



**MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE**

*Liberté
Égalité
Fraternité*

Secrétariat général

Direction du numérique
pour l'éducation
Sous-direction des services
numériques
Bureau des services et outils
numériques pour l'éducation
(DNE SN1)

99, rue de Grenelle
75357 Paris SP 07

Secrétariat général
Service de l'action
administrative et des
moyens
Sous-direction des achats
(SAAM B)
Bureau de la stratégie
et de l'ingénierie des achats
(SAAM B1)

61-65, rue Dutot
75732 Paris Cedex 15

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

ANNEXE 04.20 : Contrat d'interface EDUGAR & Guichets

Procédure : MEN-SG-AOO-24002

Objet : Prestations de prise en charge de la solution du gestionnaire d'accès aux ressources (GAR), d'hébergement, d'exploitation, de maintenance, de support et de développement de ladite solution pour le compte du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.



**MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS**

*Liberté
Égalité
Fraternité*

Délégation de l'authentification du GAR aux guichets de l'Éducation nationale

Spécifications techniques à destination du GAR

**Version diffusée 2.4
Mai 2022**

Table des matières

1. INTRODUCTION.....	2
2. OFFRE DE SERVICE GUICHETS	3
3. PARCOURS UTILISATEURS	4
3.1. Comptes	4
3.1.1. Élèves	4
3.1.2. Agents.....	4
3.2. Connexion et accès à partir d'un service porté par le GAR.....	5
3.2.1. Phase 1 : choix du fournisseur d'identité.....	5
3.2.2. Phase 2 : authentification.....	5
3.2.3. Phase 3 : accès au service porté par le GAR	6
3.3. Agents : accès à l'IHM d'affectation du GAR à partir d'un portail de l'Éducation nationale	6
3.3.1. Phase 1 : authentification.....	6
3.3.2. Phase 2 : accès au service	6
4. INTERCONNEXION TECHNIQUE	7
4.1. OpenID Connect / OAuth.....	7
4.1.1. Endpoint de récupération de l'identifiant GAR	7
4.2. Schémas des interactions.....	8
4.2.1. Médiacentre	8
4.2.2. Accès à une ressource.....	9
4.2.3. IHM d'affectation du GAR	10
4.3. Guichet élèves : EduConnect	10
4.3.1. Paramètres généraux	10
4.3.2. Endpoints	11
4.3.3. Clients	12
4.3.4. Identité transmise pour les élèves.....	12
4.4. Guichet agents : Hub agent.....	13
4.4.1. Paramètres généraux	13
4.4.2. Endpoints	13
4.4.3. Clients	14
4.4.4. Identité transmise pour les agents	16
5. FONCTIONNALITÉS COMPLÉMENTAIRES	18
5.1. EduConnect.....	18
5.1.1. Accès à la gestion de compte (« self-service »).....	18
5.1.2. Gestion de la déconnexion.....	18
5.1.1. Politique de mot de passe.....	18
5.2. Hub agent	18
5.2.1. Gestion de la déconnexion.....	18
5.2.2. Politique de mot de passe.....	19
5.2.3. Durée de session	19
6. PLATE-FORME DE TESTS POUR LA DÉLÉGATION D'AUTHENTIFICATION À EDUCONNECT	20
7. LEXIQUE	21

1. Introduction

L'Éducation nationale a mis en place des guichets d'authentification nationaux permettant aux services éligibles de déléguer la fonction d'authentification.

Ces guichets permettent de couvrir actuellement les catégories suivantes d'utilisateurs du système d'information de l'Éducation nationale :

- les élèves immatriculés (ayant un INE) scolarisés dans un établissement public ou privé sous contrat (sur la base du volontariat) ;
- les représentants légaux de ces élèves ;
- les agents.

Dans une version ultérieure, les guichets adresseront également les personnes en charge des élèves qui doivent pouvoir accomplir des actes usuels.

Ce document décrit l'offre de service et les modalités techniques d'interconnexion du GAR avec ces guichets pour les utilisateurs suivants :

- les élèves immatriculés (ayant un INE) scolarisés dans un établissement public ou privé sous contrat (sur la base du volontariat) ;
- les agents.

2. Offre de service guichets

On entend par guichets d'authentification de l'Éducation nationale les dispositifs fonctionnels et techniques permettant :

- d'authentifier les utilisateurs : selon le cas d'usage, vérification d'un couple login/mot de passe, délégation d'authentification à FranceConnect, vérification d'une authentification OTP ;
- d'identifier les utilisateurs : leur attribuer un profil fonctionnel et le transmettre au service cible ;
- de gérer les comptes utilisateurs : attribution (par distribution ou auto-enrôlement), activation, modification (par l'utilisateur ou par un administrateur), dépannage (par l'utilisateur ou par une assistance) ;
- de proposer à l'utilisateur l'accès à des services numériques sans réauthentification.

L'interconnexion de ces guichets d'authentification avec le Gestionnaire d'accès aux ressources du MENJS (GAR), sous responsabilité de traitement du MENJS, incluant l'alimentation de ce service par des exports issus des bases académiques AAF, s'effectue par la mise en place d'une fédération d'identité OpenID Connect.

Dans ce cadre, l'Éducation nationale joue le rôle de fournisseur OpenID Connect (OP) et le GAR le rôle de client OpenID Connect (Client).

Plusieurs types de guichets d'authentification sont disponibles en fonction de la population cible :

- élèves et représentants légaux¹ ;
- agents.

Les élèves dans le 1er et 2nd degrés ainsi que les représentants légaux d'enfants scolarisés dans le 1er et le 2nd degrés sont dotés d'une identité unique nationale gérée au travers du dispositif EduConnect.

Les agents de l'Éducation nationale disposent aujourd'hui d'une identité académique. Un dispositif appelé « hub de fédération agents » (appelé Hub agent dans le reste du document) permet de présenter un guichet « unifiant » les identités académiques des agents vis-à-vis des services.

¹ Le présent contrat d'interface s'applique au pilote 1D dont le périmètre n'inclut pas les élèves 2D ni les représentants légaux 1D ou 2D

3. Parcours utilisateurs

Ce chapitre décrit les différents parcours utilisateurs pour accéder au GAR dans l'hypothèse où :

- pour les élèves, le guichet d'authentification est EduConnect ;
- pour les agents, le guichet d'authentification est un des guichets académiques (ou de l'Administration centrale le cas échéant), présentés de manière unique au GAR par l'intermédiaire du Hub agent).

3.1. Comptes

3.1.1. Élèves

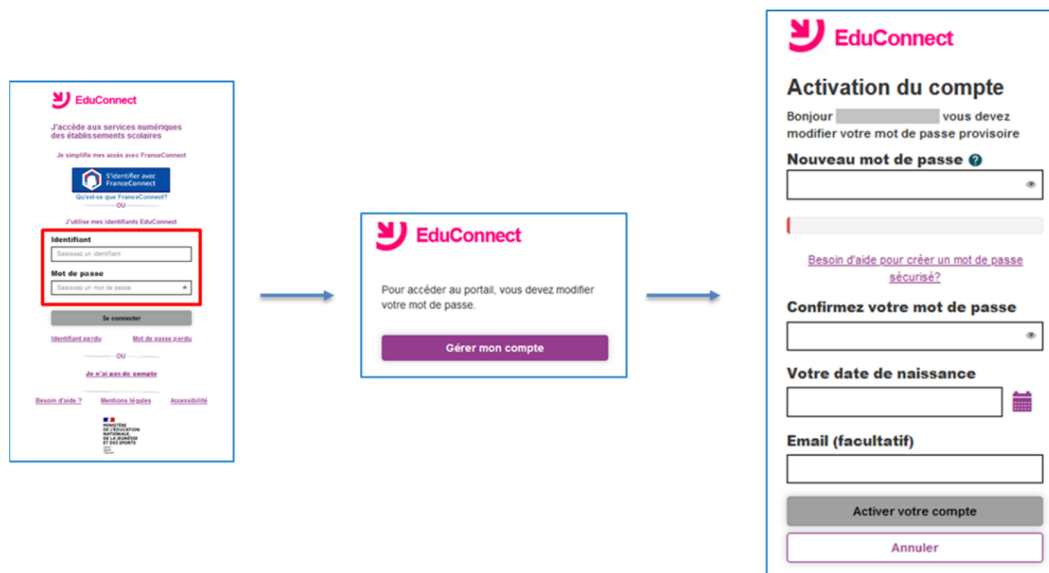


Figure 1 : Activation d'un compte élève par distribution d'un identifiant/mot de passe temporaire

Le directeur d'école, le chef d'établissement ou toute personne habilitée peut, dans l'application d'administration des comptes EduConnect, générer une liste des comptes des élèves, contenant leur identifiant et un mot de passe temporaire, à fournir aux élèves. À la première connexion, l'élève devra modifier le mot de passe fourni et saisir sa date de naissance.

Lors des connexions suivantes, il utilisera l'identifiant qui lui a été communiqué et le mot de passe qu'il aura créé au moment de l'activation de son compte.

3.1.2. Agents

Tout agent de l'Éducation Nationale a une identité fournie par son académie, ou l'Administration centrale pour les agents du ministère.

3.2. Connexion et accès à partir d'un service porté par le GAR

Dans ce scénario, l'utilisateur démarre sa navigation depuis un service porté par le GAR au travers de son URL GAR. Cette URL peut désigner

- l'accès à une ressource mise à disposition au travers du GAR ;
- l'accès à un médiacentre GAR ;
- l'accès à l'IHM d'affectation des ressources (pour les agents seulement).

3.2.1. Phase 1 : choix du fournisseur d'identité

Cette phase est commune aux élèves et aux agents.

Le parcours utilisateur est le suivant :

1. l'utilisateur accède à l'URL GAR du service GAR. Ce lien peut se trouver dans un portail ou tout autre application (ou même depuis les favoris) ;
2. si l'utilisateur possède déjà une session GAR valide, ce dernier amorce le processus nominal d'accès au service (cf. phase 3 ci-dessous) ;
3. si l'utilisateur ne possède pas une session GAR valide :
 - dans le cas où l'URL GAR contient le paramètre indiquant le profil de l'utilisateur (elv, ens...), le GAR redirige l'utilisateur vers le guichet correspondant ;
 - dans le cas contraire, le GAR propose à l'utilisateur une mire de choix du fournisseur d'identité en fonction du profil de l'utilisateur (WAYF : *Where Are You From*) sur lequel l'utilisateur doit cliquer pour initier la fédération d'identité :
 - pour les élèves, le fournisseur d'identité est EduConnect,
 - pour les agents de l'Éducation nationale, le fournisseur d'identité est le Hub agent,
 - pour les autres utilisateurs du service, le fournisseur d'identité peut être celui du service ou d'un fournisseur d'identité tiers – ce cas d'usage est en dehors du périmètre de ce document.

3.2.2. Phase 2 : authentification

3.2.2.1. Éléves

Dans l'étape précédente : l'élève est redirigé vers la page d'authentification d'EduConnect.

Si l'élève dispose déjà d'une session EduConnect valide, l'élève est authentifié et le processus continue avec la phase suivante.

Si l'élève ne dispose pas d'une session EduConnect valide, EduConnect affiche à l'élève la mire de connexion. L'élève saisit son identifiant et son mot de passe et valide.

Si l'identifiant ou le mot de passe saisis sont incorrects, ou si l'utilisateur n'a pas les droits suffisants pour accéder au service, une erreur est affichée et la navigation est interrompue.

Après authentification, l'accès au service se poursuit comme décrit §3.2.3.

3.2.2.2. Agents

Dans l'étape précédente : l'agent est redirigé vers le Hub agent.

Si l'agent dispose déjà d'une session valide sur le Hub agent, l'agent est authentifié et le processus continue avec la phase suivante.

Si l'agent ne dispose pas d'une session valide sur le Hub agent, ce dernier lui affiche une mire de choix (WAYF) permettant à l'agent de sélectionner son fournisseur d'identité (académies et Administration centrale). L'agent est redirigé vers le fournisseur d'identité sélectionné.

Si l'agent dispose déjà d'une session d'authentification valide sur le fournisseur d'identité, il est authentifié et redirigé vers le Hub agent et le processus continue avec la phase suivante.

Si l'agent ne dispose pas d'une session d'authentification valide sur le fournisseur d'identité choisi, celui-ci lui affiche la mire de connexion. L'agent saisit son identifiant et son mot de passe et valide.

Si l'identifiant ou le mot de passe saisis sont incorrects, ou si l'utilisateur n'a pas les droits suffisants pour accéder au service, une erreur est affichée et la navigation est interrompue.

Après authentification, l'accès au service se poursuit comme décrit §3.2.3.

3.2.3. Phase 3 : accès au service porté par le GAR

Cette phase est identique pour les élèves et les agents.

Une fois authentifié, l'utilisateur est automatiquement redirigé vers le GAR, qui crée une session GAR pour l'utilisateur puis amorce le processus nominal d'accès au service. Ce processus est en dehors du périmètre de ce document.

3.3. Agents : accès à l'IHM d'affectation du GAR à partir d'un portail de l'Éducation nationale

Dans ce mode, l'utilisateur démarre sa navigation depuis une URL d'un portail de l'Éducation nationale.

Ce mode de navigation n'étant pas standard dans les cinématiques OpenID Connect, une URL spécifique devra être prévue par le service pour le permettre (voir spécifications techniques plus bas).

3.3.1. Phase 1 : authentification

Dans le cas d'un agent, le portail est ARENA ou le PIA académique.

L'agent saisit l'adresse du portail auquel il souhaite accéder.

Si une session d'authentification est valide, l'agent accède au portail.

S'il n'existe pas de session d'authentification valide, l'agent est redirigé vers la mire de connexion de son fournisseur d'identité académique. L'agent saisit son identifiant et son mot de passe et valide.

Après authentification, l'accès au service se poursuit comme décrit §3.3.2.

3.3.2. Phase 2 : accès au service

Une fois authentifié, l'agent est automatiquement redirigé vers le portail, qui lui présente les liens vers les services numériques disponibles pour l'utilisateur, dont le lien vers l'IHM d'affectation du GAR.

Ce lien (URL technique) doit permettre de réaliser un accès authentifié au service, pour permettre une navigation fluide de l'utilisateur sans devoir repasser par la mire de choix du fournisseur d'identité.

L'utilisateur clique sur ce lien pour accéder au service : il arrive directement authentifié sur le service.

Dans le cas où ce scénario n'est pas retenu, l'accès au service se réalise comme décrit en 3.2.

4. Interconnexion technique

4.1. OpenID Connect / OAuth

La fédération d'identité entre les fournisseurs OpenID Connect (OP) Éducation Nationale et le client OpenID Connect GAR se fera en utilisant l'implémentation du standard OpenID Connect.

Les échanges OpenID Connect utiliseront le mode « authorization_code_flow et si nécessaire le mode « refresh_token flow ».

Optionnellement, le mécanisme « PKCE » avec encodage S256 (code_challenge_method) pourra être utilisé en sécurisation supplémentaire.

Un « vecteur d'identité » sera porteur des éléments permettant de faire le lien avec une identité délivrée par l'OP et celle connue dans le GAR.

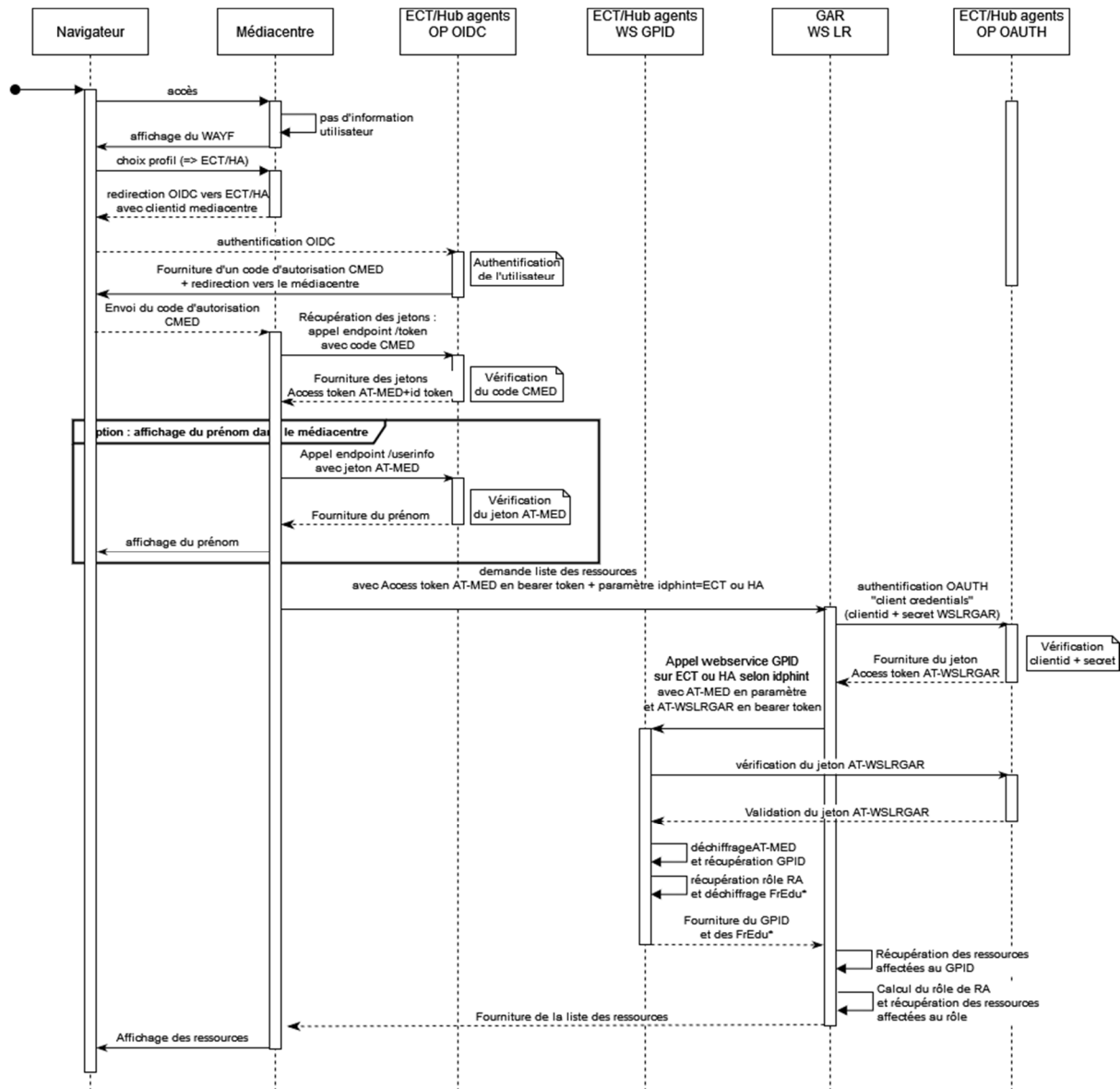
Ce vecteur d'identité sera récupéré par le GAR en retour de l'appel à « userinfo ».

4.1.1. Endpoint de récupération de l'identifiant GAR

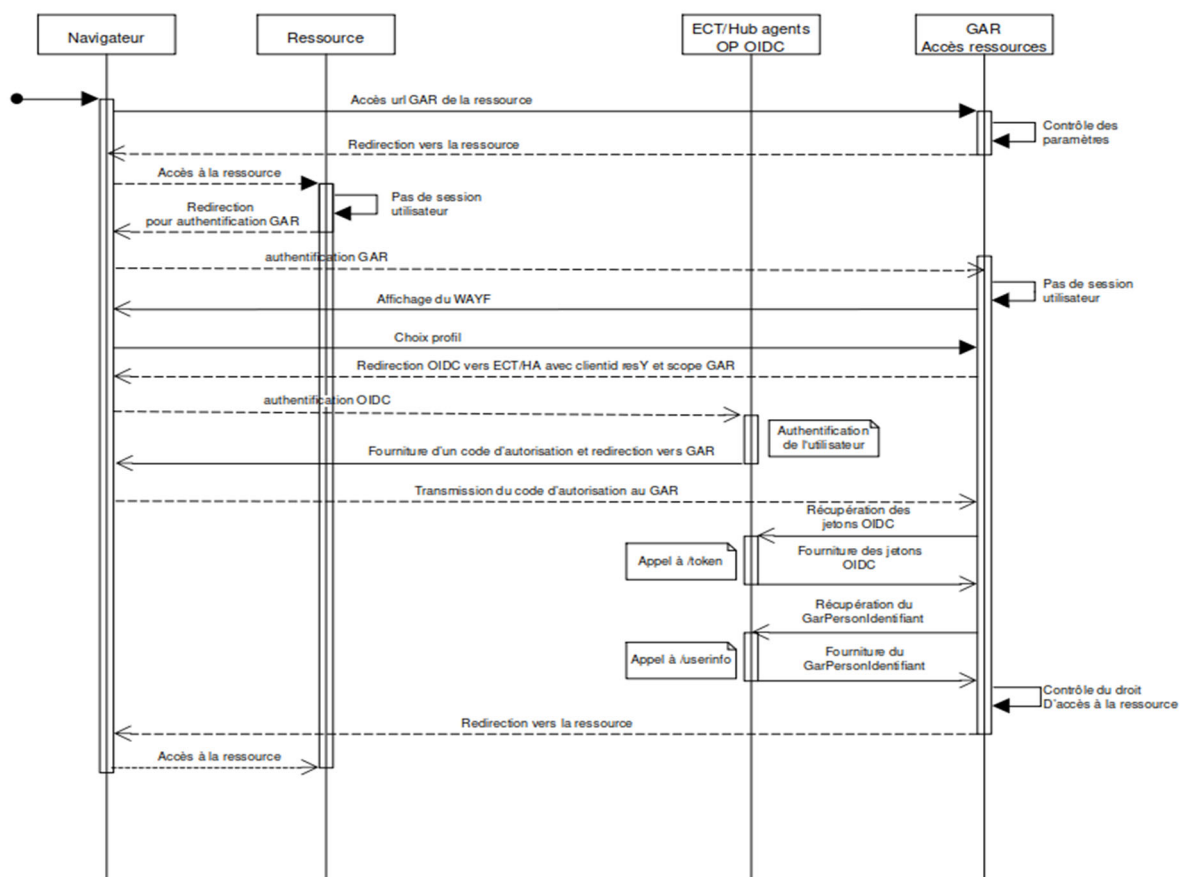
Pour le cas particulier de la récupération par le médiacentre des ressources affectées à l'utilisateur dans le GAR, un endpoint spécifique, protégé par OAuth, est mis à disposition du GAR sur chaque OP et permet la récupération par le Web Service « ListeRessources » du GAR de l'identifiant GAR de l'utilisateur connecté au médiacentre.

4.2. Schémas des interactions

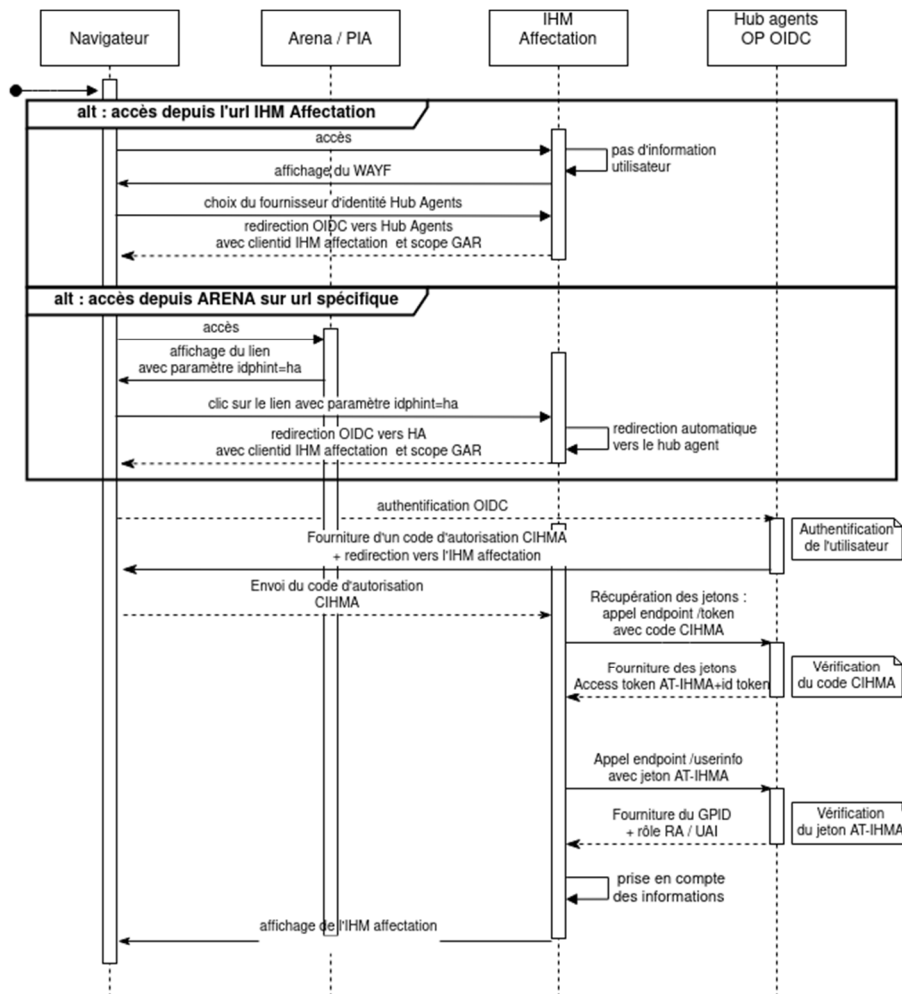
4.2.1. Médiacentre



4.2.2. Accès à une ressource



4.2.3. IHM d'affectation du GAR



4.3. Guichet élèves : EduConnect

Le fournisseur OpenID Connect (OP) est EduConnect, les médiacentres étant clients OpenID Connect.

Le Web Service ListeRessources du GAR est client OAUTH.

4.3.1. Paramètres généraux

Paramètre	Désignation	Valeur
<ECT_OP_BASE_URI>	Base des URL d'interfaçage EduConnect	À fournir par les équipes EduConnect avec
<ECT_OP_ISSUER>	Identifiant du fournisseur OpenIDConnect de EduConnect	À fournir par les équipes EduConnect
<ECT_OAUTH_URI>	URL du serveur OAUTH	À fournir par les équipes EduConnect

<ECT_API_URI>	URL du serveur API	À fournir par les équipes EduConnect
---------------	--------------------	--------------------------------------

4.3.2. Endpoints

Endpoint	Valeur
OIDC - Configuration	<ECT_OP_BASE_URI>/well-known/openid-configuration
OIDC - Autorisation	<ECT_OP_BASE_URI>/idp/profile/oidc/authorize
OIDC - Récupération des tokens	<ECT_OP_BASE_URI>/idp/profile/oidc/token
OIDC - Userinfo	<ECT_OP_BASE_URI>/idp/profile/oidc/userinfo
OIDC - Introspection du token	<ECT_OP_BASE_URI>/idp/profile/oauth2/introspection
OIDC - Logout	<ECT_OP_BASE_URI>/logout
OAUTH - Configuration	<ECT_OAUTH_URI>/auth/realms/omogen/well-known/openid-configuration
OAUTH – Récupération du token	<ECT_OAUTH_URI>/auth/realms/omogen/protocol/openid-connect/token
Récupération de l'identifiant GAR	<ECT_API_URI>/ect/gpid-pr?atmed=X

4.3.2.1. Endpoint de récupération de l'identifiant GAR

4.3.2.1.1. Entrées

Type	Nom	Description
Paramètre GET	atmed	Token associé au GarPersonIdentifiant et fourni au médiacentre Valeur : access token du médiacentre au format urlencodé
Header	Authorization	Token d'autorisation OAUTH Valeur: Bearer <access_token>
Header	IDPHint	Identification du fournisseur du token atmed Valeur : ect

4.3.2.1.2. Sorties

Code retour	Corps de la réponse HTTP	Description
200	{gpid : "valeur"}	Succès : la requête a été correctement traitée
204	vide	La requête a été correctement traitée mais ne retourne aucun résultat
400		Mauvaise requête – La requête était invalide ou ne peut pas aboutir
401		Non autorisé
403		Token OAUTH non valide
412		L'entête de la requête n'est pas valide
500		Erreur interne de l'application

4.3.3. Clients

4.3.3.1. Client OIDC de type médiacentre GAR

Chaque médiacentre est déclaré comme client OIDC sur l'OP EduConnect. Il n'est pas autorisé de partage d'identifiants OIDC entre médiacentres, ni avec le GAR. Le paramétrage est le suivant :

Paramètre	Désignation	Valeur
client_id_medX_ect	Identifiant OIDC du client médiacentre X	À fournir par les équipes EduConnect/Hub agent
client_secret_medX_ect	Secret de connexion OIDC du client médiacentre X	À fournir par les équipes EduConnect/Hub agent
<MEDX_ECT_CLIENT_REDIRECT_URI>	URL de redirection du médiacentre X	À fournir par le médiacentre

4.3.3.1. Client OIDC de type accès aux ressources GAR

L'accès aux ressources GAR est porté par un client OIDC sur l'OP EduConnect. Il n'est pas autorisé de partage d'identifiants OIDC entre clients, ni avec le GAR. Le paramétrage est le suivant :

Paramètre	Désignation	Valeur
client_id_resY_ect	Identifiant OIDC du client Y d'accès aux ressources	À fournir par les équipes EduConnect/Hub agent
client_secret_resY_ect	Secret de connexion OIDC du client Y d'accès aux ressources	À fournir par les équipes EduConnect/Hub agent
<RESY_ECT_CLIENT_REDIRECT_URI>	URL de redirection du client Y d'accès aux ressources	À fournir par le client

4.3.3.2. Client OAUTH WSLR GAR

Le Web Service ListeRessources du GAR s'authentifie en tant que client OAUTH pour accéder au Web Service de récupération de l'identifiant GAR

Paramètre	Désignation	Valeur
client_id_gar_ect_oauth	Identifiant OAuth du client GAR	À fournir par les équipes EduConnect/Hub agent
client_secret_gar_ect_oauth	Secret de connexion OAUTH du client GAR	À fournir par les équipes EduConnect/Hub agent

4.3.4. Identité transmise pour les élèves

Le format EduConnect de l'identité transmise pour les élèves est le suivant :

	Claims	Description	GAR	Médiacentre
id_token	sub	Valeur chiffrée de l'identifiant interne ECT, unique par client Format : chaîne de 256 caractères UTF-8	X	X

Scope	Claims	Description	GAR	Médiacentre
ect.scope.gar	FrEduCtEleveINEHash	Hash de l'INE Format : chaîne de 32 caractères UTF-8	X	
ect.scope.cnx	FrEduCtDateConnexion	Date de dernière connexion de l'utilisateur Format : AAAA-MM-JJ HH:mm:ss	X	X
	FrEduOrigAuth	Origine de l'authentification courante Format : valeur ECT ou ECT-FC	X	X
	FrEduUrlRetour	URL de retour Format : <i>url</i>	X	X
ect.scope.med	givenName	Prénom de l'élève à des fins de personnalisation de l'affichage		X

4.4. Guichet agents : Hub agent

Le fournisseur OpenID Connect (OP) est le hub de fédération agents, les médiacentres et l'IHM d'affectation du GAR étant clients OpenID Connect.

4.4.1. Paramètres généraux

Paramètre	Désignation	Valeur
<HUB_OP_BASE_URI>	Base des URL d'interfaçage avec le Hub agent	À fournir par les équipes Hub agent
<HUB_OP_ISSUER>	Identifiant du fournisseur OpenIDConnect du Hub agent	À fournir par les équipes Hub agent
<HUB_OAUTH_URI>	URL du serveur OAUTH	À fournir par les équipes EduConnect
<HUB_APIM_URI>	URL du serveur API Manager	À fournir par les équipes Hub agent

4.4.2. Endpoints

Endpoint	Valeur
OIDC - Configuration	<HUB_OP_BASE_URI>/well-known/openid-configuration
OIDC - Autorisation	<HUB_OP_BASE_URI>/idp/profile/oidc/authorize
OIDC - Récupération des tokens	<HUB_OP_BASE_URI>/idp/profile/oidc/token
OIDC - Userinfo	<HUB_OP_BASE_URI>/idp/profile/oidc/userinfo

Endpoint	Valeur
OIDC - Introspection du token	<HUB_OP_BASE_URI>/idp/profile/oauth2/introspection
OIDC - Logout	<HUB_OP_BASE_URI>/logout
OAUTH - Configuration	<HUB_OAUTH_URI>/auth/realms/omogen/.well-known/openid-configuration
OAUTH – Récupération du token	<HUB_OAUTH_URI>/auth/realms/omogen/protocol/openid-connect/token
Récupération de l'identifiant GAR	<HUB_OP_BASE_URI>/hub-agent/gpid-pr?atmed=X

4.4.2.1. Endpoint de récupération de l'identifiant GAR

4.4.2.1.1. Entrées

Type	Nom	Description
Paramètre GET	atmed	Token associé au GarPersonIdentifiant et fourni au médiacentre Valeur : access token du médiacentre au format urlencodé
Header	Authorization	Token d'autorisation OAUTH Valeur: Bearer <access_token>
Header	IDPHint	Identification du fournisseur du token atmed Valeur : ha

4.4.2.1.2. Sorties

Code retour	Corps de la réponse HTTP	Description
200	{ gpid: "valeur", FrEduResDel: ["valeur1", "valeur2", "valeur3"], FrEduRneResp: ["valeur", "valeurb"], FrEduFonctAdm : ["DIR"] }	Succès : la requête a été correctement traitée voir § 4.4.4.1 pour le détail
204	vide	La requête a été correctement traitée mais ne retourne aucun résultat
400		Mauvaise requête – La requête était invalide ou ne peut pas aboutir
401		Non autorisé
403		Token OAUTH non valide
412		L'entête de la requête n'est pas valide
500		Erreur interne de l'application

4.4.3. Clients

4.4.3.1. Client OIDC de type médiacentre GAR

Chaque médiacentre est déclaré comme client OIDC sur l'OP du Hub agent. Il n'est pas autorisé de partage d'identifiants OIDC entre médiacentres, ni avec le GAR.

Le paramétrage est le suivant :

Paramètre	Désignation	Valeur
client_id_medX_hub	Identifiant OIDC du client médiacentre X	À fournir par les équipes EduConnect/Hub agent
client_secret_medX_hub	Secret de connexion OIDC du client médiacentre X	À fournir par les équipes EduConnect/Hub agent
<MEDX_HUB_CLIENT_REDIRECT_URI>	URL de redirection du médiacentre X	À fournir par le médiacentre

4.4.3.2. Client OIDC de type accès aux ressources GAR

L'accès aux ressources GAR est porté par un client OIDC sur l'OP Hub agent. Il n'est pas autorisé de partage d'identifiants OIDC entre clients, ni avec le GAR. Le paramétrage est le suivant :

Paramètre	Désignation	Valeur
client_id_resY_hub	Identifiant OIDC du client Y d'accès aux ressources	À fournir par les équipes EduConnect/Hub agent
client_secret_resY_hub	Secret de connexion OIDC du client Y d'accès aux ressources	À fournir par les équipes EduConnect/Hub agent
<RESY_HUB_CLIENT_REDIRECT_URI>	URL de redirection du client Y d'accès aux ressources	À fournir par le client

4.4.3.3. Client OIDC IHM d'affectation du GAR

L'IHM d'affectation du GAR est déclarée comme client OIDC sur l'OP du Hub agent. Il n'est pas autorisé de partage d'identifiants OIDC entre médiacentres, ni avec le GAR.

Paramètre	Désignation	Valeur
client_id_gar_hub	Identifiant OIDC du client GAR	À fournir par les équipes EduConnect/Hub agent
client_secret_gar_hub	Secret de connexion OIDC du client GAR	À fournir par les équipes EduConnect/Hub agent
<GAR_HUB_CLIENT_REDIRECT_URI>	URL de redirection du GAR	À fournir par le GAR
<GAR_HUB_CLIENT_IDP_INIT_URI>	URL permettant une connexion de type « idp initiated »	OPTIONNELLE À fournir par le GAR

La cinématique assimilée au mode « idp initiated » présent dans les fédérations SAML pourra être mise en place si le paramètre <GAR_HUB_CLIENT_IDP_INIT_URI> est fourni.

Dans ce cas, cette URL sera appelée avec un paramètre idphint=ha et devra déclencher un appel à l'URL d'autorisation correspondante, sans action de l'utilisateur.

La valeur du paramètre idphint devra être connue et vérifiée par le GAR pour éviter toute tentative de redirection vers un service illicite.

4.4.3.1. Client OAUTH WSLR GAR

Le Web Service ListeRessources du GAR s'authentifie en tant que client OAUTH pour accéder au Web Service de récupération de l'identifiant GAR

Paramètre	Désignation	Valeur
client_id_gar_hub_oauth	Identifiant OAuth du client GAR	À fournir par les équipes EduConnect/Hub agent
client_secret_gar_hub_oauth	Secret de connexion OAUTH du client GAR	À fournir par les équipes EduConnect/Hub agent

4.4.4. Identité transmise pour les agents

Le format Hub agent de l'identité transmise pour les agents est le suivant

	Claims	Description	GAR	Médiacentre
id_token	sub	Valeur chiffrée de l'identifiant interne Hub agent, unique par client Format : chaîne de 256 caractères UTF-8	X	X

Scope	Claims	Description	GAR	Médiacentre
hub.scope.gar	FrEduNumenHash	Hash du NUMEN Format : chaîne de 32 caractères UTF-8	X	
hub.scope.aff	FrEduFonctAdm FrEduRneResp FrEduResDel	Attributs portant les informations sur le rôle de RA 2D et les UAI concernés, voir § 4.4.4.1	X	
hub.scope.cnx	FrEduDateConnexion	Date de dernière connexion de l'utilisateur Format : AAAA-MM-JJ HH:mm:ss	X	X
	FrEduUrlRetour	URL de retour Format : <i>url</i>	X	X
hub.scope.med	givenName	Prénom de l'agent à des fins de personnalisation de l'affichage Note : ce scope contient également des claims techniques internes au hub qui sont à ignorer par le médiacentre		X

4.4.4.1. Définition du rôle de RA dans le 2D

Le rôle de RA dans le 2D est porté de plein droit par les chefs d'établissements et adjoints, dans ce cas, ce sont les attributs (claims) suivants qui contiennent les informations nécessaires :

- **FrEduFonctAdm**
 - Monovalué
 - La seule valeur acceptable est **DIR**
- **FrEduRneResp**
 - Multivalué avec une valeur par établissement en responsabilité
 - Format : <UAI établissement >\$<UAA ou UAJ>\$<PU ou PR>\$<Flag activité N ou A ou F>\$T<1er chiffre du code TNA>\$<code TTY>\$<code TNA>
 - Valeur composée des éléments suivants, séparés par « \$ » :

- **l'UAI de l'établissement en responsabilité**
- le type administratif
- la catégorie (PU pour public ou PR pour privé)
- **le statut en activité de l'utilisateur (N normal ou A anticipé ou F pour final) : la valeur « N » signifie que l'utilisateur est en responsabilité à ce moment**
- la lettre T suivi du 1er chiffre du code TNA de l'établissement,
- le code TTY de l'établissement (nomenclature BCN : N_TYPE_UAI) exemple : "LYC" pour Lycée
- le code TNA de l'établissement (nomenclature BCN : N_NATURE_UAI)
- Exemple de valorisation : **0120002M\$UAJ\$PU\$N\$T3\$CLG\$340**

Le rôle de RA dans le 2D peut être également attribué par délégation du chef d'établissement à un personnel de l'établissement, en utilisant l'application DelegCE2. Dans ce cas, c'est l'attribut (claim) suivant qui contient les informations nécessaires :

FrEduResDel

- Multivalué avec une valeur par ressource déléguée (Liste des codes UAI de l'établissement, chaque code étant accompagné de la fonction déléguée = FrEduFonctAdm).
- Format :
<nomappli>|<nomressource>|<datedebut>|<datefin>|<delegant>|<fredurnerresp>|<idserveur>|<fonctiondeleguee>|
- Valeur composée des éléments suivants, séparés par « | » :
 - Nom de l'application : **garaffectation**
 - Nom de la ressource :
/mdp/redirectionhub/redirect.jsp?applicationname=garaffectation
 - **Date de début de validité** de la délégation au format jj/mm/aaaa
 - **Date de fin de validité** de la délégation au format jj/mm/aaaa (peut être valorisée à 31/12/9999)
 - Identifiant du délégant : uid LDAP
 - FrEduRneResp=<...> : FrEduRneResp du délégant séparés par un « ; »
 - Zone serveur
 - (optionnel) FrEduFonctAdm du délégant : doit être DIR si présent
- Exemple de valorisation : **garaffectation
/mdp/redirectionhub/redirect.jsp?applicationname=garaffectation|06/11/2021|31/12/9999|pdupont|FrEduRneResp=0120002M\$UAJ\$PU\$N\$T3\$CLG\$340|rev-proxy-dmz||**

5. Fonctionnalités complémentaires

5.1. EduConnect

5.1.1. Accès à la gestion de compte (« self-service »)

L'accès à la gestion de compte EduConnect est possible depuis un médiacentre ou un service du GAR.

Deux fonctionnements sont possibles :

- sans bouton permettant le retour vers le service, l'URL (en production) est alors de la forme **`https://moncompte.educonnect.education.gouv.fr/`**
- avec bouton permettant le retour vers le service, l'URL (en production) est alors de la forme **`https://educonnect.education.gouv.fr/educt-redirect/redirect?urlEduconnect=https://moncompte.educonnect.education.gouv.fr/&urlRetour=<url de retour vers le service>`**

Cette URL comporte un paramètre à renseigner avec l'URL de retour vers le service. Celle-ci doit être préalablement connue d'EduConnect et déclarée en « liste blanche ».

5.1.2. Gestion de la déconnexion

Deux fonctionnements sont possibles :

- sans bouton permettant le retour vers le service, l'URL (en production) est celle spécifiée dans les endpoints décrits en 4.3.2 ;
- avec bouton permettant le retour vers le service, l'URL (en production) est alors de la forme **`https://educonnect.education.gouv.fr/educt-redirect/redirect?urlEduconnect=<url de déconnexion spécifiée en 4.3.2.>/&urlRetour=<url de retour vers le service>`**

Cette URL comporte un paramètre à renseigner avec l'URL de retour vers le service. Celle-ci doit être préalablement connue d'EduConnect et déclarée en « liste blanche ».

5.1.1. Politique de mot de passe

La politique de mot de passe est d'au moins 8 caractères et au moins 3 des quatre critères suivants : 1 minuscule, 1 majuscule, 1 chiffre, 1 caractère spécial parmi `!@#*$(){}[]`

5.2. Hub agent

5.2.1. Gestion de la déconnexion

L'identité transmise comporte un attribut `FrEduUrlRetour`, qui contient le lien vers lequel renvoyer l'utilisateur après déconnexion du service.

De plus, la déconnexion du Hub agent peut être provoquée en appelant l'URL spécifiée dans les endpoints décrits en 4.4.2.

5.2.2. Politique de mot de passe

La politique de mot de passe est spécifique à chaque académie.

5.2.3. Durée de session

La durée de la session d'authentification du Hub agent est de 1h. La durée de la session d'authentification des fournisseurs d'identité académiques est de la responsabilité de chaque académie.

6. Plate-forme de tests pour la délégation d'authentification à EduConnect

Cette partie sera complétée ultérieurement.

7. Lexique

AAF (Annuaire Académique Fédérateur) : dispositif permettant l'export d'information issues des systèmes d'information académiques vers des partenaires

ARENA – Portail d'Accès aux Ressources de l'Éducation Nationale et aux ressources Académiques

GPID – GARPersonIdentifiant – Identifiant unique GAR de l'utilisateur, généré par les ENT pour les projets ENT et utilisation de l'INE et du NUMEN hashés pour les utilisateurs hors projet ENT

OTP (One Time Password) : périphérique physique ou logiciel permettant une authentification substantielle à deux facteurs

OIDC – OpenID Connect

OP : OpenID Connect Provider (fournisseur d'identité OpenID Connect)

PIA – Portail Intranet Académique

SSO – Single-Sign-On

WAYF – Service de découverte Were Are You From

WSLR – Web Service ListeRessources