



**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 04.15** : Spécifications des SSO des interfaces GAR

**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 - SSO des IHM GAR

## DSFD

Le 08/08/2024

	Version	En date du
<b>Référence :</b> RENATER-GAR-E/DSFD.0025 SSO des IHM GAR	09.00	08/08/2024

Version	Rédigé par	Objet	Vérifié		Validé	
			Par	Le	Par	Le
09.00	WORLDLINE	Version 8.0	Worldline	08/08/2024	RENATER  Re_GAR Spécification	07/08/2024

## Évolutions successives

Version	Date	Description	Auteur(s)
1.0	31/08/2018	Création pour l'évolution 25 Ajout de profils au niveau du portail GAR	WORLDLINE
1.1	12/09/2018	évolution 25 Ajout de profils au niveau du portail GAR	WORLDLINE
01.02	16/07/2021	Évolution 146 : Pilote 1D	WORLDLINE
01.03	29/07/2021	Évolution 146 : Pilote 1D, prise en compte des remarques Renater	WORLDLINE
01/04	09/08/2021	Évolution 146 : Pilote 1D, prise en compte des remarques Renater du 04/08/2021	WORLDLINE
02.00	01/12/2021	Validation de la spécification dans le cadre de la release 6.0	WORLDLINE
02.01	15/12/2021	Evolution 348 (WL 155) Pilote 1D étendu au 2D Evolution 341 (WL : 140) – Message d'erreur utilisateur enrichi	WORLDLINE
02.02	05/01/2022	Evolution 348 (WL 155) Pilote 1D étendu au 2D	WORLDLINE
02.03	06/01/2022	Evolution 348 (WL 155) Pilote 1D étendu au 2D : prise en compte des remarques RENATER	WORLDLINE
02.04	10/01/2022	Evolution 348 (WL 155) - Pilote 1D étendu au 2D : prise en compte des remarques RENATER	WORLDLINE
02.05	18/01/2022	Evolution 348 (WL 155) - Pilote 1D étendu au 2D : prise en compte des retours du MEN	WORLDLINE
02.06	20/01/2022	Evolution 341 (WL : 140) – Message d'erreur utilisateur enrichi : prise en compte des retours RENATER	WORLDLINE
03.00	21/01/2022	Version validée pour le lot 1 de la release 6.1	WORLDLINE
03.01	23/03/2022	Correction documentaire Evolution 348 (Pilote 1D étendu au 2D)	WORLDLINE
03.02	28/03/2022	Correction Documents de référence	WORLDLINE
04.00	13/04/2022	Version validée pour la release 6.1	WORLDLINE

04.01 04.02 04.03	03/06/2022 23/06/2022 01/07/2022	Evolution 364 (WL 162) : OIDC pour les ENT Evolution 320/321 (WL 166) : Amélioration de l'accessibilité pour les IHM Affectation et Portail	WORLDLINE
05.00	06/07/2022	Version validée par RENATER	WORLDLINE
05.01	15/11/2022	[GAR 6.2] Modification de la page de déclaration d'accessibilité	WORLDLINE
06.00		Version validée	WORLDLINE
06.01	09/12/2022	- Evolution 284 (WL 157) : Mise en cache des métadonnées ENT - Evolution 376 (WL 184) : Gestion des Métadonnées ENT et Guichets OIDC	WORLDLINE
07.00	09/01/2023	Version validée par RENATER pour la release 7.1	WORLDLINE
07.01	06/11/2023	Evolution 438 - Portail GAR - Gestion du mot de passe	WORLDLINE
07.02	28/11/2023	Evolution 438 - Prise en compte des retours	WORLDLINE
07.03	07/12/2023	Evolution 438 - Déport des notifications dans un paragraphe dédié	WORLDLINE
08.00	15/01/2024	Evolution 438 : prise en compte des retours mineurs, complément (ajout d'un lien) & validation	WORLDLINE
08.01	01/08/2024	Version 8.0 : Précision de la gestion des accès	WORLDLINE
08.02	01/08/2024	Suppression des commentaires de la version précédente	WORLDLINE
09.00	08/08/2024	Version validée	WORLDLINE

## Table des matières

1	Introduction .....	6
1.1	Objet du document .....	6
1.2	Responsabilités liées au document .....	6
1.3	Documents de référence .....	6
1.4	Abréviations .....	6
1.5	Glossaire .....	6
1.6	Présentation générale .....	7
2	Gestion de l'authentification .....	9
2.1	Principe .....	9
2.2	Respect de l'accessibilité .....	10
2.3	Authentification via l'ENT .....	11
2.3.1	Gestion des métadonnées des ENT .....	11
2.3.2	Authentification via l'ENT en SAML2.0 .....	11
2.3.3	Authentification via l'ENT en OIDC .....	12
2.4	Authentification locale .....	13
2.4.1	Principe .....	13
2.4.2	Gestion du mot de passe .....	14
2.5	Authentification via les guichets .....	17
2.5.1	Protocole d'accès .....	17
2.5.2	Gestion des métadonnées des guichets .....	17
2.5.3	Accès aux guichets .....	17
2.6	Gestion des rôles de Responsable d'Affectation pour le 2D RDMEN .....	19
2.7	Durée de session .....	20
2.8	Gestion des droits d'accès .....	20
2.9	Affichage d'une page d'erreur .....	20
2.9.1	Description de la page .....	20
2.9.2	Exemple .....	20

3	Gestion de la déconnexion .....	22
3.1	Principe .....	22
3.2	Diagramme de séquence de propagation de la déconnexion depuis l'ENT .....	22
3.3	Propagation de la déconnexion de l'ENT .....	23
3.4	Cas de l'authentification déléguée à un guichet .....	23
4	Utilisation du SSO GAR par les IHM .....	24
5	Notifications .....	25
5.1	Création de mot de passe Portail GAR .....	25
5.2	Réinitialisation de mot de passe Portail GAR .....	25

## Table des illustrations

Figure 1: Schéma de principe du SSO des IHM GAR .....	8
Figure 2: Page de login .....	10
Figure 3: Diagramme de séquence de l'authentification par ENT .....	12
Figure 4 : Diagramme de flux de la modification de mot de passe .....	16
Figure 5: Diagramme global de séquence de l'authentification avec un guichet .....	18
Figure 6: Diagramme de séquence propagation de la déconnexion ENT .....	22
Figure 7: Diagramme de séquence propagation de la déconnexion – cas des guichets .....	23

# 1 Introduction

## 1.1 Objet du document

Le but de ce document est de décrire l'ensemble des fonctionnalités du SSO des IHM 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 est responsable de sa validation.

## 1.3 Documents de référence

Numéro	Réf. Document
DR1	GAR-S2.DSFD.0014.Batch_d_import_ENT.V15.00.docx
DR2	GAR-S2.DSFD.0024.WS_Gestion des données initialisation.V07.00
DR3	GAR-S2.DSFD.0013.IHM_portail_GAR.V20.00.docx
DR4	GAR-S2.DSFD.0012.IHM_affectation et notification expiration d'abonnement.V16.00.docx
DR5	GAR-S2.DSFD.0029.Gestion_des_guichets.V04.00.docx
DR6	MENJS_articulation GuichetEN et GAR_VD2.4.pdf
DR7	GAR-S2.DSFD.0006.Specifications_des_statistiques_et_rapports.V18.00.docx
DR8	GAR-S2.DSFD.0010.Processus_d_acces_aux_ressources.V16.00.docx
DR9	GAR-S2.NOE.0003.Matrice de notifications du GAR.V20.00

## 1.4 Abréviations

Abréviation	Signification
DSF	Document de Spécifications Fonctionnelles
IHM	Interface Homme Machine
SSO	Système d'authentification unique (en anglais Single Sign-On : SSO)
WAYF	Where Are You From
OIDC	OpenId Connect

## 1.5 Glossaire

Glossaire projet : [Glossaire](#)

## 1.6 Présentation générale

Dans le cadre du projet du Gestionnaire d'Accès aux Ressources (GAR), un SSO est mis en place afin de permettre l'accès aux IHM GAR :

- L'IHM d'affectation (cf. DR4)
- Le portail GAR (cf. DR3) et son module de statistiques (cf. [DR7](#))

Ce SSO gère deux sources pour les comptes autorisés :

- Les responsables d'affectation issus :
  - De l'import des données ([DR1](#)) exportées par les ENT pour lesquels l'authentification est déléguée aux ENT
  - De l'import des données ([DR1](#)) exportées par le référentiel académique (RDMEN) pour lesquels l'authentification est déléguée aux guichets d'authentification de l'éducation nationale, pour les responsables d'affectation 1D
  - Des données d'authentification (Vecteur Identité) transmises par le guichet d'authentification des agents, Hub Agent, pour les responsables d'affectation 2D lors de la délégation de leur authentification
- Les comptes GAR issus des données d'initialisations (cf. DR2) pour lesquels l'authentification est gérée par le service décrit dans cette spécification.



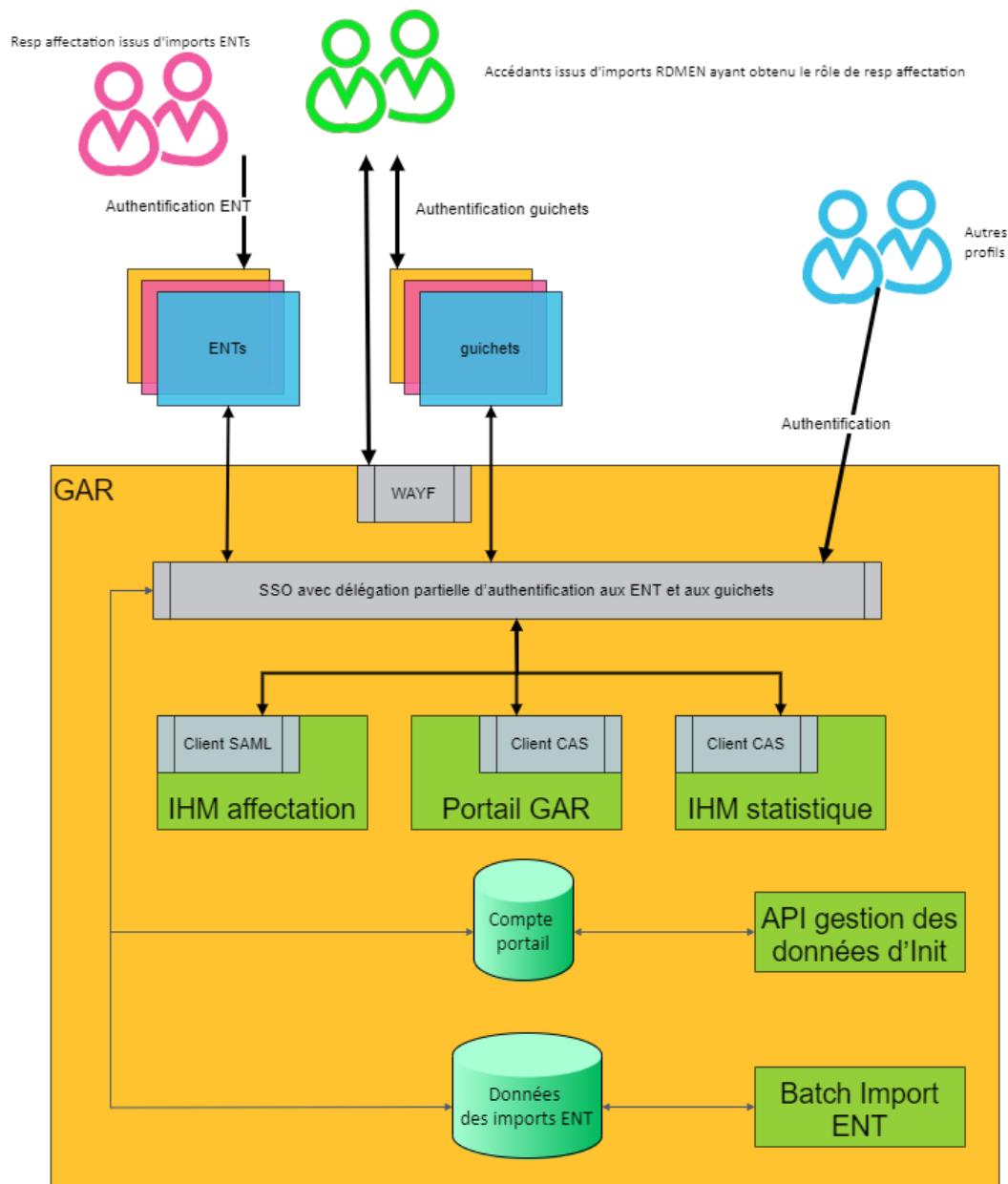


Figure 1: Schéma de principe du SSO des IHM GAR

## 2 Gestion de l'authentification

### 2.1 Principe


Le SSO des IHM du GAR propose les modes d'authentification suivants :

- une authentification locale au GAR pour les comptes créés grâce au WS de gestion des données d'initialisations (cf. DR2),
- une authentification déléguée aux ENT en SAML pour les responsables d'affectations,
- une authentification déléguée aux ENT en OpenIdConnect pour les responsables d'affectations,
- une authentification déléguée aux guichets en OpenIdConnect pour les responsables d'affectations.

Lorsque l'utilisateur n'est pas connecté, il est directement redirigé vers la page de login de l'authentification locale.

Un message configurable sur la page de login indique que les responsables d'affectation doivent accéder au service via leur ENT ou au moyen des guichets d'authentification.

Figure 2: Page de login



The screenshot shows the login page for the GAR (Gestionnaire d'Accès aux Ressources Numériques) portal. The header includes the GAR logo and the text 'LE GESTIONNAIRE D'ACCÈS AUX RESSOURCES NUMÉRIQUES' and 'PORTAIL GAR'. The main heading is 'Connexion au portail'. Below this is a pink banner with the text 'Entrez votre identifiant et votre mot de passe.' The login form consists of two input fields: 'Identifiant:' with the value 'maxime.buttitta@worldline.com' and 'Mot de passe:' with masked characters. A 'SE CONNECTER' button is below the password field. A link 'Réinitialisez votre mot de passe' is provided, followed by a security notice: 'Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.' The footer states 'Service proposé par le ministère en charge de l'Éducation nationale, certains droits réservés'.

## 2.2 Respect de l'accessibilité

L'interface se veut être accessible (en conformité RGAA 4.1 niveau AA) ; c'est-à-dire qu'elle a été conçue de sorte à ce que les personnes en situation de handicap puissent l'utiliser.

Une déclaration de conformité RGAA est accessible sur le site via le « pied de page ». Le contenu de la page « Déclaration de conformité RGAA » est produit par l'application du ministère. Il est accédé via un lien paramétrable fourni par l'application ministère : <https://conformite.education.fr/?appli=GARPortail>

Les règles d'accessibilité suivantes sont appliquées sur l'IHM :

- Éléments obligatoires (thème 8)
  - Le code de langue de la page est le français.
- Présentation de l'information (thème 10)
  - Le lien est identifiable par une indication visuelle au survol/focus
  - L'image cliquable est visible lors du passage de la souris par la présence d'un focus

## 2.3 Authentification via l'ENT

### 2.3.1 Gestion des métadonnées des ENT

La gestion des métadonnées des ENT lors de l'authentification via l'ENT en SAML et en OIDC se fait par l'utilisation d'un cache. Son fonctionnement est détaillé dans la spécification d'Accès aux Ressources (DR8) au §3.1.

### 2.3.2 Authentification via l'ENT en SAML2.0

#### 2.3.2.1 Protocole d'accès

Les responsables d'affectation peuvent se connecter au GAR à partir de leur ENT.

Le protocole d'authentification utilisé dans ce cas-là pour accéder à l'interface d'affectation est :

- SAML 2.0 en mode « Idp-initiated ».

Le projet ENT tient le rôle de fournisseur d'identité, le SSO des IHM du GAR celui de fournisseur de service.

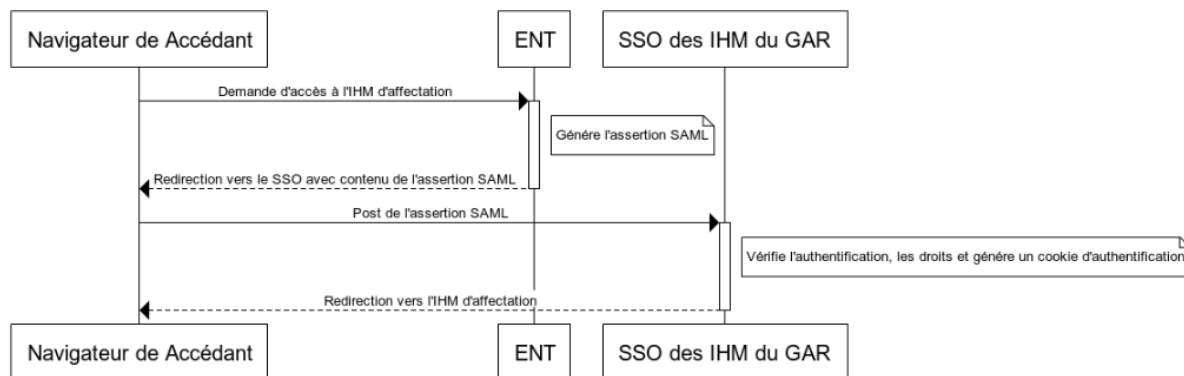
Pour l'authentification SAML : les données suivantes sont à fournir dans l'assertion SAML lors de l'accès au SSO des IHM du GAR:

- Identifiant de l'ENT de l'utilisateur (attribut idEnt)
- Identifiant de l'utilisateur interne à l'ENT (attribut GARPersonIdentifiant)

#### 2.3.2.2 Diagramme de séquence de l'authentification depuis l'ENT en SAML

Le schéma ci-dessous décrit pour les responsables (délégués) d'affectation les échanges de flux entre l'ENT, le navigateur de l'utilisateur et les IHMs du GAR :

Figure 3: Diagramme de séquence de l'authentification par ENT



L'utilisateur clique sur le lien d'accès à l'interface d'affectation depuis son ENT. L'ENT génère l'assertion SAML qui contient les attributs de l'utilisateur et redirige l'utilisateur vers le SSO des IHM du GAR.

**RG\_AUTH\_ENT\_SAML\_1:** Le SSO des IHM du GAR extrait les attributs de l'utilisateur et vérifie que :

- L'ENT est connu du GAR
- L'utilisateur est connu du GAR
- L'utilisateur a bien le rôle responsable d'affectation

Si les informations sont correctes, un cookie d'authentification est créé et l'utilisateur est redirigé vers l'interface d'affectation, sinon une erreur de type compte non connu est affichée dans les différents cas d'usage avant authentification (login, réinitialisation du mot de passe, ...).

## 2.3.3 Authentification via l'ENT en OIDC

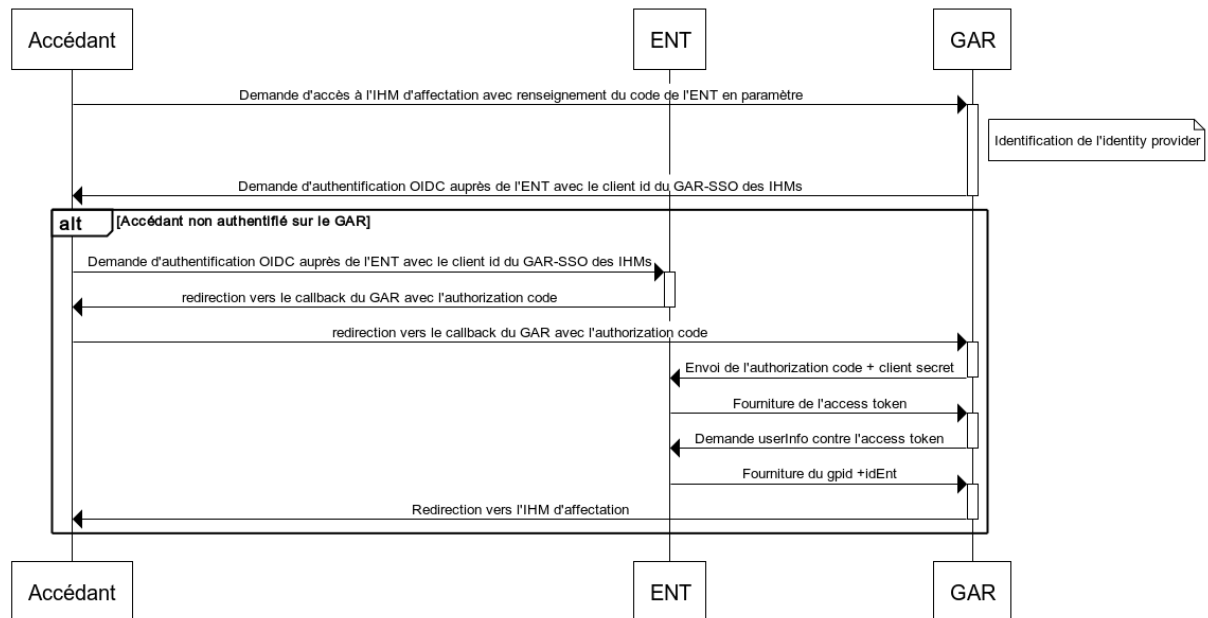
### 2.3.3.1 Protocole d'accès

Le mode IDP initiated utilisé en SAML n'existe pas en OIDC. Il faut donc que ce soit le SSO des IHMs qui initie la demande d'authentification vers l'ENT. A cet effet, l'ENT doit lui-même forger son URL d'accès à l'IHM en renseignant son code ENT en paramètre, afin que le SSO des IHMs puisse identifier le client à utiliser pour la délégation d'authentification.

Pour l'authentification en OIDC : les données suivantes sont à fournir par l'ENT lors de l'appel au endpoint */userinfo*:

- Identifiant de l'ENT de l'utilisateur (attribut *idEnt*)
- Identifiant de l'utilisateur interne à l'ENT (attribut *GARPersonIdentifiant*)

### 2.3.3.2 Diagramme de séquence de l'authentification depuis l'ENT en OIDC



A l'instar de l'authentification en SAML, la règle **RG\_AUTH\_ENT\_SAML\_1** s'applique aussi pour l'authentification en OIDC.

## 2.4 Authentification locale

### 2.4.1 Principe

Pour les comptes créés grâce au WS de gestion des données d'initialisation, les utilisateurs s'authentifient sur le portail GAR avec l'adresse mail qui a été fournie pour la création de leur compte et le mot de passe choisi pendant le processus de création de compte.

Lorsqu'un utilisateur non-authentifié arrive sur le portail GAR, une page demandant à l'utilisateur d'entrer son login et son mot de passe est affichée. Les champs login et mot de passe sont obligatoires et l'indication est donnée par une étoile. Un lien vers le formulaire de demande de réinitialisation de mot de passe est présent sous le formulaire de connexion.

Dans le cas où le couple login/mot de passe est incorrect un message d'erreur générique est affiché.

Dans le cas où l'utilisateur n'a pas changé son mot de passe dans les délais impartis, une page d'erreur avec un message lui indiquant que son compte est bloqué et qu'il doit réinitialiser son mot de passe est affichée. Un lien vers le formulaire de demande de réinitialisation de mot de passe est présent sous le message.

Note : Le délai de changement de mot de passe est paramétrable, par défaut, il est de 183 jours.

Pour les utilisateurs non connus et les responsables d'affectation, une erreur de type compte non connu est affiché dans les différents cas d'usage avant authentification (login, réinitialisation du mdp, ...)

## 2.4.2 Gestion du mot de passe

### 2.4.2.1 Création du mot de passe

Dans le cas d'une initialisation de mot de passe suite à une création de compte portail par le WS de gestion des données d'initialisation, le SSO des IHM est en charge de :

- générer un token et un code de validation utilisateur,
- envoyer un mail à l'utilisateur contenant le code de validation utilisateur et un lien d'accès à la page de saisie du code (Format de la notification définie au §5.1).

Le code correspond à une suite alphanumérique de 6 caractères et est associé au token. Ces 2 informations sont stockées dans Redis avec leur durée de vie associée.

Le token et le code sont à usage unique et avec une durée de validité paramétrable (paramétrée à 48h dans le cas d'une création de compte).

Lorsque l'utilisateur clique sur le lien du mail, il accède à la page de saisie du code (cf. §2.4.2.4).

### 2.4.2.2 Changement de mot de passe

Les mots de passe ont une durée de validité de 6 mois (configurable).

15j et 7j avant l'expiration, un mail est envoyé à l'utilisateur pour l'avertir et lui demander de changer son mot de passe.

Passé ce délai, l'utilisateur doit réinitialiser son mot de passe pour pouvoir accéder aux services.

### 2.4.2.3 Demande de réinitialisation du mot de passe

Un lien sur la page d'authentification et sur la page de mot de passe expiré permet d'accéder au formulaire de demande de réinitialisation de mot de passe. L'utilisateur doit renseigner dans ce formulaire l'adresse mail avec laquelle il se connecte sur le portail GAR.

Une fois le formulaire validé, le SSO des IHM effectue les actions suivantes :

- génération d'un token et d'un code de validation utilisateur,
- envoi d'un mail à l'utilisateur, contenant le code de validation utilisateur et un lien d'accès à la page de saisie du code (Format de la notification définie au §5.2),
- redirection de l'utilisateur vers la page de saisie du code de validation.

Le code correspond à une suite alphanumérique de 6 caractères et est associé au token. Ces 2 informations sont stockées dans Redis avec leur durée de vie associée.

Le token et le code sont à usage unique et avec une durée de validité paramétrable (paramétrée à 1h dans le cas d'une demande de réinitialisation de mot de passe).

Après redirection ou lorsque l'utilisateur clique sur le lien du mail, il accède à la page de saisie du code. La suite du processus est décrite au §2.4.2.4.

#### 2.4.2.4 Validation du code utilisateur et du token

La page de saisie du code de validation présente à l'utilisateur un texte explicatif (libellé paramétrable) et un formulaire contenant un champ de saisie du code et un bouton de validation. Un message indique également à l'utilisateur qu'un mail contenant le code de validation lui a été envoyé. Après saisie du code et validation du formulaire par l'utilisateur, le token (contenu en paramètre de l'url) et le code sont validés et consommés.

L'utilisateur a 3 tentatives de saisie du code (paramétrables). A l'issue des n essais infructueux, le code et le token sont invalidés. Un message invitant l'utilisateur à faire une nouvelle demande de réinitialisation de mot de passe est alors affiché. Ce message contient un lien permettant à l'utilisateur d'être redirigé vers la page de réinitialisation des mots de passe.

Si le code et le token sont validés, l'utilisateur est ensuite redirigé vers la page de saisie du nouveau mot de passe (cf. §2.4.2.5).

#### 2.4.2.5 Saisie du nouveau mot de passe

La page de saisie du nouveau mot de passe est constituée des éléments suivants (libellés paramétrables) :

- Un titre
- Un formulaire contenant :
  - 2 champs obligatoires, dont l'indication est donnée par une étoile : nouveau mot de passe et confirmation du nouveau mot de passe.  
Note : le copier/coller du mot de passe dans la zone de saisie de la confirmation est possible.
  - Un bouton de validation
- Un texte présentant les règles de saisie de mot de passe sous la forme suivante :
  - Une phrase introductive (libellé paramétrable)  
Exemple : « *Votre mot de passe doit être différent de vos 3 derniers mots de passe et respecter les règles suivantes :* »
  - La liste des critères de format (cf. RG-USER-001 Règles de format de mot de passe du document de référence DR3), présentés les uns en dessous des autres et précédé d'une icône de croix pour indiquer que le critère n'est pas respecté.

L'utilisateur renseigne son ancien mot de passe et son nouveau mot de passe 2 fois. Au fur et à mesure de la saisie de l'utilisateur :

- Si un critère de format est respecté, l'icône se transforme en coche verte et toute la ligne s'affiche en vert ;
- Si un critère de format n'est plus respecté, l'icône se transforme à nouveau en croix et la ligne reprend sa couleur initiale.

L'utilisateur valide le formulaire.

Le mot de passe de l'utilisateur est modifié si :

- le nouveau mot de passe est bien entré 2 fois avec la même valeur
- le nouveau mot de passe respecte les règles de format



- le nouveau mot de passe est différent des 3 derniers mots de passe utilisés précédemment

Dans le cas contraire, un message d'erreur s'affiche en rouge en dessous de chaque champ concerné, selon l'ordre de priorité présenté dans le diagramme ci-dessous. Le focus est positionné sur le premier champ en erreur.

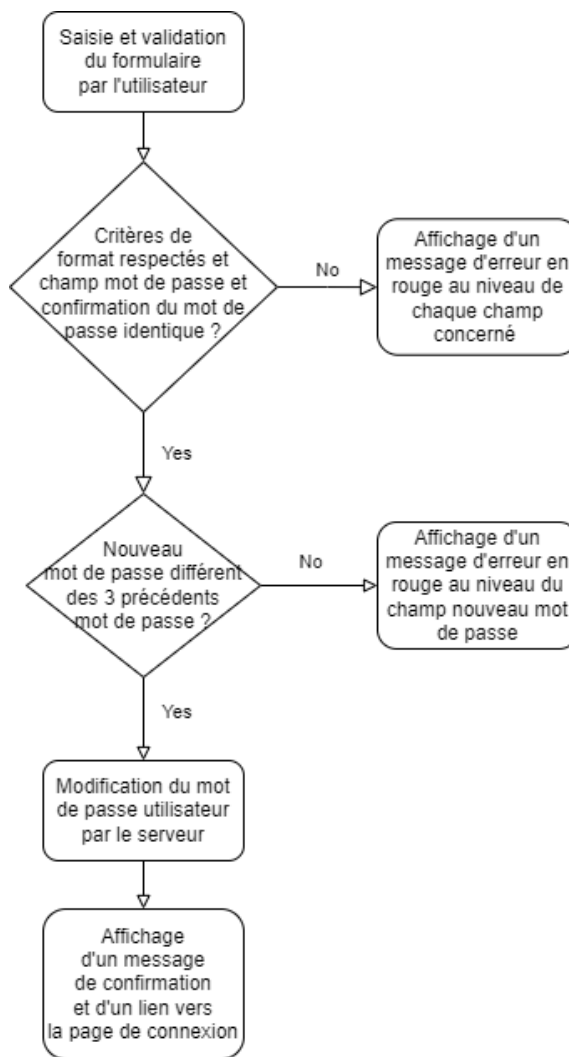


Figure 4 : Diagramme de flux de la modification de mot de passe

## 2.5 Authentification via les guichets

### 2.5.1 Protocole d'accès

Les responsables d'affectation et les agents peuvent se connecter au GAR via une authentification déléguée à un guichet d'authentification.

Le protocole d'échange entre le SSO des IHM et les guichets est OpenIdConnect, avec le SSO des IHM dans le rôle du Relying Party (fournisseur de service) et le guichet dans le rôle de l'OpenId Provider (fournisseur d'identité). Le service SSO des IHM récupère lors des échanges avec le guichet :

- l'identifiant de l'utilisateur pour le GAR (correspondant à l'attribut GAR *GARPersonIdentifiant*)
- les deux attributs *FrEduRneResp* et *FrEduResDel* si le guichet est Hub Agent. Ces attributs contiennent respectivement les listes des autorisations et de délégations pour l'affectation de ressources sur un ou plusieurs établissements (UAI) de 2<sup>nd</sup> degré.

Le détail des échanges est disponible dans le document de référence [DR6](#) de contrat d'interface avec ces guichets.

### 2.5.2 Gestion des métadonnées des guichets

La gestion des métadonnées des guichets lors de l'authentification via les guichets en OIDC se fait par l'utilisation d'un cache. Son fonctionnement est détaillé dans la spécification d'Accès aux Ressources (DR8) au §3.1.

### 2.5.3 Accès aux guichets

Si l'information du guichet choisi est déjà fournie lors de l'appel initial, le SSO des IHMs peut directement rediriger vers le guichet choisi.

Sinon, sans information de guichet fourni, l'utilisateur est simplement redirigé par la page d'authentification du SSO des IHMs GAR.

Le schéma ci-dessous résume pour les responsables d'affectation et les agents les échanges de flux entre le guichet, le navigateur de l'utilisateur, le service WAYF et le SSO des IHMs GAR :

### Accès direct sans authent IHM Affectation par guichet

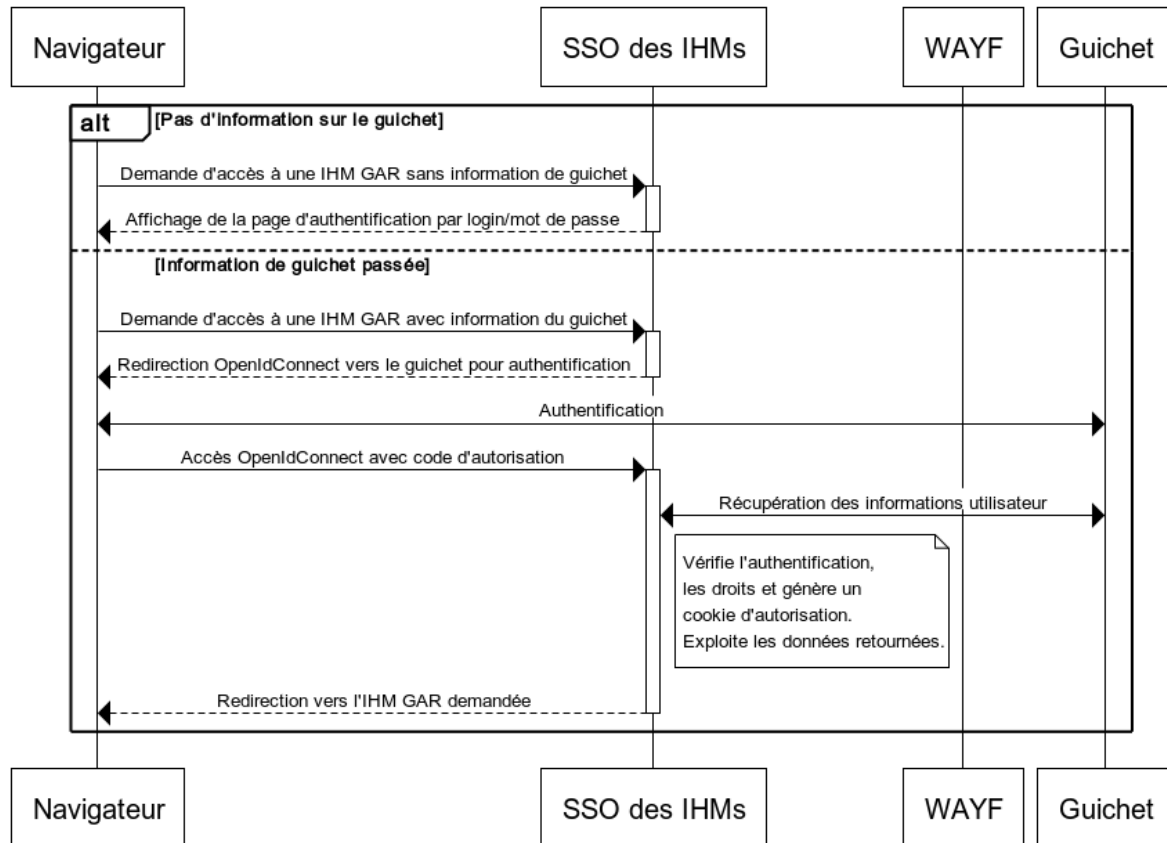


Figure 5: Diagramme global de séquence de l'authentification avec un guichet

Le Contrat d'Interface [DR6](#) détaille ce protocole dans le paragraphe *Interconnexion technique > Schéma des interactions > IHM d'Affectation du GAR*.

L'utilisateur accède à une IHM GAR depuis un lien :

- Sans information sur le guichet, l'utilisateur n'étant pas connu, le SSO des IHM GAR le redirige vers la page d'authentification du portail GAR, sans lien vers le WAYF.
- Avec l'information du guichet (paramètre `idpHint`, cf. [DR5](#)), le SSO des IHM GAR lance un dialogue OpenIdConnect entre l'utilisateur et le guichet afin de l'authentifier.

En particulier, le guichet HubAgent transmet sur appel au endpoint `/userinfo` l'information des rôles de responsable d'affectation de l'accédant, qui sont exploités par le SSO comme décrit au §2.6 Gestion des rôles de Responsable d'Affectation pour le 2D.

## 2.6 Gestion des rôles de Responsable d'Affectation pour le 2D RDMEN

Lorsque le SSO délègue son authentification auprès du guichet Hub Agent, celui-ci lui transmet les informations nécessaires à la mise à jour dans le GAR des rôles de Responsable d'Affectation sur les établissements 2D de l'accédant connecté, sous la forme des deux champs *FrEduRneResp* et *FrEduResDel*. Le format de ces attributs est décrit dans le [DR6](#), au paragraphe *Interconnexion technique > Guichet Agents > Identité transmise pour les agents > Définition du rôle de RA dans le 2D*.

Les règles de gestion suivantes s'appliquent alors :

**RG\_RA2D\_1** : Le traitement tient compte des attributs *FrEduRneResp* et *FrEduResDel* uniquement si l'accédant connecté est un utilisateur 2D, au sens présent dans le GAR suite à l'import d'une archive 2D RDMEN.

**RG\_RA2D\_2** : Pour chaque valeur du champ *FrEduRneResp* au format explicité par le [DR6](#) :

**<UAI établissement >\$<UAA ou UAJ>\$<PU ou PR>\$<Flag activité N ou A ou F>\$T<1er chiffre du code TNA>\$<code TTY>\$<code TNA>**

- Le traitement vérifie que **<1er chiffre du code TNA>** est égal à la valeur du 1er chiffre du **<code TNA>** de l'établissement (nomenclature BCN : N\_NATURE\_UAI) pour les établissements du 2D et qu'elle est égale à une valeur paramétrable (actuellement égale à 3).
  - Si oui, le traitement vérifie que l'UAI référencé **<UAI établissement >** est connu du GAR, sur le 2D, et associé à un ENT de type académique (fourni par le composant RDMEN dans une archive d'import 2D).
- Sinon, la valeur du champ est ignorée.

**RG\_RA2D\_3** : Pour chaque valeur du champ *FrEduResDel* au format explicité par le [DR6](#) :

**<nomappli>|<nomressource>|<datedebut>|<datefin>|<delegant>|<fredurnerresp>|<idserveur>|<fonctiondeleguee>|**

- Le traitement vérifie que :
  - le nom de l'application **<nomappli>** est valorisé par « *gar affectation* » (valeur paramétrable),
  - le nom de la ressource **<nomressource>** contient l'argument d'URL « *applicationname=gar affectation* » (valeur paramétrable),
  - la délégation est en cours de validité, c'est-à-dire que la date du traitement *dt* est encadrée par la date de début de validation de la délégation **<datedebut>** et la date de fin de validation de la délégation **<datefin>** communiquées :  
**<datedebut> ≤ dt ≤ <datefin>**,
  - la **RG\_RA2D\_2** s'applique sur la valeur du champ multivalué **<frEduRneResp>**
- Sinon, la valeur du champ est ignorée.

**RG\_RA2D\_4** : Les autorisations conférées par l'attribut *FrEduRneResp* prévalent sur celles de l'attribut *FrEduResDel*. Ainsi, si un UAI est présent dans ces 2 attributs, les restrictions de délégation sont ignorées.

**RG\_RA2D\_5** : Sur la base des règles **RG\_RA2D\_2** à **RG\_RA2D\_4**, la liste des autorisations RA 2D distinctes ayant cours au moment de l'authentification est constituée à partir des deux champs *FrEduRneResp* et *FrEduResDel*, puis confrontée avec celle présente pour l'utilisateur dans le GAR. Le traitement effectue si nécessaire la mise à jour en base de données des profils RA 2D de l'utilisateur correspondant aux établissements UAI listés (en ajout et suppression). Ces mises à jour n'occasionnent pas de modifications sur les préférences de notifications de chacun des profils RA de l'utilisateur.

**RG\_RA2D\_6** : Les préférences de notifications RA liées aux nouveaux profils RA de l'identité sont désactivées.

Dans tous les cas, si à l'issue de cette mécanique l'utilisateur authentifié possède au moins un profil de RA sur un établissement du GAR pour un ENT de type académique, un cookie d'authentification est créé et l'utilisateur est redirigé vers l'interface demandée. Sinon une erreur de type compte non connu est affiché dans les différents cas d'usage avant authentification (login, réinitialisation du mot de passe, ...).

## 2.7 Durée de session

La durée de session est paramétrable. La durée de session est prolongée lorsque l'utilisateur est actif. Dans tous les cas la déconnexion met fin aux sessions applicatives (cf. §3)

## 2.8 Gestion des droits d'accès

L'ensemble des comptes autorisés sur le SSO peut accéder au portail GAR et au module statistique. Seuls les responsables d'affectations peuvent accéder à l'IHM d'affectation. Si un utilisateur non authentifié essaye d'accéder à une des interfaces, il sera alors redirigé vers la page d'authentification du portail GAR.

## 2.9 Affichage d'une page d'erreur

### 2.9.1 Description de la page

En cas d'erreur, une page indiquant l'erreur est affichée à l'accédant 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

### 2.9.2 Exemple

- Corps de la page :

« La page demandée n'existe pas. Cliquez ici pour revenir à l'accueil.

»

- 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 Gestion de la déconnexion

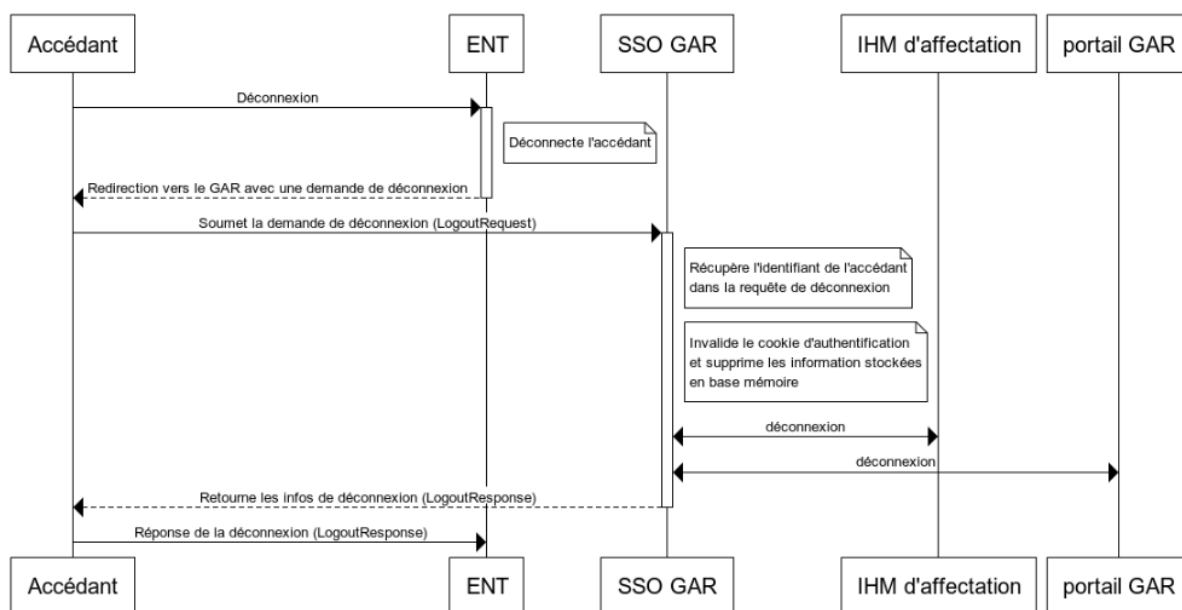
### 3.1 Principe

La déconnexion (single logout) du service SSO des IHMs peut être initiée dans les cas suivants :

- Réception d'un single logout émis par l'ENT (suite à la déconnexion de l'utilisateur sur l'ENT ou la fin de sa session ENT)
- Réception d'une déconnexion par un service GAR (cas de l'authentification par guichet)
- La session du SSO du GAR a expiré
- L'utilisateur se déconnecte de l'IHM d'affectation, du portail GAR ou de son module de statistiques

### 3.2 Diagramme de séquence de propagation de la déconnexion depuis l'ENT

Figure 6: Diagramme de séquence propagation de la déconnexion ENT



### 3.3 Propagation de la déconnexion de l'ENT

L'url de déconnexion du GAR est disponible via les métadonnées (SingleLogoutService Binding en SAML ou sur une Url logout du GAR en OIDC).  
 Les requêtes de déconnexion doivent être soumises au GAR via le navigateur de l'utilisateur (POST/redirect).  
 Le logout Request SAML envoyé au GAR doit contenir le namelid fourni lors de la connexion.  
 Le logout Request OIDC envoyé au GAR doit contenir le JSESSIONID fourni lors de la connexion.

### 3.4 Cas de l'authentification déléguée à un guichet

Le service SSO des IHMs GAR dispose d'un point d'entrée pour une déconnexion Front-channel.

Ce point d'entrée peut être appelé par le navigateur de l'utilisateur sur déclenchement par l'utilisateur depuis un service gérant l'initialisation de la déconnexion, parmi lesquels :

- le Mediacentre GAR
- l'IHM d'affectation (dans le cas d'un accès direct)
- d'éventuels Mediacentres tiers

Sur appel à ce point d'entrée, le SSO des IHMs GAR :

- propage la déconnexion aux services IHM d'affectation et portail GAR (et de son module de statistiques)
- détruit sa session pour l'utilisateur
- mais ne propage pas la déconnexion à d'autres services.

comme illustré dans le diagramme suivant :

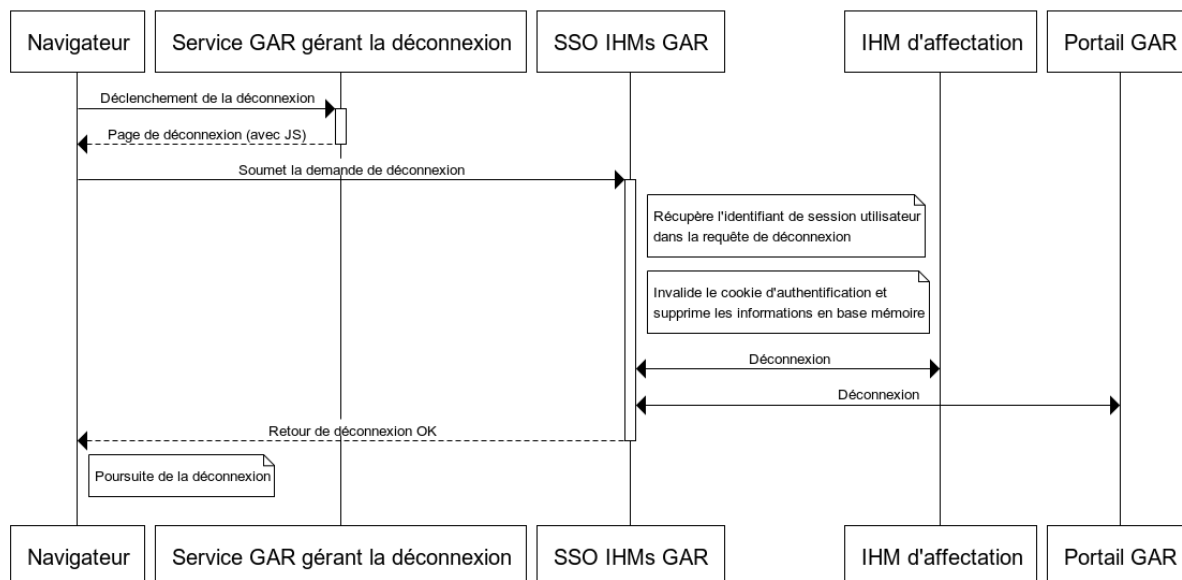


Figure 7: Diagramme de séquence propagation de la déconnexion - cas des guichets



## 4 Utilisation du SSO GAR par les IHM

Lorsque l'utilisateur est authentifié, les IHM du GAR (l'IHM d'affectation, le portail GAR et son module de statistiques) vérifient auprès du SSO que l'utilisateur est authentifié et obtiennent les informations le concernant :

- L'identité de l'utilisateur (nom/prénom)
- Les profils de l'utilisateur et les ids associés à chaque type de profil

Pour les comptes GAR, ces informations proviennent des données d'initialisations.  
Les responsables d'affectation issus (cf DR1) :

- De l'import des données exportées par les ENT,
- De l'import des données exportées par le référentiel académique (RDMEN).

Il s'agit de la liste des UAI pour lesquels l'utilisateur a le rôle de responsable d'affectation et de son uuid\_accedant.

## 5 Notifications

### 5.1 Création de mot de passe Portail GAR

Objet du mail :

[GAR] Création de votre mot de passe Portail GAR

Corps du message :

<EN-TETE>

Bonjour,

Pour accéder à votre compte portail GAR, vous devez initialiser votre mot de passe en suivant le lien ci-dessous :

<url\_accès>

Vous devrez ensuite saisir le code de validation suivant pour accéder à la page de saisie du mot de passe :

<code\_de\_validation>

Attention ce code n'est valide que 48 heures.

<SIGNATURE>

Les variables sont :

<EN-TETE>	en-tête commun à l'ensemble des mails envoyés par le GAR (cf. DR9).
<SIGNATURE>	signature commune à l'ensemble des mails envoyés par le GAR (cf. DR9).
<code_de_validation>	Code de validation de 6 caractères alphanumériques
<url_accès>	url d'accès à la page de saisie du code de validation

### 5.2 Réinitialisation de mot de passe Portail GAR

Objet du mail :

[GAR] Demande de réinitialisation de votre mot de passe Portail GAR

Corps du message :

<EN-TETE>

Bonjour,

Vous avez effectué une demande de réinitialisation de mot de passe pour votre compte Portail GAR.

Pour confirmer, utilisez le code ci-dessous :

<code\_de\_validation>

Attention ce code n'est valide qu'une heure.

Si vous n'avez pas accès à la page, vous pouvez cliquer sur le lien ci-dessous :

<url\_accès>

Si vous ne souhaitez pas réinitialiser votre mot de passe, ignorez ce mail.

<SIGNATURE>

Les variables sont :

<EN-TETE>	en-tête commun à l'ensemble des mails envoyés par le GAR (cf. DR9).
<SIGNATURE>	signature commune à l'ensemble des mails envoyés par le GAR (cf. DR9).
<code_de_validation>	Code de validation de 6 caractères alphanumériques
<url_accès>	url d'accès à la page de saisie du code de validation