



**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 04.11 : Spécifications des accès ressources - SSO

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.

RENATER - GAR - Processus d'accès aux ressources

DSFD

Le 14/12/2023

Référence :	Version	En date du
RENATER-GAR-E/DSFD.0010 Processus d'accès aux ressources	15.00	14/12/2023

Version	Rédigé par	Objet	Vérifié		Validé	
			Par	Le	Par	Le
15.00	WORDLINE	Report correctif Mantis 1435 : Complément Mise en cache des métadonnées (ALM 1891) Release 7.3 (EB 445 et 465) Version validée	Worldline	14/12/2023	RENATER	01/12/2023

Évolutions successives

Version	Date	Description	Auteur(s)
1.0	30/09/2016	Création	WORDLINE
1.1	07/10/2016	Mise à jour suite aux retours de RENATER/MEN	WORDLINE
1.2	14/10/2016	Mise à jour suite aux retours de RENATER/MEN	WORDLINE
1.3	17/10/2016	Mise à jour suite aux retours de RENATER/MEN	WORDLINE
1.4	06/01/2017	Ajout du paramètre idEtab dans les requêtes d'accès aux ressources Pas de validation attendue pour cette version	WORDLINE
1.5	07/06/2017	Ajout de la durée de vie du jeton SAML §2.3	WORDLINE
1.6	04/08/2017	Gestion de SP Global §4.4.3	WORDLINE
1.7	09/08/2017	Ajout de précisions suite aux échanges avec Renater pour la gestion de SP Global	WORDLINE
1.8	07/09/2017	R.DDC.0004.1.2.SV_(007)_OpenIDConnect	WORDLINE
1.9	15/09/2017	R.DDC.0016.1.1.SV_Id_Complémentaire Prise en compte des retours : R.DDC.0004.1.2.SV_(007)_OpenIDConnect	WORDLINE
1.10	21/09/2017	Prise en compte des retours : R.DDC.0016.1.1.SV_Id_Complémentaire Retrait des modifications OpenID Connect	WORDLINE
1.11	20/10/2017	Évolution [038] [039] - licences pluriannuelles et transférabilité	WORDLINE
1.12	15/12/2017	Évolution [049] - Modification de la grammaire second degré	WORDLINE
2.1	09/03/2018	Évolution [048] - Intégration du 1 ^{er} degré Prise en compte des retours : Évolution [049] - Modification de la grammaire second degré	WORDLINE
2.2	29/03/2018	Prise en compte des retours sur l'évolution [048] - Intégration du 1 ^{er} degré	WORDLINE
2.3	11/06/2018	Ajout de précision pour la récupération du MEF_STAT_11 Évolution 065 - cache des métadonnées des DTR Mise à jour concernant la déconnexion	WORDLINE
2.4, 2.5, 2.6	14/06/2018 17/07/2018 26/07/2018	Prise en compte des retours concernant l'Évolution 065 - cache des métadonnées des DTR	WORDLINE
2.7	24/08/2018	Évolution 071 déconnexion	WORDLINE
2.8	12/09/2018	Évolution 066 - cache des métadonnées des DTR v2	WORDLINE
2.9 2.10	09/11/2018 21/11/2018	Evolution 042 - Accès granulaire	WORDLINE
2.9B1 2.9B2	23/11/2018 04/12/2018	Évolution 085 - ajout DCP mail pour les enseignants	WORDLINE
2.11	14/12/2018	Fusion de la version 2.9.B2 vers la version 2.10	WORDLINE
2.12	14/12/2018	Evolution 080 - division de rattachement pour le DCP Groupe	WORDLINE
2.13	19/12/2018	Prise en compte des retours sur l'évolution 080 - division de rattachement pour le DCP Groupe	WORDLINE
2.14	12/03/2019	Defect 887	WORDLINE
2.15	13/05/2019	Évolution 105 – accès granulaire v2	WORDLINE
3.0	24/09/2019	Évolution 100 : Gestion des profils agents	WORDLINE
03.01	02/07/2021	Evolution 146: Pilote 1D - version initiale	WORDLINE
03.02	21/07/2021	Evolution 146: Pilote 1D - ajustements suites aux retours RENATER du 12/07/2021	WORDLINE

03.03	30/07/2021	Evolution 146: Pilote 1D - ajustements suites aux retours RENATER du 28/07/2021	WORDLINE
03.04	05/08/2021	Evolution 146: Pilote 1D - ajustements suites aux retours RENATER du 04/08/2021	WORDLINE
03.05	26/11/2021	Defect 1483	WORDLINE
03.06	01/12/2021	Defect 1494	WORDLINE
04.00	01/12/2021	Validation de la spécification dans le cadre de la release 6.0	WORDLINE
04.01 04.02	15/12/2021 10/01/2022	Evolution 343 (WL : 151) - Nouveau profil - National_aca Evolution 341 (WL : 140) - Message d'erreur utilisateur enrichi	WORDLINE
05.00	21/01/2022	Version validée pour le lot 1 de la release 6.1	WORDLINE
05.01 05.02	07/02/2022 17/02/2022	Evolution 349 (WL : 149) : Utilisateurs actifs Prise en compte des Retours sur l'évolution 349	WORDLINE
06.00	28/02/2022	Version validée pour le lot 3 de la release 6.1	WORDLINE
06.01	25/03/2022	Report de modifications pour l'évolution 341 (WL : 140) - Message d'erreur utilisateur enrichi	WORDLINE
07.00	13/04/2022	Version validée pour la release 6.1	WORDLINE
07.01	18/05/2022	Correction des ALM 1483 et 1632	WORDLINE
08.00	30/05/2022	Validation de la spécification par RENATER	WORDLINE
08.01 08.02	03/06/2022 23/06/2022	Evolution 364 (WL 162) : OIDC pour les ENT	WORDLINE
09.00	06/07/2022	Version validée par RENATER	WORDLINE
09.01	20/07/2022	Evolution 239 (WL 167) : Gestion des applications natives	WORDLINE
09.02	05/08/2022	Prise en compte des Retours sur l'évolution 239	WORDLINE
09.03	24/08/2022	Prise en compte des Retours sur l'évolution 239	WORDLINE
09.04	02/09/2022	Prise en compte des Retours sur l'évolution 239	WORDLINE
09.05	05/09/2022	Prise en compte des Retours sur l'évolution 239	WORDLINE
09.06	06/09/2022	Validation de la spécification pour l'évolution 239 Ajout de l'Option 4 : Gestion de la déconnexion	WORDLINE
09.07	26/09/2022	Prise en compte des retours sur la gestion de la déconnexion	WORDLINE
09.08	06/10/2022	Prise en compte des retours sur la gestion de la déconnexion	WORDLINE
10.00	10/10/2022	Validation de la spécification pour l'option de gestion de la déconnexion	WORDLINE
10.01	02/12/2022	Evolution 399 (WL 193) : Débrayage SLO Sources d'authentification Evolution 404 (WL 198) : Activation de l'Access Token par plateforme partenaire Evolution 402 (WL 199) : Contrôle ressource backend ressource appelante	WORDLINE
10.02	12/12/2022	Prise en compte des remarques MEN/Renater	WORDLINE
11.00	14/12/2022	Version validée pour les évolutions 399, 404 et 402	WORDLINE
11.01	09/12/2022	- Evolution 388 (WL 187) : Envoi aux FR de la DCP Date de naissance - Evolution 284 (WL 157) : Mise en cache des métadonnées ENT - Evolution 376 (WL 184) : Gestion des Métadonnées ENT et Guichets OIDC	WORDLINE

11.02	03/01/2023	Prise en compte des retours RENATER sur les évolutions 388, 284 et 376 + report des évolutions 399, 402 et 404	WORDLINE
12.00	09/01/2023	Version validée par RENATER pour la release 7.1	WORDLINE
12.01	14/03/2023	Report de la release 7.0 Evolution 411 Statistiques-comptabilisation des demandes de DCP par AT Evolution 412 Evolution terminologie Ressource Backend en RTC	WORDLINE
13.00	21/03/2023	Version validée par Renater	WORDLINE
13.01	10/05/2023	EB 395 - Ressources Web en OIDC	WORDLINE
13.02	23/05/2023	EB 395 - Ressource Web en OIDC : prise en compte des propositions	WORDLINE
13.03	31/05/2023	EB 395 - Ressource Web en OIDC : prise en compte des propositions ALM 1875	WORDLINE
13.04	08/06/2023	EB 395 - Ressource Web en OIDC : prise en compte des retours	WORDLINE
14.00	13/06/2023	Validation de la spécification	WORDLINE
14.01	20/06/2023	Complément Mise en cache des metadonnées (ALM 1891)	WORDLINE
EB445 14.01	20/10/2023	Evolution 445 : Informations sur les accès aux ressources	WORDLINE
EB445 14.02	27/10/2023	Evolution 445 : Prise en compte des retours	WORDLINE
14.03	14/11/2023	Evolution 445 : version validée Evolution 465 : Autorisation d'accès au WS RAA par Access Token	WORDLINE
14.04	22/11/2023	Evolution 465 : Prise en compte des retours	WORDLINE
15.00	14/12/2023	Report correctif Mantis 1435 : Complément Mise en cache des metadonnées (ALM 1891) Release 7.3 (EB 445 et 465) Version validée	WORDLINE

Table des matières

1	Introduction	8
1.1	Objet du document	8
1.2	Responsabilités liées au document.....	8
1.3	Documents de référence.....	8
1.4	Autres documents utilisés	8
1.5	Abréviations.....	8
1.6	Glossaire	9
1.7	Présentation générale	10
1.7.1	Urls utilisées dans le GAR.....	10
1.7.2	Accès aux ressources.....	10
2	Protocoles utilisés	12
2.1	Lien Fournisseur d'identité – GAR.....	12
2.1.1	SAML2	12
2.1.2	OIDC (ENT)	12
2.2	Lien GAR – DTR.....	12
2.2.1	SAML.....	13
2.2.2	CAS	13
2.2.3	OIDC	13
3	Lien fournisseur d'identité – GAR.....	14
3.1	Gestion des métadonnées des ENT et des guichets.....	14
3.1.1	Services concernés	14
3.1.2	Utilisation du cache des métadonnées	14
3.1.3	Mise en cache des métadonnées	14
3.1.4	Fréquence d'exécution	15
3.1.5	Durée de rétention du cache	15
3.1.6	Contrôles de validité	15
3.1.7	Notification	16
3.1.8	Objet du mail.....	16
3.1.9	Contenu du mail.....	16
3.1.10	Variables	16
3.2	Diagramme fonctionnel	18
3.3	Fonctionnement	19
3.3.1	[Auth001] Extraction des identifiants.....	19

3.3.2	[Auth002] Vérification de l'existence de la ressource.....	20
3.3.3	[Auth003] Vérification de l'existence de l'établissement	20
3.3.4	[Auth028] Identification de l'établissement et du profil à travers le WAYF NATIVES.....	20
3.3.5	[Auth004] Vérification de l'authentification au niveau du GAR.....	20
3.3.6	[Auth005] Récupération du fournisseur d'identité.....	20
3.3.7	[Auth006] Requête d'autorisation.....	21
3.3.8	[Auth007/Auth008] Validation de l'authentification.....	21
3.3.9	[Auth009] Vérification de l'autorisation d'accès	21
3.3.10	[Auth010] Création / mise à jour du cookie	21
3.3.11	[Auth011] Extraction de l'identifiant de l'accédant.....	22
3.3.12	[Auth012] Récupération de l'url de la ressource	22
3.3.13	[Auth013] Redirection vers la ressource	22
3.3.14	[Auth014] Affichage d'une page d'erreur	23
3.4	Flux lien fournisseur d'identité – GAR.....	24
3.4.1	ENT–GAR : Protocole SAML.....	24
3.4.2	ENT–GAR : Protocole OpenIdConnect.....	25
3.4.3	Guichet d'authentification–GAR : Protocole OpenIdConnect.....	26
3.5	Identification du fournisseur d'identité.....	26
3.5.1	Accès web	26
3.5.2	Accès par application native.....	28
4	Lien GAR – DTR.....	31
4.1	Description	31
4.2	Gestion des métadonnées SAML des DTR.....	31
4.2.1	Mise en cache des métadonnées	31
4.2.2	Contrôle de validité.....	32
4.2.3	Notification	32
4.3	Diagramme fonctionnel	32
4.4	Fonctionnement	34
4.4.1	[Auth015] Vérification de l'authentification au niveau du GAR.....	34
4.4.2	[Auth016] Récupération de l'identifiant de l'accédant.....	34
4.4.3	[Auth017] Récupération de l'identifiant de la ressource	34
4.4.4	[Auth018] Vérification de l'autorisation d'accès	35
4.4.5	[Auth019] Récupération des attributs de l'accédant.....	35
4.4.6	[Auth020] Fourniture des attributs à la ressource	36
4.4.7	[Auth024] Cas d'erreur.....	41
4.4.8	Usages particuliers de l'Access Token	41
4.5	Flux lien GAR–DTR	46
4.5.1	Protocole SAML.....	46

4.5.2	Protocole CAS	47
4.5.3	Protocole OpenId Connect.....	48
5	Solution technique.....	51
5.1	Lien fournisseur d'identité- GAR	51
5.1.1	Attributs attendus de la part des fournisseurs d'identité.....	51
5.1.2	Gestion du cookie d'authentification.....	51
5.2	Lien GAR – DTR.....	51
5.2.1	Validation de l'authentification	51
5.2.2	Délivrance des attributs.....	52
6	Déconnexion	56
6.1	Contexte général	56
6.2	Fonctionnement	56
6.3	Diagramme fonctionnel	57
6.4	Flux de déconnexion.....	58
6.4.1	Accès web	58
6.4.2	Accès par application native.....	58
6.5	Propagation de la déconnexion vers le GAR	59
6.5.1	Propagation de la déconnexion depuis l'ENT (SAML)	59
6.5.2	Propagation de la déconnexion depuis l'ENT (OIDC)	59
6.5.3	Propagation de la déconnexion depuis les applications du GAR	60
6.5.4	Propagation de la déconnexion depuis une ressource web	60
6.5.5	Propagation de la déconnexion depuis les applications natives	60
6.6	Propagation de la déconnexion vers les ressources	60
6.6.1	Propagation de la déconnexion vers les ressources dans le cas du protocole SAML.....	60
6.6.2	Propagation de la déconnexion vers les ressources dans le cas du protocole CAS	61
6.6.3	Propagation de la déconnexion vers les ressources dans le cas du protocole OIDC	61
6.7	Propagation de la déconnexion vers les fournisseurs d'identité	61
6.7.1	Propagation de la déconnexion vers les ENT SAML.....	61
6.7.2	Propagation de la déconnexion vers les guichets et les ENT OIDC.....	61

1 Introduction

1.1 Objet du document

Ce document est le Document de Spécifications Fonctionnelles Détaillées du processus d'accès aux ressources dans le cadre du projet Gestionnaire d'Accès aux Ressources (GAR).

1.2 Responsabilités liées au document

Le chef de projet Worldline est responsable de la rédaction du Dossier de Spécifications fonctionnelles, RENATER et le Ministère en charge de l'Éducation Nationale (MEN) sont responsables de sa validation.

1.3 Documents de référence

Numéro	Réf. Document	Type
DR1	D07-2-Annexe 2 du Marche Subsequent n°2 - Cahier des charges du GAR.pdf	
DR2	GAR-S2.DSFD.0011.Post_moissonnage.V06.00	DSFD
DR3	GAR-S2.DSFD.0002.Spécification_du_WS_Liste_Ressources.V05.00	DSFD
DR4	GAR-S2.DAT.0003.Plateforme GAR	DAT
DR5	R.DSFD.0003.1.2.VA-Gestion_des_Certificats	DSFD
DR6	GAR-S2.DSFD.0007.Spécifications_du_moissonneur.V07.00	DSFD
DR7	R.DSFD.0005.3.3.VA-Administration_du_GAR	DSFD
DR8	GAR-S2.DSFD.0029.Gestion_des_guichets.V03.00	DSFD
DR9	GAR-S2_Acces_aux_Ressources_Wording_0001.xlsx	
DR10	GAR-S2.DSFD.0040.WAYF NATIVES.V01.00	DSFD
DR11	GAR-S2.DSFD.0009.Regles_de_gestion_du_gar.V02.02.docx	DSFD
DR12	GAR-S2.DSFD.0014.Batch_d_import_ENT.V12.00	DSFD
DR13	GAR-S2.NOE.0003.Matrice de notifications du GAR.V18.00	NOE
DR14	GAR-S2.DSFD.0024.WS_Gestion des données initialisation.V05.01.docx	DSFD
DR15	GAR-S2.DSFD.0044.Informations_sur_les_accès_aux_ressources.V01.00	DSFD

1.4 Autres documents utilisés

Numéro	Réf. Document	Type
AD1	GAR_Gestion_attributsGAR_DCP_V1.0.pdf	
AD2	http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	Spécification protocole SAML
AD3	https://apereo.github.io/cas/5.1.x/protocol/CAS-Protocol-Specification.html#23-logout	Spécification protocole CAS (logout)
AD4	https://openid.net/specs/openid-connect-core-1_0.html	Spécification protocole OpenId Connect

1.5 Abréviations

Abréviation	Signification
AT	Access Token

CAS	Central Authentication Service
DSFD	Document de Spécifications Fonctionnelles Détaillées
DTR	Distributeur Technique de Ressources
EIM	Equipement Internet Mobile
GAR	Gestionnaire d'Accès aux Ressources
HTTP	HyperText Transfert Protocol
JSON	JavaScript Object Notation
MEN	Ministère en charge de l'Education nationale
OIDC	OpenIdConnect
PKCE	Proof Key for Code Exchange
RTC	Ressource Technique Commune
SAML	Security Assertion Markup Langage
XML	eXtensible Makup Langage

1.6 Glossaire

Terme	Signification
SP Global	Service Provider protégeant l'accès à plusieurs ressources
Grain	Unité éditoriale d'utilisation pédagogique d'une ressource (l'article, le média, l'exercice, etc.)
Autre personnel	Un autre personnel est un accédant issu de l'import ENT ayant au moins un profil National_dir, National_evs, National_eta National_col ou National_aca pour au moins l'un des établissements qui lui sont associés
OpenId Connect	OpenID Connect (OIDC) est une simple couche d'identification basée sur OAuth 2.0
OAuth 2.0	OAuth est un protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur.
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 ...).

Glossaire projet : [GlossaireGAR.V02.00](#)

1.7 Présentation générale

1.7.1 Urls utilisées dans le GAR

URL d'accès à la ressource (éditeur): URL de la porte SSO de la ressource dédiée au GAR (élément lom.technical.extendedLocation.location pour ressource avec une variante web et l'élément lom.technical.extendedLocation.description pour ressource avec une variante application native) .

Les ressources GAR peuvent disposer de variantes sous forme d'une application web et de une ou plusieurs applications natives :

- **L'URL d'accès GAR pour la variante web :** URL d'accès à une ressource décrite dans le GAR, obtenue par l'appel du WS ListeRessources.
Exemple :
<https://idp-auth.partenaire.test-gar.education.fr/domaineGar?idENT=WjA=&idEtab=MDU2MTkzMVY=&idRessource=YXJrOi8xMjMxMy9lQTk3ODI0MDEwMjU1MzAx>
- **L'URL d'accès GAR pour une variante application native :** URL d'accès à une ressource lors d'un échange initié par une application native. Elle correspond à l'appel au endpoint /authorize du protocole OIDC avec en paramètre l'idRessource, l'identifiant de la ressource, en plus des paramètres OIDC attendus.
Exemple :
https://idp-auth.gar.education.fr/authorize?response_type=code&redirect_uri=https%3A%2F%2Fmaressource.mondomainefr.com%2Flogin&state=TST-1-MvhCMS4gbEwfcLS0MoaPE1REmOAphLV&client_id=monappligar&scope=openid+ent.gar&idRessource=ark%3A%2F12313%2FHA97824010255301

En outre les ressources peuvent proposer un accès granulaire (accès à des Grains identifiés par l'éditeur) :

- **L'URL éditeur Grain :** URL/paramètre d'accès public à un Grain.
Exemple : <https://maressource.mondomainefr.com>
- **L'URL GAR Grain :** URL d'appel d'un Grain à transmettre au GAR, comportant l'URL GAR de la ressource, avec en paramètre, l'URL éditeur Grain.
Exemple :
<https://idp-auth.partenaire.test-gar.education.fr/domaineGar?idENT=WjA=&idEtab=MDU2MTkzMVY=&idSrc=YXJrOi8xMjMxMy9lQTk3ODI0MDEwMjU1MzAx&grain=https%3A%2F%2Fmaressource.mondomainefr.com>

1.7.2 Accès aux ressources

Dans le cadre du projet Gestionnaire d'Accès aux Ressources (GAR), la brique d'accès aux ressources permet à un utilisateur d'accéder à une ressource qui lui a été affectée. Cette action se décompose en 3 étapes :

1. Pour le mode web, l'accès GAR à la ressource est réalisé avec l'url d'accès GAR. Cette url peut être obtenue à partir d'une liste des ressources affectées à un utilisateur donné, affichée dans un médiacentre suite à l'appel du web service liste ressources ou forgée par l'éditeur de ressources.
Pour le mode application native, l'accès à la ressource est initié par l'application native en contactant directement le GAR (sans passer par un Médiacentre) via le endpoint /authorize propre au protocole OpenIdConnect. Cette url est forgée par l'éditeur de ressources.
- 2- Authentification auprès du Fournisseur d'identité (lien Fournisseur d'identité - GAR)
Lors de cette étape le GAR joue le rôle de fournisseur de service auprès des fournisseurs d'identité.
C'est le GAR qui valide que l'utilisateur est bien authentifié sur son fournisseur d'identité et qu'il a bien l'autorisation d'accéder à la ressource demandée.

- Les fournisseurs d'identité actuellement interfacés avec le GAR sont de deux types :
- les projets ENT
 - les guichets d'authentification : actuellement, EduConnect et Hub agents
- 3- Redirection vers la ressource (lien GAR – Distributeur technique de ressources)
- Lors de cette étape le GAR joue le rôle de fournisseur d'identité délégué auprès des distributeurs techniques de ressources.
- L'utilisateur est ensuite redirigé vers la ressource. Le DTR valide la demande d'accès de l'utilisateur en appelant le GAR et récupère les attributs de l'utilisateur pour la ressource demandée. L'utilisateur a alors accès à la ressource.

L'utilisateur peut également accéder à un endroit précis de la ressource grâce à un accès granulaire. Pour un accès web, il est défini par une « url GAR Grain » composée de l'url d'accès GAR et d'un paramètre contenant l'URL ou paramètre éditeur Grain. Le GAR reçoit le paramètre pour le transmettre, sans l'analyser.

Pour un accès application native, un accès granulaire peut être défini dans le redirectUri comme détaillé dans la règle [Auth013](#).

Le schéma ci-dessous présente une vue globale simplifiée de la brique d'accès aux ressources et son interaction avec les différents acteurs. Ce schéma permet d'avoir une vue d'ensemble du processus d'accès aux ressources et n'affiche que les initiateurs et destinataires des requêtes sans détailler les étapes intermédiaires (redirection http).

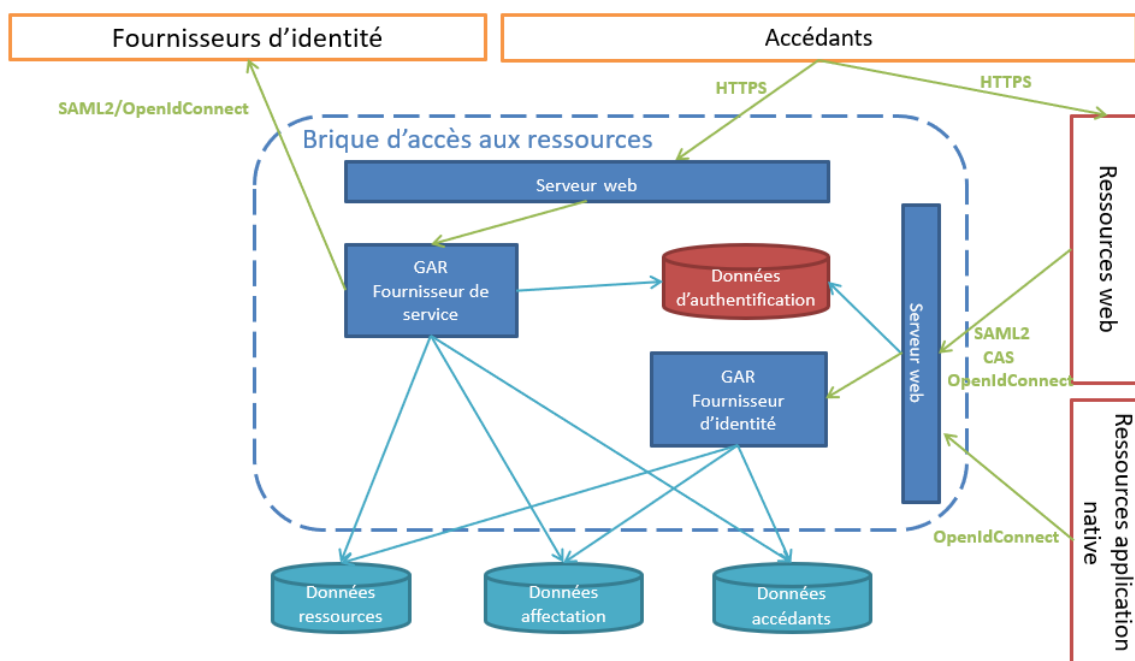


Figure 1 Vue globale simplifiée

2 Protocoles utilisés

2.1 Lien Fournisseur d'identité – GAR

Les protocoles d'échange utilisés pour le lien projets ENT – GAR sont les protocoles SAML en version 2.0 et OpenIdConnect en version 1.0.

Le protocole d'échange utilisé pour le lien guichets d'authentification – GAR est le protocole OpenIdConnect en version 1.0.

2.1.1 SAML2

Le flux utilisé dans le GAR est de type « initié par le fournisseur de service » (SP-initiated). La découverte des fournisseurs d'identité SAML2 se base sur l'identifiant du projet ENT qui est fourni dans la requête de demande d'accès à la ressource.

Le jeton SAML généré a une durée de vie de 5 minutes (configurable)

Lors de la déclaration d'un projet ENT dans le GAR les données suivantes doivent être fournies :

- L'url du projet ENT pour permettre la validation de l'authentification de l'accédant
- Certificat signé ou autosigné utilisé par le fournisseur d'identité pour signer les assertions
- Le fichier de métadonnées du fournisseur d'identité

2.1.2 OIDC (ENT)

Pour les ENT utilisant le protocole OpenIdConnect, la demande d'authentification est initiée par le RP (Relying Party). Dans cet échange, le service d'accès aux ressources du GAR tient le rôle de RP et l'ENT le rôle d'OP (OpenId Provider). Le mode d'échange implémenté est l'autorization code flow sans PKCE. A l'instar du protocole SAML, l'identification du fournisseur d'identité OIDC est basée sur l'identifiant du projet ENT qui est fourni dans la requête de demande d'accès à la ressource.

Lors de la déclaration d'un projet ENT en OIDC dans le GAR, les données suivantes doivent être fournies par l'ENT :

- le clientID : identifiant du client OIDC du projet ENT ;
- le secret : mot de passe entre l'ENT et le GAR ;
- l'url de well-known : métadonnées du client OIDC ;
- le scope : scope des informations autorisées pour le service d'accès aux ressources.

Le GAR devra quant à lui fournir les informations suivantes à l'ENT :

- le redirectUri : URI de redirection vers le GAR après obtention de l'autorization code ;
- l'url de logout : endpoint de déconnexion du GAR.

2.2 Lien GAR – DTR

Pour les accès aux variantes web des ressources, le protocole d'authentification utilisé est soit :

- SAML en version 2.0
- CAS en version 3.0
- OIDC en version 1.0

Pour les accès via application native, le protocole d'authentification utilisée est OIDC en version 1.0.

2.2.1 SAML

A compléter

2.2.2 CAS

La durée de validité du ticket de service généré par le CAS est de 10 secondes (configurable).

L'url du serveur CAS géré par le GAR doit être connue des Distributeurs Technique de Ressources pour qu'ils puissent valider l'authentification des accédants lors des accès aux ressources.

2.2.3 OIDC

Le protocole OIDC peut être utilisé pour des ressources à variante web ou native.

Quelle que soit la variante de la ressource, la demande d'authentification est initiée par le RP (Relying Party). Dans cet échange, le service d'accès aux ressources du GAR tient le rôle d'OP (OpenId Provider) et le fournisseur de ressource celui de RP. Le mode d'échange implémenté est l'autorization code flow.

Suivant les bonnes pratiques du standard OIDC, les durées de validité des différents jetons et codes seront les suivants:

- *Authorization Code* : dix secondes;
- *Access Token* : durée de la session, peut être prolongée avec le refresh token dans la limite de durée maximale de session telle que définie au paragraphe [5.1.2](#).
- *Refresh Token* : durée de la session, renouvelé à chaque appel de rafraîchissement.

2.2.3.1 Variante web

Dans le cas d'une variante web, le protocole OIDC est mis à disposition des plateformes DTR hébergeant les ressources web. Dans ce cadre, le mode d'échange authorization code flow est complété d'un secret obligatoire et de l'extension PKCE optionnelle.

Chaque plateforme DTR est reconnue par le service d'accès aux ressources comme un Relying Party OIDC, c'est-à-dire un client, à l'appui des informations que le Fournisseur de Ressources a préalablement communiquées au Gestionnaire Administratif.

Les données *clientId*, *redirectUri*, et *logoutUrl* sont transmises via le WS Données d'initialisation ou les fichiers d'initialisation tel que décrit dans le [DR14](#).

Pour des raisons de sécurité, le *secret* est transmis encapsulé dans un conteneur ZED ! via une demande de service.

2.2.3.2 Variante native

Dans le cas d'une variante native, le protocole OIDC est mis à disposition de la variante native d'une ressource. Dans ce cadre, l'extension PKCE est utilisée et obligatoire car l'application native ne peut pas garantir la sécurité d'un secret échangé entre elle et l'OP.

3 Lien fournisseur d'identité – GAR

3.1 Gestion des métadonnées des ENT et des guichets

3.1.1 Services concernés

Les services concernés par la gestion du cache des métadonnées des ENT et des guichets sont :

- L'accès aux ressources
- Le SSO des IHMs pour l'accès à l'IHM Affectation

3.1.1.1 Protocoles

Le batch de mise en cache des métadonnées comporte 2 traitements indépendants :

- Un traitement pour traiter la mise en cache des métadonnées en SAML
- Un traitement pour traiter la mise en cache des métadonnées en OIDC

Ces 2 traitements appliquent les mêmes règles de mise en cache décrites au §3.1.2.

3.1.2 Utilisation du cache des métadonnées

Les services concernés cités précédemment récupèrent les métadonnées du projet ENT/guichet au travers d'un cache des métadonnées des projets ENT/guichets.

L'utilisation du cache est implémentée avec le séquençement suivant :

- Si les métadonnées sont présentes dans le cache alors
 - Ces métadonnées sont utilisées par les services concernés pour donner l'accès à l'utilisateur
- Sinon le service n'est pas accessible et renvoie une erreur

3.1.3 Mise en cache des métadonnées

L'administrateur technique du GAR pourra forcer le rechargement des métadonnées d'un projet ENT/guichet dans le cache notamment lorsque l'exploitant ENT ou le point de contact EduGAR le demande via une demande de support.

Le cache des métadonnées est mis à jour (avec ou sans changement des métadonnées) à chaque exécution du traitement à une fréquence donnée (cf. §3.1.4 pour plus de détails) via un appel aux métadonnées de chaque projet ENT/guichet. Les métadonnées ne sont mises en cache que si elles sont valides (cf. §3.1.6).

Si elles ne sont pas valides les métadonnées sont rejetées et le cache continue d'être utilisé.

Les métadonnées sont conservées dans le cache pendant une durée paramétrable définie au §3.1.5.

Une notification (cf. §3.1.7) est envoyée au support GAR, au GT et à l'exploitant ENT ou au point de contact EduGAR concerné (pour les guichets d'authentification) pour les informer du problème avec un message adapté en fonction des cas suivants :

- Le contenu des métadonnées n'est pas valide ou pas disponible, et les métadonnées sont présentes en cache :
 - Cas 1 : depuis 2 jours maximum (configurable en Heures dans un fichier de configuration)
 - Cas 2 : depuis plus de 2 jours (configurable en Heures dans un fichier de configuration)
 - Cas 3 : depuis plus de 4 jours (configurable en Heures dans un fichier de configuration)
 - Cas 4 : depuis plus de **nbJoursCache** jours (**nbJoursCache** correspond à la durée de rétention du cache, Cf. §3.1.5 pour plus de détails), les métadonnées sont supprimées du cache.

- Le contenu des métadonnées n'est pas valide ou pas disponible, et les métadonnées ne sont pas présentes en cache :
 - Cas 5

Les adresses utilisées pour l'envoi de notification sont :

- Pour l'exploitant ENT et le point de contact EduGAR, les adresses de responsables du projet ENT/guichet (non académique/ académique en fonction du cas concerné) définies dans la table projet_ent (champ *ent_mail_responsable*)
- Pour le GT, les adresses de contacts indiquées dans les profils de type gestionnaire technique.

3.1.4 Fréquence d'exécution

3.1.4.1 Pour SAML

Le traitement de mise en cache des métadonnées ENT SAML s'exécute à une fréquence configurable (tous les jours à 7h et 13h par défaut).

3.1.4.2 Pour OIDC

Le traitement de mise en cache des métadonnées ENT/guichets OIDC s'exécute à une fréquence configurable (tous les jours à 7h et 13h par défaut).

3.1.5 Durée de rétention du cache

La durée de rétention est configurable en Heures dans un fichier de propriétés de manière indépendante pour les métadonnées SAML et OIDC.

3.1.5.1 Pour SAML

La durée de rétention pour le cache des métadonnées ENT SAML est positionnée à 168 heures (7 jours) par défaut.

3.1.5.2 Pour OIDC

La durée de rétention pour le cache des métadonnées ENT/guichets OIDC est positionnée à 168 heures (7 jours) par défaut.

3.1.6 Contrôles de validité

3.1.6.1 Pour SAML

Les contrôles réalisés sur les métadonnées ENT SAML avant leur mise en cache sont les suivants :

- Contrôle de la conformité à la xsd SAML
- Contrôle de l'Entity-id par rapport à la valeur positionnée lors de la création du projet ENT

3.1.6.2 Pour OIDC

Le contrôle réalisé sur les métadonnées ENT/guichets OIDC avant leur mise en cache est le suivant :

- Contrôle de la conformité au format des métadonnées du protocole OIDC (utilisation de la librairie java « oauth-oidc-sdk » dédiée au standard OIDC pour faire le contrôle)

3.1.7 Notification

3.1.8 Objet du mail

3.1.8.1 Pour un projet ENT

[GAR][<code_projet_ENT>] Problème de mise en cache des métadonnées <protocole>
--

3.1.8.2 Pour un guichet

[GAR][<code guichet>] Problème de mise en cache des métadonnées OIDC
--

3.1.8.3 Variables

<code_projet_ENT>	Identifiant du projet ENT en clair, non encodé
<code guichet>	Code du guichet
<protocole>	Protocole utilisé par le projet ENT (SAML ou OIDC)

3.1.9 Contenu du mail

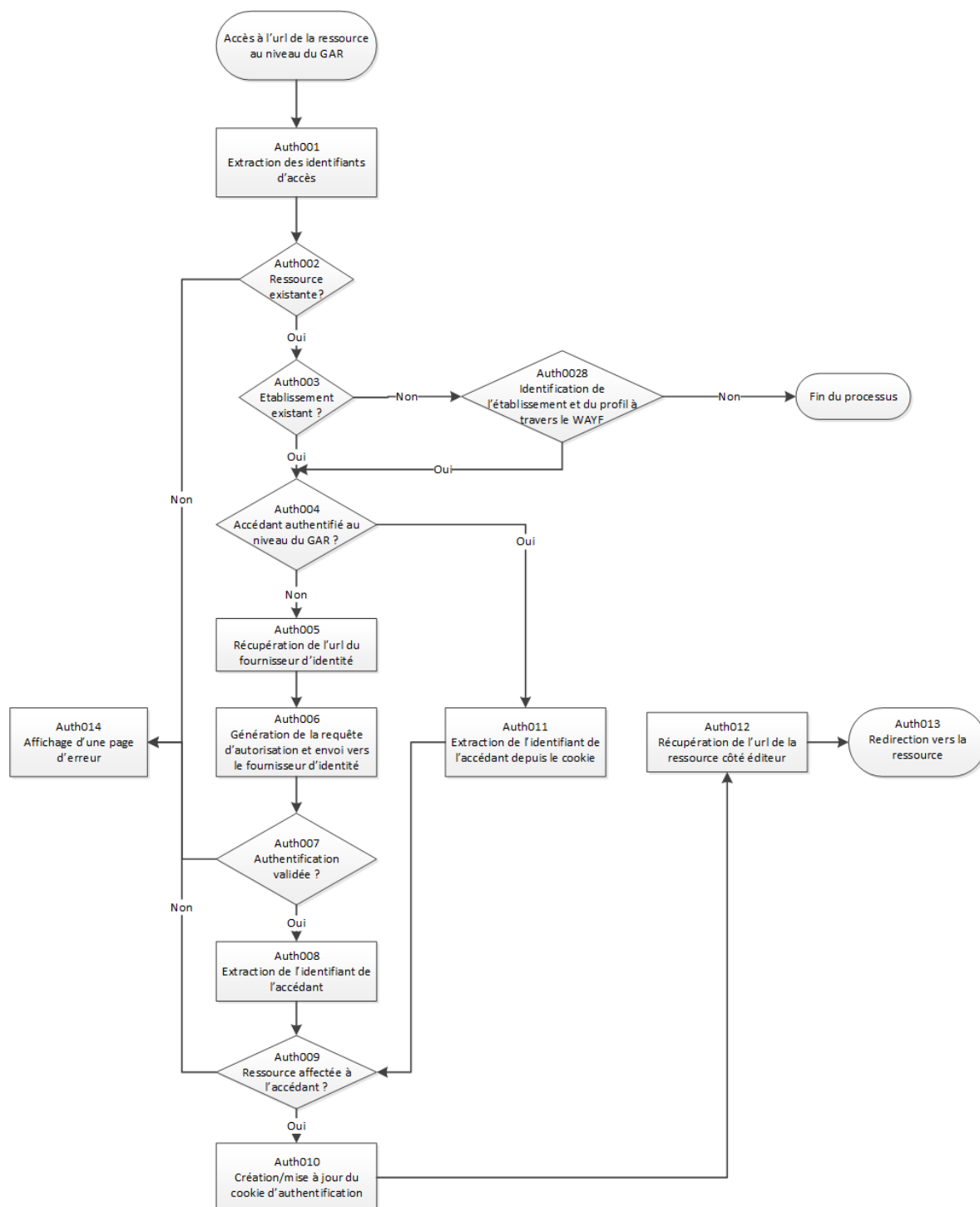
<EN_TETE> Le GAR n'a pas pu récupérer vos métadonnées pour l'accès aux ressources et à l'IHM Affectation à l'adresse : <url> L'erreur rencontrée est la suivante : <erreur> <contenu> <SIGNATURE>
--

3.1.10 Variables

<EN_TETE>	L'en-tête commun à l'ensemble des mails envoyés par le GAR (cf. DR13)
<SIGNATURE>	La signature commune à l'ensemble des mails envoyés par le GAR (cf. DR13)
<url>	Url des métadonnées
<erreur>	Exemples : <ul style="list-style-type: none"> • url non accessible • Contrôle de validité du champ <champ> • Réponse du serveur : Erreur 404
<contenu>	Cas 1 : La version du <JJ-MM-AAAA> de vos métadonnées est utilisée par le GAR depuis <nb_heures_cache_01/24 arrondi à l'entier supérieur> jours maximum. Le cache sera utilisé jusqu'au <JJ-MM-AAAA>. Ensuite l'accès aux ressources et à l'IHM Affectation sera désactivé. Cas 2 : La version du <JJ-MM-AAAA> de vos métadonnées est utilisée par le GAR depuis plus de <nb_heures_cache_02/24 arrondi à l'entier supérieur> jours. Le cache sera utilisé jusqu'au

	<p><JJ-MM-AAAA>. Ensuite l'accès aux ressources et à l'IHM Affectation sera désactivé.</p> <p>Cas 3 : La version du <JJ-MM-AAAA> de vos métadonnées est utilisée par le GAR depuis plus de <nb_heures_cache_03/24 arrondi à l'entier supérieur> jours. Le cache sera utilisé jusqu'au <JJ-MM-AAAA>. Ensuite l'accès aux ressources et à l'IHM Affectation sera désactivé.</p> <p>Cas 4 : La version du <JJ-MM-AAAA> de vos métadonnées est utilisée par le GAR depuis plus de <nb_jours_cache> jours. L'accès aux ressources et à l'IHM Affectation n'est actuellement plus possible via le GAR.</p> <p>Cas 5 : Les métadonnées ne sont pas en cache. L'accès aux ressources et à l'IHM Affectation n'est actuellement pas possible via le GAR.</p>
<SIGNATURE>	Signature commune à l'ensemble des mails envoyés par le GAR (cf. DR13)

3.2 Diagramme fonctionnel



2 Diagramme du lien fournisseur d'identité - GAR

3.3 Fonctionnement

Les étapes de validation de l'authentification pour le lien fournisseur d'identité - GAR sont décrites ci-dessous.

3.3.1 [Auth001] Extraction des identifiants

Pour l'accès en mode web :

Les requêtes d'accès à la ressource fournies par le web service liste ressource (DR3) contiennent dans leurs paramètres de requête un identifiant permettant de retrouver les données du projet ENT de l'accédant et un identifiant permettant de retrouver les données de la ressource demandée. Ces 2 paramètres sont extraits de la requête pour générer la requête SAML2 ou OpenIdConnect et la transmettre vers le fournisseur d'identité de l'accédant.

Dans le cas de l'authentification par guichet, un paramètre optionnel permet d'indiquer quel guichet doit être contacté.

L'url d'accès à la ressource au niveau du GAR est de la forme :

https://domaineGar?idENT={idENT} & [idSrc={idSrc} | idRessource={id de la ressource}] & idEtab={idEtab} [&idpHint={choix du guichet}][& grain={url du Grain}]

Dans le cadre du protocole OpenIdConnect, le FR peut directement solliciter le GAR sur le endpoint /authorize de la forme :

https://authorize?idRessource={id de la ressource}&idEtab={idEtab}&profil={profil}

Pour l'accès par application native :

L'accès initié par une application native à une ressource est réalisé sur le endpoint /authorize proposé par le protocole OpenIdConnect.

Il est de la forme suivante :

https://authorize?idRessource={id de la ressource}&idEtab={idEtab}&profil={profil}

Paramètre	Valeur	Obligatoire	Commentaire	Mode d'accès
profil	Les profils « ELV » pour les élèves et « AGT » pour les agents provenant du WAYF_NATIVES Tout type de profil défini dans le DR12 hormis le profil responsable d'affectation	non	Profil de l'utilisateur Paramètre fourni suite au renseignement du profil dans le WAYF_NATIVES	Web et Application native
idRessource	l'identifiant de la Ressource (ark) url encodé	Voir RGidRessource		
idEtab	UAI de l'établissement d'accès au GAR encodé en base 64	non		
Grain	l'url/paramètre du Grain chez l'éditeur au format url encodé	non		
idSrc	l'identifiant de la Ressource (ark) encodé en base 64	Voir RGidRessource		Web
idENT	le code du projet ENT ou EduGAR encodé en base 64	non	Paramètre ignoré. Le code projet ENT est déduit du paramètre idEtab	
idpHint	le code du guichet à contacter pour l'authentification	non	Spécifique au cas de l'authentification par guichet	

RGprofil :

Si un profil National_ELV est indiqué en paramètre, il sera interprété en profil « eleve » pour une redirection vers le bon guichet. Tous les autres profils National_* seront interprétés en profils « agent ».

RGidRessource :

1. Lors de l'appel, idSrc ou idRessource doivent être fournis
2. Si idSrc et idRessource sont fournis, alors l'idRessource est utilisé par le GAR
3. Si ni idSrc ni idRessource ne sont fournis, une erreur de type identifiant de la ressource absent sera affichée à l'utilisateur.

3.3.2 [Auth002] Vérification de l'existence de la ressource

Le GAR récupère en base de données l'identifiant de la ressource demandée à partir de l'identifiant passé en paramètre. Si la ressource n'existe pas, une page d'erreur est affichée (§3.3.14).

3.3.3 [Auth003] Vérification de l'existence de l'établissement

Le GAR récupère en base de données l'identifiant du code projet ENT de l'accédant à partir de l'établissement idEtab passé en paramètre. Si l'établissement n'existe pas, l'utilisateur est redirigé vers le WAYF NATIVES.

3.3.4 [Auth028] Identification de l'établissement et du profil à travers le WAYF NATIVES

L'utilisateur est redirigé vers le WAYF NATIVES afin d'y sélectionner son établissement et son profil. Le code projet de l'ENT est déduit de l'établissement ainsi sélectionné. S'il correspond à un projet EDUGAR, le profil est utilisé pour identifier le guichet à utiliser. Le fonctionnement du WAYF NATIVES est détaillé dans le [DR10](#).

3.3.5 [Auth004] Vérification de l'authentification au niveau du GAR

Le GAR vérifie que l'accédant possède déjà un cookie d'authentification positionné sur le domaine GAR.

- Si le cookie est présent, le GAR vérifie que le cookie correspond bien à une authentification existante.
- Si le cookie est valide, le processus se poursuit en §3.3.11.
- Si le cookie n'est pas valide sur le GAR, celui-ci est invalidé sur le navigateur et le processus se poursuit en §3.3.6.
- Si le cookie n'est pas présent le processus se poursuit en §3.3.6.

La vérification de l'authentification au niveau du GAR permet de diminuer le nombre de requêtes faites aux fournisseurs d'identité lors de l'accès à de multiples ressources.

Cette fonctionnalité est débrayable au niveau du GAR. Dans ce cas, chaque demande d'accès à une ressource générera une vérification de l'authentification de l'accédant vers son fournisseur d'identité pour pouvoir l'identifier (§3.3.6).

L'utilisation des cookies au niveau du navigateur de l'accédant doit être autorisée, que la fonctionnalité soit activée ou non.

3.3.6 [Auth005] Récupération du fournisseur d'identité

Pour l'accès en mode web :

À partir de l'identifiant du projet ENT récupéré en §3.3.3 le GAR récupère l'url du fournisseur d'identité associé à l'ENT de l'accédant. Cette donnée est fournie lors de la déclaration des projets ENT au niveau du GAR.

Dans le cas des guichets d'authentification, le GAR aiguille vers le guichet adapté en fonction des règles suivantes :

- Si le paramètre de choix de guichet a été fourni (cf. [DR8](#)), le GAR redirige vers le guichet indiqué
- Sinon, le GAR redirige vers le WAYF d'identification des guichets (cf. [DR8](#)) pour permettre à l'accédant de déterminer le guichet adapté.

Pour l'accès par application native :

Le fournisseur d'identité est déduit en fonction des informations sur l'établissement et le profil de l'utilisateur transmis soit dans l'url, soit par le WAYF NATIVES.

3.3.7 [Auth006] Requête d'autorisation

Dans le cas d'un fournisseur d'identité SAML2, le GAR génère une requête de demande d'authentification et d'attributs AuthnRequest et la transmet au fournisseur d'identité de l'accédant via une requête POST.

Dans le cas d'un fournisseur d'identité OpenIdConnect, le GAR génère une requête d'autorisation OpenIdConnect pour la faire transmettre par le navigateur de l'utilisateur.

3.3.8 [Auth007/Auth008] Validation de l'authentification

Le GAR récupère la réponse du fournisseur d'identité, vérifie si l'authentification est validée et extrait les attributs de l'accédant, dont son identifiant. Si l'authentification est invalide, une page d'erreur est affichée (§3.3.14).

3.3.9 [Auth009] Vérification de l'autorisation d'accès

Le GAR vérifie, à partir de l'identifiant de l'accédant récupéré en §3.3.8 et l'identifiant de la ressource récupéré en [§3.2.2](#) que la ressource est bien affectée à l'accédant, que la licence est toujours valide et que la fourniture des données à caractère personnel a été validée.

Si l'une des conditions n'est pas remplie, une page d'erreur est affichée (§3.3.14).

Dans le cas contraire, le GAR vérifie si l'accédant existe dans la table « utilisateurs_actifs » :

- Si oui :
 - ✓ La colonne « nb_acces » est mise à jour avec une nouvelle valeur constituée par la valeur de la colonne incrémentée de 1
- Si non :
 - ✓ L'accédant est inséré dans la table en tant qu'utilisateur actif.
 - ✓ La date de création de l'utilisateur (Date du jour) est insérée dans la table au format DATE (AAAA-MM-JJ)
 - ✓ La valeur 1 est positionnée dans la colonne « nb_acces »

A noter que les insertions ou mises à jour apportées dans la table utilisateurs_actifs ne sont réalisées qu'à des fins de surveillance et de collecte d'informations par rapport aux accès ressources du GAR.

Si une erreur survient dans les traitements liés à cette table, celle-ci doit être écrite en sortie dans les fichiers de logs applicatifs et ne doit en aucun cas bloquer le processus d'accès à la ressource.

L'usage de la table utilisateurs_actifs est détaillé dans le document de référence DR15

3.3.10 [Auth010] Création / mise à jour du cookie

Le GAR stocke dans une base de données mémoire l'identifiant de l'utilisateur et crée un cookie permettant de récupérer cet identifiant par la suite. Le cookie est déposé sur le domaine du GAR et a une durée de vie de 30 minutes (configurable).

Dans le cas d'une mise à jour, la durée de vie du cookie est renouvelée dans la limite d'une durée de vie maximale de 6 heures (configurable).

L'utilisation d'un cookie d'authentification au niveau du GAR permet de limiter le flux envoyé vers les fournisseurs d'identité lors de l'accès récurrent à de multiples ressources.

Une fois le cookie créé ou mis à jour le processus se poursuit en §3.3.12

3.3.11 [Auth011] Extraction de l'identifiant de l'accédant

Lorsque le GAR reçoit une demande d'accès à une ressource et qu'un cookie d'authentification est présent et valide, le GAR récupère dans une base de données temporaire l'identifiant de l'accédant grâce au cookie d'authentification.

3.3.12 [Auth012] Récupération de l'url de la ressource

A partir de l'identifiant récupéré de la ressource (idSrc ou idRessource), le GAR récupère l'url de la ressource demandée.

3.3.13 [Auth013] Redirection vers la ressource

Pour une ressource web :

Si le paramètre Grain est fourni (étape [Auth001] Extraction des identifiants), alors :

- Le paramètre Grain est ajouté à l'url de la ressource avec la valeur fournie ;
- L'utilisateur est redirigé vers cette url contenant le paramètre Grain ;
- Il appartient alors à la ressource d'acheminer l'utilisateur vers l'url Grain.

Exemple :

Soit une ressource d'id ark:/54037/jlnd9g5g37m1.p/InaEdu06508 dont l'url d'accès (éditeur) est <https://fresques.ina.fr/jalons/>

Lors de l'appel à :

<https://sp-auth.partenaire.test-gar.education.fr/domaineGar?idENT=WjA=&idEtab=MDU2MTkzMVY=&idRessource=ark%3A%2F54037%2Fjlnd9g5g37m1.p%2FInaEdu06508&grain=https%3A%2F%2Ffresques.ina.fr%2Fjalons%2Ffiche-media%2FInaEdu06508%2FIna-reforme-des-bourses-etudiantes.html>

L'utilisateur est redirigé vers l'URL éditeur GAR Ressource auquel le paramètre Grain est ajouté :

<https://fresques.ina.fr/jalons/?grain=https%3A%2F%2Ffresques.ina.fr%2Fjalons%2Ffiche-media%2FInaEdu06508%2FIna-reforme-des-bourses-etudiantes.html>

Si le paramètre Grain n'est pas fourni (étape [Auth001] Extraction des identifiants), l'utilisateur est redirigé vers l'url de la ressource

Exemple :

Soit une ressource d'id ark:/54037/jlnd9g5g37m1.p/InaEdu06508 dont l'url d'accès (éditeur) est <https://fresques.ina.fr/jalons/>

Lors de l'appel à :

<https://sp-auth.partenaire.test-gar.education.fr/domaineGar?idENT=WjA=&idEtab=MDU2MTkzMVY=&idRessource=ark%3A%2F54037%2Fjlnd9g5g37m1.p%2FInaEdu06508>

L'utilisateur est redirigé vers l'URL éditeur GAR Ressource :

<https://fresques.ina.fr/jalons/>

Pour une ressource accédée en OpenIdConnect :

L'utilisateur est redirigé vers l'URL contenue dans le paramètre redirectUri de l'appel /authorize, comme le prévoit le protocole OpenIdConnect. La granularité peut être gérée par le fournisseur de ressources par l'intermédiaire de ce paramètre en y ajoutant toute information relative à cette granularité. La redirection vers la ressource sera faite sur redirectUri, qu'il contienne ou non le paramètre Grain. Le paramètre redirectUri peut par exemple prendre les formes suivantes :

- <https://maressource/anglais/chapitre1>
- <https://maressource/anglais?grain=chapitre1>
- <https://maressource/anglais?chapitre=chapitre1>
- etc....

3.3.14 [Auth014] Affichage d'une page d'erreur

3.3.14.1 Description de la page

En cas d'erreur, une page indiquant à l'accédant de se connecter à son Espace Numérique de Travail pour pouvoir accéder à la ressource est affichée. Le message affiché à l'accédant est configurable et contient les informations suivantes dans le pied de page :

« En cas de contact du support GAR, veuillez communiquer les informations suivantes en complément du message d'erreur :

- Date et heure d'apparition de l'erreur : <DATE_HEURE_ERREUR>
- User-agent : <USER_AGENT>

»

Variables :

- <DATE_HEURE_ERREUR> : horodatage d'apparition de l'erreur au format AAAA-MM-JJ hh:mm:ss GMT+/-hh:mm correspondant à celui de la plateforme GAR récupéré côté serveur et transmis par le header http dans la réponse du serveur
- <USER_AGENT> : attribut « User-Agent » tel que fourni par le navigateur du poste de l'utilisateur dans le header http

3.3.14.2 Exemple

- Corps de la page :

«

Accès refusé.

Merci de passer par votre ENT pour accéder aux ressources.

»

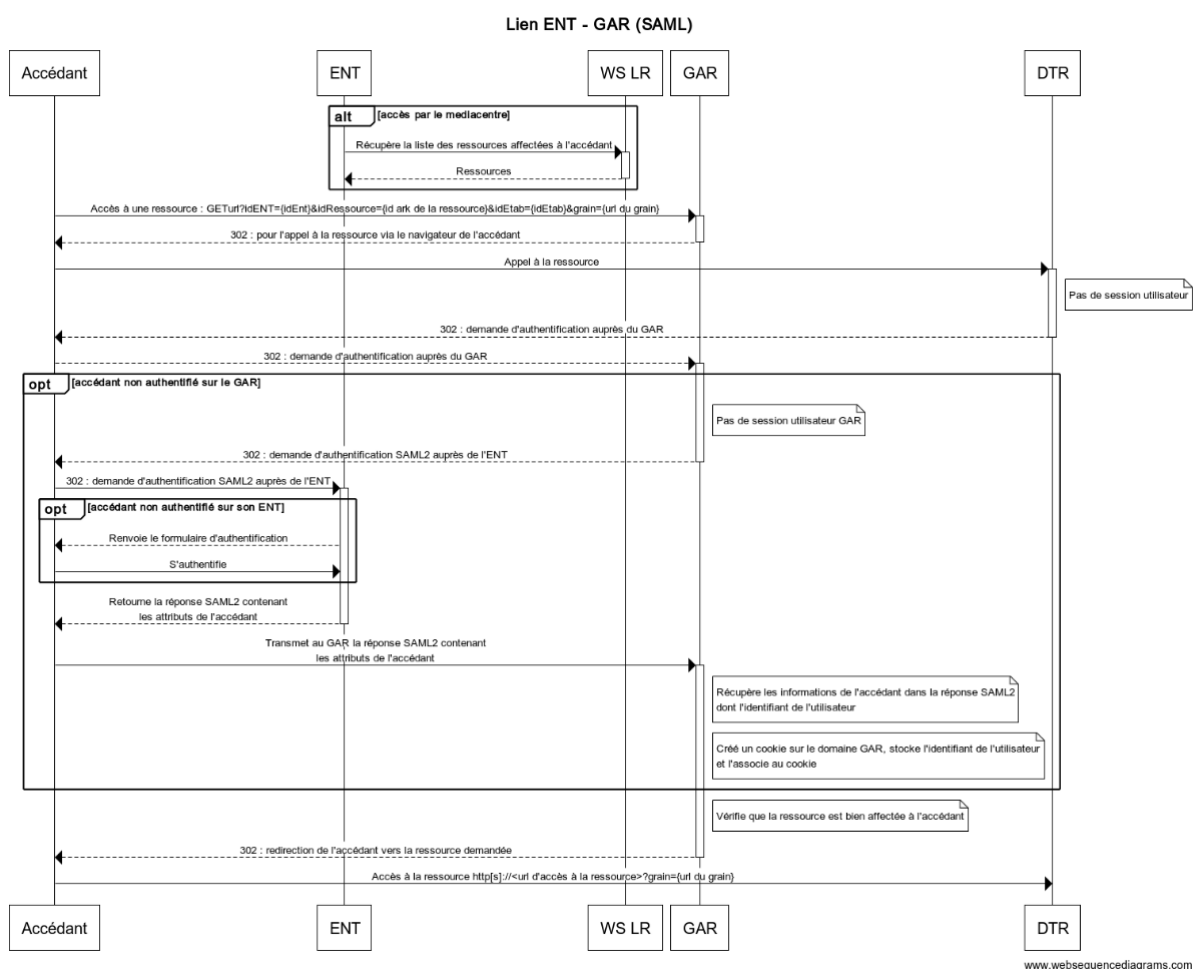
- Pied de page :

« En cas de contact du support GAR, veuillez communiquer les informations suivantes en complément du message d'erreur :

- Date et heure d'apparition de l'erreur : 2022-01-20 15:27:54 GMT+01:00
- User-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0

3.4 Flux lien fournisseur d'identité – GAR

3.4.1 ENT-GAR : Protocole SAML



3 Flux ENT – GAR (SAML)

3.4.2 ENT-GAR : Protocole OpenIdConnect

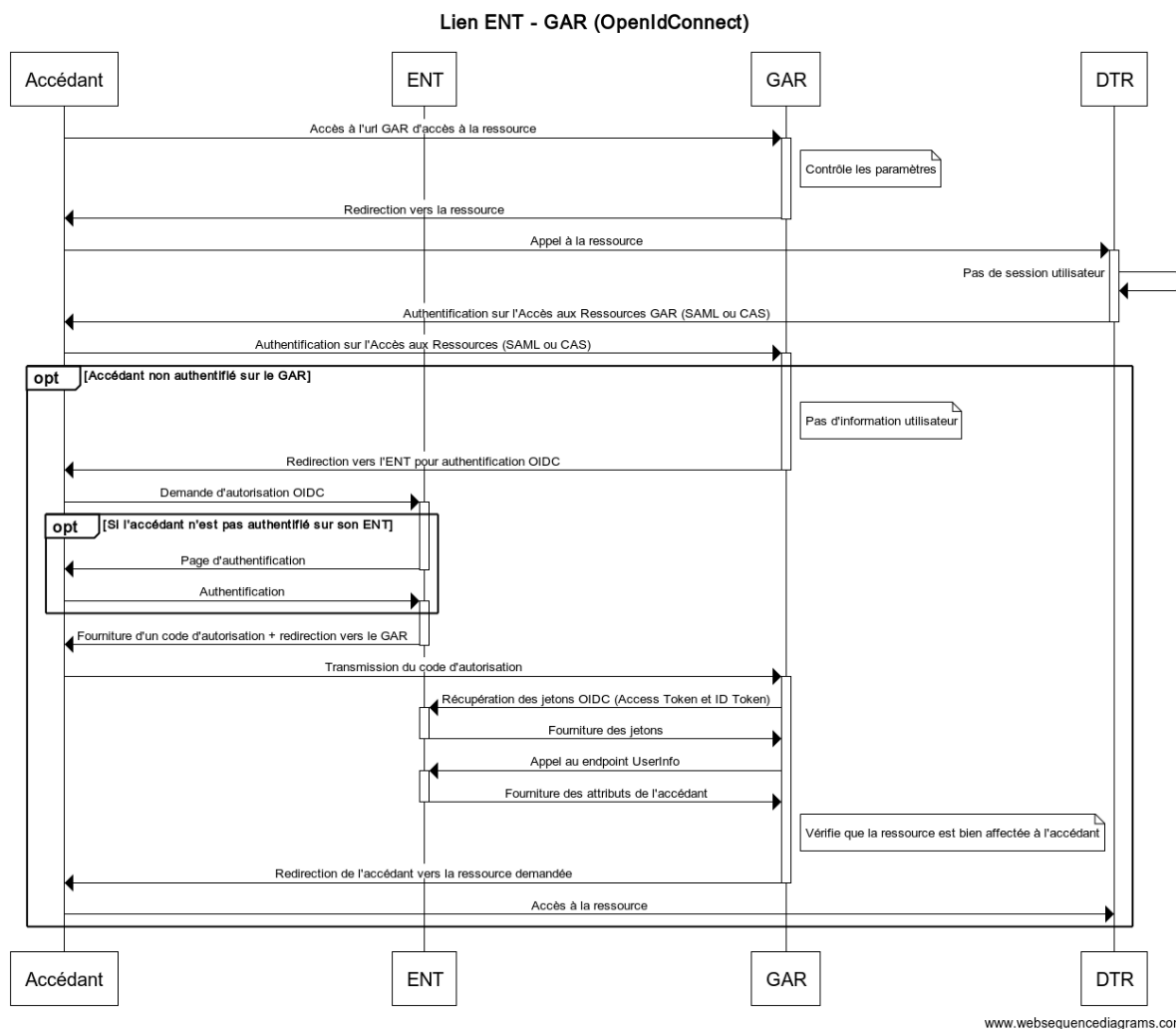


Figure 4: Lien ENT - GAR (OpenIdConnect)

3.4.3 Guichet d'authentification-GAR : Protocole OpenIdConnect

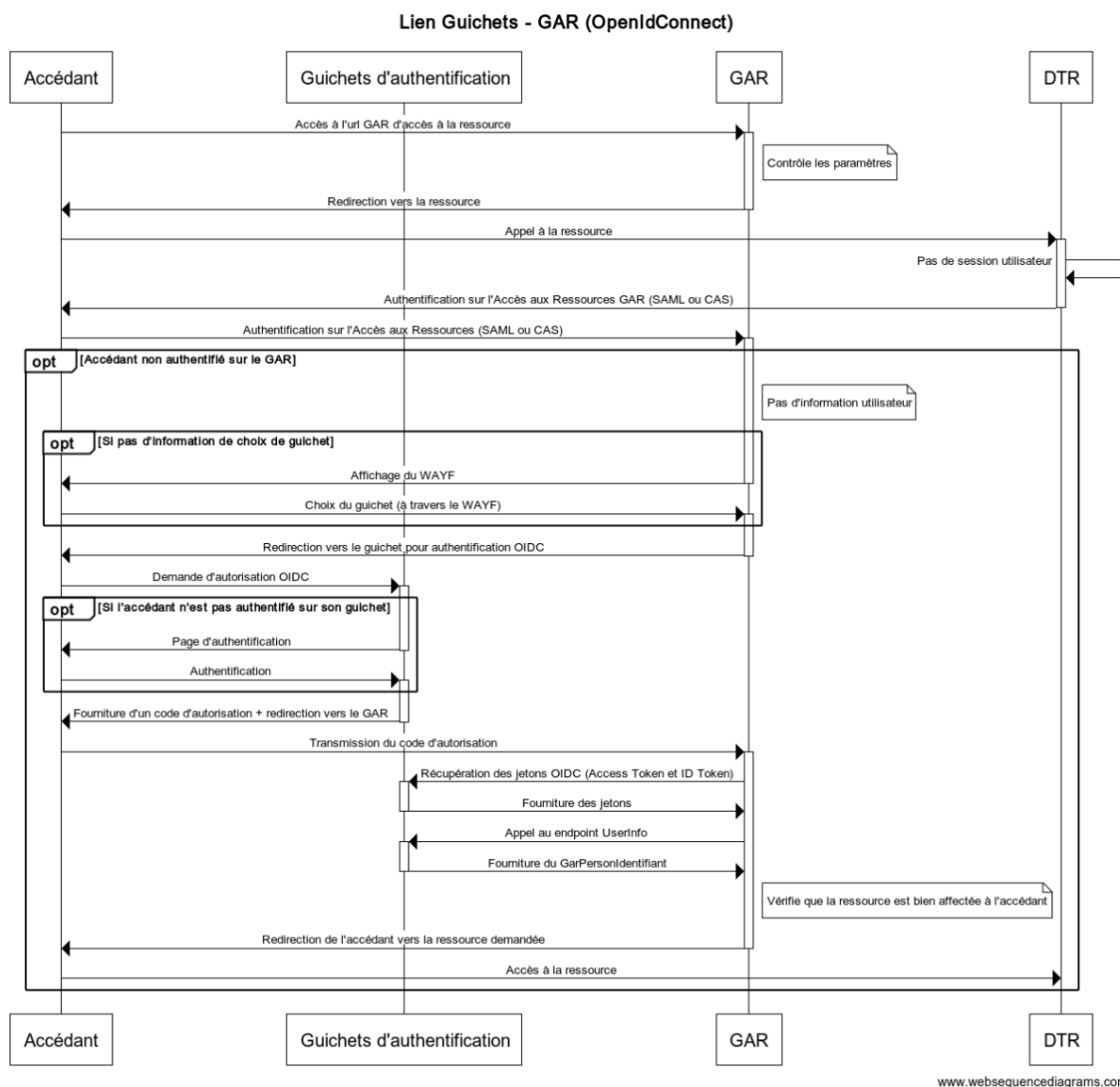


Figure 5: Lien Guichets - GAR (OpenIdConnect)

3.5 Identification du fournisseur d'identité

3.5.1 Accès web

Pour un accès web, l'URL d'accès à la ressource peut provenir d'un médiateur ou être forgée par le fournisseur de ressources. Afin de rediriger l'authentification vers l'ENT ou le guichet d'authentification de l'utilisateur, les paramètres idEtab, idpHint et profil qui peuvent être fournis dans l'URL d'accès à la ressource sont utilisés selon les règles suivantes :

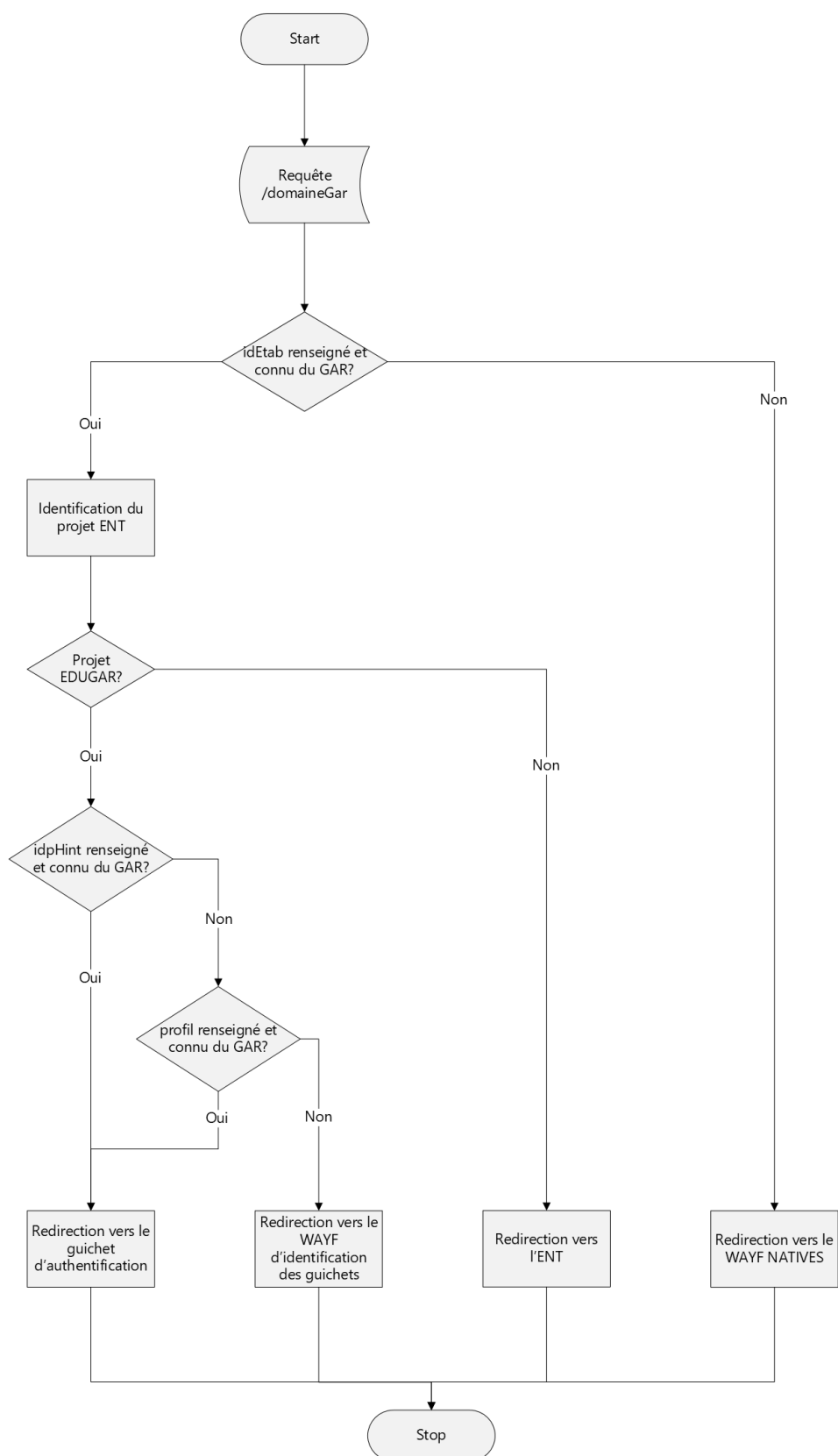


Figure 6 – Identification de l'IDP - accès web

RG	idEtab	idpHint	Profil	Description
RGIDP01	Absent ou inconnu du GAR	Ignoré	Ignoré	Redirection vers le WAYF NATIVES
RGIDP02	Présent ACA	Absent ou inconnu du GAR	Absent ou inconnu du GAR	Redirection vers le WAYF d'identification des guichets
RGIDP03	Présent ACA	Absent ou inconnu du GAR	Présent	Redirection vers le guichet d'authentification déduit du profil
RGIDP04	Présent ACA	Présent	Ignoré	Redirection vers le guichet d'authentification correspondant à l'idpHint
RGIDP05	Présent ENT	Ignoré	Ignoré	Redirection vers l'ENT

idEtab ENT se comprend comme correspondant à un établissement rattaché à un projet ENT territorial.
 idEtab ACA se comprend comme correspondant à un établissement rattaché à un projet EduGAR académique.

3.5.2 Accès par application native

Pour un accès par application native, l'utilisateur renseigne les informations nécessaires à l'identification du fournisseur d'identités par l'intermédiaire du WAYF NATIVES. A cet effet, les paramètres idEtab et profil sont positionnés sur l'url de demande de code d'autorisation selon les règles suivantes :

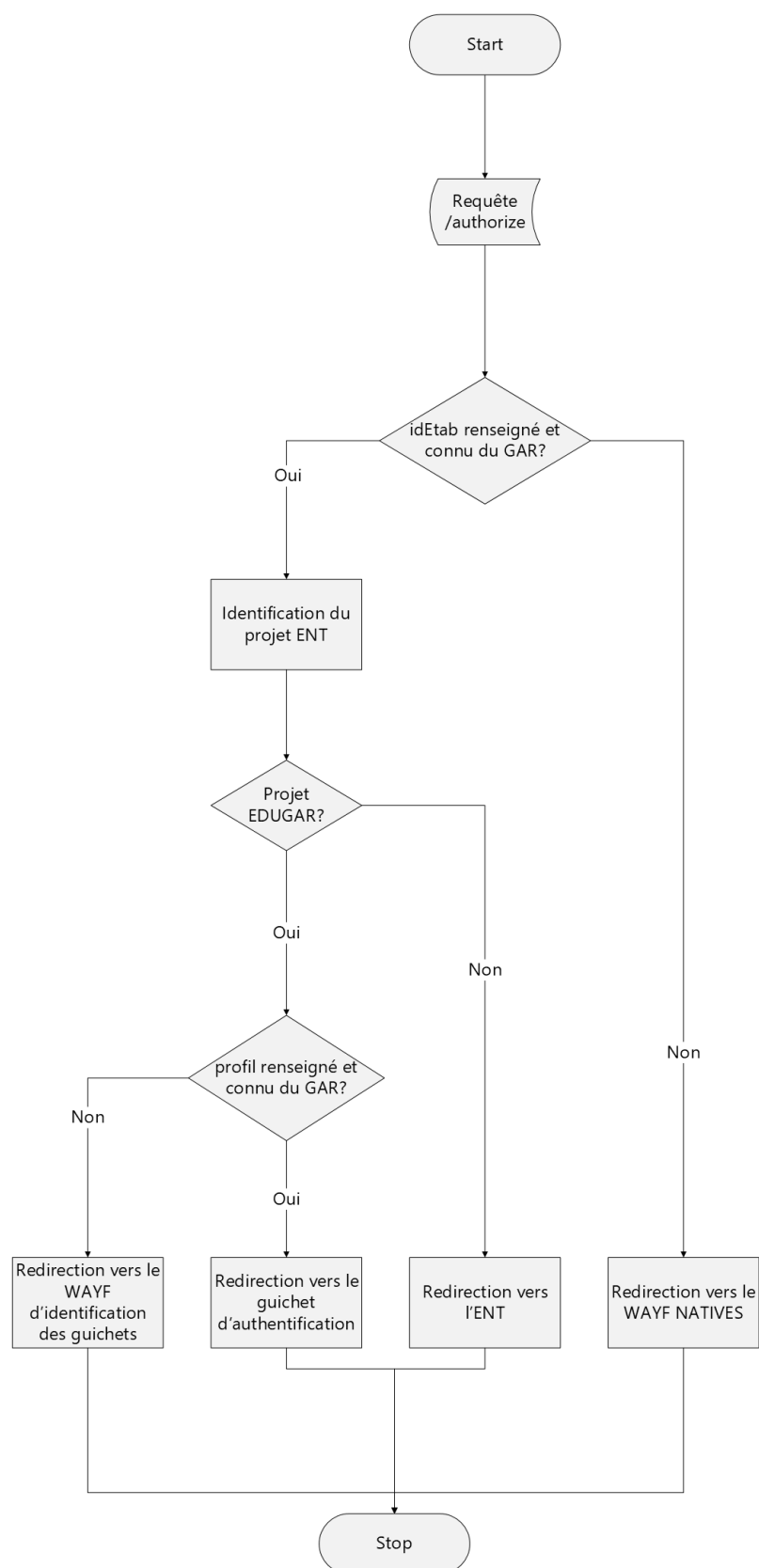


Figure 7 - Identification de l'IDP – accès par application native

RG	idEtab	Profil	Description
RGIDP06	Absent ou inconnu du GAR	Ignoré	Redirection vers le WAYF NATIVES
RGIDP07	Présent ACA	Absent ou inconnu du GAR	Redirection vers le WAYF d'identification des guichets
RGIDP08	Présent ACA	Présent	Redirection vers le guichet d'authentification pour une académie déduit du profil
RGIDP09	Présent ENT	Ignoré	Redirection vers l'ENT

idEtab ENT se comprend comme correspondant à un établissement rattaché à un projet ENT territorial.
idEtab ACA se comprend comme correspondant à un établissement rattaché à un projet EduGAR académique.

4 Lien GAR – DTR

4.1 Description

Une fois l'authentification de l'utilisateur auprès son fournisseur d'identité effectuée (voir §3) le GAR redirige l'utilisateur vers la ressource demandée.

Une fois l'utilisateur redirigé sur la ressource demandée, le Distributeur Technique de Ressource interroge le GAR pour valider que l'utilisateur est bien authentifié et pour récupérer les attributs de l'utilisateur.

Dans le cas d'un accès granulaire, le paramètre Grain peut être fourni par la ressource au GAR lors de l'échange d'authentification pour le protocole CAS dans le paramètre « Service » et pour le protocole SAML en mode SP global dans le paramètre « RelayState ». Pour le protocole SAML en mode SP monoressource le paramètre Grain ne peut pas être fourni par la ressource au GAR lors de l'échange d'authentification.

Pour l'OpenIdConnect, on utilise le paramètre *redirectUri* pour rediriger l'utilisateur vers une granularité de la ressource.

4.2 Gestion des métadonnées SAML des DTR

4.2.1 Mise en cache des métadonnées

L'accès aux ressources récupère les métadonnées du DTR à travers un cache des métadonnées des DTR.

Le cache est implémenté avec le séquençement suivant :

- Si les métadonnées sont présentes dans le cache, ces métadonnées sont utilisées par le service d'accès aux ressources
- Sinon une tentative de récupération des métadonnées chez le DTR est réalisée
 - Si les Méta Données du DTR ne sont pas disponibles, alors une tentative de récupération des MD est faite à chaque accès à une ressource de ce DTR.
 - Si les métadonnées sont accessibles, alors elles sont récupérées et mises en cache par le serveur ayant traité la demande. Ainsi, une fois mises en cache et cela durant toute la durée de validité du cache, il n'y a plus d'appel vers les MD du DTR.

Le délai de mise à jour dans le GAR en cas de changement dans les métadonnées du DTR par exemple lors de l'ajout d'une ressource dépend de la durée de conservation dans le cache.

L'exploitant GAR pourra forcer le rechargement des métadonnées d'un DTR.

Le DTR pourra créer une demande de support pour demander ce rechargement notamment en cas d'opération prévue.

Le cache des métadonnées est mis à jour quotidiennement à heure fixe via un appel aux métadonnées de chaque DTR. Les métadonnées ne sont mises en cache que si elles sont valides (cf. §4.2.2).

Si elles ne sont pas valides les métadonnées sont rejetées et le cache continue d'être utilisé.

En cas d'échec de mise en cache:

- Cas 1 : Les métadonnées ne sont pas déjà en cache, alors les ressources du DTR ne sont pas accessibles et une notification est envoyée au DTR avec les gestionnaires techniques en copie.
- Cas 2 : Les métadonnées sont en cache depuis moins de 7j (configurable), le cache est conservé et une notification est envoyée au DTR. Si les métadonnées sont en cache depuis plus de 4j (configurable), les gestionnaires techniques sont ajoutés en copie du mail.
- Cas 3 : Les métadonnées sont en cache depuis 7j (configurable), les métadonnées du DTR sont supprimées du cache, les ressources du DTR ne sont plus accessibles et une notification est envoyée au DTR avec les gestionnaires techniques en copie.

L'adresse mail utilisée pour le DTR est l'adresse de contact du site distributeur technique.

Les adresses mails utilisées pour les gestionnaires techniques sont les adresses de contact des comptes du portail GAR ayant un profil gestionnaires techniques.

4.2.2 Contrôle de validité

Les contrôles réalisés sur les métadonnées avant leur mise en cache sont les suivants.

Contrôle	actif
Conforme à la xsd SAML	Oui
La valeur de l'entity-id est bien celle fourni par le DTR	Oui
Name-id en mode transient	Non
Le profil logout en SOAP est disponible	Non

4.2.3 Notification

Objet du mail :

[GAR][<PTF>] Problème de mise en cache des métadonnées

Corps du message :

Date : <JJ-MM-YYYY>
 Module expéditeur : Mise en cache des métadonnées
 Fonction du destinataire : Distributeur technique de ressource

Le GAR n'a pu récupérer vos métadonnées pour l'accès aux ressource à l'adresse :
 <url>

L'erreur rencontrée est la suivante : <erreur>

<Conclusion>

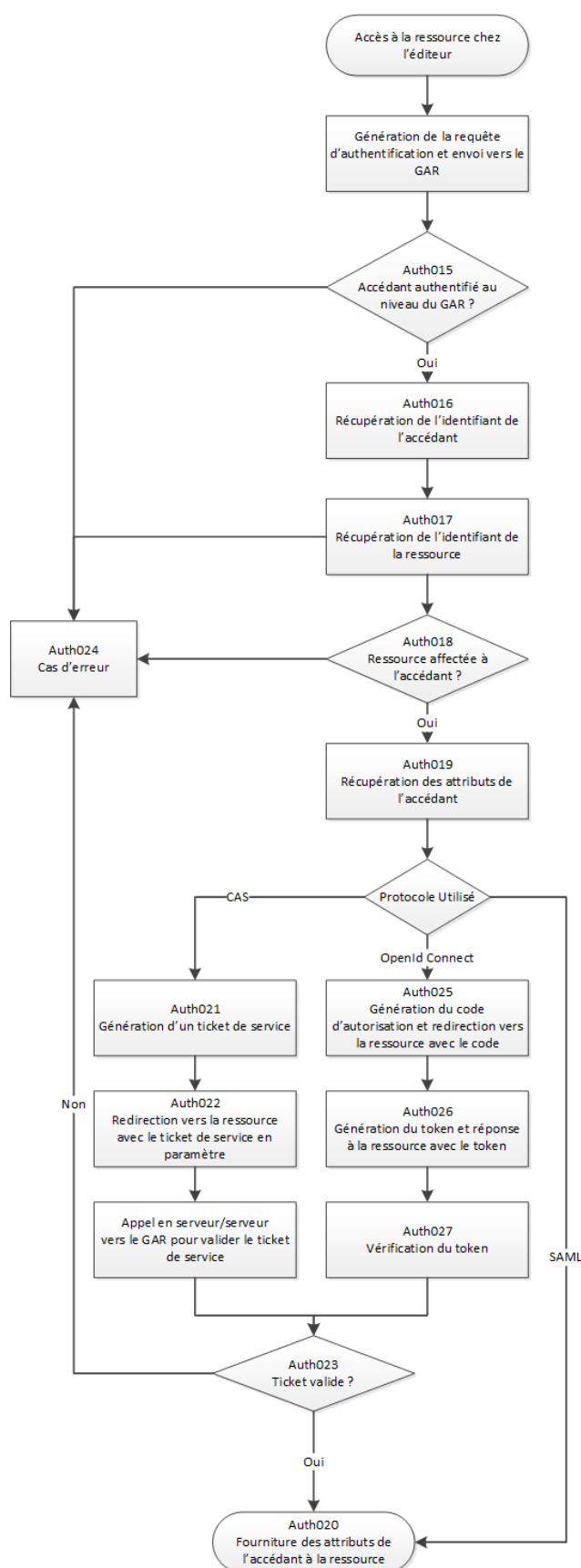
<SIGNATURE>

Les variables sont :

<erreur>	Exemples : <ul style="list-style-type: none"> • url non accessible • Contrôle de validité du champ <champ> • Réponse du serveur : Erreur 404
<Conclusion>	Cas 1 : Vos ressources ne sont actuellement pas accessibles via le GAR. Cas 2 : La version du <JJ-MM-DDDD> de vos métadonnées est utilisée par le GAR. Le cache sera utilisé jusqu'au <JJ-MM-DDDD>. Ensuite l'accès à vos ressources sera désactivé. Cas 3 : Vos ressources ne sont actuellement plus accessibles via le GAR.
<SIGNATURE>	signature commune à l'ensemble des mails envoyés par le GAR.

4.3 Diagramme fonctionnel

Le diagramme ci-dessous décrit le principe de fonctionnement du lien GAR – Ressource dans son ensemble. Les différences entre les versions CAS, SAML et OpenId Connect sont détaillées dans le paragraphe 4.4.



8 Diagramme GAR - DTR

4.4 Fonctionnement

Les étapes de validation de l'authentification pour le lien Fournisseur d'identité - GAR sont décrites ci-dessous.

4.4.1 [Auth015] Vérification de l'authentification au niveau du GAR

Le GAR vérifie si l'accédant possède déjà un cookie d'authentification positionné sur le domaine GAR. Si le cookie est présent, le GAR vérifie que le cookie correspond bien à une authentification existante. Si le cookie est invalide le GAR retourne une erreur (§0).

4.4.2 [Auth016] Récupération de l'identifiant de l'accédant

Le GAR, à partir de l'identifiant contenu dans le cookie d'authentification, récupère dans une base de données mémoire l'identifiant de l'accédant.

4.4.3 [Auth017] Récupération de l'identifiant de la ressource

Cette étape a pour but d'extraire l'url de la ressource des informations fournies par le SP appelant (paramètres de requête, assertion SAML...) et de récupérer les informations correspondantes dans les bases de données GAR (principalement l'identifiant).

Dans tous les cas, l'url de la ressource doit être unique dans la base de données GAR et si ce n'est pas le cas, une erreur est retournée (§4.4.7).

Des traitements différents sont faits selon la présence ou non du paramètre « RelayState ». Il a été convenu que :

- les SP Globaux / Multi ressources devaient utiliser le paramètre « RelayState ». Lorsque le paramètre « RelayState » est fourni, il est retransmis à l'identique à la ressource lors de la réponse (§4.4.6.1)
- Les SP mono ressources ne devaient pas utiliser le paramètre « RelayState »

À noter qu'un SP mono ressource pourrait utiliser le paramètre « RelayState », mais dans ce cas, il devra respecter le format d'appel lorsque le paramètre « RelayState » est fourni (voir détail dans le §4.4.3.1)

4.4.3.1 Cas du protocole SAML

Dans le cas de distributeurs commerciaux utilisant le protocole SAML, l'url de la ressource est extraite :

- Soit des paramètres de la requête (paramètre « RelayState ») si le paramètre « RelayState » est présent. En plus de l'url de la ressource, la valeur du paramètre « RelayState » peut contenir un paramètre Grain.
- Soit de la requête d'authentification (champ « saml2:issuer » du flux SAML) si le paramètre « RelayState » est absent

À partir de cette url, le GAR récupère l'identifiant de la ressource en base.

À noter que dans le cas où le paramètre « RelayState » est présent, l'issuer de la requête SAML doit contenir l'entityId du SP.

4.4.3.2 Cas du protocole CAS

Dans le cas de distributeurs commerciaux utilisant le protocole CAS, l'url de la ressource est récupérée dans les paramètres de la requête d'authentification (paramètre « Service »). A partir de cette url, le GAR récupère l'identifiant de la ressource en base. En plus de l'url de la ressource, la valeur du paramètre « Service » peut contenir un paramètre Grain.

4.4.3.3 Cas du protocole OpenId Connect

Variantes natives de ressources

L'url de redirection de la ressource correspond au `redirectUri` défini lors de l'appel au endpoint `/authorize`. Il doit correspondre au `redirectUri` déclaré dans la notice. Il correspond au deeplink vers la ressource dans l'application. Il peut comporter le paramètre « Grain » dans le cas d'un accès granulaire.

Variantes web de ressources

L'url de redirection de la ressource correspond au `redirectUri` défini lors de l'appel au endpoint `/authorize`. Il doit par défaut correspondre au `redirectUri` déclaré dans la plateforme via le WS Données d'initialisation tel que décrit dans le [DR14](#) mais il peut aussi comporter le paramètre Grain dans le cas d'un accès granulaire.

4.4.4 [Auth018] Vérification de l'autorisation d'accès

4.4.4.1 [Auth018a] Vérification de l'autorisation d'accès commune

Le GAR vérifie, à partir de l'identifiant de l'accédant récupéré en §4.4.2 et l'identifiant de la ressource récupéré en §4.4.3 que la ressource est bien affectée à l'accédant, que la licence est toujours valide et que la fourniture des données à caractère personnel a été validée. Cette vérification permet aussi de valider que la ressource qui appelle le fournisseur d'identité du GAR est bien déclarée au niveau du GAR. Si une des vérifications échoue, une erreur est retournée §4.4.7.

4.4.4.2 [Auth018b] Contrôle du nombre d'accédant simultané

Dans le cas d'un abonnement avec une catégorie d'affectation « flottante », le service vérifie le nombre de jeton d'accès restant, c'est-à-dire que le nombre d'accédant à la ressource est inférieur au nombre maximum d'accédant simultané autorisé dans l'abonnement correspondant.

- Si l'accédant a déjà un jeton d'accès
L'accès est autorisé, la durée de réservation du jeton est réinitialisée.

S'il reste des jetons d'accès

- Un jeton est réservé pour cet accédant et l'accès est autorisé.
- S'il ne reste pas de jeton d'accès
L'accès est refusé. Un message d'erreur spécifique indiquant que tous les jetons d'accès sont actuellement utilisés est affiché à l'accédant.

La durée de réservation d'un jeton d'accès dans le GAR est configurable (2h par défaut). Les jetons d'accès sont automatiquement libérés à l'issue du délai (horodatage du dernier accès à la ressource par l'accédant via le GAR + durée de réservation).

4.4.5 [Auth019] Récupération des attributs de l'accédant

A partir de l'identifiant de l'accédant récupéré en §4.4.2 et l'identifiant de la ressource §4.4.3 le GAR récupère en base les attributs de l'accédant.

4.4.6 [Auth020] Fourniture des attributs à la ressource

4.4.6.1 Cas du protocole SAML

Dans le cas du protocole SAML, le GAR retourne les attributs de l'accédant dans l'assertion d'authentification SAML. Dans le cas d'un SP Global, la valeur du paramètre « RelayState » fournie par la ressource est utilisée pour la réponse.

4.4.6.2 Cas du protocole CAS

Dans le cas du protocole CAS, suivant l'url appelée pour valider le ticket de service le GAR retourne la liste des attributs de l'accédant soit sous forme de XML soit sous forme de JSON.

[Auth021][CAS] Génération du ticket de service

Le GAR génère un ticket de service associé à la demande d'authentification de l'utilisateur pour la ressource demandée. Ce ticket de service n'est utilisable qu'une fois et a une durée de vie limitée (§2.2.2).

[Auth022][CAS] Redirection vers la ressource

Le GAR redirige l'accédant vers l'url passée en paramètre de la requête d'authentification (paramètre « Service ») en passant le ticket de service en paramètre et la valeur du service reçu lors de la demande d'authentification (url d'accès à la ressource et optionnellement le paramètre Grain).

[Auth023][CAS] Validation du ticket de service

Le distributeur technique de ressource appelle le GAR en mode serveur-serveur pour valider le ticket de service. La requête envoyée vers le GAR contient le ticket de service et un paramètre « Service » contenant l'url qui a reçu le ticket de service (url d'accès à la ressource et optionnellement le paramètre Grain). Le GAR valide le ticket de service passé en paramètre de requête. Si le ticket est valide, le processus se poursuit en §4.4.6.4. Si le ticket est invalide (ne correspond pas à la ressource demandée, a déjà été utilisé, inconnu au niveau du GAR) une erreur est retournée.

4.4.6.3 Cas du protocole OpenIdConnect

[Auth025][OIDC] Génération du code d'autorisation

Le GAR génère un code d'autorisation associé à la demande d'autorisation formulée par la ressource pour l'utilisateur sur la ressource demandée. Il redirige ensuite l'utilisateur vers la ressource en utilisant le redirectUri déclaré en paramètre avec le code d'autorisation. Dans le cas d'une variante native, ce redirectUri permet de rediriger l'utilisateur vers l'application native.

[Auth026][OIDC] Génération de l'Access Token

La ressource sollicite un Access Token (AT) au GAR en échange du code d'autorisation précédemment fourni. Le GAR contrôle la validité de ce code et génère l'AT qu'il renvoie à la ressource.

[Auth027][OIDC] Vérification de l'Access Token

La ressource va solliciter le GAR pour obtenir les DCP de l'utilisateur en échange de l'Access Token obtenu précédemment, de son idRessource et d'un access_mode. Le GAR contrôle la validité de cet Access Token (durée, session valide), de l'idRessource et de l'access_mode, conformément au processus décrit au §4.4.8. Si toutes les règles de gestion sont valides, le processus se poursuit en §4.4.6.4, sinon, une erreur est retournée.

4.4.6.4 Attributs DCP

Le tableau ci-dessous présente les attributs DCP (classiques, supplémentaires) retournés par le GAR et le code correspondant utilisé dans les flux de réponse d'authentification (CAS, SAML 2.0 ou OIDC).

Code	Valeur	Multivalué	Description pour les accédants de 2 nd degré	Description pour les accédants de 1 ^{er} degré
UAI	Code établissement	N	UAI (code d'Unité Administrative immatriculée)	
IDO	Id opaque	N	Identifiant de l'utilisateur spécifique à la ressource, garantissant l'absence de retour vers les informations personnelles	
PRO	Profil	O	Identifiant(s) du ou des profil(s) de l'accédant (PROFIL_NATIONAL : National_ELV, National_ENS, National_DOC, National_DIR, National_EVS, National_ETA, National_COL)	
DIV	Division(s)	O	Code de la ou des divisions, libellé de la ou des divisions	
GRO	Groupe(s)	O	Code du ou des groupes, libellé du ou des groupes	
DIV_APP	Division(s) d'appartenance	O	Code du ou des groupes, code du ou des divisions d'appartenance du ou des groupes, libellé du ou des divisions d'appartenance du ou des groupes	
E_MS1	Degré d'enseignement (élève)	O	Code (MEF_STAT_1) (cf. RG1)	Code (MEF_STAT_1) (cf. RG2)
E_MS2	Cycle de scolarité (élève)	O	Code (MEF_STAT_2) (cf. RG1)	Code (MEF_STAT_2) (cf. RG2)
E_MS3	Dispositif de formation (élève)	O	Code (MEF_STAT_3) (cf. RG1)	Code (MEF_STAT_3) (cf. RG2)
E_MS4	Niveau de formation (élève)	O	Code (MEF_STAT_4) (cf. RG1)	Code (MEF_STAT_4) (cf. RG2)
E_MS5	Filière (élève)	O	Code (MEF_STAT_5) (cf. RG1)	Code (MEF_STAT_5) (cf. RG2)
E_MAT	Enseignements suivis (élève)	O	Code des enseignements suivis tels qu'ils sont dans les référentiels sources + libellé	Vide
P_MAT	Matières enseignées (documentaliste ou enseignant ou autre personnel)	O	Codes des matières enseignées tels qu'ils sont dans les référentiels source + libellés	Vide

Code	Valeur	Multivalué	Description pour les accédants de 2 nd degré	Description pour les accédants de 1 ^{er} degré
P_MS1	Degré(s) d'enseignement (documentaliste ou enseignant ou autre personnel)	O	Code(s) (MEF_STAT_1) (cf. RG1)	Code(s) (MEF_STAT_1) (cf. RG2)
P_MS2	Cycle(s) de scolarité (documentaliste ou enseignant ou autre personnel)	O	Code(s) (MEF_STAT_2) (cf. RG1)	Code(s) (MEF_STAT_2) (cf. RG2)
P_MS3	Dispositif(s) de formation (documentaliste ou enseignant ou autre personnel)	O	Code(s) (MEF_STAT_3) (cf. RG1)	Code(s) (MEF_STAT_3) (cf. RG2)
P_MS4	Niveau(x) de formation (documentaliste ou enseignant ou autre personnel)	O	Code(s) (MEF_STAT_4) (cf. RG1)	Code(s) (MEF_STAT_4) (cf. RG2)
P_MS5	Filière(s) (documentaliste ou enseignant ou autre personnel)	O	Code(s) (MEF_STAT_5) (cf. RG1)	Code(s) (MEF_STAT_5) (cf. RG2)
CIV	Titre de civilité	N	M., Mme	
NOM	Nom d'usage	N	Nom d'usage	
PRE	Prénom usuel	N	Prénom	
NPA	Nom patronymique	N	Nom de famille	
APR	Autres prénoms	N	Autres prénoms	
E_MS6	Code de la série du bac G & T ou type de CPGE (élève)	O	Code MEF STAT 6 (cf. RG1)	Code MEF STAT 6 (cf. RG2)
E_MS7	Code de la catégorie de spécialités (élève)	O	Code MEF STAT 7 (cf. RG1)	Code MEF STAT 7 (cf. RG2)
E_MS8	Code du domaine de spécialités (élève)	O	Code MEF STAT 8 (cf. RG1)	Code MEF STAT 8 (cf. RG2)
E_MS9	Code du groupe de spécialités (élève)	O	Code MEF STAT 9 (cf. RG1)	Code MEF STAT 9 (cf. RG2)
E_MS10	Code MEF STAT 10 (élève)	O	Code MEF STAT 10 (cf. RG1)	Code MEF STAT 10 (cf. RG2)
E_MS11	Code MEF STAT 11 (élève)	O	Code MEF STAT 11 (cf. RG1)	Code MEF STAT 11 (cf. RG2)
E_MEF	MEF(s) et libellé(s) MEF (élève)	O	Module(s) élémentaires de formation(MEF) et libellé(s)	Vide
E_NAI	Date de naissance (élève)	N	Date de naissance de	

Code	Valeur	Multivalué	Description pour accédants les de 2 nd degré	Description pour accédants les de 1 ^{er} degré
			l'élève (cf. RG6)	
P_DIS	Code(s) de discipline(s) de poste (documentaliste ou enseignant ou autre personnel)	O	Discipline(s) de poste	Vide
P_SPE	Code(s) de spécialité(s) de poste (documentaliste ou enseignant ou autre personnel)	O	Vide	Codes des spécialités enseignées tels qu'ils sont dans les référentiels sources
P_MEF	MEF(s) et libellé(s) MEF (documentaliste ou enseignant ou autre personnel)	O	Module(s) élémentaires de formation(MEF) et libellé(s)	Vide
P_MS6	Code de la série du bac G & T ou type de CPGE (documentaliste ou enseignant ou autre personnel)	O	Code MEF STAT 6 (cf. RG1)	Code MEF STAT 6 (cf. RG2)
P_MS7	Code de la catégorie de spécialités (documentaliste ou enseignant ou autre personnel)	O	Code MEF STAT 7 (cf. RG1)	Code MEF STAT 7 (cf. RG2)
P_MS8	Code du domaine de spécialités (documentaliste ou enseignant ou autre personnel)	O	Code MEF STAT 8 (cf. RG1)	Code MEF STAT 8 (cf. RG2)
P_MS9	Code du groupe de spécialités (enseignant)	O	Code MEF STAT 9 (cf. RG1)	Code MEF STAT 9 (cf. RG2)
P_MS10	Code MEF STAT 10 (documentaliste ou enseignant ou autre personnel)	O	Code MEF STAT 10 (cf. RG1)	Code MEF STAT 10 complété grâce à table de correspondance
P_MS11	Code MEF STAT 11 (documentaliste ou enseignant ou autre personnel)	O	Code MEF STAT 11 (cf. RG1)	Code MEF STAT 11 (cf. RG2)
idENT	Code projet ENT	N	Code projet ENT encodé en base 64	
P_MEL	adresse(s) de courriel de	O	adresse(s) de courriel de l'enseignant (documentaliste	

Code	Valeur	Multivalué	Description pour accédants les de 2 nd degré	Description pour accédants les de 1 ^{er} degré
	l'enseignant (documentaliste ou enseignant ou autre personnel)		ou enseignant ou autre personnel)	

Le tableau ci-dessous présente les attributs DCP familles retournés par le GAR et le code correspondant utilisé dans les flux de réponse d'authentification (CAS ou SAML 2.0).

Code	Valeur	Multivalué	Description
IDC	Identifiant complémentaire	O	Identifiant(s) de la ou des famille(s) à laquelle la ressource appartient et dont les mères de famille ont été affectées à l'accédant
LRA	Liste des ressources appelées	O	Liste des ressources appelées par la ressource et qui sont affectées à l'accédant. URL d'accès à la ressource issu de la notice permettant d'initier une connexion SP-initiated

Un attribut de type multivalué est répété autant de fois dans la réponse d'authentification qu'il n'a de valeurs possibles.

Le séparateur ## est utilisé pour les attributs DIV et GRO pour séparer les codes des libellés (code##libellé).

Le séparateur || est utilisé pour les attributs DIV_APP pour séparer les codes des groupes des codes des divisions d'appartenance et le séparateur ## est utilisé pour séparer les codes des libellés (codeGroupe||CodeDivisionAppartenance##LibelleDivisionAppartenance).

Exemple :

Pour le groupe (code : grp_code1) appartenant à 2 divisions d'appartenances :

- avec le code div_code1 et libellé division1
- avec le code div_code2 et libellé division2

Les informations suivantes sont retournées :

Grp_code1||div_code1##division1

Grp_code1||div_code2##division2

Le séparateur « , » est utilisé pour les attributs IDC et LRA.

RG1 : Concernant les attributs DCP [EIP]_MSX, voici le mode de récupération pour le second degré :

1. Récupération des X premiers caractères du MEF_STAT_11 associé au MEF dans la table GAR_ENT.mef pour l'établissement de l'accédant
2. Si vide, Récupération des X premiers caractères du MEF_STAT_11 associé au MEF dans la table de correspondance N_MEF

Il n'y pas de vérification sur la taille du champ MEF_STAT_11 associé au MEF dans la table GAR_ENT.mef.

Exemple : si la taille du MEF_STAT_11 ne contient que 5 caractères alors seulement 5 caractères seront retournés pour l'attribut P_MS11.

RG2 : Concernant les attributs DCP [EIP]_MSX, voici le mode de récupération pour le premier degré :

1. Récupération des X premiers caractères du MEF_STAT_11 associé au MEF_STAT_4 dans la table de correspondance « MEF_STAT_4 / MEF_STAT_11 »

Chaque valeur de l'attribut IDC est composée sous la forme : [id_famille]_[idOpaqueFamille]

RG3 : Concernant l'attribut DIV_APP, il est automatiquement transmis dès que l'attribut GRO est demandé.

RG4 : Pour une ressource technique commune (RTC), concernant l'attribut IDO, il est généré dynamiquement lors de la demande d'attribut. (Cf. DR11 pour plus de détails sur la règle de construction de l'IDO)

RG5 : Si la plateforme à laquelle appartient la notice l'autorise, un attribut ACCESS_TOKEN est envoyé à chaque demande de DCP pour les protocoles SAML et CAS. C'est un attribut technique, il n'est pas considéré ni géré comme un DCP dans le GAR. Il est utilisé pour récupérer les attributs en échange de ce token sans passer par une réauthentification, comme l'offre le protocole OAuth (cf. §4.4.8).

RG6 : L'attribut E_NAI est transmis avec la date de naissance de l'élève ayant demandé l'accès à la ressource provenant de la table GAR_ENT.identite sous le format « AAAA-MM-JJ ».

4.4.7 [Auth024] Cas d'erreur

En cas d'erreur lors du processus d'authentification et fourniture des attributs de l'utilisateur une erreur sera remontée au distributeur de ressource conformément au protocole utilisé.

Lorsque le GAR reçoit une requête d'authentification venant d'une ressource et qu'aucun cookie d'authentification n'est présent au niveau du GAR le GAR est dans l'impossibilité d'identifier l'accédant lié à cette demande, une erreur est dans ce cas retournée vers le DTR qui a initié la requête.

4.4.8 Usages particuliers de l'Access Token

L'Access Token peut être utilisé pour demander les DCP sans passer par une authentification.

Pour fluidifier le parcours utilisateur, deux ressources peuvent avoir besoin de partager un Access Token obtenu du GAR par une autre ressource pour demander les DCP sans passer par une authentification.

4.4.8.1 Obtention de l'Access Token

La génération et l'envoi d'un Access Token par le GAR à la ressource sont systématiques dans le cas du protocole OIDC, quel que soit le paramétrage de la plateforme concernant la fourniture d'un Access Token.

Pour répondre aux cas d'usage décrits au paragraphe suivant, le GAR offre la possibilité d'obtenir un Access Token via l'authentification en CAS ou en SAML. Dans le cas d'une authentification OIDC, seul l'Access Token protocolaire est fourni.

Par défaut en CAS et en SAML, l'émission de l'Access Token est désactivée.

RENATER lors d'échange avec les DTR aura identifié les plateformes pour lesquelles l'Access Token est à fournir ou pas en CAS et en SAML. L'information est prise en compte en base de données dans un champ de la table plateforme du DTR.

Dans le cas d'une authentification en CAS ou en SAML, le GAR générera alors un Access Token si la valeur est à fournir. Cette information est récupérée à l'initialisation de la demande d'accès à la ressource sur le point d'entrée /domaineGar et réutilisée lors de la fourniture des DCP.

L'Access Token généré est envoyé parmi les attributs DCP comme l'indique la RG5 du §4.4.6.4.

4.4.8.2 Utilisation de l'Access Token

Partage de l'AT entre les différents modes d'expositions (web/natives) d'une même ressource

L'utilisateur accède à une ressource Web via une URL GAR (médiacentre, favoris, etc.).

La ressource web s'authentifie en CAS, SAML ou OIDC auprès du GAR et récupère un Access Token, selon les conditions décrites ci-dessus.

L'utilisateur accède à la même ressource en mode application native depuis son application Web.

La ressource web transmet son AT à l'application native de façon sécurisée.

L'application native présente l'AT, l'identifiant ark de la ressource et l'access_mode (« appnat ») au GAR pour récupérer ses DCP.

Le GAR vérifie que l'AT est valide (durée, session valide) et que l'identifiant ark de la ressource de l'AT est le même que celui indiqué en paramètre de la requête.

A la suite de ces contrôles, le GAR fournit les DCP associées à la ressource.

Le cas d'usage inverse (accès à la ressource en mode application native en premier puis accès à la ressource en mode web avec l'AT obtenu de l'application native) est valide également, avec le même mode de fonctionnement et les mêmes contrôles. L'access_mode indiqué sera dans ce cas « web ».

Récupération de DCP pour des ressources de type portail avec authentification unique

L'utilisateur accède et s'authentifie à une première ressource via la séquence complète d'authentification GAR.

La ressource récupère ses DCP et un Access Token.

Depuis la première ressource, l'utilisateur accède à une autre ressource, appartenant à la même plateforme DTR que la première.

La première ressource transmet de façon sécurisée son AT à la deuxième ressource.

La deuxième ressource présente au GAR son propre identifiant ark ainsi que l'AT obtenu de la première ressource et l'access_mode (« web » ou « appnat » suivant les cas) afin de demander à récupérer ses DCP. Il n'y a, dans ce cas, pas de passage par le processus d'authentification.

Le GAR vérifie que l'AT est valide (durée, session valide) et que l'identifiant ark passé en paramètre de la requête appartient à la même plateforme DTR que celui de la ressource pour lequel l'Access Token a été généré.

Le GAR vérifie ensuite les autorisations d'accès à cette deuxième ressource (cf §4.4.4).

A la suite de ces contrôles, le GAR calcule les DCP propres à cette deuxième ressource et les transmet.

Partage de l'AT entre une ressource Web/native et une ressource technique commune

L'utilisateur accède et s'authentifie à une ressource web/native (en SAML, CAS ou OIDC).

La ressource récupère ses DCP et un Access Token.

La ressource sollicite une ressource technique commune (RTC) et lui transmet son AT de façon sécurisée.

La RTC présente au GAR son propre identifiant ark ainsi que l'AT obtenu de la ressource appelante et l'access_mode (« rtc ») afin de demander à récupérer ses DCP.

Le GAR vérifie que l'AT est valide (durée, session valide) et que l'identifiant ark passé en paramètre de la requête correspond à une RTC et que l'identifiant ark de la ressource liée à l'Access Token fait partie des ressources appelantes déclarées dans la notice de la RTC.

A la suite de ces contrôles, le GAR calcule les DCP propres à la RTC et les transmet.

Autorisation d'accès au WS RAA par Access Token

L'utilisateur accède et s'authentifie à une ressource.

La ressource récupère ses DCP et un Access Token.

Le DTR sollicite le WS RAA du GAR, avec l'identifiant ark d'une ressource ainsi que l'AT obtenu lors de l'accès à la ressource.

Le WS RAA sollicite le service d'accès au ressource avec l'access_mode « wsraa » pour vérifier que :

- l'AT est valide (durée, session valide),

- l'identifiant ark passé en paramètre de la requête est identique ou appartient à la même plateforme DTR que la ressource pour lequel l'AT a été généré, ou pour le cas des RTC que l'identifiant ark de l'Access Token fait partie des ressources liés à la RTC.

A la suite de ces contrôles, le service d'accès aux ressources transmet au WS RAA les DCP IDO et UAI associées à la ressource de l'Access Token.

Récapitulatif des contrôles liés à l'access Token

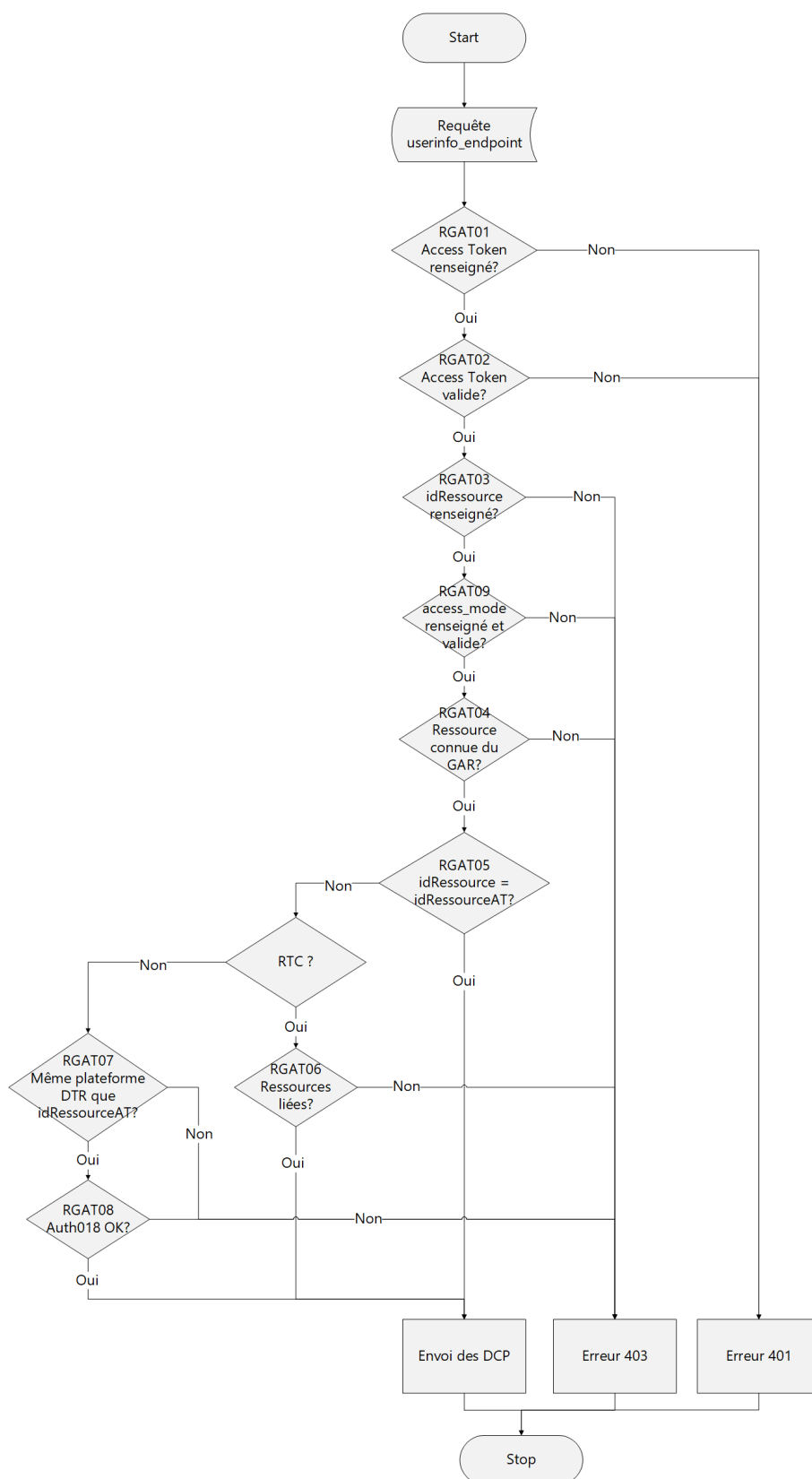


Figure 9 - Accès aux DCP via l'Access Token

Tableau 1 : Récapitulatif des contrôles liés à l'Access Token

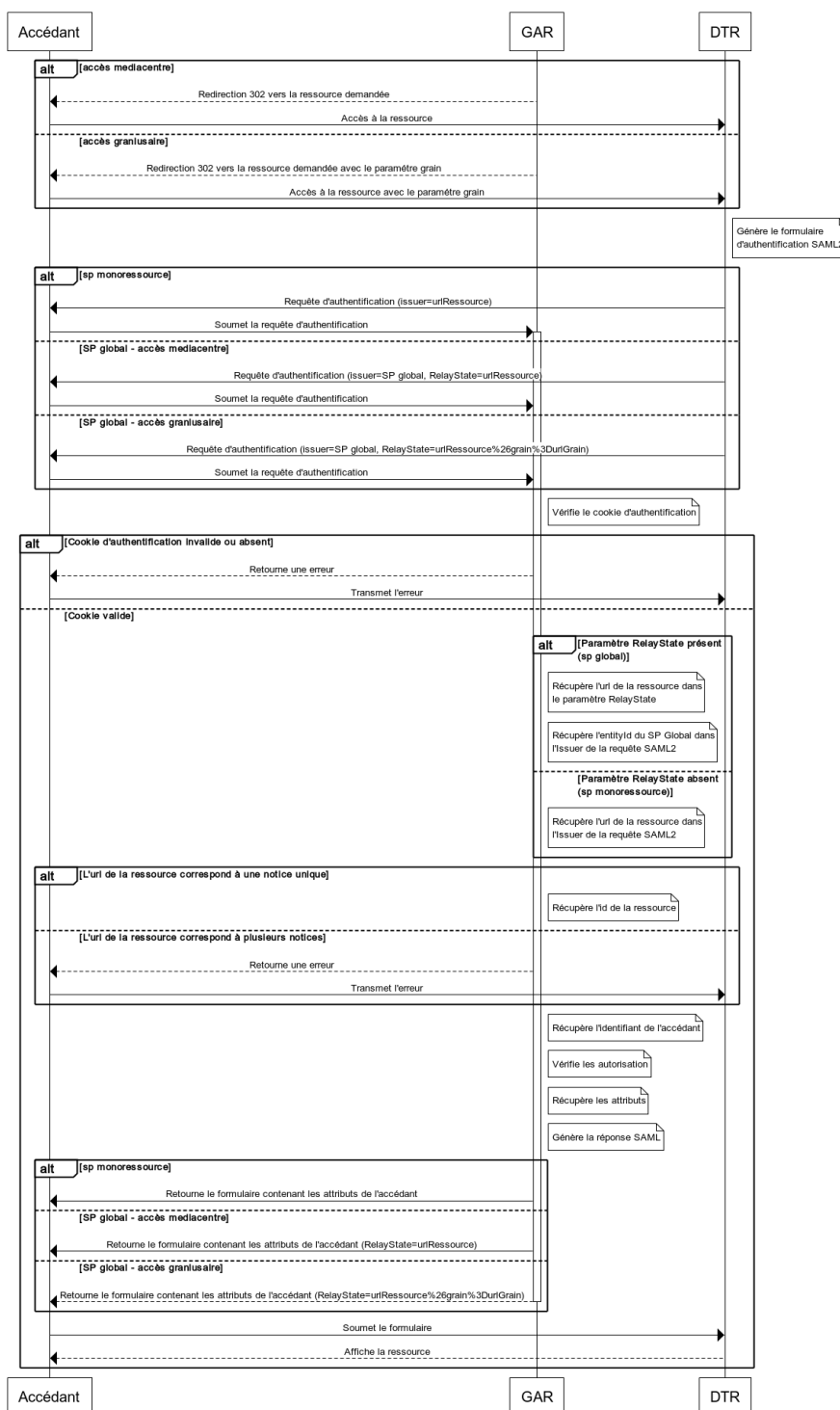
RG	Access Token	IdRessource ark	access_mode	Lien	Autorisation d'accès [Auth018]	Réponse
RGAT01	Absent	Ignoré	Ignoré	Ignoré	Ignoré	401 Unauthorized missing_accessToken
RGAT02	Invalide	Ignoré	Ignoré	Ignoré	Ignoré	401 Unauthorized expired_accessToken
RGAT03	Valide	Absent	Ignoré	Ignoré	Ignoré	403 Forbidden Paramètre idRessource obligatoire
RGAT09	Valide	Présent	Absent ou Invalide	Ignoré	Ignoré	403 Forbidden Paramètre access_mode manquant ou invalide. [web appnat rtc wsraa] attendu.
RGAT04	Valide	Non connu du GAR	Valide	Ignoré	Ignoré	403 Forbidden La ressource demandée n'existe pas
RGAT05	Valide	égal à idRessourceAT	Valide	N/A	N/A	200 OK Envoi des DCP
RGAT06	Valide	idRTC	Valide	idRessourceAT non lié	N/A	403 Forbidden La RTC demandée n'est pas liée à la ressource de l'Access Token.
RGAT06	Valide	idRTC	Valide	idRessourceAT lié	N/A	200 OK Envoi des DCP
RGAT07	Valide	différent de idRessourceAT	Valide	Plateforme DTR différente de celle de idRessourceAT	Ignoré	403 Forbidden La ressource demandée n'appartient pas à la même plateforme DTR que la ressource de l'Access Token.
RGAT08	Valide	différent de idRessourceAT	Valide	Même plateforme DTR que idRessourceAT	Invalide	403 Forbidden Cf §4.4.4
RGAT08	Valide	différent de idRessourceAT	Valide	Même plateforme DTR que idRessourceAT	Valide	200 OK Envoi des DCP

RGAT09 : Le paramètre access_mode dans la requête est obligatoire et peut prendre 4 valeurs : « appnat », « web », ou « rtc » ou « wsraa ».

RGAT10 : -Dans le cas où le mode d'accès renseigné dans la requête est « wsraa », seuls les attributs IDO et UAI de la ressource liée à l'Access Token sont retournés au service appelant (WS RAA).

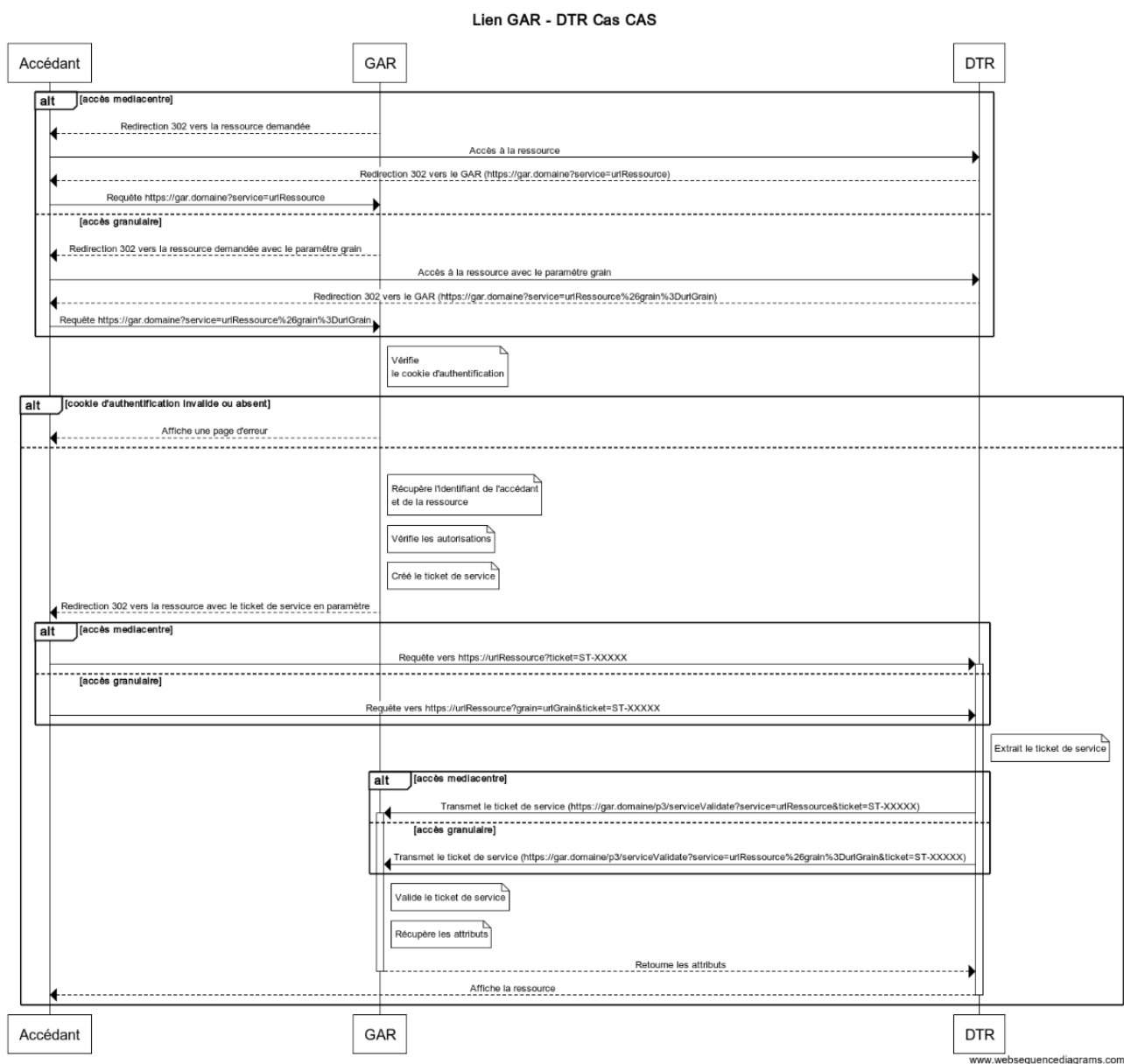
4.5 Flux lien GAR-DTR

4.5.1 Protocole SAML



10 Flux GAR - DTR (SAML)

4.5.2 Protocole CAS



11 Flux GAR - DTR (CAS)

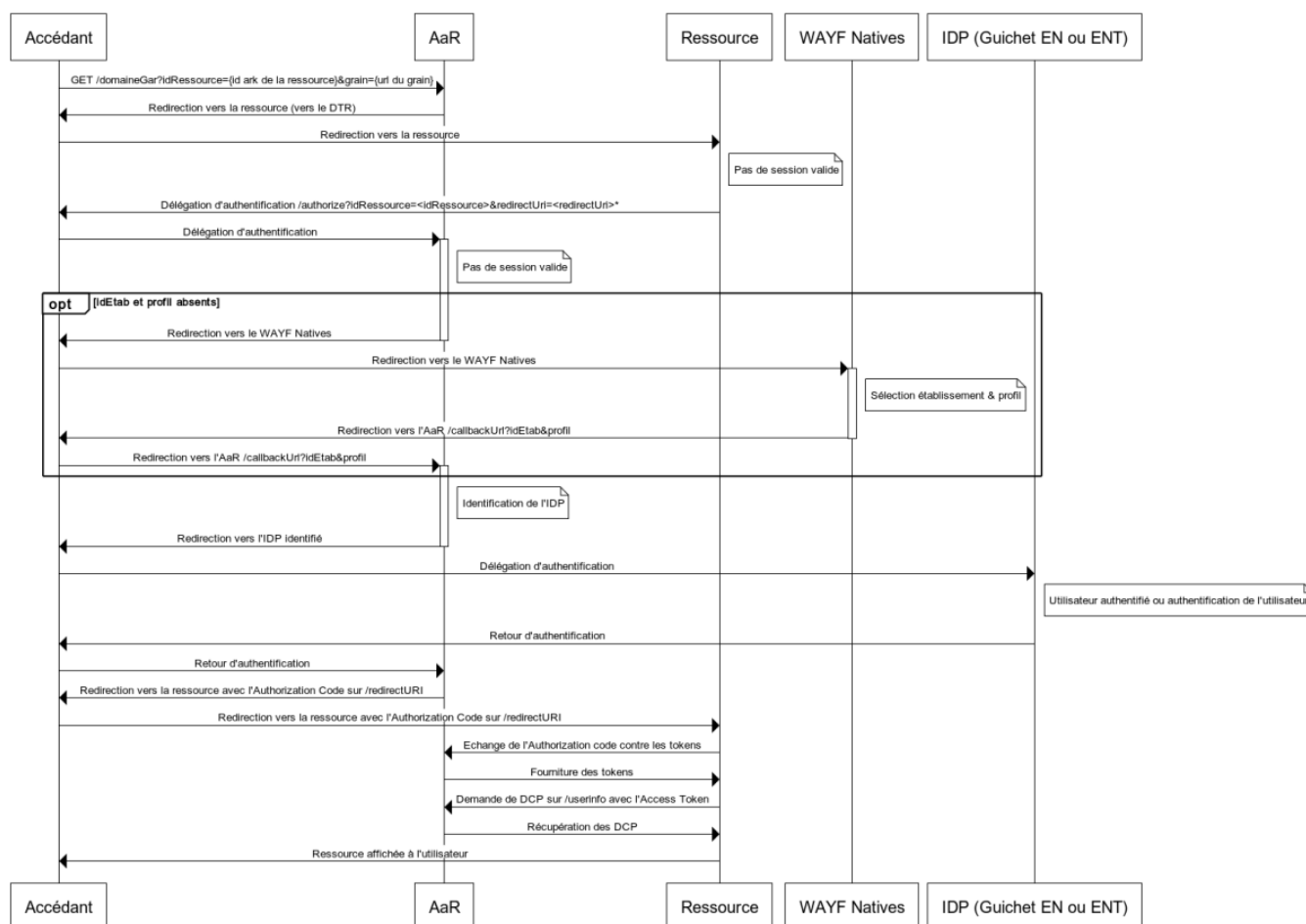
4.5.3 Protocole OpenId Connect

4.5.3.1 Ressource web

Consultation de ressource depuis un Médiacentre

Les échanges se déroulent ainsi, dans le cas d'une demande d'accès depuis un Médiacentre (EduGAR ou ENT) :

Accès ressource - Variante WEB en OIDC sans informations dans l'URL domaineGar



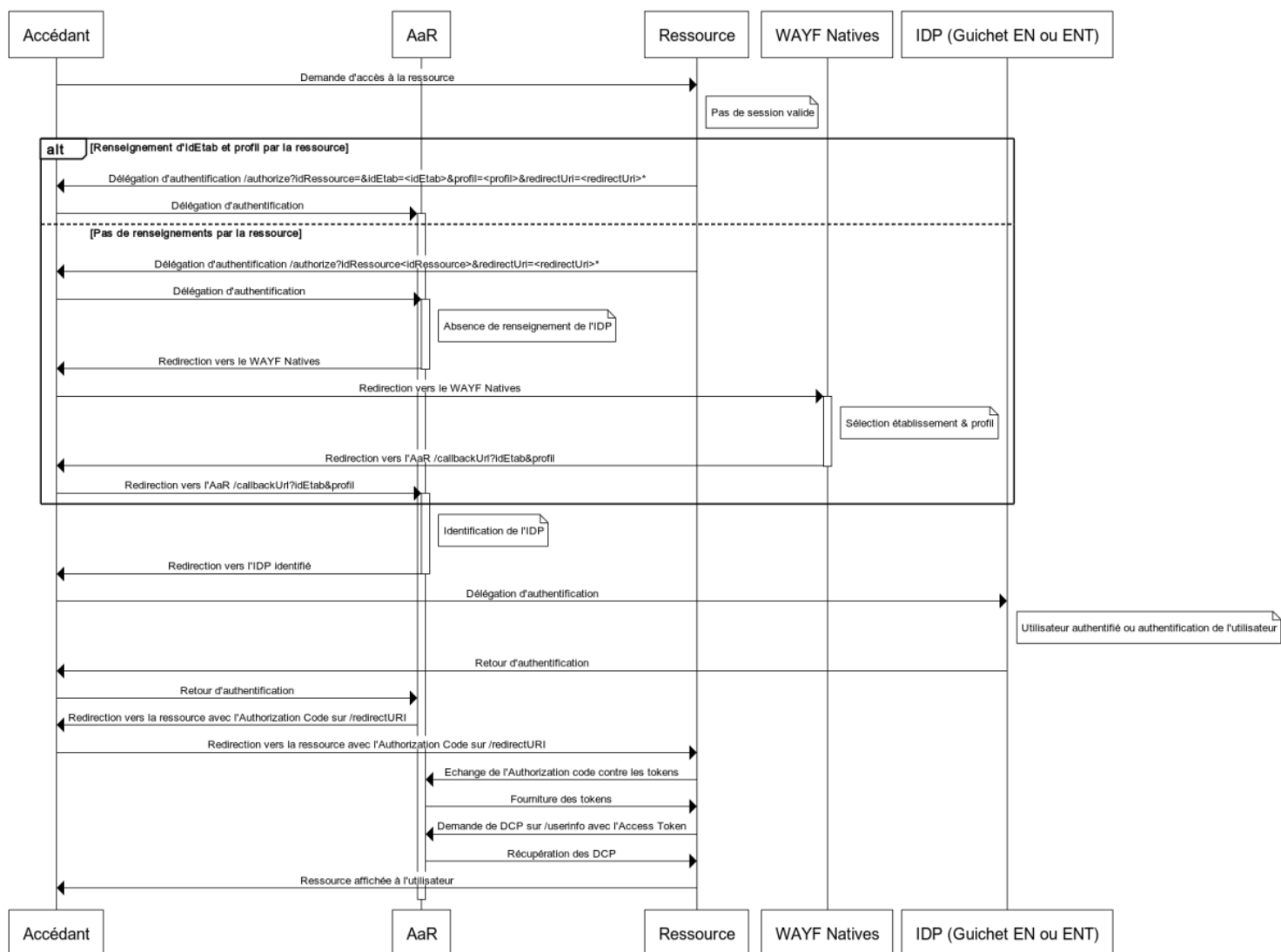
*Par soucis de lisibilité, les autres paramètres protocolaires ne sont pas indiqués

Figure 12 – Accès Ressource – Variante web en OIDC

Dans le cas où l'URL domaine GAR ne renseigne pas les informations idEtab & idpHint / Profil (si elle est forgée par le FR par exemple), l'utilisateur est redirigé vers le WAYF Natives.

Accès direct au endpoint /authorize

La plateforme DTR peut contacter le endpoint /authorize avec les informations idEtab & idpHint / Profil afin de s'affranchir de la première partie des échanges, selon le schéma suivant :

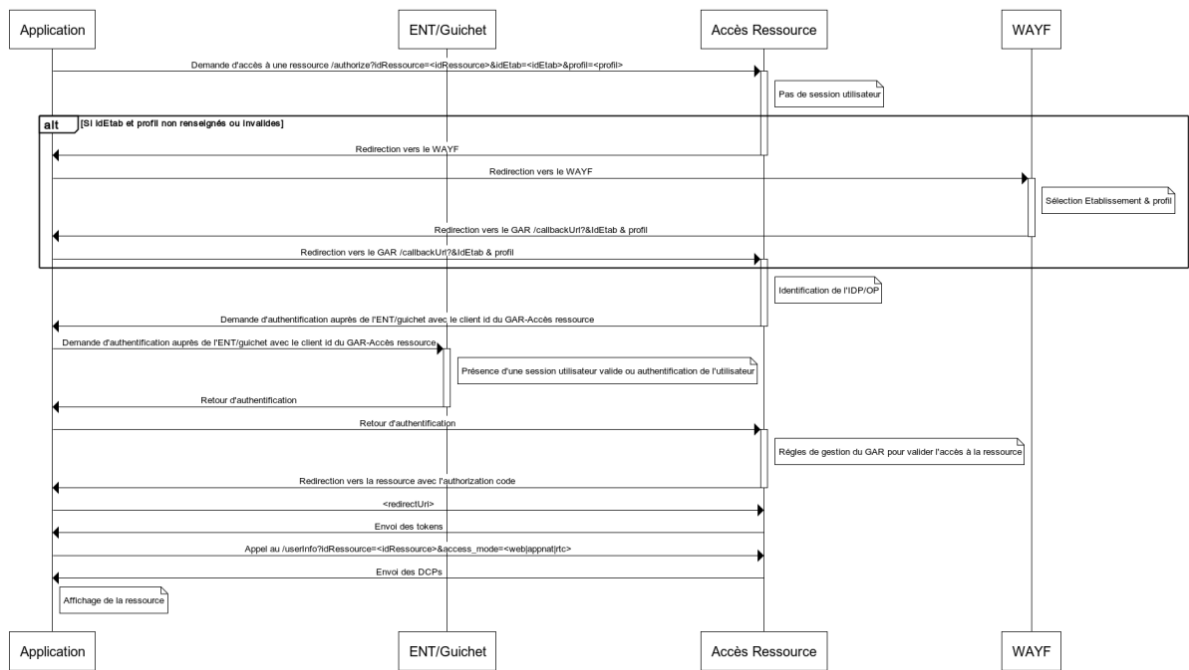


*Par soucis de lisibilité, les autres paramètres protocolaires ne sont pas indiqués

Figure 13 - Accès ressource - Variante WEB en OIDC accès direct sur /authorize depuis la ressource

4.5.3.2 Ressource native

Lien GAR - DTR Cas OpenId Connect



www.websequencediagrams.com

Figure 14 - Flux GAR-DTR (OIDC)

5 Solution technique

5.1 Lien fournisseur d'identité- GAR

Les assertions SAML2 échangées entre l'ENT et le GAR sont signées, chiffrées, et encodées en base64.

Les assertions SAML2 et les trames OpenId Connect sont échangées en https.

5.1.1 Attributs attendus de la part des fournisseurs d'identité

Le fournisseur de service du GAR s'attend, une fois l'authentification validée à recevoir les informations suivantes concernant l'accédant authentifié :

Dans le cas des ENT SAML2 et OpenId Connect :

- L'identifiant de l'ENT de l'accédant (idEnt)
- L'identifiant de l'établissement de l'accédant (UAI)
- L'identifiant de l'accédant au niveau de son ENT (GARPersonIdentifiant)

Dans le cas des guichets OpenId Connect :

- L'identifiant de l'accédant (GARPersonIdentifiant)

5.1.2 Gestion du cookie d'authentification

Lors de la récupération de l'identifiant de l'accédant le GAR génère un cookie d'authentification et stocke l'identifiant dans une base de donnée Redis en utilisant le cookie comme clé. La durée de vie du cookie et le temps de présence de la donnée dans la base Redis sont positionnés à 30 minutes (configurable). Cette durée de vie est prolongée à chaque utilisation du cookie (accès au fournisseur de ressource ou au fournisseur d'identité du GAR) dans la limite de 6h (configurable).

Le nom du cookie est :

GAR_USER

Ce cookie est positionné sur un domaine partagé entre les parties fournisseur d'identité et fournisseur de service du GAR avec les drapeaux http-only et secure.

5.2 Lien GAR – DTR

Les assertions SAML2 échangées entre le DTR et le GAR sont signées, chiffrées, et encodées en base64. Les assertions SAML2 sont échangées en https.

Les échanges via les protocoles CAS et OpenId Connect se font en https.

5.2.1 Validation de l'authentification

Le serveur web de la partie fournisseur d'identité du GAR (nginx) va, à partir du cookie d'authentification, récupérer dans la base Redis l'identifiant de l'accédant. Cet identifiant est positionné dans un en-tête HTTP puis transmis au serveur d'application, celui-ci récupère l'identifiant de l'accédant dans l'en-tête HTTP.

Avant de positionner l'identifiant de l'utilisateur dans le header, le serveur supprime tous les en-têtes de la requête d'accès ayant le même nom que celui positionné.

Le header utilisé a pour nom :

X-GAR-AUTH-USERID

5.2.2 ds:X509Certificate Délivrance des attributs

Le code des attributs fournis dans le flux de la réponse est décrit dans DR6 §6 « Annexe : GAR – Liste des attributs valides » pour les attributs proposés lors de la création d'une ressource. La liste des attributs supplémentaires disponible via l'interface d'administration du GAR est décrite dans DR2.

Si la ressource accédée est une ressource liée, et que l'accédant possède une affectation valide pour la ressource mère de famille, alors les attributs de famille validés sont également transmis :

- L'IDC (cad l'idOpaque de la mère de famille)
- Le LRA (cad la liste ressources appelées par la ressource qui sont affectées à l'accédant)

5.2.2.1 Cas du protocole SAML

Les attributs de l'accédant sont fournis dans la réponse SAML générée suite à la demande d'authentification de la ressource accédée.

Exemple de retour pour la fourniture d'attribut:

```
<?xml version="1.0" encoding="UTF-8"?> <saml2p:Response
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://DNS-ressource/saml/SSO" ID="_1481603196411469058"
InResponseTo="a18a697eagea5gdc1f7f3j9ed9h126e" IssueInstant="2019-10-
04T13:16:37.224Z" Version="2.0"> <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://idp-
auth.gar.education.fr/cas/idp</saml2:Issuer> <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" /> <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_1481603196411469058"> <ds:Transforms> <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms> <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlesc#sha256" />
<ds:DigestValue>J0JU7iEMD1nvMkdwiattOuxH2BfkCX6JspH5QBYlFaE=</ds:DigestVal
ue> </ds:Reference> </ds:SignedInfo>
<ds:SignatureValue>f5zjVQI+koTJevaK0avxIpLiD2P2ioLgbeylfNBvV29ndcSDBfo/qEf
FnH5rFfpm/WD6nMNM92bv
HQeqMbmKKJaGPaKEgaBPBJAorpAztUxhONhA4LvX+/BgNJwTFsteTJhrHVG7nYzpVWe3BXuGQy
tY
XyXj7A0Nh+BS0dFvP3fRpr7fYkahmYoGZjc+tdOmdUgMEhFwBeTAyeZM7Fs5texH1/2d5fiW2T
pE
hndzHA5RPBAvmBOJHi/F9il80c+NQuZj/fzjM3Vb8nvdszgPV9QVbwZhEs9PeNu6df6zuptNJ
6t cccyydyiJhsr5aiRe2zw4aRSI/ciULEdbe478vA==</ds:SignatureValue>
<ds:KeyInfo> <ds:X509Data>
<ds:X509Certificate>MIIDZDCCAkygAwIBAgIUfM0fpOxrfhkkOINpdCF2Q9KgEQwDQYJKo
ZIhvcNAQELBQAwLDEqMCgG
A1UEAwWhaWRwLWF1dGgucHAudGVzdClnYXJlZWR1Y2F0aW9uLmZyMB4XDTE4MDQxNzEzNDYzOF
oX
DTM4MDQxNzEzNDYzOFowLDEqMCgGA1UEAwWhaWRwLWF1dGgucHAudGVzdClnYXJlZWR1Y2F0aW
9u
LmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYsxyKe5fziJ6sp5aPNsg7THbMA
d8
scPs2vYwR2JGmnSnAQhOxy0RYkAKRsax19uqWP9YH5LpN15ySn17E0xbUnhHRRDs37aPQ2Tx6f
XN
xUx5TBxl1GY8wQwZbpaEJXh0wTfLVPSrijP7Yv/Ka/ymeE6bSEUDlKzidWYlhevTmzmJoWcoIL
```

```

pU
tvmOcvVn6CBiB+UOJPSx0EDqfzWoHS+Ai8A06yt+4ABSk/36BQzlddRds+Sn4o9iH/ycIQ12EI
CT
dqj24K2X4AsIgMI9GPN5iQ1Cs2MpkJ0b9YgnjZiL2CX9ZXaGuBmIsm59UKsXjSBY+Pt4AKoEn
C5
gv0osvv9bQIDAQABo34wfDAdBgNVHQ4EFgQUOy5jFMCda28qHrIMzCM+uqNVZDUwWwYDVR0RBF
Qw
UoIhaWRwLWFldGgucHAudGVzdClnYXJ0eWZWRlY2F0aW9uLmZyhilpZHAatYXV0aC5wcC50ZXN0LW
dh
ci5lZHVjYXRpb24uZnJpZHAvbWV0YWRhdGEwDQYJKoZIhvcNAQELBQADggEBAH5iMl5nOo0ueX
MI
8bQbZPPDOG6n/VFaJgzYaVgtRCPCvKmt+sPb2JY7YoD/ekAfAtlZI23rE/OjckLYGFKr+3wIOL
dH
FUxz0rJ1OBEupvHpxJKMzmMQDlFcEQ+qz2mJ0s2hZddNiHaqsJFogvt2aQiZBq9UDS1KEFvOZy
eh
FnUs1mVXjY9/O920PmiUpNO2S+OX9k14QTPqUK6SAOVlEgSRnoBow8Y069sMqkdK4MENYNpKbO
ob
CbM+EiO+KMaAuMVh25s+zmyfR4PxOhJWgQ8liFjolktDKVBIzDQI7raTulXWJyWLR8CXiDiZs/
ZV FACcliBkDHLhly6cwPS8tNA=</ds:X509Certificate> </ds:X509Data>
</ds:KeyInfo> </ds:Signature> <saml2p:Status> <saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" /> </saml2p:Status>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_8167337250771928520" IssueInstant="2019-10-04T13:16:37.211Z"
Version="2.0"> <saml2:Issuer>https://idp-
auth.gar.education.fr/cas/idp</saml2:Issuer> <saml2:Subject> <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
NameQualifier="https://idp-auth.gar.education.fr/cas/idp"
SPNameQualifier="entityID de la
ressource">yC9f5islCs0GsIZEt5st08eisSQ=</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData
InResponseTo="a18a697eagea5gdc1f7f3j9ed9h126e" NotOnOrAfter="2019-10-
04T13:21:37.177Z" Recipient="https://DNS-ressource/saml/SSO" />
</saml2:SubjectConfirmation> </saml2:Subject> <saml2:Conditions
NotBefore="2019-10-04T13:16:37.223Z" NotOnOrAfter="2019-10-
04T13:21:37.223Z"> <saml2:AudienceRestriction>
<saml2:Audience>https://DNS-ressource</saml2:Audience>
</saml2:AudienceRestriction> </saml2:Conditions> <saml2:AuthnStatement
AuthnInstant="2019-10-04T13:16:37.177Z" SessionIndex="ST-1-
8LylUZPGakcXwF56aZdl8M06Qs0idp-auth.gar.education.fr">
<saml2:SubjectLocality Address="195.221.81.69" /> <saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passwor
dProtectedTransport</saml2:AuthnContextClassRef> </saml2:AuthnContext>
</saml2:AuthnStatement> <saml2:AttributeStatement> <saml2:Attribute
FriendlyName="DIV" Name="DIV"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>20529~5_d##5 D</saml2:AttributeValue>
</saml2:Attribute> <saml2:Attribute FriendlyName="CIV" Name="CIV"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>M.</saml2:AttributeValue> </saml2:Attribute>
<saml2:Attribute FriendlyName="PRE" Name="PRE"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>Carl</saml2:AttributeValue> </saml2:Attribute>
<saml2:Attribute FriendlyName="IDO" Name="IDO"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>88c1dc611ef894654184ferfg5464f044f6b3cba43a2f943c199
0db4bbbe320f648f942d66e0a7954b8887a94e8f05c486ffb06a9e27074aee9f17b19a1f7f
</saml2:AttributeValue> </saml2:Attribute> <saml2:Attribute

```

```

FriendlyName="UAI" Name="UAI"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>0681654D-XXL1</saml2:AttributeValue>
</saml2:Attribute> <saml2:Attribute FriendlyName="PRO" Name="PRO"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>National_elv</saml2:AttributeValue>
</saml2:Attribute> <saml2:Attribute FriendlyName="NOM" Name="NOM"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>XXL1Eleve</saml2:AttributeValue> </saml2:Attribute>
</saml2:AttributeStatement> </saml2:Assertion> </saml2p:Response>
  
```

5.2.2.2 Cas du protocole CAS

Les attributs de l'accédant sont fournis lors de la validation du ticket de service. Le format de retour de ces attributs diffère suivant l'url appelée pour valider le ticket de service :

- /p3/serviceValidate : Retourne les attributs sous forme de xml ou de json en fonction du paramètre format passé dans la requête.
- /samlValidate : retourne un flux SAML

Exemple de retour pour la fourniture d'attribut:

```

<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
  <cas:authenticationSuccess>

    <cas:user>AAadzZWNyZXQxq6wV28f1fnopefWs/YDdRfzkKC252feaIfiz2aNa10jOrT8GLC0c
    IyfuM6gOxiplDCqt1kLNM/93rsX7LtH6HNKwedaYRJ6K6Fa7UGZwAZDSuATMF9qaPArjf9YmQ
    Z56H3EsMoZRWESyCLQkdLufQE3</cas:user>

    <cas:attributes>
      <cas:PRE>nicolas</cas:PRE>
      <cas:P_MAT>104100##EDUC. PHYSIQUE ET SPORTIVE DE
      COMPLEMENT</cas:P_MAT>
      <cas:P_MAT>100100##EDUCATION PHYSIQUE ET SPORTIVE</cas:P_MAT>
      <cas:idENT>WjA=</cas:idENT>
      <cas:PRO>National ens</cas:PRO>
      <cas:P_MS4>2211</cas:P_MS4>
      <cas:P_MS4>2212</cas:P_MS4>
      <cas:P_MS3>221</cas:P_MS3>
      <cas:NOM>ADAM</cas:NOM>
      <cas:P_MS2>22</cas:P_MS2>
      <cas:P_MS1>2</cas:P_MS1>
      <cas:DIV>1 STMG2##1 STMG2</cas:DIV>
      <cas:DIV>1 D##1 D</cas:DIV>
      <cas:DIV>2NDE 6##2NDE 6</cas:DIV>
      <cas:DIV>1 E##1 E</cas:DIV>
      <cas:DIV>1 a##1 A</cas:DIV>
      <cas:DIV>1 B##1 B</cas:DIV>
      <cas:DIV>2NDE 2##2NDE 2</cas:DIV>
      <cas:P_MS7>2211141</cas:P_MS7>
      <cas:P_MS7>2212121</cas:P_MS7>
      <cas:P_MS7>2212223</cas:P_MS7>
      <cas:P_MS7>2212131</cas:P_MS7>
      <cas:P_MS7>2212111</cas:P_MS7>
      <cas:P_MS6>221114</cas:P_MS6>
      <cas:P_MS6>221212</cas:P_MS6>
      <cas:P_MS6>221222</cas:P_MS6>
      <cas:P_MS6>221213</cas:P_MS6>
      <cas:P_MS6>221211</cas:P_MS6>
      <cas:P_MS5>22111</cas:P_MS5>
      <cas:P_MS5>22121</cas:P_MS5>
    </cas:attributes>
  </cas:authenticationSuccess>
</cas:serviceResponse>
  
```

```
<cas:P_MS5>22122</cas:P_MS5>

<cas:IDO>7845f4515fev1515ve5448006fdf9227f1896f518d3b5azq984aee5db578cf087
7ce2e5c781f74f03e30abfbf55568c26384f11700708607372c955ac21b0af499</cas:IDO
>

    <cas:P_MEL>noreply_@mail.fr</cas:P_MEL>
    <cas:UAI>1234569A</cas:UAI>
  </cas:attributes>
</cas:authenticationSuccess>
</cas:serviceResponse>
```

5.2.2.3 Cas du protocole OpenId Connect et usages particuliers de l'Access Token

Les attributs de l'accédant sont retournés au format json en échange de l'Access Token, de l'identifiant ark de la ressource et de l'access_mode (« web », « appnat », « rtc » ou « wsraa »).

```
{
  "PRE": "Nicolas",
  "NOM": "ADAM",
  "P_MAT": "104100##EDUC. PHYSIQUE ET SPORTIVE DE COMPLEMENT",
  "DIV": ["1 STMG2##1 STMG2 ", "1 D##1 D", "2NDE 6##2NDE 6"]
  "PRO": "National_ens",
  "P_MEL": "noreply_@mail.fr",
  "UAI": "1234569A",
  "sub": "248289761001",
  "service": "app.test://openid/oauthredirect/test",
  "auth_time": 1670849702,
  "id": "248289761001",
  "client_id": "a7b4fcd5-463e-474d-bb22-9df3970f41ff"
}
```


6 Déconnexion

6.1 Contexte général

Dans les établissements ou à leur domicile, les utilisateurs accèdent à leur ressource via le GAR avec des postes non sécurisés (i.e. : qui ne gèrent pas de session utilisateur). Le risque est donc important pour un utilisateur de laisser ses sessions applicatives ouvertes sur le poste. Les sessions de l'utilisateur sont alors disponibles pour les utilisateurs suivants. Dans ce contexte, il est donc nécessaire que la fédération d'identité du GAR permette la gestion d'un logout global (single logout).

La demande de déconnexion peut être initiée par l'utilisateur, par le serveur ENT ou par d'autres applications le permettant (cf. 6.5.3) à la demande de l'utilisateur dans différents use case (changement d'établissement, fin de la session sur l'ENT, déconnexion volontaire de l'ENT ou d'un service, fermeture d'une application native).

Le GAR propage alors la déconnexion vers les ressources web ou vers le fournisseur d'identité utilisé par l'utilisateur pour son authentification, en fonction de l'initiateur de la déconnexion. Le fonctionnement pour chaque cas est décrit au paragraphe suivant.

Le GAR propage également la déconnexion vers les ressources web en fin de session sur le GAR, suite à un délai d'inactivité de l'accédant ou à l'issue d'une durée maximale de session (cf. Gestion du cookie d'authentification).

6.2 Fonctionnement

Lorsque le GAR reçoit une demande de déconnexion provenant d'un ENT ou d'une application (dans le cas d'une authentification par guichet, cf §6.5.3), le GAR propage la demande de déconnexion de manière asynchrone en serveur-serveur vers chaque ressource web à laquelle l'accédant s'est connecté. Pour cela, la liste des ressources accédées par l'utilisateur est enrichie à chaque accès à une ressource, cette liste est conservée dans la session applicative GAR. Ce mécanisme est natif dans Apereo.

Le GAR propose une réception de la déconnexion :

- depuis l'ENT via le navigateur de l'utilisateur ou en serveur-serveur ;
- depuis l'application via le navigateur de l'utilisateur.

Pour les DTR CAS, si l'url de logout n'est pas disponible, alors la déconnexion n'est pas propagée à ce DTR (l'utilisateur reste donc connecté aux ressources de ce DTR)

Si un appel de logout à une ressource est en erreur, le GAR ne tient pas compte de ce retour et ne réalise pas de rejeu, la déconnexion aux autres ressources est réalisée.

Lorsque le GAR reçoit une demande de déconnexion depuis une application native, le GAR propage la demande de déconnexion vers le fournisseur d'identité utilisé par l'utilisateur lors de son authentification. Le GAR propose une réception et une propagation de la déconnexion via le navigateur utilisé par l'application native.

Si un appel de logout à un fournisseur d'identité est en erreur, le GAR ne tient pas compte de ce retour et ne réalise pas de rejeu.

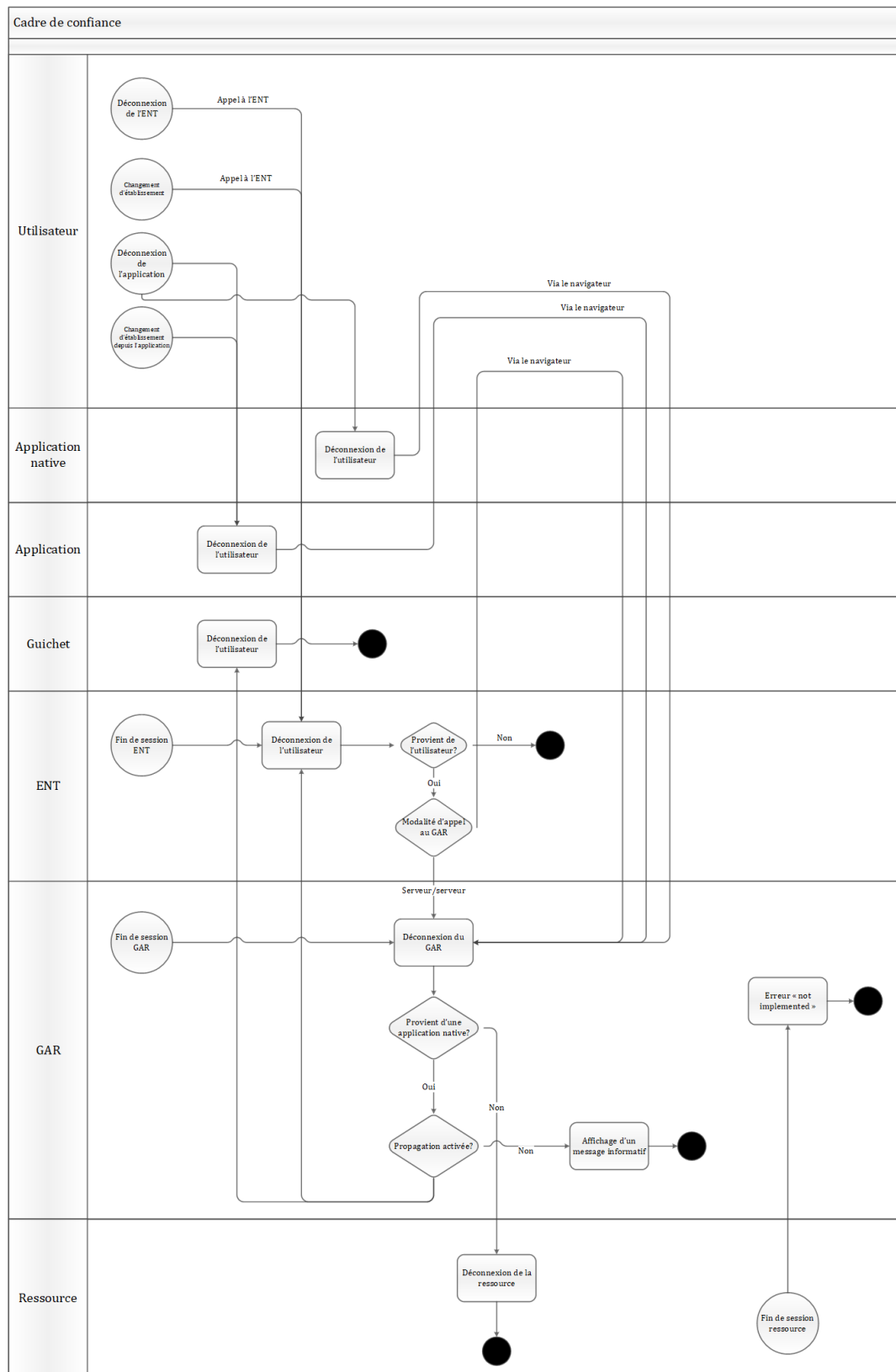
Dans les 2 cas, le GAR invalide ensuite le cookie d'authentification et l'Access Token puis supprime les informations stockées dans la base de données mémoire.

Dans le cas d'un abonnement avec une catégorie d'affectation « flottante », le GAR libère le jeton d'accès à la ressource réservé par l'accédant.

Les ENT, les guichets et les ressources sont chargés, chacun en ce qui les concerne, de la gestion de leur session utilisateur, suite à la réception d'une requête de déconnexion. La bonne prise en compte des différents use case implique une prise en compte rapide de l'ordre de déconnexion reçu.

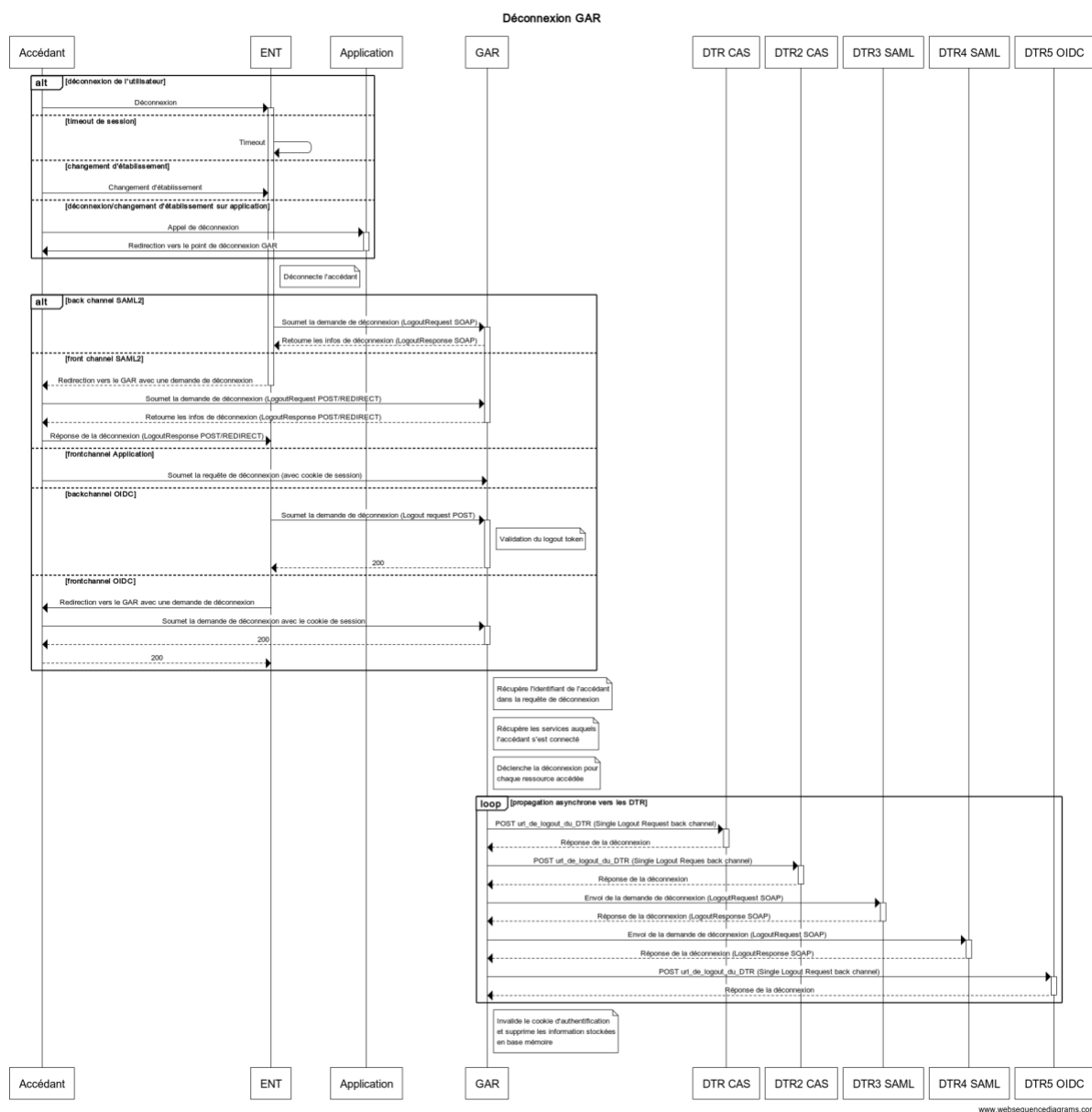
Les ENT, les guichets et les fournisseurs de ressources sont chargés d'informer l'utilisateur des mécanismes liés au SSO et donc au logout.

6.3 Diagramme fonctionnel



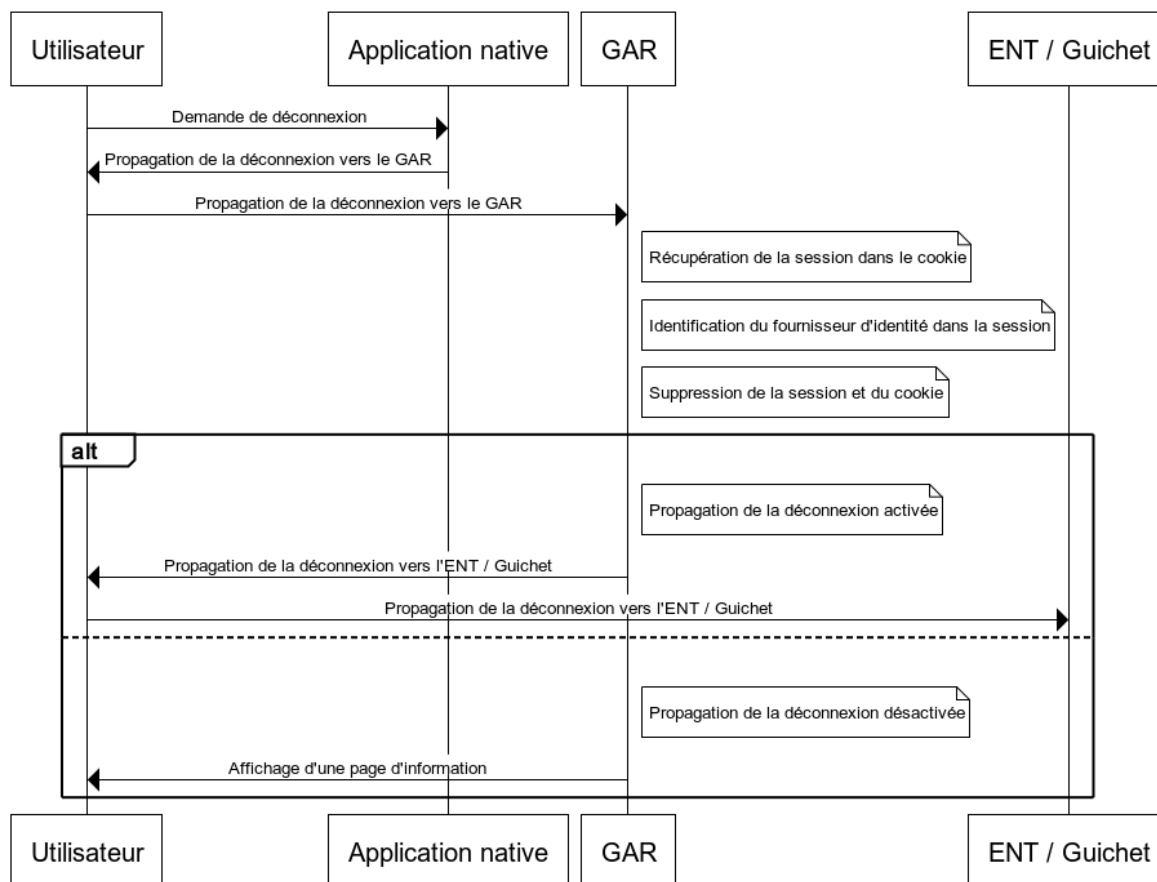
6.4 Flux de déconnexion

6.4.1 Accès web



6.4.2 Accès par application native

Déconnexion depuis une application native



6.5 Propagation de la déconnexion vers le GAR

6.5.1 Propagation de la déconnexion depuis l'ENT (SAML)

L'url de déconnexion du GAR est disponible via les métadonnées (SingleLogoutService Binding). Les requêtes de déconnexion doivent être soumises au GAR en serveur/serveur (SOAP) ou via le navigateur de l'utilisateur (POST/redirect). Le logout Request envoyé au GAR doit contenir le nameId fourni lors de la connexion. Les informations concernant le Single Logout du protocole sont disponibles en ligne ([cf. AD2](#))

6.5.2 Propagation de la déconnexion depuis l'ENT (OIDC)

La propagation de la déconnexion depuis un ENT en OIDC peut se faire :

- En backchannel : le logout token doit contenir le sid (Session ID) pour que le GAR puisse identifier la session à expirer ;
- En frontchannel : le cookie de session est utilisé pour identifier la session à expirer.

6.5.3 Propagation de la déconnexion depuis les applications du GAR

Dans le cas d'une authentification depuis les guichets, ceux-ci ne propagent pas l'information de déconnexion auprès du GAR. Ce sont donc les applications qui prennent cette charge. Les applications identifiées actuellement pour lancer cette déconnexion sont le Mediacentre GAR, l'IHM d'affectation, voire des Mediacentre tiers.

La déconnexion de l'utilisateur depuis les applications est propagée jusqu'au GAR à travers le navigateur de l'accédant vers l'url de déconnexion proposée par le GAR.

Le GAR utilise le cookie de session de l'utilisateur disponible dans la requête de déconnexion pour identifier l'utilisateur.

6.5.4 Propagation de la déconnexion depuis une ressource web

Dans les métadonnées du GAR (SAML ou OIDC), les appels single logout sont disponibles pour les ressources.

Si ces appels sont utilisés par une ressource SAML, le serveur proxy du GAR renverra à l'appelant une erreur http 501 Not Implemented.

Dans le cas où la connexion provient initialement d'une ressource web OIDC, les demandes de logout reçues depuis la ressource web déclencheront une erreur http 501 Not Implemented.

6.5.5 Propagation de la déconnexion depuis les applications natives

Dans le cas d'un accès à une ressource par application native, les requêtes de déconnexion provenant des applications natives doivent être soumises au GAR via le navigateur qu'elles utilisent (frontchannel). La requête doit contenir le cookie de session GAR.

Pour différencier les demandes de déconnexion provenant des fournisseurs d'identité ou applications des demandes de déconnexion provenant des applications natives, un endpoint de logout spécifique est exposé.

Ce endpoint est défini dans le well-known de l'OpenId Provider exposé par le GAR.

6.6 Propagation de la déconnexion vers les ressources

6.6.1 Propagation de la déconnexion vers les ressources dans le cas du protocole SAML

L'url de déconnexion des ressources doit être disponible via les métadonnées (SingleLogoutService Binding).

Les requêtes de déconnexion seront soumises par le GAR en serveur/serveur (SOAP).

La logout request est envoyée pour chaque ressource ou SP global utilisant SAML à laquelle l'utilisateur s'est connecté. Le namelid utilisé lors de la connexion est fourni lors de la déconnexion.

Les informations concernant le Single Logout du protocole sont disponibles en ligne ([cf. AD2](#))

6.6.2 Propagation de la déconnexion vers les ressources dans le cas du protocole CAS

L'url (endpoint /logout) est fournie par le DTR dans les données d'initialisation (cf.[DR14](#)).
Les requêtes de déconnexion seront soumises par le GAR en serveur/serveur (back channel).

Lors de l'appel à l'endpoint logout en back channel, le service ticket est fourni
Les informations concernant le Single Logout du protocole sont disponibles en ligne ([cf. AD3](#))

6.6.3 Propagation de la déconnexion vers les ressources dans le cas du protocole OIDC

L'url (endpoint /logout) est fournie par le DTR dans les données d'initialisation (cf.[DR14](#)).
Les requêtes de déconnexion seront soumises par le GAR en serveur/serveur (back channel).

Lors de l'appel à l'endpoint logout en back channel, le logout token est fourni et doit contenir le sid (Session ID) pour identifier la session à expirer.

6.7 Propagation de la déconnexion vers les fournisseurs d'identité

Pour les accès par application native, les demandes de déconnexion sont initiées par les applications natives comme décrit au chapitre [6.5.5](#) et peuvent être propagées aux fournisseurs d'identité.

Un paramètre par fournisseur d'identité est positionné dans la configuration du service pour indiquer si la demande de déconnexion doit lui être propagée.

Si le paramètre est désactivé, le GAR affiche une page d'information indiquant à l'utilisateur que la déconnexion n'a pas été propagée à son ENT/Guichet et l'invitant à se déconnecter auprès de ce dernier. Le message est configurable et défini dans le fichier de wording du service (cf **Erreur ! Source du renvoi introuvable.**).

Si le paramètre est activé, le GAR propage la déconnexion au fournisseur d'identité selon le protocole, décrit ci-dessous.

6.7.1 Propagation de la déconnexion vers les ENT SAML

L'url de déconnexion doit être disponible dans les métadonnées de l'ENT sur le binding HTTP-Redirect. La logout request est envoyée sur ce endpoint en frontchannel. Elle contient le namelid utilisé lors de la connexion pour identifier la session de l'utilisateur.

6.7.2 Propagation de la déconnexion vers les guichets et les ENT OIDC

Le fournisseur d'identité doit supporter la déconnexion en frontchannel et indiquer l'url de déconnexion dans ses métadonnées (well-known).

La requête de déconnexion est envoyée sur ce endpoint en frontchannel. Elle contient le sid (session ID) utilisé lors de la connexion en paramètre d'url pour identifier la session de l'utilisateur.