



**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 06.3 : RTFS contrat SSO (FR)

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.

Référentiel technique, fonctionnel et de sécurité

Contrat d'interface SSO GAR avec les FR

Documentation à destination des partenaires GAR :
FR : Fournisseurs de ressources

Version GAR 7.4 – Août 2024

gar.education.fr

Suivi des évolutions du document

Date	Version	Description
15/10/2019	1.0	Version initiale
30/01/2023	2.0	Version 7.0 du GAR : Ajout de l'attribut ACCESS_TOKEN dans les protocoles CAS et SAML Mise à jour des liens vers la documentation CAS Gestion du protocole OIDC pour les applications natives
19/10/2023	3.0	Version 7.2 du GAR : Gestion du protocole OIDC pour les ressources web
26/03/2023	4.0	Version 7.2 du GAR : Mise en conformité des échanges d'authentification avec l'activation de la vérification des ACS url Mise en conformité des échanges FR-GAR avec le blocage des urls contenant « // »
08/08/2024	5.0	Version 7.4 du GAR : Précisions apportées sur les RedirectUri en OIDC»

Table des matières

1.	Nouveautés des nouvelles versions du GAR.....	5
1.1.	Nouveautés de la version 7.2 du GAR	5
1.1.1	Gestion du protocole OIDC pour les ressources WEB	5
1.1.2	Mise en conformité des échanges d'authentification avec l'activation de la vérification des ACS URLs.....	5
1.1.3	Mise en conformité des échanges ENT-GAR avec le blocage des urls contenant un « // »	5
2.	Description fonctionnelle des interfaces	6
2.1.	Interface SSO entre le GAR et les FR	6
2.1.1	Documents de référence SAML	6
2.1.2	Documents de référence CAS.....	6
2.1.3	Documents de référence OIDC.....	6
2.2.	Accès aux ressources en SAML.....	6
2.2.1	Métadonnées GAR pour l'accès aux ressources.....	6
2.2.1.1	Exemple.....	6
2.2.1.2	Description	11
2.2.2	Métadonnées FR pour l'accès aux ressources.....	11
2.2.2.1	Exemple.....	11
2.2.2.2	Description	13
2.2.3	Auth Request FR pour l'accès aux ressources	13
2.2.3.1	Exemple.....	13
2.2.3.2	Description	14
2.2.4	Auth Response GAR pour l'accès aux ressources	14
2.2.4.1	Exemple.....	14
2.2.4.2	Description	16
2.2.5	Logout Request SOAP de l'accès aux ressources.....	17
2.2.5.1	Exemple.....	17
2.2.5.2	Description	18
2.2.6	Éléments techniques fournis par le GAR	19
2.3.	Accès aux ressources en CAS.....	19
2.3.1	Validation service ticket (récupération des attributs).....	19
2.3.1.1	Exemple.....	19
2.3.1.2	Description	21
2.3.2	Logout Request de l'accès aux ressources	21
2.3.2.1	Exemple.....	21
2.3.2.2	Description	21
2.4.	Accès aux ressources en OIDC.....	22
2.4.1	Métadonnées GAR pour l'accès aux ressources.....	22
2.4.1.1	Description	22

2.4.1.2	Exemple	22
2.4.2	Spécificités d'implémentation d'OIDC pour le GAR.....	25
2.4.2.1	authorization_endpoint	25
2.4.2.2	userinfo_endpoint.....	25
2.4.2.3	Déconnexion	27
2.4.3	Éléments techniques à fournir dans la notice pour les applications natives.....	27
2.4.4	Éléments techniques à fournir par le FR pour les ressources web.....	27
2.4.5	Éléments techniques fournis par le GAR	28
2.5.	Durées de vie des sessions GAR	28

Table des schémas et tableaux

Tableau 1: Description des métadonnées du GAR.....	11
Tableau 2 : Description des métadonnées d'un FR.....	13
Tableau 3 : Description de la Auth Request.....	14
Tableau 4 : Description de la Auth Response.....	17
Tableau 5 : Description de la requête de logout SAML.....	19
Tableau 6: Description de la réponse CAS	21
Tableau 7: Description de la requête de logout CAS	21
Tableau 8 : Paramètres GAR supplémentaires pour l'appel au "authorization_endpoint"	25
Tableau 9 : Paramètres GAR supplémentaires pour l'appel au "userinfo_endpoint"	26
Tableau 10 : "userinfo_endpoint" - Description des codes retours en cas d'échec.....	26
Tableau 11 : Eléments techniques à fournir par le fournisseur de ressources dans la notice	27
Tableau 12 : Eléments techniques fournis par le GAR	28
Tableau 13 : Description des durées de vie des éléments de sessions GAR	28

1. Nouveautés des nouvelles versions du GAR

1.1. Nouveautés de la version 7.2 du GAR

1.1.1 Gestion du protocole OIDC pour les ressources WEB

L'accès aux ressources web en OIDC est pris en charge par le GAR.

1.1.2 Mise en conformité des échanges d'authentification avec l'activation de la vérification des ACS URLs

Une vérification des *AssertionConsumerServiceURL* (ACS) est mise en place lors de l'accès aux ressources en SAML. Les ACS présentes dans la *SAMLRequest* transmise au GAR doivent correspondre à celles définies dans les métadonnées. Si elles ne correspondent pas, la requête sera ignorée.

Exemple :

une ACS URL reçue dans la SAMLRequest

```
AssertionConsumerServiceURL="https://integ-saml-  
protection.apps.pubqlf.caasnopr.worldline-solutions.com/saml/SSO"
```

Il est nécessaire de retrouver ces ACS URL dans les métadonnées exposées au GAR:

```
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-  
POST" Location="https://integ-saml-protection.apps.pubqlf.caasnopr.worldline-  
solutions.com/saml/SSO" index="0" isDefault="true"/>  
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-  
Artifact" Location="https://integ-saml-  
protection.apps.pubqlf.caasnopr.worldline-solutions.com/saml/SSO" index="1"/>
```

1.1.3 Mise en conformité des échanges ENT-GAR avec le blocage des urls contenant un « // »

Les requêtes ne doivent pas contenir deux "/" consécutifs. Les requêtes contenant deux "/" consécutifs seront rejetées.

Exemple

L'appel à <https://idp-auth.integration.test-gar.education.fr//p3/serviceValidate> devra être modifié pour <https://idp-auth.integration.test-gar.education.fr/p3/serviceValidate> pour être accepté.

2. Description fonctionnelle des interfaces

2.1. Interface SSO entre le GAR et les FR

Ce document décrit l'interface SSO entre le FR et le GAR pour l'accès aux ressources. Cette interface utilise le protocole SAML, CAS ou OIDC pour permettre l'authentification d'un utilisateur à une ressource via le GAR.

Le Module d'accès aux ressources permet aux élèves et aux enseignants d'accéder aux ressources qui leur sont proposées dans le médiacentre ou via d'autres liens dans l'ENT (le cahier de textes par exemple). Ce module permet de garantir que les données utilisateurs fournies lors de l'accès aux ressources sont limitées à celles qui ont été validées en amont, lors de la déclaration des ressources dans le GAR.

Les diagrammes de séquences sont disponibles dans le document RTFS Référentiel technique pour les fournisseurs de ressources.

Les URLs des services par environnement seront communiquées lors de la phase d'accrochage. Les URLs présentes dans les exemples sont données à titre illustratif.

2.1.1 Documents de référence SAML

<http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>

<https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

2.1.2 Documents de référence CAS

<https://apereo.github.io/cas/5.3.x/protocol/CAS-Protocol.html>

<https://apereo.github.io/cas/5.3.x/protocol/CAS-Protocol-Specification.html>

2.1.3 Documents de référence OIDC

https://openid.net/specs/openid-connect-core-1_0.html

https://openid.net/specs/openid-connect-discovery-1_0.html

https://openid.net/specs/openid-connect-rpinitiated-1_0.html

NB : les préconisations de l'OWASP pour prévenir les « path traversal attacks » doivent être respectées (cf. https://owasp.org/www-community/attacks/Path_Traversal).

2.2. Accès aux ressources en SAML

2.2.1 Métadonnées GAR pour l'accès aux ressources

2.2.1.1 Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```



```

xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xml="http://www.w3.org/XML/1998/namespace"
xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" entityID="https://idp-
auth.gar.education.fr/cas/idp">

  <IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">

    <Extensions>
      <shibmd:Scope regexp="false">idp-auth.gar.education.fr</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="fr">GAR
Métadonnées</mdui:DisplayName>
        <mdui:Description xml:lang="fr">IDP du GAR plateforme de
Production</mdui:Description>
        <mdui:Logo height="80" width="80">https://idp-
auth.gar.education.fr/static/images/Logo.png</mdui:Logo>
      </mdui:UIInfo>
    </Extensions>

    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIDRTCCAi2gAwIBAgIIVALATbMh8jFBIVonNz++fwzOcZBQ4MA0GCSqGS Ib3DQEB
CwUAMCQxIjAgBgNVBAMMGWlkC1hdXRoLmdhci5lZHVjYXRpb24uZnIwHhcNMTgw
NDE3MTM1MzE5WWhcNMZgwnDE3MTM1MzE5WjAkMSIwIA YDVQQDBlpZHAtYXV0aC5n
YXJiUzZWR1Y2F0aW9uLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
yLsWaxYrTWa68aCNMX14Ga1ZXHLuYPRPERWT6McBCx39lWn9+ro5le6DlPpYw3cY
1PHrpm+UPohoQ00A9ap+qIzZ+ogyBYCQV6cDDmX2bPH0ihyq8zcVhLGfSURK+ayZ
tEu0VtHsnX83bXJTGZTdbaq4LD3XpDzz9f8Cxn4ElECR/PizJuoCeDsATkdKuBE3
DonIMTVqsY3PbpSvICfYJzBhHJgstSFpeLV12orTlhPq7tLsjpcZI477hUS2v6fS
fzCrEF5yN3IPnF/F+Mp0rJUaNDEg8vyuIKQgNjYjtdBgnYBYS6rVdPe/9Qi30yoP
WJUQOZagR6cLi0oxTOoQ3wIDAQABO24wbDAdBgNVHQ4EFgQUmsKI+8liIOikrAnA
AXvmdXdoIo8wSwYDVR0RBEQwQoIZaWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcoYl
aWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcmlkcC9tZXRhZGF0YTANBgkqhkiG9w0B
AQsFAAOCAQEAZmfsxha6Hu+9Yd71SyLaPXX4mUSoqC8TRQiFsJvQy5TZGP6ZDlL7
PRD7kr+cwdWrzobVAWymPb25fI3pfv0E+VYb5KlMgLuK3jDpOIw6BfeHtR82TcYo
V/cp2R5LtuV7+/UuAvWtKFFInX+wyI+t9JrM/ka3Ws1D7XzZ2QANTZNHorklXauh
2Y+Sw9Y/0Kp04MD6TuvT6XEjIBd3jwRYzg3tdWvBrMGiy3cOcU2PwcW7uDMQyXzj
nEaZsIKhHxreRNvoyRXHNr8PEloI4g8QDNjFrzakUKDrtTUHgLXw1ZY7XPODYC7L
f87NC9n+7ok/J+ifkR23cpXKiBhgkjZUbQ==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:KeyDescriptor>
  </IDPSSODescriptor>
</SAMLResponse>

```

```

</KeyDescriptor>
<KeyDescriptor use="encryption">
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
MIIDRTCCAI2gAwIBAgIVAJtwdfG2jWfAGQp58NygMatav4pMA0GCSqGSIb3DQEBA
CwUAMCQxIjAgBgNVBAMMGWlkcC1hdXRoLmdhci5lZHVjYXRpb24uZnIwHhcNMTgw
NDE3MTM1MzE5WWhcNMZgwnDE3MTM1MzE5WjAkMSIwIAYDVQQDBlZHAAtYXV0aC5n
YXIuZWR1Y2F0aW9uLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
jyioZG+5K3F2jEqR5KJePpx0eDuUmLSlm9zAqC5m44FvtsyjShoViEGJBGTqn+ip
8hlj+7XF/TdIfk/OHh/q1bSriO1fGldC3iPB8DCSxhA+IhK5xycQmE6r3wNcycbr
BLhMaIf+/2Cy9WE9D1brbYhKNf44XZQ6HMRa8Xf7aOF3QBVVbJS8VdW5B1S4zQM
5K9YJUGl/ie9bWiBTbyzuOIXlGUMrzDa32eVNnmpEObISaM+hrG6AuxJfllmbcLW
vk+H1poKtZsJI6kxeasi7heh//b2C1ynwm0tKQRfDy4K8GLTz0WfjP6wj5S/fli+
m+3QsFlFRZwJDMVeh3I2wIDAQABO24wbDAdBgNVHQ4EFgQUqvgiooVlYo0wSQSsz
Xf5M3Kf7h9AwSwYDVR0RBEQwQoIzaWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcoYl
aWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcmlkcC9tZXRhZGF0YTANBgkqhkiG9w0B
AQsFAAOCAQEATsbZH44GAaDaKkN4qgXpXNjVNftCHmxd/n9tbVyThhORcsrDQxfl
yTv+kbP57U4wliYL44Zzkw9ql/k7Zi9iwppl3oghPKVzkyaCmo51lcRd8b08faL
lgQi3r3CZTnFs+Hvb0XgEOpAleMlvJQ+aHJXvzQHB98+tq1SDaPj7F2OniQC2m0B
glWaBx1t8kB8ZdnL3mUqfHDMzeHkrSr7G71CJdF6X6mBDrGzQP3ZrpdIRU4zIM44
vy5A8eeY2BD7gUmxC5/LYAYLv2qslqZ5AvTkSh30v2p/aj6GyOs7bsSRzdDDZ3C7
ZKd2dQAY1wt5tR8Md6IU13feuPQwbAlFVg==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</KeyDescriptor>

  <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
Location="https://idp-
auth.gar.education.fr:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>
  <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://idp-
auth.gar.education.fr:8443/idp/profile/SAML2/SOAP/ArtifactResolution" index="2"/>

  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://idp-
auth.gar.education.fr/idp/profile/SAML2/Redirect/SLO"/>
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://idp-auth.gar.education.fr/idp/profile/SAML2/POST/SLO"/>
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST-SimpleSign" Location="https://idp-
auth.gar.education.fr/idp/profile/SAML2/POST-SimpleSign/SLO"/>

```

```

<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp-auth.gar.education.fr:8443/idp/profile/SAML2/SOAP/SLO"/>

<NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
<NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</NameIDFormat>

<SingleSignOnService
Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://idp-
auth.gar.education.fr/idp/profile/Shibboleth/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://idp-auth.gar.education.fr/idp/profile/SAML2/POST/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST-SimpleSign" Location="https://idp-
auth.gar.education.fr/idp/profile/SAML2/POST-SimpleSign/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://idp-
auth.gar.education.fr/idp/profile/SAML2/Redirect/SSO"/>

</IDPSSODescriptor>

<AttributeAuthorityDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">

  <Extensions>
    <shibmd:Scope regexp="false">idp-auth.gar.education.fr</shibmd:Scope>
  </Extensions>

  <KeyDescriptor use="signing">
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
MIIDRTCCAi2gAwIBAgI VALATbMh8jFBIVonNz++fwzOcZBQ4MA0GCSqGSIb3DQEB
CwUAMCQxIjAgBgNVBAMMGWlkcC1hdXRoLmdhci5lZHVjYXRpb24uZnIwHhcNMTgw
NDE3MTM1MzE5WWhcNMzgWwNDE3MTM1MzE5WjAKMSIwIAYDVQQDBlpZHA tYXV0aC5n
YXIuZWR1Y2F0aW9uLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
yLsWaxYrTWa68aCNMXl4GalZXHLuYPRPERWT6McBCx39lWn9+ro5le6DlPpYw3cY
1PHrpm+UPohoQ00A9ap+qIzZ+ogyBYCQV6cDDmX2bPH0ihyq8zcVhLGfSURK+ayZ
tEu0VtHsnX83bXJTGZTdbaq4LD3XpDzz9f8Cxn4ElECR/PizJuoCeDsATkdKuBE3
DonIMTVqsY3PbpSVicfYJzBhHJgstSFpeLVl2orTlhPq7tLsjpcZI477hUS2v6fS
fzCrEF5yN3IPnF/F+Mp0rJUaNDEg8vyuIKQgNjYjtdBgnYBYS6rVdPe/9Qi30yoP
WJUQOZagR6cLi0oxToOQ3wIDAQABo24wbDADBgNVHQ4EFgQUmsKI+8liIOikrAnA
AXvmdXdoIo8wSwYDVR0RBEQwQoIZaWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcmlk
aWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcmlkC9tZXRhZGF0YTANBgkqhkiG9w0B
AQsFAAOCAQEAMfSxha6Hu+9Yd71SyLaPXX4mUSoqC8TRQiFsJvQy5TZGP6ZDlL7

```

```

PRD7kr+cwdWrzobVAWymPb25fI3pfv0E+VYb5KlMgLuK3jDpOIw6BfeHtR82TcYo
V/cp2R5LtuV7+/UuAvWtKFFInX+wyI+t9JrM/ka3Ws1D7XzZ2QANTZNHorklXauh
2Y+Sw9Y/0Kp04MD6TuvT6XEjIBd3jwRYzg3tdWvBrMGiy3cOcU2PwcW7uDMQyXzj
nEaZsIKhHxreRNvoyRXHNr8PEloI4g8QDNjFrzakUKDrtTUHgLXw1ZY7XPODYC7L
f87NC9n+7ok/J+ifkR23cpXKiBhgkjZUbQ==

    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>

</KeyDescriptor>
<KeyDescriptor use="encryption">
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
MIIDRTCCAi2gAwIBAgIVAjtwdfG2jWfAQp58NygMatav4pMA0GCSqGSIb3DQEB
CwUAMCQxIjAgBgNVBAMMGWlkcC1hdXRoLmdhcj5lZHVjYXRpb24uZnIwHhcNMjgw
NDE3MTM1MzE5WWhcNMzgWWhcNMjgwNDE3MTM1MzE5WjAKMSIwIAYDVQQDBlpZHAAtYXV0aC5n
YXJlZWR1Y2F0aW9uLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
jyioZG+5K3F2jEqR5KJePpx0eDuUmLSlm9zAqC5m44FvtsyjShoViEGJBGTqn+ip
8hlj+7XF/TdIfk/OHh/q1bSriO1fGldC3iPB8DCSxhA+IhK5xycQmE6r3wNcycbr
BLhMaIf+/2Cy9WE9D1brbYhKNf44XZQ6HMRa8Xf7aOF3QBVVbJS8VdW5B1S4zQM
5K9YJUGl/ie9bWiBTbyzuOIXlGUMrzDa32eVNnmpEObISaM+hrG6AuxJfllmbcLW
vk+H1poKtZsJI6kxeasi7heh//b2C1ynwm0tKQRfDy4K8GLTz0WfjP6wj5S/fli+
m+3QsFlFRZwJDMVe1h3I2wIDAQABO24wbDADBgNVHQ4EFgQUqvgiooVlYo0wSQSs
Xf5M3Kf7h9AwSwYDVR0RBEPwQoIzaWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcoYl
aWRwLWF1dGguZ2FyLmVkdWNhdGlvbi5mcmllkcC9tZXRhZGF0YTANBgkqhkiG9w0B
AQsFAAOCAQEATsbZH44GAaDaKkN4qgXpXNjVNftCHmxd/n9tbVyThhORcsrDQxfl
yTv+kbP57U4w1iYL44ZzWk9ql/k7Zi9iwppl3oghPKVzkyaCmo51lcRd8b08faL
lgQi3r3CZTnFs+Hvb0XgEOpAleMlvJQ+aHJXvzQHB98+tq1SDaPj7F2OniQC2m0B
glWaBx1t8kB8ZdnL3mUqfHDMzeHkrSr7G71CJdF6X6mBDrGzQP3ZrpdIRU4zIM44
vy5A8eeY2BD7gUmxC5/LYAYLv2qslqZ5AvTkSh30v2p/aj6GyOs7bsSRzdDDZ3C7
ZKd2dQAY1wt5tR8Md6IU13feuPQwbAlFVg==
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>

</KeyDescriptor>

  <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-
binding" Location="https://idp-
auth.gar.education.fr:8443/idp/profile/SAML1/SOAP/AttributeQuery"/>
  <AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://idp-
auth.gar.education.fr:8443/idp/profile/SAML2/SOAP/AttributeQuery"/>

```

```
</AttributeAuthorityDescriptor>
```

```
</EntityDescriptor>
```

2.2.1.2 Description

Balise	Attribut	Description
EntityDescriptor	entityID	Identifiant du service GAR
IDPSSODescriptor	protocolSupportEnumeration	Liste des versions du protocole SAML supportées par le service, ordonnée par priorité.
KeyDescriptor use="signing"	X509Data	Clef publique permettant de vérifier la signature des requêtes émises par le GAR
KeyDescriptor use="encryption">	X509Data	Clef publique permettant de vérifier le cryptage des requêtes émises par le GAR
SingleLogoutService	Binding	Modalités supportées pour l'appel au logout
SingleLogoutService	Location	Points d'accès pour l'appel logout
SingleSignOnService	Binding	Modalités supportées pour la requête d'authentification
SingleSignOnService	Location	Points d'accès correspondant pour la requête d'authentification
NameIDFormat		Formats de nameid supportés par le GAR
AttributeAuthorityDescriptor	AttributeService	Indique les url supportées pour une requête d'attributs définie dans le protocole SAML

Tableau 1: Description des métadonnées du GAR

2.2.2 Métadonnées FR pour l'accès aux ressources

2.2.2.1 Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https___DNS-ressource" entityID="https://DNS-ressource">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDUjCCAjqgAwIBAgIEUOLIQTANBgkqhkiG9w0BAQUFADBrMQswCQYDVQQGE
wJGSTEQMA4GA1UE
CBMHVXVzaWlhYTERMA8GA1UEBxMISGVsc2lua2kxGDAWBgNVBAoTD1JNNSBTb2Z0d2FyZSBPeTEM
MAoGA1UECwwDUiZEMQ8wDQYDVQQDEwZhcG9sbG8wHhcNMTMwMTAxMTEyODAxWhcNMjIxMjMwMTEy
ODAxWjBrMQswCQYDVQQGEwJGSTEQMA4GA1UECBMHVXVzaWlhYTERMA8GA1UEBxMISGVsc2lua2kx
GDAWBgNVBAoTD1JNNSBTb2Z0d2FyZSBPeTEMMAoGA1UECwwDUiZEMQ8wDQYDVQQDEwZhcG9sbG8w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXqP0wqL2Ai1haeTj0alwsLafhrDtUt00E
5xc7kdD7PISRA270ZmpYMB4W24Uk2QkuwaBp6dI/yRdUvPfOT45YZrqIxMe2451PAQWtEKWF5Z13
F0J4/1B71TtrzyH94RnqSHXFfvRN8EY/rzuEzrpZrHdtNs9LRyLqcRTXMMO4z7QghBuxh3K5gu7K
```

```

qxpHx6No83WNZj4B3gvWLRWv05nbXh/F9YMeQC1TX1iBNAhLQxWhwXMKB4uliPQ/KSaa13R26pON
UUm1qVtU1quQozSTPD8HvsDqGG19v2+/N3uf5dRYtvEPfwXN3wIY+/R93vBA61nl5nTctZIRsyg
0Gv5AgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAFQwAAYUjsolVwjDc2kypK/RRcB8bMAUUIG0hLGL
82IvnKouGixGqAcULwQKIvTs6uGmlgbSG6Gn5ROb2mlBztXqQ49zRvi5qWNRttir6eyqWRFGOM6A
8rxj3Jhxi2Vb/MJn7XzeVHHLzA1sV5hwl/2PLnaL2h9WyG9QwBbwtmkMEqUt/dgixKblRvby/tBu
RogWgPONNSACiW+Z5o8UdAOqNMZQozD/ilgOjBXoF0F50ksjQN7xoQZLj9xXefxCFQ69FPcFDeEW
bHwSoBy5hLPNALaEUoa5zPDwlixwRjFQTc5XXaRpgIjy/2gsL8+Y5QRhyXnLqgO67B1LYW/GuHE=</ds:
X509Certificate>

    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>

<ds:X509Certificate>MIIDUjCCAjqgAwIBAgIEUOLIQTANBgkqhkiG9w0BAQUFADBrMQswCQYDVQQGE
wJGSTEQMA4GA1UE
CBMHVXVzaW1hYTERMA8GA1UEBxMISGVsc2lua2kxGDAWBgNVBAoTD1JNNsBTb2Z0d2FyZSBPeTEM
MAoGA1UECwwDUiZEMQ8wDQYDVQQDEwZhcG9sbG8wHhcNMjMTAxMTEyODAxWhcNMjIxMjMwMTEy
ODAxWjBrMQswCQYDVQQGEwJGSTEQMA4GA1UECBMISGVsc2lua2kxGDAWBgNVBAoTD1JNNsBTb2Z0d2FyZSBPeTEMMAoGA1UECwwDUiZEMQ8wDQYDVQQDEwZhcG9sbG8w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXqP0wqL2AilhaeTj0alwsLafhrDtUt00E
5xc7kdD7PISRA270ZmpYMB4W24Uk2QkuwaBp6dI/yRdUvPfOT45YzrqIXme2451PAQWtEKWF5Z13
F0J4/1B71TtrzyH94RnqSHXffvRN8EY/rzuEzrpZrHdtNs9LRyLqcRTXMMO4z7QghBuxh3K5gu7K
qxpHx6No83WNZj4B3gvWLRWv05nbXh/F9YMeQC1TX1iBNAhLQxWhwXMKB4uliPQ/KSaa13R26pON
UUm1qVtU1quQozSTPD8HvsDqGG19v2+/N3uf5dRYtvEPfwXN3wIY+/R93vBA61nl5nTctZIRsyg
0Gv5AgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAFQwAAYUjsolVwjDc2kypK/RRcB8bMAUUIG0hLGL
82IvnKouGixGqAcULwQKIvTs6uGmlgbSG6Gn5ROb2mlBztXqQ49zRvi5qWNRttir6eyqWRFGOM6A
8rxj3Jhxi2Vb/MJn7XzeVHHLzA1sV5hwl/2PLnaL2h9WyG9QwBbwtmkMEqUt/dgixKblRvby/tBu
RogWgPONNSACiW+Z5o8UdAOqNMZQozD/ilgOjBXoF0F50ksjQN7xoQZLj9xXefxCFQ69FPcFDeEW
bHwSoBy5hLPNALaEUoa5zPDwlixwRjFQTc5XXaRpgIjy/2gsL8+Y5QRhyXnLqgO67B1LYW/GuHE=</ds:
X509Certificate>

    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://DNS-ressource/saml/SingleLogout" />
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://DNS-ressource/saml/SingleLogout" />
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://DNS-ressource/saml/SingleLogout" />
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</md:NameIDFormat>

```

```

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://DNS-
ressource/saml/SSO" index="0" isDefault="true" />
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://DNS-ressource/saml/SSO" index="1" />
</md:SPSSODescriptor>
</md:EntityDescriptor>

```

2.2.2.2 Description

Balise	Attribut	Description
EntityDescriptor	entityID	Identifiant de la ressource (unique en mono SP et partagé par d'autres ressources en sp global)
SPSSODescriptor	AuthnRequestsSigned	Indique si la requête d'authentification sera signée
SPSSODescriptor	WantAssertionsSigned	Indique si les réponses doivent être signées
SPSSODescriptor	protocolSupportEnumeration	Listes des versions du protocole SAML supportées par le service, ordonnée par priorité.
KeyDescriptor use="signing"	X509Data	Clef publique permettant de vérifier la signature des requêtes émises par la ressource
KeyDescriptor use="encryption">	X509Data	Clef publique permettant de vérifier le cryptage des requêtes émises par la ressource
SingleLogoutService	Binding	Modalités supportées pour l'appel au logout
SingleLogoutService	Location	Points d'accès pour l'appel logout
SingleSignOnService	Binding	Modalités supportées pour la requête d'authentification
SingleSignOnService	Location	Points d'accès correspondant pour la requête d'authentification
NameIDFormat		Formats de nameid supportés par la ressource

Tableau 2 : Description des métadonnées d'un FR

2.2.3 Auth Request FR pour l'accès aux ressources

2.2.3.1 Exemple

```

<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://DNS-ressource/saml/SSO"
Destination="https://idp-auth.gar.education.fr/idp/profile/SAML2/Redirect/SSO"
ForceAuthn="false" ID="a18a697eagea5gdc1f7f3j9ed9h126e" IsPassive="false"
IssueInstant="2019-10-04T13:16:23.763Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0" >
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://DNS-
ressource</saml2:Issuer> </saml2p:AuthnRequest>

```


2.2.3.2 Description

Balise	Attribut	Description
AuthnRequest	AssertionConsumerServiceURL	Optionnel. Point d'accès FR correspondant pour la réponse d'authentification à utiliser.
AuthnRequest	Destination	Optionnel. Point d'accès du GAR pour la requête d'authentification
AuthnRequest	ID	Obligatoire. Identifiant de la requête.
AuthnRequest	ForceAuthn	Optionnel. Indique au GAR qu'il n'est pas nécessaire de demander l'authentification de l'utilisateur s'il est déjà authentifié
AuthnRequest	IsPassive	Optionnel. Autorise le GAR à interagir avec l'utilisateur de manière visible.
AuthnRequest	IssueInstant	Obligatoire. Date de la requête
AuthnRequest	ProtocolBinding	Optionnel. Modalité à utiliser pour la réponse d'authentification
AuthnRequest	Version	Obligatoire. Version SAML utilisée
Issuer		Obligatoire. Identifiant du FR (entityID). Identifiant de la ressource (unique en mono SP et partagé par d'autres ressources en sp global)

Tableau 3 : Description de la Auth Request

NB : conformément aux spécifications SAML2 (cf. Documents de référence SAML), l'*AssertionConsumerServiceURL* renseignée dans la *SAMLRequest* doit correspondre à ce qui est défini dans les métadonnées.

2.2.4 Auth Response GAR pour l'accès aux ressources

2.2.4.1 Exemple

```

<?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/xmenc#sha256" />
<ds:DigestValue>J0JU7iEMD1nvMkdwiattOuxH2BfkCX6JspH5QBYlFaE=</ds:DigestValue>
</ds:Reference> </ds:SignedInfo>
<ds:SignatureValue>f5zjVQI+koTJevaK0avxIpLiD2P2ioLGbeylfnBvV29ndcSDBfo/qEfFnH5rFf
pm/WD6nMNM92bv
H9eqMbmKKJaGPaKEgaBPBjAorpAztUxhONhA4LvX+/BgNJwTFsteTJhrHVG7nYzpvWe3BXuGQytY

```



```

XyXj7A0Nh+BS0dFvP3fRpr7fYkahmYoGZjc+tdOmdUgMEhFwBeTAyeZM7Fs5texH1/2d5fiW2TpE
hndzHA5RPBAvmBOJHi/F9il80c+NQuZj/fzjM3Vb8nvdszgPV9QVbwZhEs9PeNu6df6zuptNJ6t
ccyydyiJhsr5aiRe2zw4aRSI/ciULEdbe478vA==</ds:SignatureValue> <ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDZDCCAkygAwIBAgIUTfM0fpOxrfhkkOINpdCF2Q9KgEqwDQYJKoZIhvcNA
QELBQAwLDEqMCgG
A1UEAwWhaWRwLWF1dGgucHAudGVzdClnYXluc2V0aW9uLmZyMB4XDTE4MDQxNzEzNDYzOFoX
DTM4MDQxNzEzNDYzOFowLDEqMCgGA1UEAwWhaWRwLWF1dGgucHAudGVzdClnYXluc2V0aW9u
LmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYsxyKe5fziJ6sp5aPNsg7THbMAD8
scPs2vYwR2JGmnSnAQhOxy0RYkAKRsax19uqWP9YH5LpN15ySn17E0xbUnhHRRDs37aPQ2Tx6fXN
xUx5TBx11GY8wQwZbpaEJXh0wTfLVPSrijP7Yv/Ka/ymeE6bSEUDlKzidWYlhevTmzmJoWcoILpU
tvmOcvVn6CBiB+UOJPSx0EDqfzWoHS+Ai8A06yt+4ABSk/36BQzlddRds+Sn4o9iH/ycIQ12EICT
dqjp24K2X4AsIgMI9GPN5iQ1Cs2MpkJ0b9YgnjZiL2CX9ZXaGuBmIsm59UKsXjSBY+Pt4AKoEnC5
gv0osvv9bQIDAQABo34wfdADBgNVHQ4EFgQUOy5jfMCda28qHrIMzCM+uqNVZDUWwYDVR0RBFQw
UoIhaWRwLWF1dGgucHAudGVzdClnYXluc2V0aW9uLmZyhilpZHAAtYXV0aC5wcC50ZXN0LWdh
ci5lZHVjYXRpb24uZnJpZHAvbWV0YWRhdGEwDQYJKoZIhvcNAQELBQADggEBAH5iMl5nOo0ueXMI
8bQbZPPDOG6n/VfAJgzYaVgtRCPCvKmt+sPb2JY7YoD/ekAfAtlZi23rE/0jckLYGfKkr+3wI0LdH
FUxz0rJ10BEupvHpxJKMzmMQDlFcEQ+qz2mJ0s2hZddNiHaqsJFogvt2aQiZBq9UDS1KEFvOZyeh
FnUslmVXjY9/O920PmiUpNO2S+OX9k14QTPqUK6SAOVLEgSRnoBow8Y069sMqkdK4MENYNpKbOob
CbM+EiO+KMaAuMVh25s+zmyfR4PxOhJWgQ8liFjo1ktdkVBIzDQI7raTu1XWJyWLR8CXiDIzS/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>Password Protec
tedTransport</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>88c1dc611ef894654184ferfg5464f044f6b3cba43a2f943c1990db4bbb
e320f648f942d66e0a7954b8887a94e8f05c486ffb06a9e27074aee9f17b19alf7f</saml2:Attrib
uteValue> </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:Attribute FriendlyName="ACCESS_TOKEN" Name="ACCESS_TOKEN"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3OD
kwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P
Ok6yJV_adQssw5c </saml2:AttributeValue> </saml2:Attribute>
</saml2:AttributeStatement> </saml2:Assertion> </saml2p:Response>

```

2.2.4.2 Description

Balise	Attribut	Description
EntityDescriptor	entityID	Identifiant de la ressource (unique en mono SP et partagé par d'autres ressources en sp global)
SPSSODescriptor	AuthnRequestsSigned	Indique si la requête d'authentification sera signée
SPSSODescriptor	WantAssertionsSigned	Indique si les réponses doivent être signées
SPSSODescriptor	protocolSupportEnumeration	Liste des versions du protocole SAML supportées par le service, ordonnée par priorité.
KeyDescriptor use="signing"	X509Data	Clef publique permettant de vérifier la signature des requêtes émises par la ressource
KeyDescriptor use="encryption">	X509Data	Clef publique permettant de vérifier le cryptage des requêtes émises par la ressource
SingleLogoutService	Binding	Modalités supportées pour l'appel au logout
SingleLogoutService	Location	Points d'accès pour l'appel logout
SingleSignOnService	Binding	Modalités supportées pour la requête d'authentification
SingleSignOnService	Location	Points d'accès correspondant pour la requête d'authentification
NameIDFormat		Formats de nameid supportés par la ressource

Tableau 4 : Description de la Auth Response

2.2.5 Logout Request SOAP de l'accès aux ressources

2.2.5.1 Exemple

```

<?xml version="1.0" encoding="UTF-8"?>
<soap11:Envelope xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
  <soap11:Body>
    <saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
      Destination="https://DNS-ressource/saml/SingleLogout" ID="_2885049634369543319"
      IssueInstant="2019-10-04T09:40:20.067Z" Version="2.0">
      <saml2:Issuer
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">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="#_2885049634369543319">
            <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/xmldsig#sha256" />
            <ds:DigestValue>CPCh5xDjFHWHe91U/U6cbJ2yvMvN7v3ypbV6wu/z3o=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>QZzVctGM97nGDvPdTYe5fAEqgZeSZIf06p4RmKU8rv7GRWp3IY5Y+0Ju41VzKG
          txk3Fahc6+GPKE
          9WVSZIn0cy/MzJWS80/0zQtHt47flu8L53oX+HdS2P0nkXlIOR4ypNp0uB1lEIJjlROb1kK++L82
          iVyA+54XSuvbBlnohXE</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIICiDCCAfGgAwIBAgIJAISh7kt4W+DRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBg
              gNVBAYTAkZSMRMw
              EQYDVQQIDApTb211LVN0YXRlMRIwEAYDVQQKDA1Xb3JsZGxpbnUxJTAjBgNVBAMMHG1kcC5nYXJl
              cWxmLWLRwc2suYXcuYXRvcy5uZXQwHhcNMTYwODE5MDgxNTI1WhcNMTCwODE5MDgxNTI1WjBdMQsw
              CQYDVQQGEwJGUjETMBEGA1UECAwKU29tZS1TdGF0ZTESMBAGA1UECgwJV29ybGRsaW5lMSUwIiwYD
              VQDDDBxpZHAuZ2FyLnFsZi1kcHNrLmF3LmF0b3MubmV0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
              iQKBgQDBDiUCYlMPVBuvWGNphVDtD8yWQYaAQzv3g9XNDP+rrZKpqBWzMsEayS7efGlcHvDIODN

```

```

a3kmcV+bfSpX8cuVvkwHg+cphyFnEzmZyI18aAd3wMGjyVFYZVdVXNzKhrM2fKQZEZhG1BWaxROE
I9BqF+C9bg7hgZu7OQFp1TrhbQIDAQABolAwTjAdBgNVHQ4EFgQUQP4rU4Xx+y+D+6P8ceuND0bg
etowHwYDVR0jBBGwFoAUQP4rU4Xx+y+D+6P8ceuND0bgetowDAYDVR0TBAUwAwEB/zANBgkqhkiG
9w0BAQsFAAOBgQC78Fa31SIuLSgmK0BHFQ5Fy7JlWhtEtcPnuD3axHqkRglVvTz6E9OsjkcgGiC
kDlot3zSTeXlkc3htdxj5JuFkb5Sq0nfq3umveya+MHwyYDGzcMMKwnIs0uHfzyu2hu+NpkBQARM
3pkSV7VVKeh+WPnul6NaA/eJxHJSwaqlAA==</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
  <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
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
">AAdzZWNYZXQxmjs74XZe9B/hz+GBZNHqXeQ2A+hGV63x9AEM4SfZhG2KkXCBJDURku9Nf01/QBzLSyJ
0jakItVoEXRbBb6LdEmXIQvjJvrm6+xroLlWADiA0cNlpVn9cKM9d3HnNkVTiT+nzvQKUAgG3nZ8UJDPj
eNFf</saml2:NameID>
    <saml2p:SessionIndex>ST-1-CBEIUBZEIUVGBZEGVFfwnCmPATHoFkidp-
auth.gar.education.fr</saml2p:SessionIndex>
  </saml2p:LogoutRequest>
</soap11:Body>
</soap11:Envelope>

```

2.2.5.2 Description

La requête de déconnexion du GAR vers la ressource est constituée d'un LogoutRequest encapsulé dans une enveloppe SOAP.

Balise	Attribut	Description
LogoutRequest	Destination	Adresse du point d'accès à laquelle est envoyée la requête
LogoutRequest	ID	Obligatoire. Identifiant de la requête.
LogoutRequest	IssueInstant	Obligatoire. Date de la requête
LogoutRequest	Version	Obligatoire. Version SAML utilisée
LogoutRequest > Issuer		entityID du GAR
LogoutRequest > Signature	CanonicalizationMethod	Doit avoir la valeur http://www.w3.org/2001/10/xml-exc-c14n#
LogoutRequest > Signature	SignatureMethod	Doit avoir la valeur http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
LogoutRequest > Signature	Transform	Doit avoir les valeurs http://www.w3.org/2000/09/xmldsig#enveloped-signature et http://www.w3.org/2001/10/xml-exc-c14n#
LogoutRequest > Signature > DigestMethod	Algorithm	Doit prendre une valeur autorisée dans les métadonnées
LogoutRequest > Signature > DigestMethod	DigestValue	Valeur du hash de la requête

LogoutRequest > Signature	SignatureValue	Obligatoire. Signature de la requête
LogoutRequest > Signature	X509Certificate	Clef publique permettant de vérifier la signature des requêtes émises par le GAR
LogoutRequest > Subject > NameID	Format	Formats de nameid utilisé
Assertion > Subject > NameID	NameQualifier	entityID du GAR
LogoutRequest > Subject > NameID	SPNameQualifier	entityID de la ressource
LogoutRequest > Subject > NameID		Obligatoire. Valeur du nameid correspondant à l'utilisateur au format demandé
LogoutRequest	SessionIndex	Identifiant de session fourni dans l'Auth Response

Tableau 5 : Description de la requête de logout SAML

2.2.6 Éléments techniques fournis par le GAR

Le GAR met à disposition des FR utilisant le protocole SAML le point d'entrée d'accès aux métadonnées SAML suivant pour l'accès aux ressources :

	Plate-forme	Contenu du champ	IP
URL de métadonnées SAML	Tests partenaires	https://idp-auth.partenaire.test-gar.education.fr/idp/metadata	195.221.81.197
	Production	https://idp-auth.gar.education.fr/idp/metadata	195.221.81.4

2.3. Accès aux ressources en CAS

2.3.1 Validation service ticket (récupération des attributs)

2.3.1.1 Exemple

```

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

<cas:user>AAdzZWNyZXQxq6wV28f1fnopefWs/YDdRfzkKC252feaIfiz2aNa10jOrT8GLC0cIyfuM6g
OxiplDCqt1kLNmM/93rsX7LtH6HNKwedaYRJ6K6Fa7UGZwAZDSuATMF9qaPArjf9YmQZ56H3EsMoZRWES
yCLQkdLufQE3</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:P_MS5>22122</cas:P_MS5>

<cas:IDO>7845f4515fev1515ve5448006fdf9227f1896f518d3b5azq984aee5db578cf0877ce2e5c
781f74f03e30abfbf55568c26384f11700708607372c955ac21b0af499</cas:IDO>
    <cas:P_MEL>noreply_@mail.fr</cas:P_MEL>
    <cas:UAI>1234569A</cas:UAI>

<cas:ACCESS_TOKEN>eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6y
JV_adQssw5c</cas:ACCESS_TOKEN>
    </cas:attributes>
    </cas:authenticationSuccess>
</cas:serviceResponse>

```

2.3.1.2 Description

Balise	Description
cas:authenticationSuccess	Obligatoire. Dans le cas d'une connexion réussie
cas:user	Obligatoire. Représente l'identifiant unique de l'utilisateur
cas:attributes	Obligatoire. Liste tous les DCP demandées par la ressource + l'ACCESS_TOKEN (si activé)

Tableau 6: Description de la réponse CAS

2.3.2 Logout Request de l'accès aux ressources

2.3.2.1 Exemple

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="LR-3-
eWeguBdiURbM-VeLwWaH4j0-" Version="2.0" IssueInstant="19-10-
04T11:17:21Z"><saml:NameID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">@NO
T_USED@</saml:NameID><samlp:SessionIndex>ST-5-l9tsei9q7Y877fQyhWwJrUuPrmwidp-
auth.gar.education.fr</samlp:SessionIndex></samlp:LogoutRequest>
```

2.3.2.2 Description

La requête de déconnexion en CAS est envoyée en Url encoded, de manière asynchrone avec un contentType de la forme suivante : application/x-www-form-urlencoded, le paramètre utilisé est nommé logoutRequest.

Balise	Attribut	Description
LogoutRequest	SessionIndex	Service ticket retourné par le GAR lors de l'authentification

Tableau 7: Description de la requête de logout CAS

2.4. Accès aux ressources en OIDC

Le service d'accès aux ressources du GAR tient le rôle d'OP (OpenId Provider) et la ressource (native ou web) celui de RP (Relying Party). La demande d'authentification est initiée par le RP. Le mode d'échange implémenté est l'Authorization Code Flow.

Pour l'application native, le PKCE est rendu obligatoire car l'application native ne peut pas garantir la sécurité du secret.

Pour les ressources web, le secret doit être implémenté et le PKCE est facultatif.

2.4.1 Métadonnées GAR pour l'accès aux ressources

2.4.1.1 Description

Le point d'entrée nommé « well-known » expose les informations techniques du GAR en tant qu'OP pour le protocole OIDC.

Les urls d'accès à ces métadonnées pour l'accès aux ressources sont disponibles dans l'annexe Informations_Techniques du Référentiel technique pour les fournisseurs de ressources.

Les algorithmes de chiffrement devront être dynamiquement choisis par le RP sur la base de la liste des algorithmes supportés par l'OP.

2.4.1.2 Exemple

Les métadonnées GAR pour l'accès aux ressources sont récupérables sur l'endpoint « /.well-known » au format json.

Exemple :

```
{
  "issuer": "https://idp-auth.gar.education.fr/issuer",
  "scopes_supported": ["openid", "scope.gar"],
  "response_types_supported": [
    "code",
    "token",
    "id_token token"
  ],
  "subject_types_supported": [
    "public",
    "pairwise"
  ],
  "claim_types_supported": [
    "normal"
  ],
  "claims_supported": [
    "CIV",
    "DIV",
    "E_MAT",
```



```

"E_MS1",
"E_MS2",
"E_MS3",
"E_MS4",
"E_MS5",
"E_MS6",
"E_MS7",
"E_MS8",
"E_MS9",
"E_MS10",
"E_MS11",
"E_MEF",
"GRO",
"IDO",
"NOM",
"PRO",
"P_MAT",
"P_MS1",
"P_MS2",
"P_MS3",
"P_MS4",
"P_MS5",
"P_MS6",
"P_MS7",
"P_MS8",
"P_MS9",
"P_MS10",
"P_MS11",
"P_MEL",
"P_DIS",
"P_SPE",
"P_MEF",
"UAI",
"DIV_APP",
"PRE",
"NPA",
"APR",
"idENT",
"decodedIdEnt",
"original_ressource_accessed",
"garpersonidentifiant"
],
"grant_types_supported": [
  "authorization_code"

```

```

],
"id_token_signing_alg_values_supported": [
  "none",
  "RS256",
  "RS384",
  {...}
],
"id_token_encryption_alg_values_supported": [
  "RSA1_5",
  {...}
],
"id_token_encryption_enc_values_supported": [
  "A128CBC-HS256",
  {...}
],
"userinfo_signing_alg_values_supported": [
  "none",
  "RS256",
  {...}
],
"userinfo_encryption_alg_values_supported": [
  "RSA1_5",
  "RSA-OAEP",
  {...}
],
"userinfo_encryption_enc_values_supported": [
  "A128CBC-HS256",
  {...}
],
"introspection_endpoint_auth_methods_supported": [
  "client_secret_basic"
],
"token_endpoint_auth_methods_supported": [
  "client_secret_basic",
  "client_secret_post",
  "client_secret_jwt",
  "private_key_jwt"
],
"code_challenge_methods_supported": [
  "plain",
  "S256"
],
"claims_parameter_supported": true,
"request_parameter_supported": false,
"backchannel_logout_supported": false,

```

```

"frontchannel_logout_supported": true,
"jwks_uri": "https://idp-auth.gar.education.fr/oidc/jwks",
"authorization_endpoint": "https://idp-auth.gar.education.fr/oidc/authorize",
"token_endpoint": "https://idp-auth.gar.education.fr/oidc/accessToken",
"userinfo_endpoint": "https://idp-auth.gar.education.fr/oidc/profile",
"registration_endpoint": "https://idp-auth.gar.education.fr/oidc/register",
"end_session_endpoint": "https://idp-auth.gar.education.fr/oidc/logout",
"introspection_endpoint": "https://idp-auth.gar.education.fr/oidc/introspect",
"revocation_endpoint": "https://idp-auth.gar.education.fr/oidc/revoke",
"backchannel_logout_session_supported": false,
"frontchannel_logout_session_supported": true
}

```

2.4.2 Spécificités d'implémentation d'OIDC pour le GAR

En plus des éléments propres au protocole OpenID Connect, le GAR nécessite l'utilisation de paramètres supplémentaires sur l'appel à différents endpoints.

2.4.2.1 authorization_endpoint

Les accès sont réalisés à l'initiative du fournisseur de ressources par l'intermédiaire du « authorization_endpoint » référencé dans les métadonnées.

L'authorization_endpoint est de la forme suivante :

[https://\[host\]/oidc/authorize?idRessource={iddeLaressource}&idEtab={idEtab}&profil={profil}](https://[host]/oidc/authorize?idRessource={iddeLaressource}&idEtab={idEtab}&profil={profil})

Paramètre	Valeur	Obligatoire
idRessource	Identifiant ark de la ressource	Oui
idEtab	Identifiant UAI de l'établissement de l'utilisateur	Non
profil	Profil de l'utilisateur	Non

Tableau 8 : Paramètres GAR supplémentaires pour l'appel au "authorization_endpoint"

- ▶ Lors de l'appel, « idRessource » doit être fourni
- ▶ Si « idRessource » n'est pas fourni, une erreur de type « identifiant de la ressource absent » sera affichée à l'utilisateur.

2.4.2.2 userinfo_endpoint

Le point d'entrée « userinfo_endpoint » permet à la ressource de récupérer les DCP associées à la ressource. La ressource accrochée en OIDC, qu'elle soit native ou web, doit présenter l'Access_token (AT) en Bearer Token dans le header « Authorization », ainsi que les paramètres « idRessource » et « access_mode » à l'endpoint « userinfo_endpoint » pour récupérer ses DCP. De la même manière, une ressource technique commune peut aussi utiliser ce point d'entrée pour récupérer des DCP sur la base d'un AT fourni par une des ressources qui lui est liée.

Le userinfo_endpoint est de la forme suivante :

[https://\[host\]/oidc/profile?idRessource={iddeLaressource}&access_mode={accessMode}](https://[host]/oidc/profile?idRessource={iddeLaressource}&access_mode={accessMode})

Paramètre	Valeur	Obligatoire
idRessource	Identifiant ark de la ressource	Oui
access_mode	Mode d'accès (web appnat rtc)	Oui

Tableau 9 : Paramètres GAR supplémentaires pour l'appel au "userinfo_endpoint"

Les DCP sont retournées au format json.

Exemple :

```

{
  "CIV": "Mme",
  "DIV": "CM1##Division CM1",
  "DIV_APP": "",
  "GRO": "CM1GR1_ELV_ENS##Groupe CM1GR1_ELV_ENS",
  "IDO": "f252e3080f8c092f7505fe94785f22deb24defe4c4deb2bbdc17a74149fcc50104b7946f90f542f945c8b0fa985b6c13698d55ae32a6ff558fe27ab10bf397ae",
  "NOM": "ENSEIGNANT_TEST",
  "P_MS2": "",
  "P_MS3": "",
  "P_MS4": "",
  "P_MS5": "",
  "PRO": "National_ens",
  "UAI": "UAITEST",
  "id": "ENSEIGNANT-TEST-ID",
  "client_id": "d6f5b008-675a-4f9f-b15e-8d643a7c4c5e"
}

```

En cas d'erreur, le GAR retournera un message d'erreur au format json. Exemple :

```

{
  "error": "La ressource demandée n'existe pas"
}

```

Code HTTP	Statut HTTP	Message
401	Unauthorized	Missing_accessToken
401	Unauthorized	Expired_accessToken
403	Forbidden	Paramètre idRessource obligatoire
403	Forbidden	La ressource demandée n'existe pas
403	Forbidden	La RTC demandée n'est pas liée à la ressource de l'Access Token
403	Forbidden	La ressource demandée n'appartient pas à la même plateforme DTR que la ressource de l'Access Token
403	Forbidden	Ressource non affectée <idRessource>
200	OK	Envoi des DCP

Tableau 10 : "userinfo_endpoint" - Description des codes retours en cas d'échec

2.4.2.3 Déconnexion

Dans le cas d'un accès depuis la variante native d'une ressource, les requêtes de déconnexion provenant des applications natives doivent être soumises au GAR via le navigateur qu'elles utilisent (frontchannel).

Ce point d'entrée « end_session_endpoint » est défini dans le fichier métadonnées /.well-known.

Le GAR ne traitera la déconnexion que si l'origine de la connexion provient d'une application native. Si l'origine de la connexion provient d'une variante web, le GAR ignorera la demande de déconnexion.

Il n'est pas attendu de requêtes de déconnexion depuis une ressource web en OIDC vers le GAR. Le cas échéant, le GAR répondra une erreur HTTP 501 Not implemented.

2.4.3 Éléments techniques à fournir dans la notice pour les applications natives

Nom du champ	Commentaire	Contenu du champ
ClientId	Identifiant client	un identifiant unique au sein du GAR. Le client id sera un UUID version 4. Obligatoire.
RedirectUri	URI de redirection vers la ressource. C'est l'URI d'accès à la ressource native et également URI de Callback lors du processus d'authentification	une URI de redirection vers laquelle la réponse à la demande d'authentification doit être envoyée. Chaîne de caractères (256. Max, URL valide). Obligatoire
ClientName	Nom permettant d'identifier une application native	un nom reconnaissable sans espace identifiant l'application native. Obligatoire

Tableau 11 : Éléments techniques à fournir par le fournisseur de ressources dans la notice

2.4.4 Éléments techniques à fournir par le FR pour les ressources web

Nom du champ	Commentaire	Contenu du champ
ClientId	Identifiant client	un identifiant unique au sein du GAR. Le client id sera un UUID version 4. Obligatoire.
RedirectUri	URI de redirection vers la ressource. C'est l'URI d'accès à la ressource native et également URI de Callback lors du processus d'authentification	une URI de redirection vers laquelle la réponse à la demande d'authentification doit être envoyée. Chaîne de caractères respectant l'expression régulière : https://(www\.)?[-a-zA-Z0-9@:%._\+~#={1,256}\.[a-zA-Z0-9()]{1,6}\b([-a-zA-Z0-9()@:%._\+~#?&/=]*). Obligatoire.
URLLogout	Lien vers le endpoint de déconnexion de la ressource	Chaîne de caractères (1024. Max, URL valide) Obligatoire
secret	« Mot de passe » partagé entre le FR et le GAR	Chaîne de caractères (comprise entre 32 et 256 caractères) Obligatoire (transmission de manière sécurisée par conteneur)

2.4.5 Éléments techniques fournis par le GAR

Le GAR met à disposition des FR utilisant le protocole OIDC le endpoint de découverte suivant pour l'accès aux ressources :

	Plate-forme	Contenu du champ	IP
URL well-known	Tests partenaires	https://idp-auth.partenaire.test-gar.education.fr/oidc/.well-known/openid-configuration	195.221.81.197
	Production	https://idp-auth.gar.education.fr/oidc/.well-known/openid-configuration	195.221.81.4

Tableau 12 : Éléments techniques fournis par le GAR

Le scope à utiliser pour récupérer les informations autorisées pour le service d'accès aux ressources est : « scope.gar ».

2.5. Durées de vie des sessions GAR

Élément de session	Durée
Durée de vie de la session	1h00
Durée maximale de la session	6h00
Durée de vie de l'Access Token	1h00
Durée maximale de l'Access Token	6h00
Durée de vie du Refresh Token	6h00

Tableau 13 : Description des durées de vie des éléments de sessions GAR