authComm Systems

authMessenger

authMessenger es una aplicación segura de mensajería instantánea que integra grandes medidas de seguridad orientadas a garantizar la integridad y privacidad de las comunicaciones y de la propia información almacenada en cada terminal cliente.

La solución

authMessenger es un cliente seguro de mensajería instantánea con un interfaz de usuario y funcionalidad similar a los clientes más conocidos actualmente, pero con una serie de medidas de seguridad extra orientadas a proteger la información tanto en el propio terminal, como en el canal de comunicaciones.

authMessenger utiliza enlaces cifrados SSL con exhaustiva verificación de certificados de servidor para la protección de todos los datos intercambiados entre clientes.

authMessenger permite establecer claves de usuario para el registro de la aplicación junto con patrones de protección de entrada y además, claves de cifrado propias para cada conversación que pueden ser solo conocidas por los integrantes de esa conversación, así, en caso de pérdida o sustracción del terminal, ningún tipo de información intercambiada se verá expuesta.

La necesidad

Actualmente las comunicaciones entre personas de texto, voz o datos es una parte vital de todos los proyectos y de la propia vida diaria. En ciertos ámbitos empresariales, son necesarios determinados aspectos de seguridad y confidencialidad que no son satisfechos por ninguna aplicación de las existentes en el mercado general.

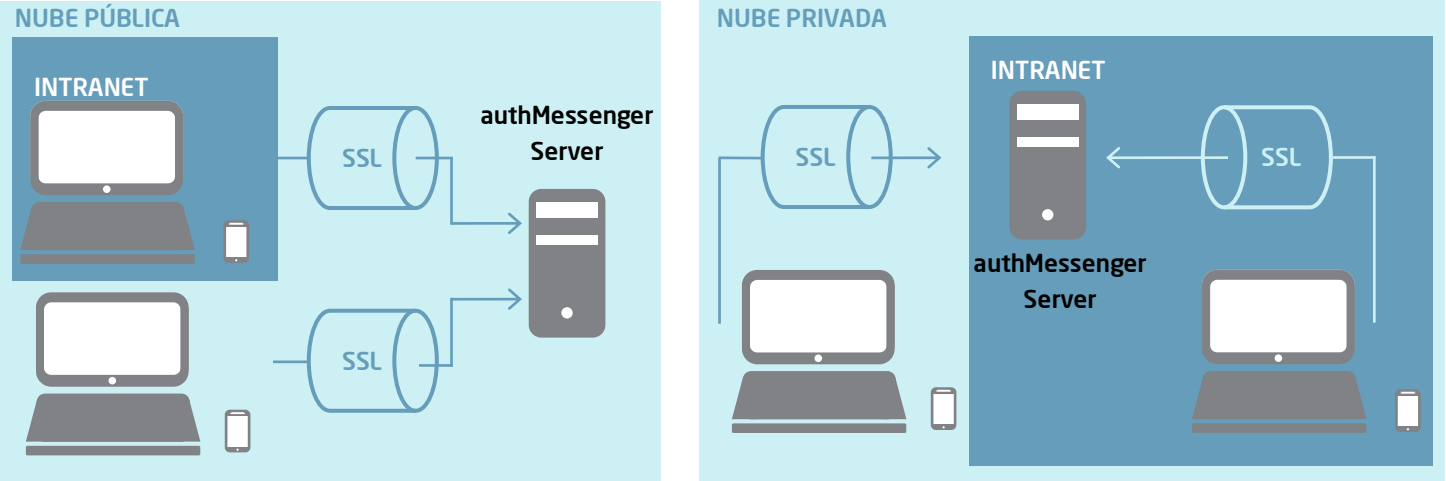
Con ello, surge la necesidad de una herramienta que garantice:

- Privacidad de la información en todas las circunstancias.
- Exclusividad de uso mediante control de entrada.
- Nivel de seguridad máxima en las conexiones.
- Gestión de usuarios y grupos por parte de administradores.

Características

- Comunicaciones SSL entre cliente y servidor con verificación de certificados.
- Clave de entrada a aplicación mediante contraseña, pin o patrón.
- Interfaz sencillo e intuitivo.
- Mantenimiento cifrado de datos en el terminal.
- Visores propios para no descifrar en ningún momento los contenidos recibidos o enviados.
- Posibilidad de incluir clave propia a cada conversación.
- El servidor no almacena ningún histórico de conversaciones y se basa en contraseña asignada en su arranque.
- Distintos perfiles de usuarios con capacidad de administración de cuentas y visibilidad de usuarios y grupos.

Arquitectura técnica de la solución



Descripción

El sistema permite el envío rápido de mensajes, imágenes y archivos entre sus usuarios. La conectividad de cada cliente se realiza utilizando canales encriptados a través de un servidor central que realiza el enlace entre ambos extremos. Este servidor, puede localizarse en la nube pública de internet, o dentro de la propia red del cliente.

Todos los datos transferidos desde los clientes son cifrados localmente en cada terminal en ambos extremos para evitar cualquier tipo de intrusión. La aplicación incluye visores específicos para garantizar que los contenidos nunca se descifran en ningún medio físico y quedan expuestos.

Así mismo, la aplicación permite incluir medidas de seguridad locales basadas en contraseñas, clave pin o clave patrón para garantizar el acceso restringido a la interfaz de control y los datos que contiene. Como medida excepcional, conversaciones específicamente privadas pueden ser encriptadas mediante contraseñas seleccionadas por el usuario.

Comunicaciones

- TLS 1.1 con certificado de 4096 bits y encriptación AES de 256 bits, con soporte para Proxy HTTP.
- Protocolo binario propietario.
- Verificación exhaustiva de la identidad del servidor (CA Privada).

Seguridad Local

- Inicio de sesión con usuario y contraseña no almacenada en el propio terminal.
- Verificación rápida con patrón o pin solicitada cada vez que se cambie entre aplicaciones o el terminal se bloquee.
- La aplicación no permite capturar la pantalla por parte del usuario o de otras aplicaciones para evitar que ningún contenido pueda quedar ex-puesto.
- La información local de conversaciones, mensajes y datos se almacena encriptada con AES128 utilizando una contraseña fuerte no almacenada en el terminal.
- Las notificaciones de la aplicación en ningún momento muestran el contenido recibido ni el remitente del mismo.
- La captura de imágenes se realiza directamente desde la cámara, encriptando y enviando la foto sin utilizar los medios de almacenamiento físico del terminal ni su propia galería.
- En la recepción de datos, los propios visores incluidos descifran y muestran el contenido sin almacenarlo en el propio terminal.
- En cualquier conversación el usuario puede proporcionar una clave propia para encriptar los mensajes que sea conocida también por los receptores. La contraseña en ningún momento se transmite o almacena permaneciendo asignada mientras la conversación está activa y desaparece automáticamente tras un corto periodo de inactividad.

Seguridad del Servidor

- El servidor no almacena histórico.

Los mensajes son eliminados en su entrega.

- El servidor encripta toda la información que maneja utilizando una contraseña que no se almacena localmente, sólo existe en RAM y es proporcionada por el administrador cuando inicia sesión.
- El servidor puede ser instalado dentro de la propia infraestructura del cliente (nube privada) o utilizar el servidor proporcionado y mantenido.

Gestión de usuarios

Por definición, los usuarios solamente pueden tienen visibilidad sobre otros usuarios que estén asignados a sus mismos grupos

El más alto rango es el usuario administrador, que puede crear usuarios, grupos y asignaciones y además, puede definir usuarios supervisores con capacidad para gestionar y crear un determinado número de usuarios y su asignación a grupos. Cada supervisor puede estar destinado a gestionar un grupo cerrado de usuarios sin visibilidad hacia los asignados a otros supervisores.

Esta estructura piramidal hace que el producto se pueda aplicar a la estructura de cualquier empresa, con un administrador único y un supervisor de cada área o departamento que gestione las comunicaciones de sus empleados.

authComm Systems
Escultor Gregorio Fernández, 9
36204 Vigo, España
T +34 902 922 910
info@authcomm.es