La gestion d'identité au Centre de Calcul

Cyril L'Orphelin, Mattieu Puel

Contexte

Situation en 2020

- Gestion des demandes liées aux comptes via des pdfs et des demandes helpdesk faites par les correspondants de collaboration
- Architecture basée sur une brique logicielle OpenIDM => (Open) IDM
- Gestion centralisée des comptes non systématique (comptes locaux)
- 1 groupe = 1 groupe de calcul

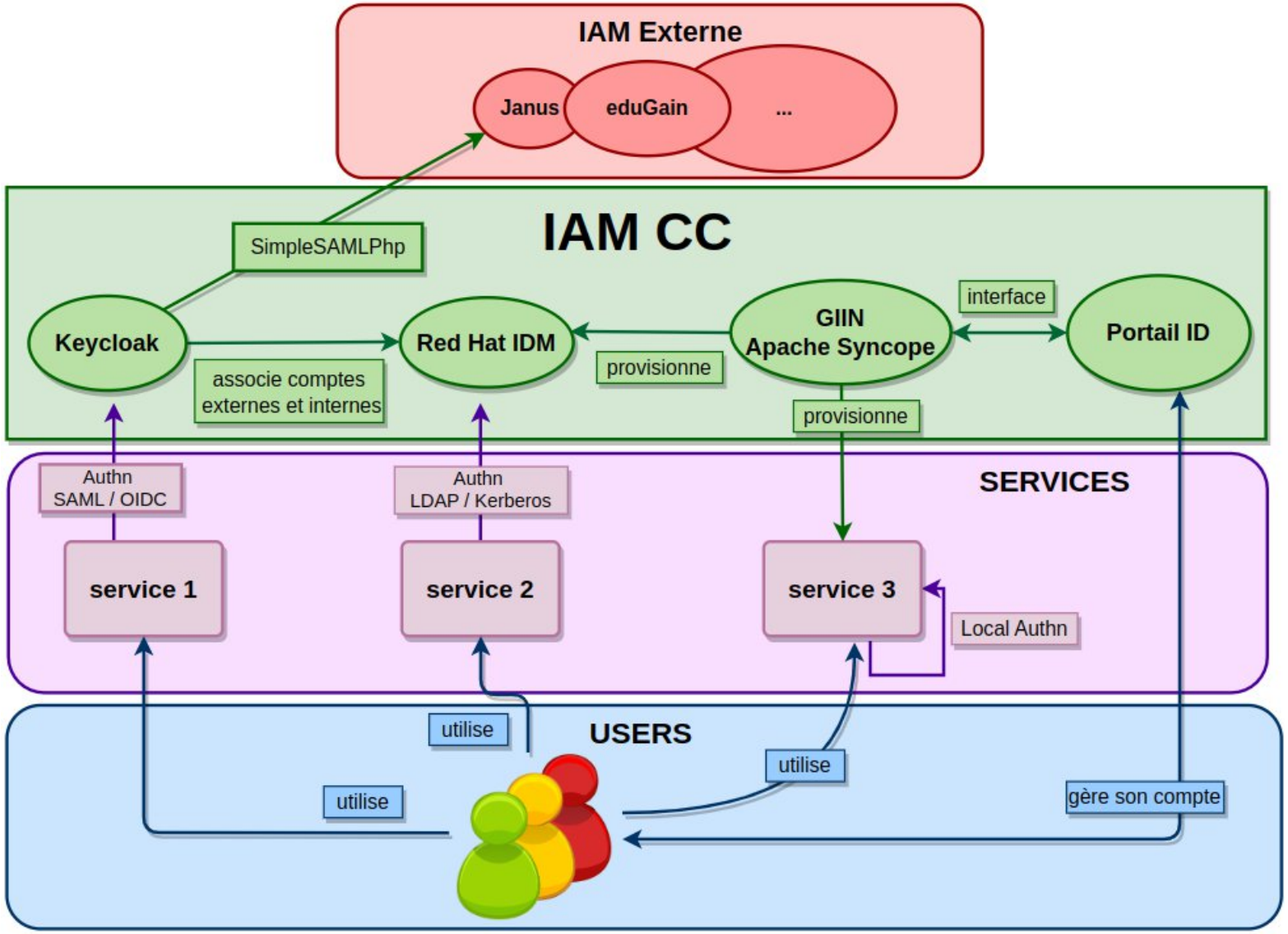
Conséquences

- Nombreuses opérations manuelles
- Services en silo
- Difficultés de gestion des accès et ressources de manière unifiée et fluide
- Pas de référentiel unique

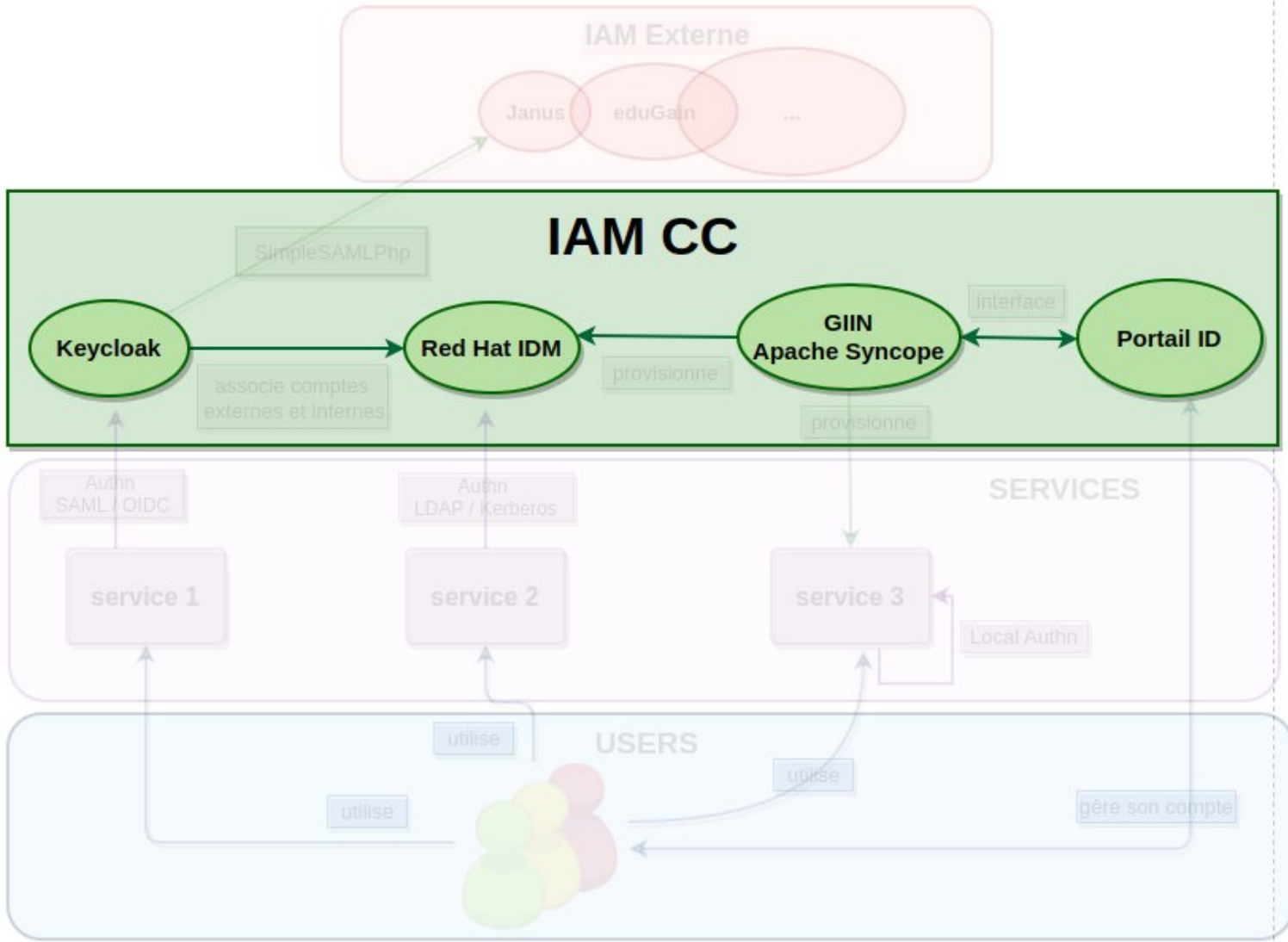
Objectifs en 2025

- Remplacement de la brique OpenIDM
- Gestion des demandes liées aux comptes via une interface web (Id)
- Automatisation de toutes les opérations
- Gestion centralisée et unifiée des identités, et des accès aux ressources
- Pilotage automatique via des connecteurs : les informations concernant les utilisateurs, les groupes et leurs accès/ressources sont homogénéisées dans les services.
- Visibilité accrue de qui à accès à quoi

Architecture globale



Briques IAM : vue globale



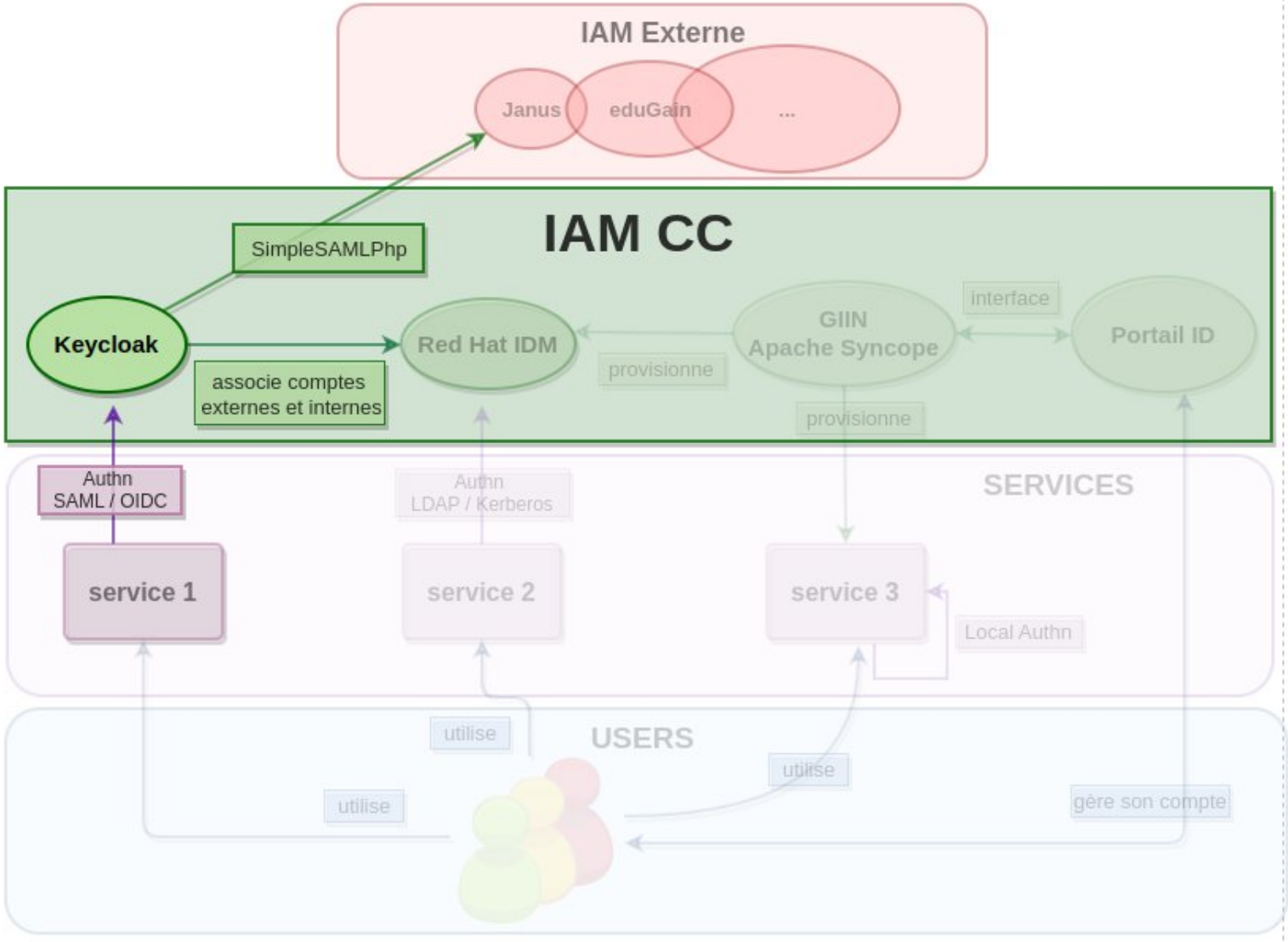
- plateforme open-source développée par RedHat

- plateforme développée par RedHat

- plateforme open-source développée par Apache

- portail web développé par le CC-IN2P3

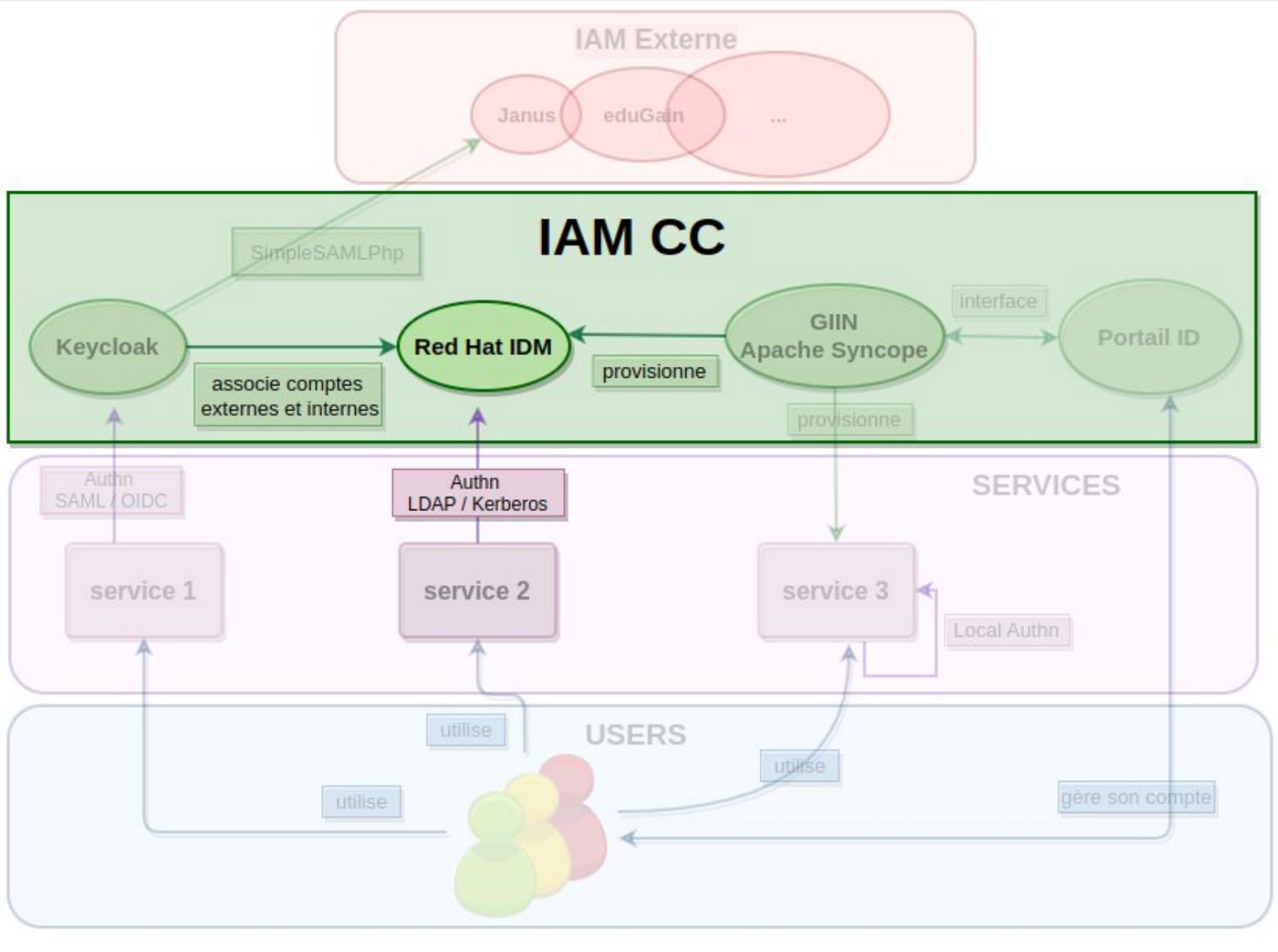
Briques IAM : keycloak



KEYCLOAK

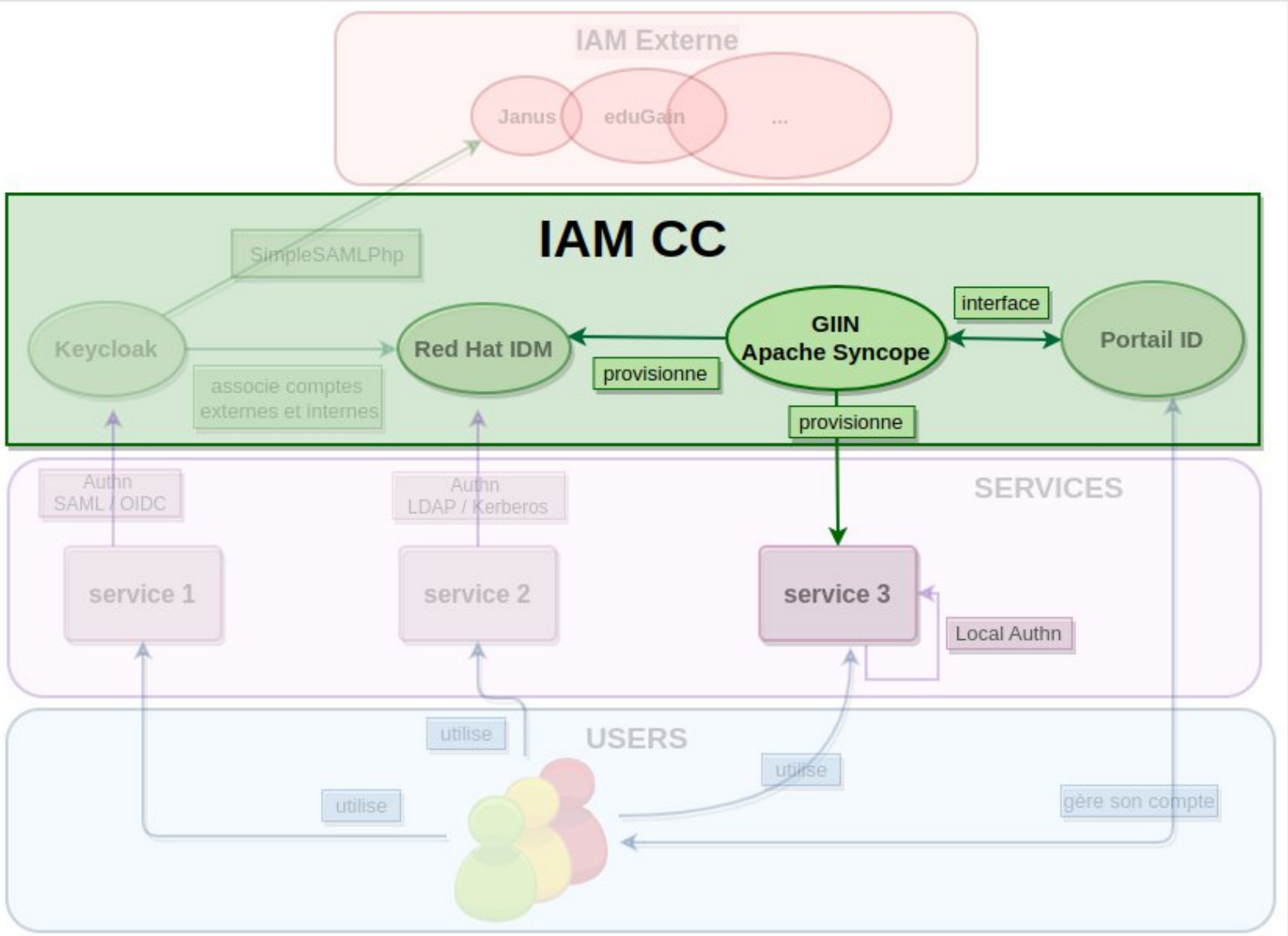
- Service de SSO
- Point d'entrée pour les utilisateurs
  - authentification locale / IDM
  - authentification via fédération (eduGain)
  - associe le compte externe au un compte local via l'e-mail
- Possibilité d'authentification 2 factors
- Deux protocoles sont supportés : SAML et OAuth/OpenID Connect.
- Via OpenID Connect / Oauth : les attributs locaux de l'utilisateur sont fournis au service

Briques IAM : IDM



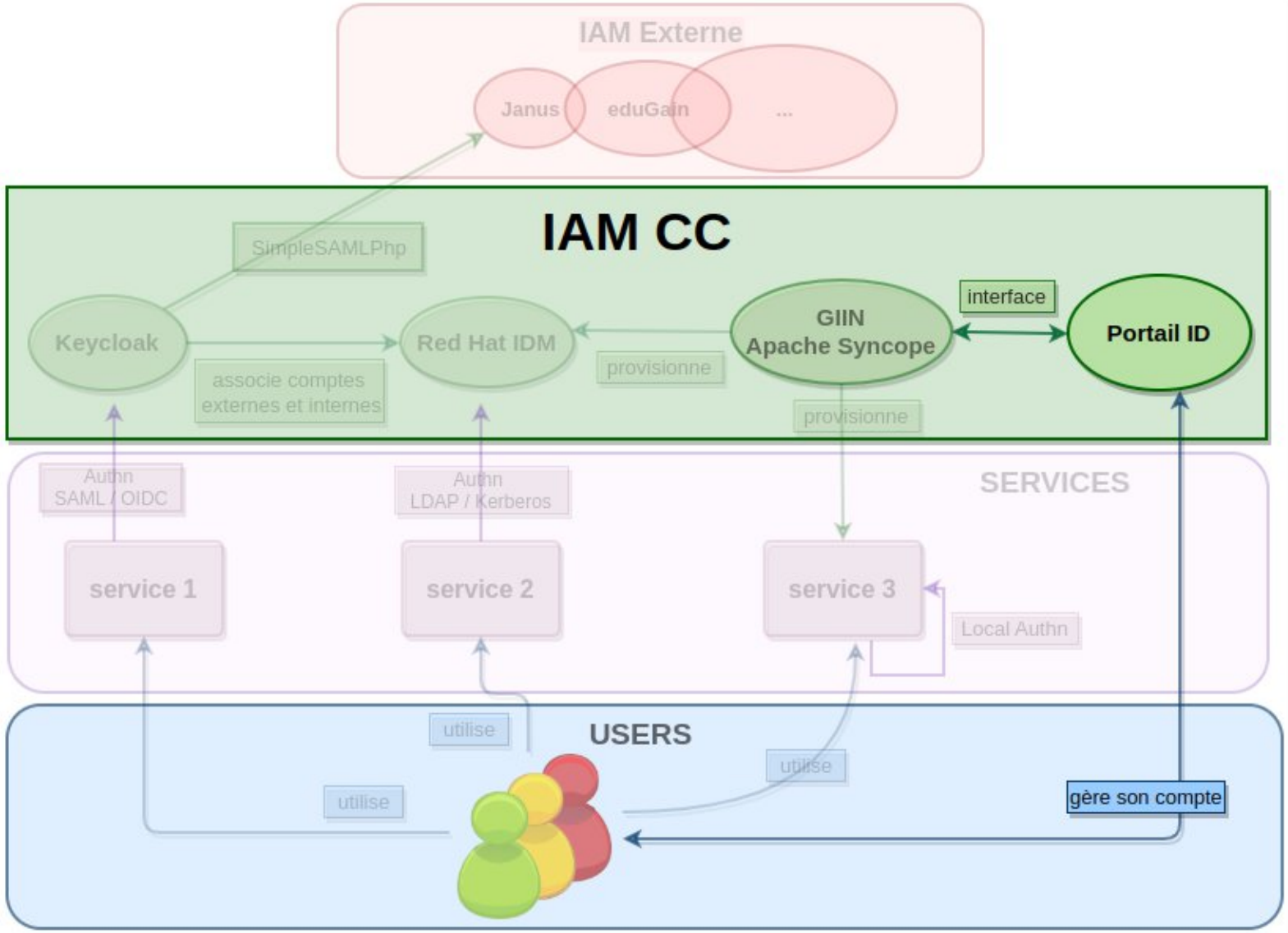
- Contrôleur de domaine (OpenLDAP)
- Gestion des accès et privilèges sur le parc informatique
- sert le royaume Kerberos (utilisateurs, machines, services)

Briques IAM : Syncope / GIIN



- centralise la gestion des comptes
- fourni une interface métier au reste du système d'information
- est la source d'information de référence pour IDM
- définit et exécute les workflows de gestion des données IAM

Briques IAM : ID



- Interface orientée utilisateurs
- Surcouche à GIIN/Syncope
- En mode self-service pour les utilisateurs
  - demande de compte
  - modification de profil
  - renouvellement mot de passe
- En mode privilégié pour les correspondants
  - validation des comptes
  - historique des actions
- En mode privilégié pour les admins
  - tableaux de bords
  - historique
  - modification des comptes
  - création de comptes spéciaux
  - désactivation des comptes

Phase 1 – Fonctions de base

- **Création de compte**
- **Rattachement de collaboration**
  - N'importe quel utilisateur peut demander le rattachement à une collaboration. Le correspondant de la collaboration intervient désormais dans ce processus : il est notifié et valide ou pas le rattachement. Le rattachement est une étape dissociée de la création.
- **Édition du profil par l'utilisateur** (nom, prénom, e-mail, nationalité).
- **Changement du mot de passe**
- **Gestion des comptes spéciaux** (comptes de production, comptes de formation)

Phase 2 – Workflow utilisateur

- **Revalidation du profil**
  - A l'expiration de son compte (1 an par défaut et < 3 ans pour un compte rattaché à une collaboration « labo »), l'utilisateur doit vérifier les informations de son compte, notamment au travers de la vérification effective de son e-mail. Le cas échéant, le correspondant de collaboration « labo » est notifié et saisit la nouvelle date d'expiration.
- **Activation / désactivation de compte**
  - Procédure permettant, dans le cadre d'un incident sécurité, de couper rapidement l'ensemble des accès de l'utilisateur : sans impact utilisateur.
- **Suppression de compte**
  - Actions réalisées après le départ de l'utilisateur
- **Ré-association de compte**
  - l'utilisateur pourra associer lui-même son identité eduGain à son compte CC

Phase 2 – Gestion des collaborations

- Création / Edition / Suppression d'une collaboration
- Revalidation de rattachement et Rattachement de collaboration
- Tableaux de bords
  - alertes
  - historique des actions
  - visualisation des comptes de la collaboration

Phase 2 – Workflow de gestion des structures de recherche

- Création / Edition / Suppression d'une structure de recherche

Renforcement de la politique d'intégration centralisée

- Disparition progressive des comptes locaux (exemple : Gitlab)
- Intégration des services via des connecteurs
- Gestion d'accès à ces mêmes services via une politique d'accès centralisée et unifiée
- Ajouts de fonctionnalités sur Id avec vos retours

Le groupe IAM

- Activité tranverse avec de nombreux contributeurs

- AZEVEDO Frédéric , CANEHAN Xavier, FERRAND Rémi, FONTANIERE Pierre-Yves, KACHELHOFFER Thomas, KHOUDER Ahmed, L'ORPHELIN Cyril, MARCHETTI Gino, PUEL Mattieu, ROUET Jean-René, SCHWARZ Lionel