

¿Cómo Alice y Bob se intercambian mensajes de amor?





Hola! Soy ReD

SecOpsDev
Formador, cuando me dejan

Activista tecnológico

- Soberanía tecnológica
- Defensor de la privacidad
- Cofundador de Hacklabs y M4H





Alice y Bob

La pareja criptográfica más famosa del mundo
Criptografía de clave pública



Nacieron en Feb **1978**

Sus padres son Ron **Rivest**
Adi **Shamir**
Leonard **Adleman**

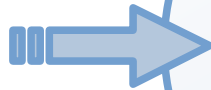




EVOLUCIÓN DE LA COMUNICACIÓN POSTAL



255 a.C.



1874 Unión postal



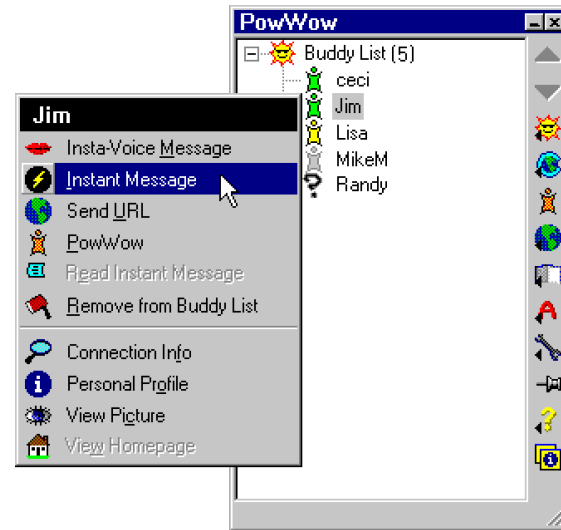
1971

EVOLUCIÓN DE LA TELEFONÍA

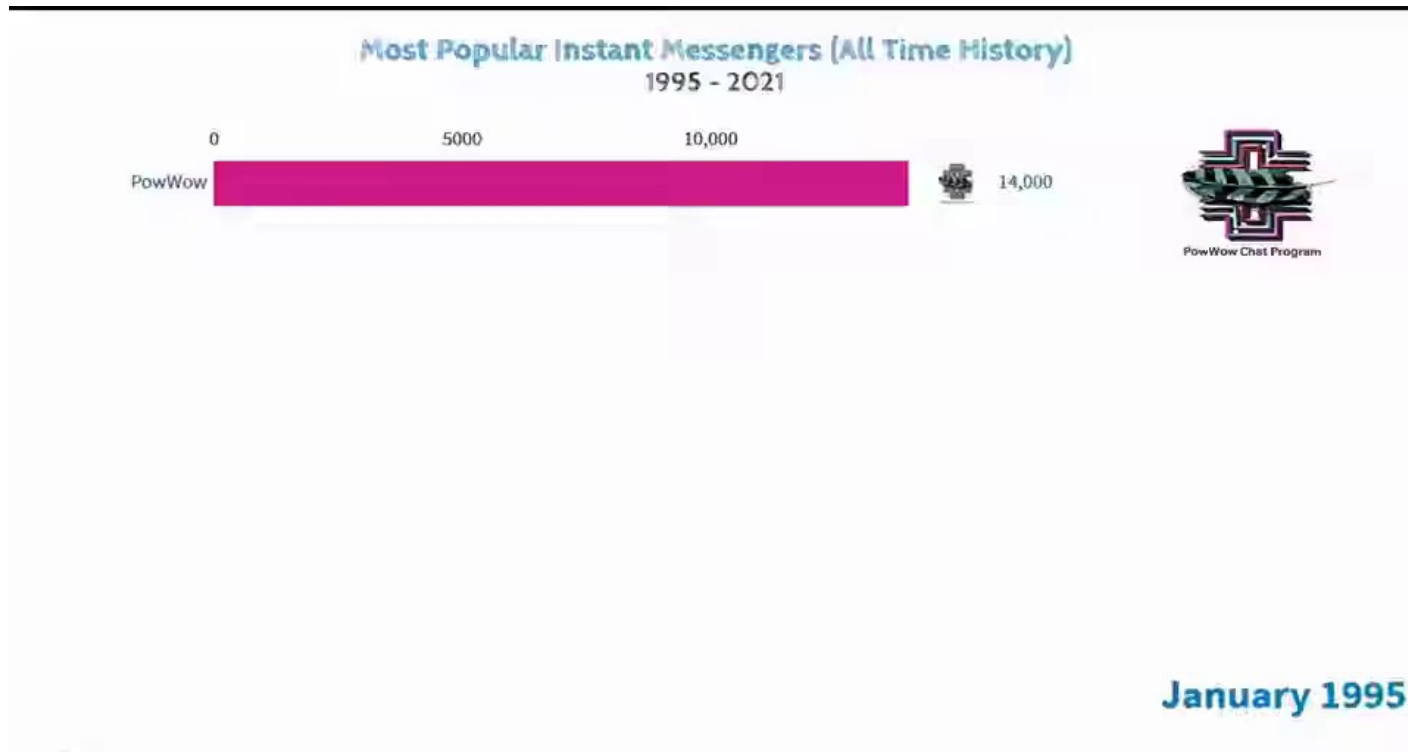


EVOLUCIÓN DE LA MENSAJERÍA

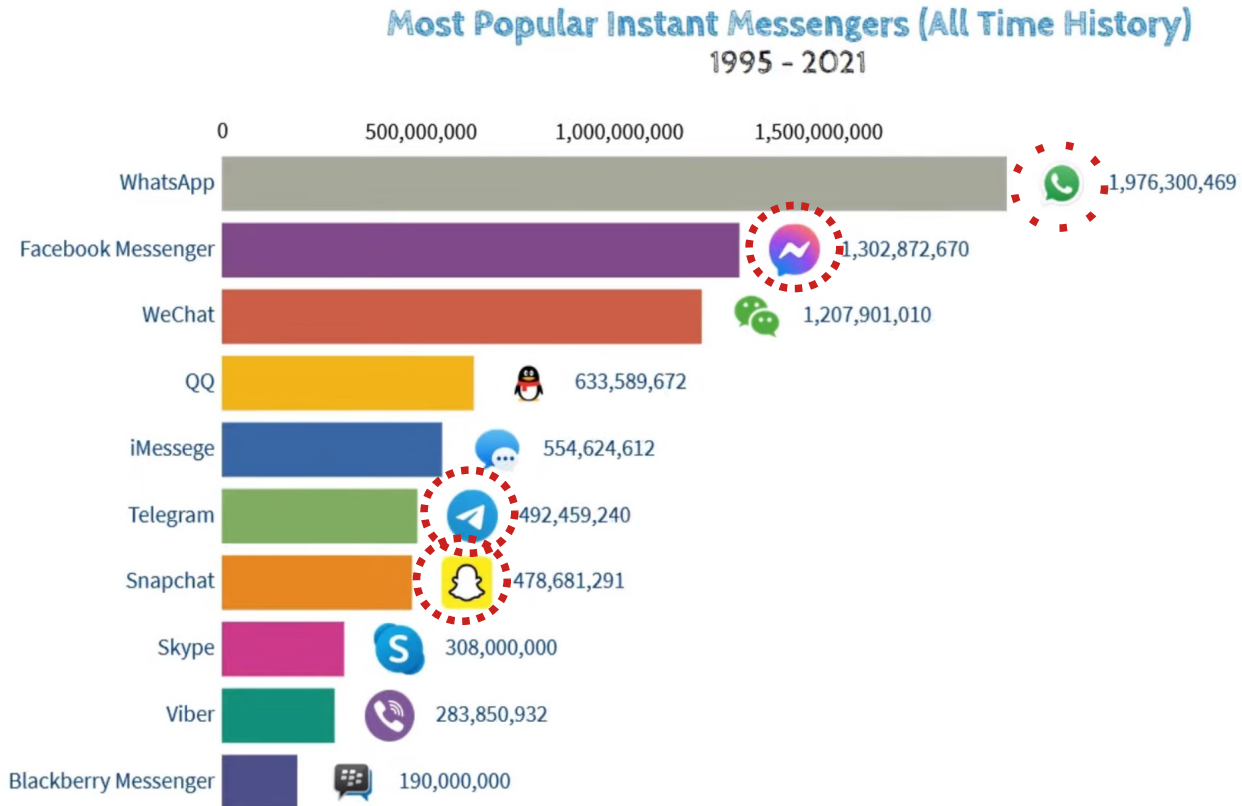
Junio 1995
14.000 usuarios



EVOLUCIÓN DE LA MENSAJERÍA



EVOLUCIÓN DE LA MENSAJERÍA



March 2021



DISTRIBUCIÓN POR EUROPA

MESSENGER Most Popular Messenger in Europe

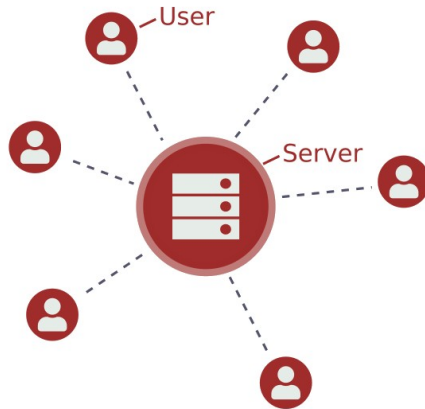
SimilarWeb.com, 2021 Data



♥ 📌 Don't Forget
Like & Save

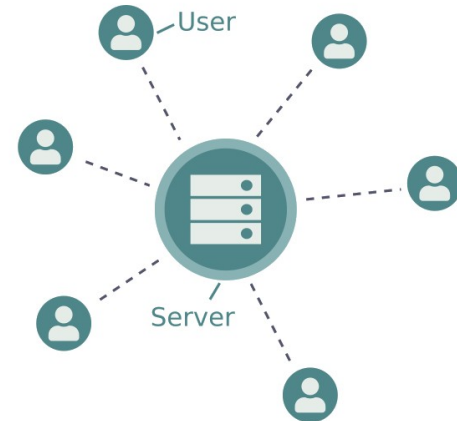
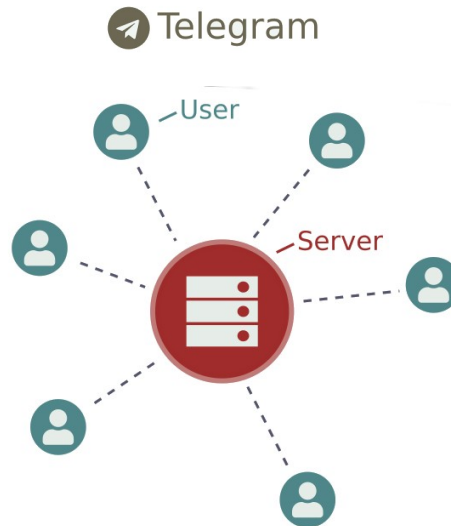
Follow
@worldstatsmaps WSM

MENSAJERÍA - CENTRALIZADA

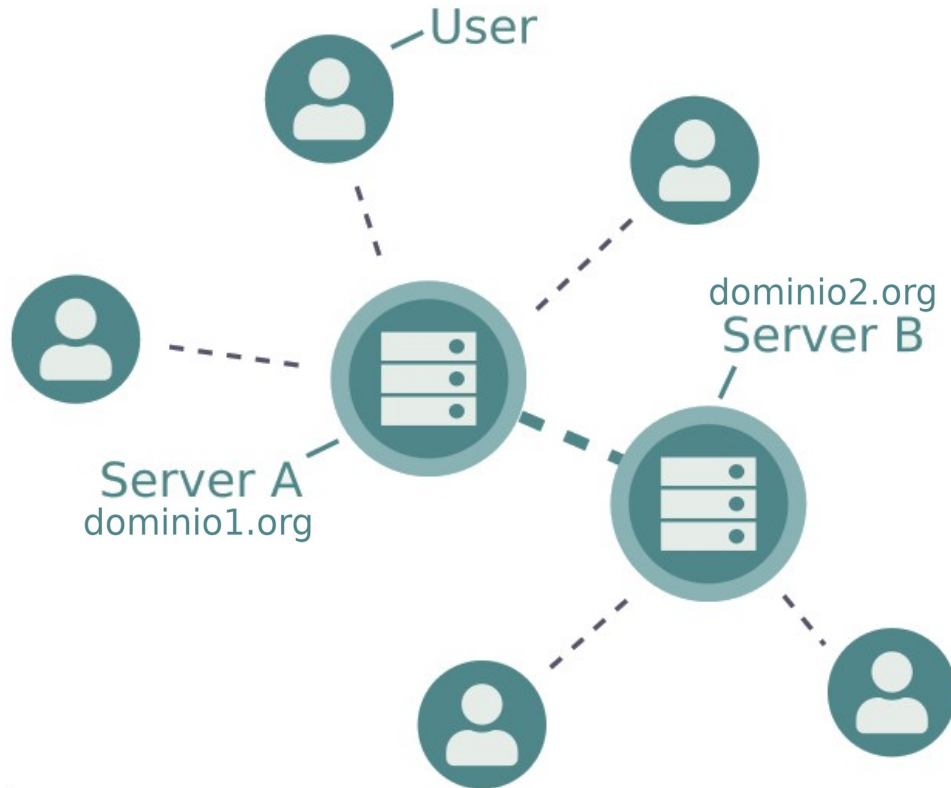


Whatsapp

Facebook
Instagram



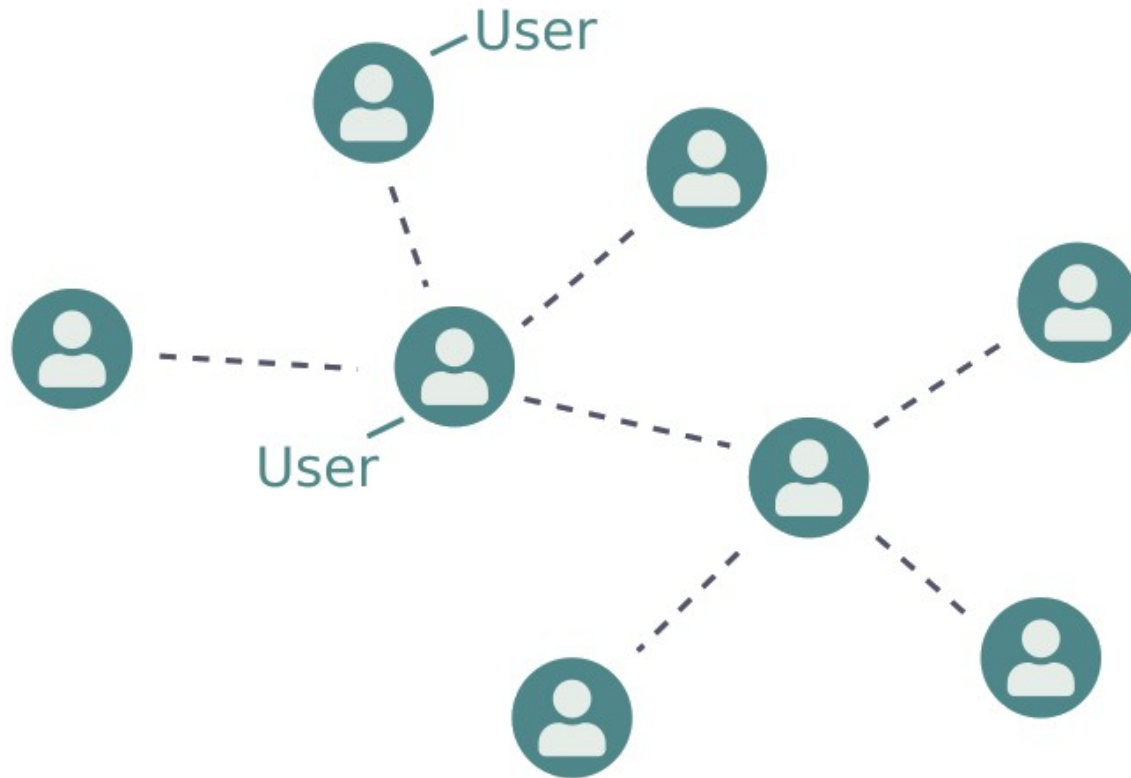
MENSAJERÍA - FEDERADA



XMPP



MENSAJERÍA - DESCENTRALIZADA



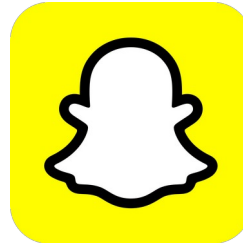
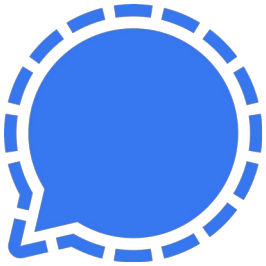
 Jami

 Tox

 Briar



MENSAJERÍA MÁS POPULAR



POR QUE SE HAN POPULARIZADO

Redes sociales físicas ♦

Quienes conocemos en IRL

Gestión de contactos ♦

Libreta de direcciones

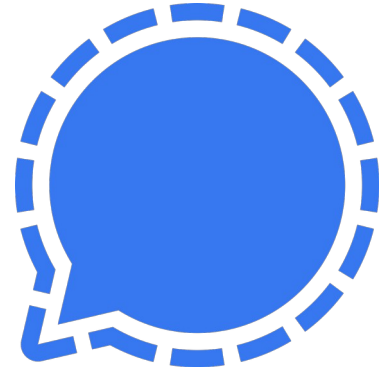
Facilidad de cambio ♦

Moverse entre redes de IM





SIGNAL



Data Not Linked to You

The following data may be collected but it is not linked to your identity:



Contact Info



Data Linked to You

The following data may be collected and linked to your identity:



Contact Info



Contacts



Identifiers



Data Linked to You

The following data may be collected and linked to your identity:



Purchases



Financial Info



Location



Contact Info



Contacts



User Content



Identifiers



Usage Data



Diagnostics



Data Linked to You

The following data may be collected and linked to your identity:



Health & Fitness



Purchases



Financial Info



Location



Contact Info



Contacts



User Content



Search History



Browsing History



Identifiers



Usage Data



Sensitive Info



Diagnostics



Other Data

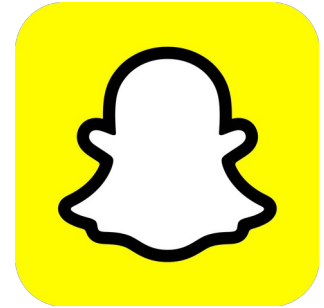




Data Linked to You

The following data may be collected and linked to your identity:

 Purchases	 Location
 Contact Info	 Contacts
 User Content	 Search History
 Identifiers	 Usage Data
 Diagnostics	



Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

 Contact Info	 Identifiers
--	---



Telegram

- Número de teléfono
- Dirección de correo electrónico
- ID del dispositivo
- Lista de contactos



WhatsApp

- Número de teléfono
- Dirección de correo electrónico
- ID del dispositivo
- ID usuario
- Lista de contactos
- Ubicación aproximada
- Historial de compras
- Uso de la aplicación

- Datos de fallos de la aplicación
- Datos de rendimiento
- Otros datos de diagnóstico
- Información de pagos
- Atención al cliente
- Otro tipo de atención al cliente
- Interacción del producto
- Datos publicitarios



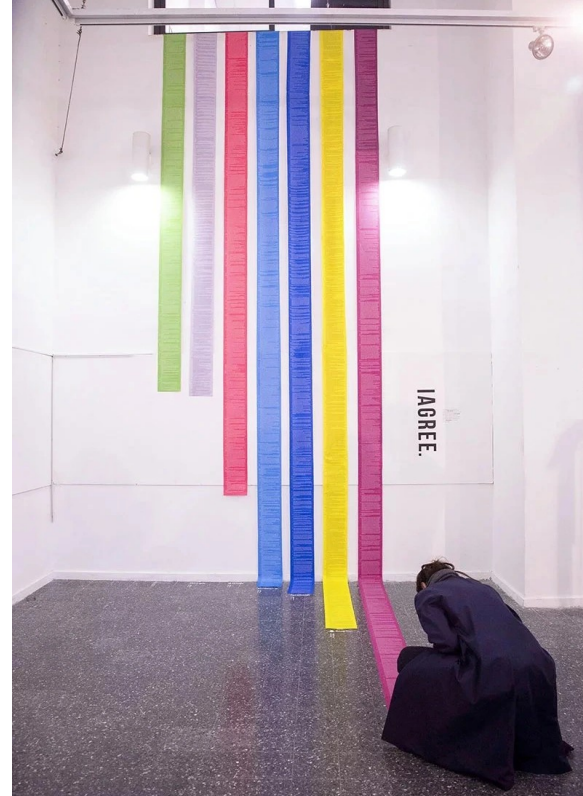
Facebook
Messenger

- Número de teléfono
- Dirección de correo electrónico
- Nombre
- ID del dispositivo
- ID usuario
- Lista de contactos
- Dirección física del usuario
- Otra información de contacto del usuario
- Ubicación aproximada
- Ubicación precisa
- Acceso al historial de mensajes
- Acceso al historial de navegación
- Historial de compras
- Otra información financiera
- Uso de la aplicación

- Datos de fallos de la aplicación
- Datos de rendimiento
- Otros datos de diagnóstico
- Usabilidad del producto
- Información de pagos
- Atención al cliente
- Otro tipo de atención al cliente
- Interacción del producto
- Datos publicitarios
- Analítica
- Datos de salud
- Otra información sensible
- Fotos o vídeos
- Datos de audio
- Contenido del juego

CONDICIONES DE USO

WhatsApp
Google
Tinder
Twitter
Facebook
Snapchat
Instagram



E2EE Y LA PRIVACIDAD



¿QUIÉN PUEDE ANALIZAR EL E2EE?

- Propietario red local
- Proveedor de Internet
- Centro de datos
- Gobiernos



VECTORES ANÁLISIS DE E2EE

metadatos

- Diferenciar por el peso (chat, fotos, chat de voz...)
- Sacar con quién hablamos y cuánto hablamos
- Zona y horas de conexión (si está de vacas ...)
- Servidores (configuración/actualizaciones)
- Ataques de app local (lectura de datos de APP)

CARACTERÍSTICAS DE CIFRADO



Repudio



Cifrar usuario offline



Cert. varios dispositivos



Perfect forward secrecy PFS

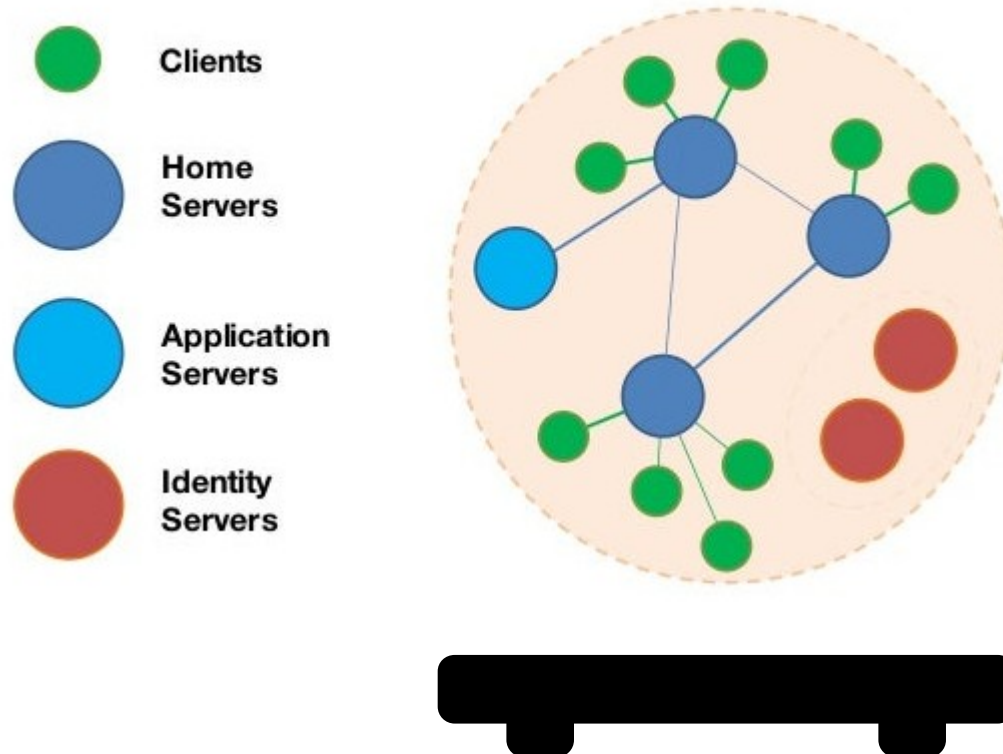


OpenPGP / OTRv4 / MEMO

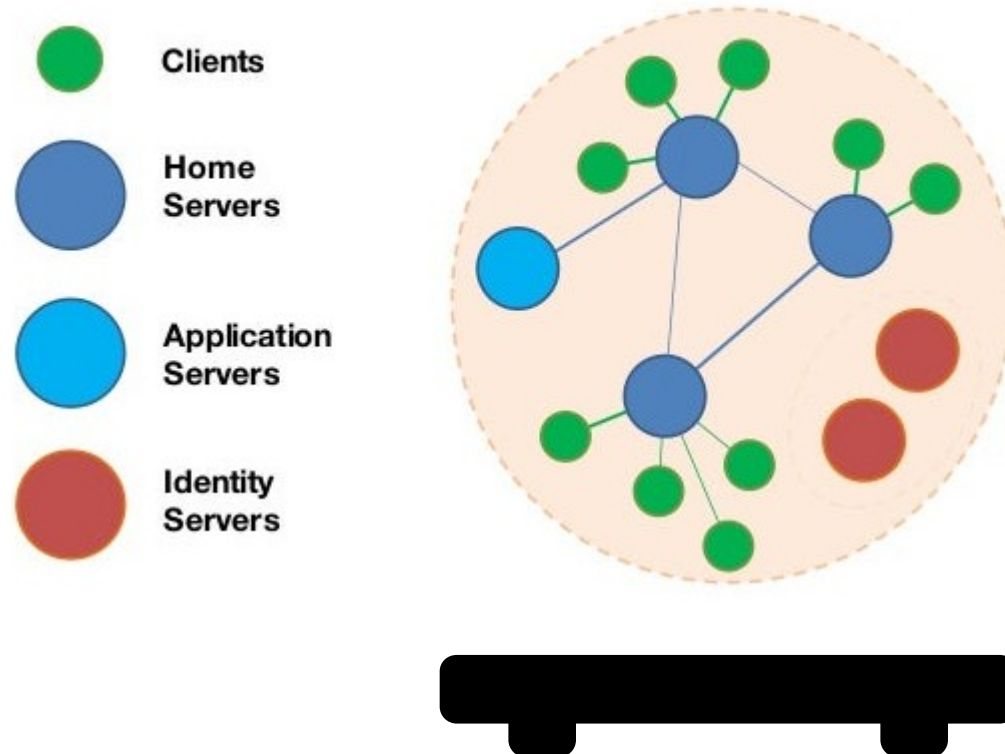


#	OpenPGP	OTR	OMEMO
Multiple Devices	Yes	No	Yes
Offline Messages / Backlog ⁵	Yes	No	Yes
File Transfer	Yes	No ¹	Yes
Verifiability	No	Yes	Yes
Deniability	Yes	Yes	Yes
Forward Secrecy ³	No	Yes	Yes
Server side archive ^{3 5}	Yes	No	No
Per Message Overhead	High	Low	Medium ⁴

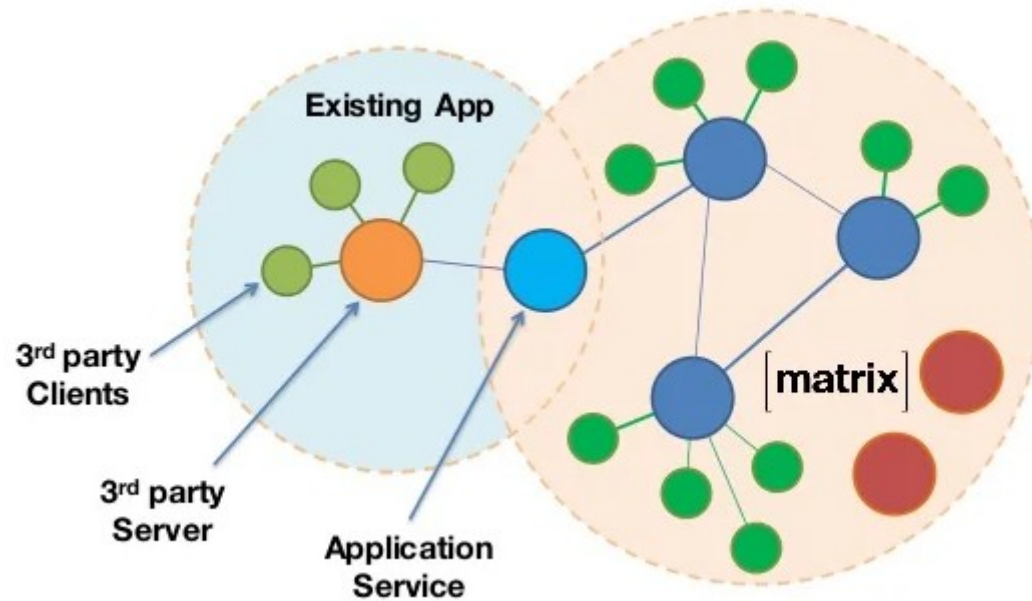
[MATRIX] ~~PROTOCOLO~~ ESPECIAL



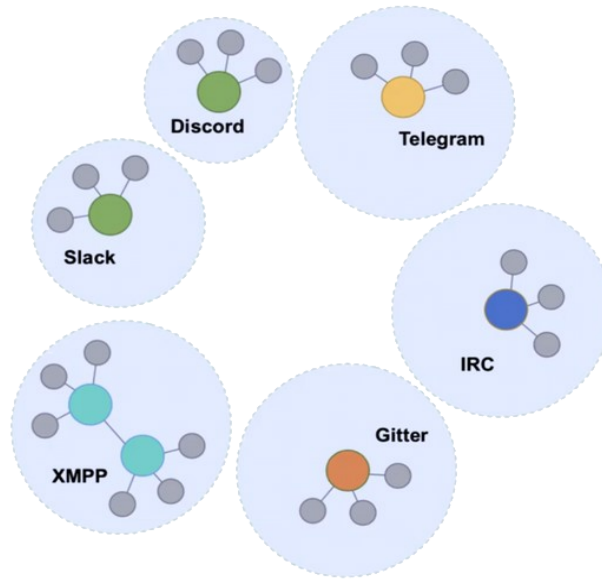
[MATRIX] ESTANDAR



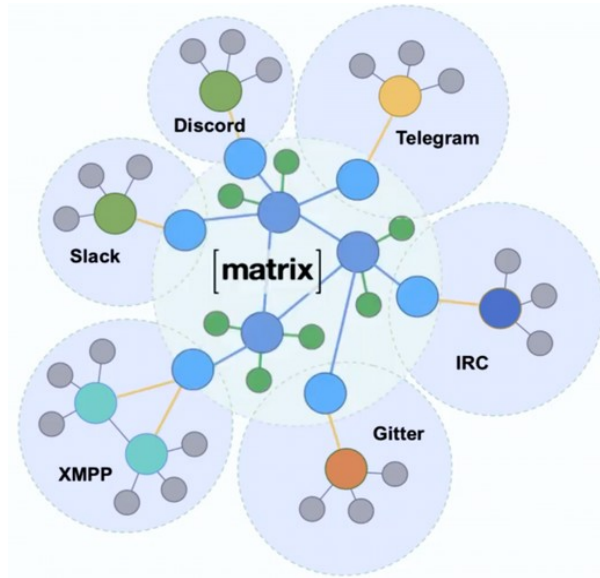
[MATRIX] ESTANDAR



[MATRIX] ESTANDAR



[MATRIX] ESTANDAR



MECANISMOS DE PROTECCIÓN



Sandboxing OS
Aislar los procesos



Pseudónimos
Usuarios con Ids
anónimos



Ofuscación
Esconde el trafico



Encriptar
Ver opciones
ampliadas



Expiración
Mensajes con
duración



CONCLUSIONES

- La tendencia no siempre es la mejor opción
- Retención de información
- Más **privacidad**, mayor **compromiso**
- Conocer las características de Encriptado
- Mensajería cerrada VS Protocolos de mensajería
Soft Libre





¡Gracias!

¿Preguntas?



red@nosoloaulas.com



red@jabber.ccc.de



[@ReD.1984](https://twitter.com/ReD.1984)

