PARSEC

FRANCE 2030

PROGRAMME DE RECHERCHE

CYBERSÉCURITÉ

Parsec : partage Data Zero Trust en asynchrone

OSSIR Paris :
Thierry Leblond, CEO & Co-fondateur
SCILLE / PARSEC

Mardi 10 septembre 2025

VISA DE SÉCURITÉ

PARSEC

FRANCE 2030

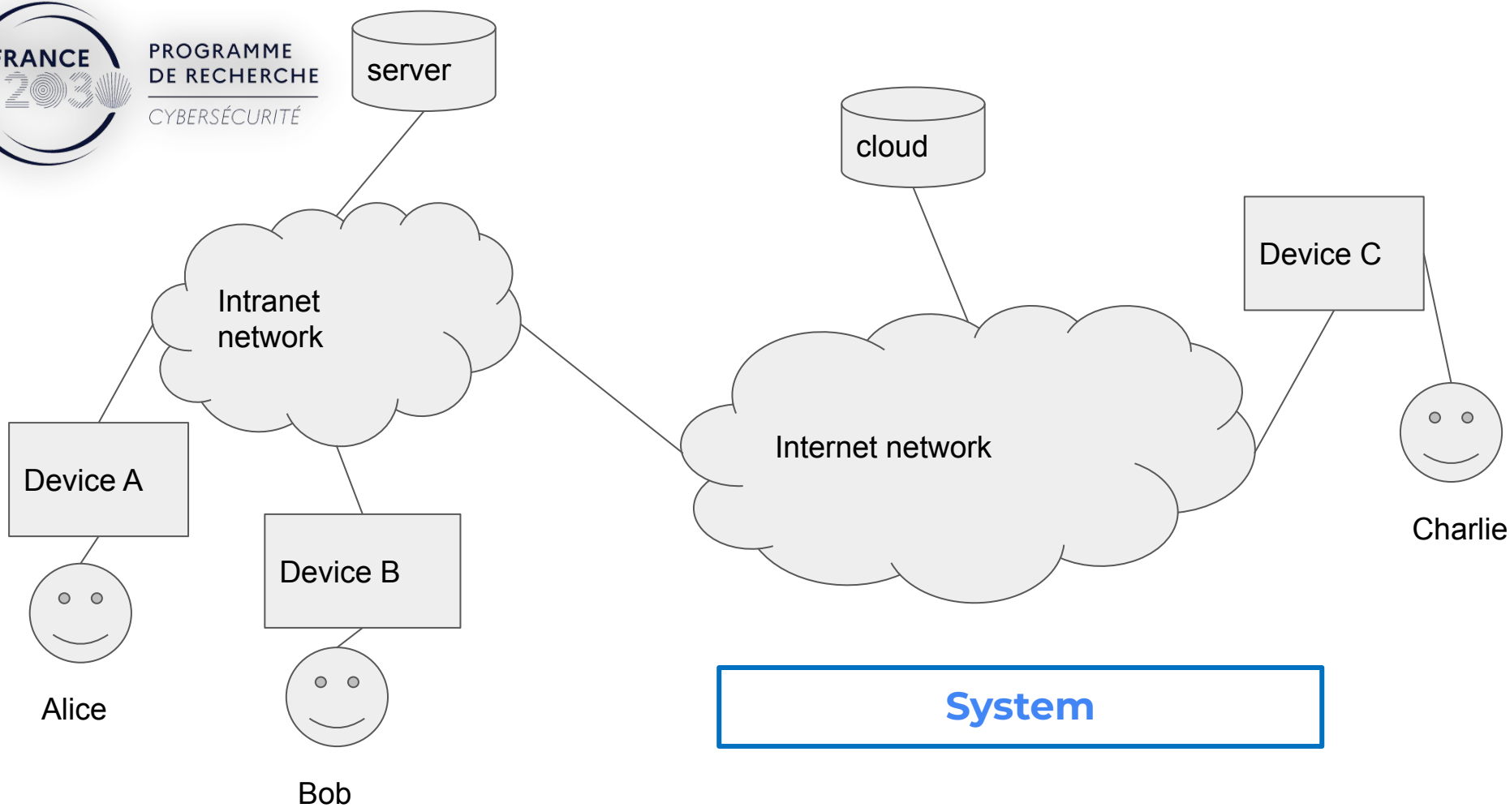
PROGRAMME DE RECHERCHE

CYBERSÉCURITÉ

25 janvier 2025

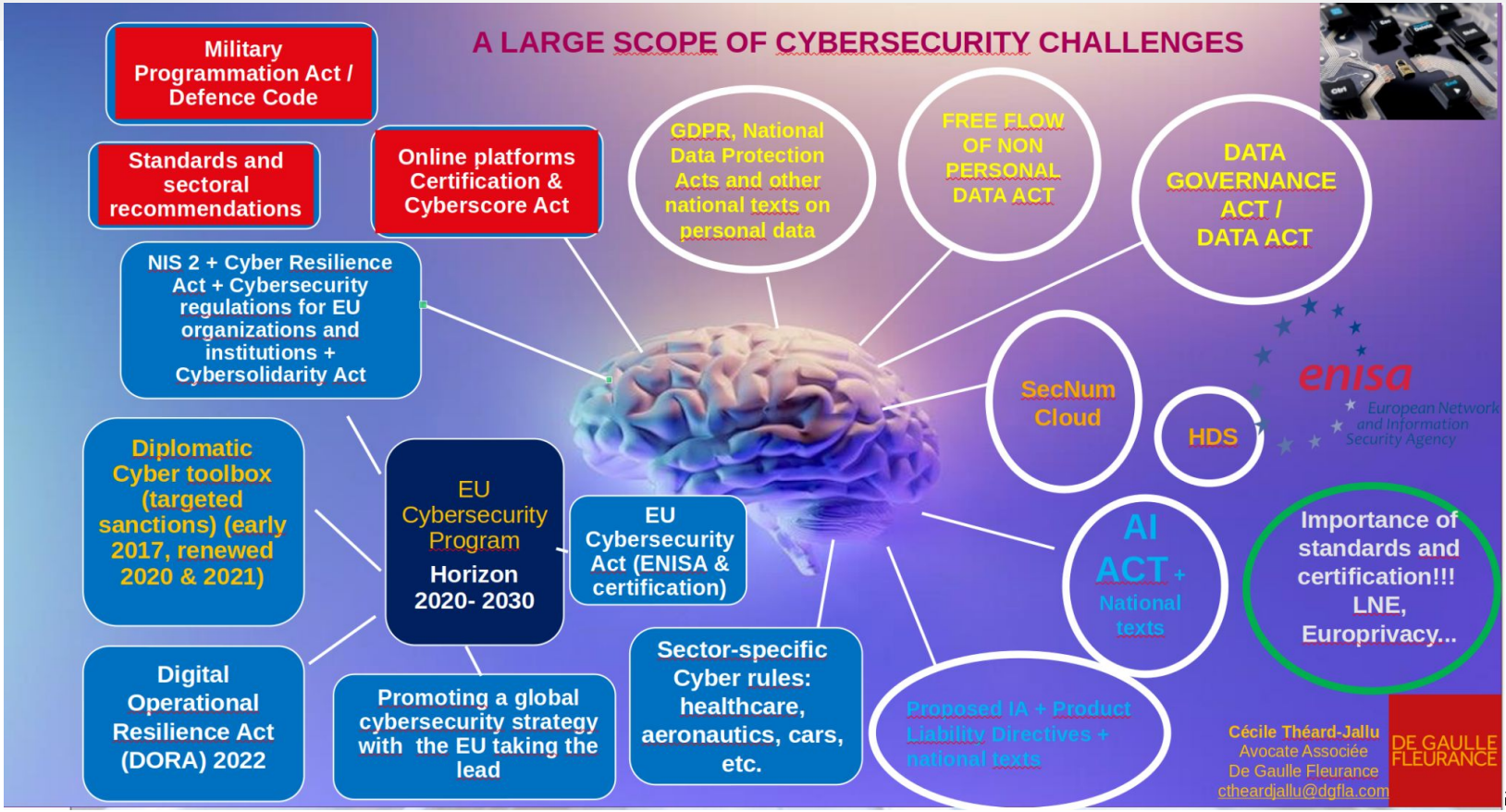
CONTEXTE

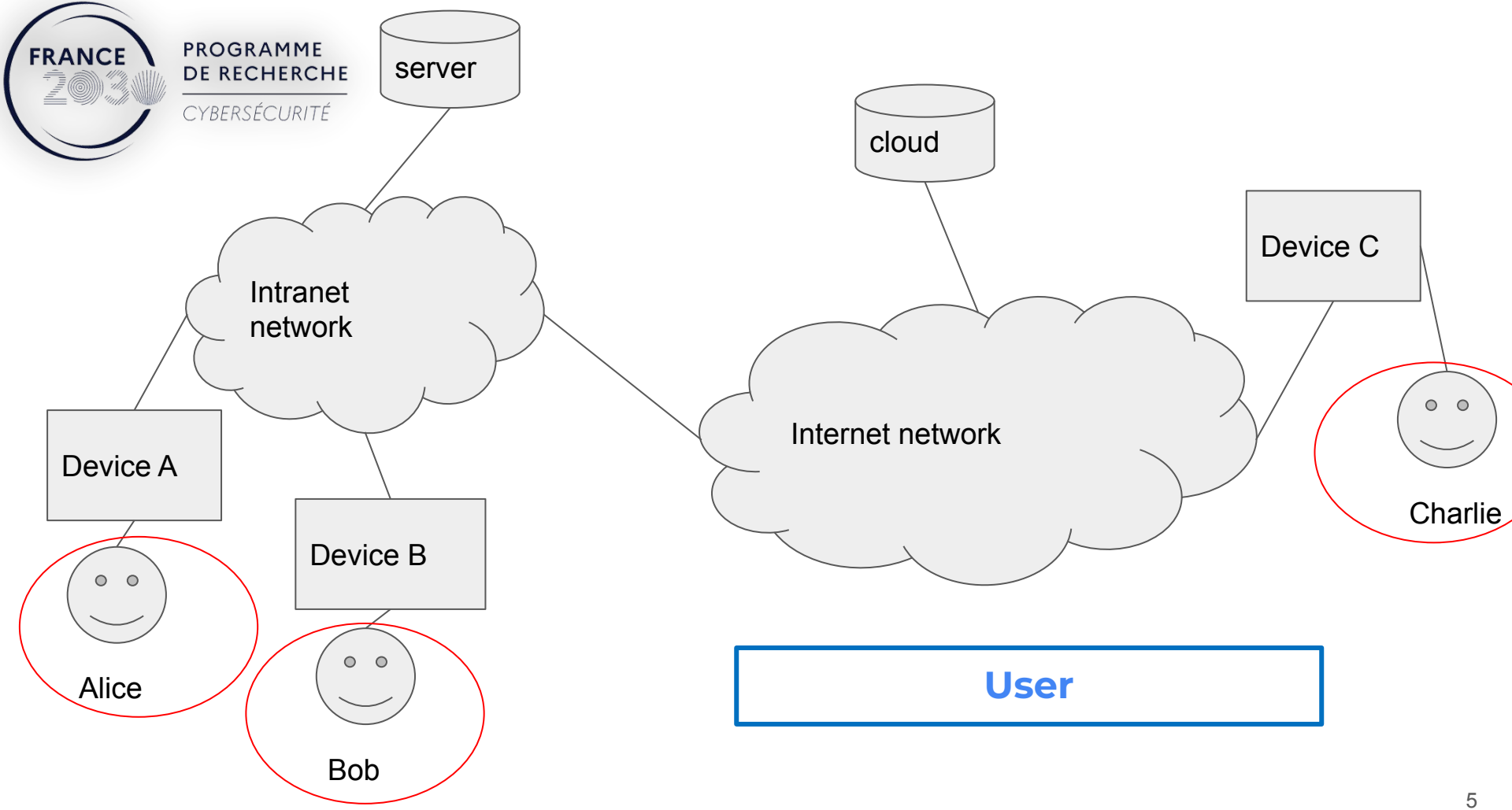
VISA DE SÉCURITÉ

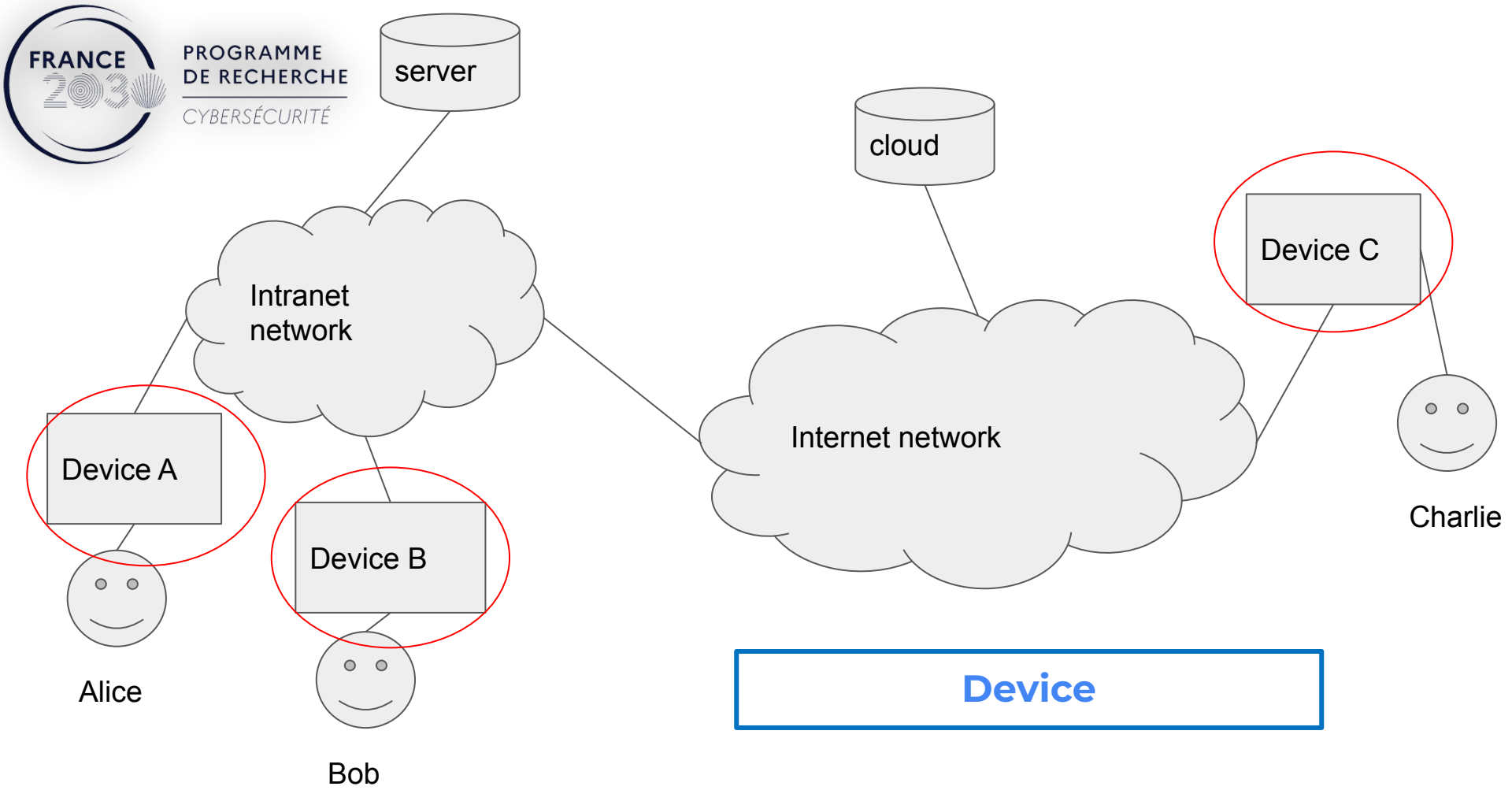

server
cloud
Intranet network
Device C
Internet network
Device A
Device B
Charlie
Alice
Bob
System

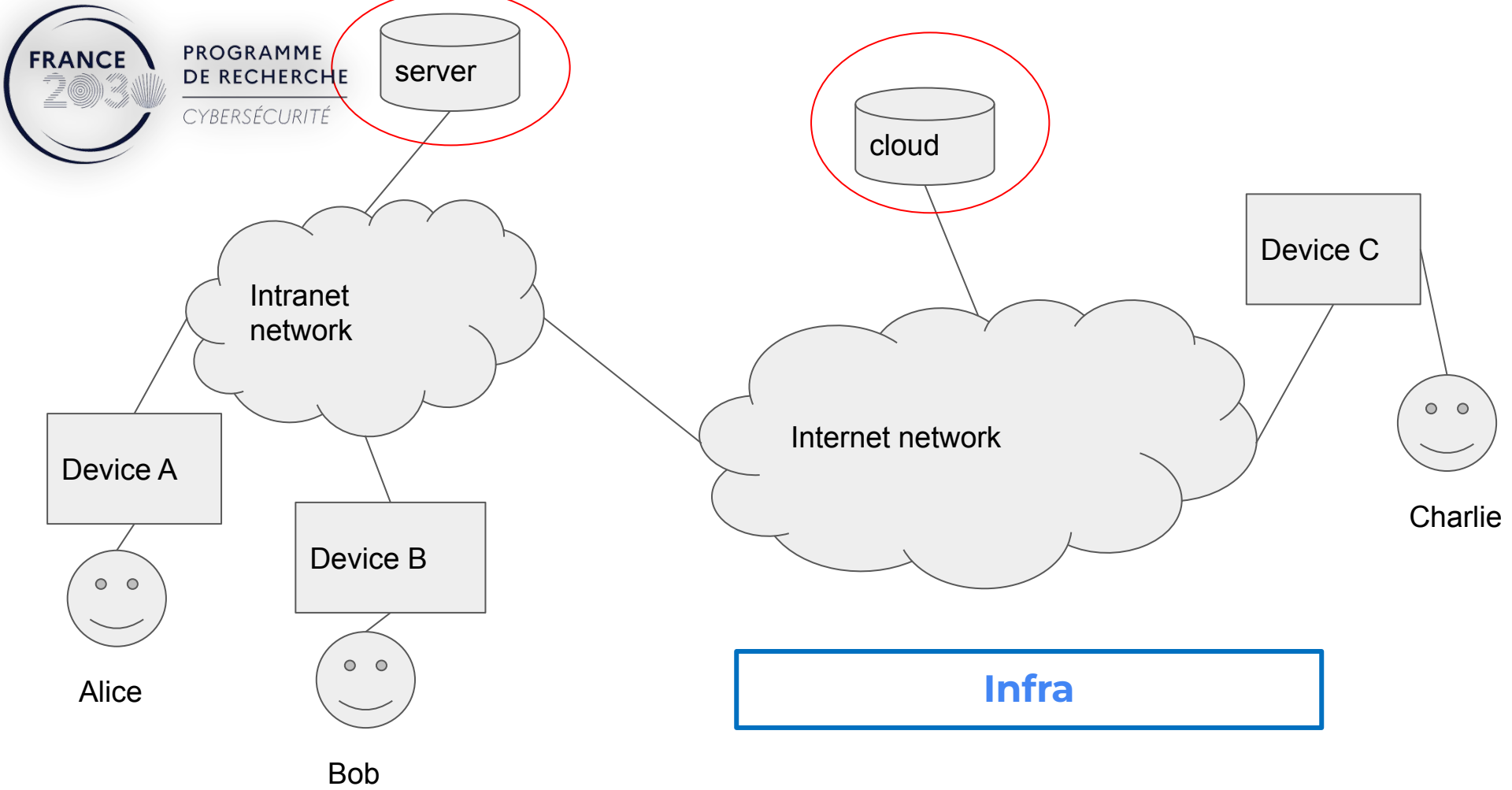
Panorama réglementaire

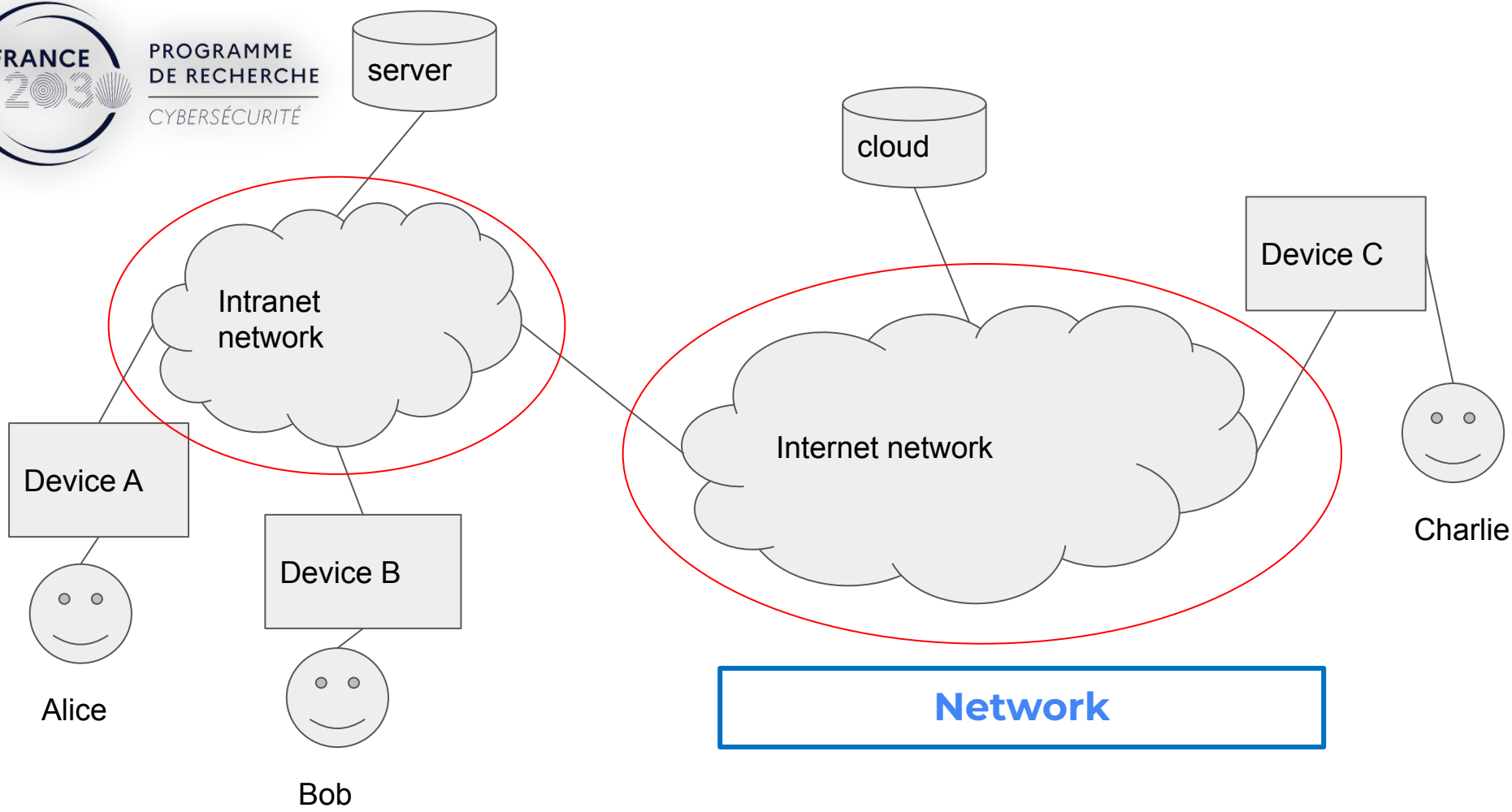
Cécile Théard-Jallu - Avocat à la Cour / Associée - +33 6 07 26 93 43 - ctheardjallu@dgfla.com

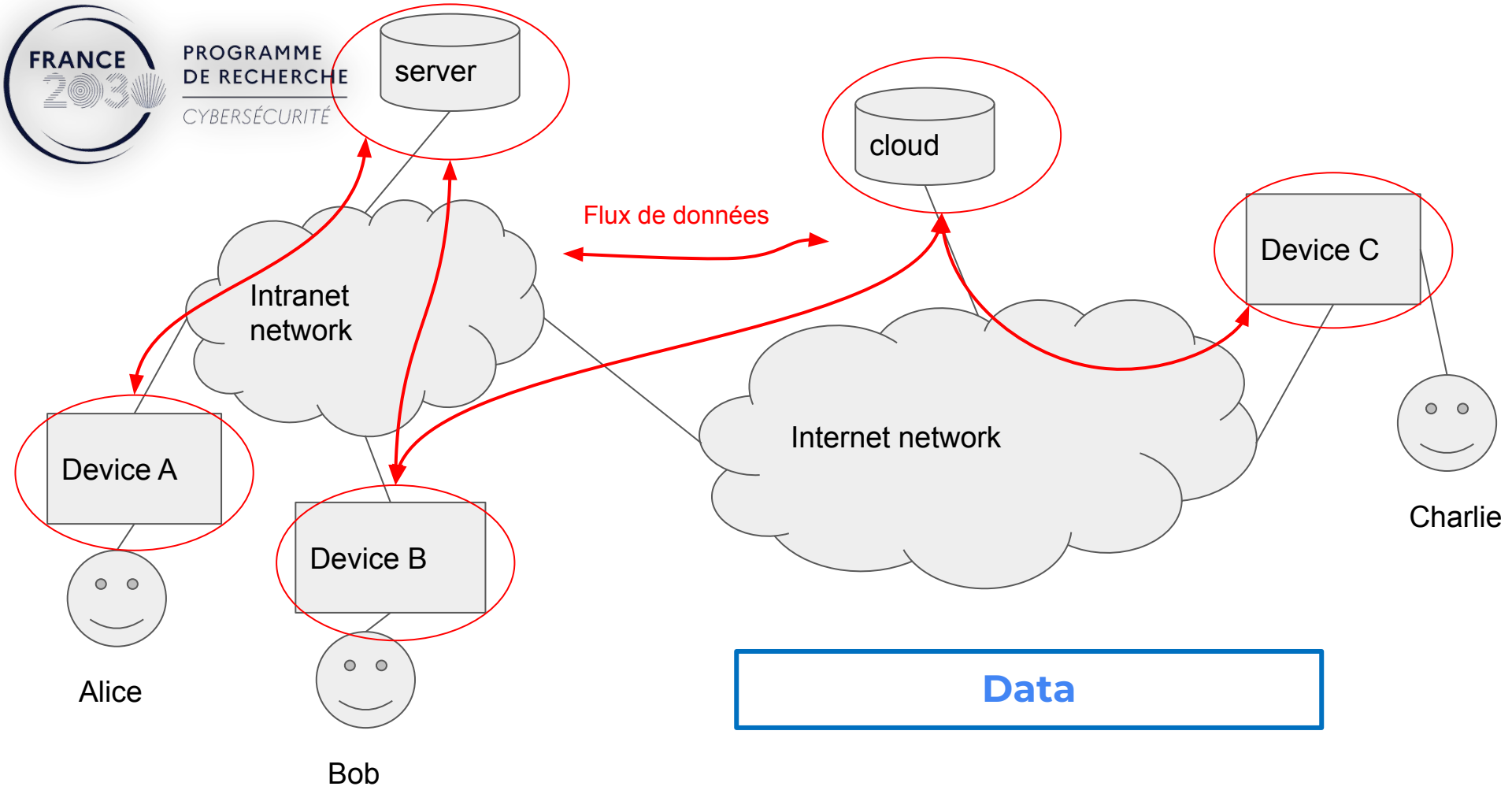



server
cloud
Intranet network
Device C
Internet network
Device A
Device B
Charlie
Alice
Bob
User

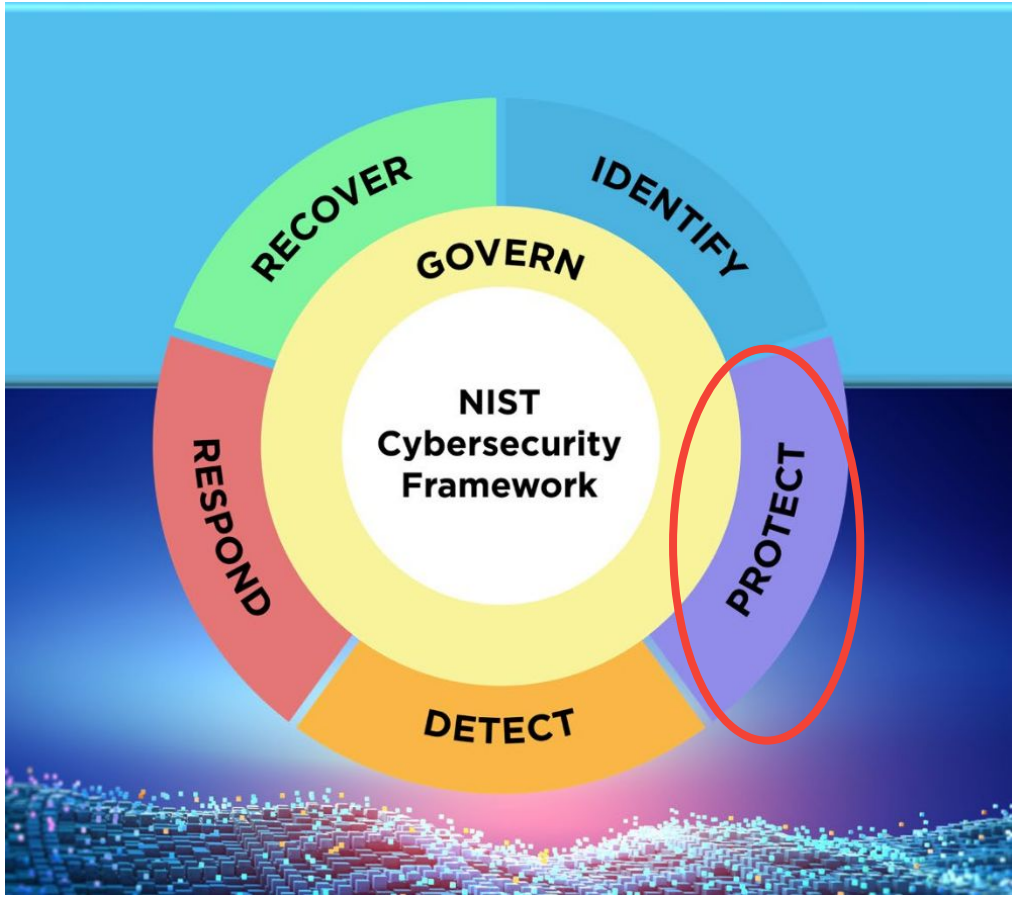

server
cloud
Intranet network
Internet network
Device A
Device B
Device C
Alice
Bob
Charlie
Device


server
cloud
Intranet network
Internet network
Device A
Device B
Device C
Alice
Bob
Charlie
Infra


server
cloud
Intranet network
Internet network
Device C
Device A
Device B
Alice
Bob
Charlie
Network


server
cloud
Flux de données
Intranet network
Device C
Internet network
Device A
Device B
Charlie
Alice
Bob
Data

The NIST Cybersecurity Framwork (CSF) 2.0



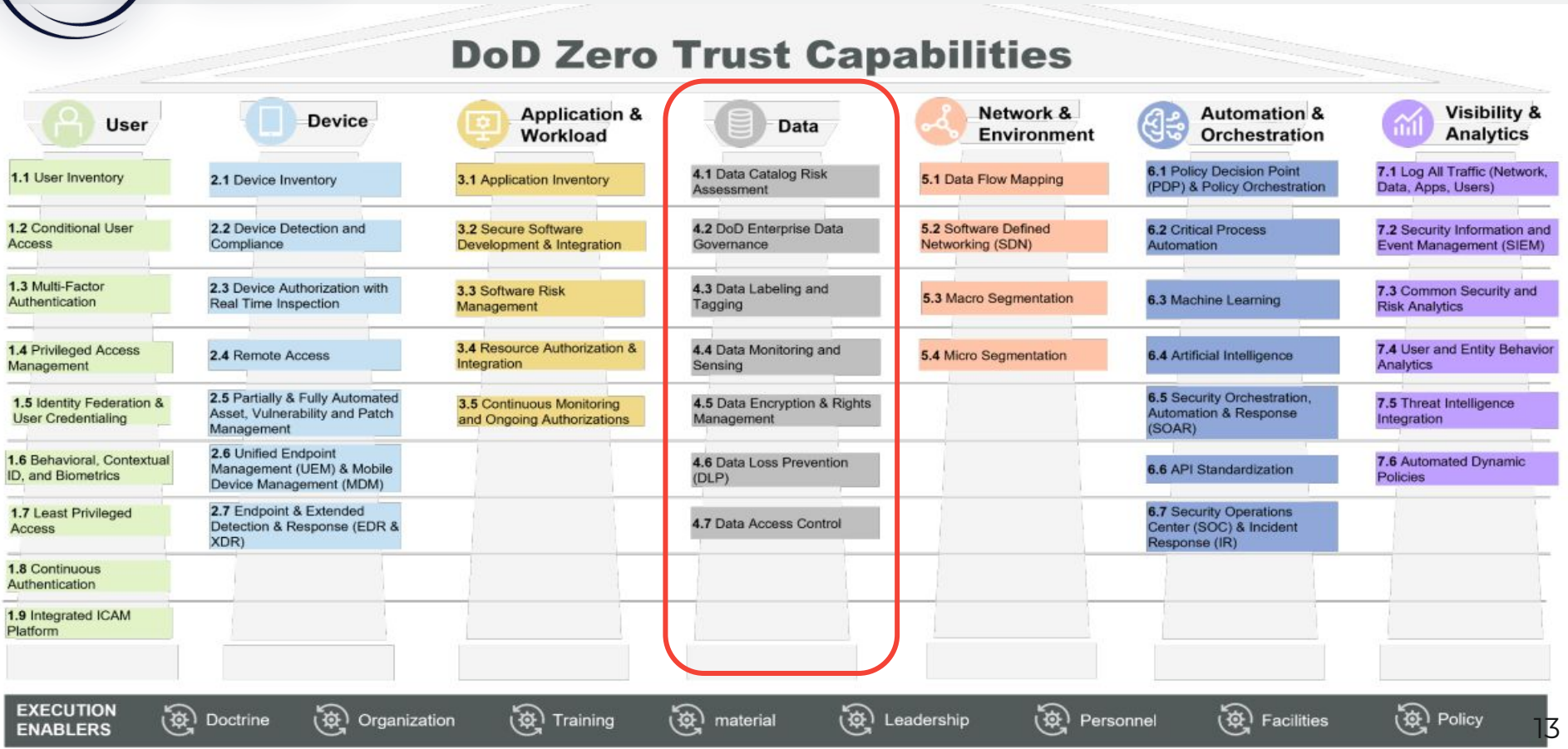
Data Zero Trust & Data Centric Security : Qu'est-ce que c'est ?

- La sécurité n'est plus une option :
  - La sécurité périmétrique est obsolète (l'ennemi est à l'intérieur)
  - Directive NIS2
  - Étancher les données sensibles vis à vis des IA
  - Zero Trust DoD strategy / US NIST standards
  - Nato ZTA & DCS standardisation
- Spécifications :
  - La sécurité doit être traitée au plus près de l'utilisateur
  - CIA+ : confidentialité, intégrité, résilience, non-repudiation, authenticité, anonymisation, traçabilité, historisation, révocation
- 3 concepts :
  - Zéro Trust ⇒ vérification systématique
  - Zero Knowledge ⇒ crypto implémentation du "droit-à-en-connaître".
  - Data Centric Security ⇒ crypto-control des données & des métadonnées

Zero Trust tenets

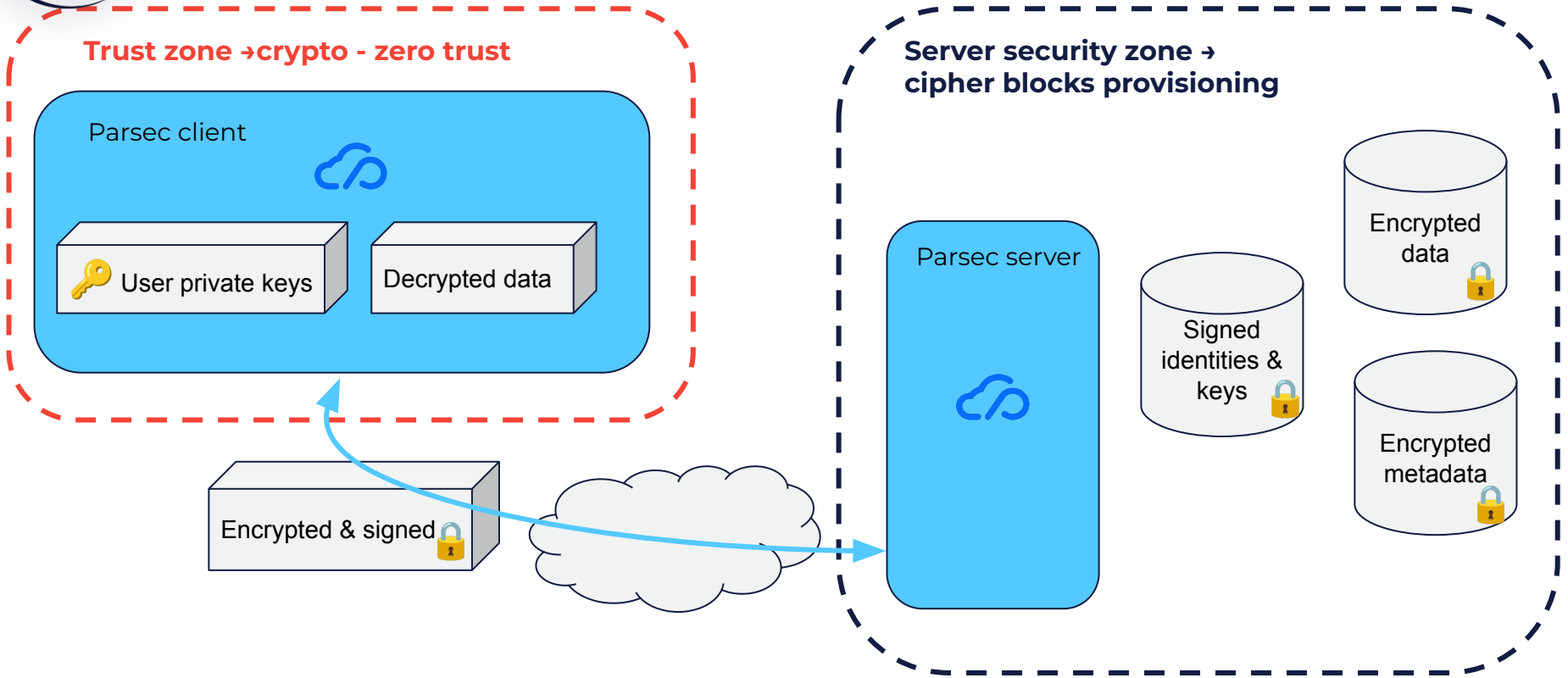
- 5 major ZT tenets.
  - Assume a Hostile Environment.
  - Presume Breach.
  - Never Trust, Always Verify.
  - Scrutinize Explicitly.
  - Apply Unified Analytics.
- NATO Zero Trust policy
  - Assume Breach.
  - Never Trust, Always Verify.
  - Verify Explicitly and Continuously.
  - Apply The Least Privilege.
  - Probabilistic and Explainable Security Decisions.
  - Transparency.

US DoD standard Zero Trust



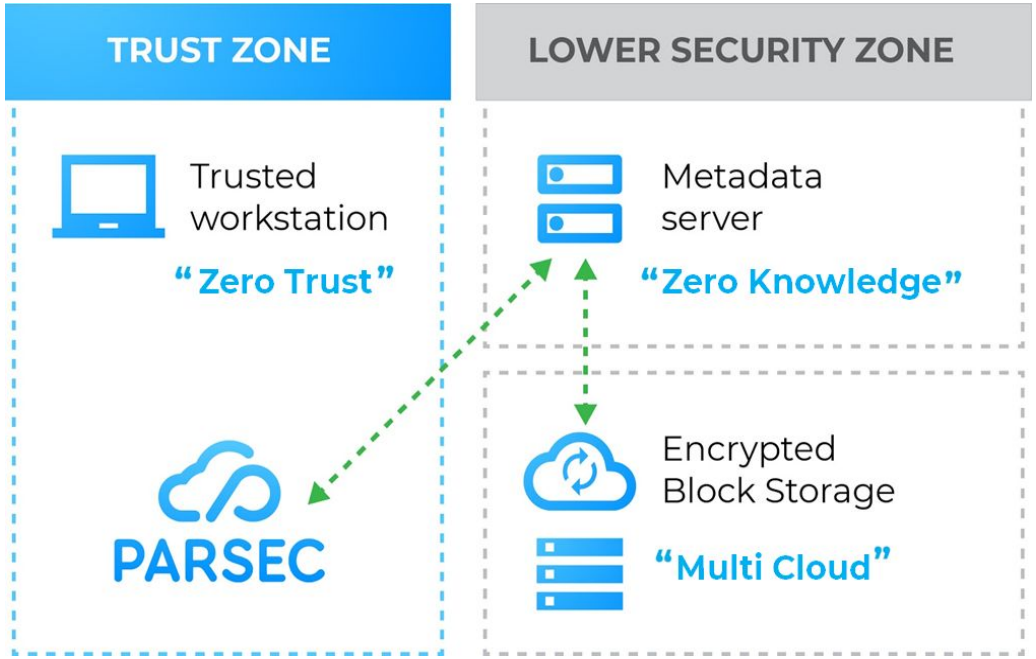

PARSEC
FRANCE 2030
PROGRAMME DE RECHERCHE
CYBERSÉCURITÉ
25 janvier 2025
PRINCIPES TECHNIQUES
VISA DE SÉCURITÉ

Parsec: Systematic user-centric encryption

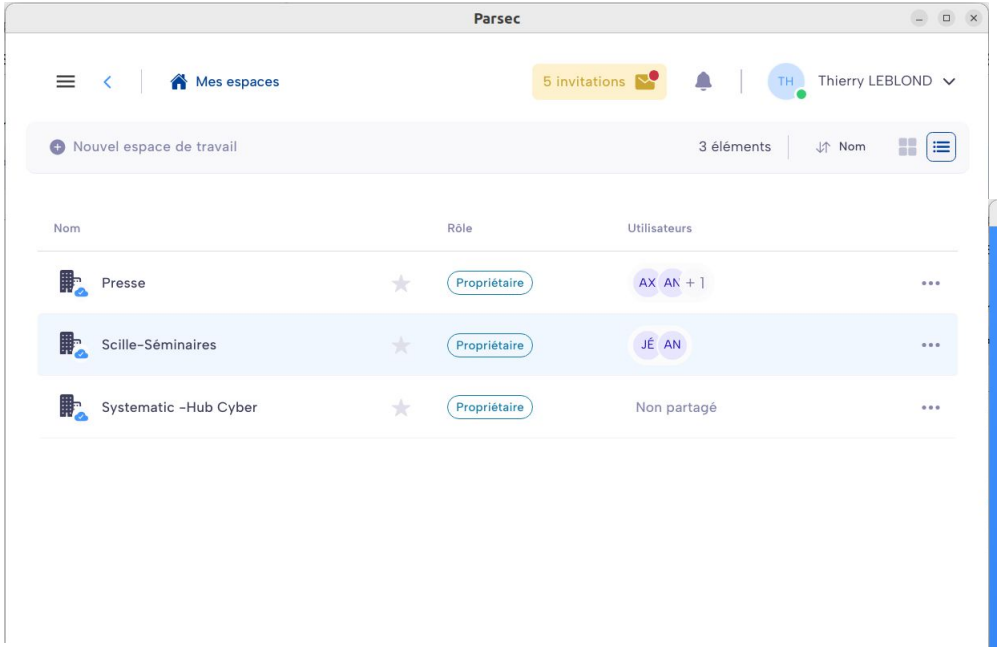


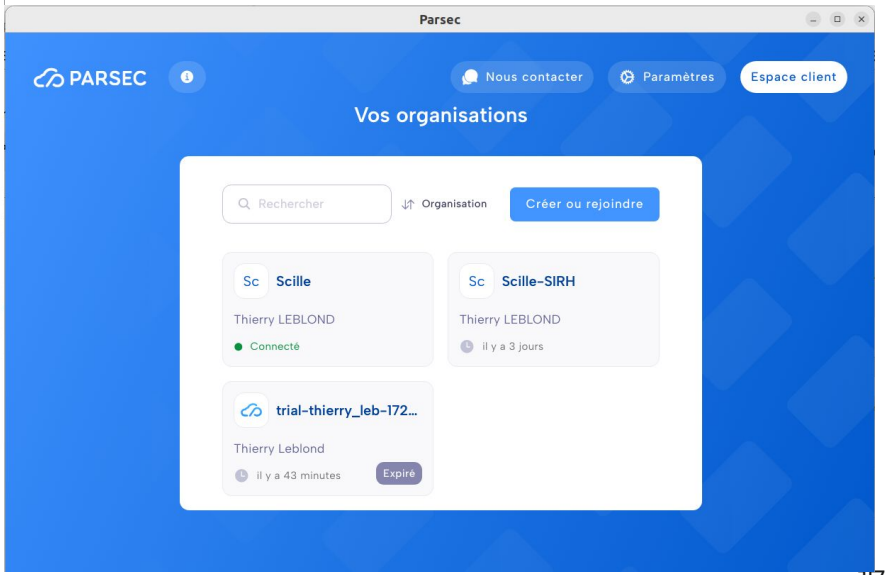
PARSEC : technologie “Zero Trust”

- Contrôle exclusif des données par des clés locales et personnelles
- Rust multi-devices (mobile, web & desktop)
- Asynchrone
- Organisations et Utilisateurs souverains

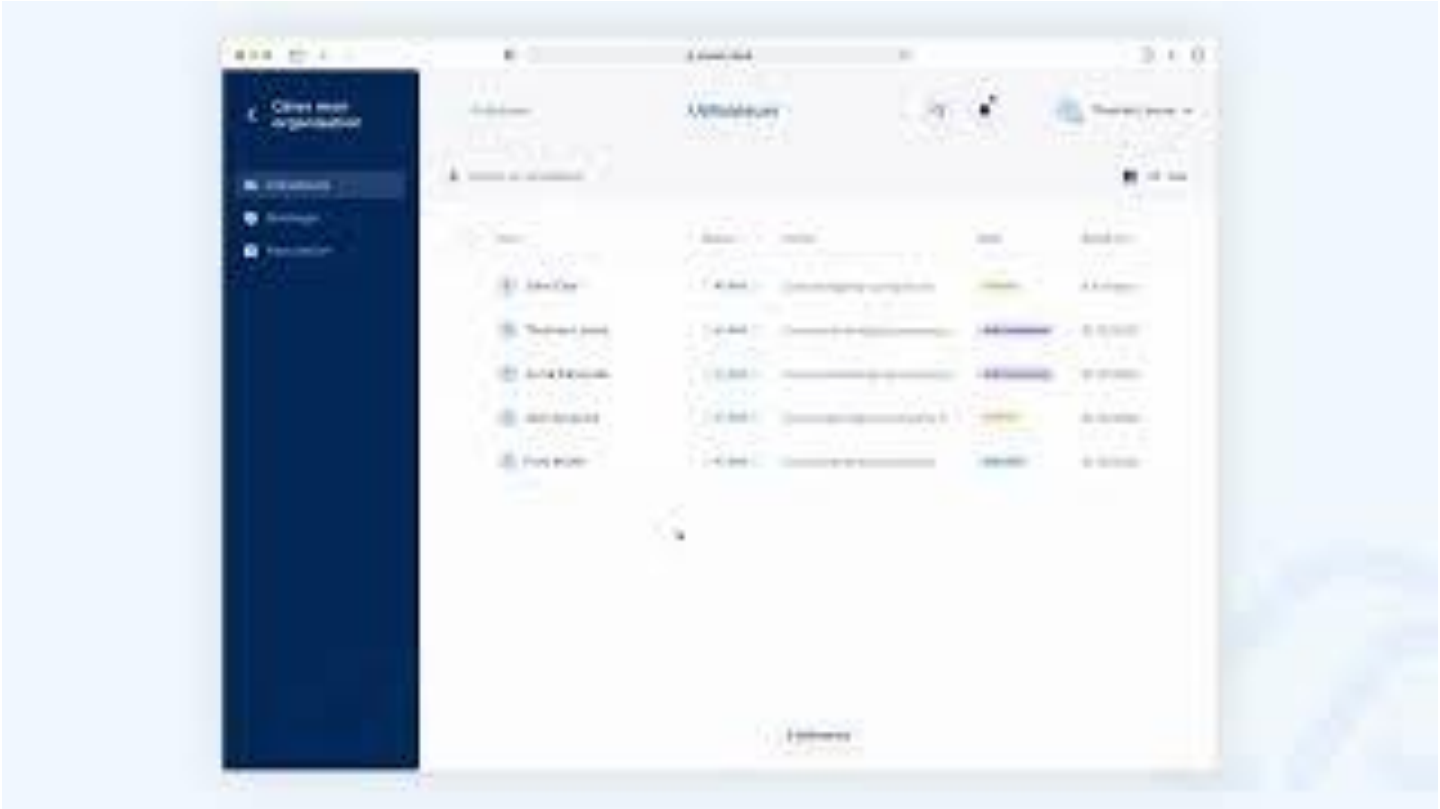


PARSEC: Interface utilisateur





PARSEC: Interface utilisateur



Concepts spécifiques à Parsec

Organisation

- Un ensemble d'utilisateurs souhaitant travailler ensemble
- Les organisations sont hermétiques entre elles
- Elles peuvent être hébergées sur le même serveur Parsec

Compte d'utilisateur

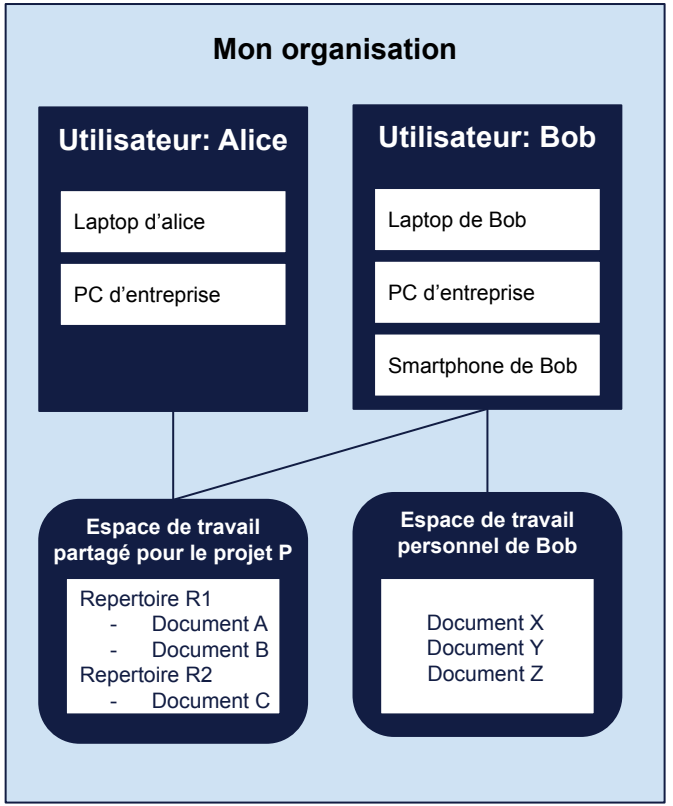
- Représente un utilisateur humain au sein d'une organisation
- Un utilisateur possède un profil administrateur, standard ou externe
- Un utilisateur accède à l'organisation via un ou plusieurs appareils

Appareil

- Correspond à un compte d'utilisateur sur un terminal donné
- En résumé, 1 appareil = 1 utilisateur au sein d'1 organisation sur 1 terminal

Espace de travail

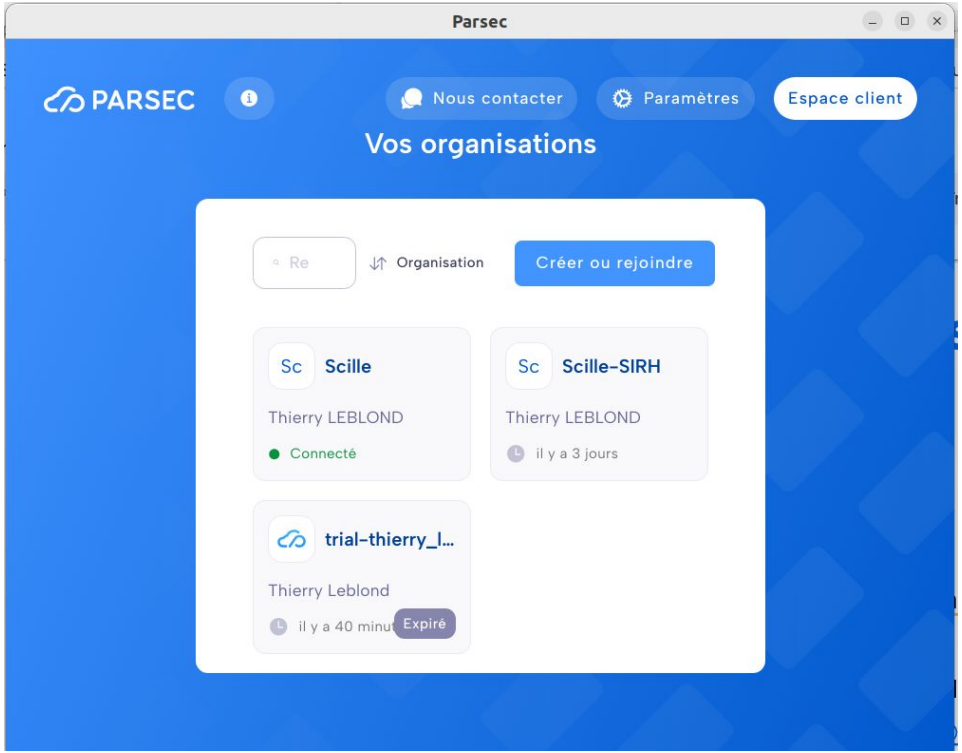
- Arborescence de documents partagés entre des comptes d'utilisateur
- Les droits en lecture, écriture et gestion sont configurables



Concepts spécifiques à Parsec

Exemple:

- Un même utilisateur humain :
  - **Thierry LEBLOND**
- Agissant sous deux identités différentes
  - thierry.leblond@scille.fr
  - thierry.leblond@m4x.org
- Sur le même terminal :
  - **Laptop**
- Dans plusieurs organisations différentes :
  - **Scille**
  - **Scille-SIRH**



Résultat: deux “appareils” différents sur ce terminal

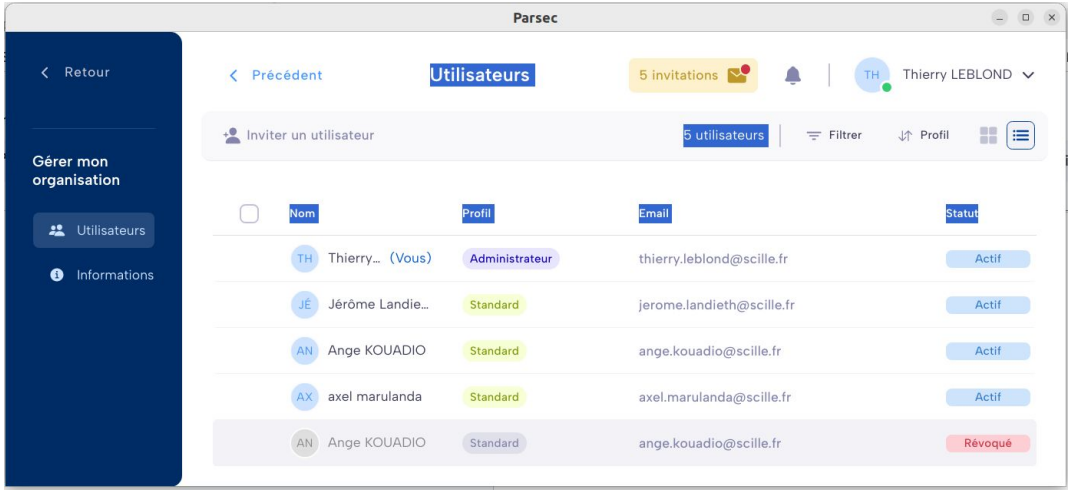
Les différents profils utilisateurs

Administrateur

- Peut inviter de nouveaux utilisateurs
- Peut revoquer des utilisateurs existants
- Peut créer et gérer des espaces de travail

Utilisateur standard

- Peut créer et gérer des espaces de travail
- A accès à la liste des utilisateurs de l'organisation



Utilisateur externe ou invité

- Peut accéder aux espaces de travail dans lesquels on l'a invité·e
- N'a **pas** pas accès à la liste des utilisateurs de l'organisation

Les rôles au sein d’un espace de travail

Quatre niveaux de privilège:

Roles	Non partagé	Lecteur	Contributeur	Gérant	Propriétaire
Accès en lecture	❌	✅	✅	✅	✅
Accès en écriture	❌	❌	✅	✅	✅
Modification des rôles “**Non Gérants”**	❌	❌	❌	✅	✅
Modification des rôles **”Gérants”**	❌	❌	❌	❌	✅

- Le créateur d’un espace de travail est son propriétaire
- Il peut ensuite déléguer la gestion à un gérant
- Le gérant peut à son tour inviter des contributeurs et des lecteurs

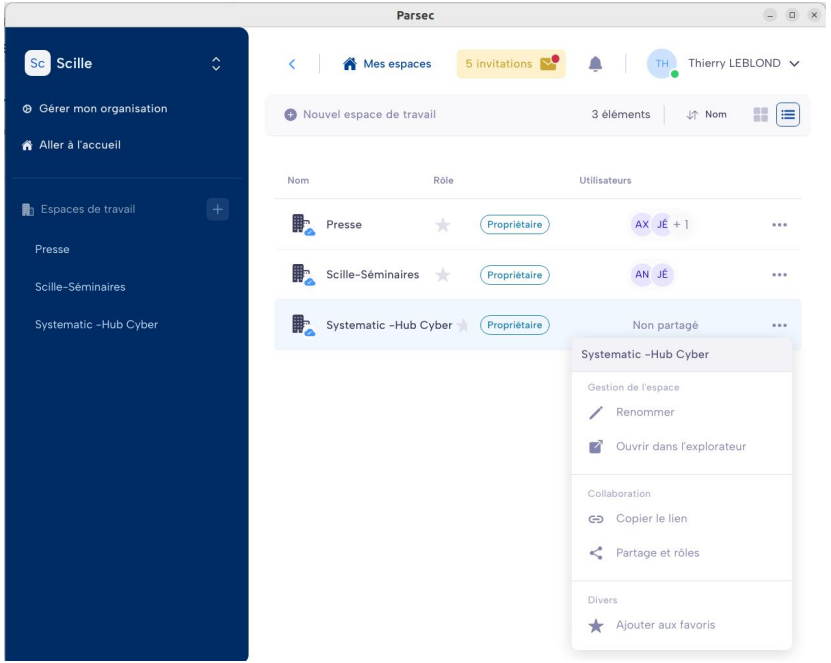
Le profil **administrateur** est indépendant de son rôle dans les espaces de travail de l’organisation.

S’il n’a pas été invité, il n’a aucun droit (pas même la lecture)

Les points de montage

L'utilisateur accède à ses espaces de travail comme à des **disques externes**

- Renforce l'idée d'enclaves séparées
- Chaque point de montage correspond à un système de fichier virtuel
- **Conséquence :** les fichiers ne sont jamais en clair sur le disque dur
- **Conséquence :** accès transparent pour les applications tierces



Enrôlement et révocation

L’enrôlement d’un **nouvel appareil** fonctionne de manière similaire à l'enrôlement d’un **nouvel utilisateur**

- Même utilisation des **codes SAS**, en local cette fois
- Possibilité de vérification automatique via **QR code** pour l'enrôlement d’un smartphone

Les utilisateurs peuvent également être **révoqués** de leur organisation.

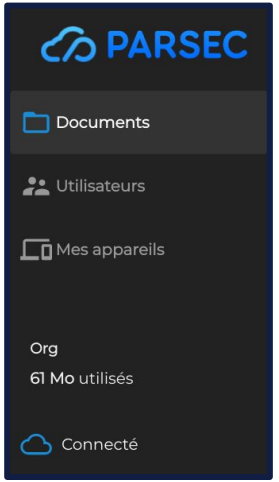
- **Tous les appareils** de l’utilisateur sont ainsi révoqués
- L’utilisateur perd les accès à **tous ses espaces de travail**
- La révocation d’un appareil seul n’est aujourd’hui **pas supporté**

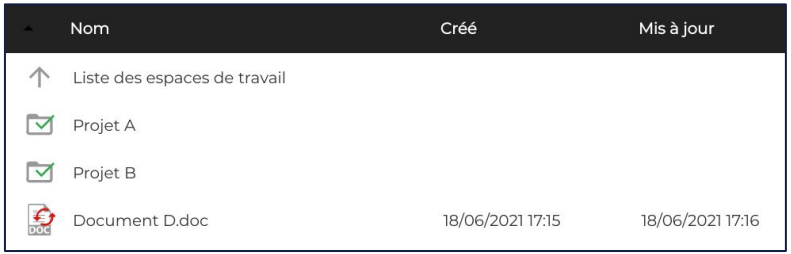
Le mode hors-ligne

Parsec est conçu pour fonctionner **hors connexion** ou sur une **connexion intermittente**

En particulier, il est toujours possible:

- d'**accéder aux répertoires** des espaces de travails
- de **créer** de nouveaux documents
- d'**éditer** des nouveaux documents
- d'**ouvrir** et de **modifier** des documents existants qui ont été lu récemment





La **synchronisation** des modifications aux espaces de travail se fait automatiquement lorsque l'appareil est **connecté**

- si les modifications sont **automatiquement propagés** aux autres appareils connectés
- les **conflits** lors de **modifications concurrentes** sont résolus automatiquement (du mieux possible)
- l'explorateur de l'application parsec indique le **statut de synchronisation** des fichiers

Présentation technique de PARSEC

Présentation fonctionnelle

- Terminologie
- Principe généraux
- Concepts spécifiques à Parsec
- Les différents profils utilisateurs
- Les roles au seins des espaces de travail
- Les points de montage
- L'enrôlement et la révocation
- Le re-chiffrement
- Le mode hors-ligne

Présentation technique

- **Le défi technique du “Zero Trust”**
- **Une application sous licence libre**
- **Architecture de Parsec**
- **Protocoles et technologies**

Le défi technique du “Zero Trust”

Les concepts fonctionnels présentées présentées précédemment ne sont **pas nouveaux**

Mais la contrainte **“Zero Trust”** fait de leur implémentation un challenge technique

Exemples de questions auxquelles répondre :

- Comment les utilisateurs **s'authentifient-ils** ?
- Comment administrer et gérer des droits **sans autorité centrale** ?
- Comment **limiter le pouvoir** du serveur d’orchestration ?
- Comment éviter qu’un **utilisateur malveillant** perturbe le système ?

Limitation de fait de certaines fonctionnalités :

- Un **enrôlement plus lourd** que les solutions web moderne
- Pas de **récupération de données** possibles en cas de perte de toutes les clés

Une application sous licence libre

L'application Parsec est sous licence mixte **BUSL + AGPLv3**

C'est une licence libre à l'avantage de **l'utilisateur**

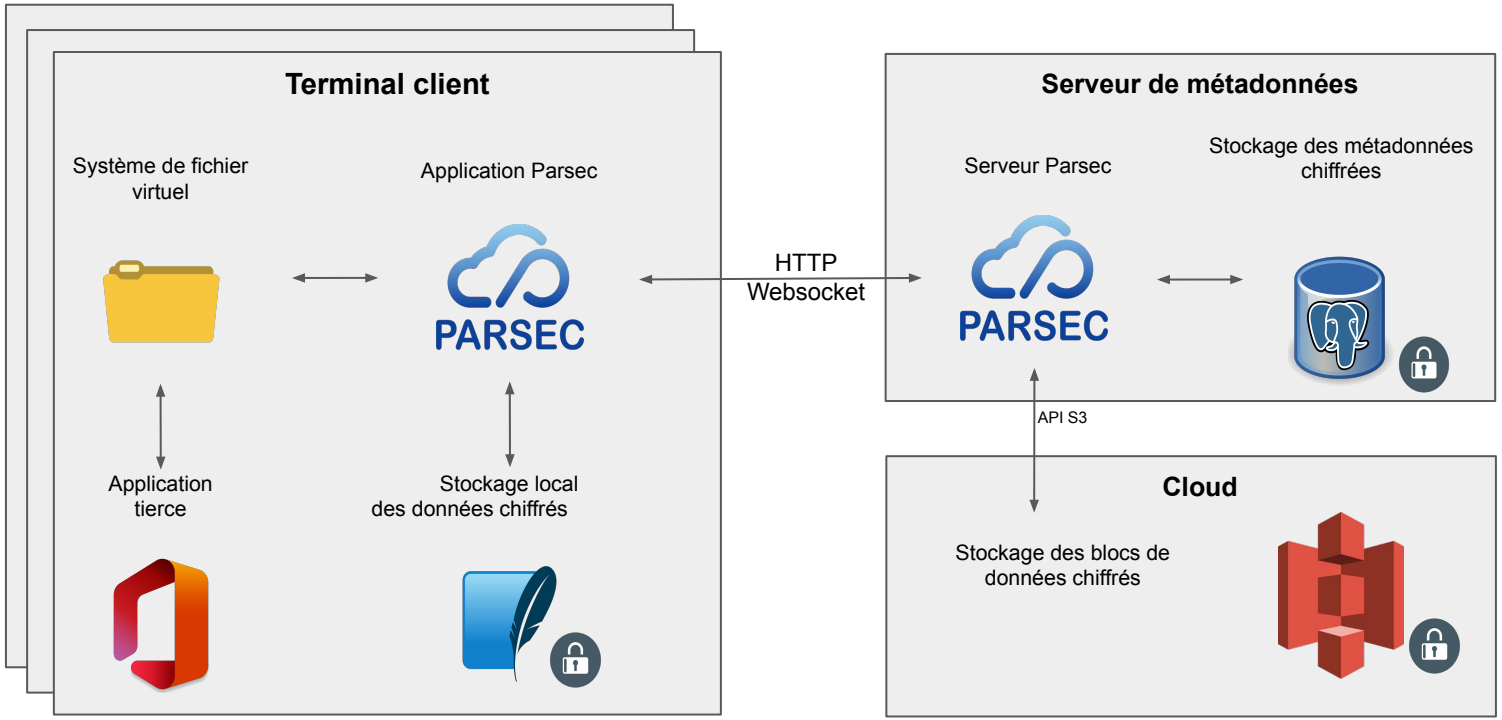
Elle lui garantit les **libertés** suivantes :

- Liberté d'**utilisation**
- Liberté de **modification**
- Liberté de **distribution**
- Liberté de **distribuer les modifications**

Cette licence est en cohérence avec le concept de **"Zero Trust"**:

- Si **seul le terminal** est digne de confiance, le logiciel installé sur le terminal se doit d'être également **digne de confiance**
- Un projet ouvert et collaboratif est plus à même de **détecter et régler** les potentielles failles **de sécurités**

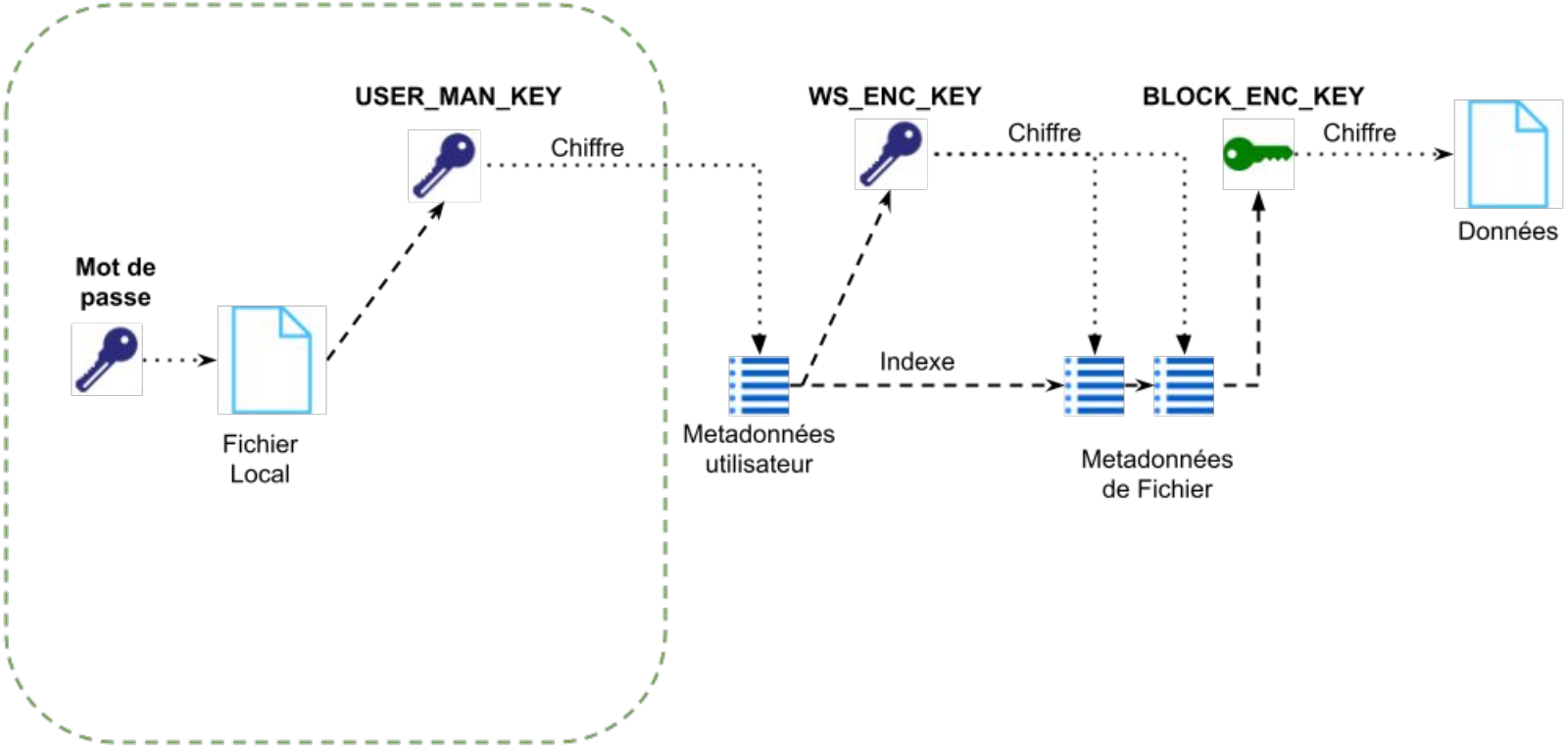
Architecture simplifiée



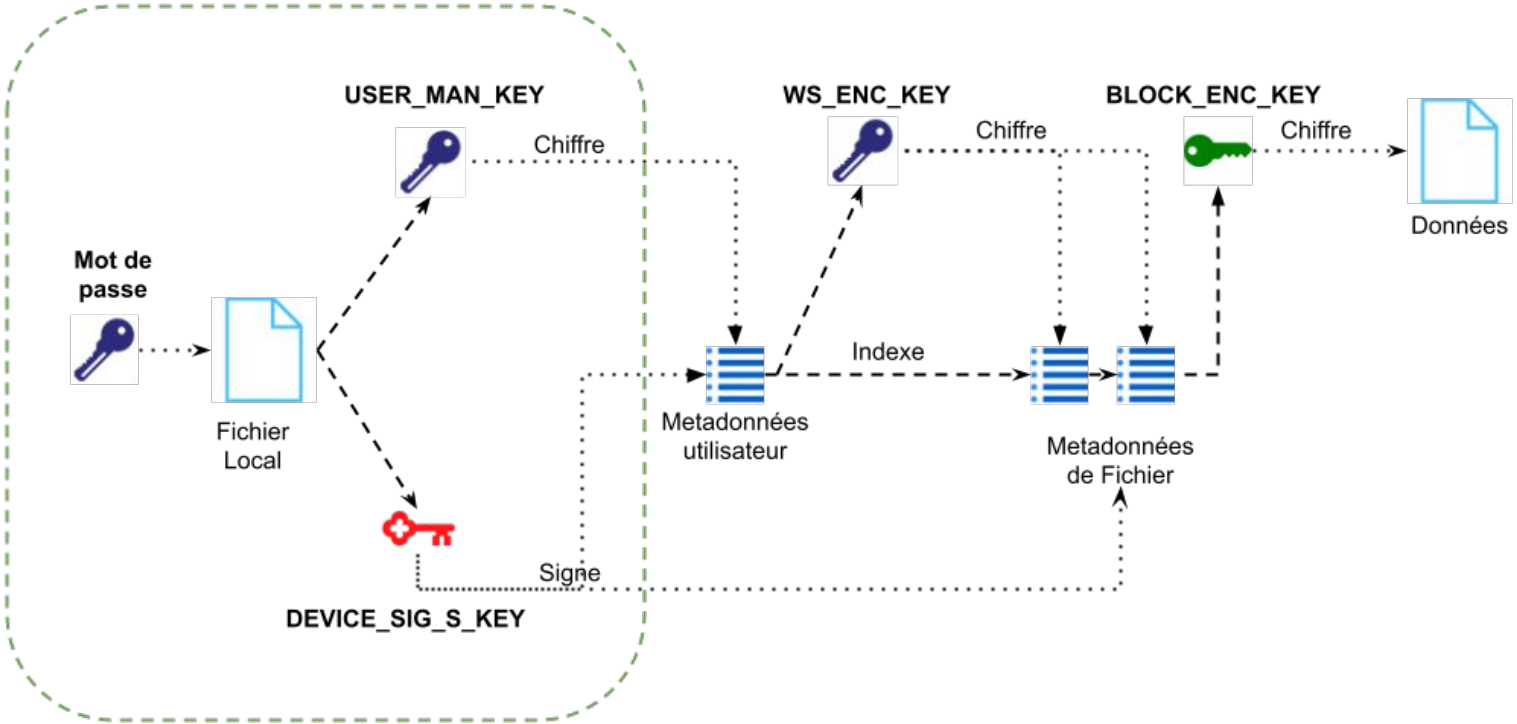
PARSEC: Certification ANSSI

https://www.ssi.gouv.fr/entreprise/certification_cspn/parsec-version-2-0-0/

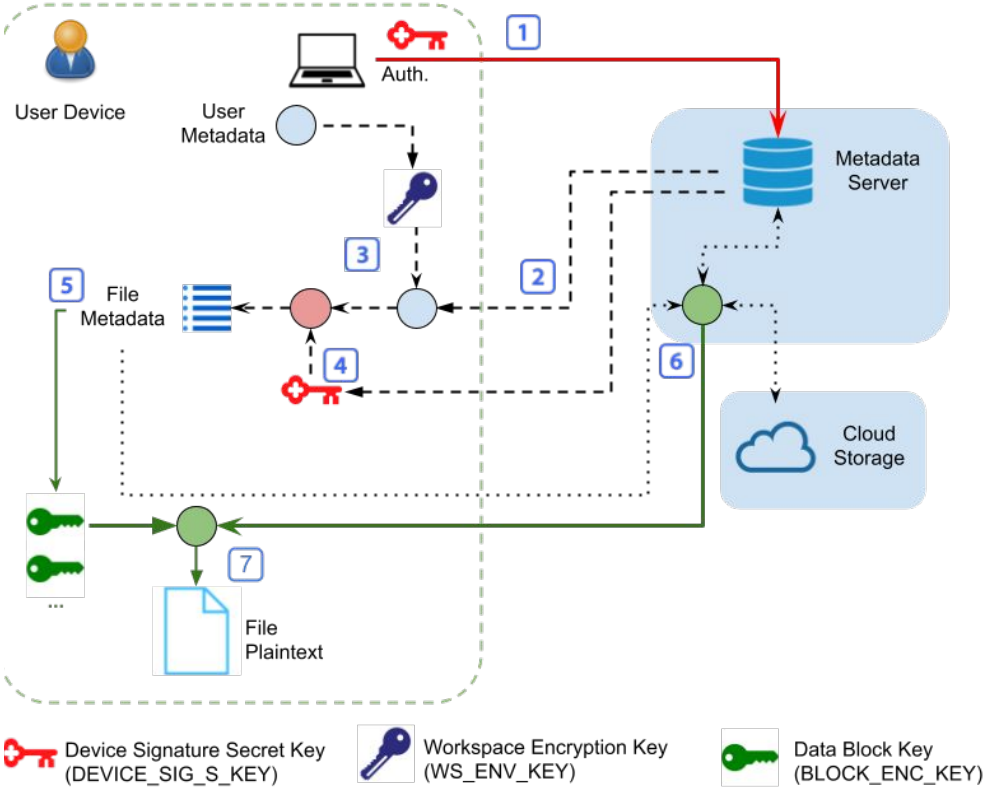
Fonction : Sécuriser localement la clé de chiffrement du UserManifest



Fonction : Garantir l'intégrité des données



Sécuriser les données



Sécuriser les données : Les clés symétriques

Clés Symétrique	Type	Stockage	Fonction
BLOCK_ENC_KEY	Chiffrement	FileManifest	Chiffre les blocs
WS_ENC_KEY	Chiffrement	UserManifest	Chiffre les métadonnées de fichier
USER_MAN_KEY	Chiffrement	Terminal utilisateur	Chiffre les métadonnées utilisateur
LOCAL_ENC_KEY	Chiffrement	Terminal utilisateur	Chiffre localement les métadonnées

Sécuriser les données: Les clés asymétriques

Clés Asymétrique	Type	Stockage	Fonction
DEVICE_SIG_P_KEY	Signature	Serveur de métadonnées	Vérifie la signature des métadonnées
DEVICE_SIG_S_KEY	Signature	Terminal utilisateur	Signe les métadonnées
USER_ENC_P_KEY	Chiffrement	Serveur de métadonnées	Chiffre un message pour un utilisateur
USER_ENC_S_KEY	Chiffrement	Terminal utilisateur	Déchiffre un message
ORG_ROOT_SIG_P_KEY	Signature	Terminal utilisateur	Vérifie la signature d'origine de l'organisation
ORG_ROOT_SIG_S_KEY	Signature	Détruite à la création de l'organisation	Première clé de signature d'un organisation (racine de la chaine de signature)

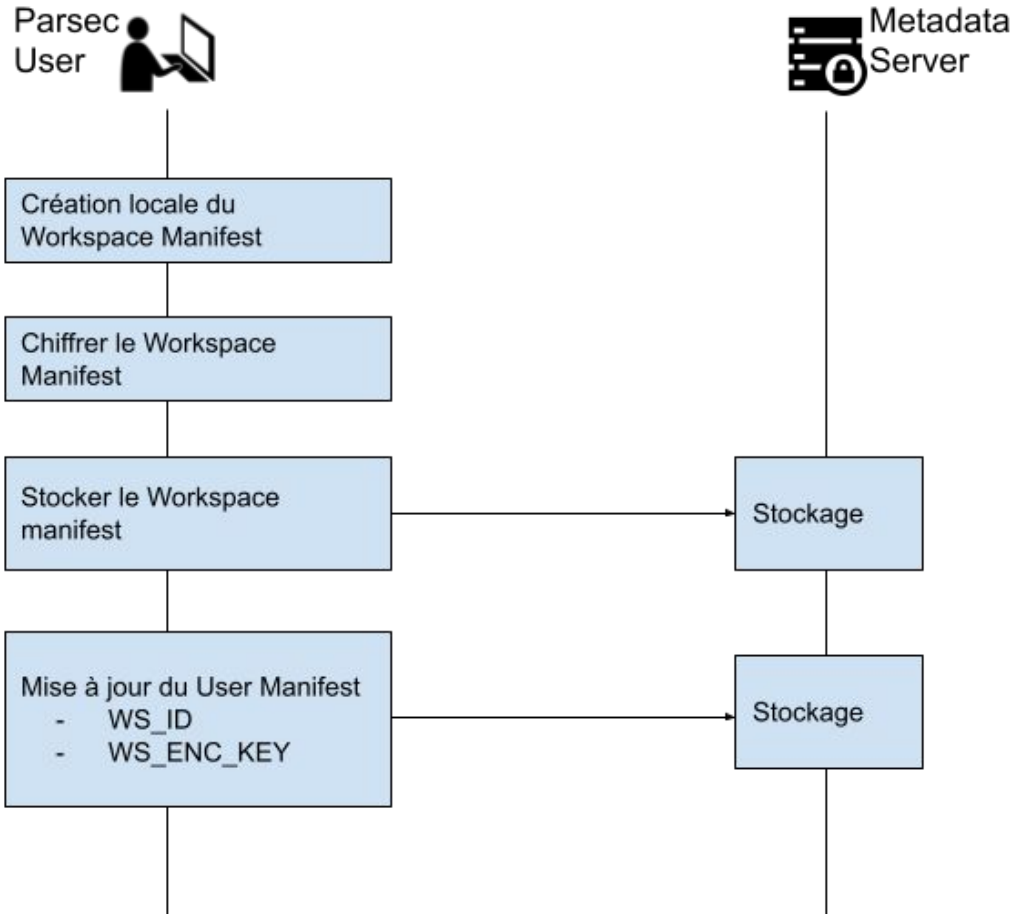
Menaces

Altération (corruption) des métadonnées	Signature des données
Altération (corruption) des blocs chiffrés stockés	Métadonnées + hachage des données
Compromission d’un poste de travail (ransomware, virus)	Historique des modifications
Altération de l’historique des fichiers	Signature des métadonnées
Compromission du secret “utilisateur”	Révocation
Compromission du secret “terminal”	Révocation
Bypass de la connexion (Man-In-the-Middle)	S.A.S. + Chiffrement Asymétrique

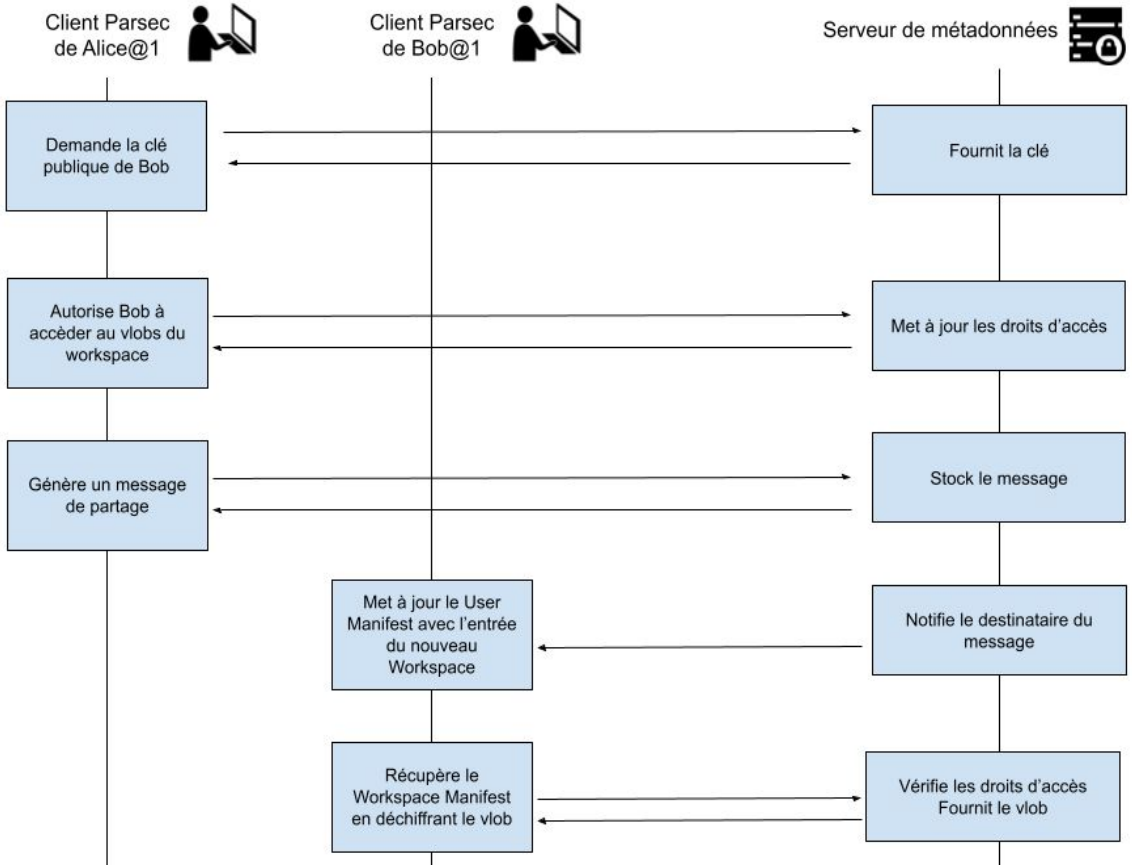
Menaces

Bypass de la vérification de signature d'un document	Chaine de signature, filtrage des documents compromis
Déni de service sur le serveur de métadonnées	Fonctionnement locale, Redondance du serveur de métadonnées
Violation de données par contournement du serveur de métadonnées et lecture directe des blocs chiffrés	Chiffrement des blocs, pas d'indexation
Perte d'un poste de travail utilisateur	Révocation
Violation de données par écoute des flux	Données chiffrée
Ingénierie sociale (vol d'information de connexion)	Révocation
Usurpation d'un terminal	Révocation

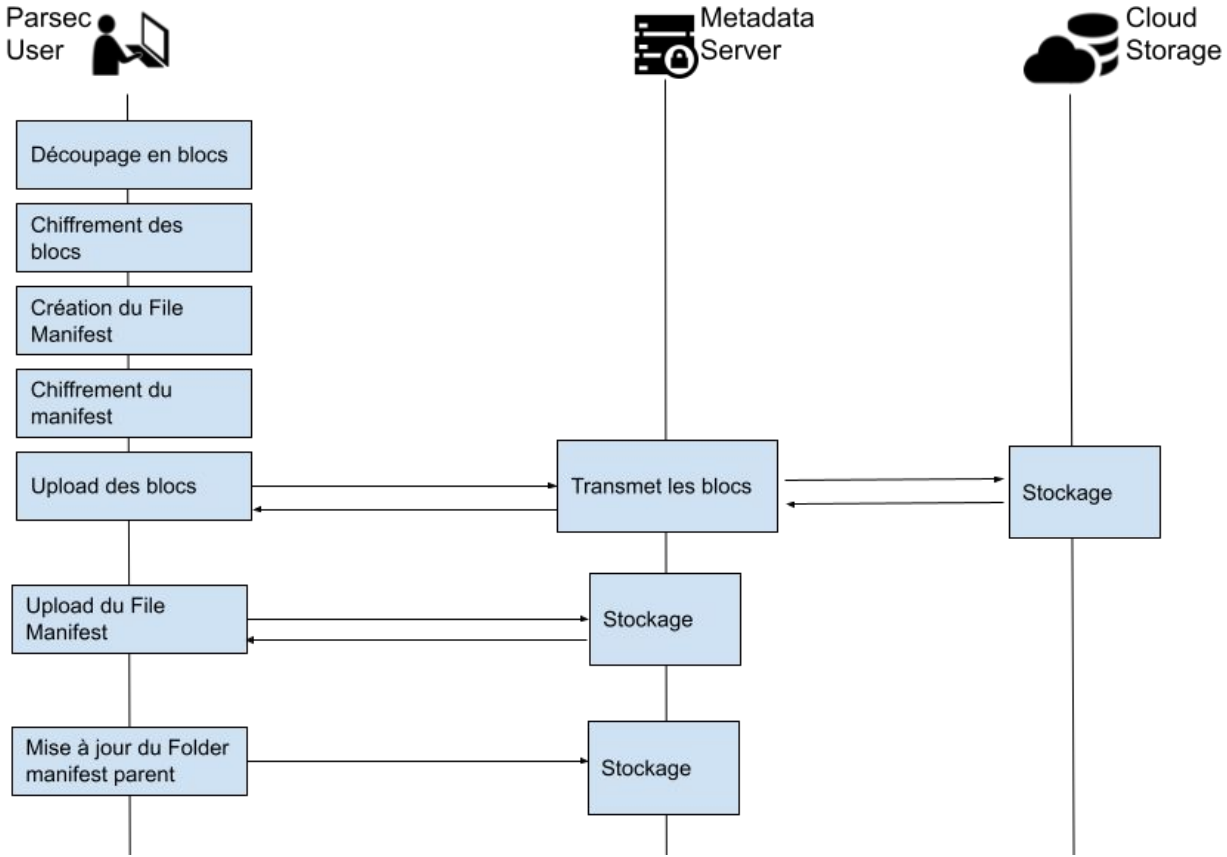
Processus “Création d’un espace de travail”



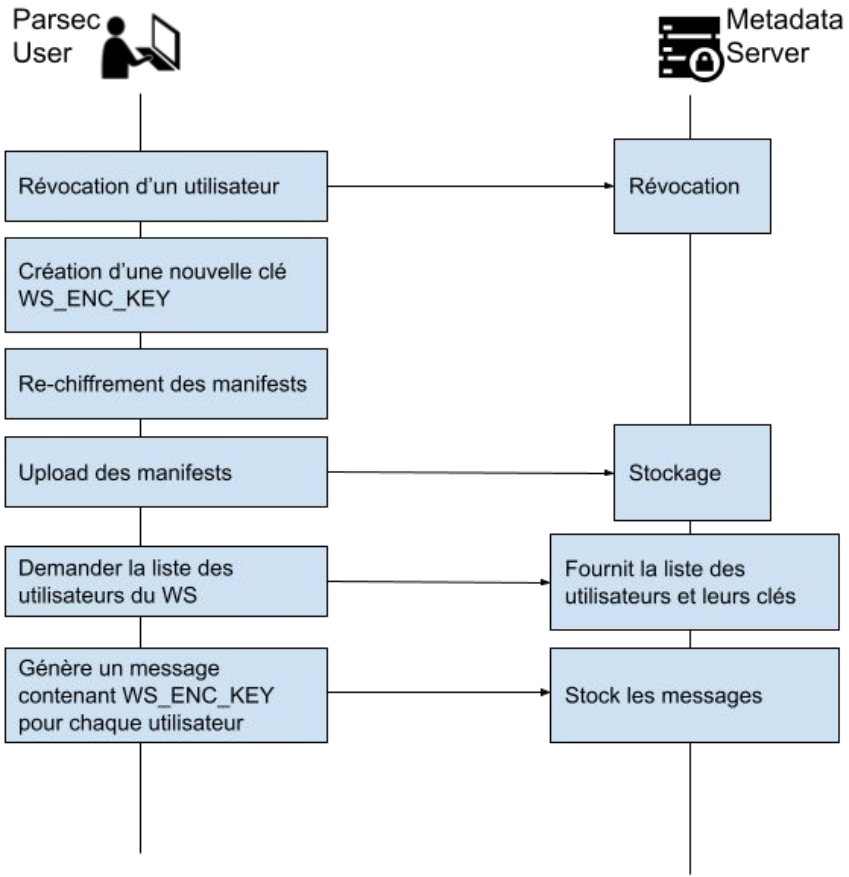
Processus “Partage d’un espace de travail”



Processus “Création d’un fichier”

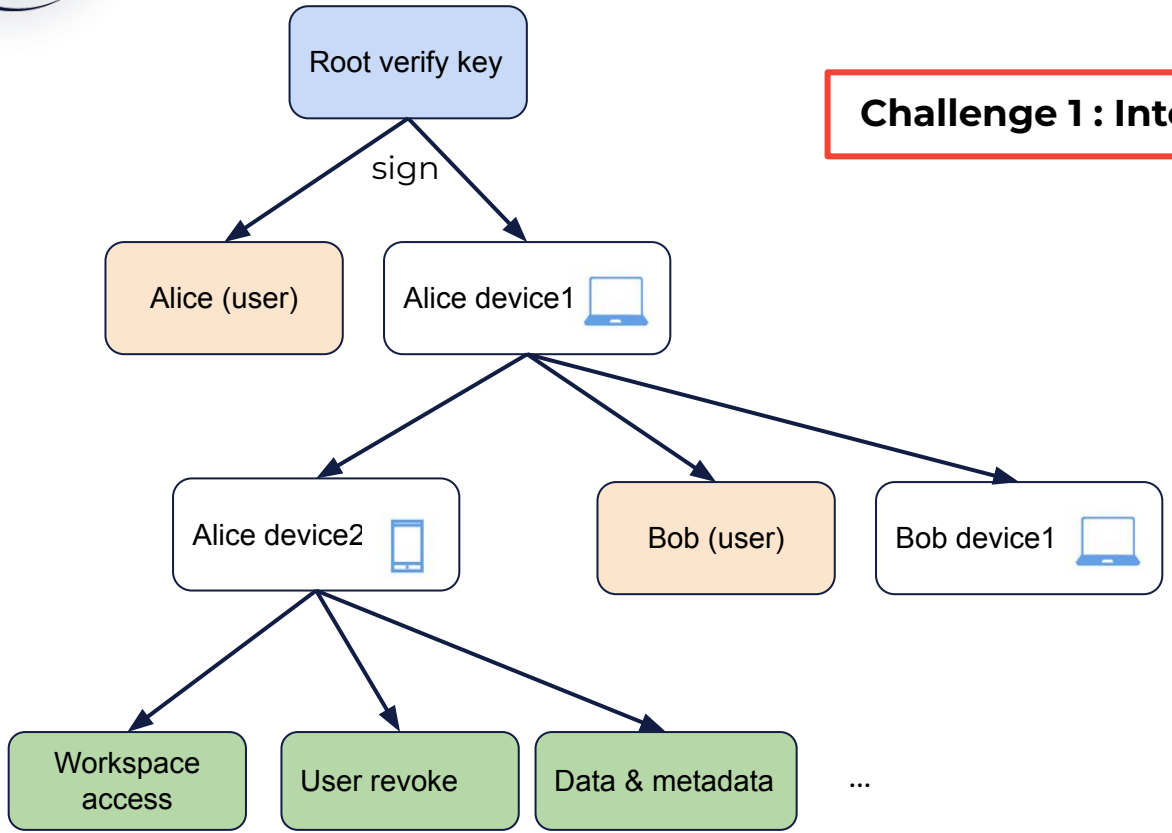


Processus “La révocation”



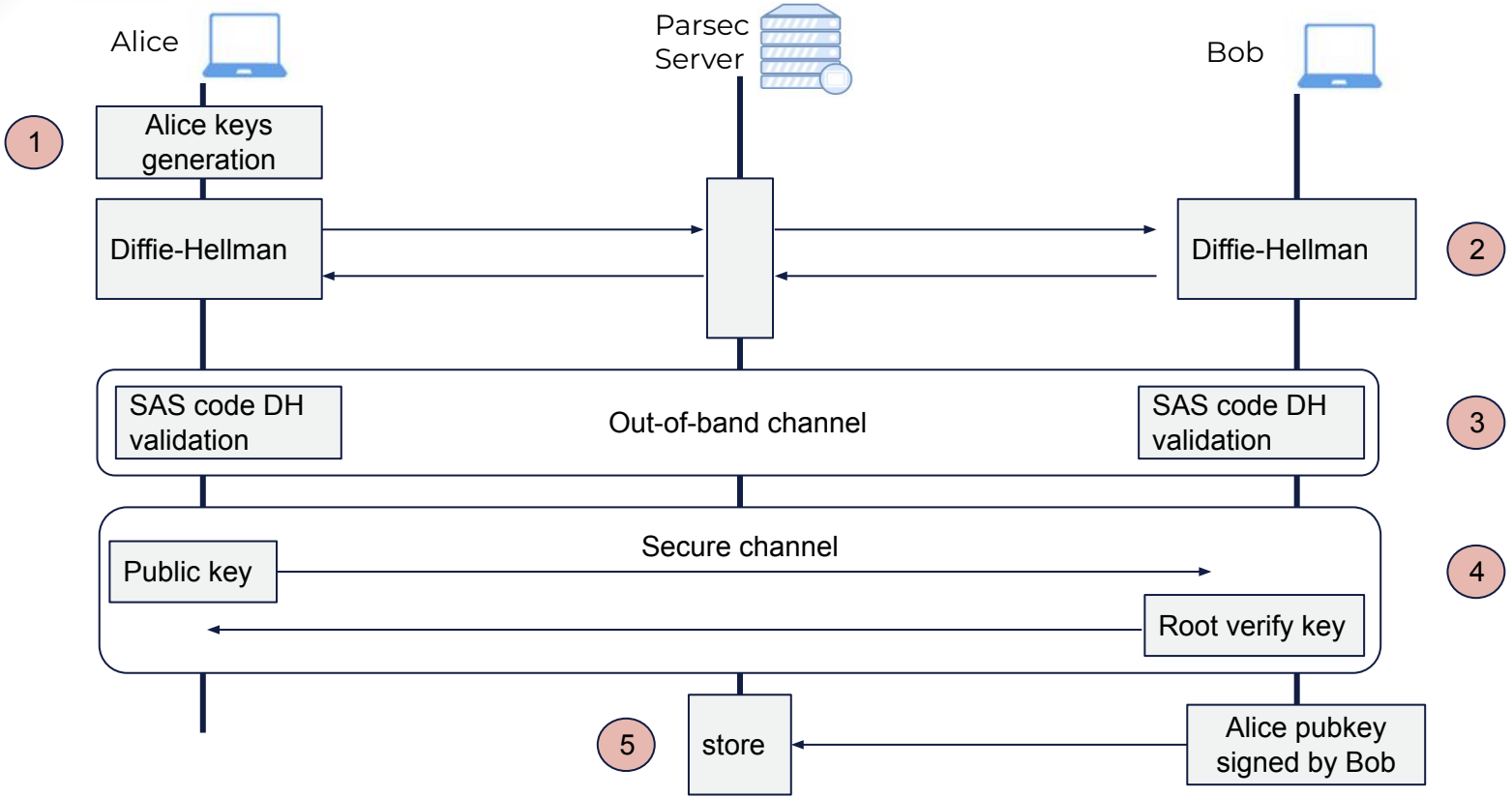

PARSEC
FRANCE 2030
PROGRAMME DE RECHERCHE
CYBERSÉCURITÉ
25 janvier 2025
CHALLENGES RÉSOLUS
VISA DE SÉCURITÉ

1) Circle of Trust management

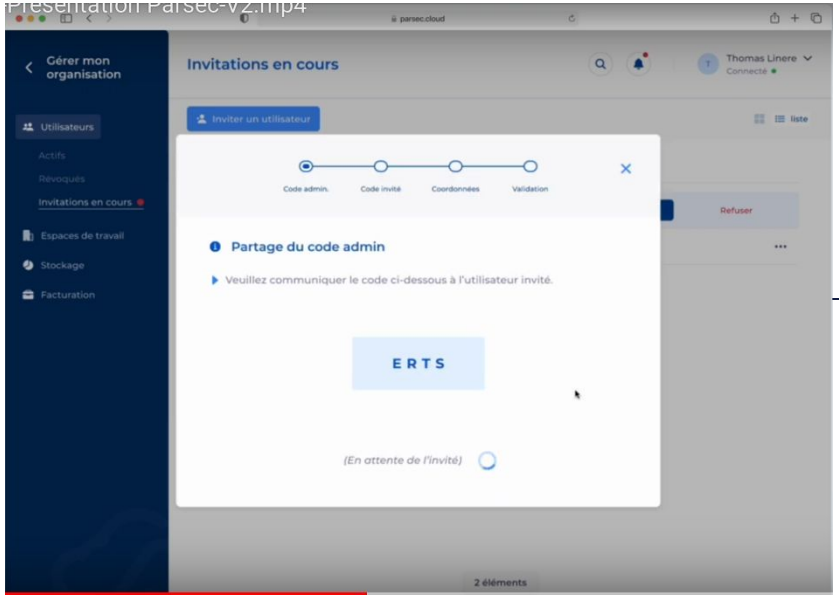


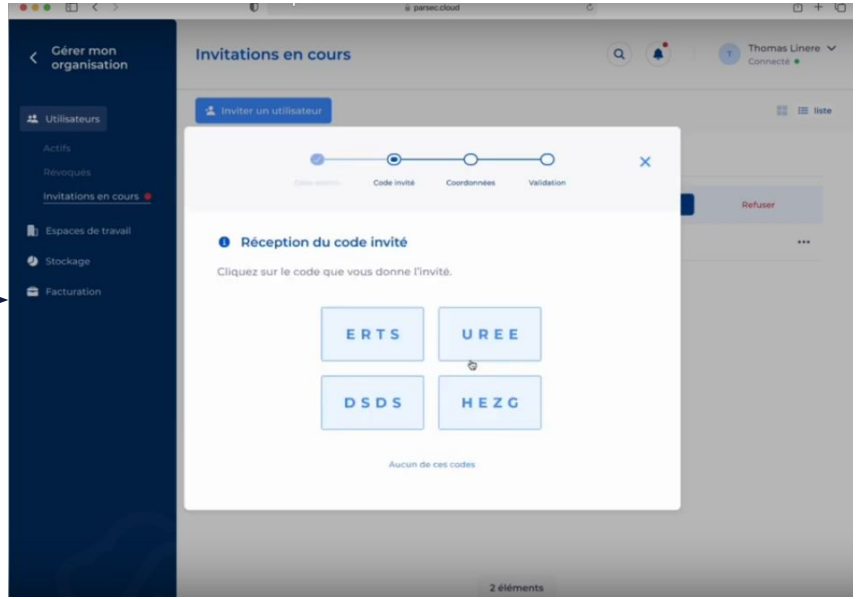
Challenge 1 : Integrate a dedicated PKI.

2) Simplified user enrollment & dedicated PKI



2) Simplified user enrollment & dedicated PKI

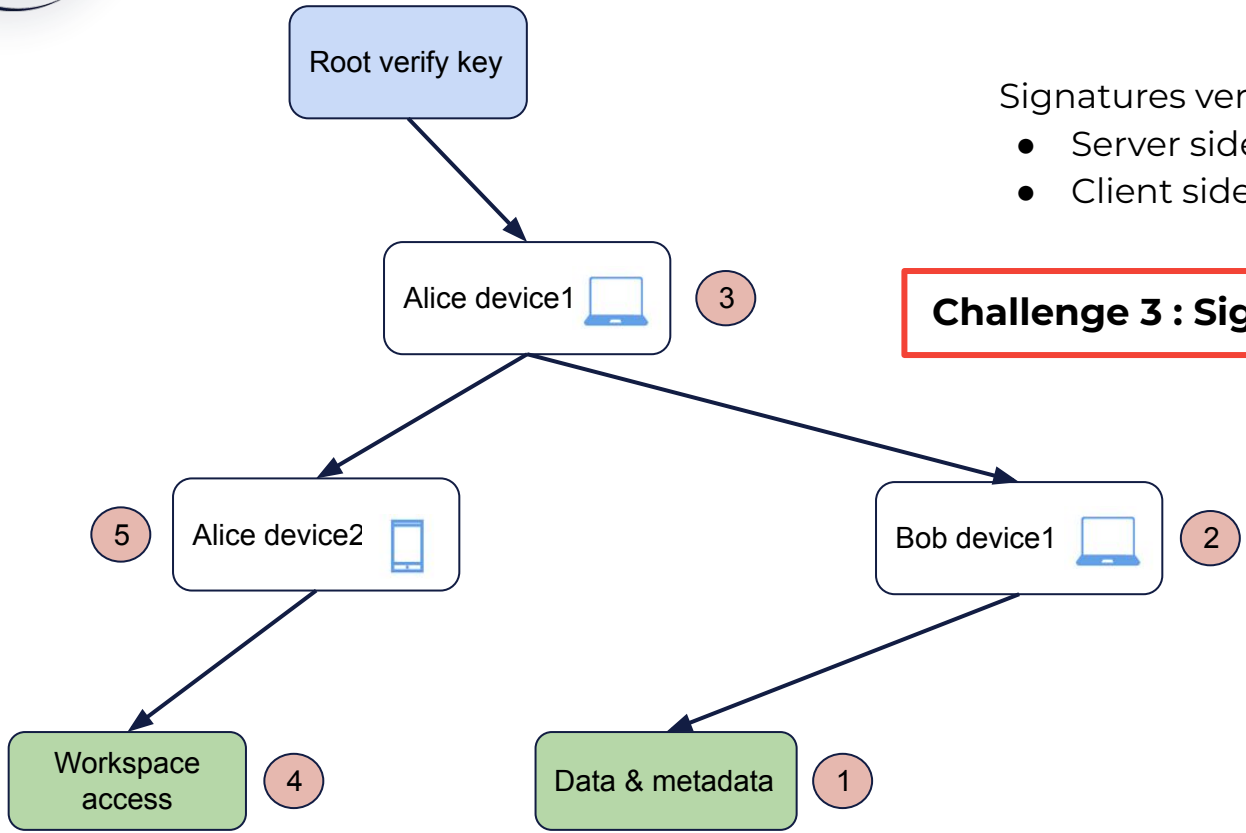




Challenge 2 : Only humans creates trust.

https://drive.google.com/file/d/1_abgGYTzRJwuTshZDQ0JMGnwb5_Opqyt/edit

3) Zero-trust data access

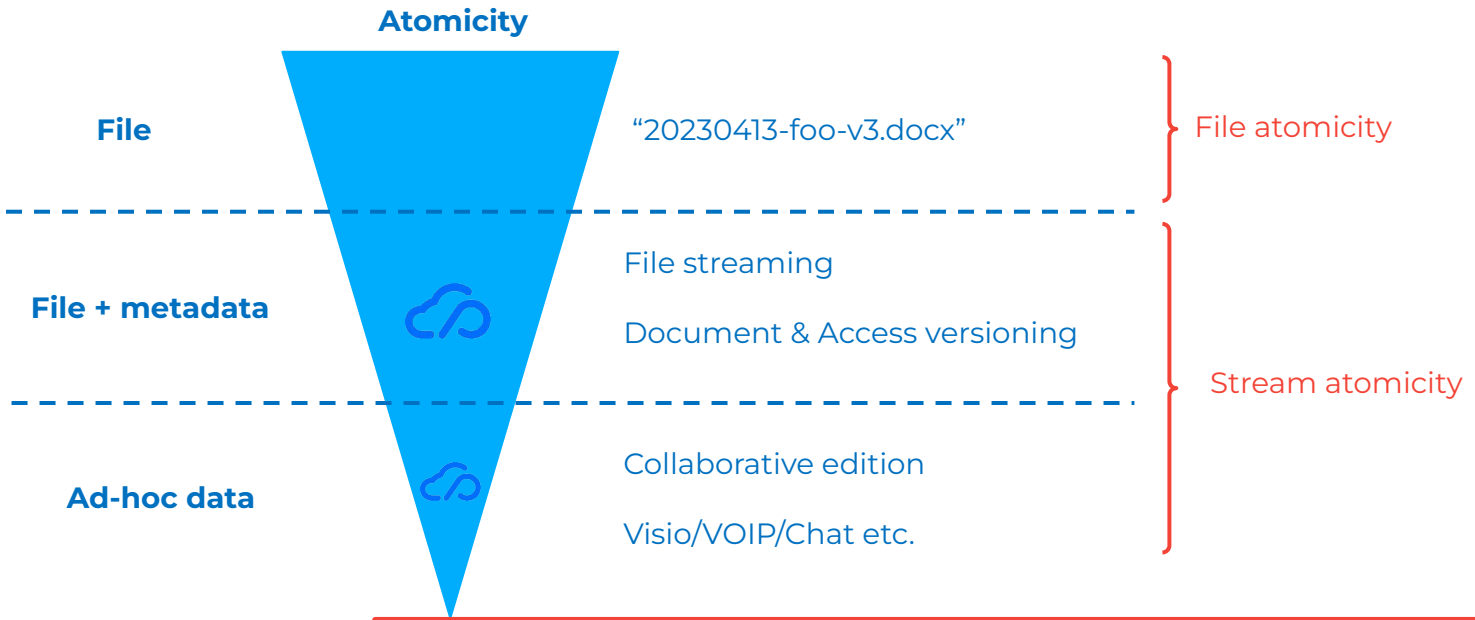


Signatures verified:

- Server side(access control)
- Client side (end-to-end trust)

Challenge 3 : Sign and encrypt everything.

4) File versus stream atomicity



Challenge 4 : Process flows, not documents.

5) Backward compatibility

In a classic web application:

- update functionalities → evolve the data model
- very simple on a centralized database

In an approach that no longer trusts the central server:

- All data is signed and encrypted, and the central server sees nothing (we don't trust it).
- How do you add a new concept (e.g., adding backward-compatible data classification)?
  - at server level
  - at client level: who signs?

Challenge 5 : Tthe end-to-end encryption issue exacerbates the resolution of data backward compatibility.

6) Strong applicative security integration

In a classic web application:

- security layer: TLS
- application layer: REST API

In a Data Centric Security application :

- REST API with signed & encrypted data
- Use case: Synchronization of (large!) Parsec files
  - divide file data into blocks
  - upload encrypted blocks to Parsec server
  - create a file manifest to reconstruct a given version of the file
  - file manifest signed and encrypted (with workspace key), uploaded to Parsec server
  - ⇒ problematic: user access revocation (file manifest re-encryption without signature change)
  - ⇒ upload order between blocks and file manifest

Challenge 6 : strong integration between security and applications.

7) Eventual consistancy

In a classic web application:

- he client is seen as the graphical interface
- a request to the server is enough to modify system state

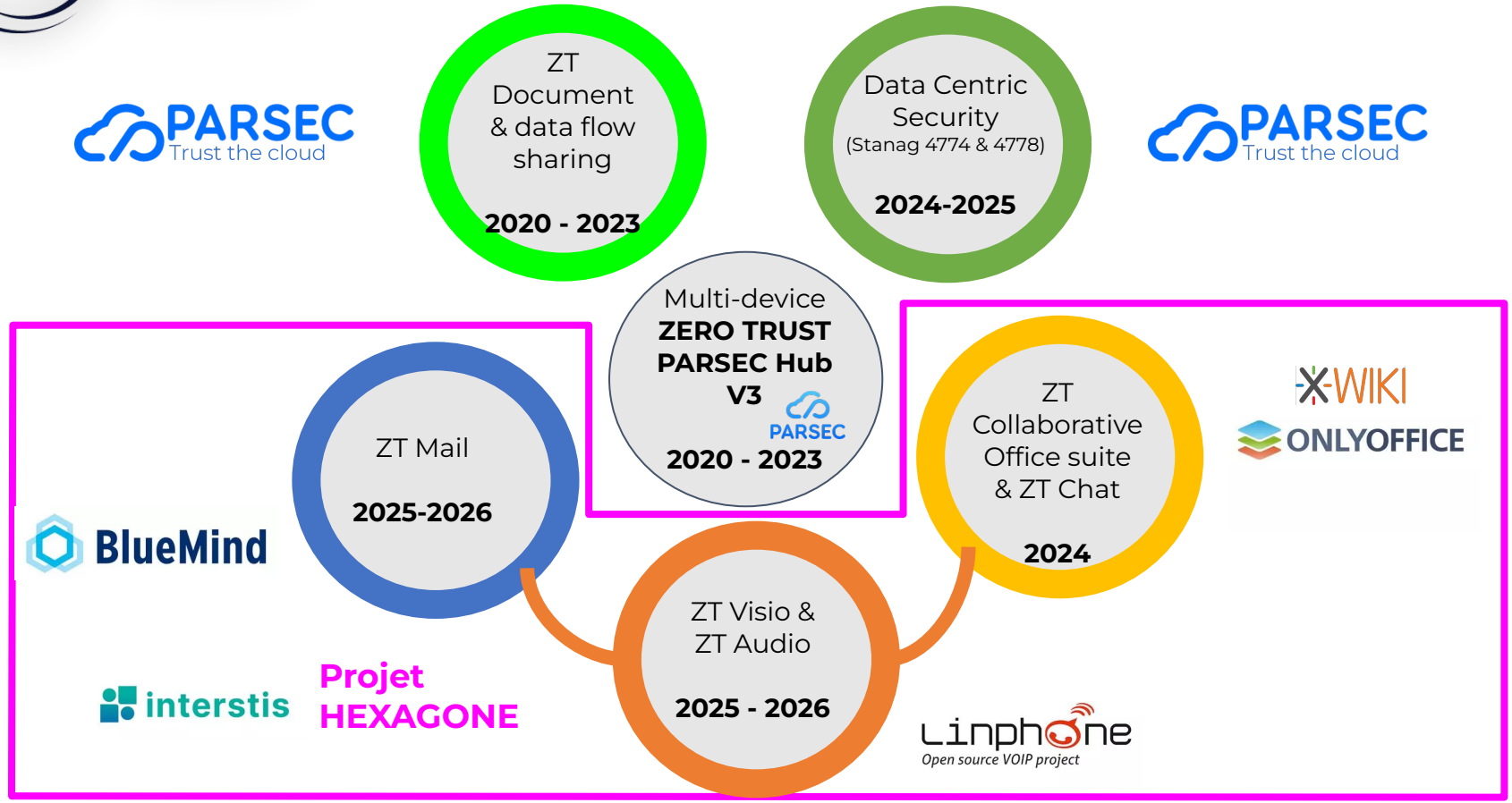
In a PARSEC logic, client and server states must be reconciled

- Issue 1) = withstand network failure
  - survive loss of connection
- Issue 2) = tolerate network latency and manage time scales
  - constant de-correlation between server state and client state
  - local modification must remain instantaneous as seen by the user
- Consequence: asynchronous operating mode:
  - operations are always performed locally
  - network outages have no consequences
  - client and server systems accept the decollation and agree when the network connection is re-established

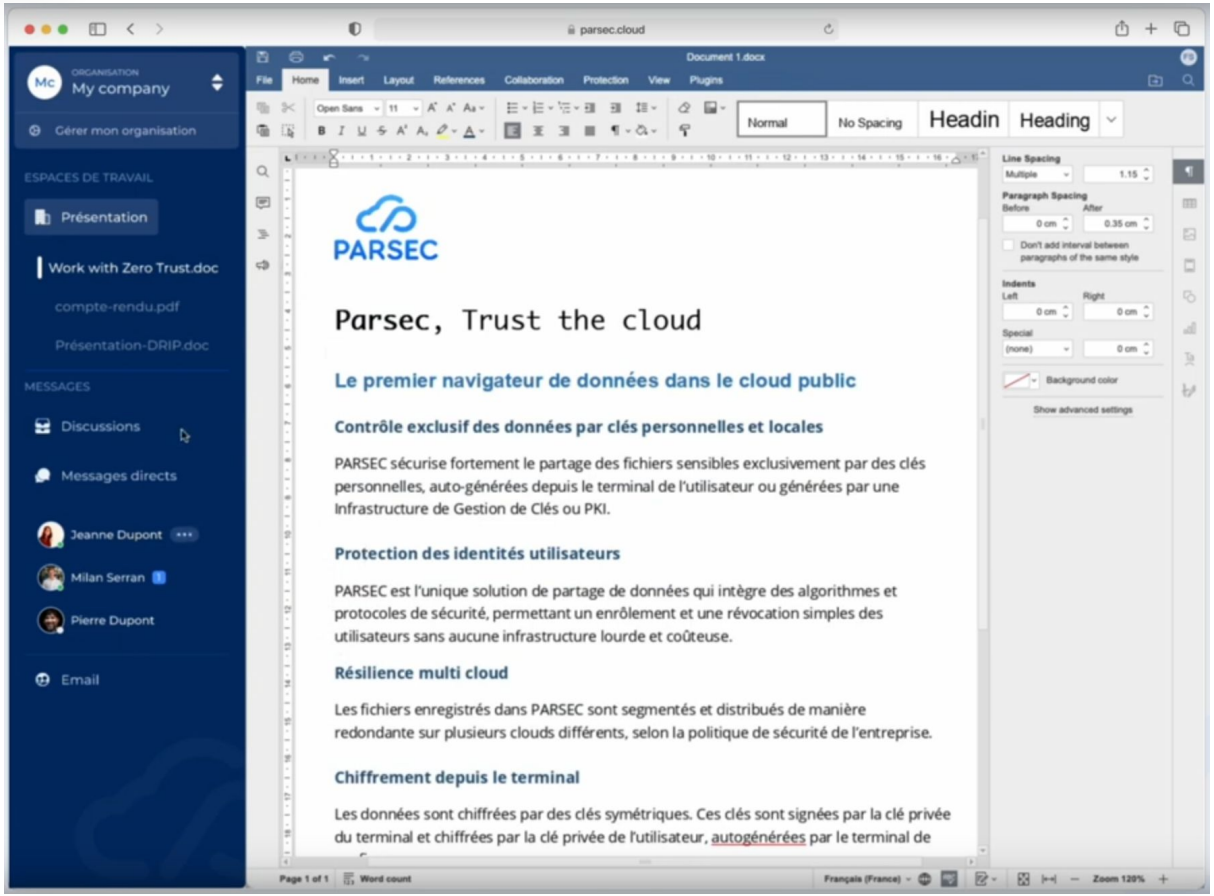
Challenge 7 = Correlate server and client status despite latency and network interruptions.


PARSEC
FRANCE 2030
PROGRAMME DE RECHERCHE
CYBERSÉCURITÉ
25 janvier 2025
APPLICATIONS DUALES
VISA DE SÉCURITÉ

Work Breakdown Structure (WBS)



Edition collaborative sur Only Office



Messagerie instantanée collaborative