Formation fédération

MARZELLEAU Benoit

COLAS Viktor

Sommaire

- Introduction
  - KE CE KE C
  - Petites définitions
- Un exemple concret : Matrix
- L’authentification unique
  - Fédération d’identité
  - Protocoles (OAuth, OIDC, SAML)
  - Keycloak
- Des exemples concrets : le CAS MiNET, FranceConnect

Introduction : KE CE KE C

- Définition :

  En informatique, une fédération est un groupe de fournisseurs ou de réseaux qui s'accordent sur des normes de fonctionnement (« physique » ou/et logiciel) de manière collective

- Fonctionnement :

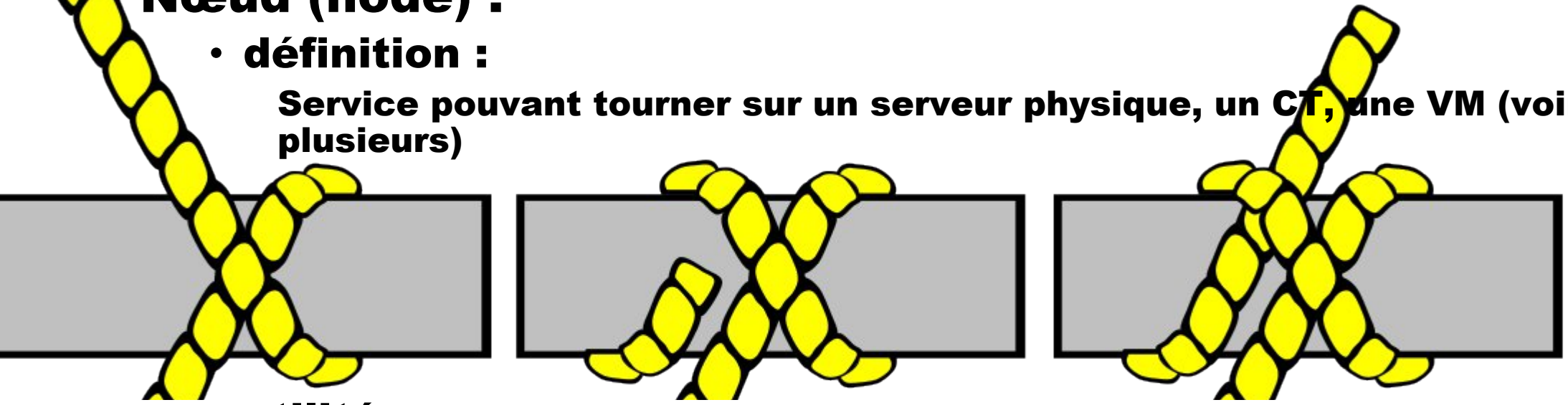
  La fédération permet une décentralisation des données et des informations tout en permettant l'accès avec une identification unique. La fédération est composée de nœuds (nodes)

Introduction : petite définition

Nœud (node) :

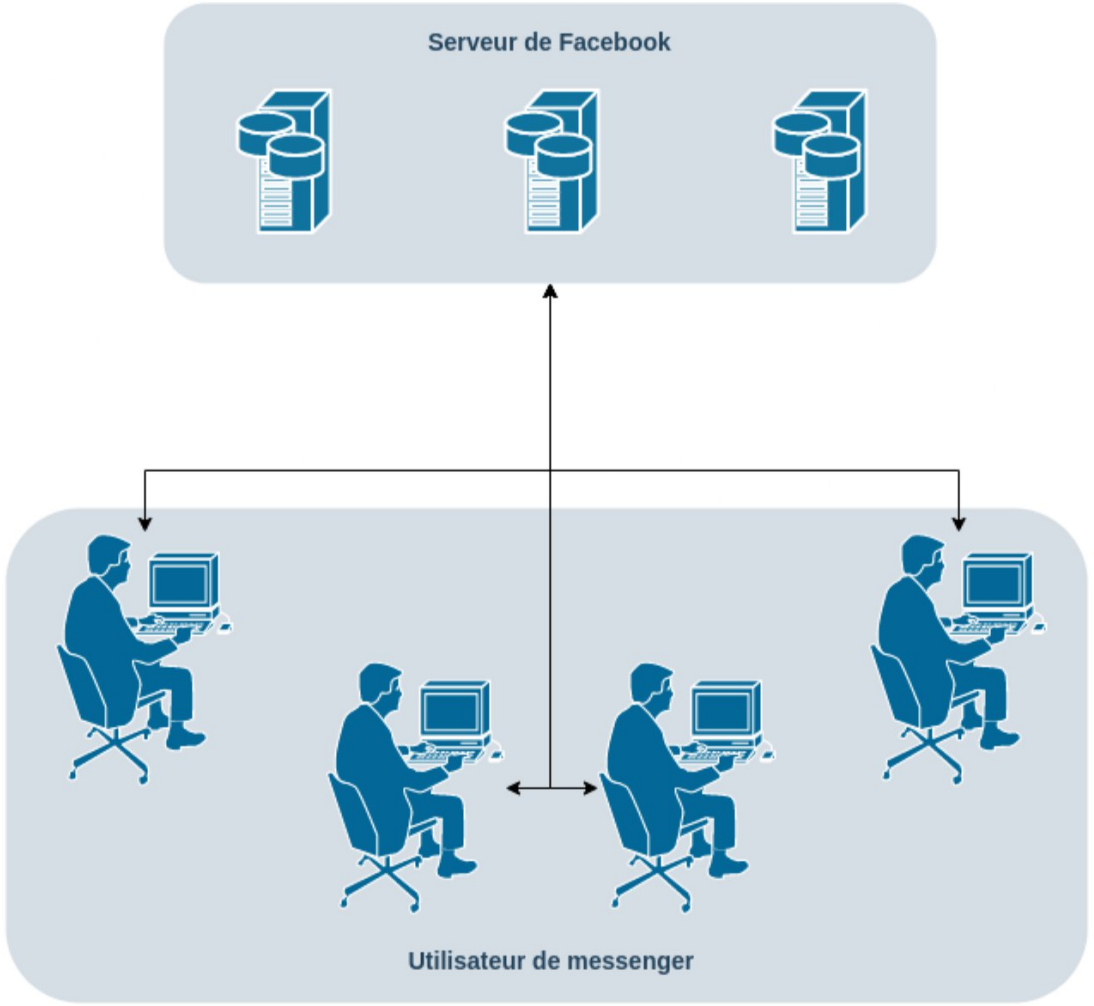
- **définition :**

  Service pouvant tourner sur un serveur physique, un CT, une VM (voire plusieurs)

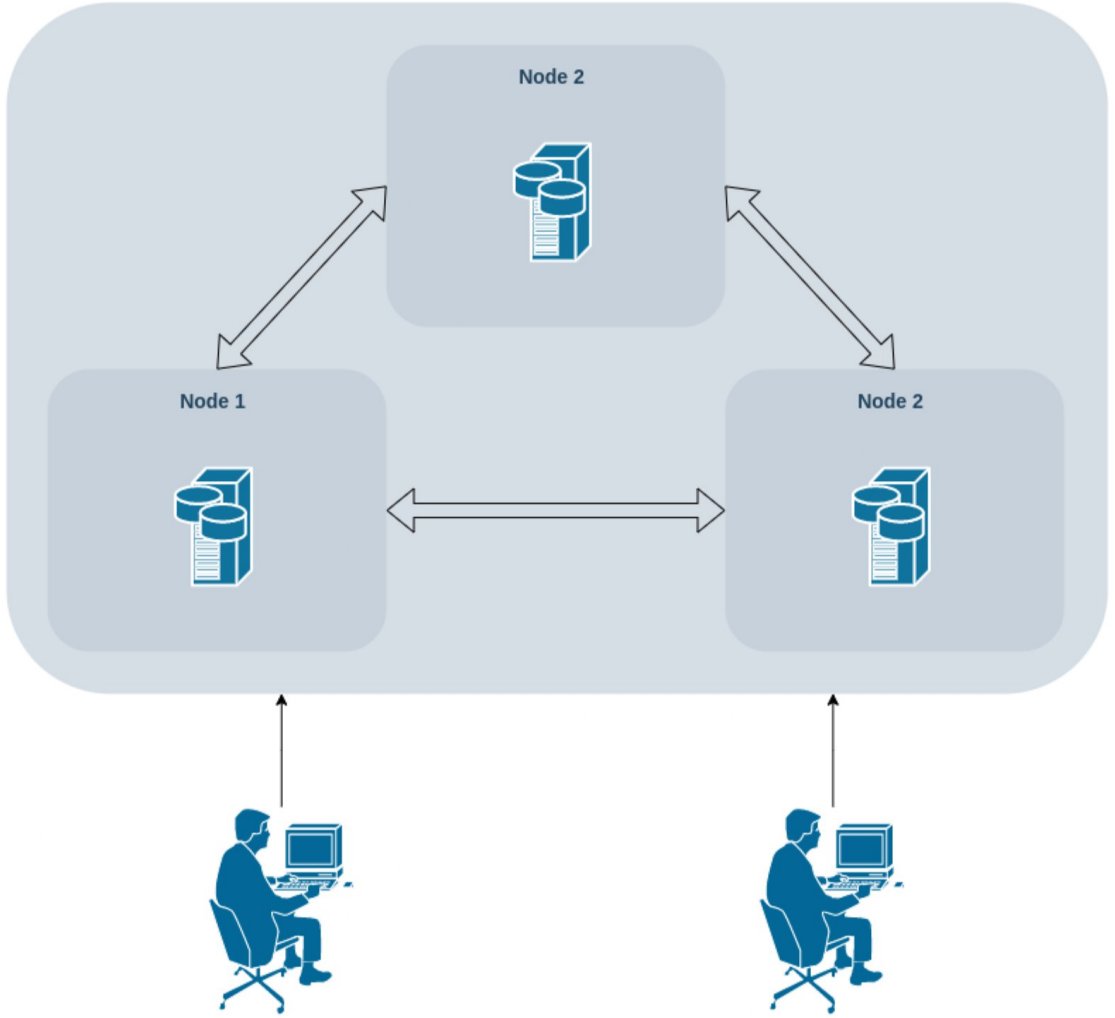


- **utilité :**
  - **Elle contient les infirmations personnelles d'un utilisateur**
  - **Elle permet l'accès (ou non) aux utilisateurs d'autres nœuds à son service**
  - **Assure la connexion aux autres nœuds**

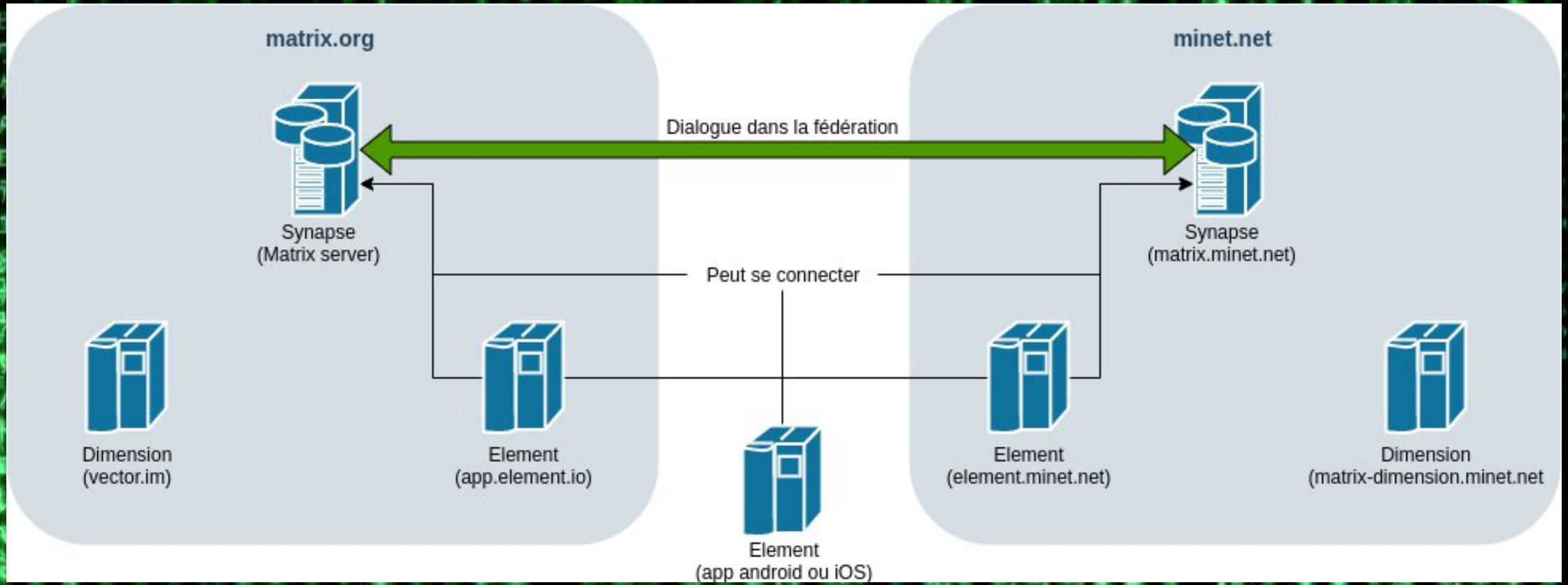
Sans fédération



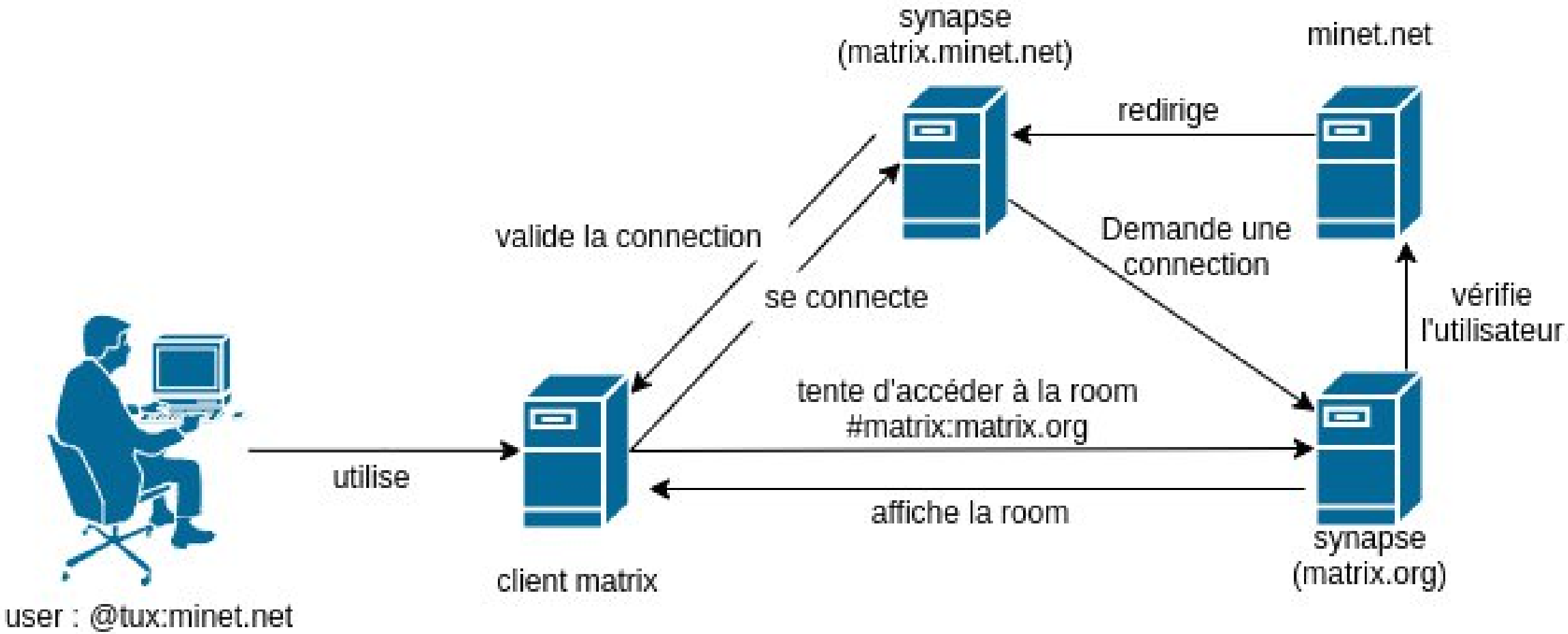
Avec fédération



Un exemple concret : Matrix

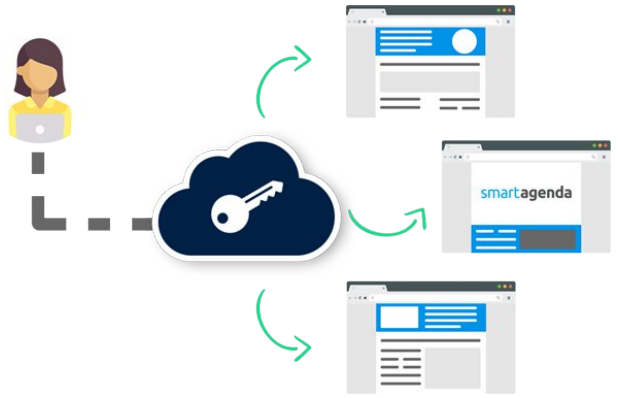


Un exemple concret : Matrix



L’authentification unique

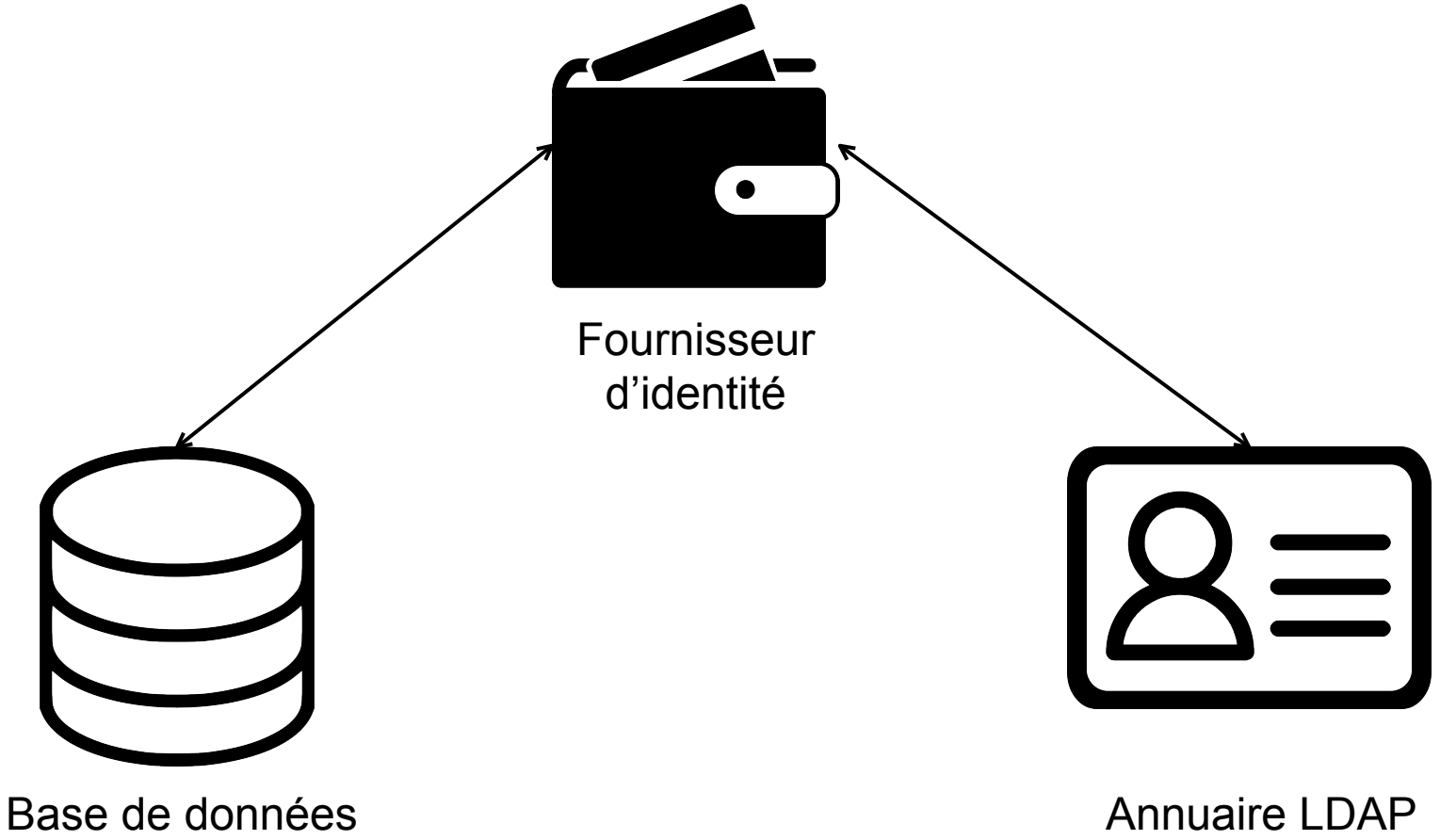
- Une seule authentification pour un ensemble de services



- Fait intervenir deux acteurs :
  - Fournisseur d’identité (*Identity Provider, IP*)
  - Fournisseur de service (*Service Provider, SP*)

Fédération d’identité

- Plusieurs sources d’identité sont rassemblées



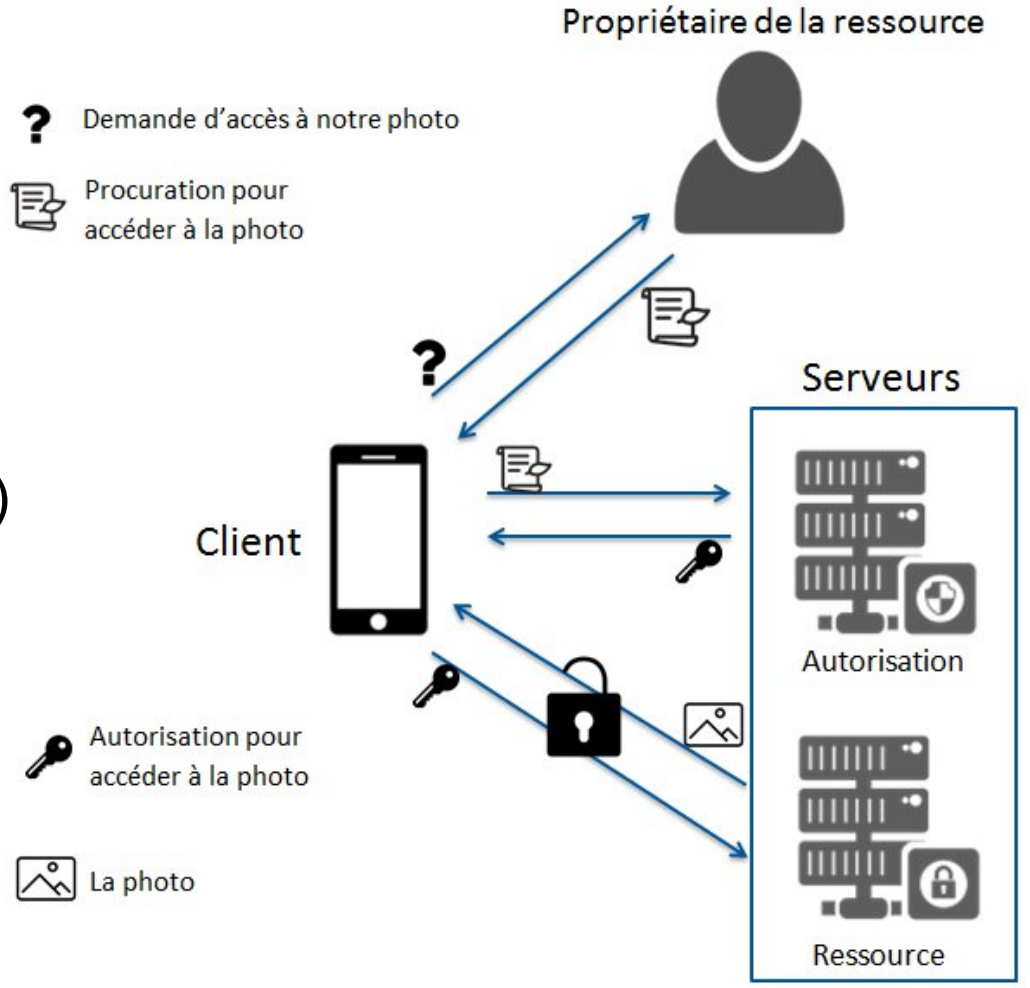
OAuth 2.0 (RFC 5849)

- Protocole de délégation d'autorisation

- Différents acteurs :
  - Propriétaire (*Resource owner*)
  - Client (*Client*)
  - Serveur de ressource (*Resource server*)
  - Serveur d'authorisation (*Authorization server*)

➢ Jeton d'accès (*Access token*)

➢ Jeton de rafraîchissement (*Refresh token*)

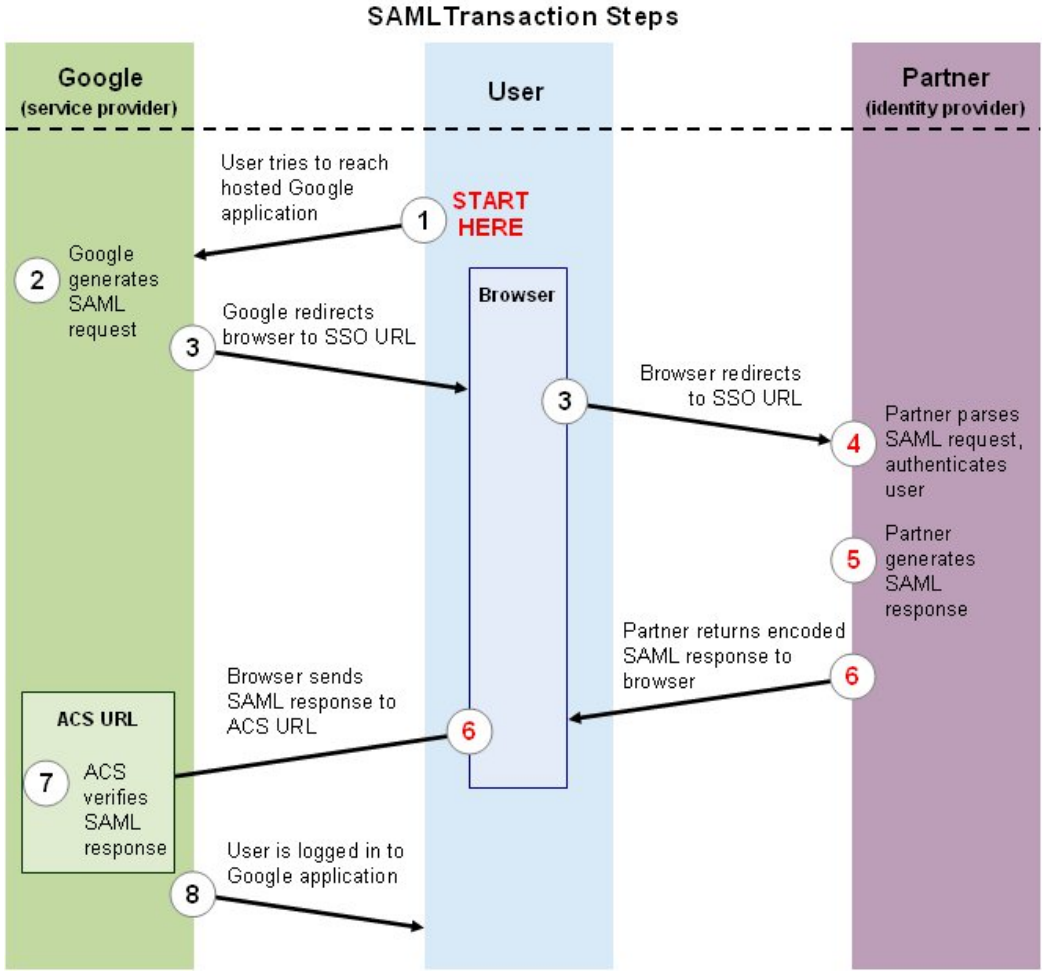


OpenID Connect (OIDC)

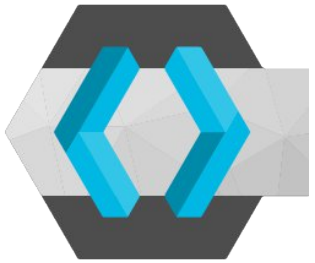
- Surcouche de OAuth permettant aux fournisseurs de service d'identifier les utilisateurs
- Spécifie une interface REST (intéopérabilité)
- Se base sur l'authentification fournie par un service d'autorisation
- Suit le processus d'obtention d'information de OAuth

SAML v2

- Standard définissant un protocole d'échange de données (XML) liées à la sécurité
  - ➢Authentification (unique !)
  - ➢Délégation



Keycloak



- Logiciel de SSO utilisant la fédération d'identité
- Utilisation de « domaines d'authentification (*realms*)
- Notion de clients
- Domaine d'accès des informations pour les clients

Dans la vie

- CAS MiNET

- FranceConnect