

Matrix

Root66

May 9, 2025



① Matrix

- écosystème
- décentralisation
- utilisation
- client
- notifications
- bridges

② Chiffrement

- Chiffrement de bout en bout
- Chiffrement dans Matrix
- détails

③ Auto-hébergement

- matériel
- homeserver

④ Questions et mise en pratique

Matrix

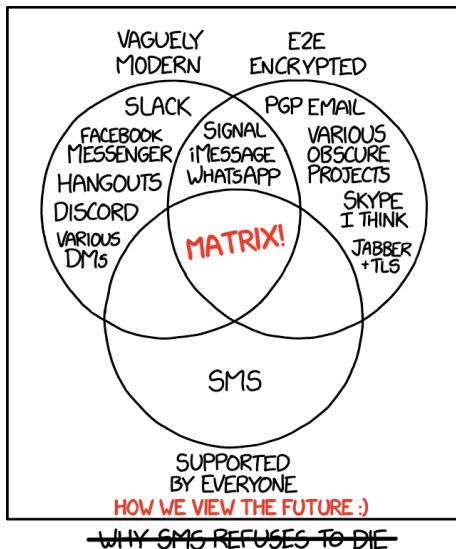
- Qu'est-ce que Matrix?



- Matrix est un protocole de communication ouvert et décentralisé

matrix

Matrix



Matrix est un protocole avec tout un écosystème autour.

- des clients
- des serveurs
- des bridges
- des intégrations et bibliothèques pour les développeurs

Matrix - écosystème

Qu'est ce qu'un client? Un serveur? Un bridge?

- Un client est l'application qu'un utilisateur installe sur sa machine ou accède via un navigateur.
(<https://matrix.org/ecosystem/clients/>)



- Un "homeserver" est la partie installée sur un serveur et formant un nœud Matrix.




























(<https://matrix.org/ecosystem/servers/>)

```
[fire@fedora ~]$ podman pod ls
```

POD ID	NAME	STATUS	CREATED	INFRA ID	# OF CONTAINERS
8d86679b4dd9	gitea	Running	13 hours ago	1c0924c05ada	3
d2811e6a9380	synapse	Running	13 hours ago	11833a8efbbf	5

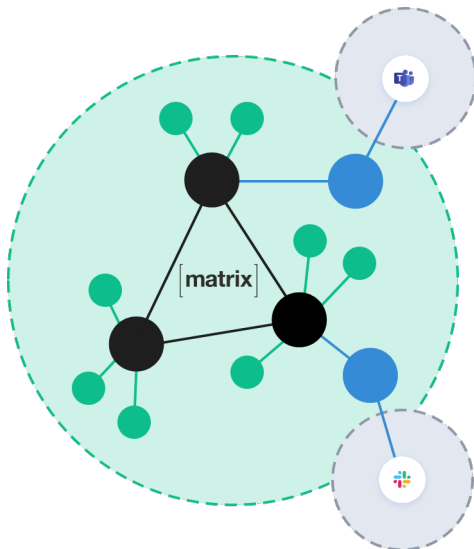
Matrix - écosystème

- Un bridge est une surcouche d'application installée à côté d'un serveur pour échanger des données avec une autre plateforme. (<https://matrix.org/ecosystem/bridges/>)

 Discord 4 bridges	 Slack 4 bridges	 Signal 1 bridge
 Telegram 1 bridge	 WhatsApp 1 bridge	 Messenger 2 bridges
 iMessage 1 bridge	 Mattermost 2 bridges	 Google Chat 1 bridge
 Mumble 1 bridge	 Instagram 2 bridges	 LinkedIn 1 bridge
 Twitter 1 bridge	 Skype 1 bridge	 SMS 3 bridges
 Email 1 bridge	 IRC 2 bridges	 Nextcloud Talk No bridge
 Mastodon No bridge	 KakaoTalk 1 bridge	 GroupMe 1 bridge
 LINE 1 bridge	 WeChat 2 bridges	 Tencent QQ 1 bridge
 Tox No bridge	 XMPP 2 bridges	 Zulip 1 bridge

Matrix - décentralisation

- Qu'est-ce que la décentralisation et pourquoi décentraliser?

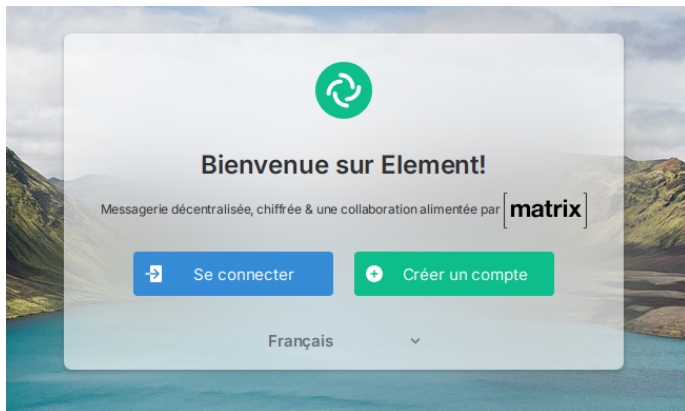


Comment créer un compte?

- le plus simple: sur l'instance officielle matrix.org
`https://app.element.io/`
- autre possibilité: Une instance publique
`https://servers.joinmatrix.org/`
- pour les utilisateurs plus avancés: héberger son propre serveur.

Matrix - utilisation

Créer un compte sur l'instance matrix.org
(<https://app.element.io> pour le faire via son navigateur)



Matrix - utilisation



Français



Créer un compte

Héberger le compte sur



matrix.org

[Modifier](#)

Rejoignez des millions d'utilisateurs
gratuitement sur le plus grand serveur public

Continuer

Vous avez déjà un compte ? [Connectez-vous ici](#)

Matrix - client

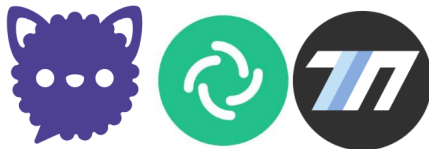
Quel client utiliser?

Il y a des dizaines de clients, avec certaines fonctionnalités ou non, voir celui qui vous convient le mieux sur

<https://matrix.org/ecosystem/clients/>

Mes recommandations:

- Fluffychat (Linux, android, web)
- Element (Linux, android, web)
- Nheko (Linux)



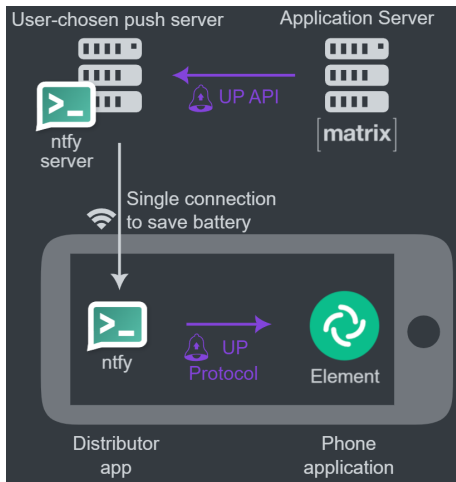
Pour les notifications avec les applications android, il y a en général 2 possibilités:

- Push notifications
Google ou UnifiedPush
- Websockets Défaut: utilisation de la batterie plus importante.

parenthèse: Signal n'utilise que des websockets pour les push notifications Google, mais le fork Molly permet d'utiliser le système UnifiedPush

Matrix - notifications

push notifications avec Unified Push



UnifiedPush permet de fournir une alternative décentralisée aux notifications push utilisant les services Google.

Comment utiliser le système UnifiedPush?

- L'application ntfy (F-Droid) sur smartphone, et un push serveur.

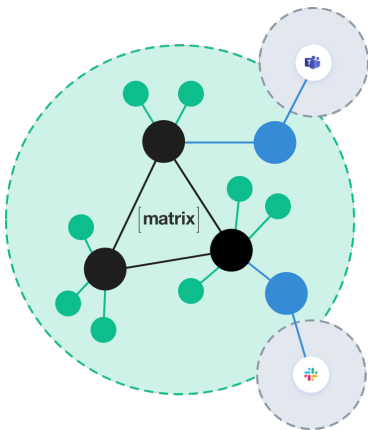


- Pour le push serveur, le plus simple: `ntfy.sh`
- Pour les utilisateurs avancés: héberger ntfy

Matrix - bridges

Comment communiquer avec des utilisateurs utilisant une autre messagerie?

Avec un bridge!



Utilisation d'un bridge:

- Le bridge doit être installé sur le serveur que vous utilisez. (pas de bridges sur l'instance officielle matrix.org)
- Il faut donc choisir son serveur en conséquence, ou le plus simple et sécurisé si on maîtrise: l'autohébergement.
- D'autres solution existent, beeper utilisant matrix et des bridge pour rassembler vos messageries mais le client n'est pas complètement open source.

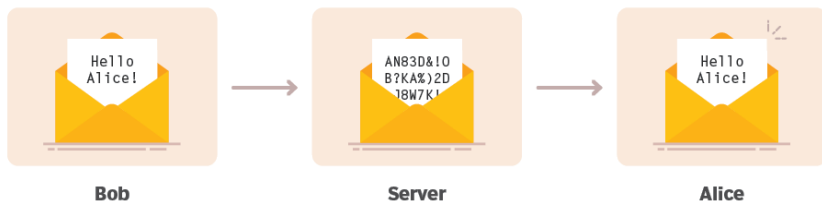
Utilisation d'un bridge:

- le bridge utilise un utilisateur, généralement le nom du service + bot (discordbot, twitterbot etc...).
- Chaque utilisateur sur le serveur peut lui fournir son nom d'utilisateur, mot de passe ou token et le bridge gère lui même l'authentification sur le service et le transfert des messages.
- Concrètement on peut envoyer et lire les messages dans un salon matrix de la même façon que pour ses conversations avec des utilisateurs de matrix.

Attention: même si le salon côté matrix est chiffré, la sécurité dépend toujours du maillon le plus faible. Autrement dit, un bridge est "pratique" mais la conversation reste non sécurisée si on bridge avec une messagerie propriétaire ou non chiffrée.

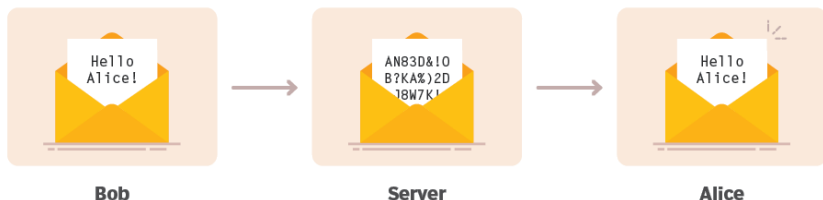
Chiffrement

- TLS avec HTTPS
connexion sécurisée entre le serveur et le client
le serveur peut lire le contenu des messages si on utilise uniquement cette couche de chiffrement.
- E2EE (End to End Encryption, chiffrement de bout en bout)
on applique une couche de chiffrement et seulement les personnes communiquant possèdent la clé.
le serveur ne connaît pas le contenu du message.



Chiffrement - E2EE

- Chiffrement de bout en bout garanti la sécurité entre l'appareil d'Alice et celui de Bob.
D'où l'importance d'un client open source pour garantir que seul le chiffré destiné à Alice soit envoyé.



- éviter les messageries non chiffrées ainsi que celles chiffrées mais avec un client propriétaire.



- Donc on utilise quoi?

[matrix]

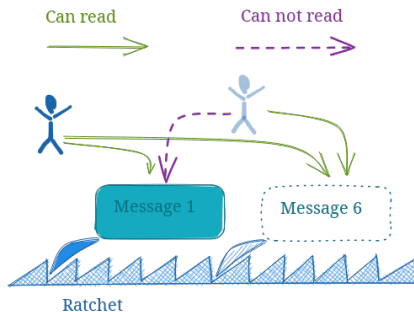
Chiffrement - double ratchet

- Comment fonctionne le chiffrement dans Matrix?
Matrix utilise les algorithmes Olm et Megolm.
- Algorithmes utilisant des "ratchet" (rochet)



Chiffrement - double ratchet

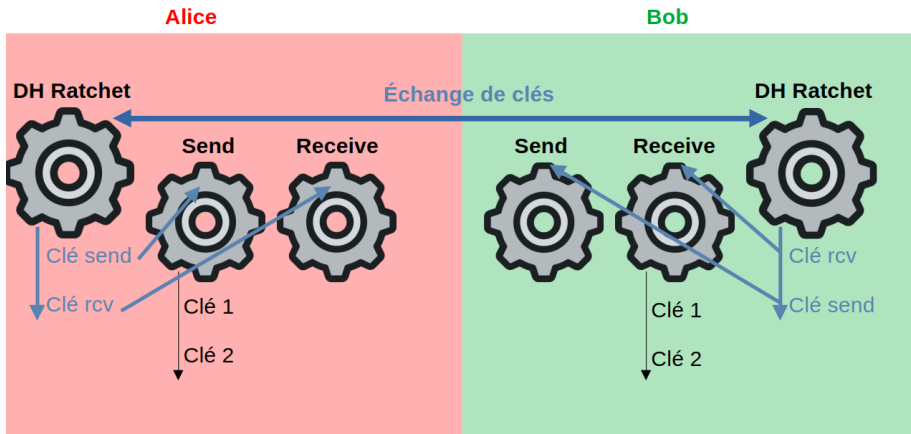
- Pourquoi utiliser des ratchets?



Un attaquant ne doit pas pouvoir lire tous les messages en compromettant une seule clé. On change de clé tous les 7 jours, ou 100 messages.

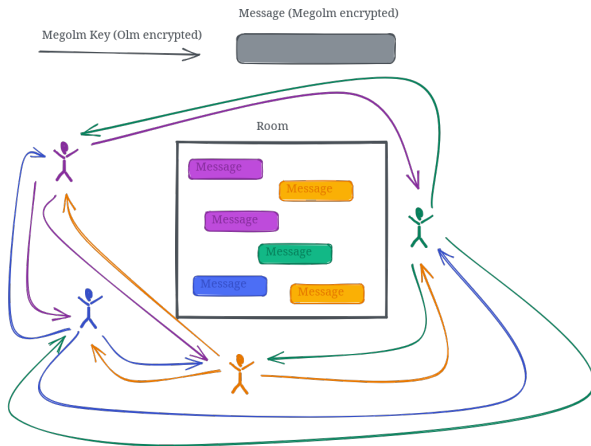
Chiffrement - double ratchet

Double ratchet Olm



Chiffrement - groupes

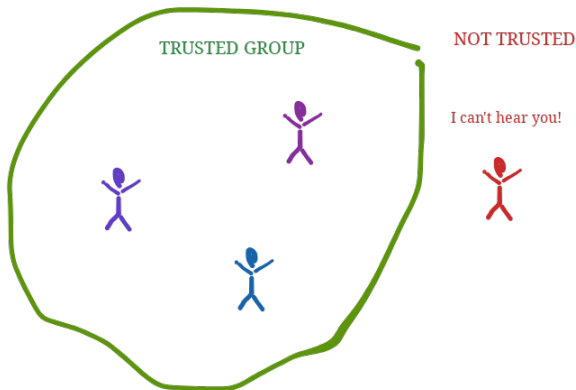
- Et dans les groupes?
On utilise Olm pour échanger une clé Megolm entre tous les membres "de confiance" du groupe.
On dérive ensuite les clé de chiffrements de la clé Megolm.



Chiffrement - groupes

Des limites au chiffrement?

- Avec Megolm on peut chiffrer sans dégradation des performances un salon avec beaucoup d'utilisateurs.
- Mais il faut savoir avec qui on peut partager la clé Megolm.



Chiffrement - plus en détail

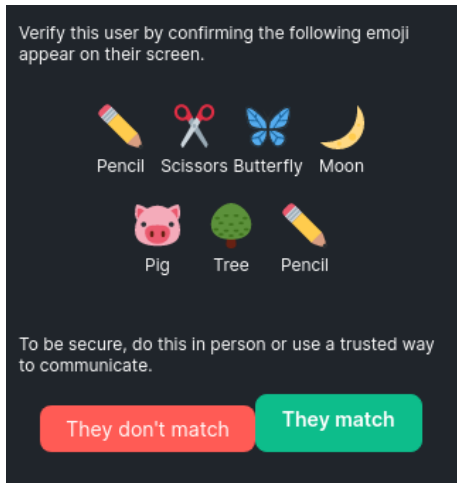
Comment dériver des clés?

Comment chiffrer?

Comment s'assurer que l'on communique avec la bonne personne?

Chiffrement - plus en détail

Pour vérifier que l'on communique avec la bonne personne Matrix utilise une vérification par émoji pour identifier les sessions et participants.



Chiffrement - plus en détail

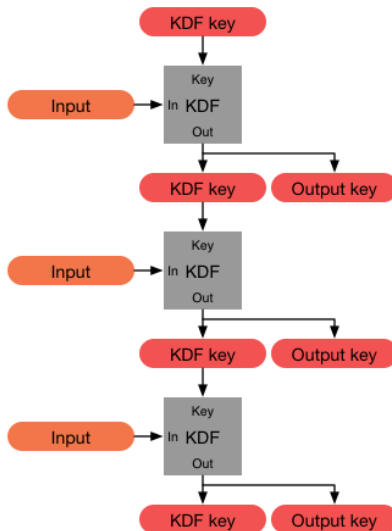
Entre les appareils, De la cryptographie sur courbe elliptique (courbe 25519) est utilisé pour signer les messages et créer des clés communes de manière sécurisée.

AES-256 avec un mode opératoire CTR est utilisé pour chiffrer les messages

Un HMAC sha-256 est utiliser pour garantir l'intégrité et l'authenticité des messages. (SHA-256 est également utilisé pour dériver des clés.)

Chiffrement - plus en détail

Comment dériver des clés?



Comment héberger un serveur matrix?

- Le matériel nécessaire?
- Quel "homeserver" installer?
- besoins supplémentaires? (bridges)

Les besoins en ressources dépendent de:

- Si on compte rejoindre des "grands" salons ou non. Fédérer avec beaucoup d'utilisateurs consomme plus de RAM.

(On peut empêcher ses utilisateurs de rejoindre des grands salons dans la configuration du homeserver).

- Quel homeserver on utilise.

Auto-hébergement - matériel

Pour communiquer avec juste des amis, installer 2 ou 3 bridges, et ne pas rejoindre de salons publics, un raspberry pi (4 ou 5) est suffisant.



Pour donner une idée, mon instance avec synapse et 2 bridges consomme 200MB de RAM

```
[fire@fedora ~]$ podman stats | grep synapse
```

0fdad92e61e4	synapse -app	0.50%	113.3MB / 17.73GB	0.64%
d7be247b6558	synapse -discord-mautrix	0.04%	35.15MB / 17.73GB	0.20%
e3f7f4cccc446	synapse -twitter-mautrix	0.01%	7.197MB / 17.73GB	0.04%
fd3404db2a7b	synapse -db	0.13%	54.42MB / 17.73GB	0.31%

(moins que nextcloud!)

Plusieurs choix pour son homeserver.

- Contrairement aux clients, les homeservers suivent un standard et les fonctionnalités sont (normalement) identiques. Seule l'implémentation diffère.
- Pour la compatibilité avec les bridges, un homeserver implémentant le standard le plus récent est mieux.

Homeservers disponibles:

- **Synapse**

avantage: stable, maintenu par la fondation Matrix

défaut: implémenté en python

- **Dendrite**

avantage: implémenté en go

défaut: maintenu par matrix quand ils ont le temps (donc très souvent en retard par rapport à synapse)

- **Conduit**

avantage: implémenté en rust, globalement mieux maintenu que dendrite

note: maintenu par des volontaires et non matrix

- et d'autres: telodendria, construct...

attention, il est difficile voire impossible de changer de homeserver tout en conservant l'historique des messages et les salons.

Des questions?