SYD

Secure Your Data

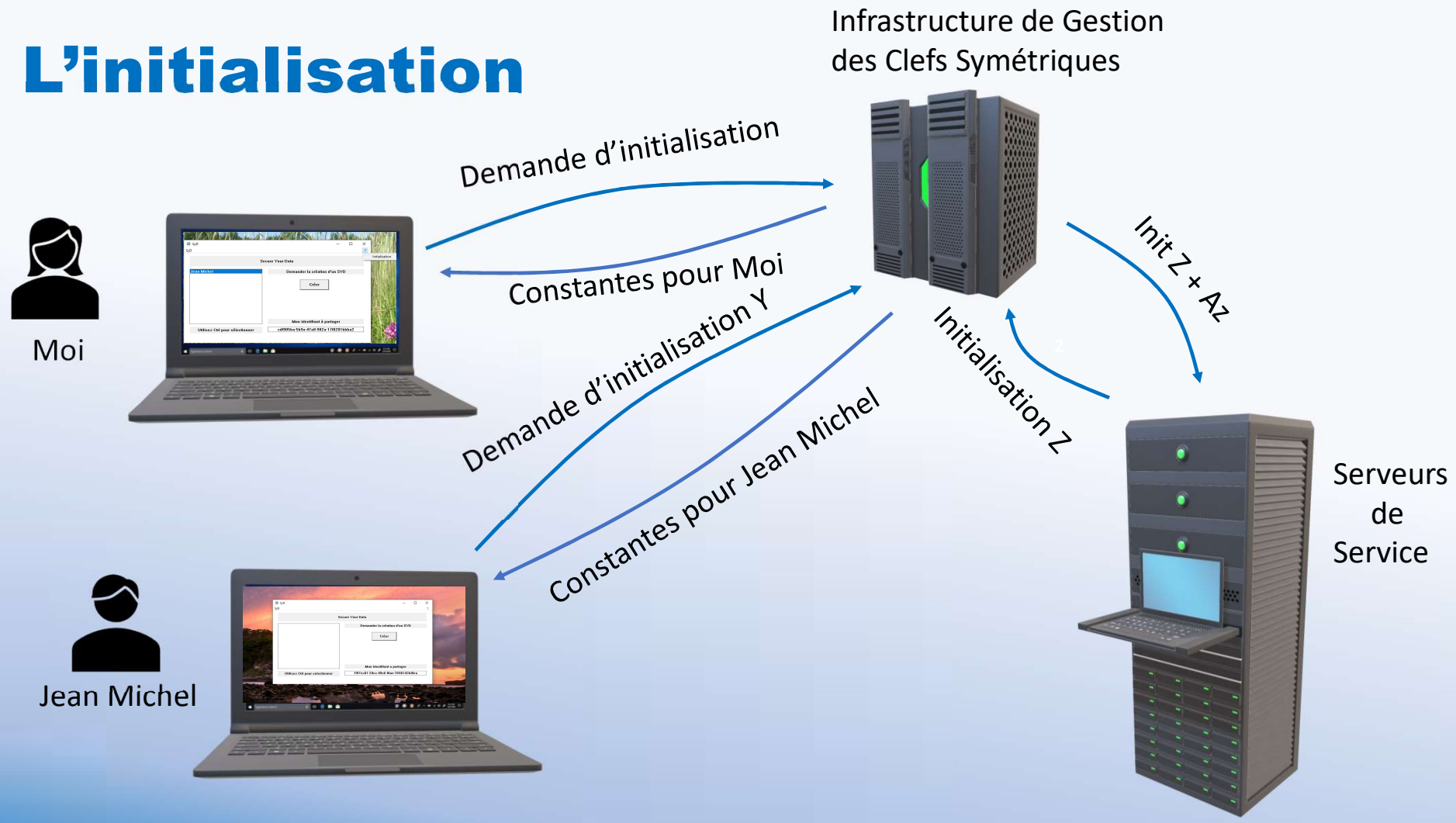
Une infrastructure de partage de clefs symétriques entre des clients.

SIREN : 939508198

Les objectifs de l'infrastructure SYD

- Le système propose une solution de partage de clefs (symétriques) sans pour autant partager les secrets;
- Les clefs symétriques sont générées a chaque usage par l'émetteur des données à destination du client des données.
- Fait disparaitre les négociations de clefs des communicants lors de la communication ;
- Moins gourmand en puissance que les méthodes asymétriques ;
- Usage symétrique est plus résistant face au quantique.

L'initialisation

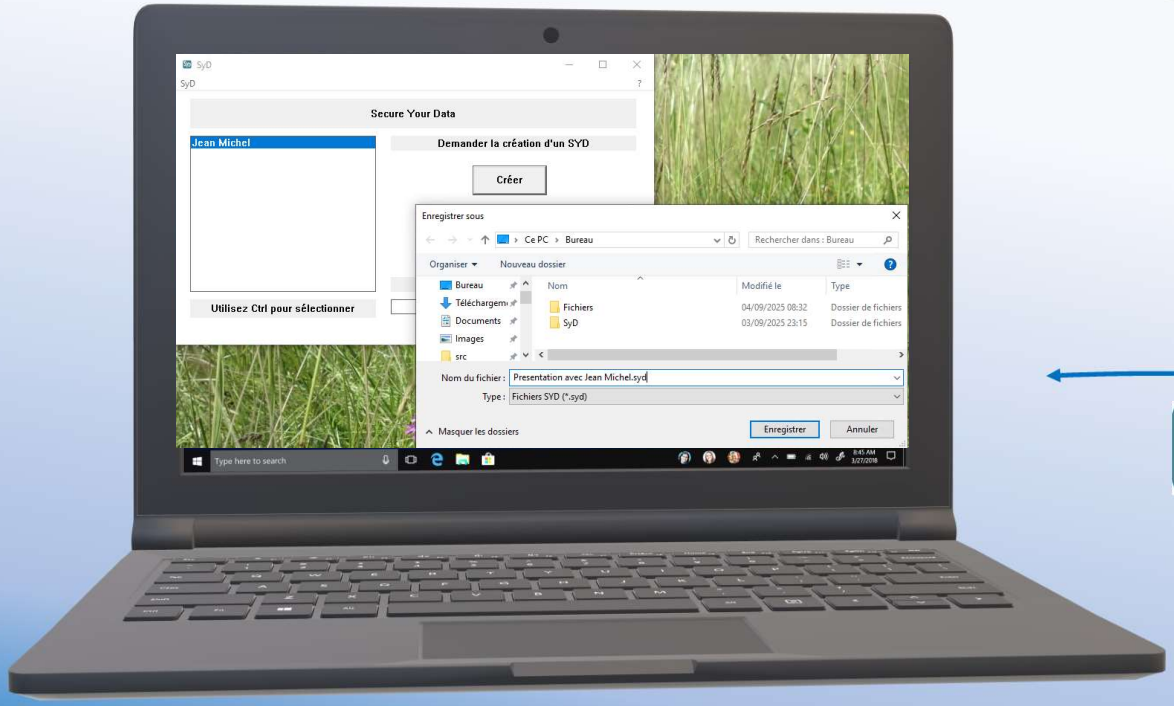


Souscription au service SyD

La demande de SyD

Infrastructure de Gestion
des Clefs Symétriques

Demande de conteneur SYD pour Jean Michel et Moi

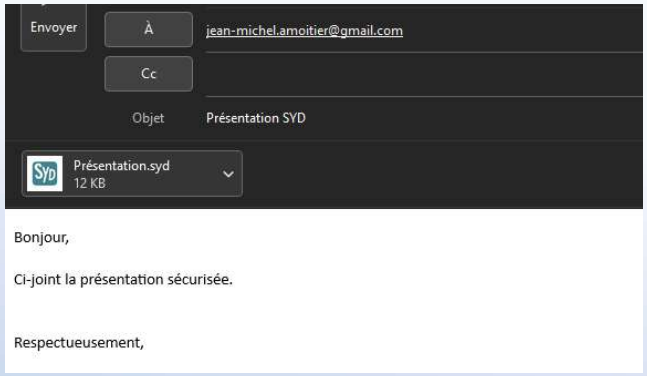


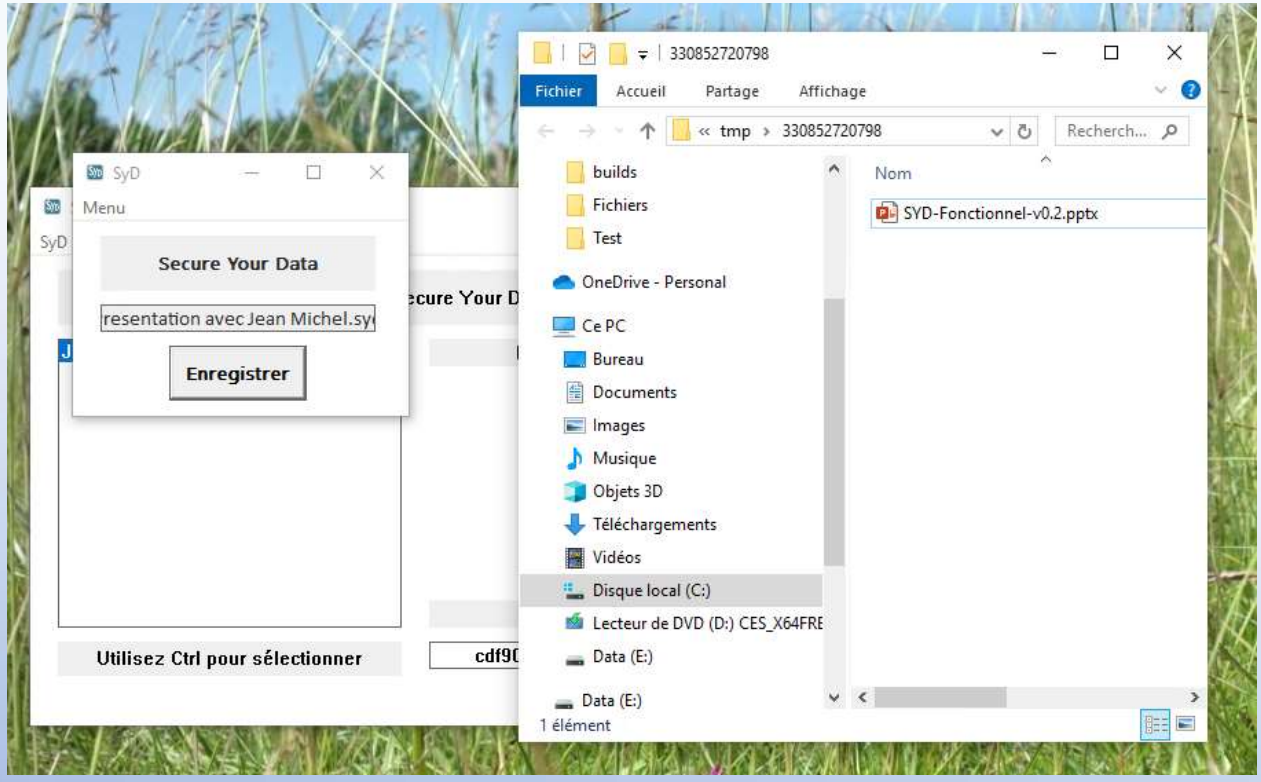
Serveurs
de
Service Z

Valide le service souscrit
Vérifie auprès de l'IGCS
et réceptionne de
constantes de pour Jean
Michel et Moi
Génère le SYD adapté

L’usage du SyD

Le conteneur accepte un document de 50 Mo et facilement partagé avec Jean Michel par Mail.





Solution technique

Le système SYD permet de calculer des clefs d'échanges de 256 à 19880 bits.

Sur les serveurs, l'entropie des aléas est basée sur plusieurs facteurs.

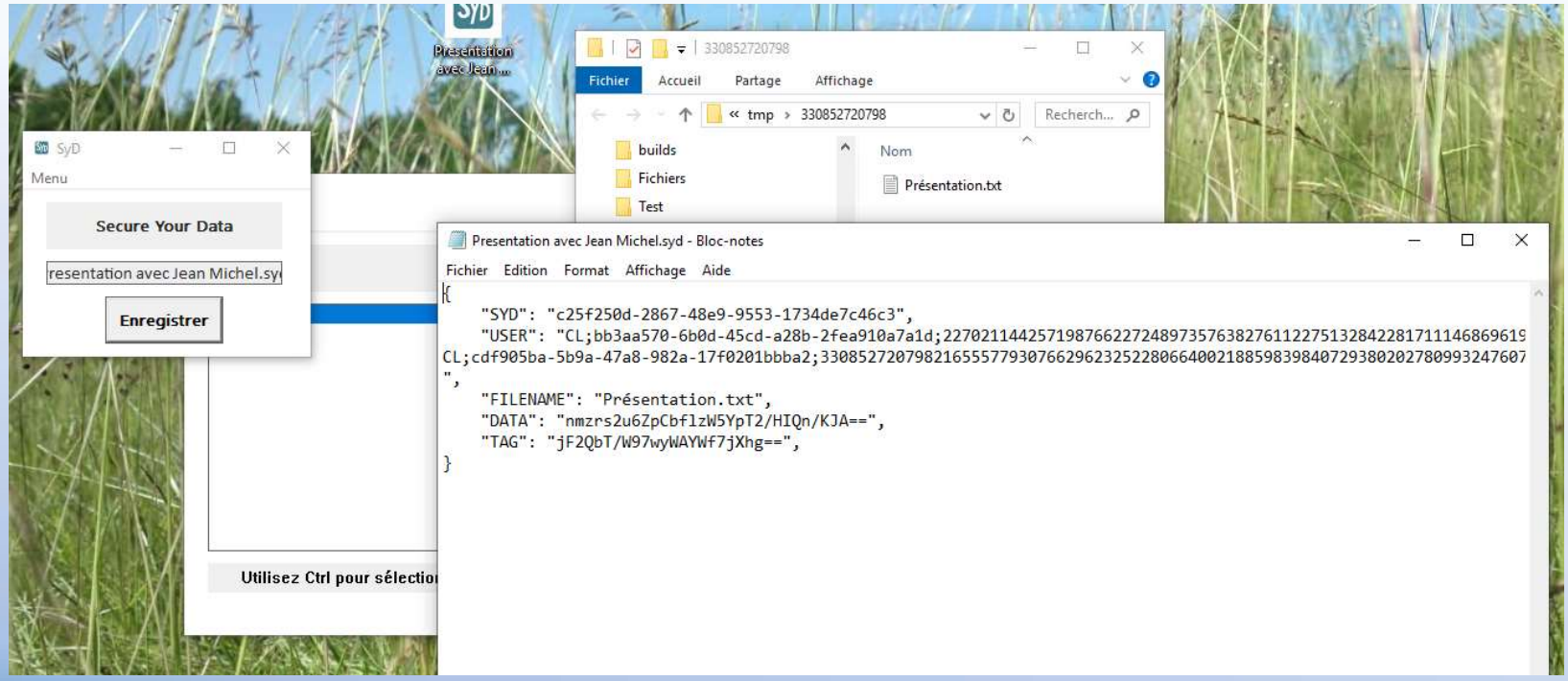
Les clefs d'échanges générées sont dérivées en clefs de 256 bits pour chiffrer en AES-256-GCM

- Codé intégralement en C.
- Exposé au travers d'une API REST structurée en JSON.

Il est prévu pour fonctionner sur un système Linux avec une emprunte mémoire limitée

Solution technique

Exemple de contenu d’un document syd



Contact

Sylvain Patureau Mirand

+336 34 30 33 86

sylvain_pm@hotmail.com

Adresse :

SyPaMir

60 rue FRANCOIS 1ER

75008 PARIS