Spécification d’interface

API des gestionnaires de consentement

Version de travail

Date : 15/04/2021

Sommaire

Description du document 3

Historique des versions 3

1 Préambule 4

1.1 Objet du document 4

1.2 Documents de référence 4

1.3 Glossaire des termes utilisés 4

2 Fonctionnement général de l'interface ROUTEUR / SGC 4

2.1 Présentation du système 4

2.2 Concepts d'implémentation 5

2.3 Contraintes techniques 5

3 Description détaillée des services 5

3.1 Service d'authentification 5

3.1.1 Modes d'authentification supportés 5

3.1.2 HTTP Basic 6

3.1.3 OAuth 2 6

3.2 API de consultation des consentements 6

3.2.1 Description du service de vérification des consentements 6

3.2.2 Description du service de récupération des consentements 8

3.2.3 Principes communs aux 2 services 12

Description du document

Emetteur	Agdatahub
Projet	Routeur agdatahub
Nom du document	Routeur_agdatahub_spécification_interfaçage_SGC_v1.5
Version	1.5 Version de travail
Rédacteurs	Edouard HUE, OBS Lauréna GENDRE, pour agdatahub

Historique des versions

Version	Opération	Nom	Date
1.0	Création	Edouard HUE	09/12/2020
1.1	Modifications	Edouard HUE	29/01/2021
1.2	Modifications, ajout de contenu	Lauréna GENDRE	05/02/2021
1.3	Réorganisation des URN	Édouard Hue	17/03/2021
1.4	Ajout de l'identifiant complémentaire aux consentements	Édouard Hue	24/03/2021
1.5	Modifications de mise en forme	Lauréna GENDRE	20/04/2021

1 Préambule

1.1 Objet du document

Ce document décrit les conditions d'interfaçage entre le routeur de consentements agdatahub et les systèmes tiers de gestion de consentements (SGC). Il complète et précise le contrat d'interface « API des gestionnaires de consentements » au format Open API 3 référencé ci-dessous.

Le dossier de spécification d'interface comprenant ce document et le contrat d'interface Open API 3 a pour but de décrire les modalités d'interfaçage d'un SGC au routeur agdatahub.

1.2 Documents de référence

Titre	Référence	Version
API des gestionnaires de consentement	consent-manager-api.yaml	1.0.0

1.3 Glossaire des termes utilisés

Terme Utilisé	Description
SGC	Système de gestion des consentements = système d'information qui stocke et gère des consentements
Ayant droit	La personne morale qui a les droits sur les données et dont le consentement est nécessaire
Fournisseur de services bénéficiaire	L'organisme qui propose du service aux agriculteurs et pour ce faire à besoin d'accéder à des données. C'est le bénéficiaire du consentement.
Fournisseur de données	La société en maitrise de la base de données qui fournit les données au fournisseur de services bénéficiaire.
Responsable d'enregistrement du consentement	L'organisme qui enregistre le consentement dans le système informatique d'un gestionnaire de consentements.

2 Fonctionnement général de l'interface ROUTEUR / SGC

2.1 Présentation du système

Le routeur agdatahub joue un rôle de façade en avant des SGC tiers participants. Le routeur définit une représentation commune permettant de décrire les consentements de façon indépendante des SGC.

Pour permettre au routeur de les interroger, les SGC doivent mettre en œuvre les interfaces définies dans le contrat d'interfaçage. Ces interfaces comprennent l'API de consultation des consentements proprement dite (vérification et récupération de consentements) et une API d'authentification.

Les nouveaux SGC sont enregistrés dans le routeur par l'administrateur Agdatahub et chaque projet d'interfaçage doit faire l'objet d'une phase de tests sur un environnement dédié (recette).

2.2 Concepts d'implémentation

L'API expose ses fonctions selon les principes REST. Notamment, elle expose une ressource « consents » sur laquelle sont réalisables les opérations HTTP HEAD (vérification de consentements) et GET (récupération de consentements). Les données sont transmises au format JSON. Les entités nommées sont, dans la mesure du possible, identifiées par des URI.

Il est conseillé aux SGC de mettre en œuvre la compression des données envoyées dans les réponses aux requêtes, selon les modalités prévues par le protocole http1.

2.3 Contraintes techniques

Le point d'accès du gestionnaire de consentement doit répondre à ces contraintes :

- Le point d'accès est disponible en permanence en service nominal. Les interruptions de service planifiées sont communiquées dès que possible à agdatahub.
- Les requêtes en provenance du routeur sont traitées en moins de 2 secondes dans 90 % des cas. On considère le temps écoulé entre la réception du premier octet de la requête et l'envoi du dernier octet de la réponse.
- Le SGC est dimensionné pour traiter avec un taux de succès de 99% :
    - un volume moyen de 1 000 requêtes par heure ;
    - un pic de 200 requêtes sur 5 minutes.

Le point d'accès est accessible uniquement en HTTPS. Le certificat autorisé est valide en tout point et est signé par une autorité de certification reconnue par le programme de certification de Mozilla[2].

3 Description détaillée des services

3.1 Service d'authentification

3.1.1 Modes d'authentification supportés

Le routeur agdatahub peut s'authentifier auprès du SGC selon deux modes au choix :

- L'envoi d'identifiants par le schème HTTP Basic[5] ;
- L'envoi d'un jeton d'accès OAuth 2 sous forme d'un *Bearer Token*[6] obtenu par le *client credentials grant*[7].

Le système OAuth 2 est préconisé.

3.1.2 HTTP Basic

Le SGC fournira à agdatahub des identifiants (nom d'utilisateur et mot de passe). Ces identifiants seront encodés selon le format défini par la RFC 7617 dans chaque requête émise par le routeur agdatahub à destination du SGC. Le SGC autorisera chaque requête porteuse d'identifiants valides.

3.1.3 OAuth 2

Le SGC fournira à agdatahub des identifiants (*client id* et *client secret*) et précisera les coordonnées permettant à au routeur d'obtenir un jeton d'accès (*access token*) à travers une requête de type *client credentials grant*. Ces coordonnées peuvent être, au choix :

- L'URL de l'*issuer location* si OpenID Connect Discovery 1.0[8] est supporté.
- Les URL du *token endpoint* et du *JWK Set*[9] en l'absence d'OpenID Connect Discovery.

Le SGC précisera également le *scope* à requérir par le routeur.

Le jeton d'accès sera encodé dans un entête HTTP *Authorization* selon le format défini par la RFC 6750 dans chaque requête émise par le routeur à destination du SGC. Le SGC autorisera chaque requête porteuse d'un jeton valide.

3.2 API de consultation des consentements

Cette API expose deux fonctionnalités : le test de l'existence d'un consentement et la recherche de consentements.

3.2.1 Description du service de vérification des consentements

Ce service permet de vérifier l'existence d'un consentement portant sur des critères renseignés en paramètres. Par exemple, cette vérification pourrait être utilisée en amont d'un transfert de données.

Le service est exposé en HEAD. En cas d'authentification via OAuth2, le token est préalablement récupéré via le service d'authentification est passé dans le header de la requête.

3.2.1.1 Paramètres transmis en entrée

Paramètre	Description	Type	Cardinalité	Obligatoire
dataSupplier	Fournisseur des données sujettes aux consentements.	n°SIRET	0..1	non
rightHolder	Ayant-droit ayant accordé des consentements.	n° SIRET n° NUMAGRIT n° EDE	1	oui
serviceProvider	Fournisseur de services bénéficiaire des consentements	n°SIRET	1	oui
family	Famille de données concernée par les consentements	Chaine de caractères	1	oui
usage	Usage consenti sur la famille de données.	Chaine de caractères	1	oui
activeAt	Moment auquel les consentements renvoyés doivent être actifs	Date heure	1	oui

Dans cette version du système, il n'est pas prévu que la date d'interrogation (activeAt) soit différente de la date du jour de l'appel par le routeur (vérification de consentements passés ou futur). L'information date est émise par le routeur au moment de la requête en envoyant la date et l'heure de l'appel.

3.2.1.2 Réponses attendues

Code	Description
200	Vérification réussie, il existe au moins un consentement répondant aux critères.
204	Vérification réussie, mais il n'existe pas de consentement répondant aux critères.
400	Requête incohérente.
401	Authentification absente ou invalide.
403	Droits de l'utilisateur insuffisants.

3.2.1.3 Précisions

Numéro	Description	Exemples

1	La vérification d'un consentement vise à déterminer si un usage spécifique est consenti. Cet usage peut être permis par un consentement accordé sur un plus large périmètre (bénéficiaires, fournisseurs de données, familles de données). Dans ce cas, la réponse attendue est positive.	Il existe chez un SGC un consentement accordé pour un usage u1 sur les familles de données f1 et f2. La vérification du consentement à l'usage u1 sur la seule famille f1 a donc un résultat positif. De la même manière, s'il existe un consentement accordé pour les usages u1 et u2 sur la famille f1, la vérification du consentement au seul usage u1 sur la famille f1 a un résultat positif.
2	Lorsque le consentement a été donné quelque soit le fournisseur de données au niveau du SGC, alors les consentements sont réputés être accordés à tout fournisseur de données.	Il existe des consentements chez un SGC pour tout fournisseur de données. Pour ce SGC, une requête portant sur le fournisseur f1 a une réponse positive dès lors qu'il existe des consentements satisfaisant tous les autres critères de la requête.
3	Si le paramètre fournisseur de données n'est pas renseigné (champ optionnel), la réponse est négative si le consentement a été donné de manière restrictive pour un fournisseur de données en particulier.	Il existe des consentements chez un SGC portant sur un fournisseur f2 de manière restrictive. Si la vérification de consentement ne mentionne pas de fournisseur de données explicitement, alors la réponse est négative.

3.2.2 Description du service de récupération des consentements

Ce service permet de récupérer une liste de consentements conformes aux paramètres transmis en entrée. Ce service est notamment utilisé pour afficher les consentements de l'ayant droit dans son portail Agri-consent. Il peut être aussi utilisé pour envoyer une liste de consentements à un bénéficiaire, un fournisseur de données ou un responsable d'enregistrement.

Le service est exposé en GET. En cas d'authentification via OAuth2, le token est préalablement récupéré via le service d'authentification est passé dans le header de la requête.

3.2.2.1 Paramètres transmis en entrée

À l'exception du critère portant sur la date d'activité qui est toujours obligatoire, aucun des critères de recherche n'est obligatoire mais au moins l'un d'eux doit être présent.

Paramètre	Description	Type	Cardinalité	Obligatoire

dataSupplier	Fournisseur des données sujettes aux consentements.	n°SIRET	0..1	non
rightHolder	Ayant-droit ayant accordé des consentements.	n° SIRET n° NUMAGRIT	0..1	non
serviceProvider	Fournisseur de services bénéficiaire des consentements	n°SIRET	0..1	non
collector	Responsable de l'enregistrement des consentements	n°SIRET	0..1	non
family	Famille(s) de données concernées par les consentements	Chaine de caractère	0..20	non
usage	Usage consenti sur les familles de données.	Chaine de caractère	0..1	non
activeAt	Moment auquel les consentements renvoyés doivent être actifs	Date heure	1	oui

3.2.2.2 Réponses attendues

Code	Description
200	Succès, tous les consentements répondant aux critères sont renvoyés. ➔Envoi de la liste de consentements
204	Succès, mais il n'y aucun consentement correspondant aux critères demandés.
400	Requête incohérente. ➔Détail de l'erreur
401	Authentification absente ou invalide.
403	Droits de l'utilisateur insuffisants. Détails

3.2.2.2.1 Description d'un consentement

Le tableau ci-après présente **à titre informatif** les données de description d'un consentement. Le format JSON à respecter pour l'exposition des données de consentement est celui présenté dans le contrat d'interface Open API 3 joint à ce document.

Champs	Description	Type	Obligatoire
id	Identifiant unique du consentement. Cet attribut doit permettre d'identifier uniquement le consentement parmi ceux sous la responsabilité du gestionnaire. Aucune garantie d'unicité globale n'est attendue.	Chaine de caractère	oui
Informations liées aux acteurs autour du consentement			
rightHolder	Identifiant de l'ayant droit ayant donné son consentement	SIRET NUMAGRIT	oui
serviceProvider	Identifiant du ou des fournisseur(s) de services bénéficiaire(s) du consentement.	SIRET	oui
dataSupplier	Identifiant du fournisseur de données.	SIRET	oui
collector	Identifiant du responsable d'enregistrement.	SIRET	oui
additionalIdentifier	Identifiant complémentaire relatif au consentement.	SIRET NUMAGRIT EDE	non
Informations liées à l'usage permis des données			
id	Identifiant du cas d'usage	Chaine de caractère	oui
label	Libellé du cas d'usage	Chaine de caractère	oui
description	Description de l'usage autorisé en texte libre (non normalisé).	Chaine de caractère	non
constraints	Liste des contraintes applicables à ce consentement. Une liste vide équivaut à une liste nulle.	Liste	non
additionalRestrictions	Restrictions supplémentaires en texte libre	Chaine de caractère	non
Informations liées aux données pour lesquelles le consentement est accordé			

id	Identifiant d'une famille de données.	Chaine de caractères	oui
label	Libellé pour cette famille.	Chaine de caractères	oui
Informations liées à la période de validité du consentement			
begin	Date d'entrée en validité.	Date/heure	oui
end	Date d'expiration	Date/heure	non
Information liée au contrat duquel peut dériver le consentement			
contract	Référence permettant d'identifier ce contrat, quand elle est connue.	Chaine de caractères	non

3.2.2.3 Précisions

Numéro	Description	Exemples
1	Les critères doivent être combinés avec un ET logique, c'est à dire que chaque consentement renvoyé doit être conforme à chacun des critères de la requête.	_
2	Les consentements sont renvoyés par le SGC selon une clé de tri déterministe. Le choix de la clé de tri est laissé au SGC mais elle doit garantir que deux requêtes identiques, dans un contexte identique, renvoient les mêmes résultats dans le même ordre.	_
3	Lorsque le consentement a été donné quelque soit le fournisseur de données, les consentements sont réputés être accordés à tout fournisseur de données et l'identifiant réservé à cet usage est utilisé dans la représentation des consentements « urn:agdatahub:agri-consent.eu/data-supplier/any ».	Il existe des consentements chez un SGC qui ont été accordés quelque soit le fournisseur de données. Pour ce SGC et les consentements concernés : Une requête portant sur le fournisseur f1 a pour résultat tous les consentements correspondant aux autres critères de la requête. Les consentements renvoyés sont

		indiqués comme valables pour tous les fournisseurs de données. Une requête sans critère de fournisseur de données a pour résultat tous les consentements correspondant aux autres critères de la requête. Les consentements renvoyés sont indiqués comme valables pour tous les fournisseurs de données.
5	La description des consentements renvoyée en réponse à une requête est exhaustive et indépendante des critères de recherche (la réponse est complète quelque soient les paramètres d'entrée). Tous les attributs sont renseignés avec toutes les valeurs prises pour le consentement représenté.	Il existe chez un SGC un consentement pour l'usage u1 sur les familles de données f1 et f2. En réponse à une recherche de consentements pour l'usage u1 sur la famille f1, le SGC retourne ce consentement en indiquant qu'il est donné pour les deux familles f1 et f2.
6	Le respect des paramètres d'entrée, du caractère obligatoire des données et la conformité de nomenclature des numéro SIRET (algorythme de Luhn) et Numagrit sont contrôlés par le routeur. La réponse du SGC n'est pas transmise si des erreurs sont détectées dans la description des consentements.	

3.2.3 Principes communs aux 2 services

3.2.3.1 Contrôles en amont du routeur

Chaque système acteur interrogeant le routeur est enrôlé par l'administrateur agdatahub avec un rôle dédié et un protocole sécurisé est utilisé pour les échanges OIDC. Le routeur joue le rôle de tiers de confiance et les restrictions opérées en entrée du routeur sont les suivantes :

- Un fournisseur de service bénéficiaire ne peut récupérer ou vérifier en tant que bénéficiaire que les consentements pour lesquels il est bénéficiaire (son propre SIRET est renseigné dans le paramètre serviceProvider)
- Un fournisseur de données ne peut récupérer ou vérifier en tant que fournisseur de données que les consentements pour lequel il est fournisseur de données (son propre SIRET est renseigné dans le paramètre dataSupplier) et les consentements donnés pour tous les fournisseurs de données

- Un responsable d'enregistrement ne peut récupérer en tant que responsable d'enregistrement que les consentements pour lesquels il est responsable d'enregistrement (son propre SIRET est renseigné dans le paramètre collector)

3.2.3.2 Nommage des entités

Cette section décrit la manière dont les entités nommées sont identifiées dans le contrat d'interface. Le principe général est de représenter les entités nommées par des URN afin d'éviter les collisions et de permettre une extension à de nouvelles entités.

On prévoit un espace de nommage propre à Agdatahub nommé « agdatahub ». Cet espace de nommage ne fait pas l'objet d'un dépôt formel à l'IANA pour le moment. Les espaces de nommage normalisés existants sont utilisés de préférence à l'espace de nommage agdatahub. Les SGC sont tenus de représenter les données dans le format indiqué ici, quelle que soit leur représentation interne par le SGC.

3.2.3.2.1 Numéros de Siret

Les numéros de Siret sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe SIRET:. Le numéro Siret est directement accolé à ce préfixe.

Exemple : urn:agdatahub:SIRET:42226020800026

Les numéros de SIRET sont contrôlés par le routeur au travers de l'algorythme de Luhn. Le SGC doit s'assurer que les numéro de SIRET transmis sont conformes.

3.2.3.3 Numéros Numagrit

Les numéros Numagrit sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe NUMAGRIT:. Le numéro Numagrit est directement accolé à ce préfixe.

Exemple urn:agdatahub:NUMAGRIT:A73001002001

La conformité de nomenclature des Numagrit est contrôlée par le routeur. Le SGC doit s'assurer que les Numagrit transmis sont conformes.

3.2.3.4 Numéros EDE

Les numéros EDE (Établissement de l'élevage) sont représentés par un URN dans l'espace de nommage agdatahub. Au sein de l'espace de nommage, ils sont identifiés par le préfixe EDE:. Le numéro EDE est directement accolé à ce préfixe.

Exemple urn:agdatahub:EDE:123456

3.2.3.5 Identification des acteurs

Les acteurs sont identifiés par des attributs spécifiques à leur situation. Ces attributs sont représentés selon le formalisme décrit précédemment.

Ayant-droits

Les ayant-droits sont identifiés par leur n° de Siret ou leur n Numagrit.

Responsables d'enregistrement

Les responsables d'enregistrement sont identifiés par leur n° de Siret.

Fournisseurs de services

Les fournisseurs de service sont identifiés par leur n° de Siret.

Fournisseurs de données

Les fournisseurs de données sont identifiés par leur n° de Siret.

Cas spécifiques

Lorsqu'un consentement est valable pour n'importe quel fournisseur de données, cet identifiant réservé est utilisé à la place de l'identifiant du fournisseur de données : « urn:agdatahub:agri-consent.eu/data-supplier/any ».

3.2.3.6 Référentiel

La version actuelle du système est une première version n'intégrant pas de normalisation des référentiels. Il est prévu qu'un travail d'harmonisation des référentiels (usages, familles de données, contraintes d'usage) soit réalisé dans le cadre du projet NUMAGRI. Cette harmonisation des référentiels aura un impact sur la représentation des données ci-dessous (codification partagée).

3.2.3.6.1 Contraintes d'usage

La représentation des contraintes d'usage ne fait l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de caractères sans formalisme particulier.

3.2.3.6.2 Familles de données

La représentation des identifiants des familles de données ne fait l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de caractères sans formalisme particulier. Le label soit être renseigné pour affichage dans le portail Agri-consent.

Exemples : Données d'élevage

3.2.3.6.3 Catégories d'usage

Les catégories d'usage ne font l'objet d'aucune normalisation dans cette version du système. Leurs identifiants sont formés d'une suite de caractères sans formalisme particulier. Le label soit être renseigné pour affichage dans le portail Agri-consent.

Exemples : Mesure de la performance

3.2.3.7 Traitements – liste des fonctions

Lorsqu'un critère optionnel n'est pas renseigné dans une requête, il est ignoré. Il n'est pas prévu de permettre la construction d'un critère portant sur une valeur nulle ou non renseignée.

3.2.3.8 Cas d'erreur

De manière générale, les SGC sont tenus de respecter le contrat d'interface Open API et les protocoles Internet en vigueur, notamment :

- Les erreurs de traitement causées par un défaut de la requête sont indiquées par un code d'erreur http de la série 400.
- Les erreurs de traitement causées par un défaut du serveur sont indiquées par un code d'erreur http de la série 500.
- Les redirections http (codes de la série 300) seront suivies par le routeur.

Les réponses en cas d'erreur (400 comme 500) sont décrites au format Problem details for HTTP APIs4 dans sa représentation en JSON.

3.2.3.9 Fonctionnement dégradé – reprise

Dans la mesure du possible, un SGC dont le fonctionnement dégradé ne permet plus de rendre le service attendu répond par une erreur http 503. La prise en compte par le routeur agdatahub du délai conseillé avant une nouvelle tentative indiqué par l'entête http Retry-After n'est pas garantie.

Les requêtes envoyées durant l'indisponibilité du SGC ne seront pas renvoyées.