mayor nivel posible.

El uso del cifrado es casi tan antiguo como el arte de la comunicación en sí mismo. Ya en el año 1900 AC, un escriba egipcio usó jeroglíficos no estándar para ocultar el significado de una inscripción.

La encriptación es una forma de maximizar la seguridad de, por ejemplo, un mensaje de correo electrónico, un mensaje de chat, una llamada o un archivo "codificando" los contenidos.

El cifrado es básicamente un proceso o método de codificación de mensajes o información de tal manera que solo las partes autorizadas e intervinientes puedan leerlo.

El cifrado es una forma segura para que las empresas y los militares se comuniquen de forma privada y segura, sin que otros (es decir, los competidores) puedan seguir o espiar las comunicaciones.

El cifrado es también, la herramienta principal que protege las comunicaciones de cualquier persona, desde grandes empresas y gobiernos, hasta pequeñas empresas y abogados, o ciudadanos comunes. El cifrado protege las infraestructuras de países enteros: *comunicaciones, energía, transporte , sistemas de salud, y Negocios*.

A medida que avanzamos con entusiasmo en la era de los dispositivos inteligentes conectados, el cifrado (si se usa) protege nuestras llamadas telefónicas, mensajes de texto, correos electrónicos y almacenamiento en la nube. Con el advenimiento de la Internet de las cosas, los expertos en seguridad piden la implementación de un fuerte cifrado en los productos IOT, que, si no se atiende, podría causar caos en los hogares e infraestructuras más grandes.

Cuando escuchas la palabra encriptación, lo primero que se te viene a la mente es, que es algo que solo los entusiastas de la tecnología o los frikis entenderían o usarían. En realidad, la idea del cifrado no es tan complicada en absoluto y nuestra plataforma ha hecho que sea muy fácil usar..

La encriptación es el mejor método para salvaguardar su privacidad.
El criptógrafo y especialista en seguridad y privacidad **Bruce Schneier** afirma:

"El cifrado debe estar disponible para todos de manera predeterminada, no como una función que solo se activa o usa solo cuando está haciendo algo que considera que vale la pena proteger".

¿Por qué usar blockchain ?

Un blockchain es un ledger (asiento contable), distribuido, abierto y descentralizado que registra las transacciones financieras (o virtualmente cualquier cosa de valor) entre dos partes, en una red punto a punto. Esta lista de registros en constante crecimiento está vinculada y asegurada con una fuerte criptografía, lo que hace que estas transacciones sean permanentemente verificables y, por lo tanto, incorruptibles.

”El Blockchain resuelve el problema de la manipulación"

Cita: Vitalik Buterin, inventor de Ethereum

Dado que el blockchain es públicamente verificable, ofrece tal seguridad y transparencia que lo hace ideal para muchos tipos de aplicaciones de seguridad.

FortKnoxster, aprovecha estas características que proporciona la tecnología de blockchain, trasladando su confianza centralizada de identidades digitales a una descentralizada, específicamente usando la cadena de bloques Ethereum, y utilizando sus contratos inteligentes.

La confianza es de vital importancia y es el elemento más importante en cualquier infraestructura criptográfica. El modelo actual de confianza para las identidades digitales en FortKnoxster está centralizado. Este modelo de confianza centralizado es hoy un desafío común, ya que se convierte en un punto único de falla

”La centralización de la identidad crea un único punto de falla y construye un repositorio de datos de alto valor que puede atraer a los piratas informáticos, los controles adecuados deben estar en su lugar para mantener la integridad.”

Cita: Informe IBM IDC sobre cadena de bloques, "Es solo una cuestión de tiempo".

El modelo de confianza distribuida, que utiliza blockchain, es una nueva forma de gestionar identidades digitales donde la tecnología blockchain permite a los usuarios controlar su propia identidad digital y compartir y comunicarse entre personas de confianza con su consentimiento. Por lo tanto, ninguna entidad individual puede comprometer la identidad digital de un usuario y no existe un solo punto de falla presente.

Además de implementar un modelo de confianza seguro y descentralizado de las identidades digitales cifradas de FortKnoxster (las claves públicas); FortKnoxster también construirá un ecosistema completo utilizando el token **FKX** y contratos inteligentes en el blockchain de Ethereum, para facilitar transacciones seguras de servicios de suscripción e incentivos para los participantes.

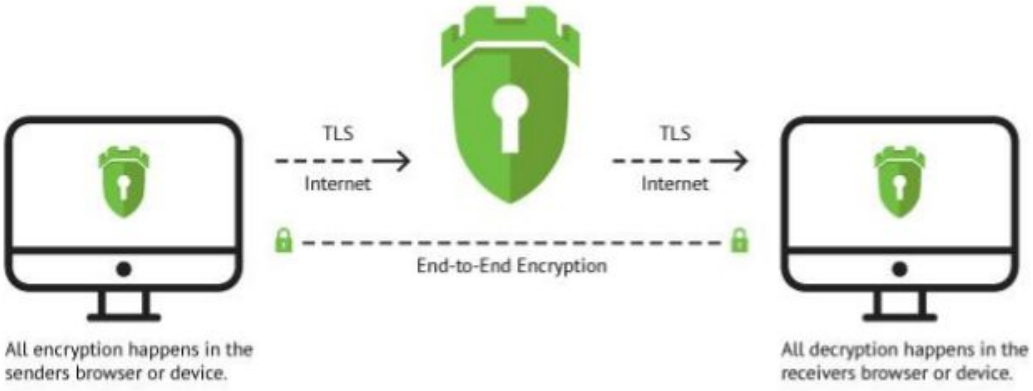
Nuestra tecnología

La siguiente es una explicación técnica del cifrado de punto a punto de FortKnoxster y describe en detalle los diseños de cifrado y la seguridad utilizando el blockchain de Ethereum, con contratos inteligentes y una confianza descentralizada de identidades digitales. Una descripción más detallada se encuentra en la sección del Apéndice.

FortKnoxster es una plataforma segura de comunicación y colaboración entre aplicaciones nativas que permite a los usuarios intercambiar mensajes y archivos (incluidos correos electrónicos, archivos adjuntos, chats, chats grupales, llamadas, documentos, imágenes, videos, mensajes de voz,.. ,) de forma segura usando una encriptación fuerte de punto a punto

En FortKnoxster, la seguridad y la privacidad tienen la más alta prioridad. Esta es la razón por la que hemos **diseñado** las arquitecturas seguras de cifrado con FortKnoxster. A diferencia de la mayoría de las otras empresas en línea, nuestro objetivo principal es proteger la privacidad de nuestros usuarios, de lo que estamos muy orgullosos.

La siguiente figura ilustra cómo el cifrado de punto a punto ocurre entre dos usuarios, a través de los servidores FortKnoxster en la conexión encriptada TLS entre los clientes, desde el navegador y hasta el servidor.



El Apéndice 1 describe en detalle cómo se produce el intercambio de mensajes de bandeja de entrada y chat, almacenamiento de archivos y llamadas, y qué operaciones de cifrado están involucradas.

FortKnoxster tiene su propia infraestructura de clave pública (PKI), que se extiende a la cadena de bloques de Ethereum. En el blockchain, la identidad digital del usuario se almacena en un registro, usando contratos inteligentes y no puede ser comprometida por una sola persona o grupo, ni siquiera por el equipo de FortKnoxster.

Cuando un usuario se registra en FortKnoxster.com, se generan cuatro conjuntos de pares de claves tipo RSA, dos conjuntos de pares de curvas elípticas (CE) y 6 protectores de claves (uno por cada clave privada) en el navegador del cliente.

Estos pares de claves de cifrado e identidad se utilizan para diferentes servicios y protocolos. A diferencia de otros protocolos de cifrado conocidos, cada uno de los servicios o protocolos de FortKnoxter necesita dos juegos de pares de claves, uno para el cifrado y el descifrado, y otro para la firma y la verificación.

El protector de clave se usa para encriptar y/o envolver cada clave privada que solo conoce el usuario.

La contraseña simple del usuario se usa para formar dos contraseñas en lado del cliente, la contraseña de la cuenta y la clave raíz.

Tenga en cuenta que la **contraseña de usuario** solo es conocida por el usuario y es muy importante comprender que la contraseña simple de usuario y la clave raíz nunca se envían a los servidores.

La **contraseña de la cuenta,** es un algoritmo o hash criptográfico de la contraseña que utiliza el algoritmo PBKDF2 con tecnología SHA-256 como algoritmo de hash, y realiza 10000 rondas de operaciones de hashing y toma el nombre de usuario @ domain como datos aleatorios. El resultado es una contraseña segura, que se envía al servidor y se almacena como otro hash criptográfico utilizando la función de derivación de clave **BCRYPT**. Esta contraseña solo se usa para autenticar al usuario y no puede descifrar ninguno de los datos de los usuarios.

La clave raíz, se calcula de la misma manera que la **contraseña de la cuenta**, pero usa una palabra generada aleatoriamente y, por lo tanto, es una contraseña completamente diferente. La clave raíz se form forma con una clave tipo AES de 32 bytes que se utiliza para cifrar / ajustar mediante un Protector de clave con tecnología AES-KW.

En este punto, cada clave privada RSA y EC se encriptan / encapsulan con AESGCM con la llave protectora de 32 bytes, que está bloqueado por la clave raíz de 32 bytes, cada uno formando un contenedor de clave.

Todas las claves públicas y los contenedores de claves son protegidos y se envían al servidor durante el registro, junto con los detalles del usuario, la contraseña de la cuenta y la identidad digital.

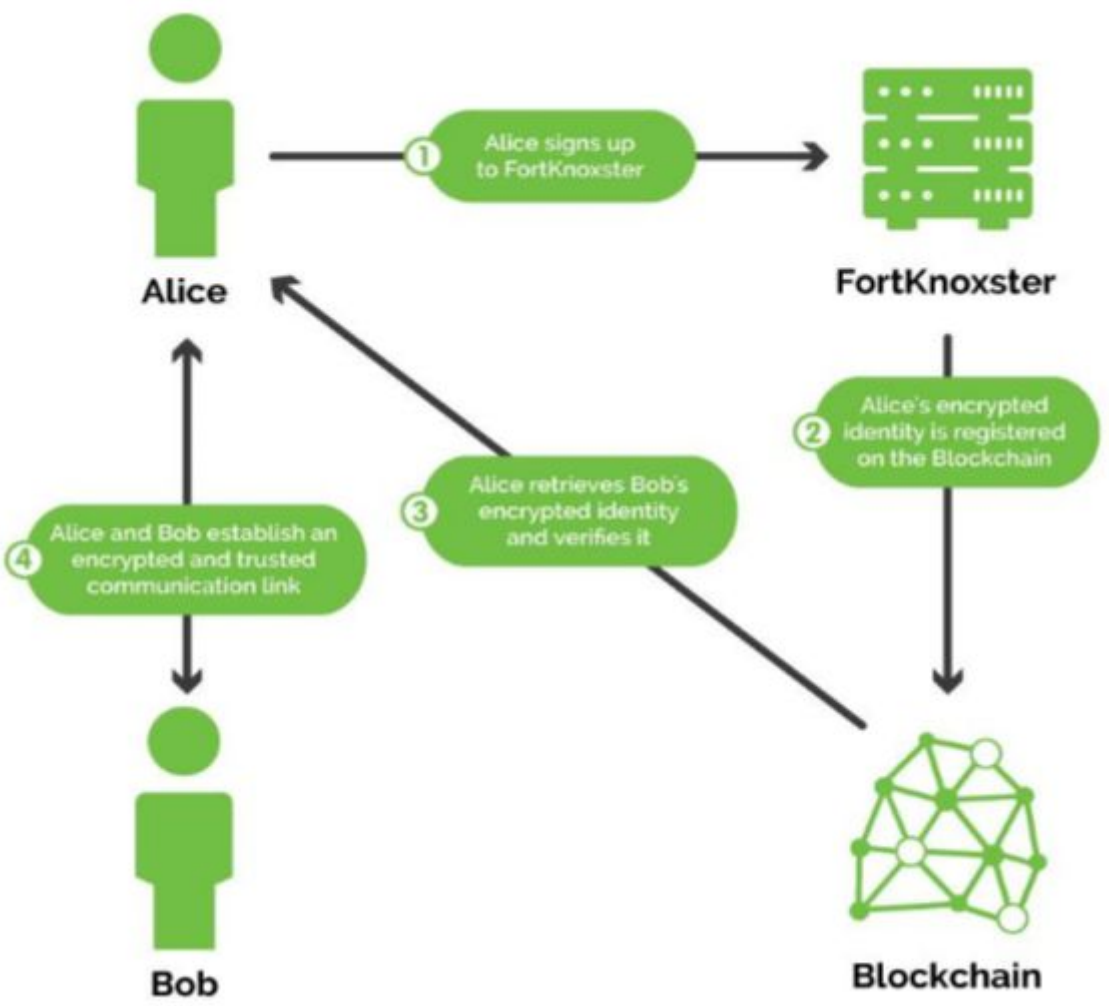
La identidad digital se construye así (en el navegador del cliente):

digital identity = User ID + Signature

Donde la Firma se calcula así:

Signature = SIGN(User ID + Public Key Fingerprint, Private Identity Key)

Se establece una sesión separada para el servidor de FortKnoxster, donde se ejecuta un nodo cliente de blockchain. El nodo recibe la identidad digital del usuario y crea una nueva transacción en la cadena de bloques que contiene la identidad digital para almacenarla en el registro de contrato inteligente.



La figura anterior ilustra, a un usuario recién registrado, Alice, configurando su identidad digital. La figura también ilustra la recuperación de la identidad digital de Bob para su verificación, antes de que pueda establecerse cualquier enlace de comunicación encriptado. Bob también habrá hecho esta verificación de la identidad digital de Alice de antemano.

Los servicios FortKnoxster consumen una gran cantidad de almacenamiento, como archivos, archivos adjuntos de mensajes y transferencias de archivos.

La infraestructura de almacenamiento completa de FortKnoxster, se construirá en un almacenamiento distribuido descentralizado en una red P2P, donde los usuarios pueden alquilar sus discos duros y ganar tokens **FKX** por uso de almacenamiento y uso de ancho de banda.

Esto es el equivalente a la minería en criptomoneda, pero en lugar de usar la CPU/GPU para extraer bloques, la capacidad disponible en el disco duro se usa para asignar almacenamiento.

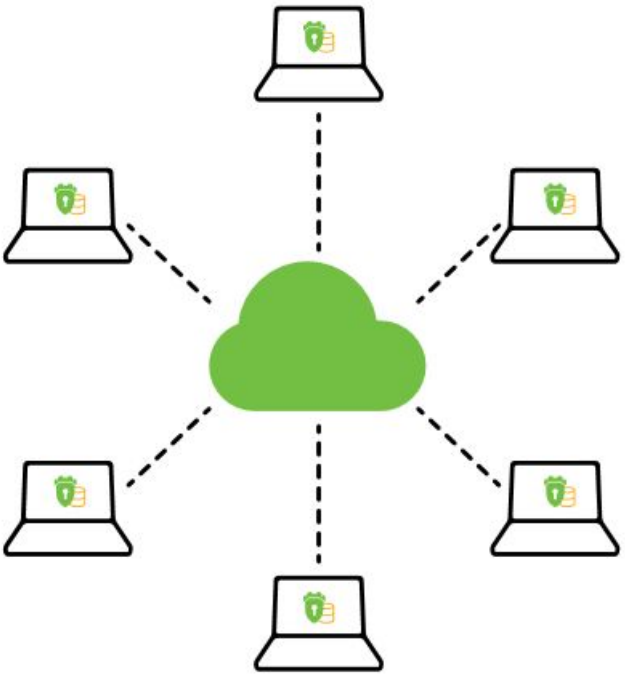
Para convertirse en un minero de almacenamiento, se requieren 3 sencillos pasos:

1) Instale el software de consola o escritorio de minero de almacenamiento, que estará disponible para los sistemas Mac / Linux / Windows.

2) Proporcione una dirección de monedero de pago de token en tecnología ERC20 para recibir pagos en **FKX**.

3) Seleccione la ubicación del disco y la cantidad de almacenamiento que puede ahorrar.

La eliminación de los servidores de almacenamiento centralizados reduce el costo de almacenamiento y mejora la velocidad de acceso y la confiabilidad. Todos los archivos cifrados se distribuyen en múltiples nodos y se replican varias veces. Ningún host único, contiene una parte importante de un archivo o cualquier archivo completo.



FortKnoxster proporciona una red tipo P2P de almacenamiento distribuido y descentralizado, donde todos los archivos se cifran de punto a punto usando claves que seguras

Los usuarios de FortKnoxster subirán archivos y archivos adjuntos desde la interfaz web y desde las aplicaciones, y estos archivos cifrados se distribuirán en el almacenamiento descentralizado, que consiste en todos los mineros de almacenamiento FKX, con una distribución equilibrada y justa.

El Ecosistema de Tokens

El token FortKnoxster (FKX) se utilizará para comprar diversos servicios y para incentivar a los usuarios a obtener diferentes recompensas.

El token **FKX** tendrá un uso claro e importante en nuestra aplicación, como un medio para incentivar un mayor desarrollo y asegurar nuestra capacidad de ejecutar y comercializar FortKnoxster en todo el mundo. La ficha **FKX** sirve para ser utilizada con el fin de los servicios FortKnoxster.

Se creará un suministro fijo para FKX durante la venta del token (135 Millones.) Se creará un libro mayor en blockchain manteniendo el token FKX, siguiendo el estándar ERC20 y permitiendo un mecanismo seguro para transferir **FKX** a otros participantes.

Los usuarios de FortKnoxster que posean tokens **FKX** podrán comprar suscripciones de servicio, tales como:

- **Almacenamiento encriptado**
  Registrarse en FortKnoxster es gratis y se asignará el almacenamiento cifrado gratuito limitado. Para aumentar el almacenamiento cifrado, el usuario deberá comprar créditos en cantidades fijas con la ficha FKX

  FortKnoxster también presentará en el futuro otros servicios y suscripciones para intercambiar por fichas FKX.

Para contribuir aún más al ecosistema de FKX, se lanzarán planes de incentivos, tales como:

- **Renta de disco duro**

  Los usuarios obtienen recompensas en el token FKX por alquilar su espacio en el disco duro como parte del almacenamiento descentralizado de FortKnoxster.

- **Referencias**

  Los usuarios obtienen una cantidad fija de tokens de FKX, invitando a otros usuarios a sumarse a la plataforma.

- **Lealtad**

  Los usuarios obtendrán recompensas con tokens FKX cuando utilicen los diversos servicios, basados en una fórmula de uso que alcanza diferentes niveles de usuario.

- **Recompensa por venta de tokens**

  Durante el período de venta del token, se usarán tokens FKX para recompensar a los usuarios de nuestra comunidad que participen activamente en nuestro programa de recompensas. Se puede encontrar más información en BitcoinTalk.org

- **Recompensa por errores.**

  Los usuarios también pueden obtener recompensas con tokens FKX enviando informes de seguridad válidos del error de PoC (Prueba de concepto). Este sistema de recompensa también funciona para hackers éticos o de guantes blancos, que participen en nuestro programa de recompensas, se deberá hacer referencia al informe enviado y al perfil del usuario.

Venta de Tokens

TÉRMINOS DE VENTA

135 Millones

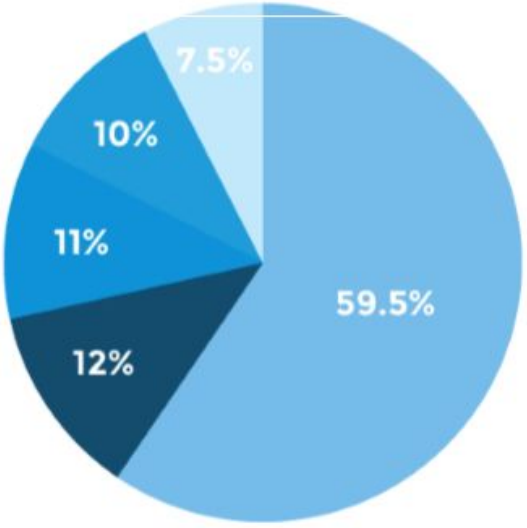
de Fichas FKX emitidas

80.325 Millones
estarán disponibles para la venta

$ 15 Millones

Máxima Capitalización de fondos

los FKX pueden ser comprados
con ETH



59.5% Venta de tokens

12% Socios y Consultores

11 % Incentivos a la comunidad

10% FortKnoxster

7.5 Fundadores

FKX es un token ETH (Se requiere wallet tipo ERC20)
La venta finaliza el 22 Dic 2017 12:00 hs CET

La venta en la etapa de "**preventa"** comenzará el miércoles, 8 de noviembre de 2017, con un descuento del 20%.

Todas las compras de preventa se manejan a través de nuestro socio simbólico **Bitcoin Suisse.**

La venta del token comenzará el viernes, 24 de noviembre de 2017 a las 12:00 CET y estará disponible aquí https://fortknoxster.com/token-sale

VALOR: **1 USD = 5.25 FKX**, donde la tarifa ETH / FKX está bloqueada de 4 a 6 horas antes de que comience la venta multitudinaria y será publicada en nuestro sitio web.

Requerimos los siguientes datos a los participantes cuando contribuyan a la venta de FKX:

- Nombre,
- Dirección
- Correo electrónico.

Se les pedirá a los participantes que confirmen que son elegibles según los términos del servicio.

MUY IMPORTANTE: *FortKnoxster NUNCA solicitará pagos a través de Telegram ni de otros medios y sitios.*

La dirección de la venta del token sólo se publicará en el sitio web oficial de FortKnoxster https://fortknoxster.com y no en otro sitio.

NUNCA envíe ningún ETH a direcciones recibidas aquí ni desde ningún otro lugar que no sea el sitio web oficial de FortKnoxster.

Todos los tokens FKX distribuidos a los fundadores y la compañía estarán bloqueados por 12 meses.

Los residentes de los Estados Unidos y Singapur no pueden participar en la venta de tokens de FortKnoxster y la distribución de tokens.

Puede participar en la venta de tokens de FortKnoxster si no es ciudadano de los EE. UU. Y Singapur ni residente permanente de los Estados Unidos o Singapur, ni tiene una residencia principal o domicilio en Singapur y los Estados Unidos, incluido Puerto Rico, las Islas Vírgenes de EE. UU. y cualquier otro territorio de los Estados Unidos.

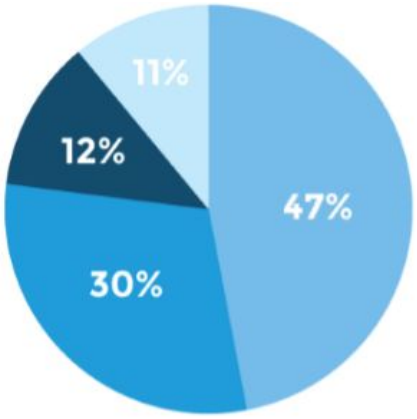
Resumen del presupuesto

47 % Ventas y marketing

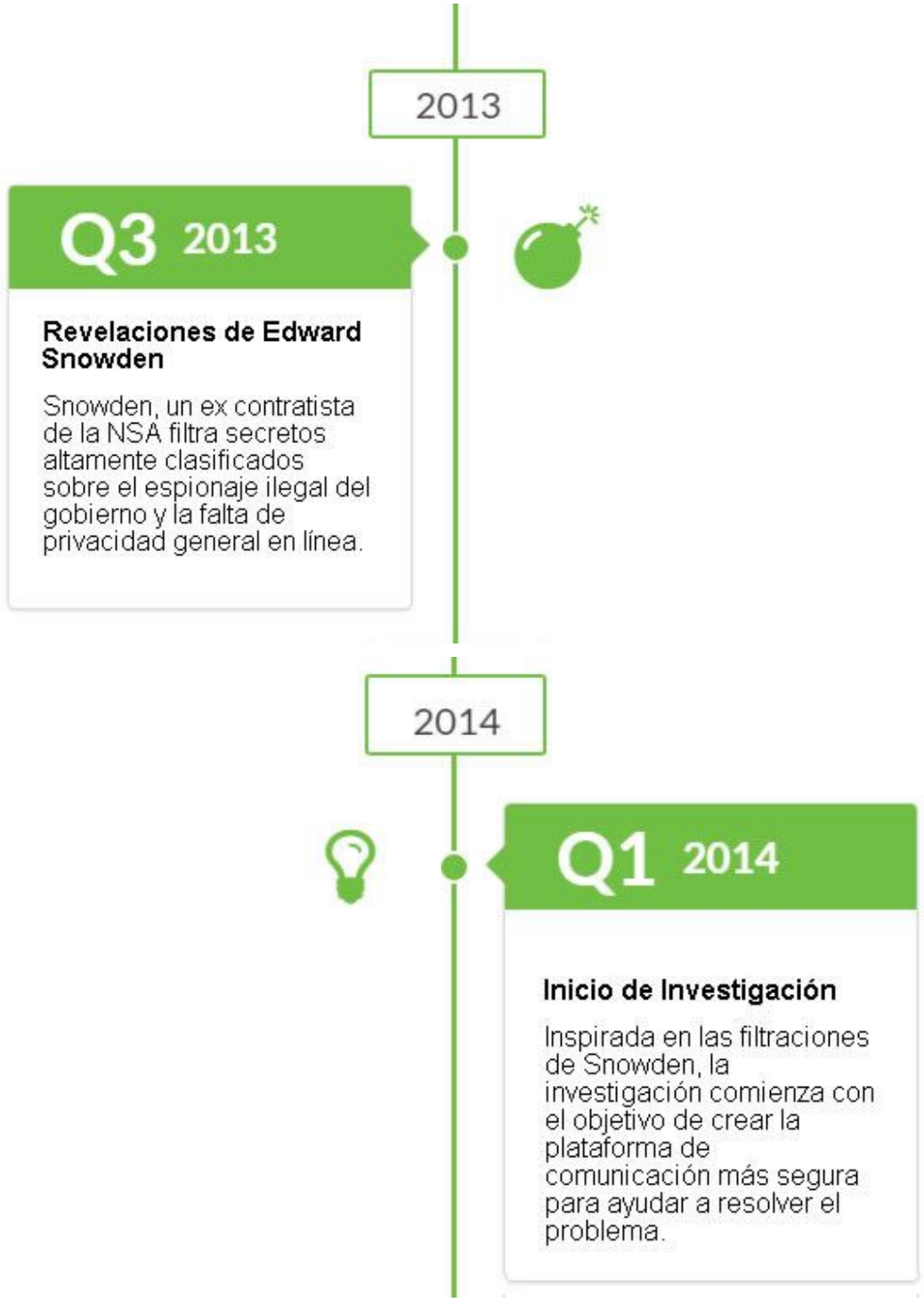
30 % Desarrollo

12 % Legal y Administración

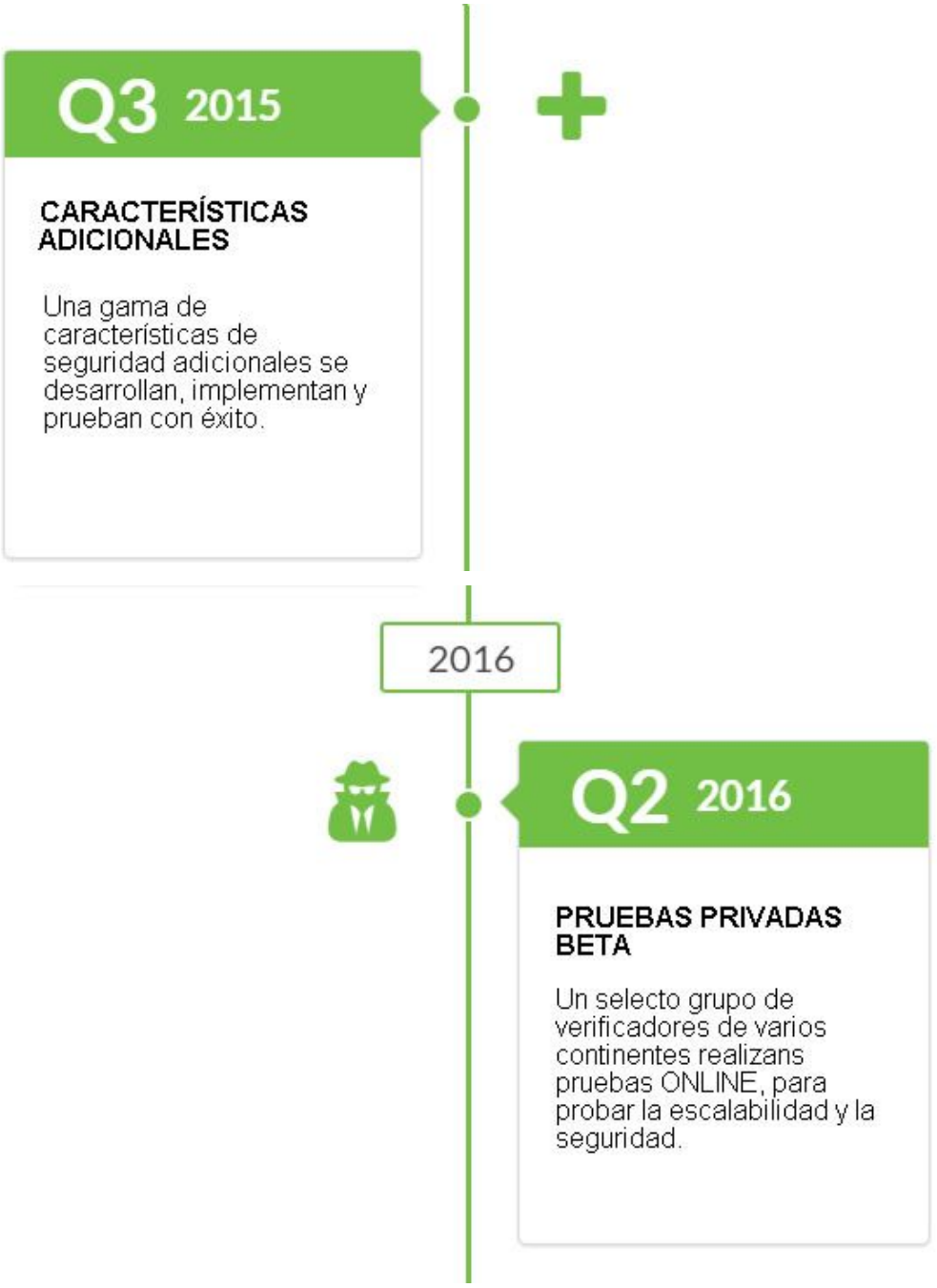
11 % Miscelaneos



Hoja de ruta de FortKnoxster




Q3 2014
Inicio del desarrollo
Arquitectura de encriptación principal y las capas de seguridad están siendo diseñadas y comienza el desarrollo inicial.
2015
Q2 2015
PRUEBAS ALFA
La primera versión alfa es probada por profesionales de seguridad y hackers de todo el mundo.


Q3 2015
CARACTERÍSTICAS ADICIONALES
Una gama de características de seguridad adicionales se desarrollan, implementan y prueban con éxito.
2016
Q2 2016
PRUEBAS PRIVADAS BETA
Un selecto grupo de verificadores de varios continentes realizans pruebas ONLINE, para probar la escalabilidad y la seguridad.


Q4 2016
USUARIOS REALES
Comienza el uso de la plataforma y las aplicaciones móviles con usuarios reales, obteniendo una excelente respuesta.
2017
Q2 2017
RE - CODIFICACION
Decidimos volver a escribir toda nuestra estructura de cifrado y código fuente para prepararnos para la integración de Blockchain y el almacenamiento descentralizado.


Q3 2017
PLANEAMOS LA VENTA DE TOKEN
Se inicia el proceso de venta de tokens y se publica el libro blanco de FortKnoxster. Se lanza la plataforma de demostración FortKnoxster.
Q4 2017
FINALIZACION DE LA VENTA DE TOKENS
La venta de tokens FKX finaliza y se distribuyen los tokens FKX.Se inicia el desarrollo del ecosistema central que utiliza contratos inteligentes en Ethereum Blockchain


2018
Q1 2018
PRUEBA DE DE LA CADENA DE BLOQUES
Se prueba la implementación FINAL de la identidad digital descentralizada, el almacenamiento descentralizado y ecosistema (pagos , lealtad, incentivos y recompensas) utilizando contratos inteligentes de Ethereum
Q2 2018
LANZAMIENTO PÚBLICO
FortKnoxster lanza oficialmente su infraestructura descentralizada Blockchain Digital Identity y la función de llamadas en grupo cifradas para la web y las aplicaciones nativas. También se lanza nuestra nueva función de invitación y referencia en el ecosistema de FKX con incentivos.

Nuestro equipo

Rasmus Birger Christiansen

CEO y Co-Fundador

Rasmus tiene más de 20 años de experiencia en telecomunicaciones y posee un título en ingeniería. Rasmus es un apasionado defensor de la privacidad, un líder fuerte y un profesional de la ciberseguridad

Mickey Joe Nathan Johnnysson

CTO y Co-Fundador

Una fuerte mentalidad analítica ha sido útil para Mickey en sus más de 15 años como desarrollador exclusivo de software. Sus principales pasiones son la ingeniería informática, las criptomonedas y el Blockchain.

René Krainert

CFO

René ha sido contador y auditor financiero durante casi 20 años. Tiene una sólida formación en finanzas y contabilidad, como contador, planificador estratégico y gurú de Excel.

Emin Roblack

Jefe de Diseño

¿Necesitas creatividad? Emin es tu hombre. Con una inclinación por el diseño, los gráficos y las animaciones, tiene un talento inestimable para convertir ideas simples en gráficos complejos.

Aram Ispiryan

Desarrollador Lìder IOS

Master en Ciencias de la Computación, Aram realiza innovaciones en comunicación. Sus puntos fuertes son los sistemas iOS que utilizan aplicaciones de audio /video y chat en tiempo real.

Armen Sisakyan

Desarrollador Lìder Android

Armen lleva el desarrollo de Android al más alto nivel de calidad y rendimiento, con un profundo conocimiento de protocolos de comunicación que sirven a millones de usuarios.

CONSULTORES

Stig Abildsø

Emprendedor e inversionista

Stig ha construido varias compañías danesas desde cero a salidas exitosas dentro del sector de TI. Es un gran emprendedor

Eddy De Heij

Emprendedor e inversionista

Con una gran cartera de inversiones en todo el mundo, Eddy es un emprendedor en serie, inversor y escritor.

Michael Vivet

Consultor Senior de TI

Michael está ayudando con el asesoramiento estratégico y táctico, así como con el desarrollo de servicios y pruebas finales.

Carlos Benvenuti

Emprendedor e inversionista

Carlos ha estado en el espacio criptográfico durante varios años y es un entrenador, asesor e inversor profesional.

Palabras finales.

FortKnoxster fué fundado por empresarios daneses y expertos en ciberseguridad, con una amplia experiencia en el campo de la seguridad en línea y la ciberdefensa. Los fundadores ya han establecido una prueba de concepto.

La plataforma FortKnoxster tiene un potencial mundial enorme y escalable. Es la primera plataforma de encriptación de punto a punto del mundo, que ofrece encriptación llave en mano con un gran conjunto de características que incluyen la implementación de blockchain.

La combinación de nuestro equipo, el modelo de negocio, el potencial de mercado extremadamente escalable y la creciente demanda de seguridad cibernética de individuos y empresas, harán de FortKnoxster un jugador líder en el mercado dentro del campo de la ciberseguridad.

Al utilizar nuestras soluciones criptográficas avanzadas combinadas con la potencia de la estructura descentralizada del blockchain, FortKnoxster ayudará a hacer del mundo un lugar más seguro, y dominaremos el mercado global de cifrado al ser la solución de cifrado "lista para usar" en cualquier lugar, y para todos.

Apéndice 1: Descripción general de la tecnología

Términos clave

A continuación se encuentra la lista de términos claves utilizados a lo largo de las explicaciones tecnológicas.

Todos los materiales clave se generan utilizando un CSPRNG (generador de números pseudo aleatorios criptográficamente seguro) inyectado con entropía de alta calidad como valores verdaderamente aleatorios utilizando la fuente de entropía del sistema operativo.

- **Contraseña de la cuenta**: clave derivada basada en la contraseña utilizada para la autenticación. Utiliza el algoritmo PBKDF2 con tecnología SHA-256 como el algoritmo de hasheo y datos aleatorios.

- **clave raíz** - Clave derivada basada en contraseña que usa el algoritmo PBKDF2 con SHA-256 como el algoritmo de hasheo y datos aleatorios. La clave derivada, se utiliza para cifrar y descifrar un Key Protector utilizando AES de 256 bits en modo KW.

- **ID de usuario**: Es un identificador único, autogenerado para identificar a un usuario en el sistema FortKnoxster y en la cadena de bloques.

- **Huella digital de clave pública**: Es un hash criptográfico único de las claves públicas del usuario utilizadas para formar la identidad digital en la cadena de bloques

- **Identidad digital**: Es un registro de clave / valor almacenado en la cadena de bloques que contiene la ID de usuario y una firma digital de la ID de usuario y la Huella digital de clave pública.

- **Clave de encriptación privada**: clave privada utilizada para el descifrado con el esquema de algoritmo RSAOAEP de 2048 bits con SHA-256 como algoritmo de hash.

- **Clave de identidad privada**: clave privada utilizada para firmar digitalmente un mensaje cifrado, utilizando el esquema de algoritmo RSASSA-PKCS1-v1_5 de 2048 bits con SHA-256 como algoritmo de hash.

- **Clave de encriptación pública**: Clave pública utilizada para el cifrado de clave AES utilizando el algoritmo RSA-OAEP de 2048 bits con SHA-256 como algoritmo hash.

- **Clave de identidad pública:** Clave pública utilizada para la verificación de la firma de mensaje utilizando el algoritmo RSASSA-PKCS1-v1_5 de 2048 bits con SHA-256 como algoritmo de hash.

- **Protector de clave**: clave de 32 bytes generada aleatoriamente utilizada para encriptar / envolver y desencriptar / desenvolver una clave privada usando encriptación tipo AES de 256 bits en modo GCM.

- **Contenedor de claves:** Es una estructura de contenedor de caja de cifrado flexible para contener una clave privada encriptada / encapsulada con su (s) Protector (es) de clave.

- **Clave de mensaje**: clave de 32 bytes generada aleatoriamente de una sola vez que se utiliza para el cifrado y descifrado de mensajes y archivos mediante el cifrado AES de 256 bits en modo CBC o modo GCM.

- **Clave de grupo:** clave de sesión de 32 bytes generada aleatoriamente utilizada para el cifrado y descifrado de mensajes grupales mediante el cifrado AES de 256 bits en modo GCM

Pares Claves

Son los pares de claves RSA utilizados para el cifrado y descifrado, cada uno consiste en una clave de cifrado público y una clave de cifrado privado y utiliza el esquema de algoritmo RSA-OAEP de 2048 bits con tecnología SHA-256 como algoritmo de hash.

Los pares de claves RSA utilizados para la firma y la verificación, cada uno consta de una clave de identidad pública y una clave de identidad privada y utiliza el esquema de algoritmo RSASSA-PKCS1-v1_5 de 2048 bits con tecnología SHA-256 como el algoritmo hash.

El par de claves, EC utilizado para derivar una clave secreta compartida, en un acuerdo de clave, consta de una clave pública y una clave privada y utiliza el algoritmo ECDH P521-bit.

El par de claves EC utilizado para la firma y verificación,consiste en una clave de identidad pública y una clave de identidad privada y utiliza el algoritmo ECDSA P521-bit.

Contactos e Intercambio de Claves

Un problema común en los sistemas de encriptación es el intercambio de clave segura de claves públicas entre usuarios, asegurándose de que la clave obtenida realmente pertenezca al destinatario deseado.

FortKnoxster, protege contra tales ataques conocidos como “Hombre en el medio” o Man-In-The-Middle (MITM) potenciales, aprovechando la tecnología blockchain junto con una lista de contactos autofirmados.

Un usuario puede invitar a otros usuarios a la plataforma o conectarse con cualquier usuario existente en la plataforma.

Cada usuario mantiene una lista de contactos donde cada registro de contacto está firmado digitalmente con la clave de identidad privada del usuario y contiene todos los detalles de contacto, como el nombre, la identificación del usuario y las claves públicas. El contacto se firma durante un proceso de solicitud y/ aceptación de contacto.

Este proceso implica recuperar la identidad digital del contacto del blockchain y verificarlo en el cliente al computar la misma huella digital de clave pública de los contactos y luego verificar la firma con la clave de identidad pública del contacto.

Una vez que se verifica el contacto, se firma y se agrega a la lista de contactos del usuario. A partir de ese momento, el usuario puede confiar en este contacto y verificar el contacto antes de usar sus claves públicas para intercambiar mensajes, archivos o llamadas.

Si la verificación de contacto falla, el intercambio de mensajes con ese contacto no se lleva a cabo y se alerta al usuario con una advertencia.

Intercambio de Mensajes

Cuando un usuario envía un mensaje a la bandeja de entrada o un mensaje de chat a otro usuario, sucede lo siguiente en el cliente del usuario emisor:

1. Si había archivos adjuntos, ya se han cifrado con su propia clave de mensaje generada y se ha tomado una Mac del archivo cifrado utilizando el algoritmo HMAC con SHA-256 y la clave de mensaje del archivo. Y en este punto, los archivos adjuntos encriptados ya han sido cargados en los servidores y se ha asignado una identificación única a cada archivo adjunto.

2. A continuación, se genera una nueva clave para el objeto de mensaje.

3. Un mensaje simple con cualquier adjunto, ya sea metadato, o archivos, o firmas HMAC y/o IDs son cifrados y se codifican con la clave de mensaje del mensaje.

4. El texto cifrado (mensaje encriptado) se firma utilizando la clave de identidad privada del usuario remitente.

   a. Antes de firmar el texto cifrado, la clave de identidad privada se descifra primero con el “Key Protector” del usuario, que se descifró en el navegador del cliente con la clave raíz y se almacenó en el almacenamiento de la sesión del navegador cuando el usuario inició sesión.

5. La clave de mensaje utilizada para encriptar el mensaje se cifra luego usando la Clave de encriptación pública del usuario receptor.
   a. Si un mensaje tiene múltiples destinatarios, este proceso en el punto 5) se repite con la Clave de encriptación pública de cada destinatario.

6. El mensaje cifrado, la firma del mensaje y las claves del destinatario cifrado se envían a los servidores donde están almacenados.

7. Antes de almacenar el mensaje, la aplicación del servidor verifica cada mensaje en caso de alteración del mismo. Esto se hace usando la clave de identidad pública del usuario remitente.

Cuando un usuario recibe un mensaje nuevo en su bandeja de entrada o un mensaje de chat, sucede lo siguiente en el cliente del navegador del usuario.

1. La firma del mensaje cifrado se verifica con la clave de identidad pública del usuario remitente.

2. La clave de mensaje cifrada se descifra con la clave de encriptación privada del usuario.

   a. Antes de descifrar el texto cifrado, la clave de cifrado privado se descifra primero con el “Key Protector” del usuario que se utilizó navegador del cliente con la clave raíz y se almacenó en el registro de sesiones del navegador cuando el usuario inició sesión.

3. La clave de mensaje recuperada se usa para descifrar el mensaje cifrado.

4. Si hubiera archivos adjuntos, el usuario receptor puede descargar cada archivo adjunto encriptado que se verificará para ver si mantiene su integridad con HMACSHA256 usando la clave de mensaje y luego se descifrará utilizando la misma clave de mensaje.

Los mensajes de chat grupales están diseñados para manejar una gran cantidad de miembros y una gran cantidad de mensajes. Esto se logra con una distribución del lado del servidor, lo que significa que un usuario envía un solo mensaje al servidor y el servidor envía una copia del mensaje a cada miembro del grupo. Este diseño transmite la menor cantidad de datos posible.

Cuando se crea un chat grupal ocurre lo siguiente:

1. El usuario que crea genera una clave de grupo.

2. La Clave de grupo luego se cifra con la Clave de encriptación pública de cada miembro.

Para todos los mensajes posteriores al grupo:

1. El remitente recupera la Clave de grupo descifrándola con la Clave de encriptación privada.

2. El remitente encripta el mensaje simple con la clave de grupo usando el modo GCM, que permite la autenticación de mensajes durante el cifrado y el descifrado.

3. El remitente firma el mensaje cifrado con su clave de identidad privada.

4. El remitente transmite el mensaje cifrado y la firma al servidor, que hace una distribución en el lado del servidor a todos los miembros del grupo

Los mensajes de chat en grupo, también son la base para el protocolo de señalización de llamadas grupales que ocurre en el mismo canal de chat grupal XMPP.

Almacenamiento en la nube y uso compartido de archivos

Los archivos y los adjuntos más grandes también están encriptados de extremo a extremo.

Los archivos adjuntos (documentos, imágenes, videos, etc.) hacen referencia a los archivos adjuntos de la bandeja de entrada y las transferencias de archivos de chat, y se codifican de la misma manera, con una clave de mensaje por archivo que utiliza el modo CBC. A continuación, se calcula una firma MAC utilizando el algoritmo HMAC con tecnología SHA-256 y la propia clave de mensaje del archivo como la clave para la función HMAC.

Los archivos de almacenamiento en la nube, están encriptados de la misma manera, sin embargo, para poder manejar grandes cargas de archivos, los archivos se fragmentan en archivos más pequeños y se encriptan con una clave de mensaje usando el modo GCM.

Se generaron dos conjuntos adicionales de pares de claves RSA específicamente para el uso del almacenamiento en la nube y el uso compartido de archivos y carpetas.

La estructura del árbol de carpetas se mantiene en estructuras de carpetas tipo JSON separadas que contienen punteros de identificación y claves AES para sus carpetas y archivos secundarios. Esas estructuras en JSON están encriptadas con una clave de mensaje usando el modo GCM y están firmadas con la clave de identidad privada del usuario. La clave AES aleatoria junto con una ID única se mantiene en la estructura de carpeta primaria JSON que también está encriptada y firmada.

Cuando un usuario comparte una carpeta con otros usuarios, la clave de mensaje para la estructura JSON se cifra con la clave de cifrado público de cada usuario y la estructura JSON cifrada se firma con la clave de identidad privada del usuario que comparte.

El usuario que comparte es el propietario de la carpeta compartida y puede definir permisos de lectura y escritura para cada miembro de la carpeta.

Llamadas y conferencias

Las llamadas individuales de audio o video, las llamadas grupales y el uso compartido de pantalla también se codifican de extremo a extremo y utilizan la tecnología WebRTC para la comunicación de audio y video en tiempo real.

WebRTC, utiliza el protocolo de transferencia segura en tiempo real (DTLS-SRTP) para establecer y codificar flujos de medios.

Antes de que se establezca una llamada de igual a igual entre dos o más usuarios, se realiza una marcación para intercambiar cierta información y configurar la llamada.

Esta señalización se realiza a través del canal Chat / XMPP existente y también se codifica de extremo a extremo utilizando el mismo esquema de cifrado para el intercambio de mensajes con AES / RSA como se describió anteriormente.

Aplicaciones nativas de Android y iOS

Las aplicaciones de Android e iOS contienen las mismas funciones de bandeja de entrada, chat, chat grupal y llamada del cliente web, se integran estrechamente con el sistema y recibirán notificaciones automáticas sobre diversos eventos, como los mensajes de la bandeja de entrada y los mensajes de chat y las llamadas entrantes.

El cifrado de extremo a extremo se diseña y desarrolla utilizando la misma encriptación y algoritmos fuertes que en los clientes de navegador. Para las aplicaciones de iOS y Android, la capa de cifrado de extremo a extremo se ha desarrollado como una única biblioteca multiplataforma escrita en lenguaje C ++ que utiliza la última distribución de OpenSSL y que se utiliza en ambas aplicaciones.

Criptografía API para WEB

Los navegadores web implementan las últimas capacidades del navegador y utilizan la API de criptografía Web (Web Crypto API), que es un estándar web definido en el World Wide Web Consortium (W3C) que permite operaciones criptográficas en aplicaciones de cliente web de JavaScript.

El uso de criptografía Web mediante la API hace que el diseño criptográfico y su implementación sean altamente estables y eficientes al realizar varias operaciones criptográficas, ya que aprovecha la implementación de la propia pila criptográfica del navegador y hace que los algoritmos criptográficos robustos estén disponibles, en comparación con otras implementaciones crypto de JavaScript puro.

Seguridad web

Los ataques de script de comandos (XSS) son probablemente los ataques más extendidos en las aplicaciones web y suceden cuando los scripts maliciosos se inyectan en los sitios web para dirigirse a los usuarios finales.

El objetivo de un ataque XSS, es hacer que algunas secuencias de comandos del navegador se ejecuten en el navegador de la víctima en sitios infectados y robar información sensible como una cookie de sesión de un usuario autenticado y luego enviarla de vuelta al servidor del atacante. El atacante puede obtener acceso a la cuenta de la víctima en ese sitio web específico utilizando esta cookie de sesión. Tal ataque puede hacerse sin que la víctima lo sepa.

Este tipo de ataque se ha realizado en servicios bien conocidos como WhatsApp, donde el atacante pudo conectar por completo a la cuenta de WhatsApp de su víctima y poder controlar la cuenta de esa víctima.

Los sitios web y las aplicaciones web son vulnerables a los ataques XSS, normalmente cuando las entradas de los usuarios no se filtran correctamente.

FortKnoxster, implementa varias medidas de seguridad para garantizar que nuestros usuarios estén protegidos contra cualquier tipo de ataque XSS, asegurándose de que las entradas de los usuarios, tales como a una bandeja de entrada o un mensaje de chat, es enviado y verificada su seguridad antes de mostrarlo, en el navegador del receptor. Además, nuestra aplicación web y configuraciones de servidor se han optimizado para establecer los marcadores de cookies **HTTPOnly**, **X-XSS-Protection** y **Content-Security-Policy.**

Nuestra investigación en **Content Security Policy** (CSP) ha resultado en una configuración de CSP muy estricta, al no permitir que se cargue ningún tipo de fuentes externas dentro del entorno de FortKnoxster.

CSP es compatible con todos los navegadores modernos y protege contra XSS al incluir en una lista blanca, las fuentes permitidas de script, estilo, medios y otros recursos cuando visita un sitio web.

Para tener este tipo de protección, las configuraciones de CSP deben realizarse en las configuraciones del servidor web y es un encabezado de respuesta especial (Política de

seguridad de contenido) enviado desde el servidor de vuelta al navegador, cuando se solicita una página.

Hemos tomado estas medidas de seguridad adicionales, para asegurarnos de que nuestras configuraciones de CSP, sean lo más estrictas posible al incluir solo recursos internos en la lista blanca y, por lo tanto, poner en lista negra cualquier tipo de carga externa de recursos en el navegador del cliente al visitar nuestro sitio web y utilizar nuestros servicios.y, por lo tanto, hacer cumplir la privacidad de nuestros usuarios.

La falsificación de solicitudes entre sitios (CSRF / XSRF) es un tipo especial de ataque, donde el atacante puede engañar a la víctima para que realice acciones no deseadas, como autorizar una transferencia bancaria.

FortKnoxster, evita las vulnerabilidades CSRF al incluir un token de sesión único en cada solicitud HTTP y una cookie especial XSRF.

Además, la cookie de sesión de FortKnoxster, está encriptada con AES-CBC de 256 bits y un MAC utilizando la función HMAC, tomando como clave una clave de servidor.

El phishing es un tipo de ataque de ingeniería social. El atacante se enmascara como el sitio confiable, engañando a la víctima para que realice acciones no deseadas, como robar credenciales de inicio de sesión, detalles de tarjetas de crédito y otros datos confidenciales.

FortKnoxster, implementa varias medidas de seguridad para prevenir también este tipo de ataques.

Seguridad de la cuenta

Para proteger a los usuarios de cualquier tipo de ataque de su cuenta, FortKnoxster impone varias medidas de seguridad y ofrece las siguientes características de seguridad de cuenta:

- Autenticación de dos factores con TOTP, SMS y FIDO U2F.
- Restringir el acceso a la cuenta por IP y país.
- Registro de auditoría de seguridad.
- Web Application Firewall (WAF) filtrado de solicitudes web.
- Bloqueo automatizado de cuentas cuando se detectan ataques de fuerza bruta u otros abusos.

Seguridad de la capa de transporte

Toda la comunicación entre los clientes (navegadores web, aplicación de Android, aplicación de iOS) y los servidores se distribuyen en capas con un canal de cifrado estricto separado adicional. Solo TLS 1.2 es compatible y está configurado con las suites de cifrado

más sólidas disponibles, incluido un parámetro Diffie-Hellman de 4096 bits para suites de cifrado DHE.

Las sólidas configuraciones de TLS permiten HTTP Strict Transport Security (HSTS), OCSP Stapling, Forward Secrecy y protegen contra todos los ataques conocidos como Bestia, Heartbleed, Poodle y muchos más.

Descripción del algoritmo

A continuación se muestra una descripción general de los algoritmos de cifrado y las operaciones de criptografía utilizadas en el diseño criptográfico de cifrado de extremo a extremo de FortKnoxster.

Algorithm	Encrypt	Decrypt	Sign	Verify	Derive	Digest	Wrap	Unwrap
RSASSA-PKCS1-v1_5			✓	✓				
RSA-OAEP	✓	✓						
ECDSA			✓	✓				
ECDH					✓			
AES-CBC	✓	✓						
AES-GCM	✓	✓					✓	✓
AES-KW							✓	✓
HMAC			✓	✓				
PBKDF2					✓			
BCRYPT					✓			
SHA-256						✓		

Apéndice 2: La próxima ley GDPR

A continuación hay una breve descripción de la próxima ley GDPR. FortKnoxster, es una herramienta buena y relevante para cumplir con la estricta ley GDPR y es fácil de implementar en cualquier organización independientemente del tamaño y la industria.

El Reglamento general de protección de datos (GDPR) (Reglamento (UE) 2016/679), es un reglamento por el cual el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea se proponen fortalecer y unificar la protección de datos para todas las personas dentro de la Unión Europea (UE).

Las empresas necesitan urgentemente que sus operaciones cumplan con el nuevo régimen de protección de datos. Aquí están los detalles más importantes del GDPR.

Cuando

La ley entrará en vigencia el 25 de mayo de 2018, después de lo cual comenzará la ejecución contra las entidades que no cumplan. Hasta entonces, se aplican las leyes nacionales de protección de datos existentes, que incluyen leyes de seguridad nacional o leyes de empleo y libertad de expresión.

Quien

El nuevo Reglamento europeo de protección de datos se aplica a cualquier empresa, independientemente de su actividad comercial o sector de la economía, si:

una empresa se establece en la UE o está sujeta a las leyes de la UE.
una empresa se establece fuera de la UE, pero

a) Ofrece servicios o bienes a los residentes de la UE;
b) supervisa el comportamiento de los residentes de la UE.

Por ejemplo, la "aplicación Runkeeper" que rastrea a sus usuarios europeos es responsable, a pesar de que es una empresa norteamericana sin una oficina en la UE.

El Reglamento Europeo de Protección de Datos introduce una expansión significativa de las empresas responsables y ahora se aplica a las entidades no europeas que se ocupan de los datos privados de los residentes europeos.

Esto también significa que los gigantes tecnológicos como Google, Facebook, Yahoo y Microsoft tendrán que cumplir. De lo contrario, las implicaciones incluyen fuertes multas.

Multas

El incumplimiento del Reglamento Europeo de Protección de Datos genera multas. La multa máxima por una infracción única es de 20 millones de euros o el 4% de la facturación global anual, cualquiera que sea mayor. El monto se establece intencionalmente alto para atraer la atención de la C-suite hacia el problema de la protección de datos y el cumplimiento de la nueva regulación.

El cifrado es la solución

El reglamento GDPR brinda sugerencias específicas sobre qué tipos de acciones de seguridad se pueden considerar "apropiadas para el riesgo", que incluyen:

> **Cifrado de datos personales**.
> La capacidad de garantizar la confidencialidad, integridad, disponibilidad y flexibilidad constantes de los sistemas y servicios que procesan datos personales.
>
> La capacidad de restablecer la disponibilidad y el acceso a los datos de manera oportuna en caso de un incidente físico o técnico.
>
> Un proceso para probar, evaluar y evaluar regularmente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento.

Si bien el Reglamento Europeo de Protección de Datos trae buenas noticias principalmente a los usuarios finales, no todas son malas noticias, esto es más trabajo y mayores gastos para las empresas. Hay una pieza particularmente valiosa en la regulación que estipula que las compañías deben cumplir con las "expectativas razonables de privacidad de datos" de los usuarios. La regulación luego sugiere que el cifrado, el anonimato y los tokens de autorización cumplen con esas expectativas. Si su compañía encripta datos corporativos y datos de usuarios en reposo y en tránsito, también cuando trata con contratistas externos y mantiene las llaves en las instalaciones de la empresa, seguras y encriptadas, también, demostrará efectivamente que cumple con las "expectativas razonables". de privacidad "de un individuo.

Apéndice 3: Términos del servicio

Términos de servicio

Vigente: 1 de agosto de 2017

Estos Términos de Servicio ("Términos") cubren su uso y acceso al Servicio llamado "FortKnoxster", ("Servicio") provisto por FortKnoxster Ltd. Al utilizar nuestros Servicios, usted acepta estar sujeto a estos Términos, y le pedimos que también revise nuestras políticas de privacidad. Si está utilizando nuestros Servicios para una organización u otra entidad legal, está aceptando estos Términos en nombre de esa organización. FortKnoxster Ltd. se reserva el derecho de cambiar este acuerdo en cualquier momento.

El servicio FortKnoxster

El Servicio FortKnoxster, proporciona un sistema que permite a un usuario acceder a nuestra plataforma de comunicación segura llamada FortKnoxster. Para recibir el Servicio, deberá crear una cuenta que conste de una dirección de correo electrónico y una contraseña.

Acceso

Para acceder a su cuenta, primero debe iniciar sesión con su nombre de usuario y contraseña de FortKnoxster, y luego pasar por el proceso de verificación. Después de esto, usted tiene acceso para usar el Servicio. El uso del Servicio requiere que obtenga acceso a Internet. Puede acceder desde una computadora o un dispositivo móvil.

Seguridad de la cuenta

Al completar el registro de este Servicio, usted acepta estar sujeto a estos Términos y condiciones y a la Política de privacidad de FortKnoxster, garantiza que tiene al menos dieciocho (18) años o que ha obtenido el consentimiento para abrir y mantener una cuenta de sus padres. Usted acepta mantener la seguridad de su contraseña e identificación, y será completamente responsable de todo el uso del Servicio FortKnoxster. Deberá notificar inmediatamente a FortKnoxster Ltd sobre cualquier uso no autorizado de su contraseña o cuenta, de cualquier pérdida o robo de su contraseña o de cualquier otra violación de seguridad.

Uso Permitido

Puede acceder y usar el Servicio de acuerdo con estos Términos y condiciones y sujeto a las reglas de operación y contrato o políticas publicadas que aparecen en el sitio web. Cualquier uso del Servicio es bajo su propio riesgo y responsabilidad.

No se permite uso ilegal

Usted declara y garantiza, como condición de uso del Servicio, que no utilizará el Servicio para ningún fin que sea ilegal, ilegal o prohibido. No deberá someter el sistema TEP a ningún tipo de spam, ataques de denegación de servicio, virus o cualquier acción, actividad o código que pueda interferir con el funcionamiento normal del sistema.

Indemnizaciones

Usted acepta defender, indemnizar y mantener a FortKnoxster Ltd., sus subsidiarias y afiliadas y directores, funcionarios, agentes, contratistas, accionistas, socios y empleados, libres de y en contra de cualquier acción, reclamo, demanda u obligación, que surja de o en relación con su violación de cualquiera de los Términos y Condiciones de este acuerdo, los derechos de cualquier tercero o su uso o conexión a este Servicio.

Ell Servicio se proporciona "tal cual" y usted acepta no responsabilizar a FortKnoxster Ltd. por los daños y perjuicios que surjan como resultado de la pérdida de uso, datos, información o ganancias relacionadas con la prestación del Servicio. Además, no responsabilizará a FortKnoxster Ltd., si algún material se libera involuntariamente como resultado de una falla de seguridad, vulnerabilidad o fuerza mayor.

Contraseña

Como no tenemos acceso a su cuenta o datos, no guardamos registros de su contraseña. Si pierde su contraseña, no podemos ayudarlo más que ofrecerle una nueva cuenta.

Cuentas Pagas

Facturación. Le cobraremos automáticamente desde la fecha en que active una cuenta de usuario y en cada renovación periódica hasta la cancelación. Usted es responsable de todos los impuestos aplicables, y le cobraremos impuestos e IVA cuando sea necesario para hacerlo.

Sin reembolsos. Puede cancelar su cuenta de actualización FortKnoxster en cualquier momento, pero no recibirá un reembolso.

Degradaciones Su cuenta de actualización permanecerá en vigencia hasta que se cancele o finalice según estos Términos. Si no paga su cuenta de actualización a tiempo, nos reservamos el derecho de suspenderla o reducir su cuenta a una cuenta gratuita.

Cambios Podemos cambiar los aranceles vigentes, pero le avisaremos con antelación de estos cambios a través de un mensaje a la dirección de correo electrónico asociada a su cuenta.

Propiedad intelectual

FortKnoxster Ltd. posee todos los derechos, títulos e intereses en y para todos los derechos de autor, marcas comerciales, secretos comerciales, patentes o cualquier otra propiedad intelectual de cualquier tipo o cualquier derecho de propiedad en y para el Servicio y estos derechos e intereses están protegidos a la máxima medida en virtud de las leyes suizas e internacionales. Sin el consentimiento previo por escrito de FortKnoxster Ltd., no deberá usar ni permitir que un tercero use ninguna marca comercial o nombre comercial, y ningún contenido de este Servicio puede copiarse, reproducirse o duplicarse de ninguna forma ni por ningún medio.

Acuerdo Total

Estos Términos y condiciones establecen el acuerdo completo con respecto al objeto del presente y reemplazan todas las comunicaciones y propuestas anteriores o contemporáneas, ya sean electrónicas, orales o escritas, entre usted y FortKnoxster Ltd

Renuncia

La falla de FortKnoxster Ltd. para ejercer o hacer cumplir cualquier derecho o disposición de estos Términos y Condiciones no constituirá una renuncia a tal derecho o disposición.

Ley aplicable

Este Acuerdo se regirá e interpretará según las leyes de Gibraltar. Todas las acciones iniciadas en virtud del presente se presentarán ante un tribunal de Gibraltar.

Cambios

Si FortKnoxster Ltd. está involucrado en una futura fusión, adquisición, reorganización o venta de nuestros activos, su información puede ser transferida como parte de esto. Le notificaremos (por ejemplo, a través de un mensaje a la dirección de correo electrónico asociada con su cuenta) de cualquier trato y esquema en detalle.

Efecto

Este acuerdo entra en vigencia en la fecha de su registro completo en FortKnoxster Ltd., o en la fecha del primer pago, y FortKnoxster Ltd. puede rescindir este Servicio en cualquier momento. El uso del Servicio es su consentimiento a los Términos de este acuerdo.

Atención al cliente

Responderemos a las solicitudes de soporte por correo electrónico dentro de un día hábil. Si tiene preguntas, ideas o inquietudes sobre nuestros Servicios, contáctenos a info@FortKnoxster.com.

Apéndice 4: Política de privacidad

POLÍTICA DE PRIVACIDAD

Vigente: 1 de agosto de 2017
La privacidad es nuestro negocio

FortKnoxster Ltd. valora, respeta y respalda la privacidad y el anonimato de todos nuestros usuarios y se compromete firmemente a proteger la seguridad e integridad confidenciales de cualquier información de acuerdo con esta Política de privacidad. Esta Política de Privacidad explica el manejo de su información por parte de FortKnoxster Ltd.

Protegiendo su información

En general. La seguridad de su información es imprescindible para nosotros, de hecho, este es el núcleo de nuestro modelo de negocio, para proteger la privacidad de nuestros usuarios y sus datos. Dentro de los límites técnicos y legales, seguiremos innovando y superando los límites para mantener la mejor plataforma de comunicación privada y segura.

Técnicamente. Utilizamos métodos de seguridad físicos, electrónicos y sofisticados para evitar el acceso no autorizado, mantener la privacidad de los datos y garantizar la protección correcta de la información. Utilizamos tecnologías de encriptación robustas que incluyen protocolos AES 256, RSA 2048, algoritmos de autenticación clave, capa de sockets seguros (SSL), etc.

Todos los datos de nuestros usuarios se almacenan en forma encriptada y ni siquiera el personal de FortKnoxster Ltd. tiene acceso a ellos en absoluto. Además, las cuentas de usuario están protegidas por autenticación multifactor (**opcional**).

Legalmente. Nuestros servidores están alojados en un centro de datos altamente seguro en Suiza. Además, nuestros Secure Sockets Layers (SSL) también son de origen suizo y, por lo tanto, están protegidos por las estrictas leyes de privacidad suizas, lo que significa que FortKnoxster Ltd. no puede ser obligado a ninguna intercepción legal u otro ataque a la privacidad. Una vez más, incluso si los datos se vieran comprometidos, no serviría de nada, ya que todos los datos están altamente encriptados. También nos referimos a la sección de No Divulgación a continuación.

Recopilación de datos

FortKnoxster Ltd. recopila y usa información anónima del usuario para los siguientes propósitos limitados:

1. **Mensajes enviados y recibidos**: no tenemos acceso a ningún contenido de mensaje, ya que está altamente encriptado. Tenemos acceso a los siguientes registros: cantidad de mensajes enviados, espacio de almacenamiento utilizado, número total de mensajes, última hora de inicio de sesión e inicio de sesión de código de país.

2. **Correos electrónicos**: Todos los correos electrónicos que se nos brindan durante el procedimiento de creación de la cuenta son información confidencial y su correo electrónico nunca será vendido, compartido, entregado, arrendado o divulgado a terceros. Debido a cuestiones de seguridad adicionales, se requiere su correo electrónico para enviarle el enlace inicial en el proceso de creación de la cuenta.

Administrando tus datos

Sus datos le pertenecen y puede eliminarlos en cualquier momento. La información de su cuenta se puede cambiar en cualquier momento iniciando sesión en su cuenta y cambiando o eliminando información. Si desea eliminar su cuenta, borraremos todos sus datos de cuenta cifrados restantes de nuestros servidores. Cualquier cuenta gratuita que esté inactiva por un período de más de 12 meses puede ser eliminada automáticamente.

Almacenamiento de datos

Todos los datos están en un momento dado almacenados en formato encriptado. Las copias de seguridad temporales también están totalmente encriptadas. No tenemos forma de acceder a sus datos cifrados y, por lo tanto, no podemos recuperar su contraseña en caso de que la pierda.

No divulgación

FortKnoxster Ltd. tiene una política de divulgación cero. No responderemos a ninguna solicitud de las autoridades con respecto a información sobre usuarios, registros, datos o similar. Cualquier autoridad debe dirigir una solicitud a las autoridades pertinentes, que luego pueden contactarnos, siguiendo el protocolo que estipula la legislación pertinente. No cumpliremos con las demandas de ninguna autoridad en mayor medida de lo que exige la ley.

Pagos

Esto se aplica solo a los usuarios que usan nuestros servicios de "actualización". Los terceros procesan todas las transacciones de pago electrónico y FortKnoxster Ltd. no retiene ninguna información de pago del cliente. Para fines de administración, necesitamos almacenar datos sobre qué cuenta fue pagada por una transacción en particular.

Atención al cliente

Responderemos a las solicitudes de soporte por correo electrónico dentro de un día hábil. Si tiene preguntas, ideas o comentarios sobre nuestros Servicios, contáctenos a info@FortKnoxster.com.

THANKS FOR YOUR INTEREST

For more information:
www.fortknoxster.com or e-mail:
tokensale@fortknoxster.com