Especificación Técnica

Sistema de Mensajería Instantánea Segura

Objeto

Dotar de un Sistema de Mensajería Instantánea Segura para sus autoridades logísticas y operacionales a los efectos de resguardar la información, manteniendo la agilidad que entrega la mensajería instantánea.

Alcance

La provisión deberá abarcar íntegramente todos los equipos centrales (servidor y conectividad) y software que componen un Sistema de Mensajería Instantánea Segura más su instalación, configuración, puesta en marcha, pruebas, capacitación del personal asignado y garantía y soporte técnico del Sistema.

Descripción

Se requiere un Sistema de Mensajería Instantánea Segura, que permite el envío y recepción de mensajes de texto cifrados en tiempo real desde teléfonos celulares con Sistema Operativo Android, utilizando una red de datos, ya sea WI-FI o una red de datos móviles 3G, 4G, LTE, etc.

El Sistema debe haber sido diseñado con énfasis en la privacidad y la seguridad.

Por defecto, el Sistema debe cifrar la base de datos de mensajes en el dispositivo del usuario, así como ambos extremos de la comunicación, con el objetivo de proteger todos los mensajes que son enviados a otros usuarios.

Se debe implementar cifrado por defecto, utilizando un algoritmo del tipo Double Ratchet, o similar.

El servidor del Sistema de Mensajería Instantánea Segura debe ser instalado en un Centro de Cómputos o locación controlada por el cliente.

El Sistema debe contar con un servidor centralizado que además de enrutar los mensajes también facilite el intercambio automático de las claves públicas de los usuarios.

Todas las comunicaciones entre el cliente y el deben estar protegidas por un canal de comunicación cifrado.

El Sistema debe tener la posibilidad de ser configurado para distintos plazos de persistencia tanto de la información contenida en los mensajes como de la metadata de los mismos. En particular se debe implementar la posibilidad de que los identificadores solo se conserven en los servidores el tiempo que sea

necesario para transmitir cada mensaje y que los servidores no mantengan registros permanentes sobre quién llamó a quién ni cuándo.

El protocolo de cifrado de extremo a extremo estará diseñado para evitar que terceros (incluyendo los administradores del Sistema) tengan acceso al texto sin formato de mensajes o llamadas. Incluso si las claves de cifrado desde el dispositivo de un usuario resulten físicamente comprometidas, no podrán ser usadas para descifrar mensajes transmitidos previamente.

Encriptación

El Sistema de Mensajería Instantánea Segura debe utilizar un mecanismo para encriptación end-to-end multi-cliente, permitiendo la sincronización de mensajes de forma segura en múltiples clientes, aun cuando algunos de ellos estén off-line.

Después de un intercambio de claves inicial, se deberá gestionar la renovación y el mantenimiento continuos de las claves de sesión efímeras.

El Sistema debe implementar la función de FS (Forward Secrecy) y garantía de no repudio, de manera que se protejan sesiones pasadas contra futuros compromisos de claves y passwords secretos.

El Sistema debe contar con una infraestructura de clave pública para la retención de claves pre-generadas de un solo uso (pre-keys) y permitir la¿’9iinicialización de sesiones de mensajería sin la presencia del par remoto (comunicación asíncrona).

El Sistema de Mensajería Instantánea Segura debe proporcionar confidencialidad, integridad, autenticación, consistencia del participante, validación de destino, secreto hacia adelante, secreto hacia atrás (también conocido como secreto futuro), preservación de la causalidad, desvinculación de mensajes, repudio de mensajes, repudio a la participación y asincronicidad. No proporcionará preservación de anonimato y requiere capacidad para la retransmisión de mensajes y el almacenamiento de material de clave pública.

Además del cifrado punto a punto de los mensajes, se considera ventajoso que el servidor se comunique con el cliente utilizando un canal con cifrado.

Funcionalidades

Otras capacidades requeridas son las siguientes:

- Permitir conversaciones en grupo.
- Permitir enviar mensajes en privado dentro de un grupo.
- Encriptar por default.

- Permitir envío de imágenes.
- Permitir envío de video.
- Permitir envío de archivos de otros formatos.
- Permitir envío de audios.
- Permitir saber si el destinatario recibió y leyó el mensaje.
- Permitir saber cuándo la contraparte está escribiendo.
- Permitir configurar el puerto en que el servidor escucha.
- Permitir deshabilitar notificaciones.
- Permitir borrar el historial.