



Présentation d'un IAM Keycloak

16/03/2023

ANS / DOPS



Sommaire

La gestion des accès et des identités au sein de votre SI

Cas pratique :

- Gestion des informations sur les scopes
- Connexion à un AD
- Fédération d'identité
- Enregistrement automatique via Pro Santé Connect



La gestion des identités et des accès

- La sécurité au service de la productivité

Le cœur de la notion d'IAM

Définition

Exemples

Identité

Document ou information contenant vos informations d'identité

Carte identité / passeport
Identifiant / mot de passe

Accès

Le niveau d'accès autorisé pour votre identité dans un référentiel cible

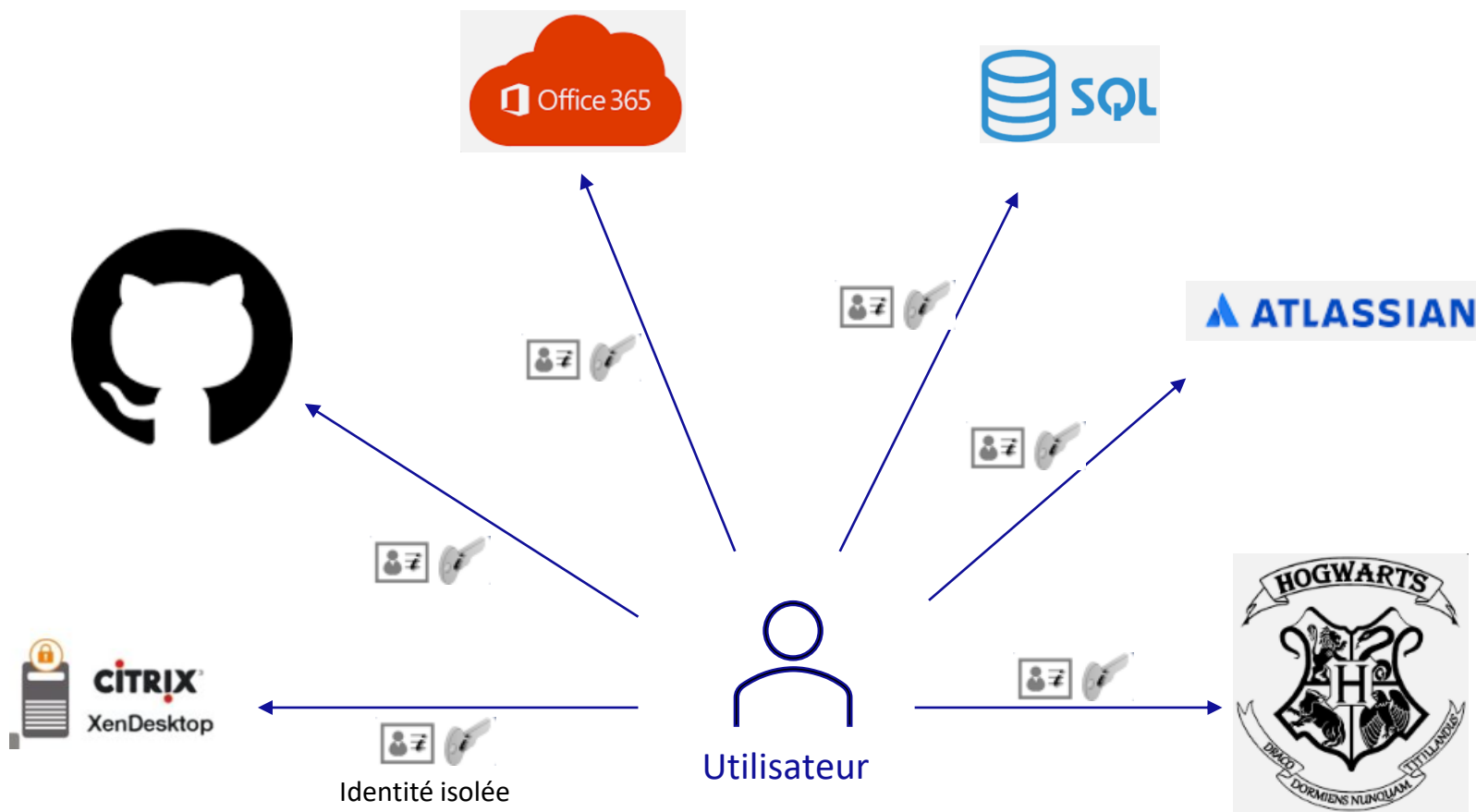
Zone VIP d'une boîte de nuit
Salle commune de Poudlard
Habilitation accordée à une profession médicale

Gestion

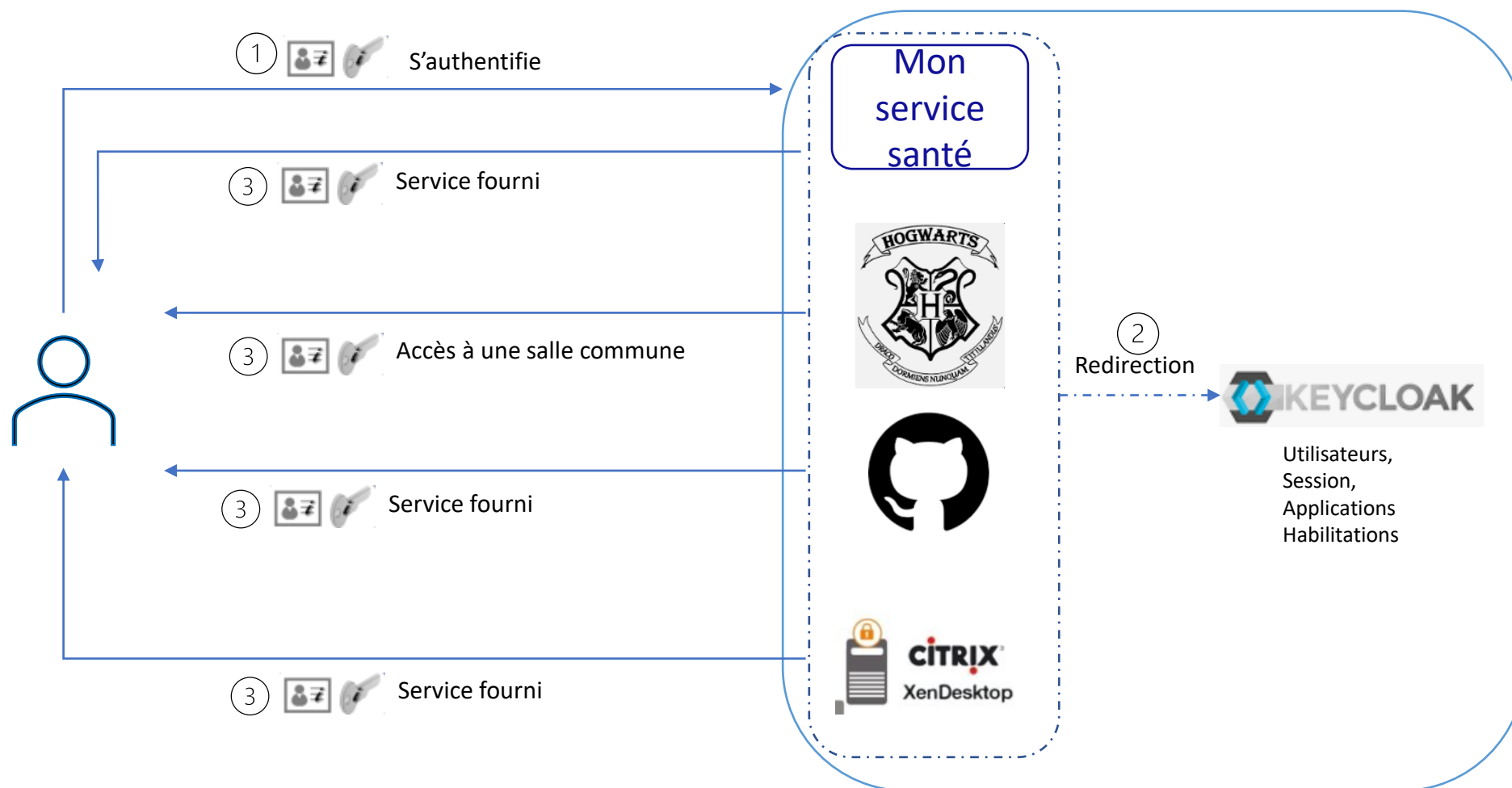
Centralisation des politiques de sécurité des identités et des accès.
Suivi de l'activité d'une identité ou bien d'un système cible

Liste des élèves
Liste des applicatifs
Critères d'adhésion

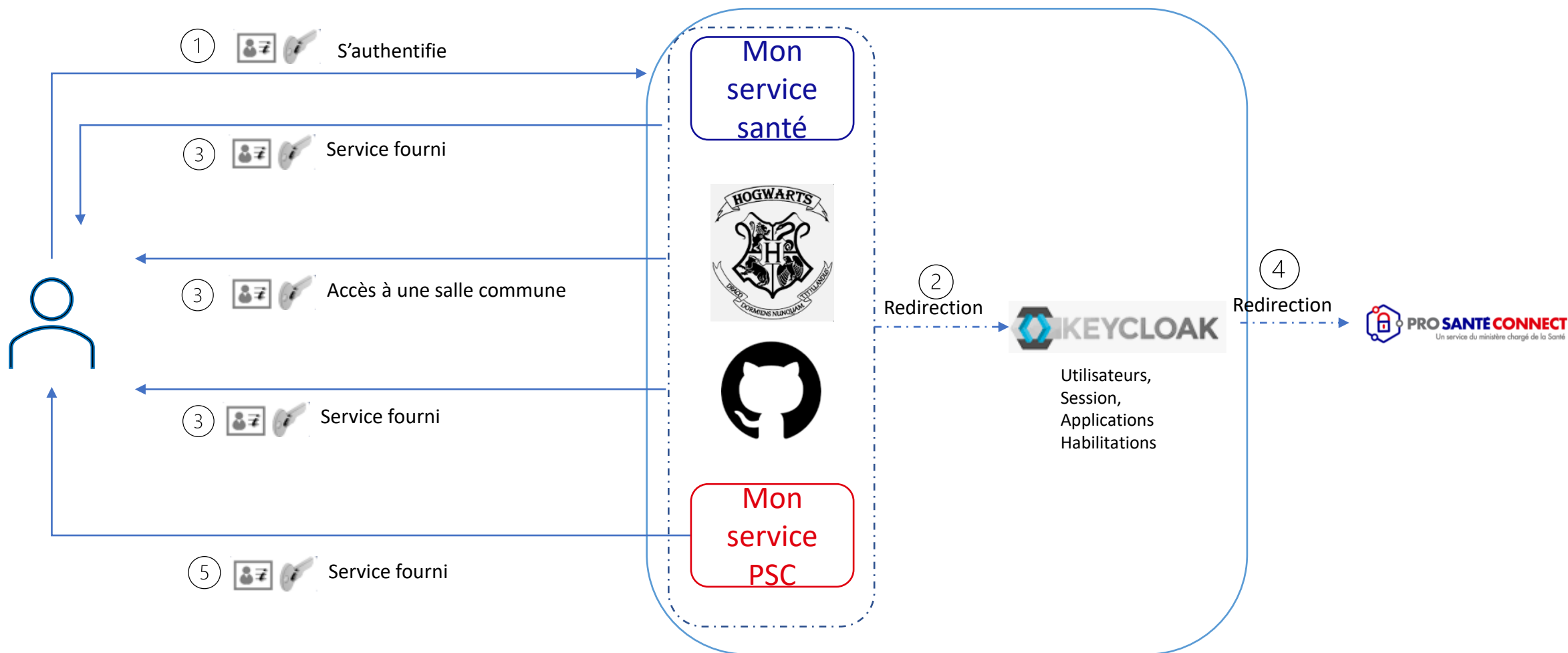
Une gestion potentiellement complexe des identités des applicatifs



IAM : Une solution facilitatrice pour gérer les accès applicatifs



Dans le contexte PSC,



Présentation des scopes



Définition

Le scope est un paramètre qui permet de :

- Demander des informations spécifiques sur l'utilisateur
- **Contrôler l'accès aux ressources protégées** en fonction des autorisations de l'utilisateur ou du fournisseur de service

Exemples

- Le choixpeau magique, **mécanisme d'enrôlement des utilisateurs** de Poudlard, a enregistré l'utilisateur Harry Potter dans la maison Gryffondor
- Si l'utilisateur **Harry Potter demande** à un portrait de Poudlard, le **fournisseur de service**, où se trouve la **salle commune de Gryffondor** le portrait lui indiquera où elle se trouve car **il est autorisé à utiliser le scope Gryffondor**.
- Si Harry demande où se trouve la salle commune de Poufsouffle le portrait déclinera sa demande car **il n'est pas habilité à utiliser le scope Poufsouffle**.

Applications Pro Santé Connect

Dans le cadre de PSC le endpoint UserInfo est **notre ressource protégée**. Il contient l'ensemble des informations sectorielles de l'utilisateur. **En tant que fournisseur de service vous pouvez récupérer sa profession, son activité, sa structure, etc...**

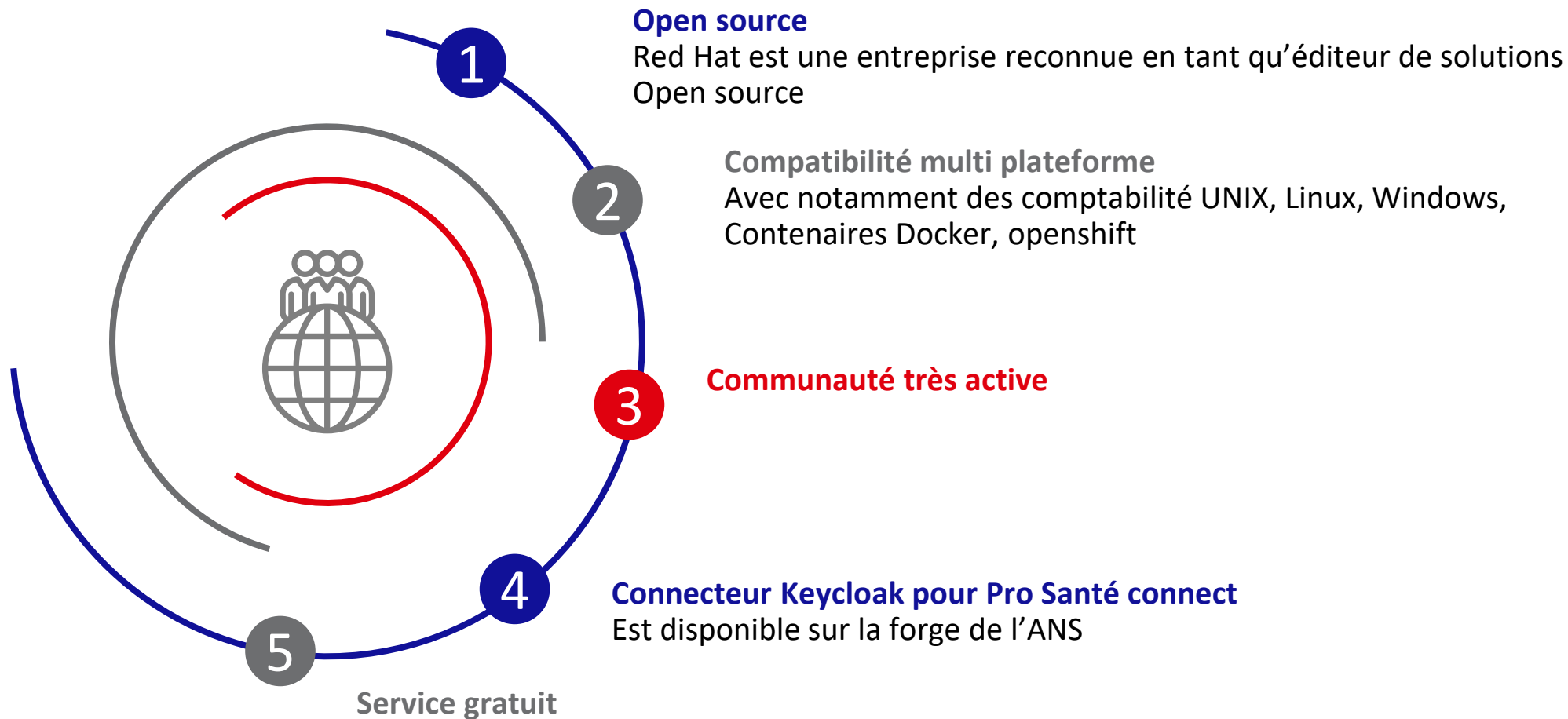
Pour obtenir l'ensemble des informations contenues dans le UserInfo la requête OIDC que vous envoyez à PSC contient le paramètre `scope=scope_all`

Scopes Pro Santé Connect disponibles

PSC vous propose d'autres scopes :

Scope	Claims du UserInfo
openid	sub
profile	given_name familyname
rpps	SubjectRefPro SubjectNameID
interopabilite	SubjectOrganization Mode_Access_raison Access_regulation_medicale UITVersion PalierAuthentification SubjectRole PSI_Locale SubjectNameID
referentiel	SubjectNameID othersIds
scope_all	Tout le contenu du UserInfo

Keycloak ? Un outil de gestion des identités et accès géré par Red Hat





esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.



@esante_gouv_fr



[linkedin.com/company/agence-du-numerique-en-sante](https://www.linkedin.com/company/agence-du-numerique-en-sante)