



**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 08.0** : Exemple d'expression de besoins applications natives

**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.



# **GAR**

## **Gestionnaire d'Accès aux Ressources**

---

### **Expression de besoin : Gestion des applications natives**

Historique des mises à jour :

Version	Date	Mises à jour	Auteur	Société
00.01	21/01/2022	Création	RENATER	RENATER
00.02	21/01/2022	Modification	RENATER	RENATER
00.03	01/02/2022	Modification	RENATER	RENATER
00.04	03/02/2022	Modification	RENATER	RENATER
01.00	04/02/2022	Version validée	RENATER	RENATER

Historique des diffusions :

Version	Date	Objectif	Destinataires/Sociétés

Historique des validations

Version	Date	Responsable	Commentaires

## Table des matières

1.	Introduction .....	3
1.1.	Objet du document.....	3
1.2.	Systèmes impactés.....	3
1.3.	Mode de réalisation souhaité .....	3
1.4.	Documents de référence.....	3
1.5.	Glossaire .....	3
2.	Expression du besoin.....	3
2.1.	Définition du périmètre .....	3
2.2.	Rappel du contexte .....	3
2.3.	Objet .....	4
2.4.	Exigences fonctionnelles .....	4
2.4.1.	Contexte d'application.....	4
2.4.2.	Principes d'authentification « par le GAR » .....	4
2.4.3.	Principe d'affectation.....	6
2.4.4.	Ressources « mixtes ».....	6
2.4.5.	Ressources avec Backend .....	6
2.4.6.	Gestion du mode hors ligne .....	6
2.4.7.	Propagation de la déconnexion .....	7
2.4.8.	Statistiques .....	7
2.5.	Exigences techniques .....	7
2.5.1.	Protocoles SSO utilisés .....	7
2.5.2.	Sécurisation des échanges entre le GAR et les applications natives .....	7
2.5.3.	Principes d'architecture.....	7
2.5.4.	Utilisation des notices .....	8
2.6.	Prérequis tiers.....	8
2.6.1.	Prérequis éditeurs de ressources .....	8
2.6.2.	Prérequis éditeurs de médiacentres .....	9
2.7.	Livrables.....	9
3.	Planning .....	9
4.	Annexe.....	9

## 1. Introduction

### 1.1. Objet du document

Ce document constitue l'expression de besoin d'évolution du GAR afin qu'il permette l'accès aux ressources de type application native dans des conditions similaires à celles des accès aux ressources actuellement accessible depuis les navigateurs web.

Référence de l'évolution : 239

### 1.2. Systèmes impactés

Cette évolution impacte le GAR ainsi que les applications natives développées par les éditeurs de ressources qui devront respecter un certain nombre de contraintes imposées par le GAR afin de se rendre compatible avec ce dernier.

Les tiers (ENT, solutions de vie scolaire ...) implémentant un Médiacentre relié au GAR pourront également le mettre à jour afin de bénéficier de l'ensemble des apports de la présente évolution et de permettre l'ouverture des applications natives.

### 1.3. Mode de réalisation souhaité

La réalisation est souhaitée dans un mode cycle en V.

### 1.4. Documents de référence

N°	Version et/ou Date	Réf. Document	Type
1	N/A	<a href="https://sourcesup.renater.fr/nuxeo/ui/#!/doc/3951399b-d213-435f-925f-3642e72eb13a">https://sourcesup.renater.fr/nuxeo/ui/#!/doc/3951399b-d213-435f-925f-3642e72eb13a</a>	Ensemble des sources des études et POC réalisés sur le sujet dans le cadre du marché S#1 du GAR

### 1.5. Glossaire

Abréviation	Signification
OIDC	Open ID Connect
DCP	Données à caractère personnel
EIM	Equipement Internet Mobile

## 2. Expression du besoin

### 2.1. Définition du périmètre

La présente évolution traite des applications natives. Il est entendu par application native, toute application qui n'est pas uniquement accessible depuis un navigateur web et qui nécessite une installation sur l'appareil de l'accédant (EIM, ordinateur ...).

La présente évolution ne traite que de la problématique de l'accès à la ressource de type application native et non pas de sa mise à disposition ou de son installation. C'est-à-dire que la distribution et l'installation de ce type de ressource sur les appareils (EIM, ordinateur ...) sont de la responsabilité de leurs propriétaires, qu'il s'agisse d'un appareil de parc établissement ou familial/personnel.

### 2.2. Rappel du contexte

Une partie des ressources numériques pédagogiques sont disponibles sous d'autres formes que des applications web (ex : applications mobiles (IOS, Android ou autre), applications desktop (Windows, MacOS, Linux ...)) et ne sont donc pas adressées par la version actuelle du GAR qui ne gère que les ressources accessibles au travers d'un navigateur web. Cette problématique est, à date, particulièrement sensible dans les territoires pour lesquels l'ensemble des manuels numériques sont disponibles sous forme d'applications natives. De plus, ces applications sont développées par les éditeurs de ressources de façon hétérogène, elles proposent en général une installation sur l'appareil de l'accédant qui permet d'accéder à un ensemble de services spécifiques et contenus, accédés donc en ligne ou en local avec une synchronisation à la reconnexion (exemple Educad hoc de Hachette livre). Ces applications délivrent leur propre jeton de session indépendamment du GAR à date et les accès aux ressources ne sont donc pas protégés au même niveau que les accès en ligne via le GAR.

## **2.3. Objet**

La problématique évoquée a été identifiée depuis le démarrage du GAR et a fait l'objet, en 2019, dans le cadre du premier marché GAR, d'un travail de levée de risque sous forme de prototypes. L'objet de cette expression de besoin consiste principalement en l'industrialisation des prototypes réalisés afin de permettre à la solution GAR d'apporter une réponse satisfaisante à tous les cas d'usage d'accès à toutes les ressources de type applications natives.

## **2.4. Exigences fonctionnelles**

### **2.4.1. Contexte d'application**

Cette évolution est liée à la mise à disposition pour les éditeurs de ressources compatibles avec les prérequis qui seront spécifiés par le GAR, tant sur les aspects techniques (objet de la présente expression de besoin), que sur les aspects contractuels (hors périmètre de la présente expression de besoin et adressés directement par le MENJS). En dehors de ce point, les principes de fonctionnement actuels du GAR doivent être respectés tout en prenant compte des particularités liées aux 2 cas de figures suivants :

- Cas 01 : Accès depuis un médiacentre :
  - Si l'application native correspondant à la ressource proposée est installée sur le terminal c'est cette dernière qui s'ouvre lors de l'appel depuis le lien médiacentre
  - Si l'application native correspondant à la ressource proposée n'est pas installée sur le terminal c'est la page web fournie par l'éditeur qui s'ouvre lors de l'appel depuis le lien médiacentre.
- Cas 02 : Accès depuis l'application native :

Cette évolution introduit la notion « d'application first » qui permet d'initier la séquence d'accès à l'application native directement depuis cette dernière sans passer par le médiacentre.

  - Si une session GAR est valide au moment de l'accès, l'application native s'ouvre directement
  - Si aucune session GAR n'est valide au moment de l'accès, l'application native proposera une page d'authentification incluant, a minima, une authentification « par le GAR » qui renverra par l'intermédiaire du GAR, après contextualisation (établissement et profil), vers le guichet d'authentification correspondant

Il est à noter que l'éditeur pourra choisir de ne « GARifier », c'est-à-dire de ne protéger par une session GAR valide, qu'un sous-ensemble de l'application native qu'il met à disposition.

### **2.4.2. Principes d'authentification « par le GAR »**

Mise en place d'une fonction simple de type WAYF portée par le GAR dont l'objectif est de permettre à l'utilisateur de l'application native de choisir son établissement de « rattachement » (celui dans le contexte duquel il souhaite consulter l'application native) et son profil (élève, agent) afin d'initier sa séquence d'authentification en passant les paramètres UAI & profil associés.

Principe de fonctionnement :

Cas d'usage 01 – première connexion à l'application native :

- L'application présente un bouton « *GAR Connect* » suivi du texte « *choix de l'établissement & du profil* »
- Lorsque l'utilisateur clique sur le bouton « *GAR Connect* », une page web, fournie par le GAR, s'ouvre dans son navigateur web. Cette page contient :
  - Logo simple et texte de présentation
  - Une cellule vide de type drop down (avec bouton de type flèche vers le bas) :
    - Un clic sur le bouton de type flèche fera apparaître sur une taille d'écran la liste de tous les établissements présents dans le GAR explicitement nommés et classés dans un ordre à préciser qui pourra être similaire à ce qui a été fait pour le médiacentre GAR
    - Le fait de sélectionner un établissement dans la liste le fait s'afficher dans la cellule de la drop down
    - Le fait de taper du texte dans la cellule de la drop down agit comme une recherche dynamique dans la liste des établissements permettant de restreindre la liste présentée aux établissements contenant la chaîne de caractères saisie
  - 2 boutons de connexion, a priori à droite de la cellule de type drop down
    - Un bouton pour se connecter en tant qu'élève et un autre tant qu'Agent
    - Un clic sur un des boutons de connexion permettra d'initier la séquence d'authentification auprès du GAR avec l'UAI de l'établissement sélectionné ainsi que le profil choisi
    - Les boutons ne sont actifs que si un établissement a été sélectionné

Cas d'usage 02 – deuxième (ou plus) connexion à l'application native :

- L'application présente 2 boutons :
  - Un bouton « *GAR Connect* » suivi du texte « *nom de l'établissement* » et « *nom du profil* »
    - La valeur de « *nom de l'établissement* » correspond au dernier établissement avec lequel l'utilisateur s'est connecté
    - La valeur de « *nom du profil* » correspond au dernier profil avec lequel l'utilisateur s'est connecté
    - Un clic sur le bouton « *GAR Connect* » permet d'initier la séquence d'authentification auprès du GAR avec l'UAI correspondant au dernier établissement avec lequel l'utilisateur s'était connecté ainsi que le profil associé
  - Un bouton « *GAR Connect* » suivi du texte « *choix de l'établissement* » et « *nom du profil* »
    - Voir cas d'usage 01

Remarques :

- Le wording et le Look & Feel final du bouton « *GAR Connect* » seront à finaliser en phase de conception. La réalisation graphique proprement dite sera à la charge de Worldline.
- Le wording final et le Look & Feel du texte « *choix de l'établissement* » et « *choix du profil* » seront à la charge des éditeurs mais devront être spécifiés en terme de fonctionnement dans la documentation.

- Le principe de fonctionnement pourra être adapté en phase de conception afin d'être optimisé, notamment pour faciliter la sélection de l'établissement
- D'une manière générale une phase de maquettage du WAYF sera à proposer

### 2.4.3. Principe d'affectation

Aucune évolution de l'IHM d'Affectation n'est demandée. L'affectation des ressources de type application native se fera de la même façon que les autres ressources.

### 2.4.4. Ressources « mixtes »

Certaines ressources numériques s'exposent à la fois dans un navigateur web mais également au travers d'applications natives spécifiques aux OS sur lesquelles elles s'exécutent. Si techniquement une même ressource numérique peut donc correspondre à plusieurs applications techniques, elle devra toutefois être gérée par le GAR comme une seule ressource pédagogique. C'est à dire qu'elle ne sera décrite que dans une seule notice, ne sera à affecter qu'une seule fois à un accédant et sera présentée de façon unique par le ws Liste\_Ressources.

### 2.4.5. Ressources avec Backend

Les applications natives qui fonctionnent avec une partie serveur, ou backend, devront, dans le cas où ce dernier nécessite l'obtention de DCP pour fonctionner, déclarer ce backend comme une ressource dans le GAR. L'utilisation du webservice RAA sera proposée pour faire le lien entre l'application native et son backend.

La transmission des DCP ne pourra toutefois se faire qu'au travers du GAR. C'est-à-dire qu'une application et son backend ne pourront pas échanger directement des DCP.

### 2.4.6. Gestion du mode hors ligne

L'évolution doit proposer aux applications natives une possibilité de gestion du mode hors ligne qui réponde aux contraintes suivantes :

- Internet accessible depuis le terminal mais session périmée : l'application native doit demander la connexion avec le GAR pour accéder à son contenu « GARifié ». Sauf si l'utilisateur souhaite volontairement travailler hors ligne. Dans ce cas l'application native ne doit pas communiquer avec des tiers techniques pour sa partie « GARifiée » et le jeton de session « hors ligne » doit être toujours valide
- Internet non accessible depuis le terminal et session périmée depuis moins de la *durée max d'accès hors ligne* : l'utilisateur accède au contenu « GARifié » de l'application native sans devoir se connecter. L'application native fonctionne alors hors GAR, soit hors du cadre de confiance GAR.
  - Si Internet devient accessible, depuis le terminal, pendant l'utilisation de l'application native aucune demande de connexion ne doit être faite. La demande de connexion sera à faire au prochain « réveil » de l'application native
- Internet non accessible depuis le terminal et session périmée depuis plus de la *durée max d'accès hors ligne* : l'utilisateur n'a plus accès au contenu « GARifié » de l'application native et doit « trouver » un accès réseau pour se reconnecter avec le GAR.

La *durée max d'accès hors ligne* est la durée pendant laquelle on accepte que l'application native puisse être accédée en mode hors ligne sans nouvelle authentification au GAR. Cette durée est un paramètre de l'application native fourni par l'éditeur de ressource sur la base des recommandations de la DNE.

Cette gestion du mode hors ligne sera à décrire précisément dans la documentation à destination des éditeurs de ressources.

#### **2.4.7. Propagation de la déconnexion**

Il est demandé de ne pas implémenter la déconnexion depuis le GAR vers les applications natives. Il est par contre attendu de permettre et de propager la déconnexion depuis les applications natives vers le GAR puis vers les guichets/ENT/services du GAR. Aucun accusé de prise en compte de la demande de déconnexion ne sera à renvoyer par le système appelé.

Les applications natives devront donc implémenter un bouton de déconnexion pour initier la séquence décrite ci-dessus.

#### **2.4.8. Statistiques**

Les statistiques devront permettre une présentation des accès aux applications natives distincte et cumulée des autres accès.

### **2.5. Exigences techniques**

#### **2.5.1. Protocoles SSO utilisés**

L'évolution devra fonctionner en OIDC & OAuth2 entre le GAR et les applications natives et devra respecter les standards de ces protocoles.

Les communications entre le GAR et les fournisseurs de données d'identité (ENT, RDMEN), les médiacentres et les guichets d'authentification (ECT, HA) ainsi que celles entre le GAR et les ressources accessibles dans un navigateur web ne devront pas être impactées.

Le type de flow OIDC (authentication ou basic) implémenté sera à préciser et devra être conforme à ce qui est mis en œuvre par les guichets ECT et HA.

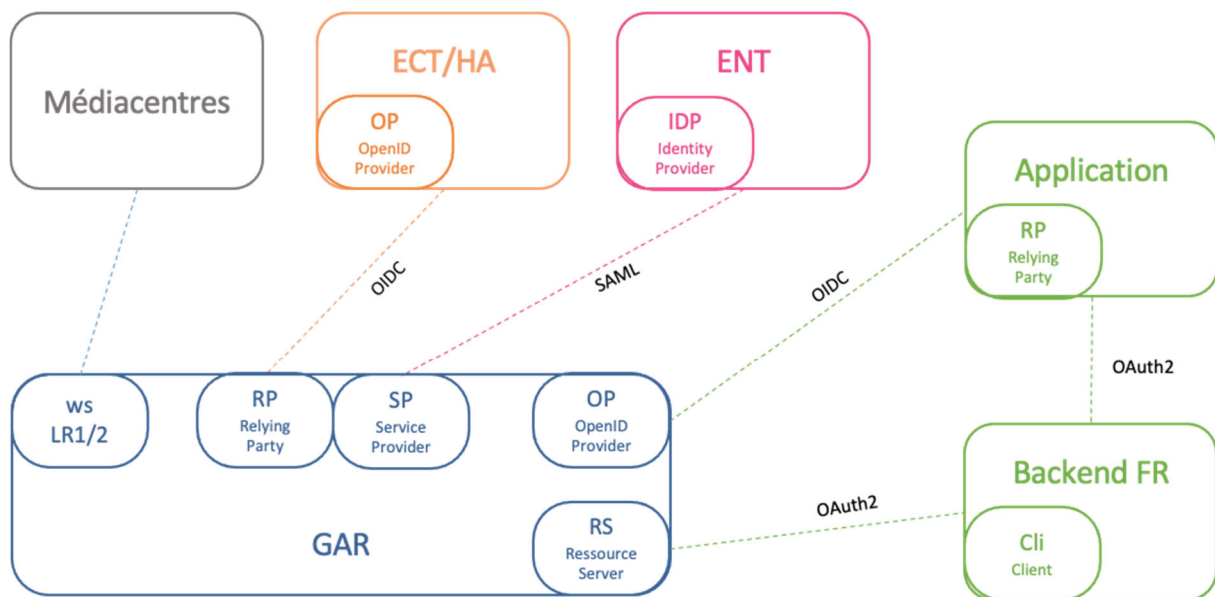
#### **2.5.2. Sécurisation des échanges entre le GAR et les applications natives**

L'utilisation de *Proof Key for Code Exchange* (PKCE) est recommandée.

#### **2.5.3. Principes d'architecture**

Le service d'accès aux ressources accessible aux applications natives en OIDC sera idéalement séparé du service d'accès aux ressources « classiques » GAR (ressources accessibles dans un navigateur web).





### 2.5.4. Utilisation des notices

L'information du caractère « application native » d'une ressource sera à décrire par les éditeurs dans les notices. L'utilisation, possiblement multiple, de bloc « extendedLocation » pour en spécifier les attributs permettra de ne pas faire évoluer le format actuel. Ces attributs seront à minima les suivants :

- Caractère « application native » de la ressource
- Lien vers l'application native installée (par OS)
- url de repli
- 2 autres valeurs qui seront à déterminer en phase de conception

Exemple d'utilisation du bloc « extendedLocation » :

```
<scolomfr:extendedLocation>
  <!-- scolomfr:location transformée pour fournir l'url de redirection -->
  <scolomfr:location>https://www.effios.fr/android\_gar/allemand5
  com.effios.allemand5:/oauthredirect</scolomfr:location>
  <scolomfr:platform>http://data.education.fr/gar/openidconnect</scolomfr:platform>
  <!-- pas de scolomfr:personalDataProcessType, à voir si le XSD le permet-->
  <lom:description>
    <lom:string>gar-oidc-clientId : effios-allemand5</lom:string>
    <!-- secret pas forcément nécessaire, à voir -->
    <lom:string>gar-oidc-secret : F4B2CF890A8B07A38F4AB924C936BAA8FE8</lom:string>
    <!-- redirectUri seulement si le scolomfr:location n'est pas utilisé pour -->
    <lom:string>gar-oidc-redirectUri : com.effios.allemand5:/oauthredirect</lom:string>
    <lom:string>gar-oidc-name : FRV Manuel allemand 5°</lom:string>
  </lom:description>
</scolomfr:extendedLocation>
```

## 2.6. Prérequis tiers

### 2.6.1. Prérequis éditeurs de ressources

Les éditeurs de ressources devront développer des applications natives compatibles avec les prérequis imposés par le GAR.

### **2.6.2. Prérequis éditeurs de médiacentres**

Les applications natives pourront être lancées depuis le médiacentre de la même façon que les ressources actuelles. Le GAR permettra au médiacentre la prise en compte et l’affichage des informations complémentaires spécifiques aux applicatives natives.

Les évolutions du médiacentre par leurs éditeurs pour la prise en compte des informations spécifiques aux applications natives devront être optionnelles.

### **2.7. Livrables**

Outre l’ensemble des livrables contractuels il est attendu également :

- En analyse d’impact, avec la proposition de réalisation en mode projet, la liste des OS compatibles avec le système des liens vers applications natives installées
- La fourniture du composant permettant l’affichage du bouton normalisé « GAR Connect »
- La fourniture d’une « ressource » de test, de type « mixte » avec backend, permettant le bout en bout à des fins de qualification et accessible dans l’ensemble des environnements du GAR
- Une documentation détaillée, technique et pédagogique, à destination des éditeurs leur permettant de développer en toute autonomie des applications natives compatibles avec le GAR.

## **3. Planning**

Nous souhaitons la mise à disposition en production avant la fin de l’année 2022.

## **4. Annexe**