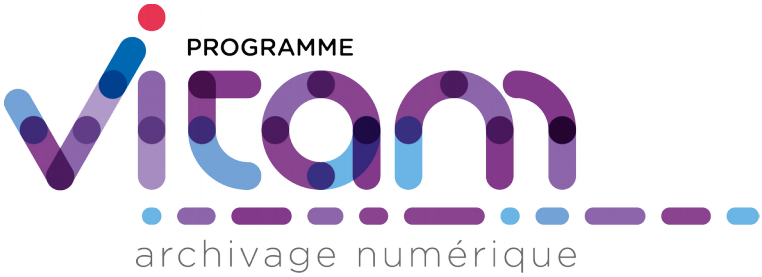


Gestion des habilitations

Date	Version
24/04/2019	6.0 (Release 10)

État du document

◯ En projet ◯ Vérifié ◉ Validé

Maîtrise du document

Responsabilité	Nom	Entité	Date
Rédaction	MVI	Équipe Vitam	28/05/2018
Vérification	Équipe	Équipe Vitam	
Validation	EVA	Équipe Vitam	15/06/2018

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	Section 2.1.2 (« Certificat personnel ») : 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
2.1	28/05/2018	MVI	Mise à jour pour tenir compte des fonctionnalités mises en œuvre pendant la *Release 7* : • section 2.1 (« Présentation des habilitations ») : ajout de contrôles dans les contrats d'entrée (types d'objet autorisés, obligation pour un bordereau de transfert de contenir des Master, contrôle supplémentaire sur le nœud de rattachement) et les contrats d'accès (interdiction d'accès). • section 2.2 (« Formalisation des habilitations ») : ajout de ces nouveaux contrôles dans le modèle de données des contrats d'entrée et d'accès ; ajout d'une empreinte dans le certificat personnel et de sa journalisation. • section 3.3 (« Entrées ») : prise en compte des nouvelles fonctionnalités. • section 3.4 (« Accès ») : prise en compte du filtre d'exclusion. • section 4.5 (« Comment utiliser les différentes habilitations ») : ajout de nouveaux cas métier : application versant des originaux numériques ;

			application versant des objets d'un type particulier ; application versant des objets de différents usages ; application devant accéder à un niveau particulier d'arbre de positionnement, de plan de classement ou de SIP ; application devant accéder à un niveau particulier d'arbre de positionnement, de plan de classement ou de SIP, mais ne devant pas avoir accès à un sous-niveau ; application devant accéder à plusieurs nœuds ; application devant accéder à plusieurs nœuds, mais ne devant pas avoir accès à plusieurs sous-niveaux
2.2	04/06/2018	MRE	Relecture
3.0	15/06/2018	MRE	Finalisation du document pour publication de la Release 7
3.1	29/08/2018	MVI	Mise à jour pour tenir compte des fonctionnalités mises en œuvre pendant la *Release 8* : • section 2.1 (« Présentation des habilitations ») : ajout de contrôles dans les contrats d'entrée (formats autorisés) et les contrats d'accès (filtre sur les droits de modification des règles de gestion et des profils d'unité archivistique, génération de logs d'accès sur les objets). • section 2.2 (« Formalisation des habilitations ») : ajout de ces nouveaux contrôles dans le modèle de données des contrats d'entrée et d'accès. • Section 3.1 (« Administration des référentiels ») : ajout de la sous-section 3.1.3 « Suppression » : révocation possible des certificats applicatif, profil de sécurité et contexte applicatif. • section 3.3 (« Entrées ») : prise en compte des nouvelles fonctionnalités. • section 3.4 (« Accès ») : prise en compte des nouveaux droits paramétrables dans les contrats d'accès. • section 4.5 (« Comment utiliser les différentes habilitations) » : ajout de nouveaux cas métier : application versant des objets au(x) format(s) connu(s), application versant des objets aux formats différents et non connus à l'avance ; application devant accéder à un seul tenant et pouvant y télécharger un objet ou intégrer un objet à un DIP ; SIA et/ou SAE devant télécharger un objet ou intégrer un objet à un DIP ; applications diverses

			devant accéder aux mêmes archives et pouvant télécharger un objet ou intégrer un objet à un DIP ; instance classifiée devant télécharger un objet ou intégrer un objet à un DIP ; application devant accéder à plusieurs tenants et pouvant y télécharger un objet ou intégrer un objet à un DIP ; application devant accéder aux archives pour simple consultation ; application devant accéder aux archives en fonction de profils utilisateurs. • annexe 1 (« Exemples d'habilitation ») : ajout d'exemples supplémentaires. • annexe 3 (« Liste des permissions et privilèges ») : ajouts de nouveaux Endpoints pour les services suivants : Audit, Gestion des opérations, Journaux, Ontologie, Profils d'unité archivistique, Règles de gestion, Services agents, Unités archivistiques et objets.
3.2	15/10/2018	MRE	Relecture
4.0	25/10/2018	MRE	Finalisation du document pour publication de la Release 8
4.1	22/01/2019	MVI	Refonte du plan du présent document : • section 2 (« Présentation des habilitations ») : fusion des sections 2.1 (« Description ») et 2.2 (« Formalisation des habilitations »). Désormais, cette section contient une section par habilitation et, pour chaque section, une sous-section « Description » et une sous-section « Formalisation ». • section 4 (« Conseils de mise en œuvre ») : création d'une sous-section 4.1 (« Généralités »), qui fusionne les anciennes sous-sections 4.7 (« Comment nommer les différentes habilitations ? »), 4.8 (« Quel accès aux différentes habilitations ? ») et 4.9 (« Comment gérer une nouvelle application ? »). Mise à jour pour tenir compte des fonctionnalités mises en œuvre pendant la *Release 9* : • section 2.2 (« Certificat applicatif») : ajout du caractère obligatoire de certains champs et précisions sur le statut d'un certificat applicatif (section 2.2.2). • section 2.3 (« Certificat personnel») : ajout du caractère obligatoire de certains champs, précisions sur le statut d'un certificat personnel et ajout d'une note de bas de page (section 2.3.2). • section 2.4 (« Profil de sécurité ») : ajout du caractère

			obligatoire de certains champs, précisions sur les droits auxquels le profil de sécurité donne accès, ainsi que sur la génération des identifiants des profils de sécurité et ajout d'une note de bas de page (section 2.4.2). • section 2.5 (« Contexte applicatif ») : explications sur l'import d'un contexte applicatif au format JSON (section 2.5.2.1) ; ajout du caractère obligatoire de certains champs, précisions sur les valeurs incrémentées par défaut par la solution logicielle Vitam (contrôle sur les tenants et statut), ajout d'une note de bas de page (section 2.5.2.2). • section 2.6 (« Contrat d'entrée ») : reformulation concertant le nœud de rattachement : soit le nœud est déclaré comme nœud de destination d'un bordereau de transfert, soit il est défini comme périmètre acceptant le rattachement d'un bordereau (section 2.6.1) ; explications sur l'import d'un contrat d'entrée au format JSON (section 2.6.2.1) ; ajout du caractère obligatoire de certains champs, précisions sur les valeurs incrémentées par défaut par la solution logicielle Vitam (statut), correction des notes de bas de page (section 2.6.2.2). • section 2.7 (« Contrat d'accès ») : explications sur l'import d'un contrat d'accès au format JSON (section 2.7.2.1) ; ajout du caractère obligatoire de certains champs, précisions sur les valeurs incrémentées par défaut par la solution logicielle Vitam (statut, usages, droit d'écriture), correction des notes de bas de page (section 2.7.2.2). • section 3.1 (« Administration des référentiels ») : les certificats applicatifs et personnels sont multi-tenant ; il est possible de supprimer un certificat personnel (section 3.1.3). • section 3.3 (« Entrées ») : reformulation concertant le nœud de rattachement : soit le nœud est déclaré comme nœud de destination d'un bordereau de transfert, soit il est défini comme périmètre acceptant le rattachement d'un bordereau. • section 4.2 (« Mise en œuvre du certificat applicatif ») : renvoi vers la documentation d'exploitation (section 4.2.1) ; ajout de la section 4.2.3 « Quand et comment supprimer un certificat

			applicatif ? ». • section 4.3 (« Mise en œuvre du certificat personnel ») : renvoi vers la documentation d'exploitation (section 4.3.1) ; ajout des sections 4.3.2 « Comment paramétrer les permissions associées à un certificat personnel ? » et 4.3.3 « Quand et comment supprimer un certificat personnel ? ». • section 4.4 (« Mise en œuvre du profil de sécurité ») : ajout de la section 4.4.2 « Comment modifier un profil de sécurité ? ». • Annexe 1 (« Exemples d'habilitation ») : ajout de deux exemples de contexte applicatif. • Annexe 3 (« Liste des permissions et privilèges ») : ajouts de nouveaux Endpoints pour les services suivants : Registre des fonds, Griffons, Scénarios de préservation, Préservation, Élimination, Unités archivistiques et objets, DIP, Traçabilité. • Annexe 4 (« Fonctionnement du log des accès ») : ajout de l'annexe.
4.2	25/01/2019	MRE	Relecture
5.0	30/01/2019	MRE	Finalisation du document pour publication de la Release 9
6.0	24/04/2019	MRE	Finalisation du document pour publication de la Release 10

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. 2.1	06/2018	
Vitam - Structuration des *Submission Information Package* (SIP) – v. 8.0.	24/04/2019	

Licence

La solution logicielle VITAM est publiée sous la licence CeCILL 2.1 ; la documentation associée (comprenant le présent document) est publiée sous Licence Ouverte V2.0.

Table des matières

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

Il s'articule autour des axes suivants :

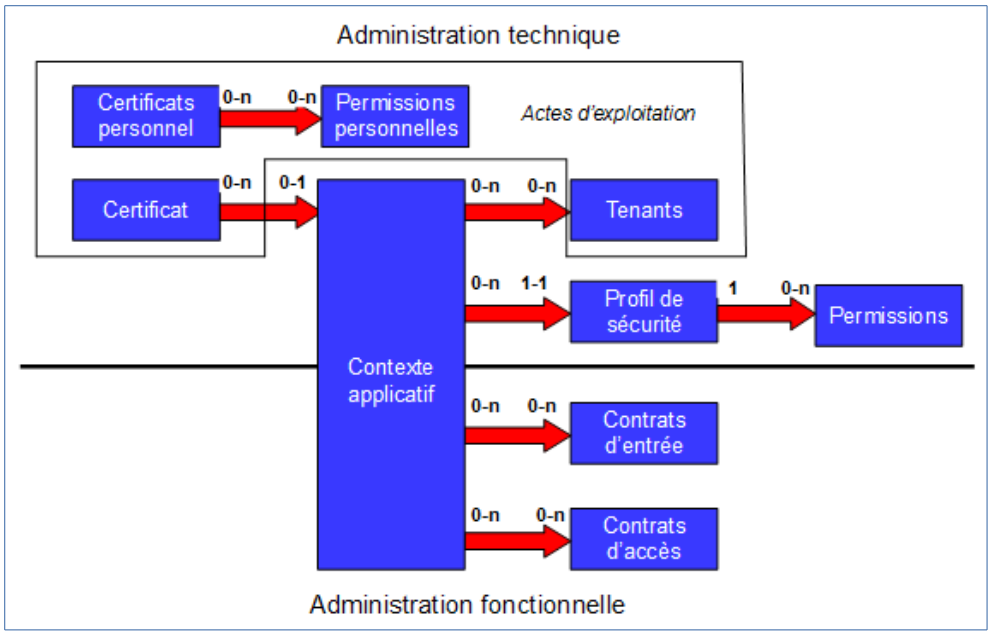
- une présentation des différentes habilitations : certificat applicatif, certificat personnel, profil de sécurité, contexte applicatif, contrat d'entrée, contrat d'accès, et de la manière dont le Standard d'échanges de données pour l'archivage (SEDA) et le modèle de données de la solution logicielle 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 9* (février 2019). 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.

2.2. Certificat applicatif

2.2.1. Définition

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.

2.2.2. Formalisation

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

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id – obligatoire) ;
- 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) ;
- statut du certificat applicatif (Status – obligatoire) :
  - Si le certificat est valide et actif, le statut a pour valeur « VALID » ;
  - Si le certificat a été révoqué, le statut a pour valeur « REVOKED ».

2.3. Certificat personnel

2.3.1. Définition

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** une personne 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 simplement transmis par le front-office dans les appels REST. A minima, la solution logicielle 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.

2.3.2. Formalisation

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

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id – obligatoire) ;
- identifiant unique du certificat personnel ou Distinguished Name (SubjectDN -

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 Idem. Un exemple de certificat personnel se trouve dans l'annexe 1 du présent document.

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) ;
- empreinte du certificat personnel (Hash - obligatoire) ;
- statut du certificat personnel (Status – obligatoire) :
  - Si le certificat est valide et actif, le statut a pour valeur « VALID » ;
  - Si le certificat a été révoqué, le statut a pour valeur « REVOKED ».

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[3].

Par ailleurs, le certificat personnel est enregistré dans le journal des opérations sous forme d'identifiant (agIdPers).

2.4. Profil de sécurité

2.4.1. Définition

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.

2.4.2. Formalisation

Le profil de sécurité est modélisé en JSON comme suit[4] :
- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id – obligatoire) ;
- identifiant donné au profil de sécurité, généré automatiquement par le système (Identifier – obligatoire). S'il est 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. Il peut également être généré par l'application à l'origine de sa création[5] ;

3 Le fonctionnement de ce fichier de configuration est précisé dans la section 4.3.2 « Comment paramétrer les permissions associées à un certificat personnel » du présent document. Une liste non exhaustive de ces services est présente dans l'annexe 3 du présent document.

4 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.

5 Un complément d'informations est donné dans la section 4.1.2 « Comment paramétrer les identifiants des différentes

- nom du profil de sécurité, qui doit être obligatoirement renseigné et unique sur la plateforme (Name – obligatoire) ;
- droit(s) au(x)quel(s) le profil de sécurité donne accès (FullAccess - obligatoire). Il peut s'agir de :
  - tous les accès (FullAccess = « true »),
  - dans le cas contraire (FullAccess = « false »), une liste de **privilèges ou droits** octroyés, sélectionnés parmi l'ensemble des services proposés par la solution logicielle Vitam (Permissions - facultatif) 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, fournie par le système (_v – obligatoire).

2.5. Contexte applicatif

2.5.1. Description

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.

2.5.2. Formalisation

2.5.2.1. Dans un fichier JSON

Un contexte applicatif prend la forme d'un fichier JSON, pouvant contenir 1 à n contexte(s) applicatif(s)[6].

```
[
  {
```

habilitations ? » du présent document.

6 Pour plus d'informations, consulter le document *Modèle de données*. Un exemple de contexte applicatif se trouve dans l'annexe 1 du présent document.

```
  "Identifier": "CT-00001",
  "Name": "Contexte_du_SIA",
  "SecurityProfile": "admin-security-profile"
}
]
```

Un contexte applicatif donné doit **obligatoirement** comporter les informations suivantes :

- identifiant signifiant (Identifier). Ce champ est obligatoire seulement s'il est généré par l'application à l'origine de sa création. Si cet identifiant est généré par la solution logicielle Vitam, il n'est pas nécessaire de le renseigner dans le fichier JSON ;
- nom du contexte (Name) ;
- identifiant du profil de sécurité associé au contexte (SecurityProfile).

Une liste des permissions (Permissions), un statut (Status) et un contrôle sur les tenants (EnableControl), facultatifs, peuvent venir compléter ces informations. Concernant les deux derniers items :

- Le premier peut contenir les valeurs « ACTIVE » ou « INACTIVE » ;
- Le deuxième les valeurs « true » ou « false ».

S'ils ne sont pas renseignés, la solution logicielle Vitam fournira automatiquement une valeur par défaut pour ces deux items :

- valeur « INACTIVE » pour le statut ;
- valeur « false » pour le contrôle sur les tenants.

2.5.2.2. Dans la solution logicielle Vitam

Le contexte applicatif est modélisé en JSON comme suit[7] :

- identifiant unique dans l'ensemble du système, fourni par ce dernier (_id - obligatoire) ;
- nom du contexte, qui doit être obligatoirement renseigné sur la plateforme (Name - obligatoire) ;
- identifiant unique donné au contexte (Identifier - obligatoire). 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 l'application à l'origine de sa création[8] ;
- version du contexte, fournie par le système (_v – obligatoire) ;
- identifiant du profil de sécurité associé au contexte (SecurityProfile - obligatoire) ;
- contrôle sur les tenants (EnableControl - obligatoire) :

7 Pour plus d'informations, consulter le document *Modèle de données*. Des exemples de contextes applicatifs se trouvent dans l'annexe 1 du présent document.

8 Par défaut, la solution logicielle Vitam attribue automatiquement un identifiant métier. Un complément d'informations est donné sur le sujet dans la section 4.1.2 « Comment paramétrer les identifiants des différentes habilitations ? » du présent document.

  - 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 » ou si le champ n'est pas présent dans le contexte applicatif importé, la solution logicielle Vitam la gère comme la valeur précédente et enregistre la valeur « 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 ;
- statut « Actif » ou « Inactif » (Status – obligatoire). Si le contexte applicatif importé ne contient pas de statut, la solution logicielle Vitam enregistre par défaut la valeur « Inactif »
- date de création du contexte, fournie par le système (CreationDate - obligatoire) ;
- dernière date de modification du contexte, fournie et mise à jour par le système (LastUpdate - obligatoire).

Un bloc **Permissions** (Permissions – facultatif), pouvant être vide, détaille le périmètre du contexte, tenant par tenant. Il comprend :

- le tenant dans lequel vont s'appliquer un ou plusieurs contrats (tenant – obligatoire si le bloc Permissions n'est pas vide) ;
- le(s) identifiant(s) de(s) contrat(s) d'accès appliqué(s) sur le tenant (AccessContracts – facultatif) ;
- le(s) identifiant(s) de(s) contrat(s) d'entrée appliqué(s) sur le tenant (IngestContracts – facultatif).

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).

2.6. Contrat d'entrée

2.6.1. Description

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 importé le contrat ;
- en option :
  - soit la destination ou point de rattachement des archives transférées dans le

système (correspond à une unité archivistique dans un plan de classement ou dans un arbre de positionnement–) ;
    - soit si les unités archivistiques contenues dans un bordereau de transfert doivent obligatoirement se rattacher sous ce point de rattachement lorsqu'elles déclarent un nœud de rattachement ;
- 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) ;
- si le bordereau doit obligatoirement contenir des objets de type « Master » ;
- le(s) type(s) d'objets ou usage(s) autorisé(s) dans un bordereau de transfert, dans le cas d'ajout(s) ultérieur(s) d'objet(s) à un groupe d'objets ;
- le(s) format(s) des objets autorisé(s) dans un bordereau de transfert ;
- si le bordereau peut contenir des objets dont le format n'est pas identifié.

2.6.2. Formalisation

2.6.2.1. Dans un fichier JSON

Un contrat d'entrée prend la forme d'un fichier JSON, pouvant contenir 1 à n contrat(s) d'entrée[9].

```
[
 {
  "Identifier": "IC-00001",
  "Name": "Contrat d'entrée_du_SIA"
 }
]
```

Un contrat d'entrée donné doit **obligatoirement** comporter les informations suivantes :

- identifiant signifiant. Ce champ est obligatoire seulement s'il est généré par l'application à l'origine de sa création (Identifier). Si cet identifiant est généré par la solution logicielle Vitam, il n'est pas nécessaire de le renseigner dans le fichier JSON ;
- nom du contrat (Name).

D'autres informations, facultatives, peuvent venir compléter ces informations. Elles sont détaillées dans la section suivante du présent document.

2.6.2.2. Dans la solution logicielle Vitam

Le contrat d'entrée est composé en JSON des éléments suivants[10] :

9 Pour plus d'informations, consulter le document *Modèle de données*. Des exemples de contrats d'entrée se trouvent dans l'annexe 1 du présent document.

10 Idem. Des exemples de contrats d'entrée se trouvent dans l'annexe 1 du présent document.

- identifiant unique par tenant, fourni par le système (_id – obligatoire) ;
- identifiant unique donné au contrat, généré automatiquement par le système (Identifier – obligatoire). 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[11] ;
- tenant dans lequel le contrat s'applique (_tenant – obligatoire) ;
- nom du contrat, qui doit être obligatoirement renseigné sur la plateforme (Name – obligatoire) ;
- description du contrat (Description – obligatoire) ;
- version du contrat (_v – obligatoire) ;
- statut « Actif » ou « Inactif » (Status – obligatoire). Si le contrat d'entrée importé ne contient pas de statut, la solution logicielle Vitam enregistre par défaut la valeur « INACTIVE » ;
- date de création du contrat, fournie par le système (CreationDate – obligatoire) ;
- dernière date de modification du contrat, fournie et mise à jour par le système (LastUpdate – obligatoire) ;
- si le contrat est actif, date d'activation du contrat, fournie par le système (ActivationDate – obligatoire) ;
- si le contrat est inactif, date de désactivation du contrat (DeactivationDate – facultatif) ;
- nom du profil d'archivage associé au contrat (ArchiveProfiles - facultatif – facultatif) ;
- identifiant du nœud auquel on souhaite rattacher les SIP versés (LinkParentId – facultatif) ;
- option imposant que les unités archivistiques soient rattachées sous le(s) nœud(s) enfant(s) du nœud précédemment défini et soient obligatoirement des nœuds enfants de ce nœud (CheckParentLink, valeur par défaut : « INACTIVE » – obligatoire) ;
- option permettant de rendre obligatoire ou non la présence d'un objet de type « Master » dans un transfert (MasterMandatory – valeur par défaut : « true » – obligatoire) ;
- usage(s) autorisé(s) dans le cas de l'ajout d'un objet à un groupe d'objets existant. Il peut s'agir de :
  - tous les usages (EveryDataObjectVersion, valeur par défaut : « false » – obligatoire),
  - une sélection d'usages (DataObjectVersion – facultatif). Ces usages peuvent être : archives physiques (PhysicalMaster), archives numériques originales (BinaryMaster), copies de diffusion (Dissemination), contenu textuel (TextContent), vignettes (Thumbnail) ;
- format(s) des objets autorisé(s) dans un bordereau de transfert. Il peut s'agir de :

11 Par défaut, la solution logicielle Vitam attribue automatiquement un identifiant métier. Un complément d'informations est donné sur le sujet dans la section 4.1.2 « Comment paramétrer les identifiants des différentes habilitations ? » du présent document.

  - tous les formats (EveryFormatType, valeur par défaut : « true » – obligatoire),
  - une sélection de formats (FormatType – facultatif), correspondant à une liste de PUID de format(s) autorisé(s) lors du transfert d'objets ;
- option autorisant le transfert d'objets dont le format n'est pas identifié (FormatUnidentifiedAuthorized, valeur par défaut : « false » – obligatoire).

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 enregistré dans le champ rightsStatementIdentifier pour toute opération de transfert (INGEST).

2.7. Contrat d'accès

2.7.1. Description

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 importé 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 nœud(s) au(x)quel(s) il n'aura pas accès ;
- tous ou 0 à n usage(s) au(x)quel(s) il aura accès.

Il permet de :

- 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 ;
- restreindre le droit d'écriture aux seules métadonnées de description ;
- activer la génération de logs en cas d'accès aux objets conservés sur la plate-forme.

2.7.2. Formalisation

2.7.2.1. Dans un fichier JSON

Un contrat d'accès prend la forme d'un fichier JSON, pouvant contenir 1 à n contrat(s) d'accès[12].

```
[
 {
```

12 Pour plus d'informations, consulter le document *Modèle de données*. Des exemples de contrats d'accès se trouvent dans l'annexe 1 du présent document.

```
  "Identifier": "AC-00001",
  "Name": "Contrat d'accès_du_SIA"
}
]
```

Un contrat d'accès donné doit **obligatoirement** comporter les informations suivantes :

- identifiant signifiant. Ce champ est obligatoire seulement s'il est généré par l'application à l'origine de sa création (Identifier). Si cet identifiant est généré par la solution logicielle Vitam, il n'est pas nécessaire de le renseigner dans le fichier JSON ;
- nom du contrat (Name).

D'autres informations, facultatives, peuvent venir compléter ces informations. Elles sont détaillées dans la section suivante du présent document.

2.7.2.2. Dans la solution logicielle Vitam

Le contrat d'accès est composé des éléments suivants[13] :

- identifiant unique par tenant, fourni par le système (_id – obligatoire) ;
- identifiant unique donné au contrat, généré automatiquement par le système (Identifier – obligatoire). 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[14] ;
- tenant dans lequel le contrat s'applique, fourni par le système (_tenant – obligatoire) ;
- nom du contrat, qui doit être obligatoirement renseigné sur la plateforme (Name – obligatoire) ;
- description du contrat (Description – facultatif) ;
- version du contrat, fournie par le système (_v – obligatoire) ;
- statut « Actif » ou « Inactif » (Status – obligatoire). Si le contrat d'accès importé ne contient pas de statut, la solution logicielle Vitam enregistre par défaut la valeur « Inactif » ;
- date de création du contrat, fournie par le système (CreationDate – obligatoire) ;
- dernière date de modification du contrat, fournie et mise à jour par le système (LastUpdate – obligatoire) ;
- si le contrat est actif, date d'activation du contrat, fournie par le système (ActivationDate – obligatoire) ;
- si le contrat est inactif, date de désactivation du contrat (DeactivationDate – facultatif) ;

13 Idem. Des exemples de contrats d'accès se trouve dans l'annexe 1 du présent document.

14 Par défaut, la solution logicielle Vitam attribue automatiquement un identifiant métier. Un complément d'informations est donné sur le sujet dans la section 4.1.2 « Comment paramétrer les identifiants des différentes habilitations ? » du présent document.

- 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, valeur par défaut : « false » – obligatoire),
  - une sélection de services producteurs (OriginatingAgencies – facultatif) ;
- usage(s) au(x)quel(s) le contrat donne accès. Il peut s'agir de :
  - tous les usages (EveryDataObjectVersion, valeur par défaut : « false » – obligatoire),
  - une sélection d'usages (DataObjectVersion – facultatif). 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) et à partir des/duquel(s) on souhaite donner accès (RootUnits – facultatif) ;
- identifiant du nœud ou des nœuds à partir de(s)quel(s) on souhaite interdire l'accès (ExcludeRootUnits – facultatif) ;
- droit d'écriture sur les archives (WritingPermission, valeur par défaut : « false » – obligatoire) ;
- droit de modification de l'ensemble des métadonnées d'une unité archivistique ou de ses seules métadonnées descriptives (WritingRestrictedDesc, valeur par défaut : « false » – obligatoire) ;
- droit d'enregistrer les accès sur les objets dans un log (AccessLog, valeur par défaut : « INACTIVE » – obligatoire).

Le contrat d'accès n'est actuellement pas déclaré dans le message ArchiveTransfer du SEDA.
Dans le journal des opérations, il est désormais enregistré dans le champ rightsStatementIdentifier 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 plusieurs fonctionnalités permettant de mettre en œuvre 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 des **options de contrôle** en entrée sur le rattachement du SIP ou sur le(s) type(s) d'objets accepté(s) ;
- 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 certificats applicatifs, des certificats personnels, 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.

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.

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 Suppression

La solution logicielle permet de supprimer unitairement certaines habilitations : certificat applicatif, certificat personnel, profil de sécurité et contexte applicatif.

Cette suppression peut avoir un impact sur les interactions entre l'application versante et/ou accédante et la solution logicielle Vitam. Cette opération ne s'effectue qu'au moyen des API et relève d'une opération d'administration technique.

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

3.1.4 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 :

- soit de rattacher des SIP à un arbre de positionnement ou un plan de classement préalablement versés dans la solution logicielle Vitam, en déclarant, dans un contrat d'entrée, l'identifiant système (le GUID) de l'unité archivistique auquel le SIP doit être rattaché. Si cette option est activée, l'/les unité(s) archivistique(s) racine(s) du SIP seront disposées sous cette unité archivistique ;soit de contrôler les nœuds de rattachement contenus dans les bordereaux de transfert, en déclarant un identifiant système (le GUID) de l'unité archivistique racine de rattachement :
  - si elle est activée, un bordereau de transfert ne pourra pas déclarer un nœud de rattachement positionné à un niveau supérieur de l'arborescence par rapport à celui qui est déclaré dans son contrat ou à un tout autre niveau sans lien avec ce dernier. La solution logicielle Vitam empêchera alors l'import.
  - si elle n'est pas activée, 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 il sera rattaché à deux nœuds différents, celui déclaré dans le bordereau de transfert et celui déclaré dans le contrat d'entrée.

Le contrat d'entrée permet également d'effectuer des contrôles sur les groupes d'objets transférés dans la solution logicielle Vitam au moyen de trois fonctionnalités :

- Une première option permet d'autoriser ou non le transfert de groupes d'objets ne contenant pas d'objets de type « Master » :
  - Si sa valeur est égale à « true », le bordereau de transfert devra nécessairement contenir des objets de type « Master », qu'ils soient binaires (« BinaryMaster ») ou physiques (« PhysicalMaster ») ;
  - Si sa valeur est égale à « false », le bordereau de transfert sera autorisé à contenir des groupes d'objets sans objet de type « Master » ;
  - Si le contrat d'entrée, lors de son initialisation, ne détermine pas l'option retenue, la solution logicielle Vitam appliquera par défaut une valeur égale à « true » et imposera la présence d'objets de type « Master » dans les bordereaux de transfert.

- Une deuxième option permet de déterminer quel(s) type(s) ou usage(s) d'objets sont attendus dans les bordereaux de transfert, dans le cas où l'on souhaite rattacher un objet à un groupe d'objets déjà conservé dans la solution logicielle Vitam :
  - Si le contrat d'entrée permet le transfert de n'importe quel type d'usage, le bordereau de transfert pourra contenir n'importe quel type d'usage ;
  - Si le contrat d'entrée précise quel(s) usage(s) il autorise, le bordereau de transfert devra nécessairement contenir le(s) seul(s) usage(s) déclaré(s) dans le contrat d'entrée, sans quoi le transfert échouera ;
  - Si le contrat d'entrée, lors de son initialisation, ne détermine pas l'option retenue, la solution logicielle Vitam acceptera n'importe quel usage en entrée.
- Une troisième option permet de déterminer quel(s) format(s) d'objets sont attendus dans les bordereaux de transfert :
  - Si le contrat d'entrée permet le transfert de n'importe quel format, le bordereau de transfert pourra contenir des objets de n'importe quel format possible ;
  - Si le contrat d'entrée précise quel(s) format(s) il autorise, le bordereau de transfert devra nécessairement contenir des objets conformes au(x) seul(s) format(s) déclaré(s) dans le contrat d'entrée, sans quoi le transfert échouera ;
  - Si le contrat d'entrée, lors de son initialisation, ne détermine pas l'option retenue, la solution logicielle Vitam acceptera n'importe quel format en entrée.

Il est également possible d'autoriser le transfert d'objets dont le format n'est pas identifié au moyen d'un paramétrage :

- Si sa valeur est égale à « true », il sera possible de transférer des objets non identifiés dans la solution logicielle Vitam malgré cette absence d'identification ;
- Si sa valeur est égale à « false » (valeur par défaut), il ne sera possible de transférer dans la solution logicielle Vitam que des objets dont le format est identifié.

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 ;
  - le(s) nœud(s) ou niveau(x) de l'arborescence à partir du(es)quel(s) un service externe n'aura pas accès.

  Dans les deux cas, 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).

Il peut également attribuer des droits de modification sur les métadonnées associées aux unités archivistiques (collection Unit) au moyen d'une restriction des droits d'écriture :

- Si sa valeur est égale à « true », le détenteur du contrat peut effectuer des mises à jour seulement sur les métadonnées descriptives ;
- Si sa valeur est égale à « false » (valeur par défaut), le détenteur du contrat peut effectuer des mises à jour sur les métadonnées descriptives, ainsi que sur les métadonnées de gestion et de contrôle de métadonnées (mise à jour du profil d'unité archivistique).

Une option permet enfin d'activer la génération d'un journal des accès sur les objets conservés dans la solution logicielle Vitam :

- Si sa valeur est égale à « ACTIVE », tout téléchargement des objets ou toute intégration d'un objet dans un DIP sera enregistré dans un fichier de log ou journal des accès ;
- Si sa valeur est égale à « INACTIVE » (valeur par défaut), aucun log ou journal des accès ne sera généré lors de téléchargement d'objets ou de l'intégration d'un objet dans un DIP[15].

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.

Points d'attention : la solution logicielle Vitam ne fait aucun contrôle de cohérence entre l'octroi d'un droit d'écriture et le paramétrage des droits de mise à jour sur les métadonnées associées aux unités archivistiques. En d'autres termes, il est possible qu'un contrat d'accès déclare à la fois un droit de lecture seule et un droit de révision de l'ensemble des métadonnées d'une unité archivistique. Le premier droit l'emporte sur le second.

15 Des précisions sur le log des accès se trouvent dans l'annexe 4 « Fonctionnement du log des accès » du présent document.

4. Conseils de mise en œuvre

À l'issue de cette dernière phase de réalisation de fonctionnalités concernant les habilitations, l'équipe projet Vitam est en mesure de fournir quelques recommandations de mise en œuvre. La solution logicielle permet de créer et 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.

4.1. Généralités

4.1.1. 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.

4.1.2. Comment paramétrer les identifiants des différentes habilitations ?

Par défaut, la solution logicielle Vitam génère les identifiants des habilitations de la manière suivante (mode « maître) :

Type d'habilitation	Paramétrage de l'identifiant
Profil de sécurité	préfixe SEC_PROFILE, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement
Contexte applicatif	préfixe CT, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement
Contrat d'entrée	préfixe IC, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement
Contrat d'accès	préfixe AC, suivi d'un tiret et d'une suite de 6 chiffres incrémentés automatiquement

Il est, néanmoins, possible de paramétrer ces identifiants, afin qu'ils soient générés par l'application à l'origine de la création des différentes habilitations concernées (mode « esclave ». Cette opération peut avoir lieu :

- soit au moment de l'installation de la plate-forme,
- soit après installation, sur une plate-forme en activité. Dans ce cas-là, une interruption temporaire de service sera à prévoir.

Pour ce faire, il faut modifier le fichier de configuration « functional-administration.conf », qui définit, entre autres, par tenant, les habilitations dont la solution logicielle Vitam ne génère pas d'identifiant[16].

```
# ExternalId configuration

listEnableExternalIdentifiers:
 0:
   - INGEST_CONTRACT
   - ACCESS_CONTRACT
 1:
   - INGEST_CONTRACT
   - ACCESS_CONTRACT
   - PROFILE
   - SECURITY_PROFILE
   - CONTEXT
```

Il est possible d'associer à un tenant l'habilitation pour laquelle on souhaite voir généré l'identifiant par une application externe, en ajoutant au tenant concerné le nom de l'habilitation concerné.

Le nom de l'habilitation concernée doit être écrit de la manière suivante :

- « INGEST_CONTRACT » pour les contrats d'entrée ;
- « ACCESS_CONTRACT » pour les contrats d'accès ;
- « SECURITY_PROFILE » pour les profils de sécurité (utile seulement sur le tenant d'administration) ;
- « CONTEXT » pour les contextes applicatifs (utile seulement sur le tenant d'administration).

La gestion des identifiants peut varier d'un tenant à l'autre, comme c'est le cas dans le tableau où :

- le tenant 1, d'administration, est esclave pour les contrats d'entrée et d'accès, les profils d'archivage, les profils de sécurité et les contextes ;
- le tenant 0 ne l'est que pour les contrats d'entrée et d'accès.

Cette opération relève d'un acte d'exploitation technique. Elle implique le redémarrage du/des composant(s), selon qu'il soit mono-instance ou multi-instances.

Points d'attention :

- En mode « esclave », il est fortement recommandé de faire débuter les référentiels

16 Cf. *Documentation d'exploitation*, chapitre 8.2.6.2.2 « Passage des identifiants des référentiels en mode esclave ».

avec d'autres chaînes de caractères que celle définies en mode « maître » ;
- Il ne faut pas oublier de répercuter cette modification sur le site secondaire.

4.1.3. Quel accès aux différentes habilitations ?

4.1.3.1. 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 ;
- seul un administrateur technique a vocation à gérer les certificats applicatifs et les certificats personnels ;
- une application versante et/ou accédante pourra, le cas échéant, avoir accès aux seules habilitations la concernant, en lecture seule ;
- un tiers n'a pas vocation a prendre connaissance des contextes applicatifs et des profils de sécurité, pour des raisons de sécurité.

4.1.3.2. 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.

4.1.4. 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 fonctionnel/ technique	- Définition des privilèges à octroyer à 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	Non	

	(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	

4.2. Mise en œuvre du certificat applicatif

4.2.1. 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[17].

4.2.2. Comment mettre à jourun 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 /	Test avant utilisation courante	Oui	

17 La procédure est détaillée dans *Documentation d'exploitation*, chapitre 9 « Intégration d'une application externe dans Vitam ».

fonctionnel			

4.2.3. Quand et comment supprimer un certificat applicatif ?

La suppression ou révocation d'un certificat applicatif peut intervenir à plusieurs occasions :

- l'application souhaitant s'authentifier à la solution logicielle Vitam est décommissionnée ;
- son certificat est obsolète et doit être remplacé.

La solution logicielle Vitam permet de le révoquer de la manière suivante :

- en transmettant à la solution logicielle Vitam la liste des certificats révoqués par une autorité fournissant des certificats applicatifs ;
- en changeant son statut, de « VALID » à « REVOKED ». Cela a pour conséquence le rejet de tout accès aux API de la solution logicielle Vitam au moyen de ce certificat révoqué.

La révocation d'un certificat applicatif dans la solution logicielle Vitam relève d'une opération d'administration technique[18].

4.3. Mise en œuvre du certificat personnel

4.3.1. 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[19].

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

18 La procédure est détaillée dans *Documentation d'exploitation*, chapitre 5.17 « Procédure d'exploitation pour la révocation des certificats SIA et Personae ». Se référer également au chapitre 12.1 « Cycle de vie des certificats ».

19 La procédure est détaillée dans *Documentation d'exploitation*, chapitre 9.2.2 « Authentification *personae* ».

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).

4.3.2. Comment paramétrer les permissions associées à un certificat personnel ?

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 : il s'agit du fichier « personal-certificate-permissions.conf »[20].

```
# Personal certification configuration for endpoint permissions

permissionsRequiringPersonalCertificate:



permissionsWithoutPersonalCertificate:
  - 'dipexport:create'
  - 'dipexportv2:create'
  - 'dipexport:id:dip:read'
  - 'logbookobjectslifecycles:id:read'
```

Ce fichier distingue :

- les services accessibles sans certificat personnel (« permissionsWithoutPersonalCertificate »). Par défaut, y sont listées l'ensemble des services mis à disposition par la solution logicielle Vitam[21] ;
- les services accessibles avec certificat personnel (« permissionsRequiringPersonalCertificate »). Par défaut, la solution logicielle Vitam ne générant pas nativement des certificats personnels, cette liste est vide.

Il est possible de :

- associer des permissions à un certificat personnel, en ajoutant à cette dernière liste vide les services souhaités ;
- supprimer des permissions accessibles sans certificat personnel.

Cette opération relève d'un acte d'exploitation technique.

4.3.3. Quand et comment supprimer un certificat personnel ?

La suppression ou révocation d'un certificat applicatif peut intervenir à plusieurs occasions :

- l'application souhaitant s'authentifier au moyen d'un certificat personnel à la solution logicielle Vitam est décommissionnée ;
- ce certificat est obsolète et doit être remplacé.

La solution logicielle Vitam permet de le révoquer de la manière suivante :

- en transmettant à la solution logicielle Vitam la liste des certificats révoqués par une autorité fournissant des certificats personnels ;
- en changeant son statut, de « VALID » à « REVOKED ». Cela a pour conséquence le

20 Cf. *Documentation d'exploitation*, chapitre 8.2.11.2.2 « Fichier personal-certificate-permissions.conf ».

21 Une liste non exhaustive de ces services est présentée dans l'annexe 3 du présent document.

rejet de tout accès aux API de la solution logicielle Vitam au moyen de ce certificat révoqué.

La révocation d'un certificat personnel dans la solution logicielle Vitam relève d'une opération d'administration technique[22].

4.4. Mise en œuvre du profil de sécurité

4.4.1. 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.

4.4.2. Comment modifier un profil de sécurité ?

Il est possible de modifier un profil de sécurité utilisé dans un ou plusieurs contexte(s) applicatif(s). Il est conseillé de suivre les étapes suivantes en fonction du contexte d'utilisation du profil de sécurité :

Contexte	Action
Avec un contexte applicatif	Désactivation du contexte applicatif, le temps de procéder à la modification, puis réactivation du contexte applicatif.
Avec plusieurs contextes applicatifs	Désactivation de l'ensemble des contextes applicatifs, le temps de procéder à la modification du profil de sécurité, puis réactivation des contextes applicatifs. Point d'attention : le profil de sécurité ainsi modifié doit toujours convenir à l'ensemble des contextes auxquels il est associé. Si ce n'est pas le cas, il faudra créer un nouveau profil de sécurité et l'associer aux contextes souhaités.

22 La procédure est détaillée dans *Documentation d'exploitation*, chapitre Procédure d'exploitation pour la révocation des certificats SIA et Personae ». Se référer également aux chapitres 12.1 « Cycle de vie des certificats » et 9.2.2.2 « Suppression d'un certificat pour l'authentification Personae ».

4.5. Mise en œuvre du contexte applicatif

4.5.1. 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.

4.5.2. Conseil d'utilisation du contexte applicatif

Intitulé	Description	Niveau de recommandation
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 créés à cette occasion.	Obligatoire
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	Conseillé

	seul tenant.	
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

4.6. Mise en œuvre du contrat d'entrée

4.6.1. 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 actif ;
- 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.

4.6.2. Conseils d'utilisation du contrat d'entrée

Intitulé	**Description**	**Niveau de recommandation**
Contrat d'entrée		
Application versante	Cette application nécessite un unique contrat	Recommandé

disposant d'un **unique profil** d'archivage	d'entrée, dans lequel on définira le profil d'archivage la concernant.	
Application versante disposant de **plusieurs profils** d'archivage	Une application versante peut générer des 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 ou de plan de classement	Un **contrat d'entrée suffit** pour déclarer un nœud unique de rattachement.	Recommandé
Application devant verser ses archives dans **plusieurs niveaux** d'arbre de positionnement ou de plan de classement	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 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	Il est recommandé de créer autant de contrats d'entrée que de profils d'archivage. Chaque contrat d'entrée fera référence aux profils d'archivage et au nœud de rattachement.	Recommandé
Application versant des originaux numériques	Pour une application devant transférer uniquement des originaux numériques, il est recommandé de contrôler au moyen du contrat d'entrée que les groupes d'objets qu'elle transfère contiennent obligatoirement un objet de type « Master » (« BinaryMaster »)	Recommandé
Application versant des objets d'un même usage à ajouter à des groupes d'objets déjà présents dans le système	Il est recommandé d'indiquer dans le contrat d'entrée quel est l'usage des objets à ajouter à des groupes d'objets déjà existant dans le système, si ces usages sont connus. Par exemple, un Portail Archives qui diffuse des copies numériques de diffusion pourrait ne devoir verser que des objets de type « Dissemination » pour compléter les groupes d'objets contenant les	Recommandé

	originaux.	
Application versant des objets de différents usages à ajouter à des groupes d'objets déjà présents dans le système	Quand on ne connaît pas les usages des objets qui pourraient être transférés dans la solution logicielle pour compléter les groupes d'objets déjà présents dans le système ou quand on ne souhaite pas imposer un contrôle sur les usages de des objets à transférer, il est recommandé d'autoriser le transfert d'objets de tous les types d'usage.	Recommandé
Application versant des objets au(x) format(s) connu(s)	Il est recommandé d'indiquer dans le contrat d'entrée quel(s) est(sont) le(s) format(s) des archives à transférer par une application versante, si ce(s) format(s) sont connus ou si l'on souhaite imposer une liste de formats propre à l'archivage. Par exemple : • un Portail Archives qui diffuse des copies numériques de diffusion pourrait ne devoir verser que des objets au format JPEG ; • un système d'archivage électronique ne souhaitant garantir la conservation d'objets qu'aux formats ODT, ODS, ODP, PDF, TIFF pourrait ne déclarer que des contrats d'entrée n'acceptant que ces seuls formats.	Recommandé
Application versant des objets aux formats différents et non connus à l'avance	Quand on ne connaît pas les formats des archives qui pourraient être transférées dans la solution logicielle ou quand on ne souhaite pas imposer des formats pour les archives à transférer et quand on souhaite, néanmoins, que ces formats soient identifiés par la solution logicielle Vitam lors du transfert des archives, il est recommandé d'autoriser le transfert de groupes d'objets contenant tous les formats possibles.	Recommandé
Application versant des objets aux formats différents et non connus à	Quand on ne connaît pas les formats des archives qui pourraient être transférées dans la solution logicielle ou quand on ne souhaite pas imposer des formats pour les archives à transférer et quand	Recommandé

l'avance	on souhaite n'effectuer aucun contrôle d'identification de format sur elles au moment de leur transfert dans la solution logicielle Vitam, il est recommandé d'autoriser le transfert de groupes d'objets contenant tous les formats possibles et de désactiver le contrôle d'identification des objets.	

4.6.3. 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 d'un 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 plusieurs contrats d'entrée	• Création d'un nouveau contrat d'entrée contenant les modifications à 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. Mise en œuvre du contrat d'accès

4.7.1. 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 (journal du cycle de vie des unités archivistiques et des objets), 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 pour autoriser ou interdire l'accès doivent exister dans la solution logicielle Vitam, sans quoi il(s) ne pourra/ont être enregistré(s) dans le contrat.

4.7.2. Conseil d'utilisation d'un contrat d'accès

Intitulé	Description	Niveau de recommandation
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 par exemple. Option 1 : Il reviendra à l'application accédante d'ajouter des filtres d'accès supplémentaires afin de réduire le périmètre des archives consultables.	Recommandé

	Option 2 : L'autre solution est d'attribuer plusieurs contrats d'accès à l'application.	
Application devant accéder à **certaines versions** des objets archivés	Il est recommandé de créer un seul contrat d'accès comportant les droits d'accès suivants : • **une partie des usages seulement** • tout ou partie des services producteurs. L'avantage est de ne pas multiplier les contrats d'accès dans son référentiel. Par exemple : • un Portail Archives détenteur d'un contrat d'accès pourra accéder aux seuls objets de certains producteurs dont l'usage est la diffusion.	Recommandé
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 portant les droits suivants : • **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. Option 2 : Une application accédante peut disposer de 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. Points d'attention : • L'utilisation d'un contrat d'accès unique peut ne pas être suffisante pour filtrer les accès. En	Recommandé

	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.	
Application devant accéder à un **niveau particulier** d'arbre de positionnement, de plan de classement ou de SIP	Un seul 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	Recommandé

	solution logicielle Vitam. • 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 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 **un niveau particulier** d'arbre de positionnement ou de plan de classement	Il est possible de permettre à une application d'accéder à un niveau particulier d'arborescence en excluant l'accès à tous les autres nœuds de même niveau. Néanmoins, si on crée a posteriori de nouveaux niveaux d'arborescence, il s'avérera nécessaire de rajouter ces nouveaux niveaux dans le périmètre d'exclusion du contrat d'accès, faute de quoi ces nouveaux niveaux seront accessibles.	Déconseillé
Application devant accéder à un **niveau particulier** d'arbre de positionnement, de plan de classement ou de SIP, mais ne devant **pas avoir accès à un sous-niveau**	Le contrat d'accès déclarera un niveau d'arborescence accessible. Il indiquera en outre comme inaccessible le répertoire disposé à un niveau inférieur à ce niveau accessible.	Recommandé
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.	Recommandé
Application devant accéder **à plusieurs nœuds**	Il est possible de permettre à une application d'accéder à plusieurs niveaux d'arborescence en excluant l'accès à tous les autres nœuds de même niveau. Néanmoins, si on crée a posteriori de nouveaux	Déconseillé

	niveaux d'arborescence, il s'avérera nécessaire de rajouter ces nouveaux niveaux dans le périmètre d'exclusion du contrat d'accès, faute de quoi ces nouveaux niveaux seront accessibles.	
Application devant accéder à **plusieurs nœuds,** mais ne devant **pas avoir accès à plusieurs sous-niveaux**	Le contrat d'accès déclarera les niveaux d'arborescence accessibles. Il indiquera en outre comme inaccessibles les répertoires disposés à un niveau inférieur à ces niveaux accessibles.	Recommand
Application devant accéder **à un seul tenant** et pouvant y télécharger un objet ou intégrer un objet à un DIP	Si une application unique doit accéder à un seul tenant de la solution logicielle Vitam et si : • elle ne requiert pas de besoins particuliers en matière de consultation des objets, • elle dispose déjà de paramétrages propres de traçabilité (ex : module de reporting, de statistiques, d'audit), il n'est pas recommandé d'activer la génération des logs d'accès dans son contrat d'accès.	Non recommandé
SIA et/ou SAE devant télécharger un objet ou intégrer un objet à un DIP	Un système d'information archivistique (SIA) et/ou un système d'archivage électronique (SAE) nécessitant un journal des consultations, il est recommandé d'activer la génération d'un log des accès.	Recommandé
Applications diverses devant accéder aux mêmes archives et pouvant télécharger un objet ou intégrer un objet à un DIP	Si plusieurs applications doivent accéder aux mêmes archives et, de fait, aux mêmes objets, il est recommandé d'activer la génération d'un log des accès dans leur contrat d'accès respectif, afin de pouvoir vérifier a posteriori quelle application a accédé à quels objets.	Recommandé
Instance classifiée devant télécharger un objet ou intégrer un objet à un DIP	En vue d'ajouter une garantie supplémentaire de traçabilité, il est recommandé d'activer la génération d'un journal des accès dans le contrat d'accès d'une instance classifiée.	Recommandé
Application devant accéder **à plusieurs tenants** et pouvant y télécharger un objet ou intégrer un objet à un DIP	Si une application peut accéder à plusieurs tenants, il est recommandé d'activer la génération d'un log des accès dans son contrat d'accès, afin de pouvoir vérifier a posteriori quels objets ont été téléchargés ou ont été intégrés dans un DIP sur quel tenant en particulier.	Recommandé
Application devant accéder aux archives **pour simple consultation**	Une application devant accéder à la solution logicielle Vitam pour la seule consultation d'archives, un portail par exemple, peut disposer d'un contrat d'accès lui attribuant des droits de lecture et non des droits d'écriture.	Recommandé
Application devant	L'utilisation d'un contrat d'accès unique peut ne pas	Recommandé

accéder aux archives en fonction de **profils utilisateurs**	être suffisante pour filtrer les droits d'accès. En effet, pour un SIA, on peut vouloir n'octroyer que des accès limités à certains droits : lecture, modification des seules métadonnées descriptives, administration. Option 1 : Il reviendra à l'application accédante d'ajouter des filtres d'accès supplémentaires afin de réduire le périmètre des droits des utilisateurs sur les archives. Option 2 : L'autre solution est d'attribuer plusieurs contrats d'accès à l'application, chacun d'eux déterminant une permission particulière : • l'un, un droit de lecture sur les archives, • un autre, un droit d'écriture et de mise à jour des seules métadonnées descriptives, • un dernier, un droit d'écriture et de mise à jour sur l'ensemble des métadonnées associées à une unité archivistique.	
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

4.7.3. 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	Désactivation du contexte ou du seul contrat d'accès, le temps de procéder à la

d’accès	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 transferts du contrat d’entrées associé au contexte applicatif.
Avec plusieurs contrats d’accès	Désactivation d’un 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==",

"Status": "VALID"

}

Certificat personnel

{

"_id": "aeaaaaaaaaftuvruabdvkalafg6q2yqaaaaq",

"SubjectDN": "O=VITAM, L=Paris, C=FR",

"SerialNumber": 2,

"IssuerDN": "O=VITAM, L=Paris, C=FR",

"Certificate": "MIIFRjCCAy6gAwIBAgIBAjANBgkqhkiG9 […] w0BAQsFADAtM",

"Hash": "6088f19bc7d328f301168c064d6fda93a6c4ced9d5c56810c4f70e21e77d841d"

"Status": "VALID"

}

Contexte applicatif


```
{
   "Name": "Contexte pour application 1",
   "Status": "ACTIVE",
   "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"
},
{
   "Name": "Contexte pour application 2",
   "Status": "ACTIVE",
   "Permissions": [
      {
         "_tenant": 1,
         "AccessContracts": [
            "AC-000017",
            "AC-000060"
         ]
      },
      {
         "_tenant": 2
      }
   ],
   "Identifier": "CT-000002",
   "SecurityProfile": "admin-security-profile"
},
```

```
{
   "Name": "Contexte pour application 3",
   "Status": "ACTIVE",
   "Permissions": [],
   "Identifier": "CT-000003",
   "SecurityProfile": "admin-security-profile"
}
```

Contrat d'entrée

Avec profil d'archivage

```
[
   {
      "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"
      ]
   }
]
```

Avec nœud de rattachement et d'exclusion

```
[
     {
          "Name":"3328_IC_INVALID",
          "Identifier":"3328_IC_INVALID",
          "Description":"3328_IC_INVALID",
          "Status" : "ACTIVE",
          "LinkParentId": "aeaaaaaaaahejegaabxyyalfwx45ejyaaaaq",
          "CheckParentLink": "aeaaaaaaaahejegaabxyyalfwx45ejyaaaaq2"
     }

]
```

Avec filtres sur les types d’objets attendus


```
[
    {
        "Name":"Contrat_FormatUnidentified_EveryFormatType_plus_autres",
        "Identifier":"Contrat_FormatUnidentified_EveryFormatType_plus_autres",
        "Description":"Contrat de test",
        "Status":"ACTIVE",
        "MasterMandatory": false,
        "EveryDataObjectVersion": true,
        "FormatUnidentifiedAuthorized":true,
        "EveryFormatType": false,
        "FormatType":["fmt/17", "x-fmt/279"]
    }
]
```


Contrat d’accès

Avec filtre sur les services producteurs


```
[
  {
    "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,    },

{
   "Name":"Archives de Paris",
    "Description":"Accès Archives de Paris",
    "Status" : "INACTIVE",
    "EveryOriginatingAgency": true
```

```
  }
]
```

Avec filtre sur les usages

```
[
    {
        "Name":"Archives du Haut-Rhin",
        "Description":"Accès Archives du Haut-Rhin",
        "Status":"ACTIVE",
        "OriginatingAgencies":["Identifier0"],
        "DataObjectVersion": ["BinaryMaster", "Dissemination"]
    },
  {
    "Name":"Archives du Bas-Rhin",
    "Description":"Accès Archives du Bas-Rhin",
    "Status" : "ACTIVE",
    "OriginatingAgencies":["FRA-54","FRA-64"]
    "EveryOriginatingAgency": false,
    "EveryDataObjectVersion": true
  }
]
```

Avec filtre sur les nœuds d’accès et d’exclusion

```
{
        "Name":"Archives du Vaucluse",
        "Description":"Accès Archives du Vaucluse",
        "Status" : "ACTIVE",
        "EveryOriginatingAgency": true,
        "EveryDataObjectVersion": true,
        "ExcludedRootUnits": ["aeaaaaaaaahejegaabxyyalfwx45ejyaaaaq"],
        "RootUnits": ["aeaaaaaaaahejegaabxyyalfwx45ejyaaaaq ?"]
    }
```

Avec filtre sur les droits

```
[
  {
    "Name":"NoUpdatesAllowed",
   "Identifier": "NoUpdatesAllowed",
    "Description":"Contrat d'accès - Sans droits de modification des unités archivistiques",
```

```
      "Status" : "ACTIVE",
    "EveryOriginatingAgency": true,
    "WritingPermission": false,
    "WritingRestrictedDesc": false
  }, {
    "Name":"AllUpdatesAllowed",
    "Identifier": "AllUpdatesAllowed",
    "Description":"Contrat d'accès - Droit de mise à jour complet",
    "Status" : "ACTIVE",
    "EveryOriginatingAgency": true,
    "WritingPermission": true,
    "WritingRestrictedDesc": false
  }, {
    "Name":"OnlyDescUpdateAllowed",
    "Identifier": "OnlyDescUpdateAllowed",
    "Description":"Contrat d'accès - Droit de modification restraint aux unités
archivistiques",
    "Status" : "ACTIVE",
    "EveryOriginatingAgency": true,
    "WritingPermission": true,
    "WritingRestrictedDesc": true
  }, {
    "Name":"DefaultWritePermissions",
    "Identifier": "DefaultWritePermissions",
    "Description":"Contrat d’accès - Modifications autorisées sans précisions
supplémentaires",
    "Status" : "ACTIVE",
    "EveryOriginatingAgency": true,
    "WritingPermission": 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
}

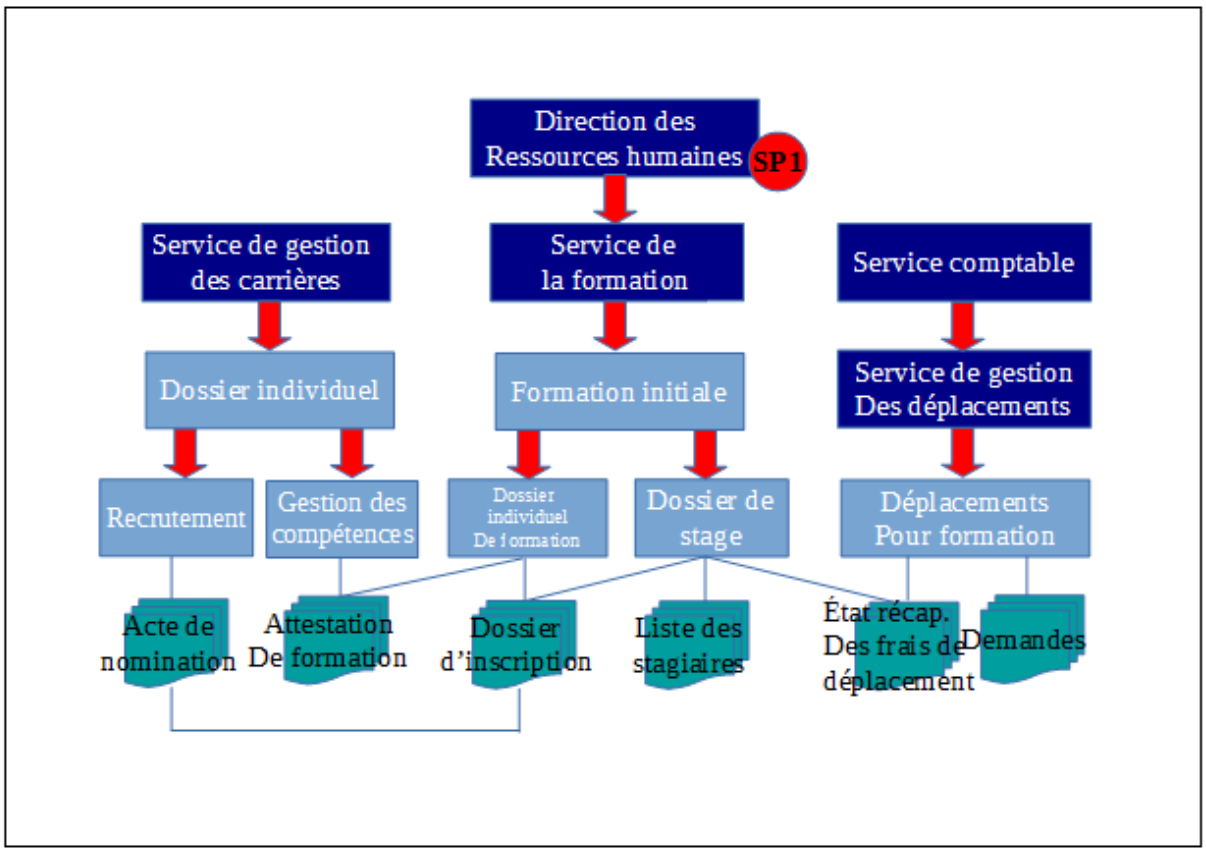
Exemple 2 :

{
"_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 des frais de déplacement ».
  - 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 »

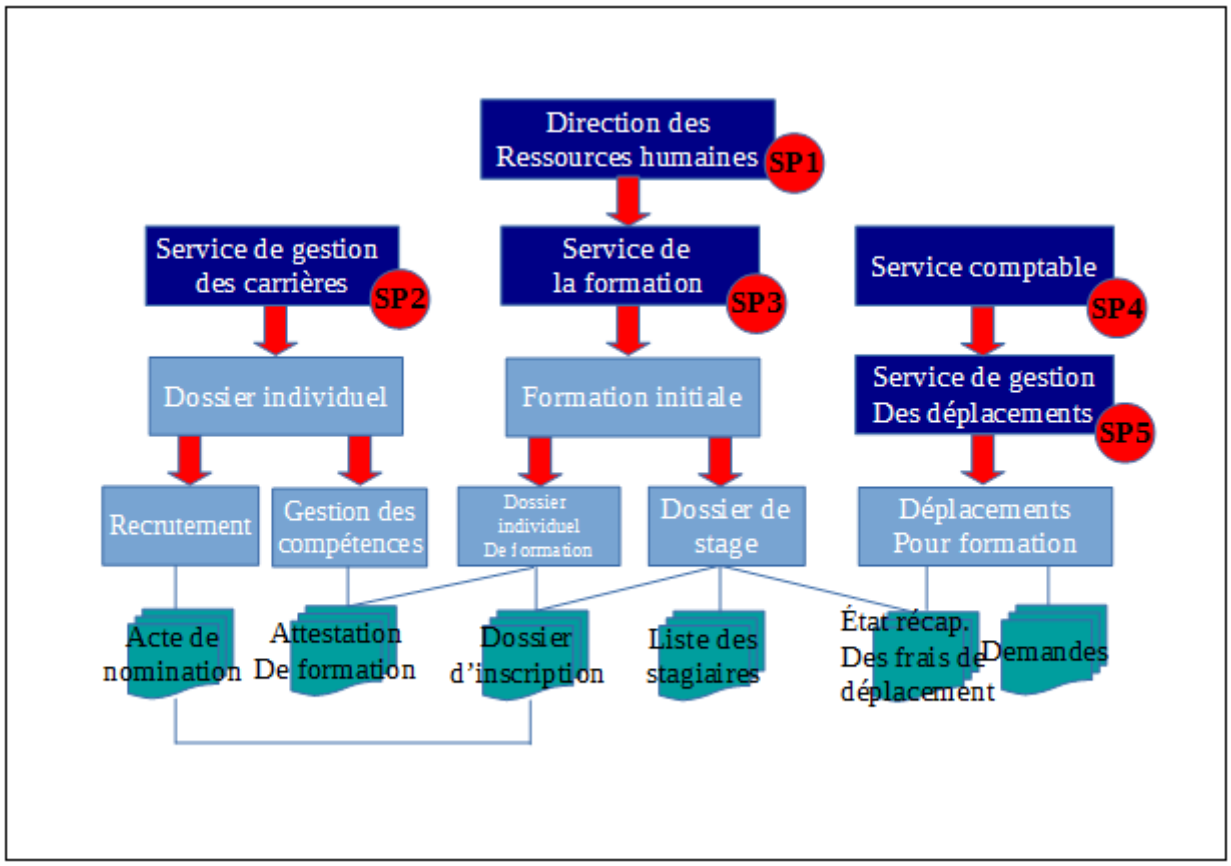
◦ 3 / Un SIRH doit accéder à l’ensemble des archives de la direction, sauf à celle du « Service comptable ». Son contrat d’accès doit déclarer les éléments suivants :

- service producteur = « Direction des ressources humaines »
- nœuds = « 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	accesscontracts:id:update

	d'accès	
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
Ontologie	Importer le référentiel ontologique	ontologies:create:json
	Lister le contenu du référentiel ontologique	ontologies:read
	Lire un vocabulaire	ontologies:id:read:json
Profils d’unité archivistique	Importer un ou plusieurs profils d’unité archivistique dans le référentiel	archiveunitprofiles:create:binary
	Ecrire un ou plusieurs profils d’unité archivistique dans le référentiel	archiveunitprofiles:create:json
	Lister le contenu du référentiel des profils d’unité archivistique	archiveunitprofiles:read
	Lire un profil d’unité archivistique donné	archiveunitprofiles:id:read:json
	Effectuer une mise à jour sur un profil d’unité archivistique	archiveunitprofiles:id:update:json
Profils	Importer des profils dans le référentiel	profiles:create:binary

d’archivage	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	rulesreport:id:read

	d'import de règles de gestion	
	Récupérer le référentiel pour une opération d'import de référentiel de règles de gestion	rulesreferential:id:read
Services agents	Vérifier si le référentiel de services agents que l'on souhaite importer est valide	agenciesfile:check
	Importer un référentiel des services agents	agencies:create
	Trouver un service agents avec son identifier	agencies:id:read
	Lister le contenu du référentiel des services agents	agencies:read
	Récupérer le référentiel pour une opération d'import de référentiel des services agents	agenciesreferential:id: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:accessi

		onregisterdetails:read
	Lister les détails d'un registre de fonds symbolique	accessionregisterssymbolic:read
Unités archivistiques et objets	Récupérer la liste des unités archivistiques	units:read
	Récupérer la liste des unités archivistiques avec leurs règles de gestion héritées	unitsWithInheritedRules:read
	Récupérer la liste des groupes d'objets	objects: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
	Mise à jour en masse des unités archivistiques	units:update
	Mise à jour en masse des règles de gestion des unités archivistiques	units:rules:update
	Téléchargement de rapports liés aux mises à jour de masse	distributionreport:id:read
	Reclassification d'unités archivistiques	reclassification: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

		dipexportv2: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
	Télécharger les journaux d'accès	storageaccesslog:read:binary
Traçabilité	Télécharger le logbook sécurisé attaché à une opération de sécurisation	traceability:id:read
	Tester l'intégrité d'un journal sécurisé	traceabilitychecks:create
	Génère un relevé de valeur probante	probativevalue:check probativevalue:create
Audit	Lancer un audit de l'existence des objets	audits:create
	Audit de traçabilité d'unités archivistiques	evidenceaudit:check
	Rectification de données suite a un audit	rectificationaudit:check
Élimination	Lance la phase d’analyse dans le cadre d’une élimination	elimination:analysis
	Lance la phase d’action dans le cadre d’une élimination	elimination:action

Griffons	Importer un référentiel des griffons	griffins:create
	Récupérer la liste des griffons	griffins:read
	Lire un griffon donné	griffin:read
Scénarios de préservation	Importer un référentiel des scénarios de préservation	preservationScenarios:create
	Récupérer la liste des scénarios de préservation	preservationScenarios:read
	Lire un scénario de préservation donné	preservationScenarios:read
Préservation	Lance le processus de préservation	preservation:update
	Télécharger le rapport de préservation	Preservationreport:id:read
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
	Force la pause sur un type d'opération et/ou sur un tenant	forcepause:check

	Retire la pause sur un type d'opération et/ou sur un tenant	removeforcepause:check
Index	Réindexer une collection	reindex:create
	Switch indexes	switchindex:create

Annexe 4 : fonctionnement du log des accès

Description

Le contrat d’accès permet de préciser si des logs d’accès doivent être générés. Par défaut, cette option n’est pas activée.

Le log des accès est généré lors d’un accès à l’objet (fichier numérique), que ce soit par téléchargement de l’objet ou export d’un DIP. Les accès à l’unité archivistique ne sont pas concernés.

Les logs de l’heure en cours peuvent être consultés sur les machines hébergeant le composant **storage** sous l’arborescence « /vitam/log/storage/access-log/ ». Chaque fichier de log est nommé « <tenant>_<date>_<id opération>.log ».

Toutes les heures, les logs sont archivés et sont alors accessibles dans des `containers` nommés ``<environnement>_<tenant>_storageaccesslog``.

Structure des logs

- "eventDateTime" : date et heure de l’accès au format AAAA-MM-JJTHH:MM:SS:[3 digits de millisecondes]
- "xRequestId" : identifiant de l’opération d’export du DIP
- "applicationId" : identifiant de l’application ayant demandé l’export du DIP
- "objectIdentifier" : identifiant de l’objet auquel on a accédé
- "size" : taille en octets de l’objet
- "qualifier" : usage de l’objet
- "version" : version de l’usage de l’objet
- "contextId" : identifiant du contexte utilisé pour l’accès
- "contractId" : identifiant du contrat utilisé pour l’accès
- "archivesId" : identifiant de l’unité archivistique dont dépend le groupe d’objets contenant l’objet auquel on a accédé

Exemple de log généré lors de l’export d’un DIP d’une unité archivistique ayant un GOT contenant un objet

{"eventDateTime":"2019-01-11T12:50:53.344",

"xRequestId":"aeeaaaaaachfmo4dabyw6aliht3q74aaaaaq",

"applicationId":"MyApplicationId-ChangeIt",

"objectIdentifier":"aeaaaaaaaahk2vrsabz26alhywthyoaaaaba",

"size":"11",

"qualifier":"BinaryMaster",

"version":"1",

"contextId":"CT-000001",

"contractId":"ContratTNR",

"archivesId":"aeaqaaaaaahk2vrsabz26alhywthzbaaaaea"}

Exemple de logs généré lors de l’export d’un DIP de sept unités archivistiques dont quatre seulement avaient un GOT contenant un objet

{"eventDateTime":"2019-01-11T12:51:46.185",

"xRequestId":"aeeaaaaaachfmo4dabyw6aliht36c6qaaaaq",

"applicationId":"MyApplicationId-ChangeIt",

"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywpmhkaaaaba",

"size":"29403",

"qualifier":"BinaryMaster",

"version":"1",

"contextId":"CT-000001",

"contractId":"ContratTNR",

"archivesId":"aeaqaaaaaaherlfzabz5salhywpmhlyaaaaq"}

{"eventDateTime":"2019-01-11T12:51:46.200",

"xRequestId":"aeeaaaaaachfmo4dabyw6aliht36c6qaaaaq",

"applicationId":"MyApplicationId-ChangeIt",

"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywpmhkiaaaaq",

"size":"68438",

"qualifier":"BinaryMaster",

"version":"1",

"contextId":"CT-000001",

"contractId":"ContratTNR",

"archivesId":"aeaqaaaaaaherlfzabz5salhywpmhlyaaabq"}

{"eventDateTime":"2019-01-11T12:51:46.208",

"xRequestId":"aeeaaaaaachfmo4dabyw6aliht36c6qaaaaq",

"applicationId":"MyApplicationId-ChangeIt",

"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywpmhjyaaaaq",

"size":"29403",

"qualifier":"BinaryMaster",

"version":"1",

"contextId":"CT-000001",

"contractId":"ContratTNR",

"archivesId":"aeaqaaaaaaherlfzabz5salhywpmhliaaaba"}

{"eventDateTime":"2019-01-11T12:51:46.221",
"xRequestId":"aeeaaaaaachfmo4dabyw6aliht36c6qaaaaq",
"applicationId":"MyApplicationId-ChangeIt",
"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywpmhjyaaabq",
"size":"29403",
"qualifier":"BinaryMaster",
"version":"1",
"contextId":"CT-000001",
"contractId":"ContratTNR",
"archivesId":"aeaqaaaaaaherlfzabz5salhywpmhlqaaaba"}

Exemple de logs générés lors de l’export d’une unité archivistique ayant un GOT comprenant trois objets

{"eventDateTime":"2019-01-11T13:22:12.686",
"xRequestId":"aeeaaaaaachfmo4dabyw6alihuj4btqaaaaq",
"applicationId":"MyApplicationId-ChangeIt",
"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywnsvrqaaabq",
"size":"44266",
"qualifier":"Thumbnail",
"version":"1",
"contextId":"CT-000001",
"contractId":"ContratTNR",
"archivesId":"aeaqaaaaaaherlfzabz5salhywnsvsaaaaaq"}

{"eventDateTime":"2019-01-11T13:22:12.700",

"xRequestId":"aeeaaaaaachfmo4dabyw6alihuj4btqaaaaq",

"applicationId":"MyApplicationId-ChangeIt",

"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywnsvraaaaaq",

"size":"127244",

"qualifier":"BinaryMaster",

"version":"1",

"contextId":"CT-000001",

"contractId":"ContratTNR",

"archivesId":"aeaqaaaaaaherlfzabz5salhywnsvsaaaaaq"}

{"eventDateTime":"2019-01-11T13:22:12.718",
"xRequestId":"aeeaaaaaachfmo4dabyw6alihuj4btqaaaaq",
"applicationId":"MyApplicationId-ChangeIt",
"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywnsvrqaaaaq",
"size":"57850",
"qualifier":"Dissemination",
"version":"1",
"contextId":"CT-000001",
"contractId":"ContratTNR",
"archivesId":"aeaqaaaaaaherlfzabz5salhywnsvsaaaaaq"}

Exemple de log généré lors de l’export d’un seul des usages de la même unité archivistique que ci-dessus

{"eventDateTime":"2019-01-11T14:17:52.472",
"xRequestId":"aeeaaaaaachfmo4dabyw6alihvdlm5aaaaaq",
"applicationId":"MyApplicationId-ChangeIt",
"objectIdentifier":"aeaaaaaaaaherlfzabz5salhywnsvrqaaaaq",
"size":"57850",
"qualifier":"Dissemination",
"version":"1",
"contextId":"CT-000001",
"contractId":"ContratTNR",
"archivesId":"aeaqaaaaaaherlfzabz5salhywnsvsaaaaaq"}