Gestion des habilitations

Date	Version
20/03/2018	2.0 (Release 6)

État du document

◯ En projet ◯ Vérifié ◉ Validé

Maîtrise du document

Responsabilité	Nom	Entité	Date
Rédaction	MVI	Équipe Vitam	12/06/2017
Vérification	Équipe	Équipe Vitam	
Validation	EVA	Équipe Vitam	20/03/2018

Suivi des modifications

Version	Date	Auteur	Modifications
0.1	12/06/2017	MVI	Initialisation
0.2	20/06/2017	EVA	Relecture et corrections
0.3	30/06/2017	MVI	Corrections
0.4	09/08/2017	MVI	Compléments
0.5	24/08/17	MVI	Corrections
0.6	09/10/17	MVI	Compléments
1.0	28/11/2017	MRE	Finalisation du document pour publication de la V1 fonctionnelle
1.1	15/02/2018	MVI	Mise à jour pour tenir compte des fonctionnalités mises en œuvre pendant la *Release 6* : • section 2.1 « Présentation des habilitations » : ajout de la section 2.1.1 sur les certificats et de la section 2.1.2 sur les certificats personnels. • section 2.2 « Formalisation des habilitations » : les intitulés des contextes, contrats d'entrée et contrats d'accès ne sont plus uniques. Ajout de la section 2.2.1 sur les certificats et de la section 2.2.2 sur les certificats personnels. • section 3.1 « Administration des référentiels » : mise à jour de la section 3.1.1 avec prise en compte des certificats et certificat personnel. • section 3.2 « Authentification » : prise en compte des certificats. • section 4.1 « Quand et comment créer une habilitation ? » ; ajout des sections 4.1.3 et 4.1.4 sur quand et comment créer un certificat et un certificat personnel. • section 4.3 « Comment nommer les différentes habilitations ? » : le nom des habilitations n'est plus unique. • section 4.4 « Quel accès aux différentes habilitations ? » : mise à jour des sections 4.4.1 et 4.4.2 pour y inclure les certificats. • section 4.6 « Comment gérer une nouvelle application ? » : nouvelle section. • section 4.7 « Comment modifier les

			habilitations ? » : nouvelle section. • Annexe 1 « Exemples d'habilitations » : ajout d'un exemple de certificat et d'un exemple de certificat personnel. • Annexe 3 « Liste des permissions et privilèges » : annexe ajoutée.
1.2	13/03/2018	JSL	Précision du concept de certificat personnel en lien avec le mécanisme « Personae »
1.3	15/03/2018	ECA	Relecture
2.0	20/03/2018	MRE	Finalisation pour livraison V1 de production

Documents de référence

Document	Date de la version	Remarques
NF Z44022 – MEDONA - Modélisation des données pour l'archivage	18/01/2014	
Standard d'échange de données pour l'archivage – SEDA – v. 2.0	31/12/2015	
Vitam - Structuration des *Submission Information Package* (SIP) – v. 4.0.	20/03/2018	

Licence

Table des matières

1. Résumé

Jusqu'à présent, pour la gestion, la conservation, la préservation et la consultation des archives numériques, les acteurs du secteur public étatique ont utilisé des techniques d'archivage classiques, adaptées aux volumes limités dont la prise en charge leur était proposée. Cette situation évolue désormais rapidement et les acteurs du secteur public étatique doivent se mettre en capacité de traiter les volumes croissants d'archives numériques qui doivent être archivés, grâce à un saut technologique.

1.1 Présentation du programme Vitam

Les trois ministères (Europe et Affaires étrangères, Armées et Culture), combinant légalement mission d'archivage définitif et expertise archivistique associée, ont décidé d'unir leurs efforts, sous le pilotage de la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), pour faire face à ces enjeux. Ils ont décidé de lancer un programme nommé Vitam (Valeurs Immatérielles Transmises aux Archives Pour Mémoire) qui couvre plus précisément les opérations suivantes :

- la conception, la réalisation et la maintenance mutualisées d'une solution logicielle d'archivage électronique de type back-office, permettant la prise en charge, le traitement, la conservation et l'accès aux volumes croissants d'archives (projet de solution logicielle Vitam) ;
- l'intégration par chacun des trois ministères porteurs du Programme de la solution logicielle dans sa plate-forme d'archivage. Ceci implique l'adaptation ou le remplacement des applications métiers existantes des services d'archives pour unifier la gestion et l'accès aux archives, la reprise des données archivées depuis le début des années 1980, la réalisation d'interfaces entre les applications productrices d'archives et la plate-forme d'archivage (projets SAPHIR au MEAE, ADAMANT au MC et ArchiPél au MA) ;
- le développement, par un maximum d'acteurs de la sphère publique, de politiques et de plates-formes d'archivage utilisant la solution logicielle (projet Ad-Essor).

La solution logicielle Vitam est développée en logiciel libre et recourt aux technologies innovantes du Big Data, seules à même de relever le défi de l'archivage du nombre d'objets numériques qui seront produits ces prochaines années par les administrations de l'État. Afin de s'assurer de la qualité du logiciel livré et de limiter les dérives calendaires de réalisation, le projet est mené selon une conduite de projet Agile. Cette méthode dite « itérative », « incrémentale » et « adaptative » opère par successions de cycles réguliers et fréquents de développements-tests-corrections-intégration. Elle associe les utilisateurs tout au long des développements en leur faisant tester les éléments logiciels produits et surtout en leur demandant un avis sur la qualité des résultats obtenus. Ces contrôles réguliers permettent d'éviter de mauvaises surprises lors de la livraison finale de la solution logicielle en corrigeant au fur et à mesure d'éventuels dysfonctionnements.

Le programme Vitam bénéficie du soutien du Commissariat général à l'investissement dans le cadre de l'action : « Transition numérique de l'État et modernisation de l'action publique » du Programme d'investissement d'avenir. Il a été lancé officiellement le 9 mars 2015, suite à la signature de deux conventions, la première entre les ministères porteurs et les services du Premier ministre, pilote du programme au travers de la DINSIC, et la seconde entre les services du Premier ministre et la Caisse des dépôts et consignations, relative à la gestion des crédits attribués au titre du Programme d'investissements d'avenir.

1.2 Présentation du document

Le document présentate les fonctionnalités associées à la gestion et à l'utilisation des habilitations dans la solution logicielle Vitam.

Il s'articule autour des axes suivants :

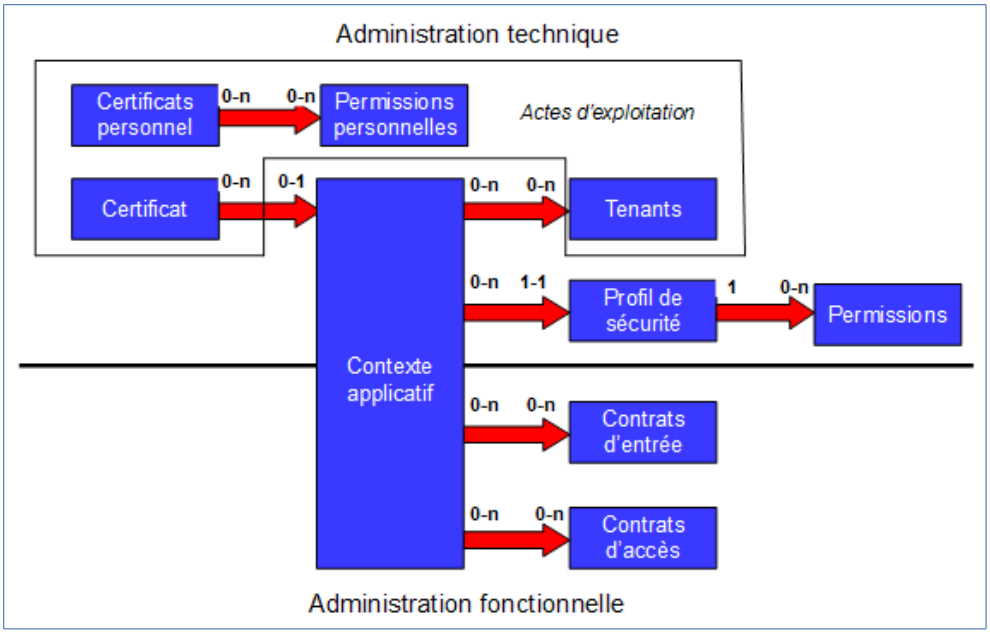
- une présentation des différentes habilitations : contexte applicatif, contrat d'entrée, contrat d'accès, profils de sécurité, et de la manière dont le Standard d'échanges de données pour l'archivage (SEDA) et le modèle de données de la solution logicielle Vitam sont utilisés pour les formaliser ;
- une présentation des mécanismes mis en œuvre dans la solution logicielle Vitam pour gérer ces habilitations ;
- des recommandations aux ministères porteurs, partenaires et utilisateurs de la solution logicielle Vitam sur la manière d'utiliser les fonctionnalités associées à ces habilitations.

Le présent document décrit les fonctionnalités qui seront offertes par la première version de production de la solution logicielle Vitam au terme de la *release 6* (mars 2018). Il a vocation a être amendé, complété et enrichi au fur et à mesure de la réalisation de la solution logicielle Vitam et des retours et commentaires formulés par les ministères porteurs et les partenaires du programme.

2. Présentation des habilitations

2.1. Description

Les habilitations sont l'ensemble des droits et permissions attribués par la solution logicielle Vitam à une application externe et permettant à cette dernière d'accéder aux différents services proposés par la solution logicielle Vitam.



La solution logicielle Vitam met à disposition un ensemble d'outils permettant de gérer les habilitations :

- les certificats applicatifs et les certificats personnels ;
- les contextes applicatifs, les contrats d'entrée, les contrats d'accès et les profils de sécurité.

2.1.1. Certificat applicatif

Le certificat applicatif correspond à une carte d'identité numérique. Il permet d'**identifier et d'authentifier une application** souhaitant accéder aux services de la solution logicielle Vitam.

Pour ce faire, il doit être obligatoirement :

- déclaré dans la solution logicielle Vitam ;
- associé à au moins un contexte applicatif.

2.1.2. Certificat personnel

Le certificat personnel correspond à un certificat propre à une **personne physique** utilisatrice en particulier de l'application souhaitant accéder aux services de la solution logicielle Vitam.

Le certificat personnel ne se substitue pas au certificat applicatif qui authentifie une application, et il sert **juste à identifier et non à authentifier** qui se connecte derrière une application. Le principe de délégation de la phase d'authentification des utilisateurs humains par les front-offices est conservé même dans ce cas, et ce certificat est juste transmis par le front-office dans les appels REST. A minima Vitam vérifie que ce certificat est présent dans la liste des certificats connus.

Son utilisation répond à un besoin de sécurité supplémentaire, associé aux fonctions d'administration avancées ou considérées comme sensibles. L'accès à certaines fonctions (EndPoints) est soumis d'une part à l'autorisation de l'application par son contexte applicatif et d'autre part à la présence d'un certificat personnel connu pour identification de l'utilisateur.

2.1.3. Profil de sécurité

Pour un contexte applicatif donné, le profil de sécurité formalise les privilèges ou droits octroyés à un service externe par la solution logicielle Vitam, et par conséquent les points d'accès (EndPoints) par lesquels ce service, une fois authentifié, pourra transmettre des requêtes à la solution logicielle Vitam.

Un profil de sécurité applicatif détermine les droits suivants :

- soit un accès à tous les services proposés par la solution logicielle Vitam ;
- soit une liste de services définis auxquels le profil de sécurité donne accès.

2.1.4. Contexte applicatif

Le contexte applicatif formalise les interactions entre un service externe et la solution logicielle Vitam. Il permet notamment d'authentifier une application et de lui affecter des droits dans la solution logicielle Vitam.

Afin qu'une application externe puisse utiliser les services fournis par la solution logicielle Vitam, son contexte applicatif doit être associé à :

- 1 à n tenant(s) ;
- 0 à n contrat(s) d'entrées, selon que l'application doit réaliser ou non des entrées ;
- 0 à n contrat(s) d'accès, selon que l'application doit accéder ou non à la solution logicielle Vitam ;
- 1 profil de sécurité.

Un paramètre permet de désactiver ce contrôle sur les tenants et les contrats : le contexte applicatif permet alors à l'application externe d'accéder à l'ensemble des services mis à disposition par la solution logicielle Vitam.

2.1.5. Contrat d'entrée

Le contrat d'entrée formalise les interactions correspondant à des transferts d'archives entre un fournisseur d'archives ou service producteur au sens de la norme NF Z44-022, son opérateur ou service versant au sens de la norme NF Z44-022 et la solution logicielle Vitam

ou service d'archives au sens de la norme NF Z44-022.

Il détermine :

- le tenant à utiliser, obligatoirement déclaré et correspondant au tenant sur lequel a été créé le contrat ;
- la destination ou point de rattachement des archives versées dans le système (correspond à une unité archivistique dans un plan de classement ou dans un arbre de positionnement - facultatif) ;
- le(s) profil(s) d'archivage attendu(s) pour les transferts d'archives (messages ArchiveTransfer au sens de la norme NF Z44-022) effectués en application de ce contrat (facultatif).

2.1.6. Contrat d'accès

Le contrat d'accès formalise les interactions correspondant à des accès aux fonds et aux archives entre un service externe et la solution logicielle Vitam.

Il détermine les filtres suivants :

- le tenant à utiliser, obligatoirement déclaré et correspondant au tenant sur lequel a été créé le contrat ;
- tous ou 0 à n service(s) producteur(s) ;
- tous ou 0 à n nœud(s) au(x)quel(s) il aura accès ;
- tous ou 0 à n usage(s) au(x)quel(s) il aura accès.

Il permet également d'octroyer des droits de lecture et d'écriture. Les droits d'écriture correspondent, par exemple, aux possibilités de modifier les métadonnées de description et de gestion des unités archivistiques.

2.2. Formalisation des habilitations

2.2.1. Certificat applicatif

Un certificat applicatif doit comporter les éléments suivants[1] :

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id) ;
- identifiant unique du certificat applicatif ou Distinguished Name (SubjectDN - obligatoire) ;
- identifiant signifiant du contexte applicatif associé au certificat applicatif (ContextId - obligatoire) ;
- numéro de série du certificat applicatif (SerialNumber - obligatoire) ;
- identifiant unique ou Distinguished Name de l'autorité de certification (IssuerDN - obligatoire) ;
- clé du certificat applicatif (Certificate – obligatoire).

1 Pour plus d'informations, consulter le document « Modèle de données ». Un exemple de certificat se trouve dans l'annexe 1 du présent document.

2.2.2. Certificat personnel

Un certificat personnel doit comporter les éléments suivants[2] :

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id) ;
- identifiant unique du certificat personnel ou Distinguished Name (SubjectDN - obligatoire) ;
- numéro de série du certificat personnel (SerialNumber - obligatoire) ;
- identifiant unique ou Distinguished Name de l'autorité de certification (IssuerDN - obligatoire) ;
- clé du certificat personnel (Certificate - obligatoire).

Au niveau de la plate-forme un fichier de configuration définit les services qui peuvent être rendus accessibles aux seuls détenteurs d'un certificat personnel.

2.2.3. Profil de sécurité

Le profil de sécurité est modélisé en JSON comme suit[3] :

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id) ;
- identifiant donné au profil de sécurité, généré automatiquement par le système (Identifier). Uniquement généré par la solution logicielle Vitam, cet identifiant se compose du préfixe SEC_PROFILE, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement ;
- nom du profil de sécurité, qui doit être obligatoirement renseigné et unique sur la plateforme (Name) ;
- droit(s) au(x)quel(s) le profil de sécurité donne accès. Il peut s'agir de :
  - tous les accès (FullAccess),
  - une liste de **privilèges ou droits** octroyés, sélectionnés parmi l'ensemble des services proposés par la solution logicielle Vitam (Permissions) au sein d'une liste de permissions. Pour chaque service, cette liste précise le type de service concerné et les droits associés (lecture, écriture, suppression) ;
- version du privilège (_v).

2.2.4. Contexte applicatif

Le contexte applicatif est modélisé en JSON comme suit[4] :

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id) ;
- nom du contexte, qui doit être obligatoirement renseigné sur la plateforme (Name) ;
- identifiant unique donné au contexte (Identifier). S'il est généré par la solution logicielle Vitam, cet identifiant se compose du préfixe CT, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement. Il peut également être généré par

2 Pour plus d'informations, consulter le document « Modèle de données ». Un exemple de certificat personnel se trouve dans l'annexe 1 du présent document.
3 Pour plus d'informations, consulter le document « Modèle de données ». Un exemple de profil de sécurité se trouve dans l'annexe 1 du présent document.
4 Pour plus d'informations, consulter le document « Modèle de données ». Un exemple de contexte applicatif se trouve dans l'annexe 1 du présent document.

l'application à l'origine de sa création ;
- version du contexte (_v) ;
- identifiant du profil de sécurité associé au contexte (SecurityProfile - obligatoire) ;
- contrôle sur les tenants (EnableControl) :
  - si la valeur est true, un contrôle est effectué sur le(s) tenant(s) et contrat(s) défini(s) dans le contexte applicatif quand une application externe accède aux services de la solution logicielle Vitam ;
  - si la valeur est false, aucun contrôle n'est effectué sur le(s) tenant(s) et contrat(s) défini(s) dans le contexte applicatif quand une application externe accède aux services de la solution logicielle Vitam ;
  - si la valeur est null, la solution logicielle Vitam la gère comme la valeur précédente : aucun contrôle n'est effectué sur le(s) tenant(s) et contrat(s) défini(s) dans le contexte applicatif quand une application externe accède aux services de la solution logicielle Vitam ;
- statut « Actif » ou « Inactif » (Status) ;
- date de création du contexte (CreationDate) ;
- dernière date de modification du contexte (LastUpdate).

Un bloc **Permissions** détaille le périmètre du contexte, tenant par tenant. Il comprend :
- le tenant dans lequel vont s'appliquer un ou plusieurs contrats (_tenant) ;
- le(s) identifiant(s) de(s) contrat(s) d'accès appliqué(s) sur le tenant (AccessContracts) ;
- le(s) identifiant(s) de(s) contrat(s) d'entrée appliqué(s) sur le tenant (IngestContracts).

Le contexte applicatif n'est pas déclaré dans le message ArchiveTransfer du SEDA.
En revanche, il est enregistré dans le journal des opérations sous forme d'identifiant de l'opération (agIdApp).

2.2.5. Contrat d'entrée

Le contrat d'entrée est composé en JSON des éléments suivants[5] :
- identifiant unique par tenant, fourni par le système (_id) ;
- identifiant unique donné au contrat, généré automatiquement par le système (Identifier). S'il est généré par la solution logicielle Vitam, cet identifiant se compose du préfixe IC, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement. Il peut également être généré par l'application à l'origine de sa création ;
- tenant dans lequel le contrat s'applique (_tenant) ;
- nom du contrat, qui doit être obligatoirement renseigné sur la plateforme (Name) ;
- description du contrat (Description) ;
- version du contrat (_v) ;
- statut « Actif » ou « Inactif » (Status) ;
- date de création du contrat (CreationDate) ;
- dernière date de modification du contrat (LastUpdate) ;

5 Idem. Un exemple de contrat d'entrée se trouve dans l'annexe 1 du présent document.

- si le contrat est actif, date d'activation du contrat (ActivationDate) ;
- si le contrat est inactif, date de désactivation du contrat (DeactivationDate) ;
- nom du profil d'archivage associé au contrat (ArchiveProfiles - facultatif) ;
- identifiant du nœud auquel on souhaite rattacher les SIP versés (LinkParentId - facultatif).

La solution logicielle Vitam impose de déclarer un contrat d'entrée, au moment de la demande de transfert à un service d'archives (message ArchiveTransfer), dans le bloc ArchivalAgreement.
Par ailleurs, dans le journal des opérations, le contrat d'entrée est désormais enregistré dans le champ rightsStatementId pour toute opération de transfert (INGEST).

2.2.6. Contrats d'accès

Le contrat d'accès est composé des éléments suivants[6] :

- identifiant unique par tenant, fourni par le système (_id) ;
- identifiant unique donné au contrat, généré automatiquement par le système (Identifier). S'il est généré par la solution logicielle Vitam, cet identifiant se compose du préfixe AC, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement. Il peut également être généré par l'application à l'origine de sa création ;
- tenant dans lequel le contrat s'applique (_tenant) ;
- nom du contrat, qui doit être obligatoirement renseigné sur la plateforme (Name) ;
- description du contrat (Description) ;
- version du contrat (_v) ;
- statut « Actif » ou « Inactif » (Status) ;
- date de création du contrat (CreationDate) ;
- dernière date de modification du contrat (LastUpdate) ;
- si le contrat est actif, date d'activation du contrat (ActivationDate) ;
- si le contrat est inactif, date de désactivation du contrat (DeactivationDate) ;
- service(s) producteur(s) associé(s) au contrat et accédant de fait au(x) fonds et archives déclarant ce(s) même(s) service(s) producteur(s). Il peut s'agir de :
  - tous les services producteurs (EveryOriginatingAgency),
  - une sélection de services producteurs (OriginatingAgencies) ;
- usage(s) au(x)quel(s) le contrat donne accès. Il peut s'agir de :
  - tous les usages (EveryDataObjectVersion),
  - une sélection d'usages (DataObjectVersion). Ces usages peuvent être : archives physiques (PhysicalMaster), archives numériques originales (BinaryMaster), copies de diffusion (Dissemination), contenu textuel (TextContent), vignettes (Thumbnail) ;
- identifiant du nœud ou des nœuds au(x)quel(x) on souhaite donner accès (RootUnits) ;

6 Pour plus d'informations, consulter le document « Modèle de données ». Un exemple de contrat d'accès de sécurité se trouve dans l'annexe 1 du présent document.

- droit d’écriture sur les archives (WritingPermission).

Le contrat d’accès n’est actuellement pas déclaré dans le message ArchiveTransfer du SEDA. Par ailleurs, dans le journal des opérations, il est désormais enregistré dans le champ rightsStatementId pour toute opération de mise à jour des métadonnées de description et de gestion des unités archivistiques (UPDATE).

3. Mécanismes mis en œuvre dans la solution logicielle Vitam

La solution logicielle Vitam offre à un service d'archives ou à un service externe plusieurs fonctionnalités lui permettant de gérer les habilitations :

- l'**administration des référentiels** des contextes applicatifs, contrats d'entrée, contrats d'accès et profils de sécurité ;
- une **authentification** au moyen d'un certificat applicatif d'un contexte applicatif ;
- le cas échéant une **identification** de l'utilisateur d'un certificat personnel ;
- en entrée du système, le **contrôle** de l'existence d'un contrat d'entrée et un éventuel **rattachement du SIP** à un arbre de positionnement un plan de classement ou un SIP ;
- en accès, un **filtre** sur les archives autorisées par un contrat d'accès.

3.1. Administration des référentiels

La solution logicielle Vitam intègre un référentiel pour chaque type d'habilitations, administrable par un utilisateur doté des droits adéquats (**administrateur fonctionnel ou technique**).

Les référentiels des contextes applicatifs et des profils de sécurité sont multi-tenants. Ils sont administrables et journalisés depuis le tenant d'administration.

Les référentiels des contrats d'entrée et des contrats d'accès sont propres à chaque tenant de la solution logicielle Vitam.

3.1.1. Import

Dans la solution logicielle Vitam, il est possible d'importer :

- 1 à n contexte(s) applicatif(s),
- 1 à n contrat(s) d'entrée,
- 1 à n contrat(s) d'accès.

Il s'agit d'une opération d'administration, tracée dans le journal des opérations de la solution logicielle Vitam.

L'ajout d'un certificat applicatif, la déclaration d'un certificat personnel ou encore la création d'un profil de sécurité relèvent d'opérations d'administration technique, tracées dans les logs, et s'effectuent au moyen des API.
Il est possible de générer ainsi :

- 1 à n certificat(s) applicatif(s),
- 0 à n certificat(s) personnel(s),
- 1 à n profil(s) de sécurité.

3.1.2 Modification

La modification des champs des contextes applicatifs, contrats d'entrée ou contrats d'accès est possible au moyen des API et de l'IHM standard, contrairement à celle des champs des profils de sécurité qui ne s'effectue qu'au moyen des API.

Cette action provoque la création d'une nouvelle version du contexte, contrat d'entrée, contrat d'accès ou privilège modifié.

Elle fait l'objet d'une journalisation dans le journal des opérations.

3.1.3 Activation / Désactivation

La solution logicielle Vitam permet de rendre actif ou inactif un contexte applicatif, un contrat d'entrée ou un contrat d'accès.
En fonction du statut du contexte applicatif et de celui du contrat d'entrée associé, un versement de SIP sera autorisé ou non :

	Contexte applicatif	**Contrat d'entrée**	**Résultat**
CAS 1	ACTIF	ACTIF	Transfert de SIP dans le système autorisé.
CAS 2	ACTIF	INACTIF	Transfert de SIP dans le système non autorisé.
CAS 3	INACTIF	ACTIF	Transfert de SIP dans le système non autorisé.
CAS 4	INACTIF	INACTIF	Transfert de SIP dans le système non autorisé.

En fonction du statut du contexte applicatif et de celui du contrat d'accès associé, un accès au système sera autorisé ou non :

	Contexte applicatif	**Contrat d'accès**	**Résultat**
CAS 1	ACTIF	ACTIF	Accès au système autorisé.
CAS 2	ACTIF	INACTIF	Accès au système non autorisé.
CAS 3	INACTIF	ACTIF	Accès au système non autorisé.
CAS 4	INACTIF	INACTIF	Accès au système non autorisé.

La modification du statut engendre la mise à jour des champs :

- Date de mise à jour ;
- Date d'activation OU date de désactivation (service non encore implémenté).

3.2. Authentification

Un service externe doit toujours s'authentifier à la solution logicielle Vitam au moyen de son

certificat applicatif qui détermine un contexte applicatif.

La solution logicielle Vitam effectuera les tâches et traitements suivants au niveau de l'API externe :

- **vérification que le certificat applicatif du service externe qui cherche à se connecter à la solution logicielle Vitam dispose d'un contexte applicatif** qui existe bien dans le référentiel des contextes applicatifs et qui est actif ;
- si un certificat personnel a été mis en place, **vérification que le certificat personnel utilisé par le service externe pour se connecter à la solution logicielle Vitam est dans la liste des certificats personnels déclarés** dans la solution logicielle Vitam ;
- **vérification sur le(s) tenant(s) déclaré(s)** dans le contexte applicatif ;
- **vérification de l'existence de(s) contrat(s) d'entrée ou d'accès** déclaré(s) dans le contexte applicatif ;
- **vérification de l'existence du profil de sécurité** déclaré dans le contexte applicatif.

Le contrôle de cohérence entre le(s) contrat(s) d'entrée et le contexte applicatif s'effectuera au niveau de l'API interne, au moment du transfert d'un SIP.

L'authentification est une étape préalable à toute opération d'entrée ou d'accès.
Si un élément fait défaut, le service externe ne pourra pas accéder aux services de la solution logicielle Vitam.

3.3. Entrées

Un SIP doit toujours déclarer un contrat d'entrée.

Dans le cadre du processus d'entrée d'un ensemble d'archives, suite à la réception d'un message ArchiveTransfer du SEDA, la solution logicielle Vitam effectue les tâches et traitements de contrôles internes suivants pour les archives déclarant un contrat d'entrée :

- **authentification** de l'application versante à la solution logicielle Vitam par l'intermédiaire d'un certificat applicatif qui vérifie la validité de son contexte ;
- **vérification que le contrat d'entrée déclaré dans le SIP est conforme au contexte applicatif** qui le déclare dans le référentiel des contextes applicatifs ;
- **vérification que le contrat déclaré dans le SIP (ArchivalAgreement) existe** bien dans le référentiel des contrats d'entrée et est actif ;
- le cas échéant, **vérification que le profil d'archivage déclaré dans le SIP (ArchiveProfile) est conforme au contrat d'entrée** qui le déclare dans le référentiel des contrats d'entrée et est actif.

La solution logicielle Vitam permet également de rattacher des SIP à un arbre de positionnement, un plan de classement ou à un SIP préalablement versé, en déclarant, dans un contrat d'entrée, l'identifiant système (le GUID) de l'unité archivistique auquel le SIP doit être rattaché.

À noter que la déclaration d'un nœud de rattachement dans le contrat d'entrée n'entraîne pas de contrôles supplémentaires sur les nœuds de rattachement contenus dans les bordereaux de

transfert. Ainsi, un bordereau de transfert pourra déclarer un nœud de rattachement positionné à un niveau supérieur de l'arborescence par rapport à celui qui est déclaré dans son contrat. La solution logicielle Vitam n'empêchera pas son import et son rattachement à deux nœuds différents.
Un contrat d'entrée ne donne pas accès au registre des fonds et aux archives. Si le service externe doit verser des archives et y accéder, il doit nécessairement disposer d'un contrat d'entrée et d'un contrat d'accès.

3.4. Accès

Les contrats d'accès permettent à un service externe authentifié d'accéder aux collections suivantes :

- unités archivistiques (collection Unit),
- groupes d'objets (collection ObjectGroup),
- registre des fonds (collection AccessionRegisterSummary et AccessionRegisterDetail).

Un contrat d'accès filtre les réponses envoyées au service externe en fonction de ce qui a été autorisé dans le contrat.

- Un contrat d'accès peut limiter la consultation dans le registre des fonds et les archives au(x) seul(s) producteur(s) qu'il déclare. Ainsi, un service externe ne pourra accéder qu'au(x) fonds et archives du ou des service(s) producteur(s) inscrit(s) dans son contrat d'accès ;
- Il permet aussi de limiter l'accès à certains usages : archives physiques (PhysicalMaster), archives numériques originales (BinaryMaster), copies de diffusion (Dissemination), contenu textuel (TextContent), vignettes (Thumbnail) ;
- Il peut aussi déterminer le(s) nœud(s) ou niveau(x) de l'arborescence à partir du(es)quel(s) un service externe pourra effectuer des recherches ou obtenir des résultats : il peut s'agir de tout ou partie d'un arbre de positionnement, d'un plan de classement ou d'un SIP.

Un contrat d'accès peut octroyer des droits d'écriture et de modification sur :

- les unités archivistiques (collection Unit),
- les groupes d'objets (collection ObjectGroup).

Un contrat d'accès ne permet pas de réaliser des transferts d'archives. Si le service externe doit verser des archives et y accéder, il doit nécessairement disposer d'un contrat d'entrée et d'un contrat d'accès.

4. Conseils de mise en œuvre

À l'issue de cette première phase de réalisation de fonctionnalités concernant les habilitations, l'équipe projet Vitam est en mesure de fournir quelques recommandations de mise en œuvre.

4.1. Quand et comment créer une habilitation ?

4.1.1. Quand et comment créer un certificat applicatif ?

Un service externe souhaitant utiliser les services de la solution logicielle Vitam doit avoir déclaré son certificat applicatif dans la solution logicielle Vitam. Ce certificat doit être associé à un contexte dès la création de celui-ci, sans quoi l'application cherchant à s'authentifier à la solution logicielle Vitam ne pourra accéder à aucun de ses services.
La déclaration d'un certificat applicatif dans la solution logicielle Vitam relève d'une opération d'administration technique.

4.1.2. Quand et comment créer un certificat personnel ?

Un service externe souhaitant utiliser les services de la solution logicielle Vitam peut disposer de certificats personnels pour tracer les actions de certains utilisateurs.
La création d'un certificat personnel et l'attribution des privilèges qui lui sont associés relèvent d'une opération d'administration technique.
Tout comme les droits octroyés par un profil de sécurité, les privilèges accordés par un certificat personnel correspondent aux services proposés par la solution logicielle Vitam (EndPoint). Ils doivent en outre se conformer aux droits définis dans le profil de sécurité du contexte applicatif utilisé.

Il est recommandé de n'utiliser ce type de certificat que pour des utilisateurs en nombre restreint :

- des administrateurs de la solution logicielle Vitam, ayant vocation à accéder à l'ensemble des services mis à disposition par cette dernière ;
- des personnes ayant des droits d'accès à certains services en particulier (on pourrait envisager d'utiliser un certificat personnel dans le cas de la gestion des archives protégées au titre du secret de la défense nationale, sur une instance classifiée).

4.1.3. Quand et comment créer un profil de sécurité ?

Un service externe souhaitant utiliser les services de la solution logicielle Vitam doit disposer d'un profil de sécurité. Ce profil doit être associé à un contexte dès sa création, sans quoi l'application cherchant à s'authentifier à la solution logicielle Vitam ne pourra accéder à aucun de ses services.

La création d'un profil de sécurité et l'attribution des privilèges qui lui sont associés relèvent d'une opération d'administration technique.

Par défaut, la solution logicielle Vitam met à disposition un profil de sécurité donnant accès à l'ensemble de ses services. Ce profil est destiné à être utilisé par un système d'information archivistique (SIA) ou une application ayant des droits d'administration de la solution logicielle Vitam.

4.1.4. Quand et comment créer un contexte applicatif ?

La création du contexte applicatif est un préalable à l'octroi de droits supplémentaires, d'entrée comme d'accès, dans la solution logicielle Vitam :

- une application souhaitant réaliser des entrées ou accéder à des archives doit nécessairement être authentifiée au moyen d'un contexte applicatif déclarant un profil de sécurité ;
- une application souhaitant réaliser des entrées ou accéder à des archives ne peut effectuer ces actions au moyen des seuls contrats, d'entrée comme d'accès.

Dès qu'on souhaite connecter une application à la solution logicielle Vitam, il faut, avant toute chose, l'authentifier au moyen d'un certificat applicatif qui détermine un contexte applicatif, avant de lui associer un profil de sécurité et des contrats, préexistants ou créés à cette occasion.

Pour assurer une étanchéité entre les tenants, il est préconisé d'associer un seul tenant par contexte. De cette manière, le mécanisme d'authentification d'une application externe à un tenant ne permet de verser et d'accéder qu'à ce seul tenant.
Le mécanisme de multi-tenant pour le contexte applicatif est mis en place pour le cas d'un système d'information des archives (SIA) qui devrait pouvoir accéder à plusieurs tenants.

4.1.5. Quand et comment créer un contrat d'entrée ?

Tout SIP qui doit être transféré dans la solution logicielle Vitam doit renseigner un contrat d'entrée dans son bordereau de transfert (ArchivalAgreement), sans quoi son transfert échouera.

De fait, avant tout transfert, il est recommandé de :

- vérifier si le contrat d'entrée déclaré dans le SIP existe dans le système mettant en œuvre la solution logicielle Vitam ;
- créer un nouveau contrat d'entrée s'il n'existe pas ;
- le cas échéant, utiliser un contrat d'entrée préalablement créé, destiné à être utilisé par l'application ;
- vérifier que le contrat d'entrée est bien déclaré dans le contexte de l'application.

Quand on crée un contrat d'entrée déclarant un nœud de rattachement, il faut veiller à ce que le nœud déclaré existe dans la solution logicielle Vitam, sans quoi il ne pourra être enregistré dans le contrat.

4.1.6. Quand et comment créer un contrat d'accès ?

Pour accéder aux données conservées dans la solution logicielle Vitam, un service externe doit obligatoirement disposer d'un contrat d'accès.

Une application ayant des droits d'administration de la solution logicielle Vitam, par exemple un système d'information archivistique (SIA), doit détenir un contrat d'accès lui permettant d'accéder à l'ensemble des fonds conservés dans la solution logicielle Vitam (EveryOriginatingAgency = true).

Pour une application transférant des archives dans la solution logicielle Vitam, la situation est la suivante :

- si elle ne doit pas nécessairement consulter ses archives, une fois ces dernières transférées, il ne sera pas utile de lui attribuer un contrat d'accès.
- si elle a besoin de consulter ses archives et les journaux de transferts, il faudra créer un contrat d'accès lui permettant d'accéder à ses seules archives.

Point d'attention :

- Il est obligatoire d'indiquer dans un contrat d'accès actif si le service externe, une fois authentifié par la solution logicielle Vitam, a accès
  - à tous les services producteurs ou au moins à l'un d'entre eux,
  - à tous les usages ou à au moins l'un d'entre eux.

  Si aucun de ces éléments n'a été renseigné, même si le contrat d'accès est actif, le service externe ne pourra accéder à aucun service de la solution logicielle Vitam.
- Le(s) nœud(s) déclarés dans un contrat d'accès doivent exister dans la solution logicielle Vitam, sans quoi il(s) ne pourra/ont être enregistré(s) dans le contrat.

4.2. Comment effectuer l'import des différentes habilitations ?

Pour chaque catégorie d'habilitation à importer dans la solution logicielle Vitam (contexte applicatif, contrat d'entrée, contrat d'accès), il est possible d'importer un référentiel complet, comprenant plusieurs items, en une seule fois. La solution logicielle Vitam ne comptabilisera qu'une seule opération, et ne prend pas en compte dans le journal des opérations la création unitaire des différents items compris dans le référentiel importé.

Afin d'optimiser la traçabilité de la création des différents référentiels d'habilitations, il est donc recommandé de créer ces derniers un par un.

4.3. Comment nommer les différentes habilitations ?

Une application externe dispose d'un contexte applicatif et d'un à plusieurs contrats, d'entrée et/ou d'accès. Au travers de ces différents référentiels, il s'agira de paramétrer les habilitations de ce seul service. C'est pourquoi, il est recommandé d'adopter des règles de nommage identiques dans les différents référentiels, en utilisant les éléments suivants :

- nom de l'application versante ou accédante,

- nom ou type d'objet archivé,
- nom du service producteur,
- code métier.

En sachant que :

- un service producteur peut avoir plusieurs contrats différents ;
- une application versante ou accédante peut détenir plusieurs contrats.

4.4. Quel accès aux différentes habilitations ?

4.4.1. Gestion des droits

La gestion des habilitations relève d'opérations d'administration. Il est donc recommandé d'en limiter l'accès :

- un administrateur fonctionnel et/ou technique peut avoir accès à l'exhaustivité de ces référentiels et les mettre à jour ;
- une application versante et/ou accédante pourra, le cas échéant, avoir accès aux seules habilitations la concernant ;
- un tiers n'a pas vocation a prendre connaissance des contextes applicatifs et des profils de sécurité, pour des raisons de sécurité ;
- seul un administrateur technique a vocation à gérer les certificats applicatifs et les certificats personnels.

4.4.2. Restitution sur une IHM

La solution logicielle Vitam mise à disposition ne propose pas d'IHM pour représenter les privilèges associés à un profil de sécurité. Dans un projet d'implémentation, il est possible d'envisager la restitution de cette fonctionnalité sur une IHM dédiée.

Profil de sécurité, contrats d'entrée et d'accès sont obligatoirement associés à un contexte applicatif. S'il y a conception d'écrans permettant d'afficher contextes, profils de sécurité, contrats d'entrée et d'accès, il est recommandé de prendre en considération les liens entre eux.

4.5. Comment utiliser les différentes habilitations ?

Intitulé	Description	Niveau de recommandation
Contexte applicatif		
Application devant accéder aux services de la solution logicielle Vitam	Dès qu'on souhaite connecter une application à la solution logicielle Vitam, il faut, avant toute chose, l'authentifier au moyen d'un certificat applicatif qui détermine un contexte applicatif, avant de lui associer un profil de sécurité et des contrats, préexistants ou	Obligatoire

	créés à cette occasion.	
Application devant accéder aux services de la solution logicielle Vitam	Pour assurer une étanchéité entre les tenants, il est préconisé d'associer un seul tenant par contexte applicatif. De cette manière, le mécanisme d'authentification d'une application externe à un tenant ne permet de verser et d'accéder qu'à ce seul tenant.	Conseillé
Système d'information des archives (SIA) devant accéder à tous les tenants et services de la solution logicielle Vitam	Le SIA devant pouvoir accéder à plusieurs tenants et à l'ensemble des services disponibles, il est recommandé de lui attribuer un contexte applicatif lui permettant d'accéder à l'ensemble des tenants et des services de la solution logicielle Vitam.	Recommandé
Contrat d'entrée		
Application versante disposant d'un unique profil d'archivage	Cette application nécessite un unique contrat d'entrée, dans lequel on définira le profil d'archivage la concernant.	Recommandé
Application versante disposant de plusieurs profils d'archivage	Une application versante peut disposer de données nécessitant plus d'un profil d'archivage. • Ces profils peuvent être déclarés dans un même contrat d'entrée. Il reviendra au SIP de signaler le profil correspondant aux données qu'il contient. • Il est également possible de créer un contrat d'entrée par profil utilisé. Il est recommandé de créer un contrat d'entrée par profil. En effet, un contrat unique ne permettrait pas a posteriori, s'il déclare plusieurs profils, de déclarer pour chacun d'eux un nœud de rattachement particulier.	Recommandé
Application devant verser ses archives à un niveau particulier d'arbre de positionnement, de plan de classement ou de SIP	Un contrat d'entrée suffit pour déclarer un nœud unique de rattachement. Il est recommandé de créer autant de contrats d'entrée qu'il y aura de nœuds de rattachement où transférer les SIP. Le contrat d'entrée déclaré dans chaque SIP orientera ce dernier vers son nœud de rattachement. Si on souhaite ne pas multiplier les contrats d'entrée pour cette seule raison, il est recommandé de gérer les rattachements au niveau des unités archivistiques de chaque bordereau de transfert.	Recommandé
Application devant verser ses archives	Dans ce cas-là, il est recommandé de créer autant de contrats d'entrée que de nœuds de rattachement. Le SIP déclarera le contrat d'entrée adéquat.	Recommandé

dans plusieurs niveaux d'arbre de positionnement, de plan de classement ou de SIP	Si l'on souhaite ne déclarer qu'un contrat d'entrée pour ce type d'application, il faudra alors gérer les rattachements au niveau des unités archivistiques de chaque bordereau de transfert.	
Application versante disposant de plusieurs profils d'archivage et devant verser ses archives à un niveau particulier d'un arbre de positionnement ou d'un plan de classement	Il est recommandé d'utiliser un contrat d'entrée unique, contenant à la fois les profils d'archivage et le nœud de rattachement.	Recommandé
Application versante disposant de plusieurs profils d'archivage et devant verser ses archives dans plusieurs niveaux d'arbre de positionnement, de plan de classement ou de SIP	Si l'application nécessite de déclarer un profil et un nœud de rattachement propre aux archives liées à ce profil, il est recommandé de créer autant de contrats d'entrée que de profils d'archivage.	Recommandé

Contrat d'accès		
Application devant accéder à l'ensemble des archives et des objets conservés dans la solution logicielle Vitam	Les utilisateurs de l'application accédante auront alors accès à la solution logicielle Vitam tel que défini dans le contrat : • tous les services producteurs, • tous les usages, • des droits d'écriture. Par exemple : un SIA détenteur d'un contrat d'accès pourra avoir accès à l'ensemble des services producteurs et des usages, des droits d'écriture. Points d'attention : • L'utilisation d'un contrat d'accès unique peut ne pas être suffisante pour filtrer les accès. En effet, pour un SIA, on peut vouloir n'octroyer des accès limités qu'à certains types d'archives : des archives de certains domaines fonctionnels. Il reviendra à l'application accédante d'ajouter des filtres d'accès supplémentaires afin de réduire le périmètre des archives consultables. L'autre solution est d'attribuer plusieurs contrats d'accès à l'application.	Recommandé
Application devant filtrer les accès en fonction de profils utilisateurs	L'utilisation d'un contrat d'accès unique peut ne pas être suffisante pour filtrer les accès. En effet, pour un SIA, on peut vouloir n'octroyer des accès limités qu'à certains types d'archives : des archives de certains domaines fonctionnels. Option 1 : Il reviendra à l'application accédante d'ajouter des filtres d'accès supplémentaires afin de réduire le périmètre des archives consultables. Option 2 : L'autre solution est d'attribuer plusieurs contrats d'accès à l'application.	Recommandé
Application devant accéder à certaines versions des objets archivés	Il est recommandé de créer un seul contrat d'accès. L'avantage est de ne pas multiplier les contrats d'accès dans son référentiel. Les utilisateurs de l'application accédante auront alors accès à la solution logicielle Vitam tel que défini dans le contrat : • tout ou partie des services producteurs, • une partie des usages. Par exemple : ◦ un Portail Archives détenteur d'un contrat	Recommandé

	d'accès pourra accéder aux seuls objets de certains producteurs dont l'usage est la diffusion.	
Application devant accéder à une liste déterminée de services producteurs	Deux options sont possibles : • créer un contrat unique, • créer autant de contrats que de services producteurs. Option 1 : On peut choisir de ne créer qu'un contrat d'accès par application. Les utilisateurs de l'application accédante auront alors accès à la solution logicielle Vitam tel que défini dans le contrat : • certains services producteurs, • tout usage, • le cas échéant, des droits d'écriture. Par exemple : ◦ Un SIRH détenteur d'un contrat d'accès pourra accéder aux archives dont le service producteur est la Direction des ressources humaines. Points d'attention : • L'utilisation d'un contrat d'accès unique peut ne pas être suffisant pour filtrer les accès. En effet, pour un SIRH, on peut vouloir n'octroyer des accès limités qu'à certains types d'archives : des archives produites par le SIRH qui peuvent n'être qu'une partie des archives versées par la Direction des ressources humaines. Il sera alors nécessaire d'ajouter des filtres d'accès supplémentaires (ex : accès à un ou plusieurs nœuds) afin de réduire le périmètre des archives consultables Si cette solution ne suffit pas, il est recommandé d'attribuer plusieurs contrats d'accès à l'application. • Le choix de la granularité du service producteur est un élément déterminant. Si on reprend l'exemple du SIRH, plutôt que de lui donner accès à l'ensemble des archives de la Direction, il peut être judicieux de lui octroyer des droits sur les archives d'un service particulier tel que le Service de Gestion des Carrières. Cela est possible si les archives versées l'ont été par service et non pas par direction. Option 2 : Une application accédante peut disposer de	Recommandé

	plusieurs contrats d'accès, qui lui servent alors de filtre pour accéder à différents types d'archives. Ainsi, un SIA ou une GED transverse pourront détenir plusieurs contrats qui leur permettront de cibler, dans chacun de ces contrats, les services producteurs ou les types d'objets accessibles. Dans ce choix d'implémentation, les contrats d'accès servent d'éléments filtrants.	
Application devant accéder à un niveau particulier d'arbre de positionnement, de plan de classement ou de SIP	Un contrat d'accès suffit pour déclarer un nœud unique auquel l'application doit accéder, mais ce filtre devra nécessairement être couplé avec la déclaration d'un à plusieurs services producteurs, sans quoi l'application n'accédera pas aux contenus de la solution logicielle Vitam. Déclarer un nœud permet en effet de réduire le périmètre d'accès aux archives relatives à un ou plusieurs services producteurs. Par exemple : ◦ Un Portail Agent pourra accéder aux seuls bulletins de paie, préalablement versés par la Direction des ressources humaines au moyen de son contrat, tandis qu'un SIRH aura accès à l'ensemble des archives produites par cette même direction au moyen de son contrat qui, lui, ne précisera pas de nœud en particulier. L'application accédera ainsi au nœud en question et à son arborescence descendante. Points d'attention : • Les nœuds déclarés dans un contrat d'accès doivent obligatoirement exister dans la solution logicielle Vitam. • Le contrat d'accès ne permet pas de bloquer l'accès à des sous-répertoires du nœud déclaré. Si on souhaite rendre inaccessible des dossiers, il suffit de déclarer dans le contrat les seuls nœuds auxquels l'application pourra accéder. • L'usage de ce filtre peut s'avérer nécessaire si on souhaite restreindre les accès d'archives d'un service producteur (ex : Bureau des carrières) qui ont été rattachées à un plan de classement d'un autre service producteur (ex : Direction des ressources humaines). Sans filtre sur ses archives, le premier service producteur peut accéder à l'ensemble des archives de l'autre service producteur. • À des fins de maintien d'une bonne visibilité sur la gestion des nœuds d'accès, il est	Recommandé

	conseillé d'adopter, dans la mesure du possible, une pratique uniforme sur la déclaration des nœuds. Par exemple, il n'est pas recommandé, pour un service producteur donné, de créer autant de contrat qu'il y a de nœuds de description.	
Application devant accéder à plusieurs nœuds	Un contrat d'accès unique permet de déclarer plusieurs nœuds auxquels l'application doit accéder, mais ce filtre devra nécessairement être couplé avec la déclaration d'un à plusieurs services producteurs, sans quoi l'application n'accédera pas aux contenus de la solution logicielle Vitam. La détermination de plusieurs nœuds d'accès permet réellement d'affiner la granularité des accès. Les points d'attention décrits dans le point précédent s'appliquent également dans le cas présent.	Recommandé
Application disposant d'un contrat d'entrée et d'un contrat d'accès	Une application peut être à la fois versante et accédante. Ce qu'il faut retenir, qu'une application n'ait qu'un ou plusieurs contrats d'accès, avec ou sans contrat d'entrée, est qu'elle est dépendante de la manière dont les archives, quelles qu'elles soient, ont été versées. Le choix du service producteur est déterminant en entrée. Si une GED transverse multi-producteurs verse des SIP en ne déterminant qu'un seul service producteur, en accès, il ne sera pas possible de créer des contrats d'accès par sous-producteur, dans la mesure où les SIP ne les désignent pas nommément. Une des solutions pour éviter cet écueil est de rattacher ces SIP à des nœuds déclarant des producteurs différents. Ainsi, on pourra désigner ces derniers dans les contrats d'accès à associer au contexte de la GED transverse. Et en fonction de ces contrats, il sera possible d'accéder à un sous-producteur.	Recommandé

4.6. Comment gérer une nouvelle application ?

Pour connecter une application à la solution logicielle Vitam, il est recommandé de suivre les étapes suivantes :

Qui ?	Quoi ?	Via l'IHM démo Vitam ?	Commentaires
Administrateur	- Définition des privilèges à octroyer à	Non	

fonctionnel/ technique	une application et à associer ultérieurement à un profil de sécurité, - Définition des profils utilisateurs à mettre en place dans le Front Office et définition de leur mode de connexion (LDAP, certificat personnel, authentification gérée par le Front Office).		
Administrateur technique	Création d'un profil de sécurité	Non	Préalable à la création d'un contexte
Administrateur fonctionnel/ technique	Création d'un contexte : - sans permission - avec un profil de sécurité - statut « Inactif »	Oui	Préalable à la création d'un certificat
Administrateur technique	Création d'un certificat applicatif	Non	Déclare le contexte précédemment créé
Administrateur technique	Création de certificat(s) personnel(s)	Non	Étape facultative.
Administrateur fonctionnel	Création et paramétrages des contrats d'entrée et/ou d'accès	Oui	
Administrateur fonctionnel	Association des contrats d'entrée et/ou d'accès au contexte applicatif	Oui	
Administrateur fonctionnel	Activation du contexte	Oui	À la date souhaitée pour commencer les interactions entre l'application versante et/ou accédante et la solution logicielle Vitam
Administrateur technique / fonctionnel	Test avant utilisation courante	Oui	

4.7. Comment modifier des habilitations ?

La solution logicielle permet de modifier l'ensemble des habilitations disponibles. La modification de certains éléments peut avoir un impact sur les interactions entre l'application versante et/ou accédante et la solution logicielle Vitam.
Voici quelques recommandations sur les étapes à suivre en cas de modification des habilitations.

4.7.1. Mise à jour d'un certificat applicatif

Un certificat applicatif a une durée de vie limitée et nécessite d'être ponctuellement mis à jour, voire remplacé. On peut procéder de la manière suivante :

Qui ?	Quoi ?	Via l'IHM démo Vitam ?	Commentaires
Administrateur fonctionnel/ technique	Désactivation du contexte associé au certificat applicatif à changer	Oui	
Administrateur technique	Création d'un nouveau certificat applicatif, destiné à remplacer le certificat en production	Non	NB : déclaration du contexte désactivé.
Administrateur technique	Révocation du précédent certificat applicatif	Non	But : éviter un conflit de certificats lors de la réactivation du contexte.
Administrateur fonctionnel/ technique	Activation du contexte	Oui	
Administrateur technique / fonctionnel	Test avant utilisation courante	Oui	

4.7.2. Modification d'un contrat d'entrée

Il est possible de modifier un contrat d'entrée utilisé dans un contexte applicatif particulier. Il est conseillé de suivre les étapes suivantes en fonction du contexte d'utilisation du contrat :

Contexte	Action
Avec un contrat d'entrée	Désactivation du contexte applicatif ou du seul contrat d'entrée, le temps de procéder à la modification
Avec un contrat d'entrée et un contrat d'accès	Désactivation du seul contrat d'entrée, le temps de procéder à la modification, de manière à ne pas interrompre l'accès associé au contexte applicatif.
Avec plusieurs contrats d'entrée	Désactivation du seul contrat d'entrée, le temps de procéder à la modification, de manière à ne pas interrompre l'utilisation des autres contrats d'entrée associés au contexte applicatif.
Avec un ou	• Création d'un nouveau contrat d'entrée contenant les modifications à

plusieurs contrats d'entrée	apporter. • Association de ce contrat d'entrée au contexte applicatif. • Activation de ce contrat d'entrée. • Déclaration de ce nouveau contrat d'entrée dans les bordereaux de transfert. • Désactivation de l'ancien contrat d'entrée. • Suppression du lien entre l'ancien contrat d'entrée et le contexte applicatif.

4.7.3. Modification d'un contrat d'accès

Il est possible de modifier un contrat d'accès utilisé dans un contexte applicatif particulier. Il est conseillé de suivre les étapes suivantes en fonction du contexte d'utilisation du contrat :

Contexte	Action
Avec un contrat d'accès	Désactivation du contexte ou du seul contrat d'accès, le temps de procéder à la modification
Avec un contrat d'accès et un contrat d'entrée	Désactivation du seul contrat d'accès, le temps de procéder à la modification, de manière à ne pas interrompre les contrats d'entrées associés au contexte applicatif.
Avec plusieurs contrats d'accès	Désactivation du seul contrat d'accès, le temps de procéder à la modification, de manière à ne pas interrompre l'utilisation des autres contrats d'accès associés au contexte applicatif.
Avec un ou plusieurs contrats d'accès	• Création d'un nouveau contrat d'accès contenant les modifications à apporter. • Association de ce contrat d'accès au contexte applicatif. • Activation de ce contrat d'accès. • Désactivation de l'ancien contrat d'accès. • Suppression du lien entre l'ancien contrat d'accès et le contexte applicatif.

Annexe 1 : exemples d'habilitations

Nota bene : les cas présentés ci-dessous sont des exemples fictifs et visent simplement à vérifier la bonne mise en œuvre des mécanismes relatifs aux habilitations dans la solution logicielle Vitam.

Certificat applicatif


```
{
   "_id": "aeaaaaaaaaftuvruabdvkalafg6qe5yaaaaq",
   "SubjectDN": "CN=ihm-demo, O=vitam, L=paris, ST=idf, C=fr",
   "ContextId": "CT-000001",
   "SerialNumber": 252,
   "IssuerDN": "CN=ca_intermediate_client-external, OU=authorities, O=vitam, L=paris,
ST=idf, C=fr",
   "Certificate": "Q2VydGlmaWNhdGU6CiA […] 0tLQ=="
}
```


Certificat personnel


```
{
   "_id": "aeaaaaaaaaftuvruabdvkalafg6q2yqaaaaq",
   "SubjectDN": "O=VITAM, L=Paris, C=FR",
   "SerialNumber": 2,
   "IssuerDN": "O=VITAM, L=Paris, C=FR",
   "Certificate": "MIIFRjCCAy6gAwIBAgIBAjANBgkqhkiG9 […] w0BAQsFADAtM"
}
```


Contexte applicatif


```
{
   "Name": "Contexte pour application 1",
   "Status": true,
   "Permissions": [
      {
         "_tenant": 1,
         "AccessContracts": [
            "AC-000017",
            "AC-000060"
         ],
         "IngestContracts": [
            "IC-000060"
         ]
      },
      {
         "_tenant": 2,
         "AccessContracts": [AC-000001],
```

```
        "IngestContracts": [IC-000001]
      }
   ],
   "Identifier": "CT-000001",
   "SecurityProfile": "admin-security-profile"
}
```

Contrat d’entrée

```
[
   {
      "Name":"Contrat Archives Départementales",
      "Description":"Test entrée - Contrat Archives Départementales",
      "Status" : "ACTIVE",
   },
   {
      "Name":"Contrat Archives Nationales",
      "Description":"Test entrée - Contrat Archives Nationales",
      "Status" : "INACTIVE",
      "ArchiveProfiles": [
        "PR-000001"
      ]
   }
]
```

Contrat d’accès

```
[
   {
      "Name":"Archives du Doubs",
      "Description":"Accès Archives du Doubs",
      "Status" : "ACTIVE",
      "ActivationDate":"10/12/2016",
      "OriginatingAgencies":["FRA-56","FRA-47"]
   },
   {
      "Name":"Archives du Calvados",
      "Description":"Accès Archives du Calvados",
      "Status" : "ACTIVE",
      "ActivationDate":"10/12/2016",
      "DeactivationDate":"10/12/2016",
      "OriginatingAgencies":["FRA-54","FRA-64"]
      "EveryOriginatingAgency": false,
      "EveryDataObjectVersion": true,    }
]
```

Profil de sécurité

Exemple 1 :

{
“_id”: “aegqaaaaaaeucszwabglyak64gjmgbyaaaba”, “Identifier”: “SEC_PROFILE-000002”,
“Name”: “demo-security-profile”, “FullAccess”: false, “Permissions”: [
“securityprofiles:create”, “securityprofiles:read”, “securityprofiles:id:read”,
“securityprofiles:id:update”, “accesscontracts:read”, “accesscontracts:id:read”,
“contexts:id:update”
],
"_v": 0
}

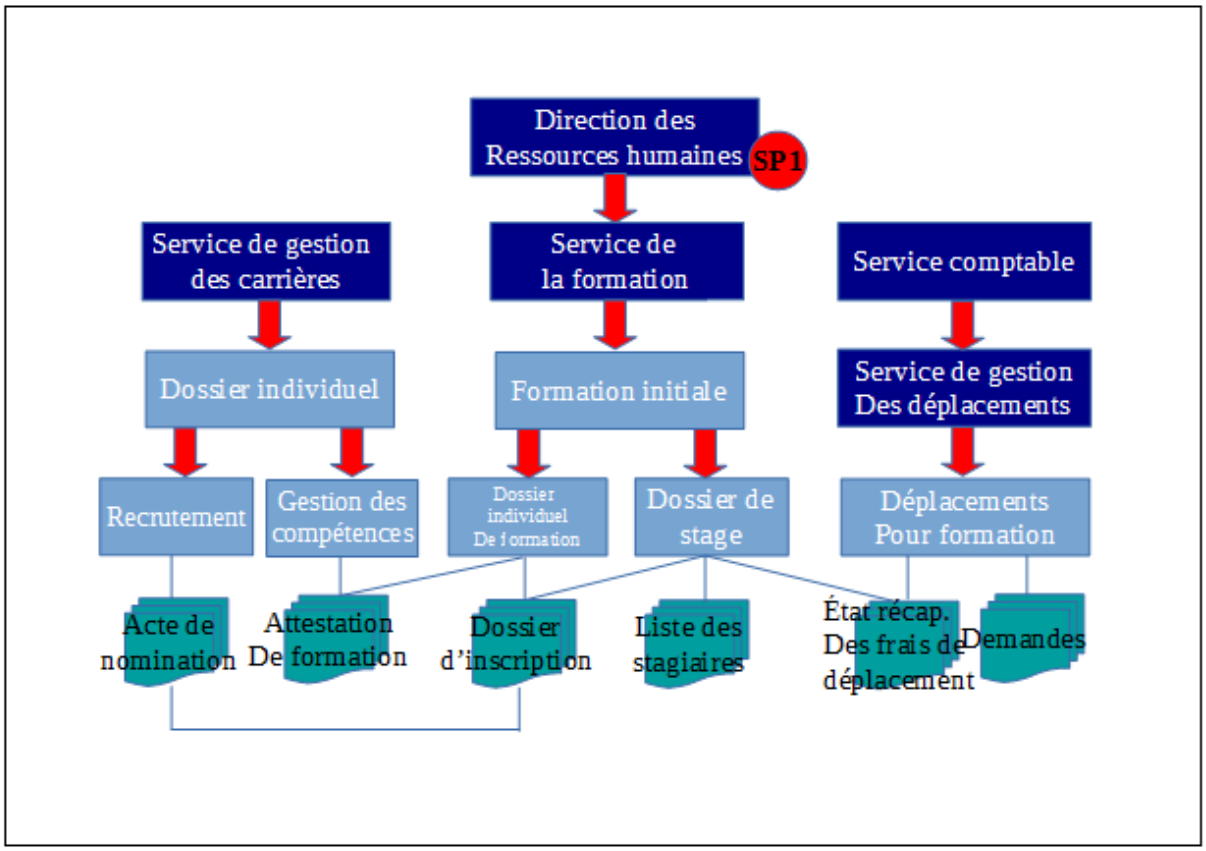
Exemple 2 :

{
"_id": "aegqaaaaaahe4mtkaa4vwak7ysw3jdyaaaaq",
"Identifier": "admin-security-profile",
"Name": "admin-security-profile",
"FullAccess": true,
"_v": 0
}

Annexe 2 : cas d'utilisation des habilitations

Nota bene : les cas présentés ci-dessous sont des exemples fictifs. Ils visent simplement à vérifier la bonne mise en œuvre des mécanismes relatifs aux habilitations dans la solution logicielle Vitam.

Cas 1 :



L'ensemble du plan de classement et des SIP ont pour unique producteur « Direction des Ressources humaines ».

- **Contrat d'entrée**
  - 1 / Une application comptable devant transférer des états récapitulatifs aura un contrat d'entrée lui permettant de verser des SIP dans le répertoire « État récapitulatif ».
  - 2 / Un SIRH doit transférer pour archivage courant des SIP dans les différents dossiers du plan de classement : il faudra créer autant de contrat d'entrée qu'il y a de dossiers de destination dans le plan de classement. Le SIP déclarera le contrat d'entrée mentionnant le nœud de rattachement adéquat.
- **Contrat d'accès**
  - 1 / Une application comptable devra accéder aux états récapitulatifs. Son contrat

d'accès aura pour paramètres :

- service producteur = « Direction des ressources humaines »
- nœud : « Etat récapitulatif des frais de déplacement »
  La déclaration du nœud est **obligatoire**, sans quoi l'application accèderait à l'ensemble des archives de la direction.

◦ 2 / Un SIRH doit accéder à l'ensemble des archives de la direction. Son contrat d'accès doit déclarer les éléments suivants :

- service producteur = « Direction des ressources humaines »

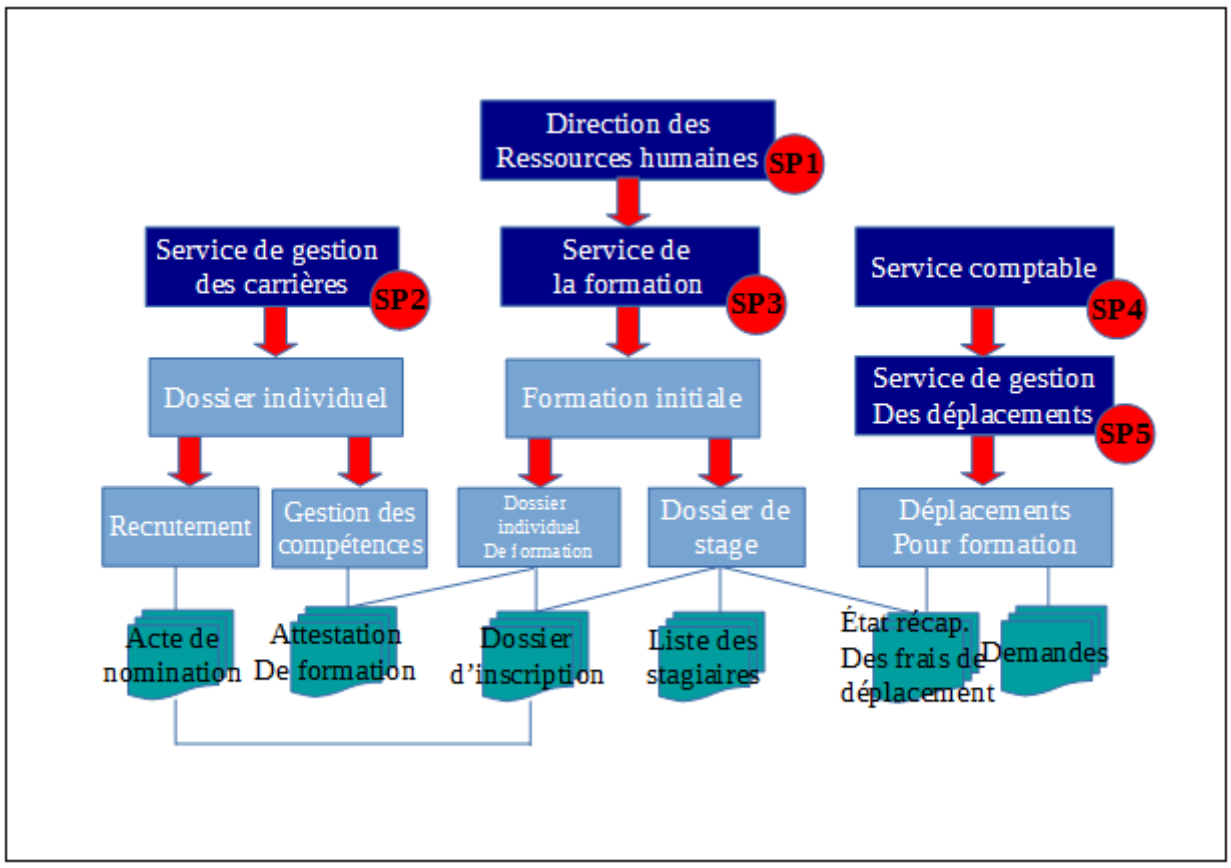
◦ 3 / Un SIRH doit accéder à l'ensemble des archives de la direction, sauf à celle du « Service comptable ». Son contrat d'accès doit déclarer les éléments suivants :

- service producteur = « Direction des ressources humaines »
- nœud = « Service de gestion des carrières », « Service de la formation ».

◦ 4 / Un SIRH veut filtrer ses accès par service. Il aura autant de contrat d'accès qu'il y a de services, soit 3. Chaque contrat devra déterminer :

- service producteur = « Direction des ressources humaines »
- nœud : chaque contrat déterminera le nœud à partir duquel un service pourra consulter ses archives. Dans le cas présent, le nœud correspond au niveau « Service... ».

Cas 2 :



Un plan de classement ayant pour producteur « Direction des Ressources humaines » englobe des plans de classement propres à chaque service, ayant chacun leur propre service producteur. L'un d'eux, « Service comptable », dispose d'un nouveau plan de classement inférieur, pour le « Service de gestion des déplacements ».
Ce cas d'usage vaut également si les plans de classement de niveau « Service » sont remplacés par des SIP.

- **Contrat d'entrée**
  - Rien ne change dans la déclaration des contrats d'entrée. Les exemples définis précédemment fonctionnent.
- **Contrat d'accès**
  - 1 / Une application comptable devra accéder aux états récapitulatifs. Son contrat d'accès aura pour paramètres :
    - service producteur = « Direction des ressources humaines » ou « Service comptable » ou « Service de gestion des déplacements ».
    - nœud : « État récapitulatif des frais de déplacement »
      La déclaration du nœud est **obligatoire**, sans quoi l'application accéderait à l'ensemble des archives de la direction ou des services.
  - 2 / Un SIRH doit accéder à l'ensemble des archives de la direction. Son contrat d'accès doit déclarer les éléments suivants :
    - service producteur = « Direction des ressources humaines »
  - 3 / Un SIRH doit accéder à l'ensemble des archives de la direction, sauf à celle du « Service comptable ». Son contrat d'accès doit déclarer les éléments suivants :
    - service producteur = « Service de gestion des carrières » et « Service de la formation ».
  - 4 / Un SIRH veut filtrer ses accès par service. Il aura autant de contrat d'accès qu'il y a de services, soit 3. Chaque contrat devra déterminer :
    - service producteur = le service concerné par le contrat.
  - 5 / Un portail « Ordre de mission » doit accéder au « Dossier de stage » et aux archives du « Service de gestion des déplacements ». Son contrat d'accès comportera les paramètres suivants :
    - service producteur = « Service de la formation » et « Service de gestion des déplacements ».
    - nœud = « Dossier de stage ». Si on ne déclare pas ce nœud, le portail accédera à l'ensemble des archives du Service de la formation.

Annexe 3 : liste des permissions et privilèges

Liste des permissions qui peuvent être associées à :

- un profil de sécurité,
- un certificat personnel (à l'exception des trois permissions écrites en italiques).

Nota bene : Cette liste n'est pas forcément exhaustive.

Service	Fonctionnalité	EndPoint correspondant
Contextes applicatifs	Importer des contextes dans le référentiel	contexts:create:json
	Lister le contenu du référentiel des contextes	contexts:read
	Lire un contexte donné	contexts:id:read
	Effectuer une mise à jour sur un contexte	contexts:id:update
Contrats d'entrée	Importer des contrats d'entrées dans le référentiel	ingestcontracts:create:json
	Lister le contenu du référentiel des contrats d'entrée	ingestcontracts:read
	Lire un contrat d'entrée donné	ingestcontracts:id:read
	Effectuer une mise à jour sur un contrat d'entrée	ingestcontracts:id:update
Contrats d'accès	Importer des contrats d'accès dans le référentiel	accesscontracts:create:json
	Lister le contenu du référentiel des contrats d'accès	accesscontracts:read
	Lire un contrat d'accès donné	accesscontracts:id:read
	Effectuer une mise à jour sur un contrat d'accès	accesscontracts:id:update
Profils de sécurité	Importer des profils de sécurité dans le référentiel	securityprofiles:create:json
	Lister le contenu du référentiel des profils de sécurité	securityprofiles:read
	Lire un profil de sécurité donné	securityprofiles:id:read
	Effectuer une mise à jour sur un profil de sécurité	securityprofiles:id:update
Profils d'archivage	Importer des profils dans le référentiel	profiles:create:binary

	Écrire un profil dans le référentiel	profiles:create:json
	Lister le contenu du référentiel des profils	profiles:read
	Importer un fichier xsd ou rng dans un profil	profiles:id:update:binaire
	Télécharger le fichier xsd ou rng attaché à un profil	profiles:id:read:binary
	Lire un profil donné	profiles:id:read:json
	Effectuer une mise à jour sur un profil	profiles:id:update:json
Formats	Importer un référentiel des formats	formats:create
	Lister le contenu du référentiel des formats	formats:read
	Lire un format donné	formats:id:read
	Vérifier si le référentiel des formats que l'on souhaite importer est valide	formatsfile:check
Règles de gestion	Lister le contenu du référentiel des règles de gestion	rules:read
	Vérifier si le référentiel de règles de gestion que l'on souhaite importer est valide	rulesfile:check
	Lire une règle de gestion donnée	rules:id:read
	Importer un référentiel des règles de gestion	rules:create
	Récupérer le rapport pour une opération d'import de règles de gestion	rulesreport:id:read
Services agents	Vérifier si le référentiel de services producteurs que l'on souhaite importer est valide	agenciesfile:check
	Importer un référentiel des services producteurs	agencies:create
	Trouver un service producteur avec son identifier	agencies:id:read
	Lister le contenu du référentiel des services producteurs	agencies:read
Entrées	Récupérer l'accusé de réception pour une opération d'entrée donnée	ingests:id:archivetransfertreply :read
	Récupérer le bordereau de versement pour une opération d'entrée donnée	ingests:id:manifests:read

	Envoyer un SIP à Vitam afin qu'il en réalise l'entrée	ingests:create
	Envoyer un SIP en local à Vitam afin qu'il en réalise l'entrée	ingests:local:create
Registre des fonds	Lister le contenu du référentiel des registres des fonds	accessionregisters:read
	Lister les détails d'un registre de fonds	accessionregisters:id:accessionregisterdetails:read
Unités d'archives et objets	Récupérer la liste des unités archivistiques	units:read
	Obtenir le détail d'une unité archivistique au format json	units:id:read:json
	Réaliser la mise à jour d'une unité archivistique	units:id:update
	Télécharger le groupe d'objet technique de l'unité archivistique donnée	units:id:objects:read:json
	Télécharger un objet	units:id:objects:read:binary
DIP	Générer le DIP à partir d'un DSL	dipexport:create
	Récupérer le DIP	dipexport:id:dip:read
Journaux	Lister toutes les opérations	logbookoperations:read
	Récupérer le journal de cycle de vie d'une unité archivistique	logbookunitlifecycles:id:read
	Récupérer le journal de cycle de vie d'un groupe d'objet	logbookobjectslifecycles:id:read
	Récupérer le journal d'une opération donnée	logbookoperations:id:read
Traçabilité	Télécharger le logbook sécurisé attaché à une opération de sécurisation	traceability:id:read
	Tester l'intégrité d'un journal sécurisé	traceabilitychecks:create
Audit	Lancer un audit de l'existence des objets	audits:create
Gestion des opérations	Récupérer les informations sur une opération donnée	operations:read
	Récupérer le code HTTP d'une opération donnée	operations:id:read:status
	Récupérer le statut d'une opération donnée	operations:id:read

	Changer le statut d'une opération donnée	operations:id:update
	Annuler une opération donnée	operations:id:delete
	Récupérer la liste des tâches des workflows	workflows:read
Index	*Réindexer une collection*	reindex:create
	Switch indexes	switchindex:create