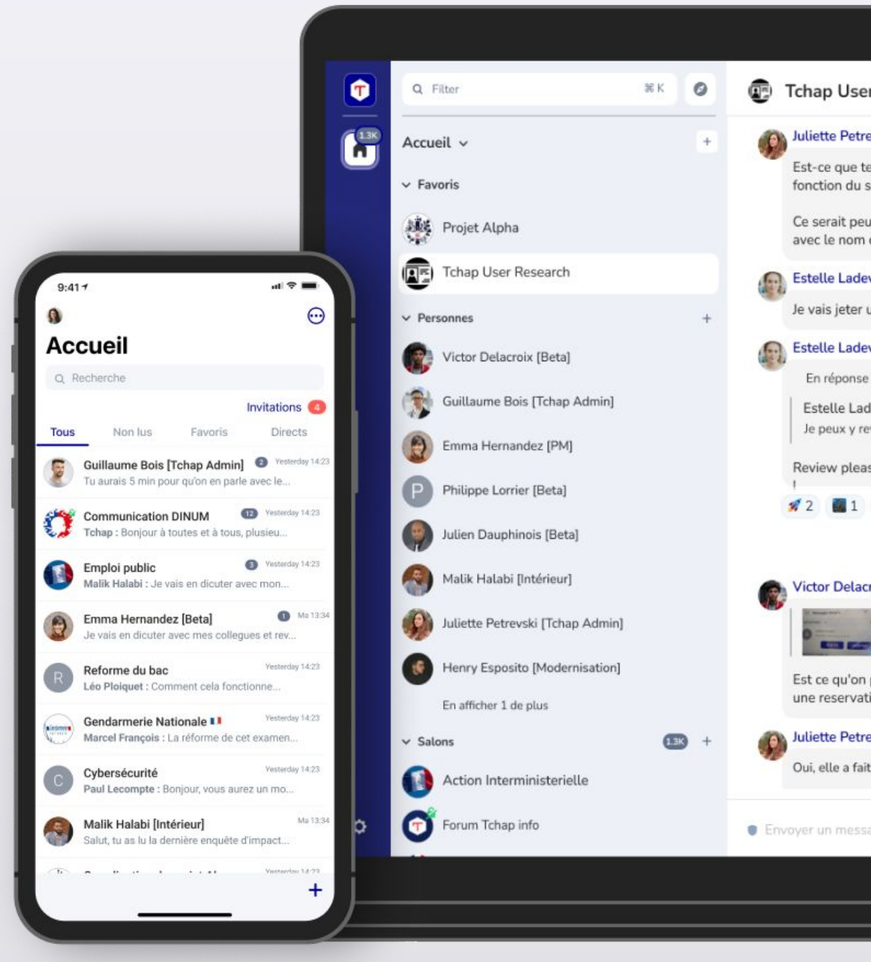
Matrix Conf 2025

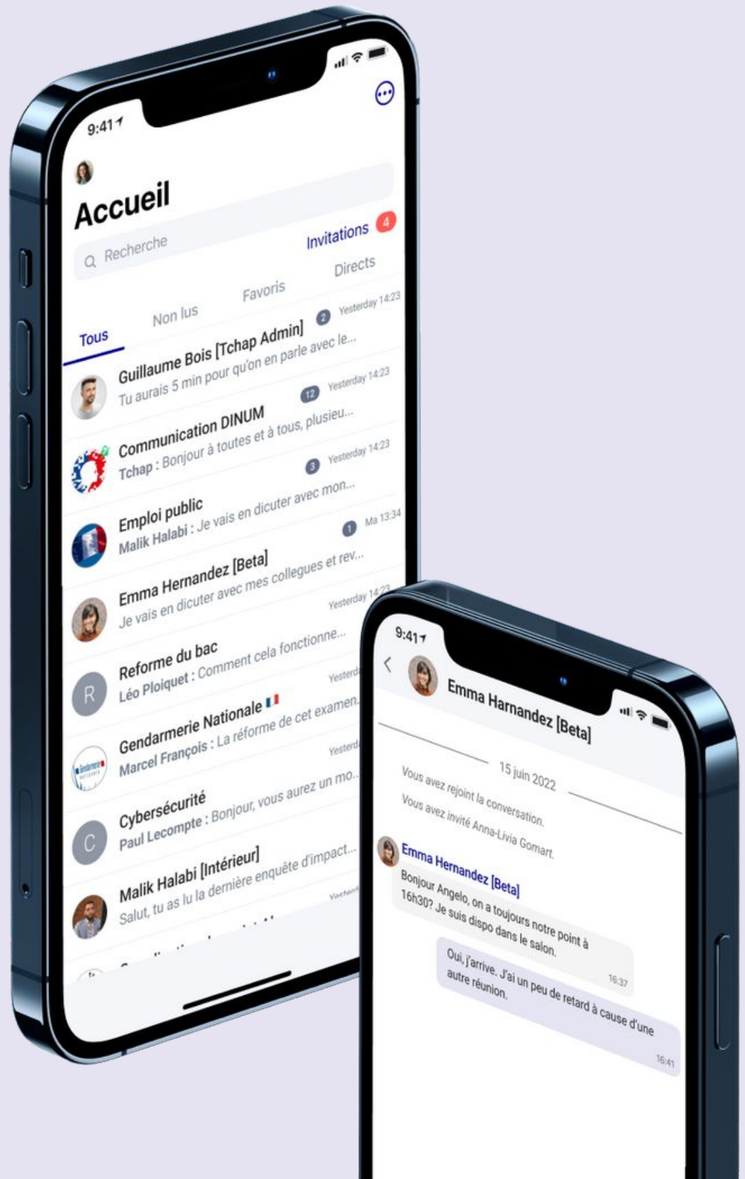
Tchap

Matrix French gov deployment: opening a private federation securely



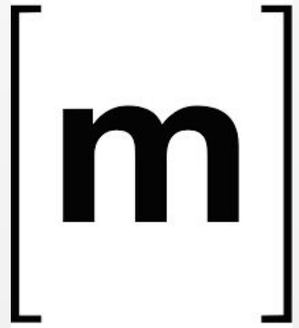
What we’re going to talk about

- Matrix in France
- Tchap’s specificities
- Tchap’s aspirations
- Open the Federation
  - Simple Border Gateway
  - Trust model



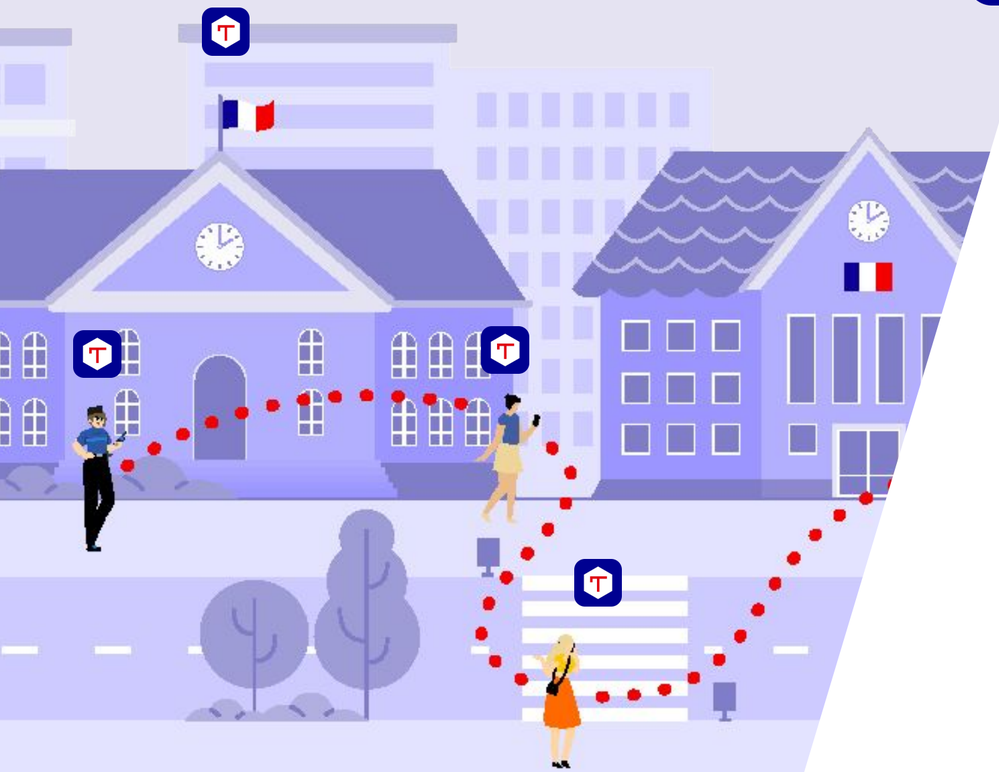
The Matrix Protocol

Tchap



Matrix

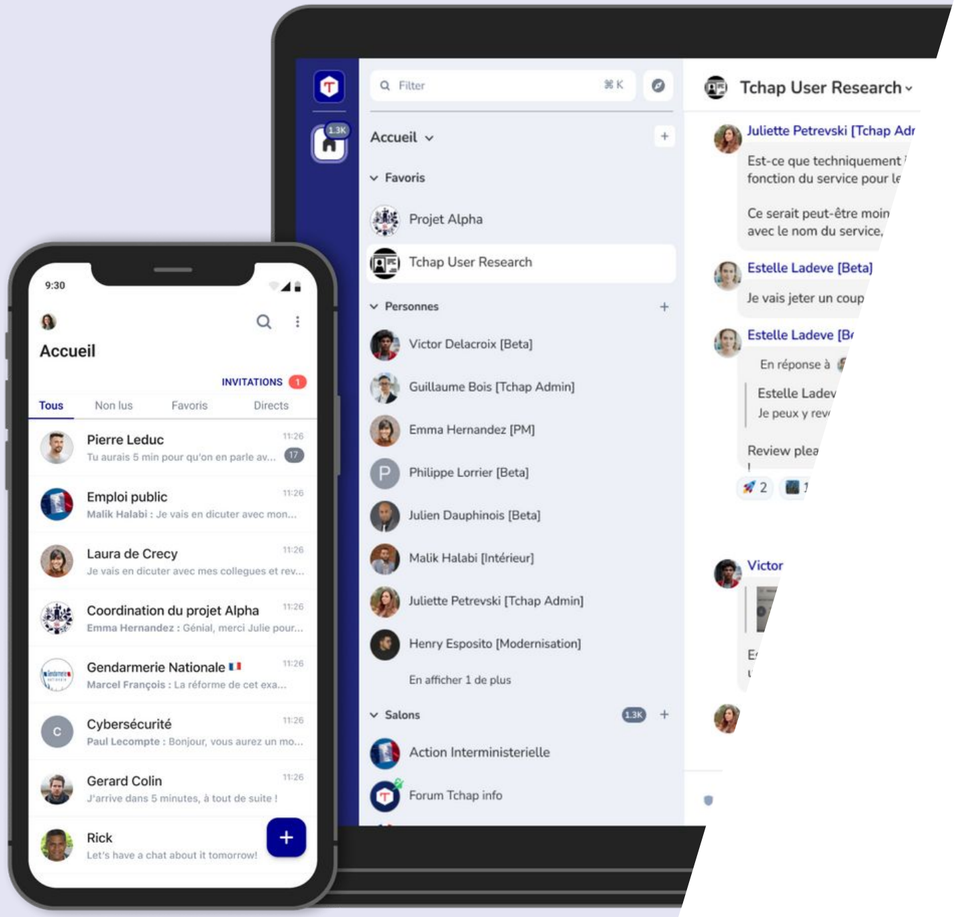
About Tchap



Tchap is the French public sector instant messaging tool.

It’s part of **La Suite** Numerique : some collaborative work tools offered by la Direction Interministérielle du Numérique (DINUM) to all public agents.

Tchap’s specificities



- **Closed federation** but external users (private sector) with restricted possibilities
- 17 homeservers: one for each ministry + one for local authorities + external users
- Antivirus
- Private room vs public room
- Native directory built with email addresses

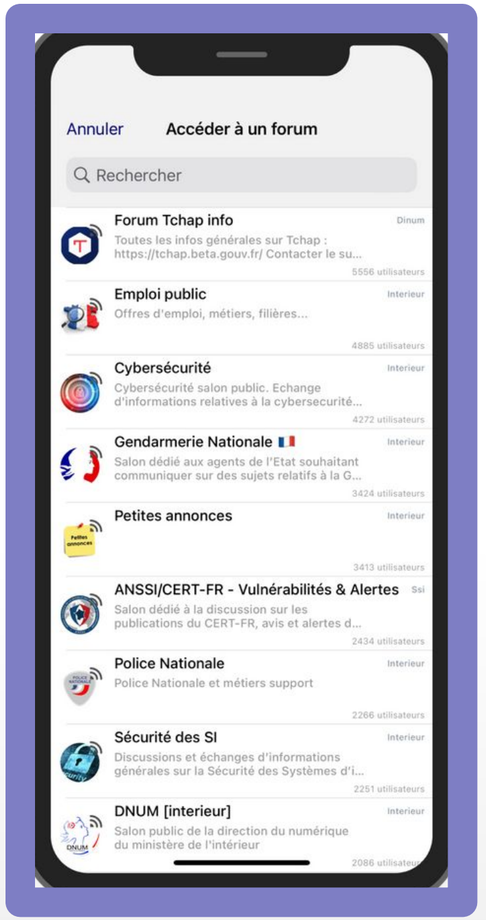
About Tchap

3 clients : Tchap Web, Tchap android, Tchap ios

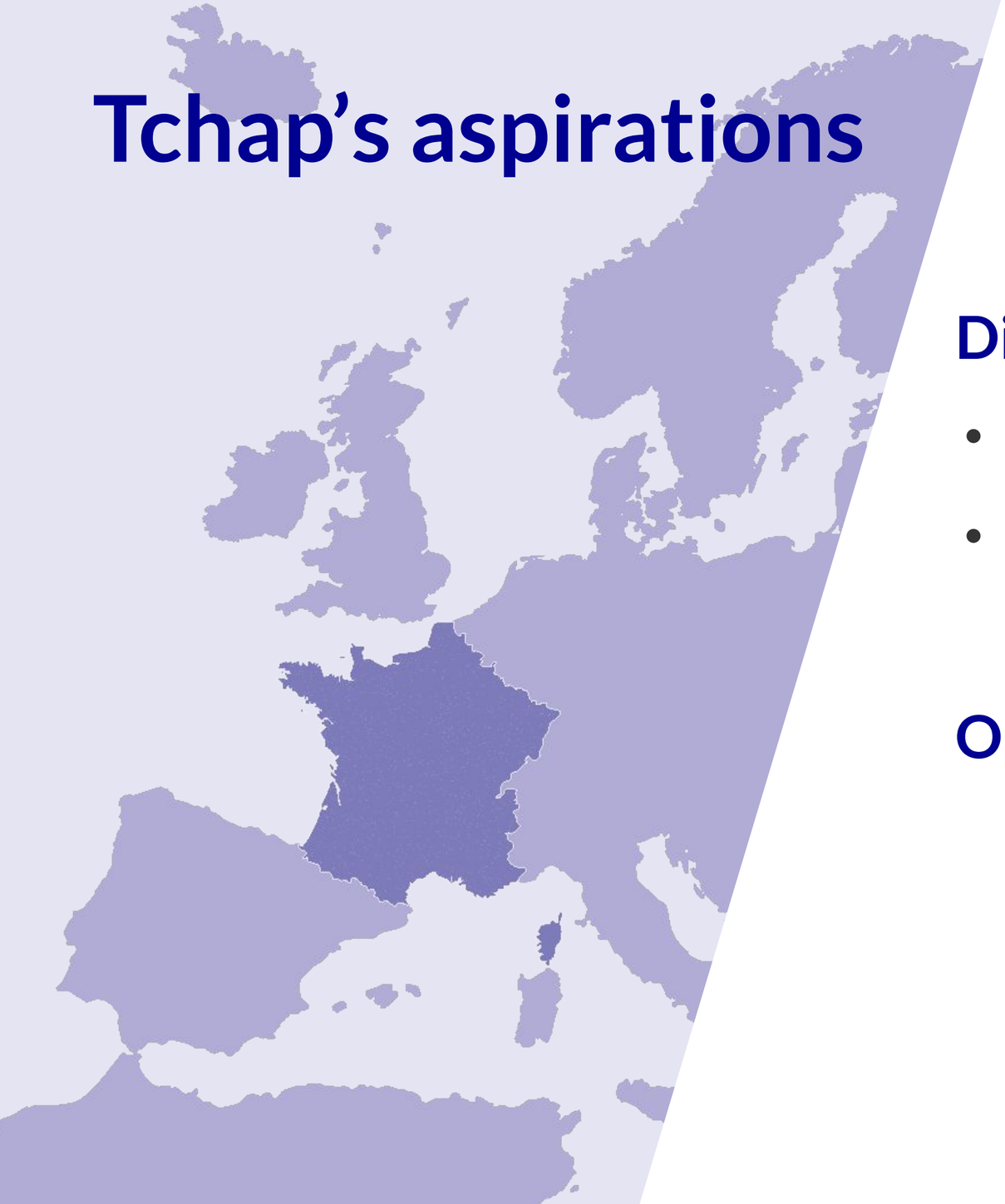
665 000
Accounts on Tchap

10 million
Messages sent each month

375 000 (+25% since May !)
Active users each month



Tchap's aspirations



Digital suite

- Be part of a **La Suite** using ProConnect SSO
- Deeper integration of other tools of La Suite

Open our federation to some others

- Help local authorities deploy Matrix nodes and connect with them
- Connect with other countries too !

Open the Federation, securely!

User impersonation is a big challenge

- Connect to trusted parties only
- Those parties must control their users => the trusted homeserver must be connected to an user directory or SSO
- Display name must be enforced and not user changeable

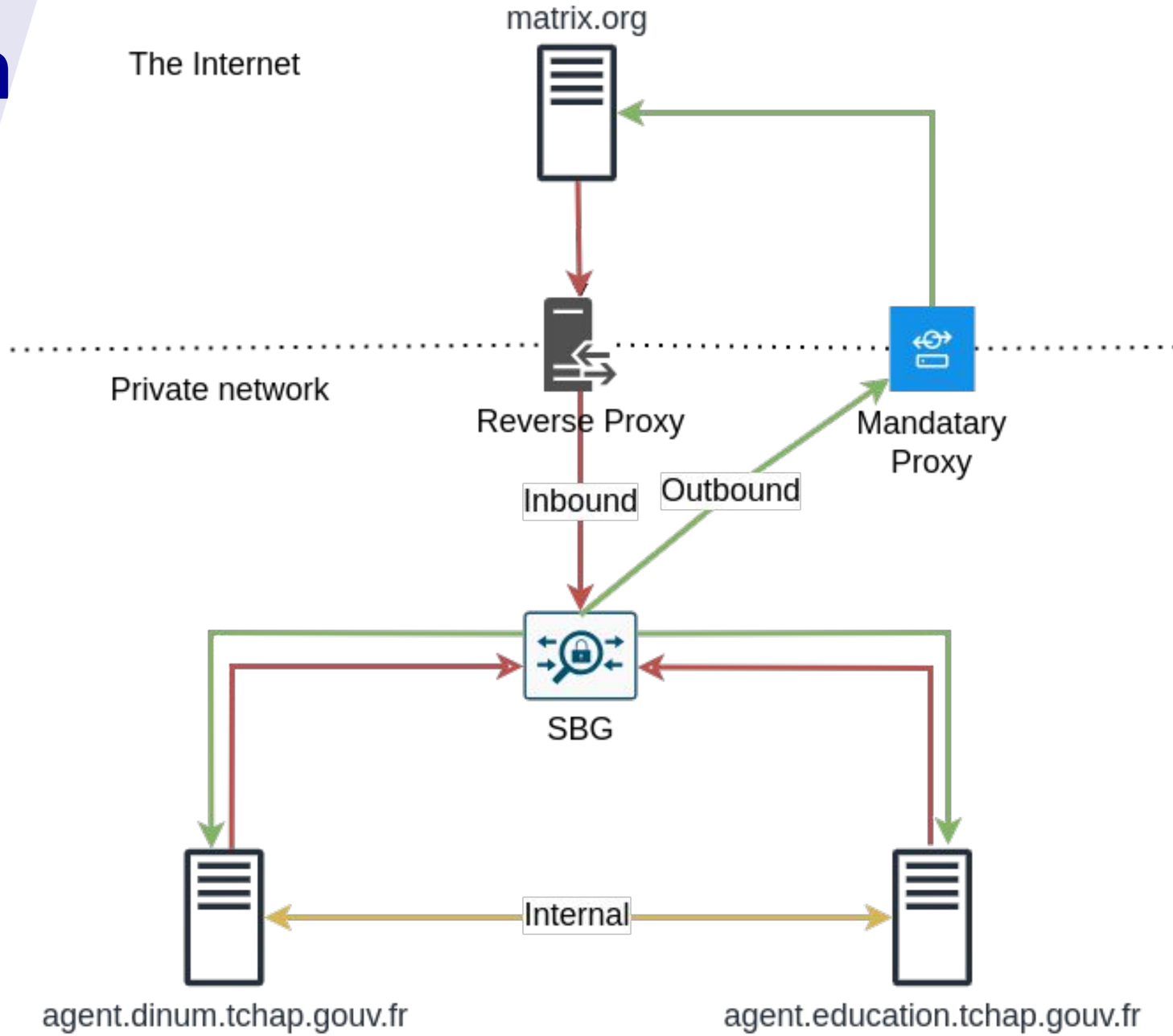
Later on, uses trust levels: needs a LOT of UX/UI work on top of protocol changes

Open the Federation, securely!

Protect Tchap deployment with a border gateway

- Sort of Matrix specific WAF put at the boundary of the network
- Filter both inbound and outbound traffic
- Easy kill switch in case of attack

Open the Federation securely!



Open the Federation, securely!

Inbound traffic

- Only trusted homeservers are allowed
- Signature of authenticated requests is verified
- TLS MITM is avoided (state actor)
  - Matrix signing key is pinned in config

Open the Federation, securely!

Outbound traffic

- Only trusted homeservers are allowed
- We trust the requester so no verification of the request signature here
- Federation domain of the trusted server is pinned in config
  - TODO: pin the TLS root CA? Can help with state actor. Less important than inbound traffic however.

Open the Federation, securely!

Out of scope

- Changing the content of a Matrix transaction
  - Not really possible easily, we would need to resign the transactions with another key and make our homerservers accept this new key
- In the end we still want to restrict some events
  - 2 layers approach
  - room/user level will be done with Synapse modules

Open the Federation, securely!

Trust model

- V1 (ETA end of the year)
  - Can connect to trusted homeservers
  - Homeserver identity is verified, and users are identifiable
  - Will be tested first with some French local authorities
  - Can be opened to some other countries instances later on

Open the Federation, securely!

Trust model

- V1 (ETA end of the year)
  - Users outside of the main Tchap federation have the same set of rights that current external users
    - can only be invited by a Tchap user in a Tchap room opened to external people
    - can’t be nominated as mod/admin
  - Publicly joinable rooms cannot be join at all, in either direction

Open the Federation, securely!

Trust model

- V2 (later in the year)
  - Local authorities should have more rights than external users
  - They should be able to join public rooms of Tchap for example, or even administer rooms
    - big problem here : people from untrusted homeservers could join by transitivity
    - TODO: check existing m.room.server_acl event and current T&S WIP

Open the Federation, securely!

Trust model

- V3 one day?
  - Protocol and clients have evolved to support several trust levels
  - UX needs to be top-notch, securing end users behavior without compromising usability is already hard with a single trust domain
  - On fully open federation one day?

Any questions ?

Tchap

Public money open code

https://github.com/tchapgouv

Don’t hesitate to write to tchap@beta.gouv.fr

Join us in the Federation !