

Une messagerie instantanée qui respecte vos libertés ?



Présentation

Libre en Communs



- site web : <https://www.a-lec.org>
- réseau social : <https://toot.a-lec.org>
- courriel : contact@a-lec.org

Présentation (2)

Adrien Bourmault aka *neox*



- trésorier et responsable de l'infrastructure de Libre en Communs
- membre de la XMPP Standards Foundation
- membre de la FSF et du Libreplanet Committee
- mainteneur de GNU Boot

Sommaire

- Histoire du web et de la centralisation
- Les messageries centralisées
- Une messagerie instantanée acentrée ?
- Du chiffrement pour tous ?

Histoire du web



Naissance d'internet

- années 1960s
 - création du projet ARPANET/NCP
 - réseau non centralisé, par nécessité militaire
 - NPL Network, premier réseau de paquets
 - européen, mais un peu oublié par l'Histoire

Naissance d'internet (2)

- années 1970s
 - création du courriel sur ARPANET/NCP
 - idée de réseau hétérogène, mais NCP ne peut pas faire l'affaire
 - création de TCP/IP puis UDP

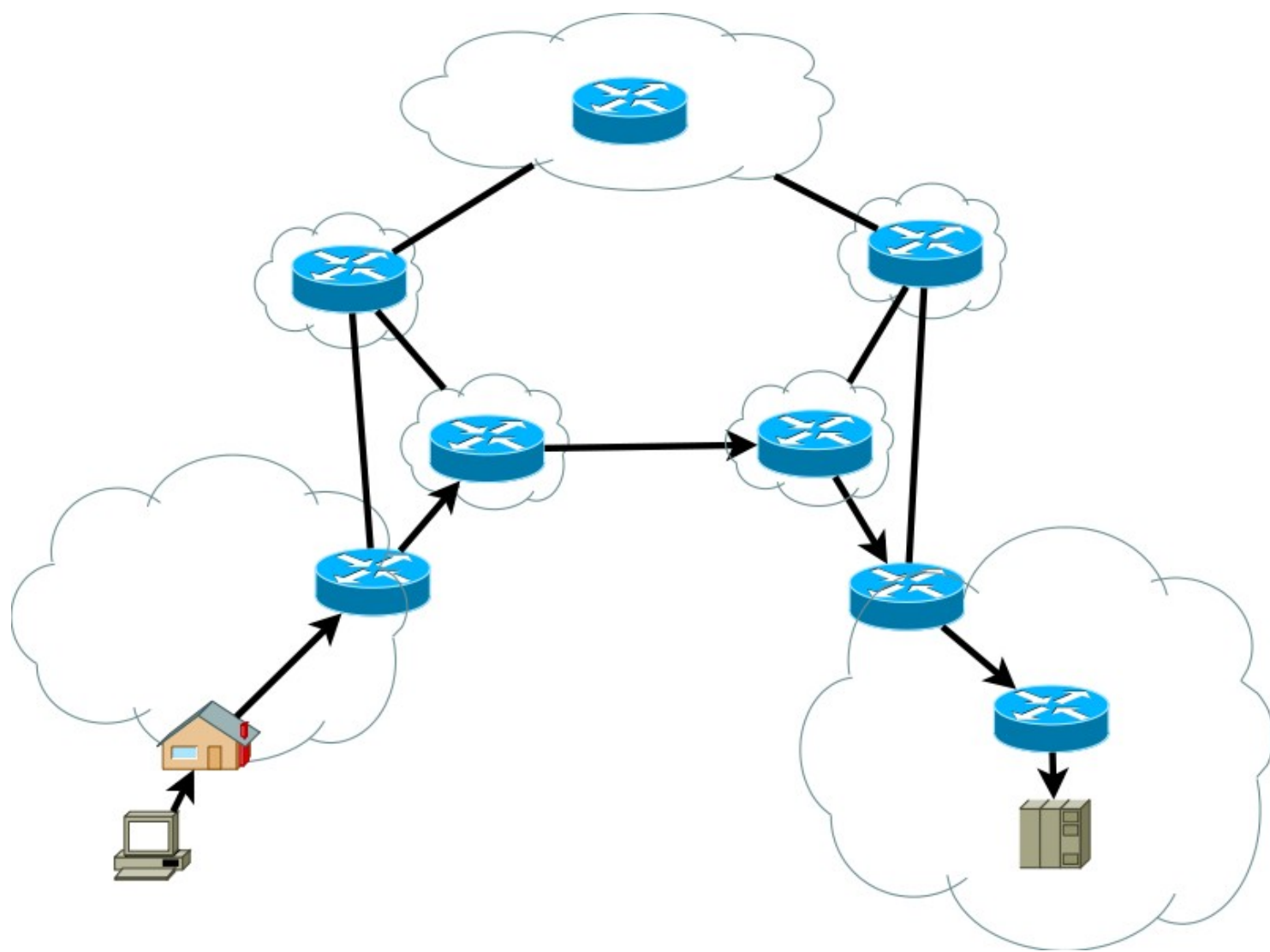
Naissance d'internet (3)

- années 1980s
 - TCP/IP version 4
 - actuelle version la plus utilisée au monde
 - création du modèle OSI
- années 1990s
 - apparition du World Wide Web
 - démocratisation des ordinateurs dans les foyers

Centralisation progressive

- années 1990s
 - nombreux acteurs « pionniers »
 - Yahoo!, Amazon, eBay, Netscape, AOL et d'autres
 - naissance de Google
 - diverses institutions :
 - IANA
 - ICANN
 - IETF

Fondamentalement, Internet et le web sont décentralisés...



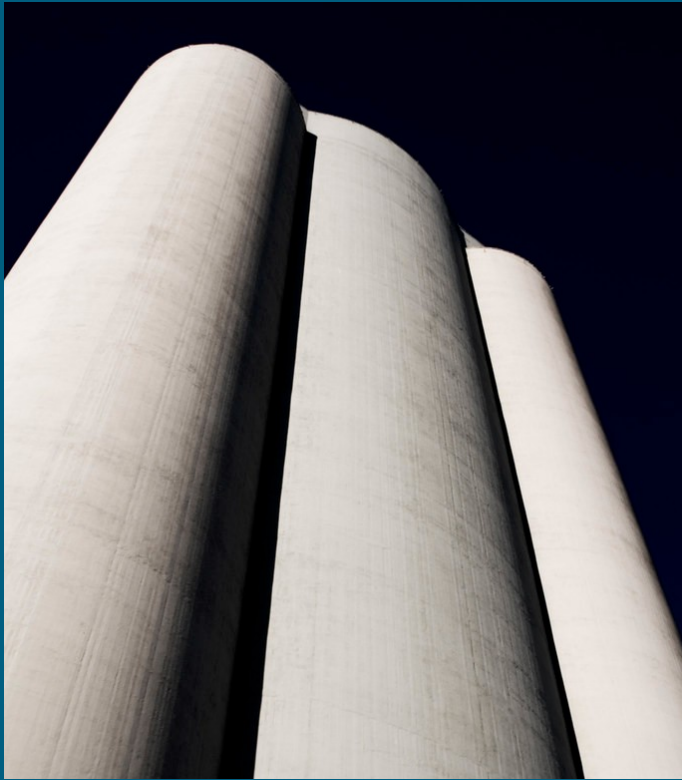
Centralisation progressive (2)

- plusieurs facteurs
 - concentration du marché
 - certains silos deviennent (trop) populaires
 - répartition géographique inégale
 - politique artificielle d'incompatibilité/fermeture
 - notamment « webisation »

Centralisation progressive (3)

- apparition des API REST basées sur HTTP (1996)
 - pas des vrais protocoles (pas de RFC)
 - dépendant de couches complexes
- apparition des clients web
 - utilisent REST
 - programmés en Javascript (s'exécutent dans le navigateur)

Messageries centralisées



Messagerie instantanée ?

- apparition dans les années 1980s
 - parallèle au courriel
 - texte simple, court
 - Talk (temps réel, p2p)
 - IRC (temps différé, serveur)
- commercialisation popularisation 1990s

Messagerie instantanée (2)

- Popularisation avec les « pionniers »
 - ICQ
 - créé par Mirabilis (1996), racheté par AOL (1998)
 - première messagerie à inscription
 - massivement adoptée (~100M en 2001)
 - AIM (AOL)
 - MSN
 - créé par Microsoft en 1999
 - massivement adopté (~330M en 2009)

Messagerie instantanée (3)

- centralisation par les « pionniers » !
 - ICQ
 - serveur unique géré par AOL
 - AIM (AOL)
 - serveur unique géré par AOL
 - MSN
 - serveur unique géré par Microsoft

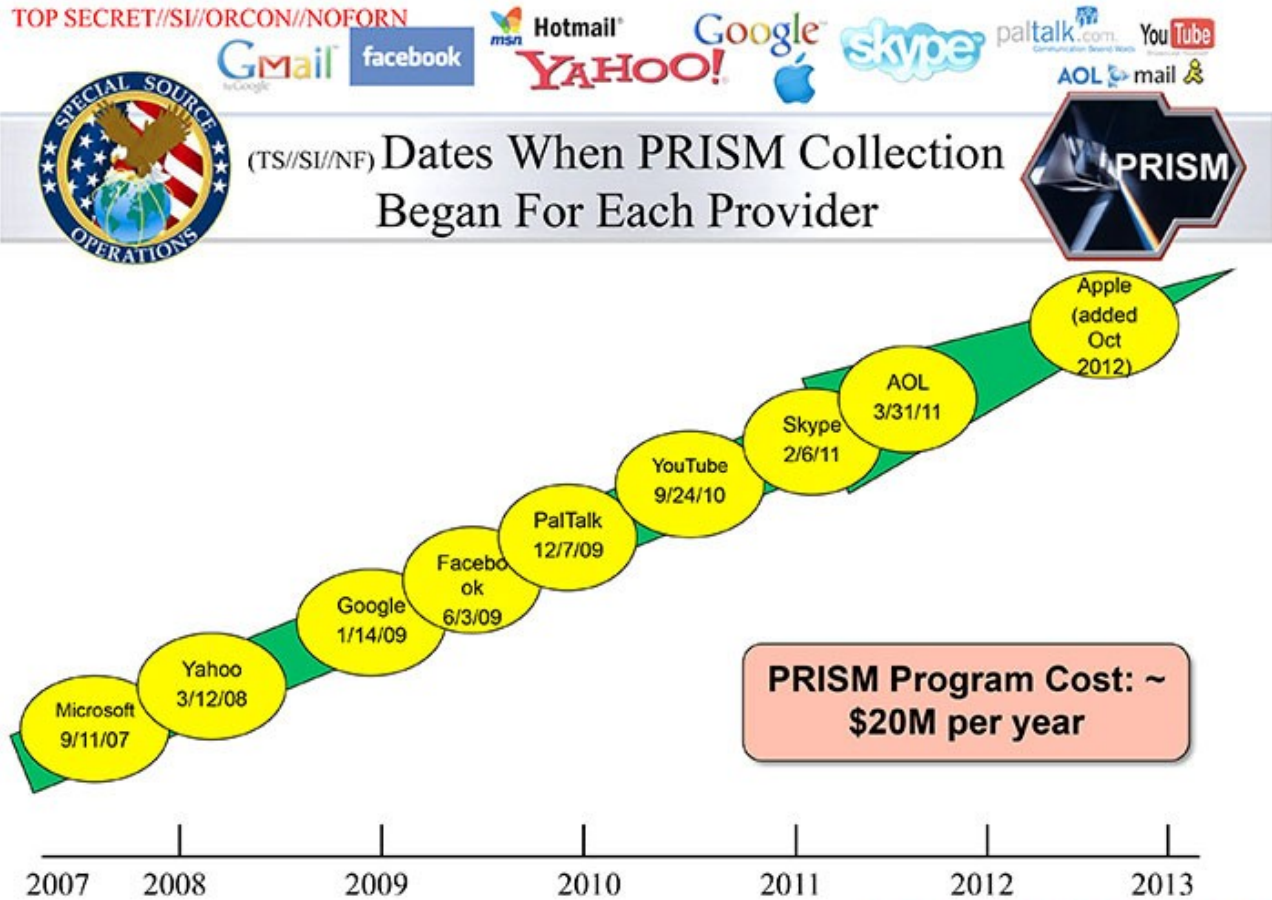
Centralisée... et alors ?

- dépendance à compagnie spécifique
 - CGU et politique de données
 - son existence...
- bien souvent, centralisé = opacité
 - pas d'interopérabilité
 - logiciel non libre

Centralisée... et alors ? (2)

- dangers nombreux
 - censure
 - surveillance de masse
 - enclosure
 - monétisation des données personnelles
 - ...
- pas libre donc impossible à vérifier
- centralisé donc impossible à contourner
- si législation USA, portes dérobées sur demande !

Centralisée... et alors ? (3)



Centralisée... et alors ? (4)



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection
(Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:

Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Le cas Facebook

- publications centralisées
 - interface web sur le site internet
 - API REST fermée et client Javascript non libre
 - application (Facebook)
 - non libre
- messagerie instantanée centralisée
 - interface web sur le site internet
 - API REST fermée et client Javascript non libre
 - application (Messenger)
 - non libre

Le cas Facebook (2)

- cas de censure et de manipulations connus
 - Cambridge Analytica (2018)
 - Facebook Files (2021)
- surveillance avérée
 - PRISM, XkeyScore, etc
 - vente de données personnelles à des publicitaires
 - dénonciation d'avortement (2022, Messenger)

Le cas Whatsapp

- appartient à Facebook !
 - acheté par Facebook/Meta en 2014
- supposée sécurisée parce que chiffrée
 - mais pas les méta-données !
- massivement utilisée dans le monde
 - ~350M en 2013
 - ~2Mds en 2020

Le cas Whatsapp (2)

- centralisée !
- cas de surveillance connus
 - The Guardian (2017) informe sur une porte dérobée du chiffrement
 - condamnation CNIL (2017) pour transfert
 - tentative d'achat/intégration de Pegasus (2020)
 - vente de données personnelles à des publicitaires (CGU)
 - loi USA...

En résumé...



- centralisé = opacité
- non libre = pas auditable
- USA = surveillance potentielle
- même chiffré, vous êtes en danger : méta-données

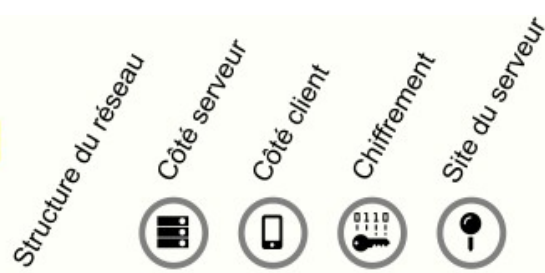
Messageries acentrées
























Principes de décentralisation



- plusieurs degrés
 - réseaux multiples
 - IRC
 - fédéralisme de serveurs
 - XMPP
 - Matrix
 - ActivityPub (Mastodon, Pleroma, etc)
 - pair-à-pair
 - Jami
 - Briar
 - XMPP

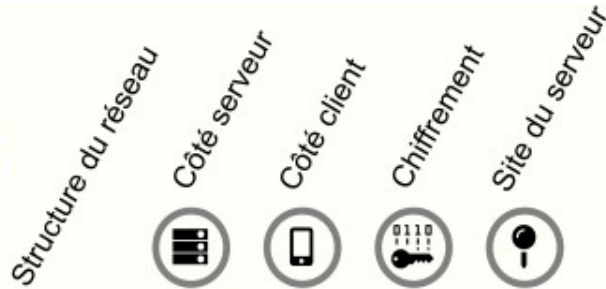
-  Code source ouvert (libre) **Recommandation**
-  Code source fermé (privateur)































Systemes pour converser en ligne normalement (à la WhatsApp)

Systeme	Code source	Structure du réseau	Côté serveur	Côté client	Chiffrement	Site du serveur
 Briar  Jami  Tox décentralisé (sans serveur/intégré) = indépendant du fournisseur		-			-sans-	
 chat standard (XMPP) <small>Conversations, Quicksy, blabber, monocles, Snikket, Yaxim, Gajim, Monal, Siskin, Dino, ...</small>				au choix		
 Matrix <small>FluffyChat, ditto, ...</small>  SimpleX décentralisé (fédéral) <i>chacun peut choisir librement</i> = indépendant du fournisseur				au choix		
 E-Mail / IMAP <small>Delta Chat, Dib2Qm, ...</small>				au choix		
 Wire centralisé <i>malgré l'ouverture du code source du serveur les propriétaires (titulaires de droits) n'autorise pas de fédération = dépendant du fournisseur</i>				UE (A)		
 Signal centralisé <i>malgré l'ouverture du code source du serveur les propriétaires (titulaires de droits) n'autorise pas de fédération = dépendant du fournisseur</i>	 (S)			ÉT.-UNIS (A)		
 Threema				Suisse		
 Telegram centralisé <i>le code source du prog. côté serveur est secret, l'app peut éventuellement être open source</i>			 (T) 1	inconnu 2		
 Whatsapp  Viber = dépendant du fournisseur				ÉTATS-UNIS/ inconnu		
 Skype  Facebook Messenger			 1	ÉTATS-UNIS		
 WeChat  QQ			 -	Chine		

-  Code source ouvert (libre) **Recommandation**
-  Code source fermé (privateur)



Solutions de chat d'équipe (avec fonctions supplémentaires pour le travail de groupe à la Slack)

 Matrix <small>Element, SchildiChat, ...</small>	décentralisé (fédéral) = indépendant du fournisseur				au choix
 Rocket.Chat (la fédération entre serveurs est limitée)					au choix
 Mattermost  Zulip  Nextcloud Talk	décentralisé				au choix
 Webex	centralisé				ÉT.-UNIS+UE
 Slack  Teams  VooV	<i>tout le code source (serveur et application) sont secrets d'entreprise</i> = dépendant du fournisseur				ÉT.-UNIS/CN
 Discord					ÉTATS-UNIS

XMPP



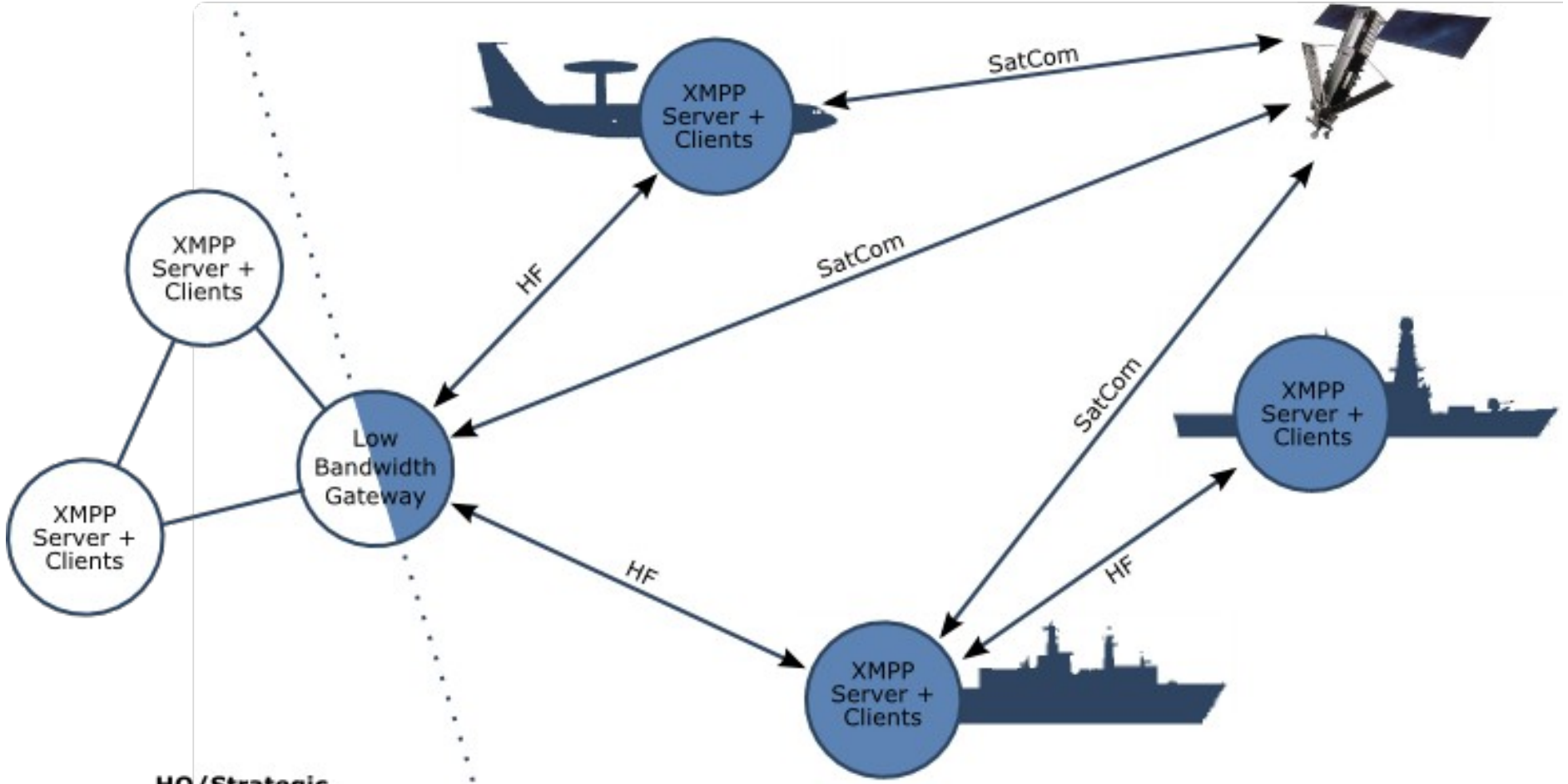
C'est quoi XMPP ?

- protocole créé en 1999
 - anciennement nommé Jabber
 - cœur du protocole normé par l'IETF
 - norme étendue gérée par la XMPP Standards Foundation (XSF)
- libre
- fédéré (décentralisé)

Fonctionnalités de XMPP

- messagerie instantanée
 - 1:1 et groupe (salons)
 - texte simple et riche
 - fichiers (dont images, vidéos, etc)
 - chiffrement
- appels
 - 1:1 et groupe
 - audio/vidéo
 - chiffrement
 - en pair-à-pair
- pas uniquement une messagerie
 - domotique, transfert de données, etc
 - microblog (avec Movim, Libervia, etc)
 - usage militaire !

**Deployed/Tactical
(Low Bandwidth Links)**



**HQ/Strategic
(High Bandwidth Links)**

Client ? Serveur ?...

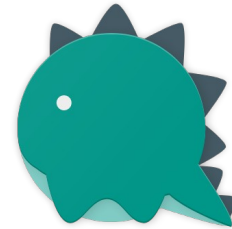
- client = application pour communiquer
 - au choix de l'utilisateurice
- serveur = logiciel opéré par un fournisseur
 - au choix du fournisseur/opérateur
- service = instance d'un serveur d'opérateur
 - au choix de l'utilisateurice

Clients XMPP

- client = domicile des données
 - client libre ?
- fonctionnalités ?
 - respect des normes/XEPs ?
 - client à jour ?
- accessibilité ?

Clients XMPP (2)

- beaucoup de clients !
 - PC (GNU/Linux)
 - Gajim
 - Dino
 - Kaidan
 - PC (Windows)
 - Gajim
 - Téléphone (GNU/Linux)
 - Dino
 - Téléphone (Android)
 - Conversations (et dérivés comme Monocles)
 - Web
 - Movim



Clients XMPP (3)

- beaucoup de clients !
 - Téléphone (iOS)
 - situation plus complexe
 - environnement hostile
 - Siskin
 - Monal



Services XMPP

- service = domicile des méta-données et données non chiffrées
 - serveur libre ?
 - admins éthiques ?
- fonctionnalités ?
 - respect des normes/XEPs ?
 - serveur à jour ?

Services XMPP (2)

- CHATONS
 - quelques services qui tournent bien
 - voir sur <https://www.chatons.org>
- XMPP Providers
 - liste de serveurs audités
 - <https://providers.xmpp.net/>



Services XMPP (3)

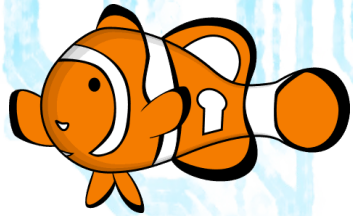
- Libre en Communs
 - chalec.org



OMEMO



C'est quoiOMEMO ?



- protocole de chiffrement
 - basé sur le protocole Signal
 - algorithme « double ratchet » amélioré
 - XEP
- géré par la majorité des clients
- géré par tous les serveurs

	Telegram	Off-the-Record	OpenPGP	Signal	OMEMO
Quasi-instantanée	Excellent	Non ou Médiocre	Excellent	Excellent	Excellent
Décentralisation	Non ou Médiocre	Excellent	Excellent	Non ou Médiocre	Excellent
PFS	Insuffisant	Excellent	Non ou Médiocre	Excellent	Excellent
Déniabilité	?	Perfectible	Non ou Médiocre	Excellent	Excellent
Identifiants	Insuffisant	Excellent	Excellent	Insuffisant	Excellent
Algo. crypto.	Non ou Médiocre	Non ou Médiocre	Insuffisant	Perfectible	Excellent
Implémentations libres	Non ou Médiocre	Excellent	Excellent	Excellent	Excellent
Spécifications publiques	Non ou Médiocre	Excellent	Excellent	Perfectible	Excellent
Fiabilité de l'IGC	Non ou Médiocre	Excellent	Excellent	Insuffisant	Excellent
Déploiement	Excellent	Insuffisant	Insuffisant	Perfectible	Insuffisant

Légende :

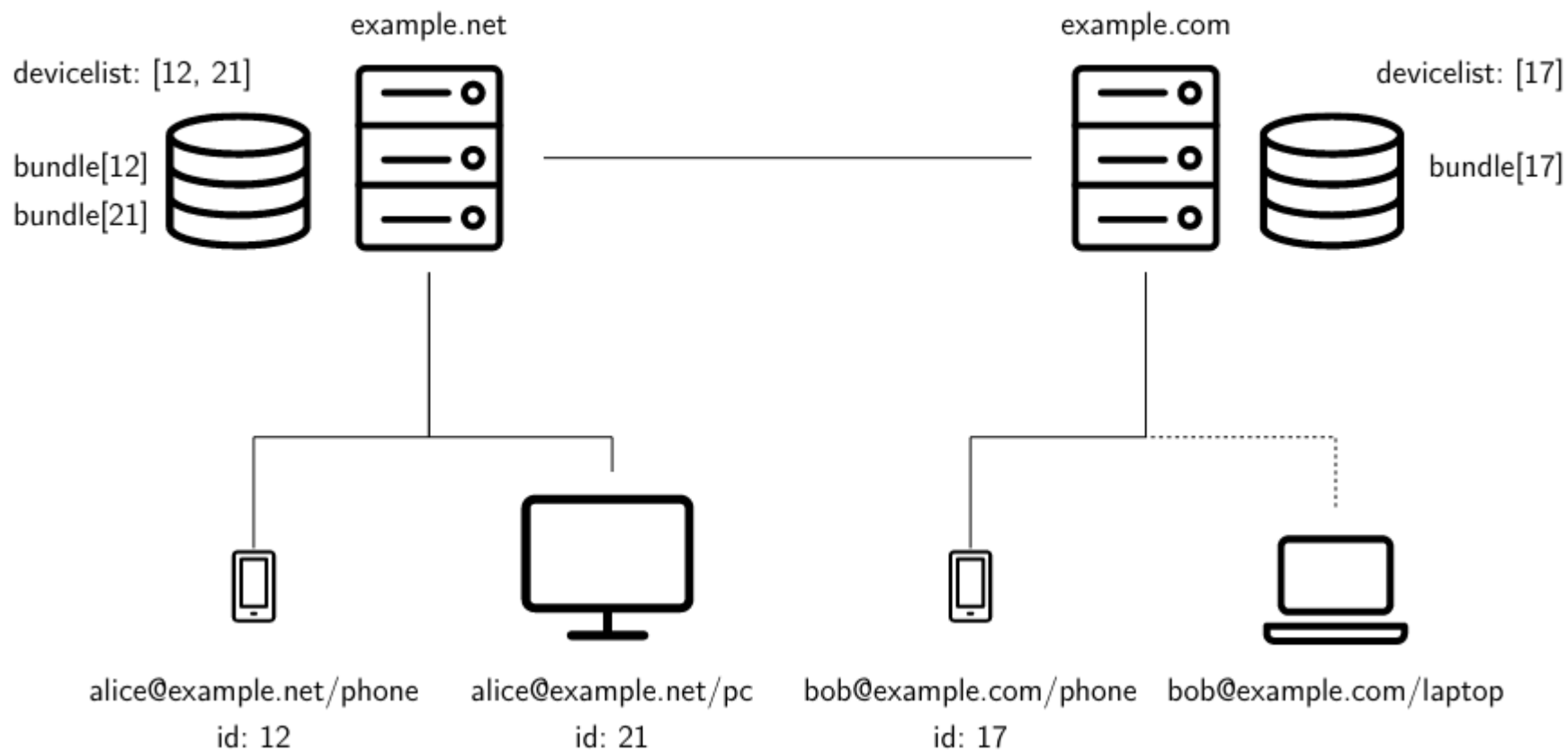
? = Inconnu

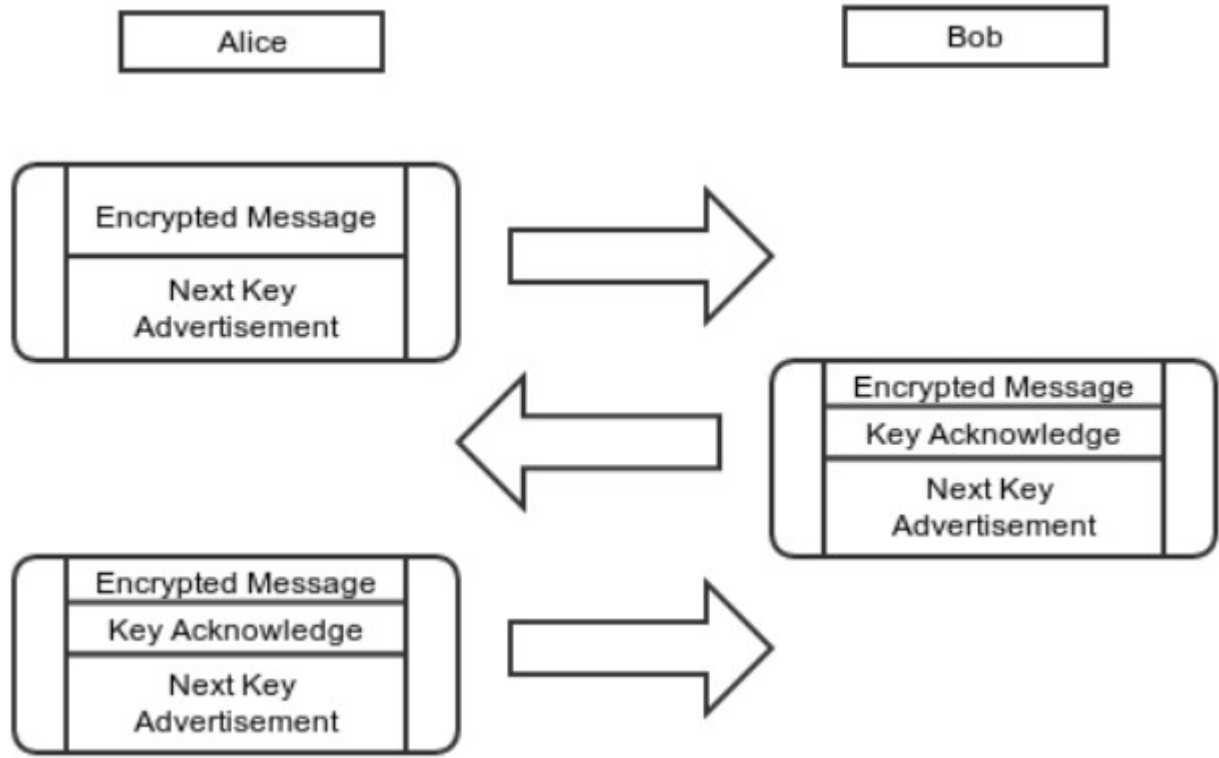
Oui ou Excellent

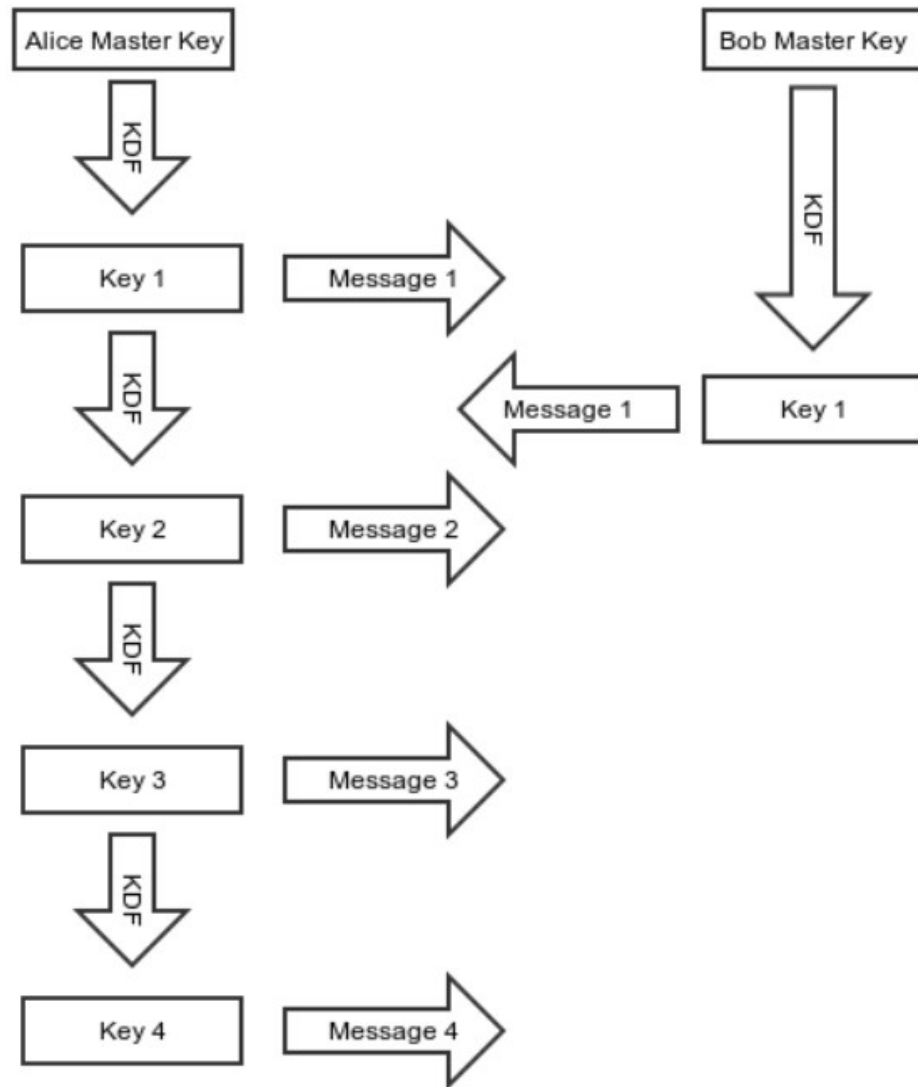
Perfectible

Insuffisant

Non ou Médiocre







État dans les clients

- utilisé pour la messagerie instantanée
 - 1:1 (textes et fichiers)
 - Conversations : par défaut
 - Gajim, Dino, Movim : activable
 - groupes privés (textes et fichiers)
 - Conversations : par défaut
 - Gajim, Dino, Movim : activable
- appels : utilisé pour authentifier
 - utilisation de DTLS-SRTP pendant l'appel
- sous iOS : encore des problèmes...



Quelques captures ?





- Libre en Communs
-
- Épinglé
- Libre en Communs 14:20
Moi : Par contre je tiens compte...
- CA Hier
cpm : echolib, merci, corrigé.
- Membres de Libre en Communs mar.
cpm : https://www.a-lec.org/ac...
- Cominfra 15:55
Moi : Cool, c'est planifié
- Cominfra Supervision juin 08
lsengard : ...
- Chalec 19:02
Moi : Woah on a de la pub pour nou...
- Comcom Hier
Moi : oui !
- Commécénat ven.
cpm : à voir si ça peut être une sour...
- Les Communs et nous mai 10
Moi : echolib, d'accord, j'ai considér...
- LibreXperience Hier
Moi : J'ai vu que snowden en f...
- LibreHardware mai 31
Moi : Pour information, le service X...
- Libre et Éducation juin 11



Libre en Communs

Salon public de l'association Libre en Communs (<https://www.a-lec.org>)

Pro A-LEC



Invisiter à cette discussion

Rechercher des participants...

Propriétaires (5/22)

- neox (You)
- Claudia
- jean
- julian
- cpm

Participants/tes (17/22)

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-



o0JbiqcyTyCi0slUs2SKRw.jpg
284,7 Ko

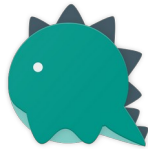


G0FZwtLQRK6gSQ6a6LKF-A.jpg
320,4 Ko



cpm sam. 17 juin 2023 14:48:38
hoouo, marrant une table ronde, très joliment décorée, bavo \o/
merci pour les photos, très belles





Sécurité & Vie Privée

Respect de la vie privée, des données personnelles et problèmes liés à la sécurité, mais aussi un zeste de politique, et du feu ...

eduroam ou pas. Et c'est connu XMPP c'est surtout pour organiser des attentats, donc bon je les comprends.
Alors normalement eduroam c'est le RENATER, donc ils devraient pas interdire l'utilisation de XMPP qui est fortement utilisé dans la recherche pour les communications de données de labo.

Mais en effet, y a des facs et des centres de recherche où il se passe des trucs bizarres

18:19
Inria a fermé son serveur XMPP (qui était tout pourri de toute façon) au début du confinement pour mettre en place mattermost --
Mais à ma connaissance, dans les centres Inria, Eduroam ne bloque pas salement XMPP, c'est déjà ça...

21:26 ✓
neox Est-ce que quelqu'un ici saurait où retrouver l'image qui présentait un tableau comparatif des messageries instantanées en fonction de leur décentralisation ?

neox la cherche désespérément et ne trouve plus

19:59 ✓
neox Ok trouvée : https://www.freie-messenger.de/dateien/system/Messenger_FR.PDF

20:32
neox, tu as aussi https://eylenburg.github.io/im_comparison.htm mais qui est moins graphique.

20:43 ✓
neox Nicoss, je cherchais pour ma conf demain, donc ouais besoin de graphique :x

20:44
En effet, ça sera plus simple.

21:05
(Concernant l'infographie) J'ai pas particulièrement envie de défendre signal, mais ils ne luttent pas activement contre les clients tiers (ils n'aident pas non plus) et le code source du serveur est maintenant publié.

À l'instant ✓
neox nicoco, pas entièrement cf <https://signal.org/blog/keeping-spam-off-signal/>

+

☰

Sécurité & Vie Privée À l'instant
neox: nicoco, pas entièrement cf https:...

Hier

Il y a 7 minutes
I sent you an OMEMO encrypted me... 2

21:28
XMPP Service Operators 142
it's unethical

21:06
Gajim 371
I have version 0.11.10 - as fa...

20:55
Conversations Offtopic
welcome to georgiastan

20:48

20:42
LOL fungag@muc.chapril.org 35

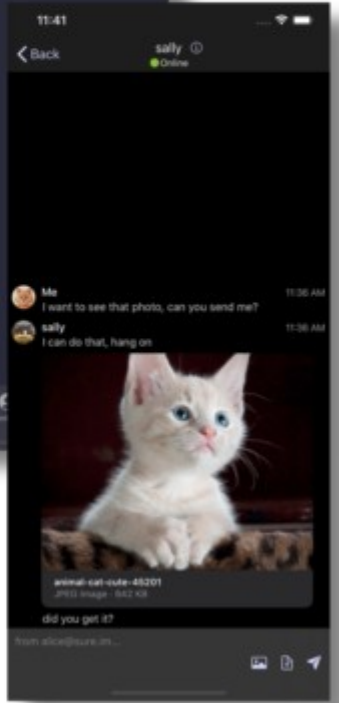
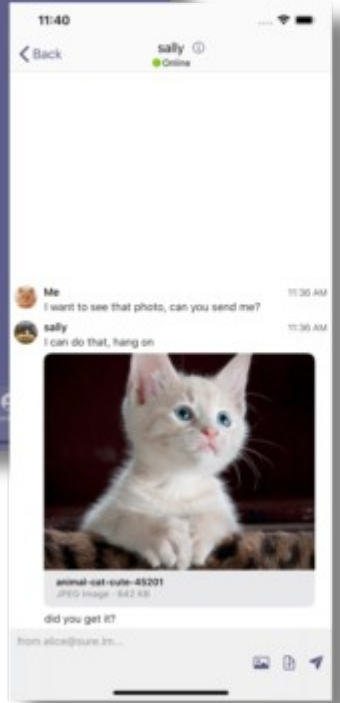
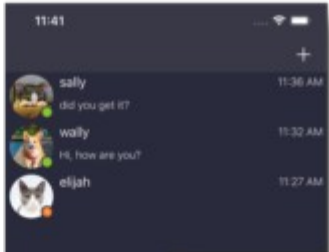
19:57
ejabberd@conference.pro... 2
i like sqlite3, cause in certai...

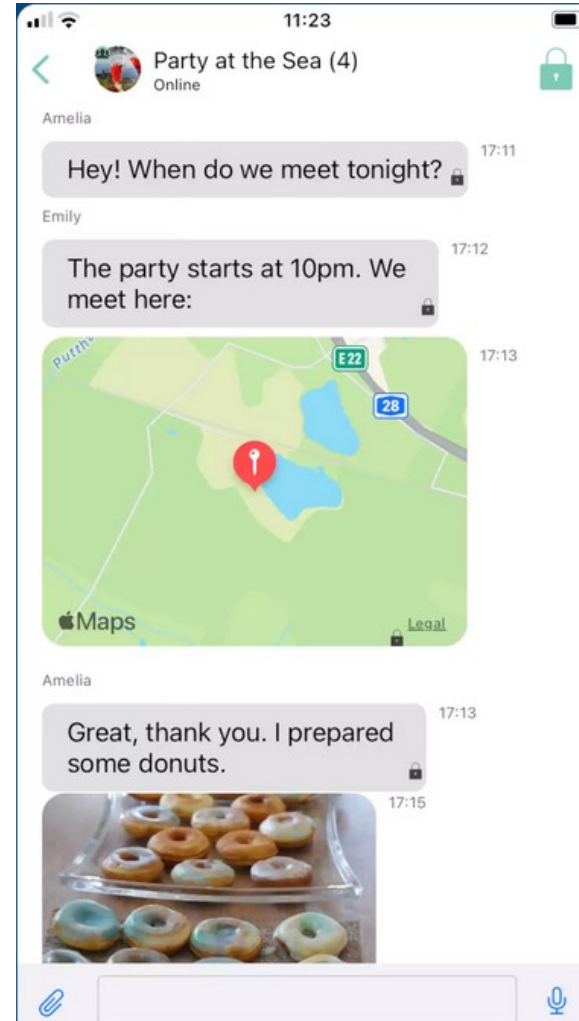
19:02
Chalec
Woah on a de la pub pour nous ...

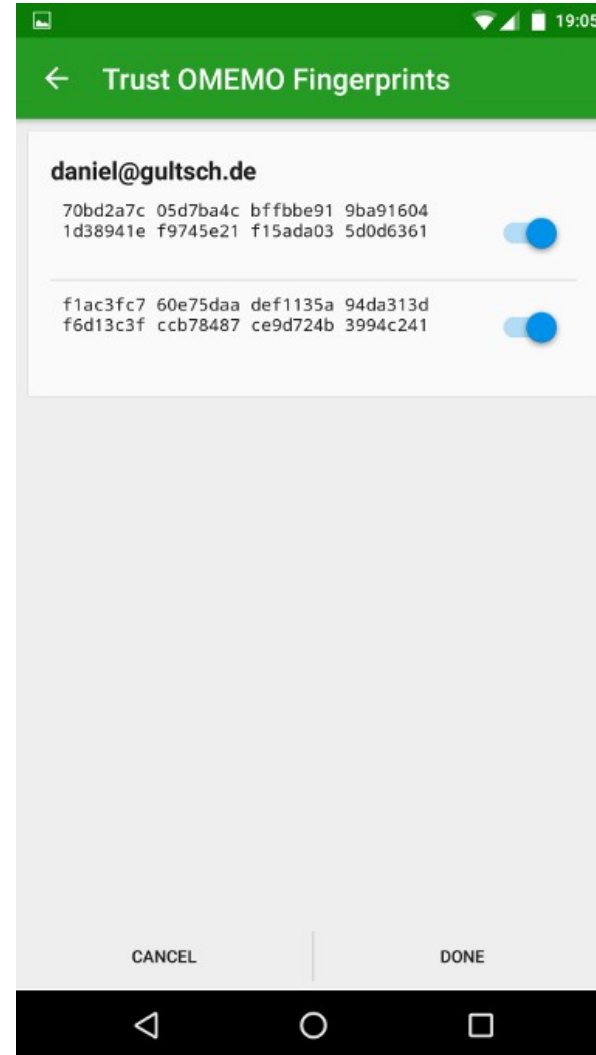
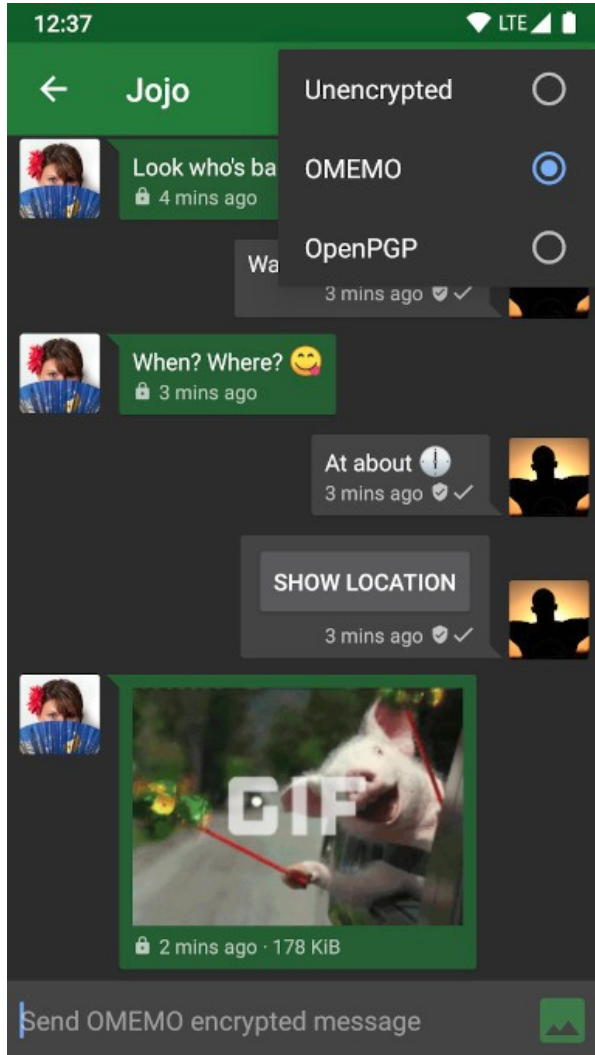
18:55
Open Hardware Chat 75
did like their warnin...

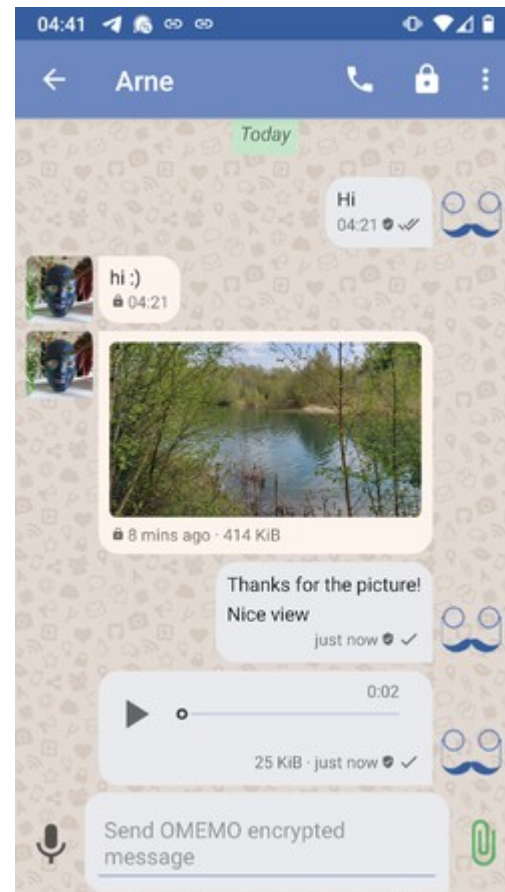
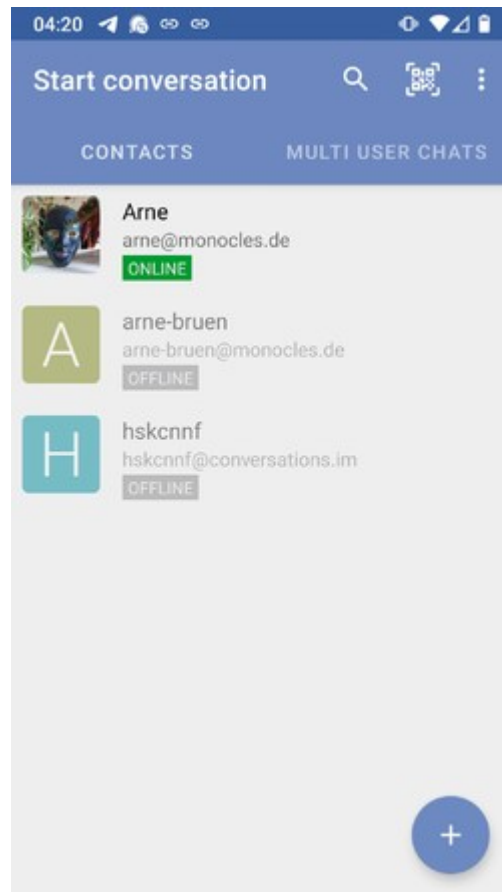
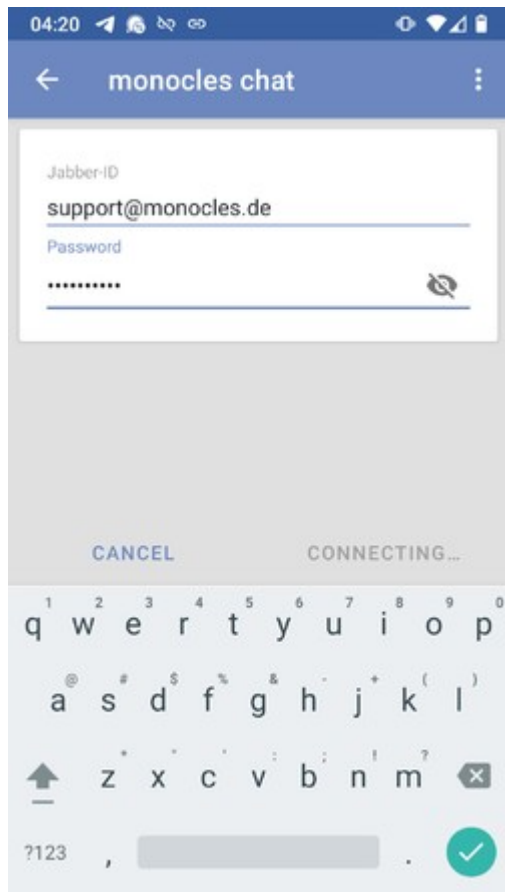
🔗 |

😊









Conclusion

- Évitez les messageries centralisées et privatives !
- Utilisez XMPP :
 - libre
 - fédéré :
 - choisissez vos client
 - choisissez vos services (voire autohébergez !)
 - changez de service quand vous avez envie !
- Diffusez !

Références

- <https://arstechnica.com/information-technology/2009/06/windows-live-messenger-has-330-million-active-users/>
- <https://www.techspot.com/article/1771-icq/>
- <https://web.archive.org/web/20101030030304/http://www.bigblueball.com/forums/general-other-im-news/34413-im-market-share.html>
- <http://gregoire.menuel.free.fr/slides/aldil-2009-02-05.pdf>
- <https://en.wikipedia.org/wiki/PRISM>
- https://www.lexpress.fr/economie/high-tech/scandales-de-facebook_1492120.html
- https://www.lemonde.fr/pixels/article/2022/08/11/avortement-illegal-aux-etats-unis-facebook-critique-pour-avoir-fourni-a-la-justice-des-messages-privés_6137767_4408996.html
- <https://www.01net.com/actualites/oui-whatsapp-peut-lire-vos-messages-dans-certains-cas-2047992.html>
- <https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users>
- <https://appleinsider.com/articles/20/04/03/facebook-tried-to-buy-nso-groups-ios-spyware-to-monitor-iphone-users>
- https://www.ssi.gouv.fr/uploads/2017/10/chiffrement_messaging_instantanee_fmaury_anssi.pdf
- <https://conversations.im/omemo/audit.pdf>

Médias

- Comparaison de différentes messageries (CC BY-SA 4.0 www.freie-messenger.de), https://www.freie-messenger.de/dateien/system/Messenger_FR.PDF
- XMPP usage militaire (CC BY-SA 4.0 www.freie-messenger.de), <https://www.freie-messenger.de/grafiken/xmpp-military.png>
- Logos des applications XMPP, tous publiés sous licences libres par leurs auteurices respectifs
- Logo du World Wide Web, (Tim-Berners Lee, CC0)
- Image de silo à grain (Anonyme, CC0)
- Captures d'écran des documents PRISM (NSA/CIA, domaine public)
- Image paysage montagne et lac (Anonyme, CC0)
- Images provenant de <https://signal.org/blog/advanced-ratcheting/>
- Captures d'écran Gajim et Dino personnelles
- Captures de <https://monal-im.org/>, <https://siskin.im/>, <https://conversations.im/>, https://monocles.wiki/index.php?title=Monocles_Chat publiées sous licences libres diverses



Merci !