Documentation produit

Authentification, administration et habilitation des utilisateurs

Cloisonnement des données

Date	Version
31/03/2023	5.0 Version 6

État du document

◯ En projet ◯ Vérifié ◉ Validé

Maîtrise du document

Responsabilité	Nom	Entité	Date
Rédaction	JBR	Equipe Vitam - VaS	19/05/2020
Vérification	Equipe	Equipe Vitam - VaS	
Validation	AGR	Equipe Vitam	31/03/2023

Suivi des modifications

Version	Date	Auteur	Modifications
0.1	19/05/2020	JBR	Initialisation
0.2	08/03/2021	JBR	Mise à jour
1.0	15/03/2021	AGR	Relecture et finalisation en vue de la publication de la *release 16*
2.0	27/09/2021	AGR	Relecture et finalisation en vue de la publication de la *version 5.RC*
3.0	04/03/2022	AGR	Relecture et finalisation en vue de la publication de la *version 5*
4.0	27/01/2023	AGR	Relecture et finalisation en vue de la publication de la *version 6.RC*
5.0	31/03/2023	AGR	Finalisation en vue de la publication de la *version 6* *A noter qu'un travail de relecture globale va être lancé pour cette documentation.*

Documents de référence

N/A

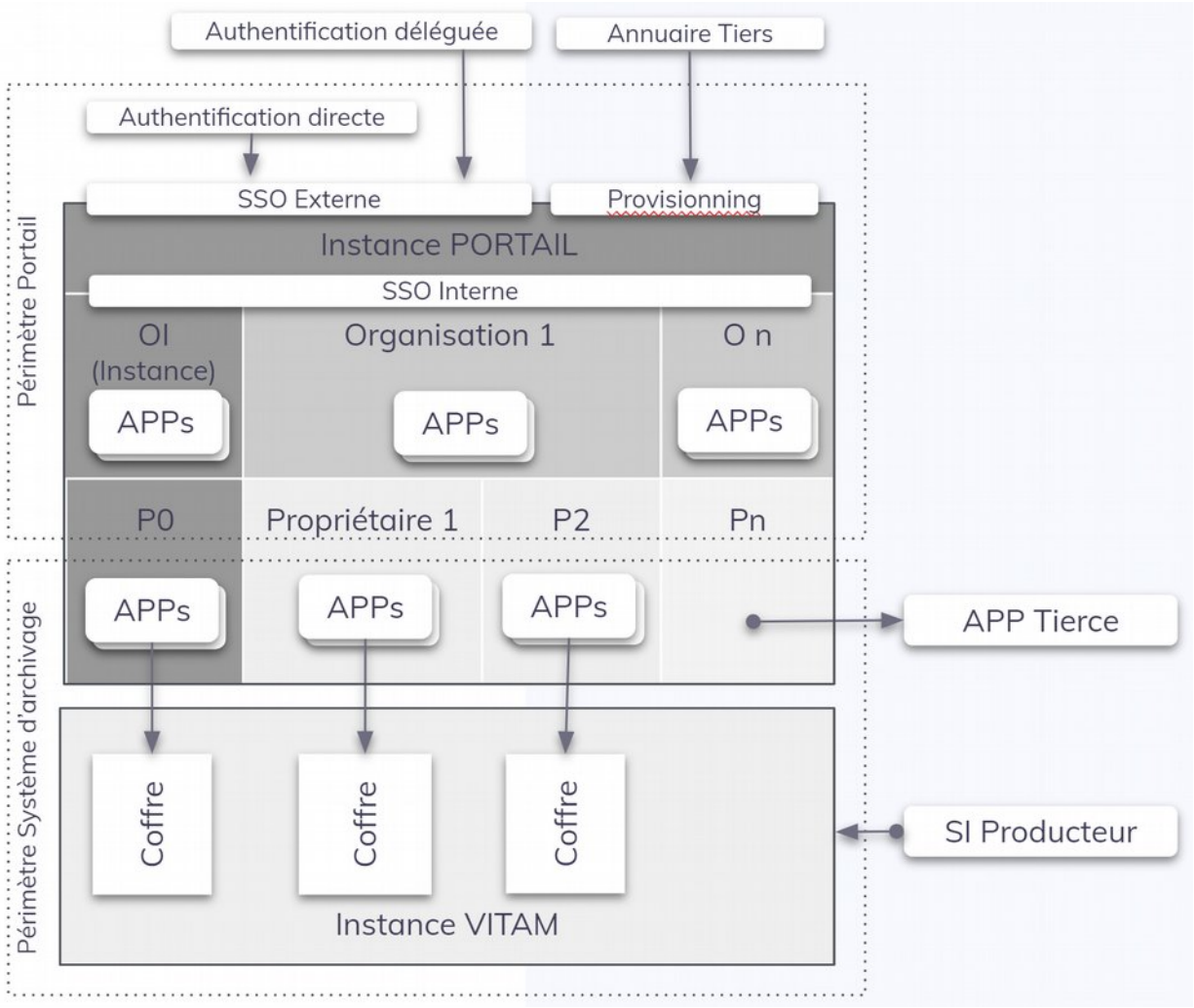
Licence

Table des matières

1. Panorama des fonctions du portail VitamUI

Le portail supporte :

- Les fonctions d'**accès** aux APPs (Applications) utilisées par des personnes ainsi que l'automatisation d'authentification (SSO) avec la solution
- Le mécanisme d'**habilitations** et d'**administration des utilisateurs**
- La sécurité de **communication** entre les APPs et le socle **Vitam**
- La gestion du **cloisonnement** entre les **organisations** utilisatrices d'une instance mutualisée et l'isolation des fonctions dédiées à l'opérateur d'instance (OI)
- L'attribution du **cloisonnemen**t documentaire en **coffres** (tenants de donnée Vitam) pour chaque organisation



Cette documentation produit concerne le périmètre fonctionnel portail et les APPs permettant d'utiliser ce périmètre.

2. Concepts et fonctions clés du produit

Ce chapitre présente les concepts pris en compte pour la conception fonctionnelle et technique de la solution.

Il s'agit des concepts et fonctions :

- d'identité et d'authentification dans la solution ;
- d'architecture en APP modulaires ;
- de gestion des droits et de séparation de rôles ;
- de cloisonnement des fonctions et des données ;
- de customisation des environnements (thèmes graphiques, multilingue).

La bonne compréhension de ces concepts est un prérequis pour :

- le paramétrage et l'administration de la solution ;
- le développement de nouvelles APP ou l'évolution de fonctions existantes.

2.1 Identité numérique

L'identité **numérique** est définie comme un lien technologique entre une entité réelle (personne, organisme ou composant informatique logiciel ou physique) et des entités virtuelles (sa ou ses représentations numériques).

L'identité peut être enregistrée sur la base d'un identifiant (dans un annuaire par exemple) ou reposer sur l'existence d'un certificat numérique.
La fiabilité de l'identité et du certificat dépend du niveau de contrôle réalisé par une autorité d'enregistrement de l'identité (déclaratif, fourniture de justificatif, vis-à-vis).

La solution dispose de son propre modèle permettant de gérer les identités de personnes et des composants informatiques internes et externes, préalablement enregistrés en amont de la solution.

Les fonctions du portail assurent la fédération d'identité des personnes et le lien entre les identités techniques des systèmes sous-jacents. L'objectif est d'administrer l'ensemble des droits de la solution et d'assurer la traçabilité exhaustive des transactions du système qu'elles soient initiées par utilisateur humain et/ou un mécanisme informatique.

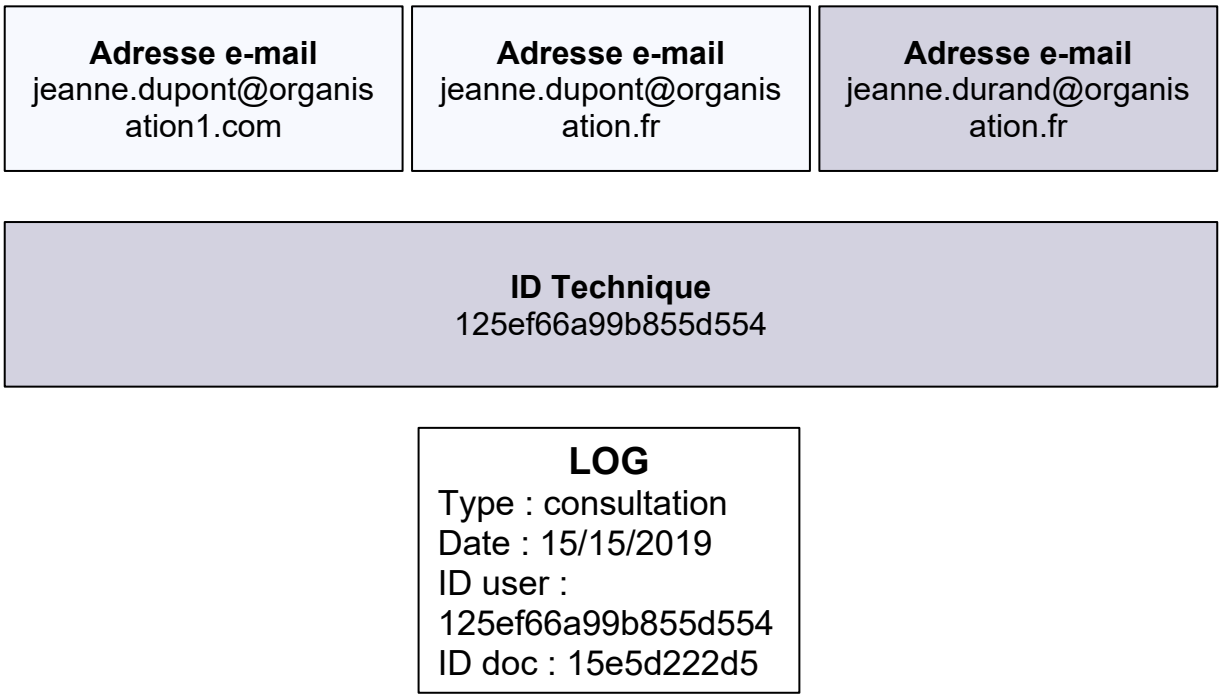
La traçabilité des identités est essentielle pour maintenir la capacité d'audit sur des durées longues, notamment pour historiser les responsabilités dans les transactions relatives au cycle de vie des archives.

2.2 Identité de personne

Les personnes physiques disposent de deux identifiants :

- adresse e-mail, nécessairement connue par l'utilisateur, utilisée en tant que login ;
- identifiant technique, attribué par la solution.

Les deux identifiants sont uniques au système à un instant T. L'adresse e-mail peut cependant évoluer dans le temps de manière à permettre de gérer les évolutions de domaines e-mail et d'identité des personnes (changement de nom, correction d'erreurs…).



L'identifiant technique est persistant dans la solution ainsi que le système de traçabilité qui devra être conservé au-delà de la durée d'exploitation de la solution, notamment pour les archives à durée de conservation longue ou illimitée.

Cette dualité d'identifiant permet :

- d'inscrire l'identifiant technique dans les traces et journaux du système. Une trace journalisée n'est pas modifiable ni effaçable ;
- d'anonymiser l'identité d'un utilisateur tout en conservant les traces techniques des opérations réalisées.

Le choix de l'e-mail nominatif comme identifiant de connexion pour l'utilisateur permet :

- une mémorisation simple pour l'utilisateur ;
- une unicité de l'identifiant « universelle » ;
- la limitation de @domaines professionnels maîtrisés par les organisations.

2.2.1. Annuaire

Le portail dispose de son propre annuaire des utilisateurs.

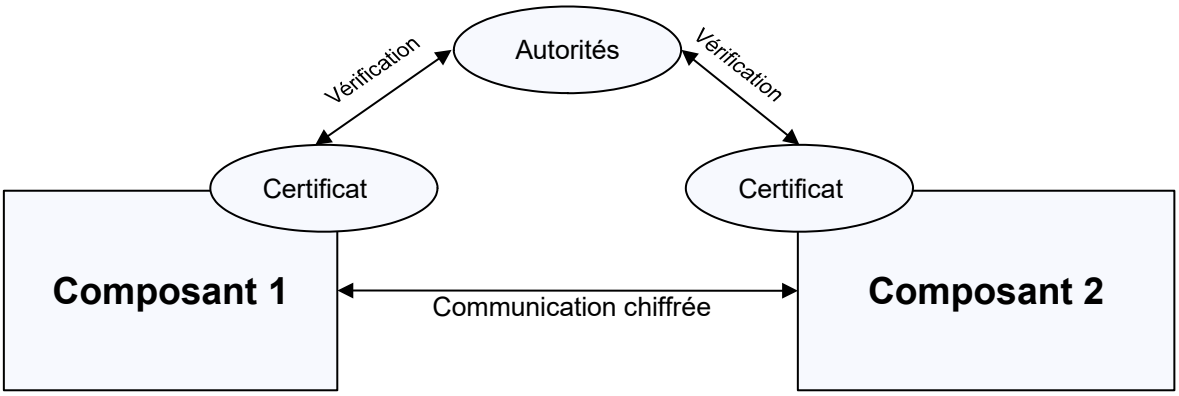
L'annuaire contient les deux identifiants utilisateurs (email et identifiant technique) ainsi que des informations liées à l'utilisateur (nom, prénom, coordonnées, préférences de langue…)

L'annuaire peut être synchronisé avec un annuaire tiers.
Il ne peut être substitué par un annuaire tiers car il est nécessaire de maintenir l'historique d'un utilisateur dans la solution.

2.2.2. Identité de composants informatiques

Chaque composant applicatif de la solution ainsi que les composants physiques d'infrastructure sont identifiés par des certificats numériques.

Les composants tiers interfacés à la solution doivent également être identifiés par certificat numérique



La validité des certificats utilisés par un composant doit pouvoir être vérifiée par consultation des trusted list des autorités de certifications ayant émis les certificats.

L'usage des certificats permet de garantir l'identité des composants et d'initialiser les canaux de chiffrement des communications entre les composants internes et externes à la solution.

2.3 Authentification

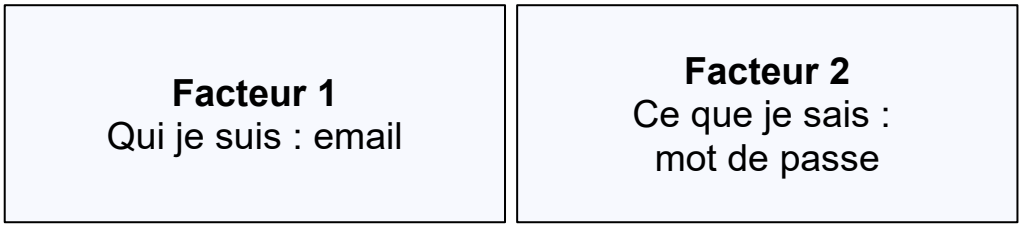
L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système...) afin d'autoriser l'accès de cette entité à des ressources du système conformément au paramétrage du contrôle d'accès.

La solution dispose de l'ensemble des fonctions permettant d'authentifier :

- des utilisateurs humains pour accéder à des interfaces utilisateurs (APPs) ;
- des services techniques entre eux, par exemple un connecteur de versement ou de consultation ;
- des APPs appelant des services techniques internes à la solution.

2.3.1. Authentification simple de personnes

L'authentification simple consiste à associer l'identifiant e-mail et un mot de passe connu de l'utilisateur via l'interface d'authentification au portail.



L'authentification est réalisée en deux étapes : saisie de l'adresse e-mail puis du mot de passe. En cas d'erreur sur l'une ou l'autre des informations, l'authentification est rejetée.

Les tentatives de connexion sont limitées à quatre (paramétrable au niveau de l'instance). L'utilisateur est bloqué durant 20 minutes après la quatrième tentative.

Ce dispositif, associé à une robustesse suffisante, permet de limiter le risque de résultat d'une attaque par force brute du mot de passe.

La robustesse du mot de passe est paramétrable au niveau de l'instance.
La durée de validité du mot de passe est paramétrable au niveau de chaque organisation.

2.3.2. Authentification forte de personnes

L'authentification forte consiste à compléter un facteur à l'authentification « simple » accessible par un dispositif en possession de l'utilisateur.

Facteur 1 Qui je suis : email	**Facteur 2** Ce que je sais : mot de passe	**Facteur 3** Ce que j'ai : téléphone

La solution propose en standard l'envoi d'un code de confirmation par SMS nécessitant de disposer d'un dispositif matériel (téléphone portable avec une carte SIM valide).

La solution peut être interfacée en spécifique avec des hard ou soft token permettant de générer de codes temporaires à usage unique (One Time Password ou OTP).

L'usage du troisième facteur d'authentification est paramétrable à deux niveaux :

- organisation : aucun OTP, OTP obligatoire pour tous les utilisateurs, Option OTP attribuée par l'administrateur des utilisateurs ;
- administration : si l'administrateur dispose du droit d'activation / désactivation de l'OTP sur les utilisateurs, il choisira d'affecter l'option OTP selon une stratégie définie par l'organisation.

Par sécurité, les utilisateurs ne peuvent pas activer ou désactiver l'option OTP ni modifier le numéro de téléphone en destination du code de validation.

2.3.3. Authentification de personnes par certificat

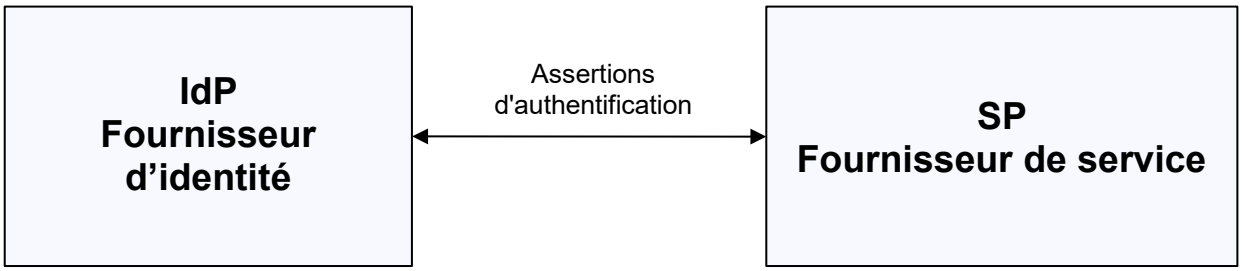
La solution permet l'usage de certificats numériques (X509…) contenus dans des cartes à puces (Badge d'accès aux locaux physiques et/ou poste de travail, carte CPS…).

Facteur 1 Qui je suis : certificat	**Facteur 2** Ce que je sais : code carte	**Facteur 3** Ce que j'ai : carte

Ce moyen d'authentification forte nécessite un interfaçage spécifique selon la technologie utilisée par l'organisation utilisatrice du service d'authentification par certificat de personnes.

2.3.4. Authentification déléguée de personnes (Single Sign On ou SSO)

L'authentification déléguée consiste à réaliser le processus d'authentification des utilisateurs par un fournisseur d'identité tiers (Identity provider ou IdP).



Suite à cette authentification, une communication est réalisée entre l'IdP et un fournisseur de service (Service Provider ou SP) afin d'autoriser l'accès automatiquement.

Le portail est SP pour des IdP des organisations ou de fournisseur d'identité tiers (France Connect, Agent Connect…)

Ce type d'authentification présente deux avantages :

- simplicité pour l'utilisateur qui n'a pas à s'authentifier dans la solution ;
- sécurité pour l'organisateur car en cas de départ d'un utilisateur, celui-ci ne pourra pas s'authentifier à la solution si son compte est désactivé par l'IdP.

En cas d'usage du SSO, la sécurité de l'authentification est de la responsabilité de l'IdP.

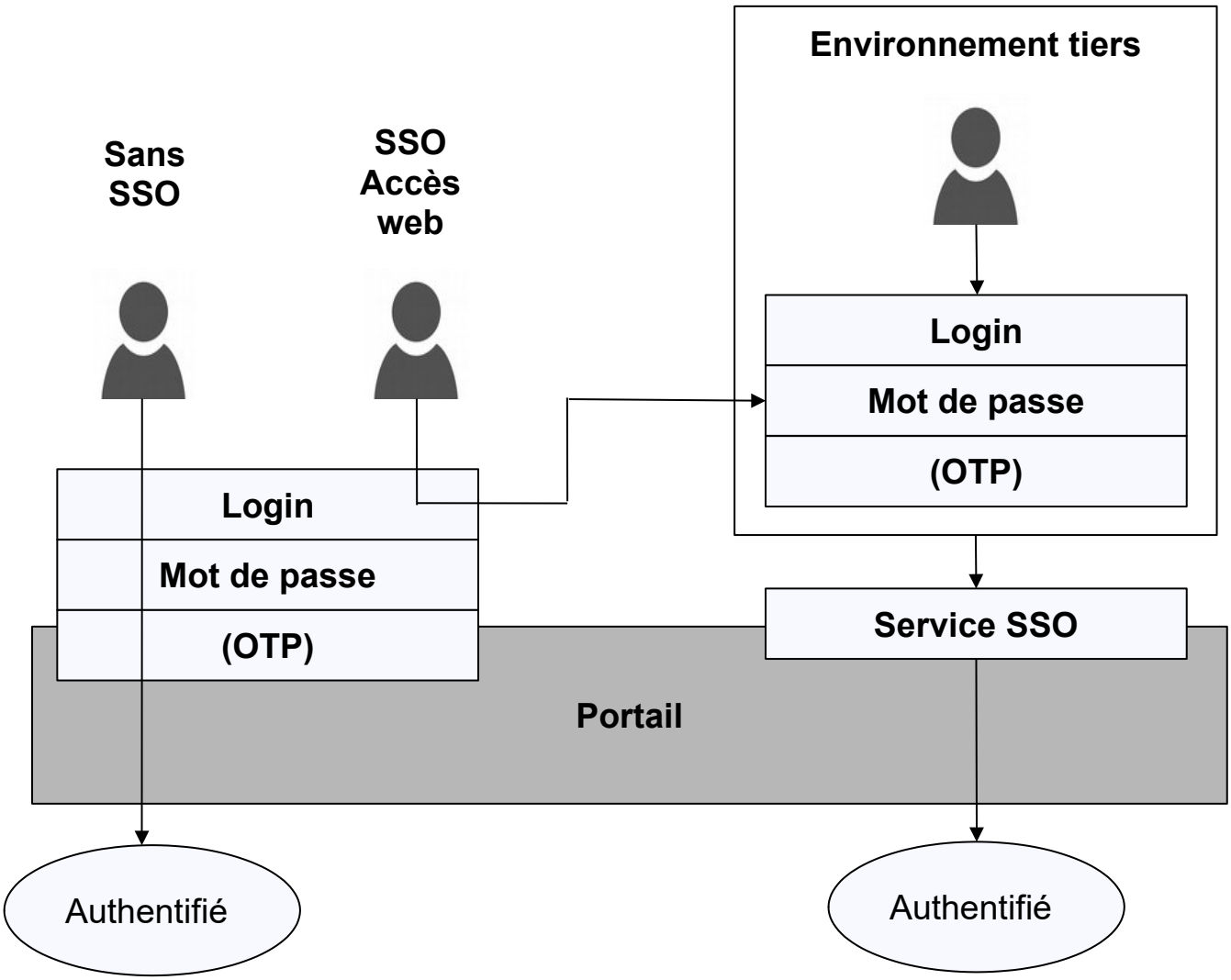
La solution supporte le SSO selon les protocoles SAML V2, Open ID et CAS. Elle dispose des interfaces de paramétrage du service SSO.

La solution peut supporter plusieurs protocoles dans la même organisation pour plusieurs fournisseurs d'identité interopérables en SSO.

La solution identifie l'IdP d'un utilisateur selon son domaine e-mail.

La solution supporte un accès utilisateur bidirectionnel :

- authentification préalable dans l'environnement de l'organisation ou d'un tiers puis authentification automatique à la solution ;
- identification par l'utilisateur dans la solution (par exemple depuis un intranet ou internet), routage vers le dispositif d'authentification de l'organisation puis authentification automatique à la solution



2.3.5. Provisionnement[1] automatisé des utilisateurs

Le provisioning des utilisateurs permet de synchroniser l'annuaire d'un IdP et l'annuaire de la solution.

Les transactions liées au provisionning sont :

- création d'un utilisateur,
- modification d'un utilisateur (informations, droits),
- désactivation d'un utilisateur.

La solution propose ces fonctions en tant qu'interface de programmation applicative (API REST) nécessitant un projet d'interfaçage entre la solution et l'IdP.

Le provisioning peut intégrer ou ne pas intégrer le portage des droits :

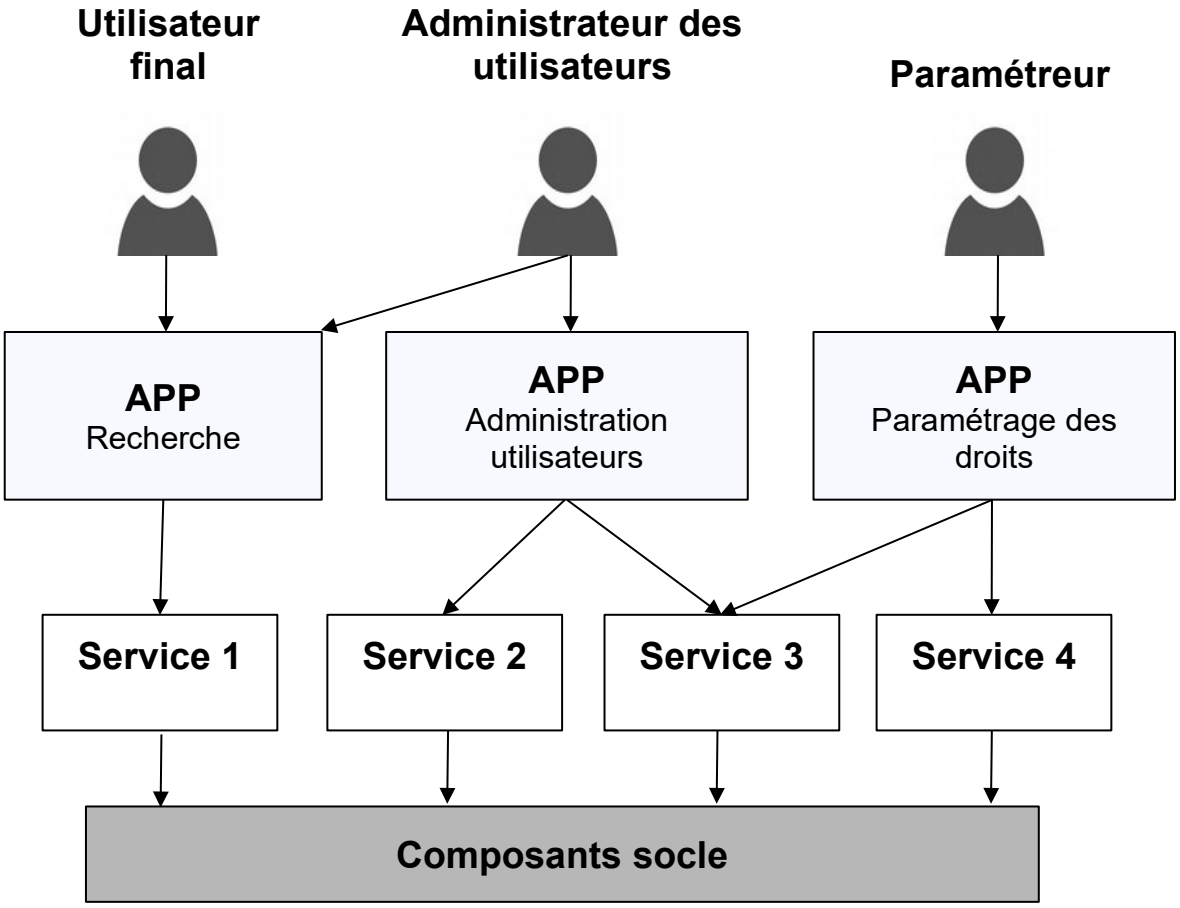
1 Le ***provisionnement*** - calque français du mot ***provisioning***, mot anglais désignant l'approvisionnement - est un terme utilisé dans le monde de l'informatique, désignant l'**allocation automatique de ressources**. Page Wikipédia consultée le 09/03/2021

- Si le provisionning supporte le partage des droits dans la solution, aucune intervention d'administration n'est nécessaire
- Si le provisionning fournit uniquement l'identité et les informations utilisateur, il sera nécessaire qu'un administrateur affecte les droits pour chaque création d'utilisateur et dispose d'un processus organisationnel pour modifier les droits en cas modification des fonctions de l'utilisateur.

Le provisioning est généralement associé au SSO. Il est cependant possible d'activer le SSO sans provisioning. Un processus organisation devra être mis en œuvre pour créer et modifier les utilisateurs dans la solution.
Le lien d'identification entre l'IdP et la solution sera l'adresse e-mail par défaut. Il est possible d'associer un identifiant technique d'utilisateur fourni par l'IdP.

2.4 APP

Une APP (APPlication) est une interface utilisateur (User Interface ou UI) dont le périmètre est le traitement d'un objet métier (utilisateur, profil, document, organisation…). Il est nécessaire de paramétrer les accès aux APP selon le besoin lié à l'utilisation de l'objet métier.



Une APP communique avec un ensemble de services dits « back-office » exposés sous forme d'API dans le domaine réseau des APP. Les services communiquent avec les composants socles (Base de données, moteur de recherche…).

Cette architecture modulaire en APP permet de gérer finement les droits dans la solution et prévient le risque d'élévation de privilèges.

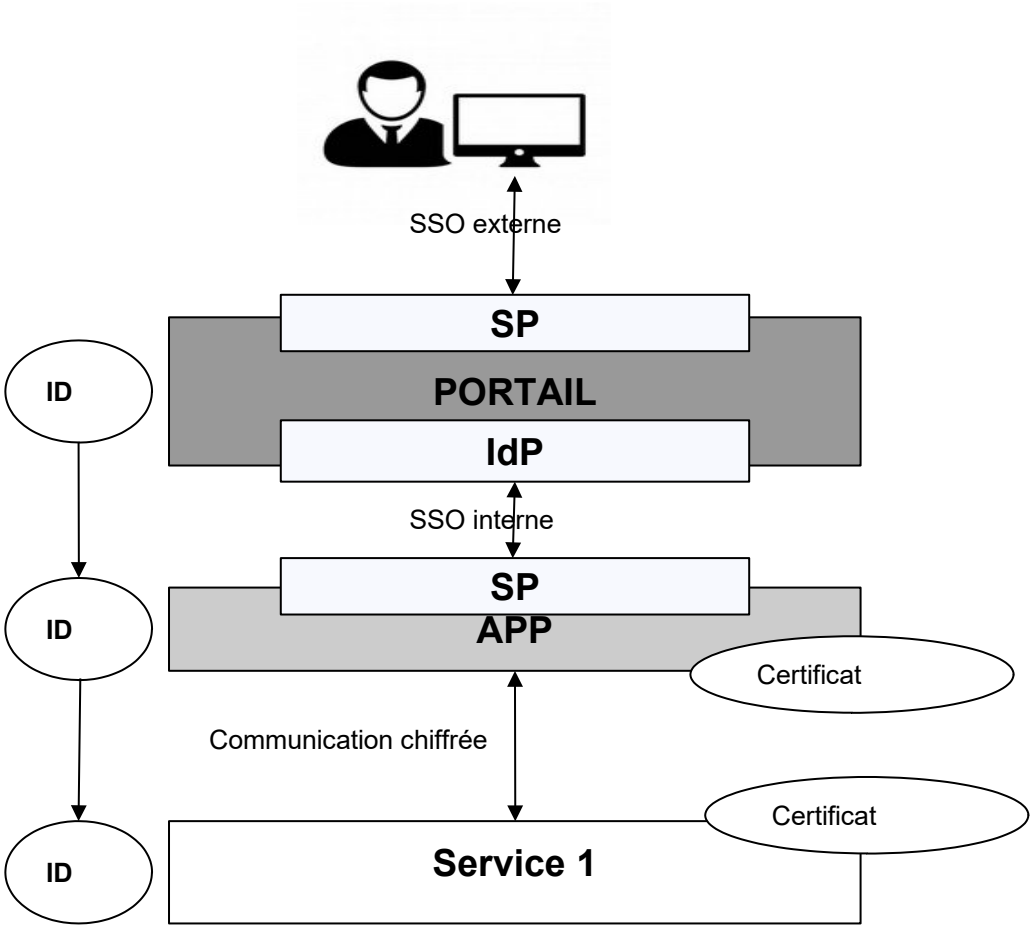
L'ensemble des communications entre les postes utilisateurs, les APPs, les services et les composants socles sont chiffrées. Chaque entité dispose de certificats.

L'imputabilité des transactions, notamment celles générées par une personne dans une APP est assurée par une communication de l'identifiant technique de l'utilisateur dans les communications avec les composants techniques sous-jacents.

Authentification à une APP

Chaque utilisateur préalablement authentifié dans le portail est automatiquement authentifié en SSO dans une APP :

- Le portail est alors un fournisseur d'identité interne à la solution (IdP)
- L'APP est un fournisseur de service



L'authentification ouvre une session pour l'utilisateur. Le token de session est propagé dans les APPs utilisées et dans les services sous-jacents. La propagation du token permet d'identifier quel utilisateur a initié la transaction entre une APP et un service sous-jacent.

Chaque APP et chaque service dispose d'un certificat afin de s'authentifier mutuellement à l'initialisation d'une communication et d'opérer le chiffrement des transactions.

Le service SSO interne, en tant que service, dispose également de deux certificats :

- celui du fournisseur d'identité interne (IdP) : le portail ;
- celui de chaque APP en tant que fournisseur de service (Service Provider ou SP) afin de s'identifier et de chiffrer les assertions d'authentification.

2.5 Gestion des profils de droits et des contrats

Ce chapitre présente les concepts de gestion des droits dans la solution.

Les droits concernent les personnes et les composants techniques :

- un profil de droit est affecté à une personne ;
- un contrat et un fichier technique sont affectés à un composant technique.

2.5.1. Profil de droits par défaut

Un profil de droit associe le privilège d'usage des fonctions de l'APP et autorise l'accès à un périmètre d'objets métiers gérés dans l'APP.

Profil de droit	
Privilège d'usage de fonctions SI (Rôle)	Habilitation d'accès à un périmètre de donnée

Un utilisateur doit disposer d'un profil pour s'authentifier à l'APP. S'il ne dispose pas de profil, l'APP n'est pas visible dans le portail pour l'utilisateur.

Un seul profil est attribuable à un utilisateur pour chaque APP de la solution. Ceci permet d'éviter d'éventuels conflits entre des profils de droits concurrents.

2.5.2. Profil de droits par défaut

Chaque APP dispose d'un profil de droits par défaut permettant l'accès à l'ensemble des objets

métiers et à toutes les fonctions de l'application.

2.5.3. Profils de droit spécifiques

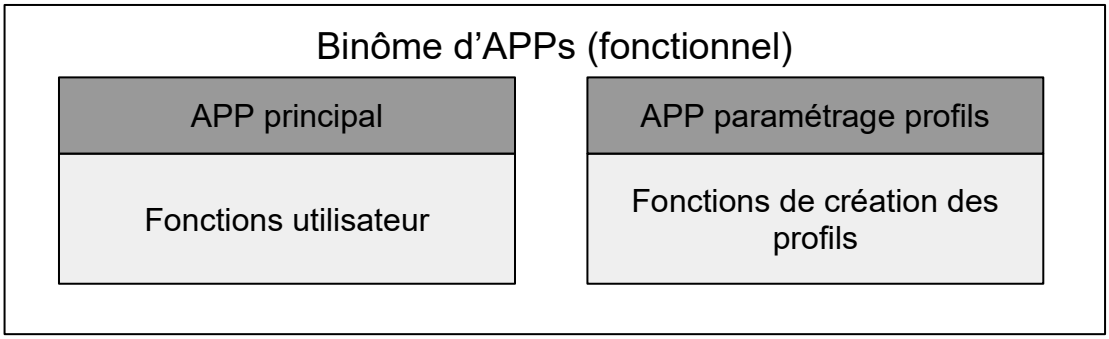
Lorsqu'il est nécessaire de restreindre les droits d'un utilisateur dans une APP, un profil spécifique est créé. Il permet :

- de restreindre l'usage de certaines fonctions (ex : créer, modifier, supprimer) ;
- de limiter l'accès à un périmètre de données (population d'utilisateurs, coffre, collection documentaire, type de bordereaux...)

Dans certains cas, plusieurs profils de droit peuvent être configurés en standard dans la solution pour chaque APP. Ces profils préconfigurés ne sont pas modifiables.

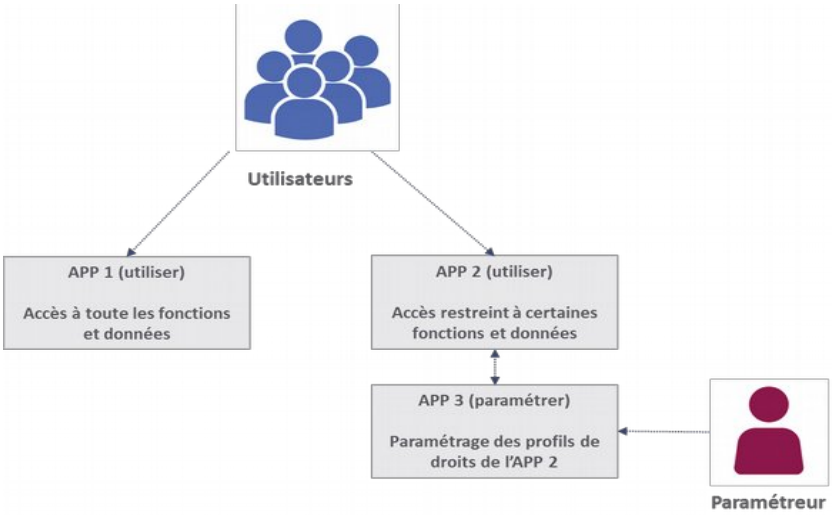
2.5.4. APP de paramétrage de profils de droits

Lorsqu'il est nécessaire de permettre à un paramétreur de créer ou modifier un profil de droit spécifique via les interfaces, une APP de paramétrage de profil spécifique est développée.



Les APP de paramétrage de profils de droit permettent de gérer le référentiel des profils de droits de la solution. Chaque organisation dispose de son propre référentiel.

En synthèse, la solution permet aux utilisateurs d'une organisation d'accéder à un ensemble d'APPs s'ils disposent d'un profil. S'il est nécessaire de paramétrer des profils spécifiques, un utilisateur disposant d'un profil à une APP de paramétrage pourra les configurer.



2.5.5. Option de hiérarchisation des profils

La solution propose en option une fonction de hiérarchisation des profils qui permet :

- de limiter l'attribution de profils à une portée d'utilisateurs ;
- d'adapter la séparation des rôles : les profils sont attribuables uniquement :
  - dans la portée de l'administrateur,
  - à des hiérarchies de droit inférieures à la sienne.

Exemple :

- Un administrateur peut affecter un profil à des utilisateurs mais ne peut pas créer ou modifier un autre administrateur.
- Un administrateur de catégorie RH peut affecter :
  - des profils de portée RH,
  - des profils de portée inférieure à RH, par exemple RH Paie.

Le nombre de niveaux de portée n'est pas limité par la solution.
Si l'option de hiérarchisation des profils est utilisée, un groupe de profil appartient à un niveau et tous les profils contenus sont du même niveau ou de niveau inférieur.

2.5.6. Groupes de profils

Un utilisateur devant accéder à plusieurs APP doit disposer d'autant de profils.

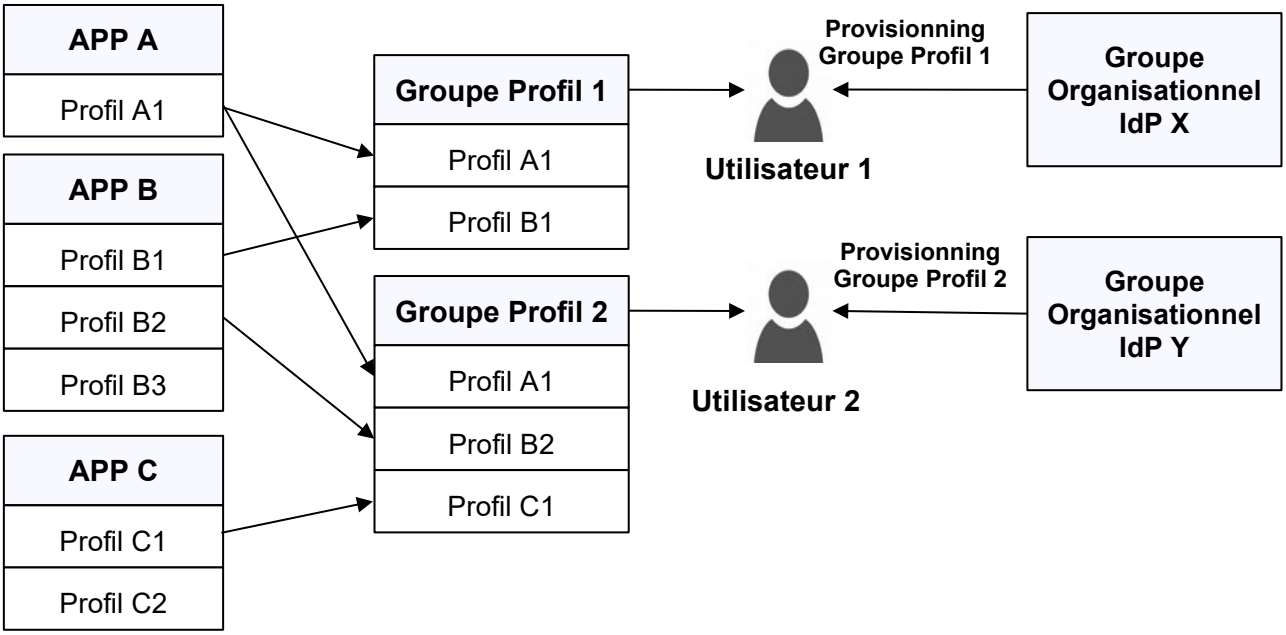
Pour les APP « documentaires » (ex : dépôt et suivi des versements, recherche et consultation des archives, référentiels métiers…), les profils sont liés à des coffres (tenants Vitam) de l'organisation. Un utilisateur devant accéder à plusieurs coffres disposera d'autant de profils.

La solution dispose d'une fonction de regroupement de profils qui permet :

- de simplifier l'administration des utilisateurs : un groupe de profil unique est affecté à un

utilisateur,

- d'automatiser simplement le provisionning des utilisateurs.



Au même titre qu'un utilisateur ne peut disposer que d'un profil dans chaque APP, il est affecté à un groupe de profil unique.

En cas d'interfaçage avec un service de provisioning automatisé, le fournisseur d'identité doit fournir le groupe de profil de l'utilisateur afin de lui octroyer automatiquement ses droits. Ce groupe de profil peut être associé à un groupe organisationnel de l'annuaire tiers.

Si l'option de hiérarchisation des profils est utilisée, un groupe de profil appartient à un niveau et tous les profils contenus sont du même niveau ou de niveau inférieur.
Seul un administrateur affecté à un groupe de profil de même niveau ou de niveau supérieur peut attribuer à des utilisateurs un groupe de même niveau ou de niveau inférieur.

2.6 Cloisonnement

La solution est nativement conçue pour une exploitation d'une instance mutualisée multi-tenant par un opérateur d'archivage en mode SaaS (public ou privé) devant gérer plusieurs organisations dans la même instance de la solution.

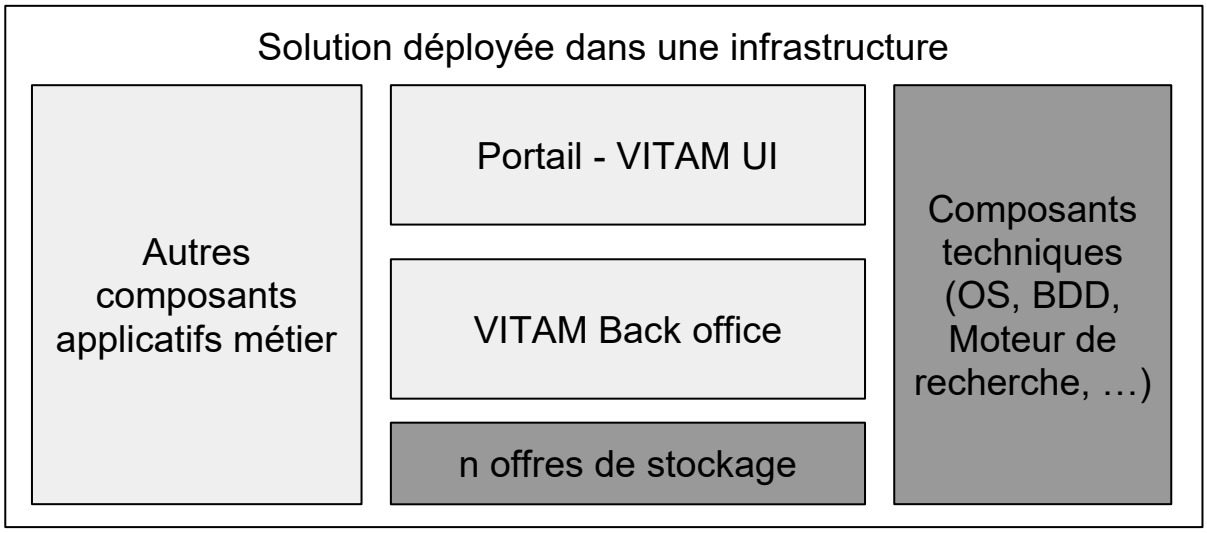
Chaque organisation peut exploiter :

- un ou plusieurs tenants de données Vitam pour les fonctions du système d'archivage électronique ;

- l'accès à d'autres applicatifs que le SAE (parapheur, GED…).

2.6.1. Instance

La solution est une agrégation de composants interfacés qui sont opérés dans une infrastructure technique :



Une instance produit est caractérisée par le déploiement de l'ensemble des applicatifs dans ses environnements, disposés sur au moins deux data centres. Il s'agit des environnements :

- de production ;
- de pré-production ;
- de recette et/ ou qualification ;
- ...

Le nombre de déploiements dépend de l'architecture mise en œuvre par le projet d'implémentation.

Par exemple une instance peut être composée de 8 déploiements :

- 3 environnements de production, un par data-centre ;
- 3 environnements de pré-production, un par data-centre ;
- 1 environnement de qualification en version n et un autre en version n+1 (prochain déploiement).

Selon le niveau de cloisonnement souhaité et le besoin de capacité de l'instance, les environnements peuvent être exploités :

- sur une infrastructure matérielle dédiée,
- sur une infrastructure mutualisée de type cloud privé ou public.

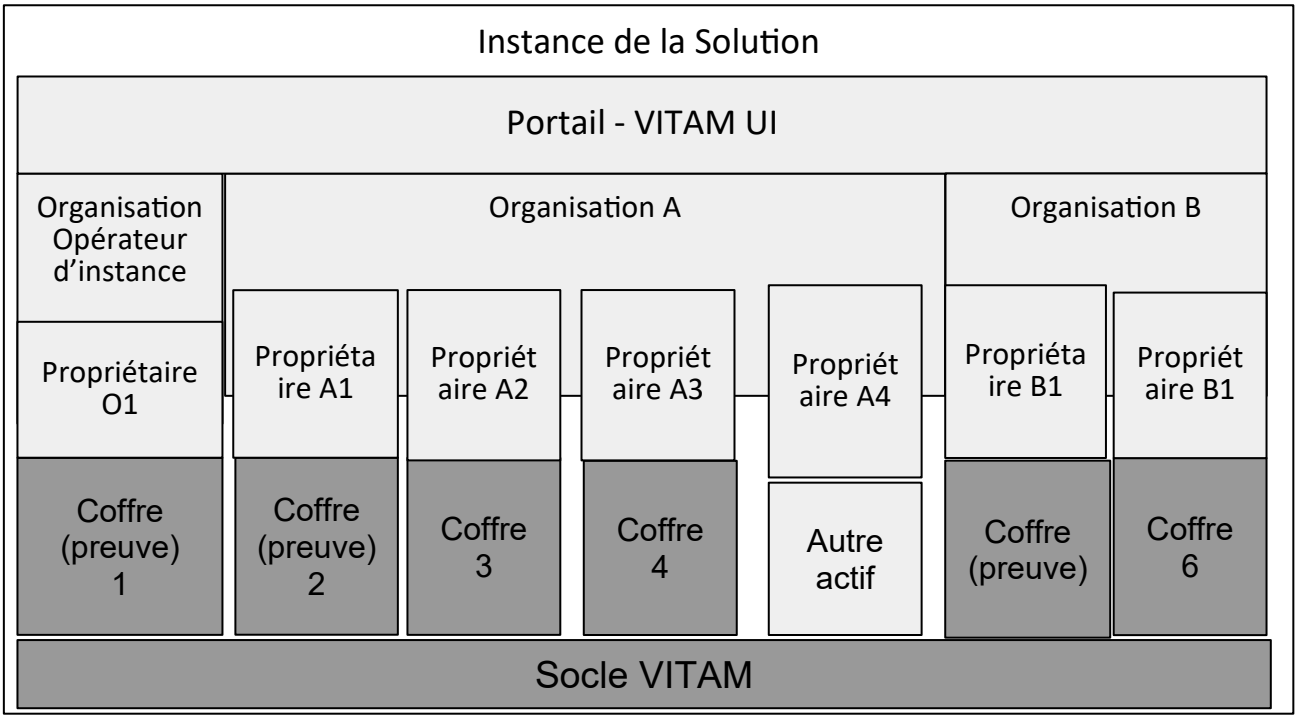
Les offres de stockage peuvent également être dédiées à chaque environnement ou mutualisées

avec d'autres actifs.
Un environnement peut exploiter une offre de stockage opérée dans un autre environnement.

La mise en œuvre d'une instance nécessite une étude d'architecture préalable pour chaque projet d'implémentation.

2.6.2. Organisation, propriétaires et coffres (tenants)

Le cloisonnement de la solution est illustré dans le schéma suivant :



La solution est dite multi-multi-tenant pour cloisonner deux types d'objets « métiers » :

- les objets métier documentaires via le cloisonnement de Vitam en tenants,
- les objets métiers « Organisation » et « Propriétaire » permettant de cloisonner les « utilisateurs » via le cloisonnement VitamUI.

Un utilisateur d'une organisation peut être habilité à accéder à plusieurs tenants de l'organisation.
Le concept utilisateur de VitamUI est donc « cross tenant ».

2.6.3. Socle Vitam et tenants

Le socle Vitam est nativement multi-tenant.
Un tenant Vitam permet de cloisonner l'ensemble des données :

- unités archivistiques (AU),
- indexs Elastic Search,
- logs,

- journaux chaînés.

Vitam dispose nativement d'un ensemble de fonctions d'usage et de paramétrage permettant de tester le socle back-office. L'IHM dite de démonstration ne permet pas de filtrer les accès humains sur un tenant.

Les accès aux fonctions du socle Vitam sont accessibles via un ensemble d'API disposants de droits applicatifs spécifiques

2.6.4. Socle Vitam et VitamUI

VitamUI « Portail » a pour objectif de gérer les accès et les droits d'utilisateurs humains pour des interfaces utilisateurs (ou User Interface, UI). Les UI disposent des droits applicatifs pour accéder aux fonctions du socle VitamUI.

Afin de permettre une exploitation mutualisée de la solution pour plusieurs organisations complexes (holding, administration) dans la même instance, la solution augmente la capacité de cloisonnement de Vitam en permettant :

- d'affecter des tenants Vitam à des organisations,
- de gérer les accès à d'autres actifs indépendants de Vitam (GED, parapheur…).

2.6.5. Organisation

Dans le cas d'usage d'une instance SaaS mutualisée, il sera possible de réaliser des organisations de l'instance adaptées aux besoins de segmentation des rôles et des responsabilités. Par exemple :

- plusieurs organisations peuvent être gérées dans un seul tenant (par exemple un ministère et des services déconcentrés) si le service d'archives est commun à ces organisations. Les habilitations pourront reposer sur les arbres de positionnement du tenant ;
- chaque organisation (ministères, opérateurs…) dispose d'un tenant pour permettre de définir des modalités d'accès individualisées par tenant.

Deux types d'organisation sont configurés dans la solution :

- organisation de l'opérateur d'instance,
- organisation utilisatrice.

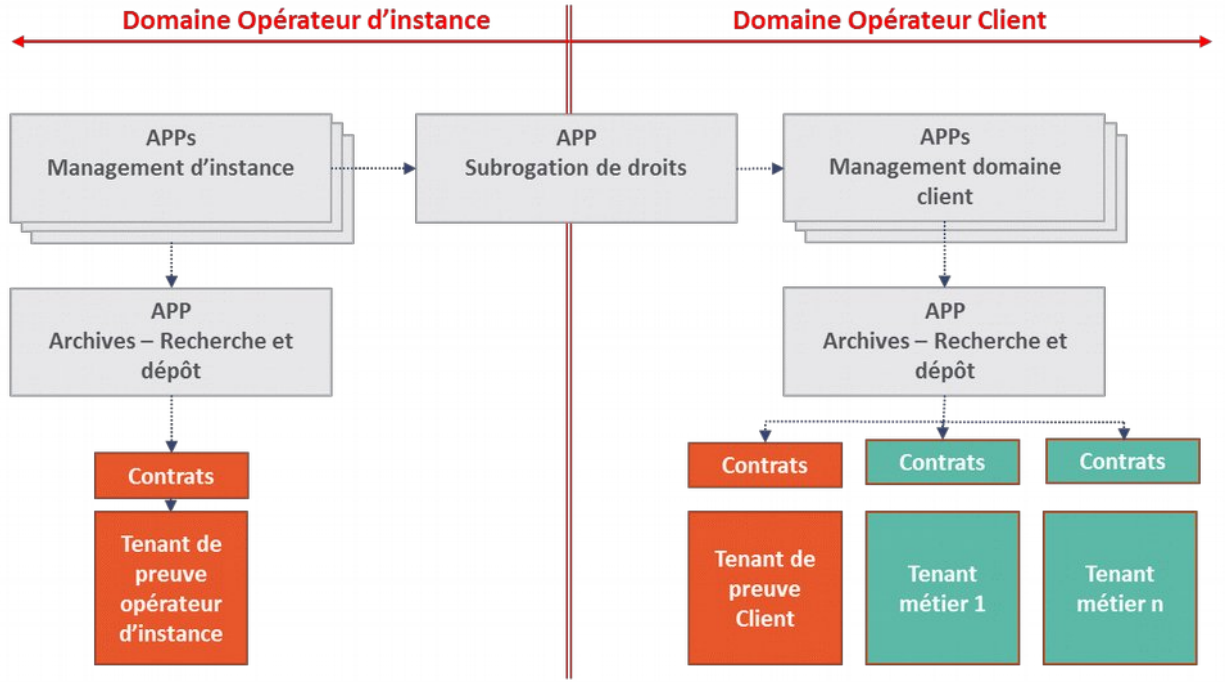
L'organisation de l'opérateur d'instance dispose des fonctions de cloisonnement de l'instance ainsi qu'une certaines fonctions à haut privilège :

- création d'une organisation et affectations de tenants,
- paramétrage de la sécurité d'authentification des organisations (SSO, …),
- paramétrage des authentifications de connecteurs.

2.7 Administration d'instance et subrogation

L'architecture applicative modulaire en APP de VitamUI permet d'affecter des profils de droits selon une logique de séparation des rôles pour les utilisateurs d'une organisation ainsi que pour l'opérateur d'archivage.
À cet effet :

- L'opérateur d'archivage ne dispose d'aucune interface d'accès aux données et paramétrages des organisations. L'accès aux APP d'administration et de paramétrage au niveau instance est autorisé. À l'inverse, les utilisateurs des organisations ne peuvent pas accéder aux APP d'administration et paramétrage d'instance.
- Pour un besoin de service, l'opérateur d'archivage peut accéder aux APP de l'organisation uniquement s'il l'autorise via une fonction de subrogation de droits sécurisée et tracée.



Cette organisation permet de concilier un strict respect de la confidentialité des données de l'organisation tout en permettant à l'opérateur d'instance de proposer des services à valeur ajoutée selon des règles prédéfinies.
Les périmètres du service peuvent être très restreints comme très étendus selon le niveau d'autonomie souhaité par chaque organisation.

Le respect de ces principes clé est auditable par l'organisation qui dispose de l'ensemble des traces d'accès dans son domaine directement via les interfaces graphiques et les journaux.

2.7.1. Cloisonnement de l'opérateur d'instance

La solution distingue :

- les organisations, disposant d'un domaine cloisonné,
- l'opérateur d'instance, en tant qu'organisation spécifique ayant accès aux APPs de management d'instance et à ses propres données d'exploitation du système.

Les APP accessibles dans le domaine de l'opérateur d'instance sont déployées dans des zones protégées accessibles uniquement par l'opérateur d'instance.

Les APP accessibles dans les domaines des organisations sont déployées dans l'infrastructure de production dans une zone publique (en SaaS) ou privée (mode hébergé et one premise).

2.7.2. Subrogation de droits

La fonction de subrogation de droits consiste, pour un utilisateur support d'instance, à hériter des profils de droits d'un utilisateur d'une organisation.

L'identité de la personne ayant opéré la subrogation est tracée pour toute transaction réalisée durant la session de subrogation (il ne s'agit pas d'une subrogation d'identité de l'utilisateur).

Une subrogation peut-être :

- temporaire pour un support à un utilisateur nominatif, dont le profil autorise la subrogation et préalablement acceptée par l'utilisateur.
- permanente, sur des utilisateurs génériques créés dans le domaine de l'organisation pour assurer des prestations d'administration ou de paramétrage pour le compte de tiers lorsque l'organisation l'autorise. Un utilisateur générique ne peut pas s'authentifier dans le système. Il est uniquement subrogeable par le support d'instance lorsque ce droit est ouvert.

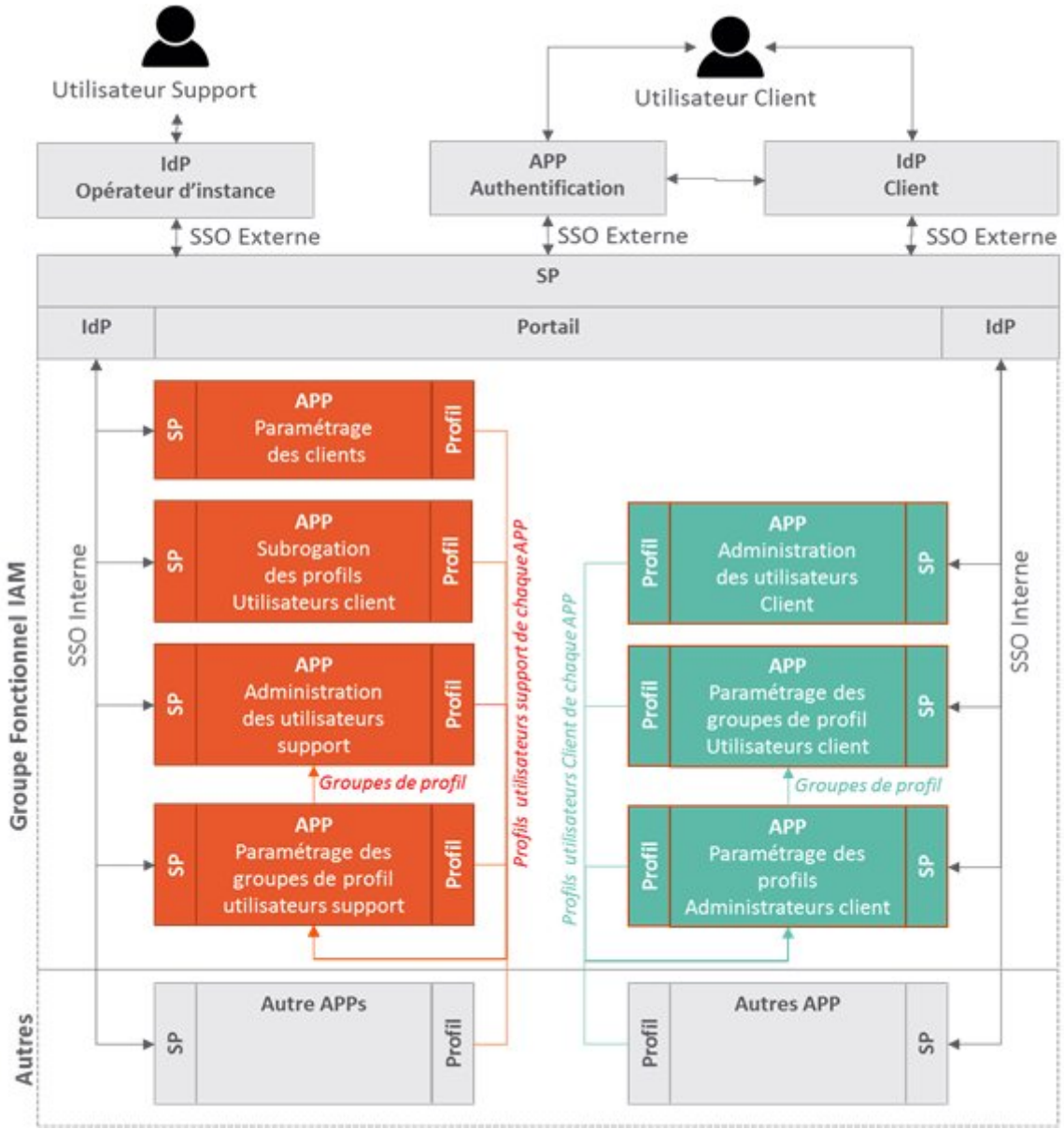
La politique de subrogation est paramétrable de manière à :

- interdire la subrogation
- laisser l'autonomie à un administrateur qui dispose du paramètre, de décider s'il autorise ou interdit la subrogation d'un utilisateur nominatif et gérer les droits de subrogation sur les utilisateurs génériques.

3. Cartographie des APPs portail

3.1 Architecture fonctionnelle du Portail

Le schéma d'architecture fonctionnel de VitamUI IAM est le suivant :



*SP : Service Provider - IdP : Identity Provider

3.2 Description des APPs du domaine fonctionnel Portail

APP	Fonction	Portée
VitamUI IAM et APP d'authentification	Le module technique de fédération d'identité permet d'authentifier un utilisateur amont de l'écosystème (SSO externe) et dans l'écosystème (SSO interne). Si le système n'est pas interfacé, une APP d'authentification est activée : login, mot de passe et OTP en option.	Transverse
Portail	Le portail permet à un utilisateur de naviguer entre les différentes APP autorisées. Le portail contient une APP « Mon compte » ainsi que les modules d'assistance.	Transverse
APP de paramétrage des organisations et des tenants	Cette APP permet de créer une organisation et d'y affecter des tenants dans VitamUI	Opérateur d'instance
APP de paramétrage des groupes de profil	Chaque APP intégrée dans l'écosystème dispose d'un ou plusieurs profils d'autorisations. Cette APP permet de regrouper les profils afin de simplifier l'administration des utilisateurs ainsi que le portage des autorisations vers un IDP tiers (provisioning d'utilisateurs automatisé)	Administrateur d'organisation
APP de paramétrage des profils d'administrateurs	Cette APP permet de définir différents profils d'administrateur de l'organisation contenant les droits fonctionnels ainsi que les populations d'utilisateurs administrées.	Administrateur d'organisation
APP d'administration des utilisateurs	Cette APP permet, selon le profil de l'administrateur, de créer, modifier, désactiver et anonymiser un utilisateur.	Administrateur d'organisation
APP de subrogation	Cette APP permet à un utilisateur support d'instance, de subroger les droits d'un utilisateur générique de l'organisation (administration pour compte de tiers) ou d'un utilisateur nominatif, après autorisation de celui-ci.	Opérateur d'instance

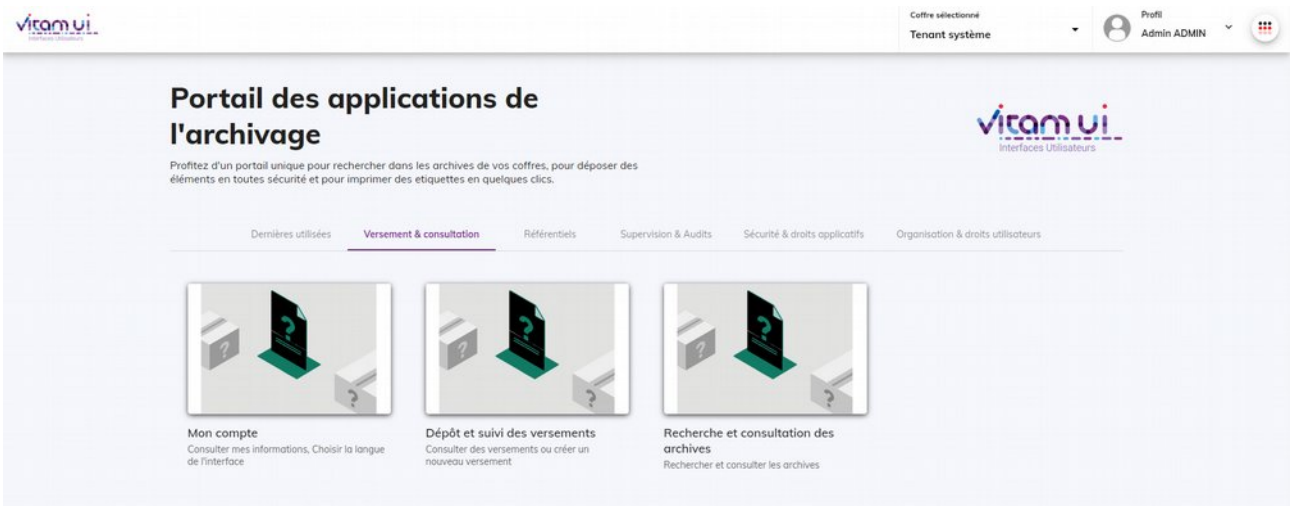
3.3 Home page et launcher

L'APP portail est constituée :

- d'une page d'accueil pour l'utilisateur,
- d'un bandeau de navigation reproduit dans chaque APP pour permettre la navigation entre les APP de l'écosystème,
- de l'accès à l'APP « Mon Compte » où l'utilisateur peut accéder aux paramètres qui lui sont ouvert, selon ses profils d'autorisation.

3.3.1. Page d'accueil

La page d'accueil de l'écosystème reprend les dernières APPs consultées par l'utilisateur via l'onglet « Dernières utilisées ».



À la première connexion, il est demandé à l'utilisateur de choisir son tenant par défaut qui est ensuite enregistré dans la barre de navigation.

3.3.2. Bandeau

Le bandeau est similaire dans chaque APP de l'écosystème. Il permet :

- de naviguer entre les APP via un launcher séparant les APPs par catégories,
- de changer de coffre dans le cas d'un utilisateur ayant accès à plusieurs coffres,
- de se déconnecter de la session,
- d'accéder à l'APP Mon compte.

3.4 UX Design et Customisation

3.4.1. Ergonomie générale de la solution

L'eXperience Utilisateur (UX) de la solution est le résultat d'une étude approfondie des usages.

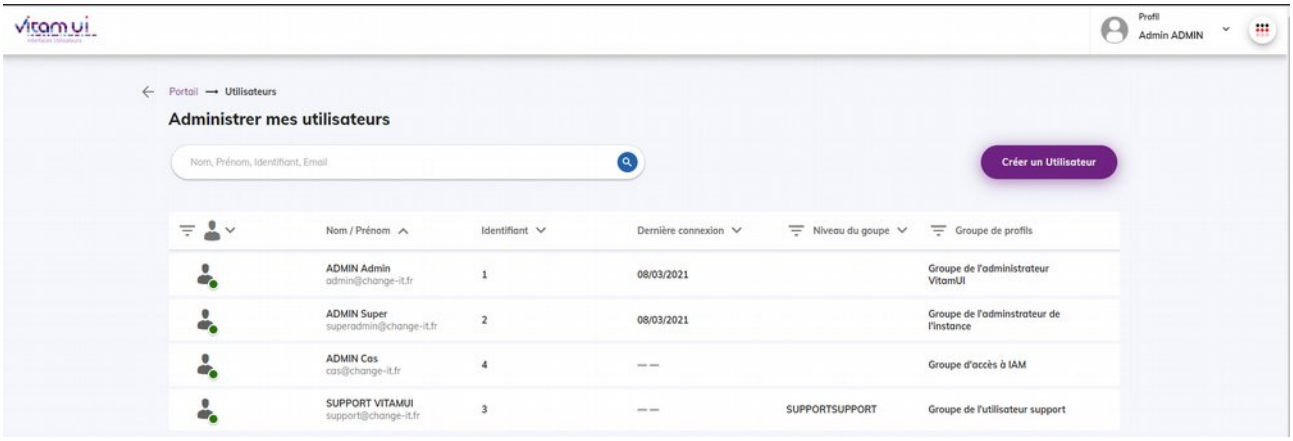
L'ensemble des maquettes de chaque APP de la solution compose le Design System VitamUI, utilisé et maintenu à jour à chaque évolution.

La solution est un écosystème d'APP (APPs d'usage, paramétrage, supervision…). L'ergonomie de chaque APP est homogène et répond aux principes suivants :

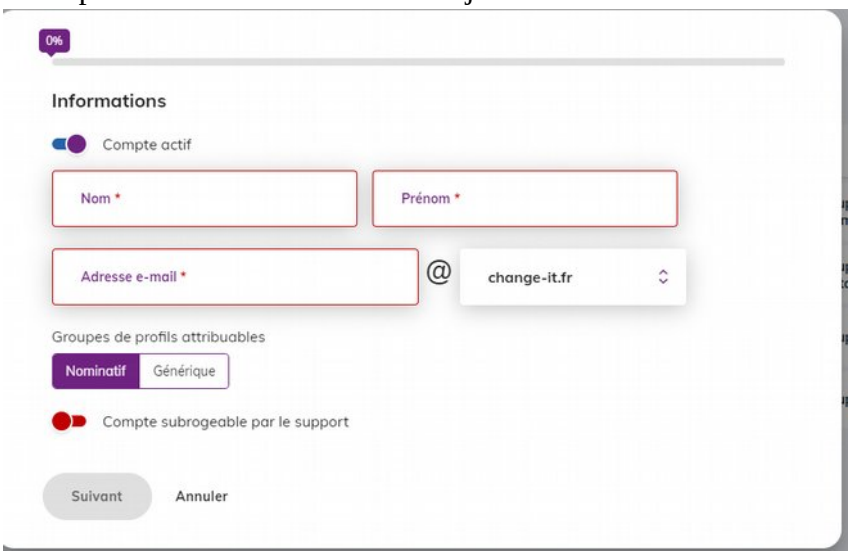
- design épuré avec accès à une liste simple des objets gérés par l'APP,
- bouton de l'action principale de l'APP, généralement la création d'objet permettant de lancer un processus progressif avec assistance de l'utilisateur à l'usage de l'APP,
- accès systématique au détail des opérations réalisés sur l'objet,
- entrée progressive dans les fonctions avancées via des onglets spécifiques à chaque APP.

Exemple de page d'accueil d'une APP d'administration :

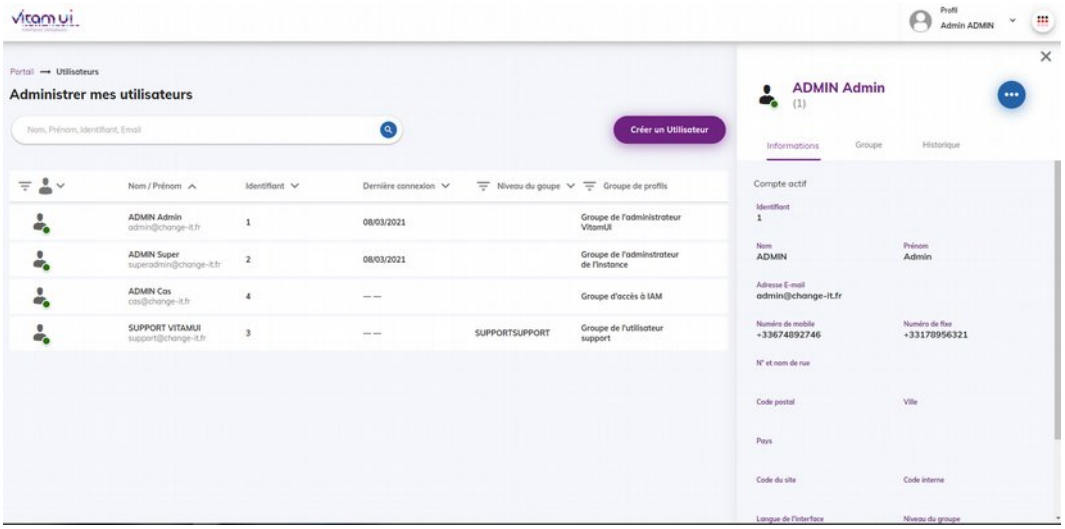
- bandeau de navigation entre les APPs,
- accès à un objet (Organisation, tenant, utilisateur, profil, …) via une recherche générale,
- bouton principal pour l'action de création d'un nouvel objet (wizard).



Exemple de wizard de création d'objet :



Exemple du mode modification et accès aux fonctions spécifiques à l'APP via le bandeau de droite :



3.4.2. Moteur de thème graphique

La solution permet de personnaliser :

- 3 logos par organisation (1 header, 1 footer, 1 portail),
- le titre du portail ainsi que sa description d'accueil,
- le thème graphique de chaque organisation.

L'ensemble des feuilles de styles des interfaces sont variables selon trois couleurs principales :

- couleur principale personnalisable,
- couleur secondaire personnalisable,
- couleur tertiaire personnalisable,
- couleurs de fonds (header, footer, fond du portail).

Les couleurs principales et secondaires sont nuancées automatiquement par calcul dans l'application afin de définir des états particuliers, par exemple l'état d'inactivité d'un bouton d'action.

La personnalisation du thème d'une organisation nécessite de disposer de la charte graphique de l'organisation et de la sélection.