MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE
Liberté Égalité Fraternité

GAR LE GESTIONNAIRE D'ACCÈS AUX RESSOURCES NUMÉRIQUES

DNE-GAR

Référentiel technique, fonctionnel et de sécurité

Contrat d'interface SSO GAR avec les ENT

Documentation à destination des partenaires GAR :
ENT : Exploitants ENT

Version GAR 7.2 – Mars 2024

gar.education.fr

RENATER
CONNECTEUR DE SAVOIRS

Suivi des évolutions du document

Date	Version	Description
28/06/2019	1.0	Version initiale
04/08/2021	2.0	Description détaillée de l'interface d'accès à l'interface d'affectation
12/10/2022	3.0	Ajout du protocole OIDC
03/04/2023	4.0	Version 7.0 du GAR : Propagation de déconnexion des applications natives vers les ENT
15/06/2023	5.0	Version 7.1 du GAR : Mise en cache des métadonnées ENT SAML et OIDC
26/03/2024	6.0	Version 7.2 du GAR : Mise en conformité des échanges SAML par rapport au paramètre RelayState Mise en conformité des échanges ENT-GAR avec le blocage des urls contenant un « // »

Table des matières

Table des schémas et tableaux

1. Nouveautés des nouvelles versions du GAR

1.1. Nouveautés de la version 7.2 du GAR

1.1.1 Mise en conformité des échanges SAML par rapport au paramètre RelayState

Le paramètre *RelayState* envoyé par le GAR au moment de la *SAMLRequest* doit être renvoyé à l'identique au moment de la *SAMLResponse*.

1.1.2 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 par https://idp-auth.integration.test-gar.education.fr/p3/serviceValidate pour être accepté.

1.2. Nouveautés de la version 7.1 du GAR

1.2.1 Mise en cache des métadonnées ENT pour les protocoles OIDC et SAML

Une mise en cache des métadonnées ENT pour les protocoles SAML et OIDC est en place.

1.3. Nouveautés de la version 7.0 du GAR

1.3.1 Intégration des applications natives dans le cadre de confiance du GAR

L'architecture du GAR permet aux ressources disponibles sous la forme d'applications « natives » de fonctionner dans un cadre de confiance renforcé et basé sur le protocole OpenId Connect.

Lors de la déconnexion d'une application native, les partenaires ENT peuvent recevoir la propagation de cette déconnexion et déconnecter l'utilisateur de l'ENT.

2. Description fonctionnelle des interfaces

2.1. Interface SSO entre le GAR et les ENT

Ce document décrit l'interface SSO entre l'ENT et le GAR pour l'accès aux ressources et le SSO des IHMs du GAR. Ces interfaces utilisent les protocoles SAML ou OIDC pour permettre l'authentification via GAR depuis un ENT.

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 bien celles qui ont été validées lors de la déclaration des ressources dans le GAR.

Le SSO des IHMs permet l'accès de l'utilisateur final à l'interface d'affectation et au portail GAR. L'interface d'affectation de ressources numériques permet au responsable d'affectation et son/ses délégués de gérer l'affectation de toutes les ressources de l'établissement dans le respect des abonnements. Le portail GAR leur permet de gérer leurs informations de compte, et les notifications par établissements.

> *Les diagrammes de séquences sont disponibles dans le document RTFS Informations détaillées pour les exploitants ENT*

> *Les URLs des services par environnement sont disponibles dans le document RTFS Document d'accompagnement pour les équipes techniques*

2.1.1 Documents de référence SAML

https://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 OIDC

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

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

2.2. Description SSO en SAML2

2.2.1 SSO Accès aux ressources

2.2.1.1 Gestion du cache des métadonnées ENT

Les métadonnées SAML des ENT sont mises en cache par le GAR afin de minimiser le volume d'échanges et de minimiser l'impact d'éventuelles erreurs d'accès. De ce fait, la propagation des mises à jour des ENT au GAR n'est pas instantanée ; les métadonnées sont actualisées et contrôlées deux fois par jour (début de matinée et début d'après-midi).

2.2.1.2 Métadonnées GAR Accès aux ressources en SAML

Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_gmpm3efixktzxfhrgidul6fxnecuhftppiwgta8" entityID="https://sp-
auth.gar.education.fr" validUntil="2039-03-20T09:25:21.960Z">
    <md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport">
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha384"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha224"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha512"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha384"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-
sha1"/>
    </md:Extensions>
    <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
        <md:Extensions xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-
init">
            <init:RequestInitiator
Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
Location="https://idp-auth.gar.education.fr/login"/>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>

<ds:X509Certificate>MIICnzCCAYegAwIBAgIBATANBgkqhkiG9w0BAQUFADATMREwDwYDVQQDDAh0c
HJlbjAxczAeFw0x
OTAzMjAwOTEzMDNaFw0yMDAzMjAwOTEzMDRaMBMxETAPBgNVBAMMCHRwcmVuMDFzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjVuFRIUnA9HbCTyUQaAolqOV7Xp1pDbuRZcWIQNMJT+q
t7JkEut8X17iarjTqtu6F5cz8g42r4G7E8qo/6G0BRzFHv4emE6DNwWY9ASX3S3lI07fSke3I4xm
6mBxx3mHZY3697TGCwz0GfDGYK0tGspHKHq7EKDhTYEs9rM3D1T5V+E8zafCgjNLIrDHGX0Uosjy
wMe/e2cEpC22GQmmzeR5YH/Cbey0NaxXJzViYhlTguXldM/WAmqz7SRcrULNNK7/1sGLsFZrApSQ
9hBgWezhZmfhJy+T5Kjqb8xRv0y4JIOcfhdyEbG7DwSFitA9BndFeUsjpewTFifY2cZsTwIDAQAB
MA0GCSqGSIb3DQEBBQUAA4IBAQAiay1EIbNcz96HidvPydG190xNI+csc4RLqFGed2LpyoDXANor
9A6kZae5Zbp8liZUslmMo3aQShXY48CNmFzzJfeB1Euz8sD27PXSzse2y+ZnmjRk6lmPaHs2Phz3
R8fv3WrFZQTG3WAJI3l2wxROr75k9PKtwIkzH4PCOEaxjqa4Lq5DuwPev5lVGAcDQEuYeS5zoU3L
P+UkoGhmPWOCcZr0q7GFZZ5VJtvxpoaO+wGPkVC+8qCS9j++/Fk+ZJk4wr4RPTYawrmVcEMWqj95
```

```
A1rasdyEQ1rMn5+S0gmcz7wiCcYn05itseAwABKzAwqkRij0WIYVlq5NT6PUdmbA</ds:X509Certific
ate>
                </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>MIICnzCCAYegAwIBAgIBATANBgkqhkiG9w0BAQUFADATMREwDwYDVQQDDAh0c
HJlbjAxczAeFw0x
OTAzMjAwOTEzMDNaFw0yMDAzMjAwOTEzMDRaMBMxETAPBgNVBAMMCHRwcmVuMDFzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjVuFRIUnA9HbCTyUQaAolqOV7Xp1pDbuRZcWIQNMJT+q
t7JkEut8X17iarjTqtu6F5cz8g42r4G7E8qo/6G0BRzFHv4emE6DNwWY9ASX3S3lI07fSke3I4xm
6mBxx3mHZY3697TGCwz0GfDGYK0tGspHKHq7EKDhTYEs9rM3D1T5V+E8zafCgjNLIrDHGX0Uosjy
wMe/e2cEpC22GQmmzeR5YH/Cbey0NaxXJzViYhlTguXldM/WAmqz7SRcrULNNK7/1sGLsFZrApSQ
9hBgWezhZmfhJy+T5Kjqb8xRv0y4JIOcfhdyEbG7DwSFitA9BndFeUsjpewTFifY2cZsTwIDAQAB
MA0GCSqGSIb3DQEBBQUAA4IBAQAiay1EIbNcz96HidvPydG190xNI+csc4RLqFGed2LpyoDXANor
9A6kZae5Zbp8liZUslmMo3aQShXY48CNmFzzJfeB1Euz8sD27PXSzse2y+ZnmjRk6lmPaHs2Phz3
R8fv3WrFZQTG3WAJI3l2wxROr75k9PKtwIkzH4PCOEaxjqa4Lq5DuwPev5lVGAcDQEuYeS5zoU3L
P+UkoGhmPWOCcZr0q7GFZZ5VJtvxpoaO+wGPkVC+8qCS9j++/Fk+ZJk4wr4RPTYawrmVcEMWqj95
A1rasdyEQ1rMn5+S0gmcz7wiCcYn05itseAwABKzAwqkRij0WIYVlq5NT6PUdmbA</ds:X509Certific
ate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://idp-
auth.gar.education.fr/login?logoutendpoint=true"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://idp-auth.gar.education.fr/login?logoutendpoint=true"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://idp-
auth.gar.education.fr/login?logoutendpoint=true"/>
        <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:emailAddress</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://idp-
auth.gar.education.fr/login" index="0"/>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Description

Balise	Attribut	Description
EntityDescriptor	entityID	Identifiant du service GAR
EntityDescriptor	validUntil	Date maximum à laquelle le rechargement des métadonnées doit être fait
Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"	DigestMethod	Algorithmes de calcul du hash d'intégrité des requêtes supportés par le service
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 supporté 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
AssertionConsumerService	Binding	Modalités supportées pour la réponse d'authentification
AssertionConsumerService	Location	Points d'accès correspondant pour la réponse d'authentification
NameIDFormat		Formats de nameid supporté par le GAR

Tableau 1: Description des métadonnées du GAR

2.2.1.3 Métadonnées ENT Accès aux ressources en SAML

Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
entityID="https://simulent1d2d.validation.test-
gar.education.fr/idp/profile/SAML2/Redirect/SSO">
   <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="encryption">
         <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIICVjCCAb+gAwIBAgIBADANBgkqhkiG9w0BAQ0FADBIMQswCQYDVQQGEwJmc
jEO
MAwGA1UECAwFUGFyaXMxDDAKBgNVBAoMA0NHSTEbMBkGA1UEAwwSaHR0cHM6Ly93
d3cuY2dpLmZyMB4XDTE3MTAxNzE1MDMxMVoXDTIyMTAxNjE1MDMxMVowSDELMAkG
A1UEBhMCZnIxDjAMBgNVBAgMBVBhcmlzMQwwCgYDVQQKDANDR0kxGzAZBgNVBAMM
```

```
Emh0dHBzOi8vd3d3LmNnaS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
1k+8r7/0wdfsG4FkL+zqaHQmsa+UUV0jWAH3jJ+2Ej9isvgH0l50MKaibNFNoVx9
BqN+ZOj4SX0/daituav5jqp0ti0fyb7a4NtJV63ENXwkiFYNL49F7jtclguoANjJ
1rFk3sGK6MdCTYdjlKGt27EzqcY+cBg44mEwaTuehiMCAwEAAaNQME4wHQYDVR0O
BBYEFDSfTethPSjao5I0iDSEivhlWZ9wMB8GA1UdIwQYMBaAFDSfTethPSjao5I0
iDSEivhlWZ9wMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQENBQADgYEAZTgLKYtn
pAzaghUSVyIlsSqfglELR5LejcWiKIg/ucaddQp8G9OHMZKVYi7azUUG3o7cbLXj
0r52WcJdEIKPkV40LvVvKkG/9d/+yfOsUliFdbJESQZO1FsZxr0zS/Fc/mZ36rmB
R1lKUhXGPwFt0JCE6Bxw5Wt+uJ+1VGAPlyc=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
         <md:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
      </md:KeyDescriptor>
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIICVjCCAb+gAwIBAgIBADANBgkqhkiG9w0BAQ0FADBIMQswCQYDVQQGEwJmc
jEO
MAwGA1UECAwFUGFyaXMxDDAKBgNVBAoMA0NHSTEbMBkGA1UEAwwSaHR0cHM6Ly93
d3cuY2dpLmZyMB4XDTE3MTAxNzE1MDMxMVoXDTIyMTAxNjE1MDMxMVowSDELMAkG
A1UEBhMCZnIxDjAMBgNVBAgMBVBhcmlzMQwwCgYDVQQKDANDR0kxGzAZBgNVBAMM
Emh0dHBzOi8vd3d3LmNnaS5mcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
1k+8r7/0wdfsG4FkL+zqaHQmsa+UUV0jWAH3jJ+2Ej9isvgH0l50MKaibNFNoVx9
BqN+ZOj4SX0/daituav5jqp0ti0fyb7a4NtJV63ENXwkiFYNL49F7jtclguoANjJ
1rFk3sGK6MdCTYdjlKGt27EzqcY+cBg44mEwaTuehiMCAwEAAaNQME4wHQYDVR0O
BBYEFDSfTethPSjao5I0iDSEivhlWZ9wMB8GA1UdIwQYMBaAFDSfTethPSjao5I0
iDSEivhlWZ9wMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQENBQADgYEAZTgLKYtn
pAzaghUSVyIlsSqfglELR5LejcWiKIg/ucaddQp8G9OHMZKVYi7azUUG3o7cbLXj
0r52WcJdEIKPkV40LvVvKkG/9d/+yfOsUliFdbJESQZO1FsZxr0zS/Fc/mZ36rmB
R1lKUhXGPwFt0JCE6Bxw5Wt+uJ+1VGAPlyc=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://simulent1d2d.validation.test-
gar.education.fr/auth/logout" />
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://simulent1d2d.validation.test-
gar.education.fr/auth/saml/post/sso/" />
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://simulent1d2d.validation.test-
gar.education.fr/auth/saml/redirect/sso/" />
   </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Description

Balise	Attribut	Description

EntityDescriptor	entityID	Identifiant de l'ENT
EntityDescriptor	validUntil	Date maximum à laquelle le rechargement des métadonnées doit être fait
IDPSSODescriptor	WantAssertionsSigned	Indique si les réponses doivent être signées
IDPSSODescriptor	protocolSupportEnumeration	Listes des versions du protocole SAML supporté 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 L'URL de déconnexion déclarée est utilisée par le GAR uniquement si l'ENT a demandé l'activation de la propagation de la déconnexion
SingleSignOnService	Binding	Modalités supportées pour la requête d'authentification
SingleSignOnService	Location	Points d'accès correspondant pour la requête d'authentification

Tableau 2 : Description des métadonnées d'un ENT

2.2.1.4 Auth Request Accès aux ressources en SAML

Exemple

```
<saml2p:AuthnRequest AssertionConsumerServiceURL="https://idp-
auth.validation.test-gar.education.fr/login" AttributeConsumingServiceIndex="0"
Destination="https://simulent1d2d.validation.test-
gar.education.fr/idp/profile/SAML2/Redirect/SSO" ForceAuthn="false"
ID="_l97sglffx68bbwx6pr08xi4vymavm9tgu0twn12" IsPassive="false"
IssueInstant="2019-07-05T08:05:03.355Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
ProviderName="pac4j-saml" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" >
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
NameQualifier="https://sp-auth.validation.test-gar.education.fr"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" >https://sp-
auth.validation.test-gar.education.fr</saml2:Issuer>
</saml2p:AuthnRequest>
```

Description

Balise	Attribut	Description
AuthnRequest	AssertionConsumerServiceURL	Optionnel. Point d'accès GAR correspondant pour la réponse d'authentification à utiliser.
AuthnRequest	AttributeConsumingServiceIndex	Optionnel. Index du point d'accès dans les métadonnées du GAR.
AuthnRequest	Destination	Optionnel. Point d'accès de l'ENT pour la requête d'authentification
AuthnRequest	ID	Obligatoire. Identifiant de la requête.

AuthnRequest	ForceAuthn	Optionnel. Indique à l'ENT qu'il n'est pas nécessaire de demander l'authentification de l'utilisateur s'il est déjà authentifié
AuthnRequest	IsPassive	Optionnel. Autorise l'ENT 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	Format	Optionnel. Indique que la valeur sera un entityID
Issuer	NameQualifier	Optionnel. Valeur non significative
Issuer		Obligatoire. Identifiant du service GAR (entityID)

Tableau 3 : Description de la Auth Request

2.2.1.5 Auth Response Accès aux ressources en SAML

Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://idp-auth.validation.test-gar.education.fr/login"
ID="_3f296eaea1c1eee3bf6c42d6e5c447a0"
InResponseTo="_l97sglffx68bbwx6pr08xi4vymavm9tgu0twn12" IssueInstant="2019-07-
05T08:05:04.757Z" Version="2.0">
   <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://simulent1d2d.validati
on.test-gar.education.fr/idp/shibboleth</saml2:Issuer>
   <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="_f533e2b32c23312d025f42f268c8af2d" IssueInstant="2019-07-05T08:05:04.757Z"
Version="2.0">
      <saml2:Issuer>https://simulent1d2d.validation.test-
gar.education.fr/idp/shibboleth</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="#_f533e2b32c23312d025f42f268c8af2d">
               <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/xmlenc#sha512" />
```

```
<ds:DigestValue>UMh3fZWsnz4JenIA8Jmwuk/y6IytRrCimLa1yxQwTeAuzhe5WwnHEkH5goeQxo7XZ
y/8BLxlmTB2
486t1DpHzw==</ds:DigestValue>
            </ds:Reference>
         </ds:SignedInfo>

<ds:SignatureValue>iHrsqNEHKdp7OQVMvfxAS1/U7EyjZ7RI7Y91NOfJHnJPLNJcFBpt4yYV+uLXND
XAOUnd+1iE+vme
sXf+FuJo4/iqCcstoH9DNmWasSdt3hURM/9Zv3gn8hkCNi3MVTAuzd3F1FpeJC8FDT4zZWUVJJaa
0uERiIJW+GsT9lOvVvGaEIQS6bA6u+fprjAL01W3K6lMq5OqAIjqaOQztC+W6mk2QHBL0+zOrEH0
RIJJE8909LCE9+bhlbPlB2kuTaCwakQ5yJXf6sgtcXF5XFD9APd4XsV72xxy1/HCxYhZLyACoyry
V8EmbbjWhiAL9hIQO1BMCN+tFvSdO3IMOG2rxg==</ds:SignatureValue>
         <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIDkTCCAnmgAwIBAgIUAzthS2zGnC85lbbXs6xMp0/J+ZYwDQYJKoZIhvcNA
QELBQAwNDEyMDAG
A1UEAwwpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIwHhcNMTcwMzEz
MTcxMjAyWhcNMzcwMzEzMTcxMjAyWjA0MTIwMAYDVQQDDClzaW11bGVudC52YWxpZGF0aW9uLnRl
c3QtZ2FyLmVkdWNhdGlvbi5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ5OFEBy
6evANBTJtm1/u2ODSpYSy0YXpflUz0C2TFiRJ1nD0Zasf2onBAUECV5lsFwH61kRBIROXqaHDscf
ywi+uFcaTkP+v1urvfPnSZR0DH2Iq6fEoCofbnOFPc5T3PfGBDbIhyYEBiP4WyAmx1t7BVbYJitz
s2XxoFhMOlh8+E55u0genTxiVGIwjBj+t1MEY+m70DQY9LLuHxAKWV7K7cwgzsiPtM939wngpuCp
2JOovzCqOF/a5HPrXSffk0JZZe/gEpRxEg/7aJJTDFykHSr4eH7ATUnKZQBWzbStEtY3mW7fh6/T
sLbjN45XUcy062ib6hvMN1E1WC6WZSUCAwEAAaOBmjCBlzAdBgNVHQ4EFgQUemjLva9FWiCumd3R
YJJ4AaJYkZgwdgYDVR0RBG8wbYIpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRp
b24uZnKGQGh0dHBzOi8vc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIv
aWRwL3NoaWJib2xldGgwDQYJKoZIhvcNAQELBQADggEBAC3VtuUoYYNnxXP02HX6UaXIaeJ7ZLWA
wTdwW28uy5sKG7sDSh83rGNEPNhhRNvfBPi49S9UNrdmz99IDwswvXslZK6yARfG2ZLErrczfmmg
CQIpkwzH+ySYf1ODG/Q+WF4CTw3jX5yXkVbwS//9qNhYhII0IBFyppDfcLqv/BGekonfrV3Bor94
QlpdxSkY7Yy42whqWb698c7qnWX5IOBHbWCBfi4mFs051Bg+JRN15GjOeWoX93sjnJtw8oFReCVd
RIPcW9Gg6LE99Tk2GvPtU/wfscMT+Wj+3wpwigBpeWbpN5nXUIzqGs+grVT+uBQX8ZCdayyAwFaC
zJPZdtg=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
      <saml2:Subject>
         <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient" NameQualifier="https://simulent1d2d.validation.test-
gar.education.fr/idp/shibboleth" SPNameQualifier="https://sp-
auth.validation.test-
gar.education.fr">AAdzZWNyZXQxwhdubUb5oP7n/E6t1zRAeJxKX72VM6W5/kUGaUC3SrXIC+WPVDD
BQsGZcRX88HoeGjRjHCPay5KTu6n05CcA/oUIXK3ZwxU0+cENIk05HmPUO4vgBkY3Ohwzn5gr7TfaRclA
CJ+S0v8ZrHSSrzmHn/HZfQbzSA==</saml2:NameID>
         <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData Address="160.92.7.69"
InResponseTo="_l97sglffx68bbwx6pr08xi4vymavm9tgu0twn12" NotOnOrAfter="2019-07-
05T08:10:04.765Z" Recipient="https://idp-auth.validation.test-
gar.education.fr/login" />
```

```
         </saml2:SubjectConfirmation>
      </saml2:Subject>
      <saml2:Conditions NotBefore="2019-07-05T08:05:04.757Z" NotOnOrAfter="2019-
07-05T08:10:04.757Z">
         <saml2:AudienceRestriction>
            <saml2:Audience>https://sp-auth.validation.test-
gar.education.fr</saml2:Audience>
         </saml2:AudienceRestriction>
      </saml2:Conditions>
      <saml2:AuthnStatement AuthnInstant="2019-07-05T08:05:04.740Z"
SessionIndex="_38f336791a3167198320c8ccdde3f148">
         <saml2:SubjectLocality Address="160.92.7.69" />
         <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtec
tedTransport</saml2:AuthnContextClassRef>
         </saml2:AuthnContext>
      </saml2:AuthnStatement>
      <saml2:AttributeStatement>
         <saml2:Attribute FriendlyName="idEnt" Name="idEnt"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue>Z1</saml2:AttributeValue>
         </saml2:Attribute>
         <saml2:Attribute FriendlyName="GARPersonIdentifiant"
Name="GARPersonIdentifiant" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
            <saml2:AttributeValue>0c068e95-9702-4fa2-8560-
204e3629d075</saml2:AttributeValue>
         </saml2:Attribute>
      </saml2:AttributeStatement>
   </saml2:Assertion>
</saml2p:Response>
```

Description

Balise	Attribut	Description
Response	Destination	Adresse du point d'accès auquel est envoyée la requête
Response	ID	Obligatoire. Identifiant de la requête.
Response	InResponseTo	Identifiant de la requête d'authentification reçue.
Response	IssueInstant	Obligatoire. Date de la requête
Response	Version	Obligatoire. Version SAML utilisée
Response > Issuer		entytiID de l'ENT
Status	StatusCode	Doit valoir urn:oasis:names:tc:SAML:2.0:status:Success pour une authentification réussie
Assertion	ID	Obligatoire. Identifiant de la requête.
Assertion	IssueInstant	Obligatoire. Date de la requête
Assertion	Version	Obligatoire. Version SAML utilisée

Balise	Attribut	Description
Assertion	Issuer	Obligatoire. entytiID de l'ENT
Assertion > Signature	CanonicalizationMethod	Doit avoir la valeur http://www.w3.org/2001/10/xml-exc-c14n#
Assertion > Signature	SignatureMethod	Doit avoir la valeur http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Assertion > 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#
Assertion > Signature > DigestMethod	Algorithm	Doit prendre une valeur autorisée dans les métadonnées
Assertion > Signature > DigestMethod	DigestValue	Valeur du hash de la requête
Assertion > Signature	SignatureValue	Obligatoire. Signature de la requête
Assertion > Signature	X509Certificate	Clef publique permettant de vérifier la signature des requêtes émises par le GAR
Assertion > Subject > NameID	Format	Formats de nameid utilisé
Assertion > Subject > NameID	NameQualifier	entytiID de l'ENT
Assertion > Subject > NameID	SPNameQualifier	entytiID du GAR
Assertion > Subject > NameID		Obligatoire. Valeur du nameId correspondant au format/utilisateur
Assertion > Subject > SubjectConfirmation	Method	Indique la méthode de contrainte d'utilisation de l'assertion
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	Address	IP de l'utilisateur pour lequel l'assertion est valide
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	InResponseTo	Identifiant de la requête d'authentification reçue
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	NotOnOrAfter	Date à partir de laquelle la requête est invalide
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	Recipient	Point d'accès GAR autorisé pour lequel l'assertion est valide
Assertion > Conditions	NotBefore	Date à partir de laquelle la requête est valide
Assertion > Conditions	NotOnOrAfter	Date à partir de laquelle la requête est valide
Assertion > Conditions	Audience	EntytiId destinataire de la requête
Assertion > AuthnStatement	AuthnInstant	Date de la requête
Assertion > AuthnStatement	SessionIndex	Identifiant de la session de l'ENT
Assertion > AuthnStatement > SubjectLocality	Address	IP de l'utilisateur authentifié par l'ENT
Assertion > AuthnStatement	AuthnContext	Contexte d'authentification sur l'ENT

Balise	Attribut	Description
Assertion > AttributeStatement > Attribute	FriendlyName	l'idEnt et le GARPersonIdentifiant sont obligatoires
Assertion > AttributeStatement > Attribute	Name	l'idEnt et le GARPersonIdentifiant sont obligatoires
Assertion > AttributeStatement > Attribute	AttributeValue	Valeur de l'idEnt ou GARPersonIdentifiant connu du GAR

Tableau 4 : Description de la Auth Response

NB : conformément aux spécifications SAML 2 (cf. Documents de référence SAML), le paramètre *RelayState* envoyé par le GAR au moment de la *SAMLRequest* doit être renvoyé à l'identique au moment de la *SAMLResponse*.

2.2.1.6 Logout Request front Accès aux ressources en SAML

Exemple

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://idp-auth.validation.test-
gar.education.fr/login?logoutendpoint=true"
ID="_81667aac280a626694f1ae6607347d3b" IssueInstant="2019-07-05T14:12:44.742Z"
Version="2.0">
   <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://simulent1d2d.validati
on.test-gar.education.fr/idp/shibboleth</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="#_81667aac280a626694f1ae6607347d3b">
            <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/xmlenc#sha512"
/>

<ds:DigestValue>RlNhbgggnZxDxNODsIjfv9p/he1GTvWJssecgRhTie/aF6uHdsztFSb3Fj5EyP/80
nLVj8V2lIOO Cn+2gKdqvg==</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>

<ds:SignatureValue>VawR9hqqCUpjyGI9NyTE9wKw4EBwrBXRw2DuWQXLVAXsrXwJDiazzJ0DPVjtXk
BBAfFqoAtxxGl+
ycsbblRHrdcfVfgSz8h9C7NEq7e4k0AuZA4hZDT/iilKkHt46YKW0oQsP+hfZo96jfG1G0DMG9f+
```

```
m5PhenEeUkrGz2MAwkZBhnqe1brywmMG9vzoA9RVzAz2eD7hDvj3/zDGoljSwUJwb9klAoCLep+r
WyyiMbpj1yx/xH2XMeplXhKalK9itFhMgUW9yemnYVBkURIR3zsDdL2wduFNdsv2vrzxZJsE6H8m
bm4tHV6hGhLcBL13fS1v3dU5NkcZeGDZGceLEw==</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>

<ds:X509Certificate>MIIDkTCCAnmgAwIBAgIUAzthS2zGnC85lbbXs6xMp0/J+ZYwDQYJKoZIhvcNA
QELBQAwNDEyMDAG
A1UEAwwpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIwHhcNMTcwMzEz
MTcxMjAyWhcNMzcwMzEzMTcxMjAyWjA0MTIwMAYDVQQDDClzaW11bGVudC52YWxpZGF0aW9uLnRl
c3QtZ2FyLmVkdWNhdGlvbi5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ5OFEBy
6evANBTJtm1/u2ODSpYSy0YXpflUz0C2TFiRJ1nD0Zasf2onBAUECV5lsFwH61kRBIROXqaHDscf
ywi+uFcaTkP+v1urvfPnSZR0DH2Iq6fEoCofbnOFPc5T3PfGBDbIhyYEBiP4WyAmx1t7BVbYJitz
s2XxoFhMOlh8+E55u0genTxiVGIwjBj+t1MEY+m70DQY9LLuHxAKWV7K7cwgzsiPtM939wngpuCp
2JOovzCqOF/a5HPrXSffk0JZZe/gEpRxEg/7aJJTDFykHSr4eH7ATUnKZQBWzbStEtY3mW7fh6/T
sLbjN45XUcy062ib6hvMN1E1WC6WZSUCAwEAAaOBmjCBlzAdBgNVHQ4EFgQUemjLva9FWiCumd3R
YJJ4AaJYkZgwdgYDVR0RBG8wbYIpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRp
b24uZnKGQGh0dHBzOi8vc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIv
aWRwL3NoaWJib2xldGgwDQYJKoZIhvcNAQELBQADggEBAC3VtuUoYYNnxXP02HX6UaXIaeJ7ZLWA
wTdwW28uy5sKG7sDSh83rGNEPNhhRNvfBPi49S9UNrdmz99IDwswvXslZK6yARfG2ZLErrczfmmg
CQIpkwzH+ySYf1ODG/Q+WF4CTw3jX5yXkVbwS//9qNhYhII0IBFyppDfcLqv/BGekonfrV3Bor94
QlpdxSkY7Yy42whqWb698c7qnWX5IOBHbWCBfi4mFs051Bg+JRN15GjOeWoX93sjnJtw8oFReCVd
RIPcW9Gg6LE99Tk2GvPtU/wfscMT+Wj+3wpwigBpeWbpN5nXUIzqGs+grVT+uBQX8ZCdayyAwFaC
zJPZdtg=</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
NameQualifier="https://simulent1d2d.validation.test-
gar.education.fr/idp/shibboleth" SPNameQualifier="https://sp-
auth.validation.test-
gar.education.fr">AAdzZWNyZXQxwhdubUb5oP7n/E6t1zRAeJxKX72VM6W5/kUGaUC3SrXIC+WPVDD
BQsGZcRX88HoeGjRjHCPay5KTu6n05CcA/oUIXK3ZwxU0+cENIk05HmPUO4vgBkY3Ohwzn5gr7TfaRclA
CJ+S0v8ZrHSSrzmHn/HZfQbzSA==</saml2:NameID>
   <saml2p:SessionIndex>_375bb6e129e4405dd265346710b77124</saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

Description

Balise	Attribut	Description
LogoutRequest	Destination	Adresse du point d'accès auquel 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		entytiID de l'ENT
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-

Balise	Attribut	Description
		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
LogoutRequest > Subject > NameID	NameQualifier	entytiID de l'ENT
LogoutRequest > Subject > NameID	SPNameQualifier	entytiID du GAR
LogoutRequest > Subject > NameID		Obligatoire. Valeur du nameId correspondant au format/utilisateur
LogoutRequest	SessionIndex	Identifiant de session fournit dans l'Auth Response

Tableau 5 : Description de la Logout Request

2.2.1.7 Logout Request SOAP Accès aux ressources en SAML

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="url de destination (non utilisé dans le contexte SOAP)" ID="_-
6921761874666457460" IssueInstant="2019-01-15T07:28:06.911Z" Version="2.0">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">Issuer de
l'ENT</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="#_-6921761874666457460">
            <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/xmlenc#sha512"
/>
            <ds:DigestValue>hash permettant de valider l'intégrité de la
requête</ds:DigestValue>
         </ds:Reference>
```

```
      </ds:SignedInfo>
      <ds:SignatureValue>signature de la requête</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>certificat public permettant de vérifier la
signature des requête</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:unspecified">AAdzZWNyZXQxfW+/JYj+Au2SxToP4zU+/TXEz66f+F/YXioKTuwaWXO/s4+gn
HlRoG/hQB9WCNJ14mpKi9opxAjKIjPcJCO3SBeIBtVpIiKVy38jFcFu1QfkLbrdr+BzgVFggMxfM/Rjlk
iGsMyAo8Osf7Rk5MAo0LSkETC2bXNm3kIdl0FuOg==</saml2:NameID>
   <saml2p:SessionIndex>session identifier fournit par le GAR lors de
l'authentification (optionnel)</saml2p:SessionIndex>
</saml2p:LogoutRequest>
</soap11:Body>
</soap11:Envelope>
```

Description

LogoutRequest (cf. Logout Request front Accès aux ressources en SAML) encapsulé dans un élément soap11:Envelope > soap11:Body

2.2.2 SSO des IHMs du GAR (Interface d'affectation & Portail GAR)

2.2.2.1 Métadonnées GAR SSO des IHMs

Exemple

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_daqi55jjq3je8x6an6v4njll4pmflbc0b7v3fi0"
entityID="urn:gar:ihmAffectation:seclin" validUntil="2039-03-20T09:28:05.437Z">
    <md:Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport">
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha384"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#sha224"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha512"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha384"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
        <alg:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-
sha1"/>
    </md:Extensions>
```

```
    <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
        <md:Extensions xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-
init">
            <init:RequestInitiator
Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
Location="https://sso-portail.gar.education.fr/login"/>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>

<ds:X509Certificate>MIIDPjCCAiYCCQCQPJzNuh7k1zANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGE
wJGUjENMAsGA1UE
CAwETm9yZDEPMA0GA1UEBwwGU2VjbGluMQ0wCwYDVQQKDARBVE9TMRIwEAYDVQQLDAlXb3JsZGxp
bmUxDzANBgNVBAMMBmFwb2xsbzAeFw0xNzA4MDkwODMxNDRaFw0xODA4MDkwODMxNDRaMGExCzAJ
BgNVBAYTAkZSMQ0wCwYDVQQIDAROb3JkMQ8wDQYDVQQHDAZTZWNsaW4xDTALBgNVBAoMBEFUT1Mx
EjAQBgNVBAsMCVdvcmxkbGluZTEPMA0GA1UEAwwGYXBvbGxvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAv0tolhk6KlRWaIxsUc2Nv+OE2qLIGB4Z/jtailLvEqVQvNyP26kX7yoN9/hM
zMP0cqsQOmUgtodhReYZ5ZzVt30OuGkWl1GKUMXktVAq8BYWGzJkw+pJyKy5YZjkKmxf1iaRXBIF
mHG1QuMkpYAjMPyOWdHUSsfKauUUTo/lHGyoUhO7XR9jqT5mGt2iyvJHfjZ1pFHyKk/RcEBYezLM
0xJ2JU16j3OgjcshZH5PJF+eihyfzTYwT3K5EW6nA929zLikOGA0jx32CIbGS/r6P/1rU2AMS6YO
ooxjnQKdA85cPgiIB206soEX9V5p8GELNey/DR5s4Y5tklBaozgRlQIDAQABMA0GCSqGSIb3DQEB
BQUAA4IBAQAfACKI9CPNCFKKV1eca9iwtqxF461GKpc5TUL5Wtd4IdwvopeQHgQYyGHom65vX3N+
QHkPorKKUffmaOiiXWNESQBgDxhVfn/GSrw0cSDK9qK/gLoCHC0flT9fYP94F4mAdfgK8AoV7smr
xcWfhCA6tKSp3A5BdBPWIpNg4ghbK586Us7H55uwwhsS9HE/hLHnn74NjuqV83pTLtaG1X0YZmuy
hvDmX/n4AHVefApDIA7cWImQ7djQFtM9ZggZvga8D5t0hLcy6K/P1bcNXRgkARTZ/OQ9gfjLmrNh
1MXEZNbijgl0fa82Q7SVlNQUVfQ41KcejRZaC5ipBEB91gjl</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>MIIDPjCCAiYCCQCQPJzNuh7k1zANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGE
wJGUjENMAsGA1UE
CAwETm9yZDEPMA0GA1UEBwwGU2VjbGluMQ0wCwYDVQQKDARBVE9TMRIwEAYDVQQLDAlXb3JsZGxp
bmUxDzANBgNVBAMMBmFwb2xsbzAeFw0xNzA4MDkwODMxNDRaFw0xODA4MDkwODMxNDRaMGExCzAJ
BgNVBAYTAkZSMQ0wCwYDVQQIDAROb3JkMQ8wDQYDVQQHDAZTZWNsaW4xDTALBgNVBAoMBEFUT1Mx
EjAQBgNVBAsMCVdvcmxkbGluZTEPMA0GA1UEAwwGYXBvbGxvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAv0tolhk6KlRWaIxsUc2Nv+OE2qLIGB4Z/jtailLvEqVQvNyP26kX7yoN9/hM
zMP0cqsQOmUgtodhReYZ5ZzVt30OuGkWl1GKUMXktVAq8BYWGzJkw+pJyKy5YZjkKmxf1iaRXBIF
mHG1QuMkpYAjMPyOWdHUSsfKauUUTo/lHGyoUhO7XR9jqT5mGt2iyvJHfjZ1pFHyKk/RcEBYezLM
0xJ2JU16j3OgjcshZH5PJF+eihyfzTYwT3K5EW6nA929zLikOGA0jx32CIbGS/r6P/1rU2AMS6YO
ooxjnQKdA85cPgiIB206soEX9V5p8GELNey/DR5s4Y5tklBaozgRlQIDAQABMA0GCSqGSIb3DQEB
BQUAA4IBAQAfACKI9CPNCFKKV1eca9iwtqxF461GKpc5TUL5Wtd4IdwvopeQHgQYyGHom65vX3N+
QHkPorKKUffmaOiiXWNESQBgDxhVfn/GSrw0cSDK9qK/gLoCHC0flT9fYP94F4mAdfgK8AoV7smr
```

```
xcWfhCA6tKSp3A5BdBPWIpNg4ghbK586Us7H55uwwhsS9HE/hLHnn74NjuqV83pTLtaG1X0YZmuy
hvDmX/n4AHVefApDIA7cWImQ7djQFtM9ZggZvga8D5t0hLcy6K/P1bcNXRgkARTZ/OQ9gfjLmrNh
1MXEZNbijgl0fa82Q7SVlNQUVfQ41KcejRZaC5ipBEB91gjl</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sso-
portail.gar.education.fr/login?logoutendpoint=true"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://sso-portail.gar.education.fr/login?logoutendpoint=true"/>
        <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://sso-
portail.gar.education.fr/login?logoutendpoint=true"/>
        <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:emailAddress</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sso-
portail.gar.education.fr/login" index="0"/>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Description

Balise	Attribut	Description
EntityDescriptor	entityID	Identifiant du service GAR
EntityDescriptor	validUntil	Date maximum à laquelle le rechargement des métadonnées doit être fait
Extensions xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"	DigestMethod	Algorithmes de calcul du hash d'intégrité des requêtes supportés par le service
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 supporté 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

Balise	Attribut	Description
AssertionConsumerService	Binding	Modalités supportées pour la réponse d'authentification
AssertionConsumerService	Location	Points d'accès correspondant pour la réponse d'authentification
NameIDFormat		Formats de nameid supporté par le GAR

Tableau 6: Description des métadonnées du GAR

2.2.2.2 Métadonnées ENT SSO des IHMs

Les métadonnées publiées par l'ENT pour l'accès ressource sont également utilisées pour l'interface d'affectation. Cf. Métadonnées ENT Accès aux ressources

2.2.2.3 Auth Request SSO des IHMs

L'accès au SSO des IHMs est initié par l'IDP, il n'y a donc pas Auth Request transmise à l'ENT.

2.2.2.4 Auth Response SSO des IHMs

Exemple

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 Destination="https://sso-portail.gar.education.fr/login"
                 ID="_09dccc775d191c01600aa43c35fad932"
                 IssueInstant="2021-08-05T08:37:44.107Z"
                 Version="2.0"
                 >
    <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://entzen.gar.renater.fr/
idp/shibboleth</saml2:Issuer>
    <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="_09049174acfeb05a52abcd35cfd5e76f"
                     IssueInstant="2021-08-05T08:37:44.107Z"
                     Version="2.0"
                     >
        <saml2:Issuer>http://entzen.gar.renater.fr/idp/shibboleth</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="#_09049174acfeb05a52abcd35cfd5e76f">
                    <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/xmlenc#sha512" />

<ds:DigestValue>votyCNTarfsc0QuLt3w8+ucjKQhswgl3BLd18uoIeZUhCI6tcdA88i6ltVK07N18H
wk+ZxugTWWN
5UyHOnW2UQ==</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>
Ol6bSjJykdjPcppbeuI88O9Stkk1ExJ/WHe+oU3EJcTDtyzAWjlBaeY/SSq0ONRQHpqEaoqubq9+
P4Ta3MPUaqRqG+FCG1lD36SU3Xjz0PVrWqun1lxfhcMh3UvqnpjGfJ7mEEKkZ1M5ILUDOcmIYsS4
vg3tSJI+r8n4lkvvgsZdyB1+Y9gRmFfrL0RX1reBGInlTUIYeV0I3qta/U9QyCxmP2cky4OG05sH
LdCD1U1Jk48QpMR8RNkL0fhN6SgmtSd65KafLfP6Umg9a65y1heVO1oT33XV7a0tcLrseQCZixiq
9tuDGChqc1LdfP4ru/GB6vzWG9va+IBANK9jQA==
</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:X509Data>

<ds:X509Certificate>MIIDkTCCAnmgAwIBAgIUAzthS2zGnC85lbbXs6xMp0/J+ZYwDQYJKoZIhvcNA
QELBQAwNDEyMDAG
A1UEAwwpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIwHhcNMTcwMzEz
MTcxMjAyWhcNMzcwMzEzMTcxMjAyWjA0MTIwMAYDVQQDDClzaW11bGVudC52YWxpZGF0aW9uLnRl
c3QtZ2FyLmVkdWNhdGlvbi5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ5OFEBy
6evANBTJtm1/u2ODSpYSy0YXpflUz0C2TFiRJ1nD0Zasf2onBAUECV5lsFwH61kRBIROXqaHDscf
ywi+uFcaTkP+v1urvfPnSZR0DH2Iq6fEoCofbnOFPc5T3PfGBDbIhyYEBiP4WyAmx1t7BVbYJitz
s2XxoFhMOlh8+E55u0genTxiVGIwjBj+t1MEY+m70DQY9LLuHxAKWV7K7cwgzsiPtM939wngpuCp
2JOovzCqOF/a5HPrXSffk0JZZe/gEpRxEg/7aJJTDFykHSr4eH7ATUnKZQBWzbStEtY3mW7fh6/T
sLbjN45XUcy062ib6hvMN1E1WC6WZSUCAwEAAaOBmjCBlzAdBgNVHQ4EFgQUemjLva9FWiCumd3R
YJJ4AaJYkZgwdgYDVR0RBG8wbYIpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRp
b24uZnKGQGh0dHBzOi8vc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIv
aWRwL3NoaWJib2xldGgwDQYJKoZIhvcNAQELBQADggEBAC3VtuUoYYNnxXP02HX6UaXIaeJ7ZLWA
wTdwW28uy5sKG7sDSh83rGNEPNhhRNvfBPi49S9UNrdmz99IDwswvXslZK6yARfG2ZLErrczfmmg
CQIpkwzH+ySYf1ODG/Q+WF4CTw3jX5yXkVbwS//9qNhYhII0IBFyppDfcLqv/BGekonfrV3Bor94
QlpdxSkY7Yy42whqWb698c7qnWX5IOBHbWCBfi4mFs051Bg+JRN15GjOeWoX93sjnJtw8oFReCVd
RIPcW9Gg6LE99Tk2GvPtU/wfscMT+Wj+3wpwigBpeWbpN5nXUIzqGs+grVT+uBQX8ZCdayyAwFaC
zJPZdtg=</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </ds:Signature>
        <saml2:Subject>
            <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                          Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient"

NameQualifier="http://entzen.gar.renater.fr/idp/shibboleth"
                          SPNameQualifier="urn:gar:ihmAffectation:seclin"

>AAdzZWNyZXQxs85ibhXSb+tfOfqYB7+pSrSbWILba/JMKbtI/61Wd0Rz4lK/xqlkKsL/1lElzeaxPmVY
N9yEpiLYL5vv0pjK/k02+DRnPrZ6eQrQTFGT8W9Z+cbhnyapospMDZorTwLvRH3FPVXcJI4t0UY=</sam
l2:NameID>
```

```
            <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData Address="160.92.7.69"
                                               NotOnOrAfter="2021-08-
05T08:42:44.202Z"
                                               Recipient="https://sso-
portail.gar.education.fr/login"
                                               />
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2021-08-05T08:37:44.107Z"
                          NotOnOrAfter="2021-08-05T08:42:44.107Z"
                          >
            <saml2:AudienceRestriction>
                <saml2:Audience>urn:gar:ihmAffectation:seclin</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2021-08-05T08:37:43.823Z"
                              SessionIndex="_398b3a8f4135bc7be57e728b6e79cf8d"
                              >
            <saml2:SubjectLocality Address="160.92.7.69" />
            <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtec
tedTransport</saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute FriendlyName="idEnt"
                             Name="idEnt"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                             >
                <saml2:AttributeValue>ZEN</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="GARPersonIdentifiant"
                             Name="GARPersonIdentifiant"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                             >
                <saml2:AttributeValue>e0023114-51ab-4bd6-a1fa-
7885132c8b5b</saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

Description

Balise	Attribut	Description
Response	Destination	Adresse du point d'accès auquel est envoyée la requête
Response	ID	Obligatoire. Identifiant de la requête.
Response	IssueInstant	Obligatoire. Date de la requête
Response	Version	Obligatoire. Version SAML utilisée
Response > Issuer		entityID de l'ENT
Status	StatusCode	Doit valoir urn:oasis:names:tc:SAML:2.0:status:Success pour une authentification réussie
Assertion	ID	Obligatoire. Identifiant de la requête.
Assertion	IssueInstant	Obligatoire. Date de la requête
Assertion	Version	Obligatoire. Version SAML utilisée
Assertion	Issuer	Obligatoire. entytiID de l'ENT
Assertion > Signature	CanonicalizationMethod	Doit avoir la valeur http://www.w3.org/2001/10/xml-exc-c14n#
Assertion > Signature	SignatureMethod	Doit avoir la valeur http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Assertion > 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#
Assertion > Signature > DigestMethod	Algorithm	Doit prendre une valeur autorisée dans les métadonnées
Assertion > Signature > DigestMethod	DigestValue	Valeur du hash de la requête
Assertion > Signature	SignatureValue	Obligatoire. Signature de la requête
Assertion > Signature	X509Certificate	Clef publique permettant de vérifier la signature des requêtes émises par le GAR
Assertion > Subject > NameID	Format	Formats de nameid utilisé
Assertion > Subject > NameID	NameQualifier	entytiID de l'ENT
Assertion > Subject > NameID	SPNameQualifier	entytiID du GAR
Assertion > Subject > NameID		Obligatoire. Valeur du nameId correspondant au format/utilisateur
Assertion > Subject > SubjectConfirmation	Method	Indique la méthode de contrainte d'utilisation de l'assertion
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	Address	IP de l'utilisateur pour lequel l'assertion est valide

Balise	Attribut	Description
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	InResponseTo	Identifiant de la requête d'authentification reçue
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	NotOnOrAfter	Date à partir de laquelle la requête est invalide
Assertion > Subject > SubjectConfirmation > SubjectConfirmationData	Recipient	Point d'accès GAR autorisé pour lequel l'assertion est valide
Assertion > Conditions	NotBefore	Date à partir de laquelle la requête est valide
Assertion > Conditions	NotOnOrAfter	Date à partir de laquelle la requête est valide
Assertion > Conditions	Audience	EntytiId destinataire de la requête
Assertion > AuthnStatement	AuthnInstant	Date de la requête
Assertion > AuthnStatement	SessionIndex	Identifiant de la session de l'ENT
Assertion > AuthnStatement > SubjectLocality	Address	IP de l'utilisateur authentifié par l'ENT
Assertion > AuthnStatement	AuthnContext	Contexte d'authentification sur l'ENT
Assertion > AttributeStatement > Attribute	FriendlyName	l'idEnt et le GARPersonIdentifiant sont obligatoires
Assertion > AttributeStatement > Attribute	Name	l'idEnt et le GARPersonIdentifiant sont obligatoires
Assertion > AttributeStatement > Attribute	AttributeValue	Valeur de l'idEnt ou GARPersonIdentifiant connu du GAR

Tableau 7 : Description de la Auth Response

2.2.2.5 Logout Request front SSO des IHMs

Exemple

```
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                      Destination="https://sso-
portail.gar.education.fr/login?logoutendpoint=true"
                      ID="_fa22fee6ad824df70d0c042df9d99302"
                      IssueInstant="2021-08-05T08:43:49.194Z"
                      Version="2.0"
                      >
    <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://entzen.gar.renater.fr/
idp/shibboleth</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="#_fa22fee6ad824df70d0c042df9d99302">
                <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/xmlenc#sha512" />

<ds:DigestValue>GcLcPJm5rfFW+tXD+YnQ+7ipD5t90vgrgWwvDitS10KalSj+NDs8eSoKjrv4K3dfk
6VvM1Zh5mxs
9dY/D+XUAg==</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
PeSBFZ6iDcbSq1FDwk0Tp8Yfwnk5FiNTkkmsWWiUYfMbOUKCdeB6YgsW9NcinGe86QJRFcCDyg71
AYpCRMsC6BktDwCq5Wnct+wWQbfBx4lUbyQzmA02YZaxFVJpPYTaRBZFoSZWjAc5XJIIzHtyThVw
evIWcStEthrr2gn03B1VM2B0C9zLVotwmn4qcUCXFZ/uKMys6ZuIgpQHBcXmSxFo+kmXzn/61VXP
Rrg0baNEKWC2IT6GWEJ0Y2gv6eQqqXOYZuqV+onbpdaz3guzsnxf8IL0nzNbrdAXzarF1Qvn9ynC
aPa0oFgq1d8q7OwbP1Gl5W9hkw/mFfUW0p+1Cg==
</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIDkTCCAnmgAwIBAgIUAzthS2zGnC85lbbXs6xMp0/J+ZYwDQYJKoZIhvcNA
QELBQAwNDEyMDAG
A1UEAwwpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIwHhcNMTcwMzEz
MTcxMjAyWhcNMzcwMzEzMTcxMjAyWjA0MTIwMAYDVQQDDClzaW11bGVudC52YWxpZGF0aW9uLnRl
c3QtZ2FyLmVkdWNhdGlvbi5mcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ5OFEBy
6evANBTJtm1/u2ODSpYSy0YXpflUz0C2TFiRJ1nD0Zasf2onBAUECV5lsFwH61kRBIROXqaHDscf
ywi+uFcaTkP+v1urvfPnSZR0DH2Iq6fEoCofbnOFPc5T3PfGBDbIhyYEBiP4WyAmx1t7BVbYJitz
s2XxoFhMOlh8+E55u0genTxiVGIwjBj+t1MEY+m70DQY9LLuHxAKWV7K7cwgzsiPtM939wngpuCp
2JOovzCqOF/a5HPrXSffk0JZZe/gEpRxEg/7aJJTDFykHSr4eH7ATUnKZQBWzbStEtY3mW7fh6/T
sLbjN45XUcy062ib6hvMN1E1WC6WZSUCAwEAAaOBmjCBlzAdBgNVHQ4EFgQUemjLva9FWiCumd3R
YJJ4AaJYkZgwdgYDVR0RBG8wbYIpc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRp
b24uZnKGQGh0dHBzOi8vc2ltdWxlbnQudmFsaWRhdGlvbi50ZXN0LWdhci5lZHVjYXRpb24uZnIv
aWRwL3NoaWJib2xldGgwDQYJKoZIhvcNAQELBQADggEBAC3VtuUoYYNnxXP02HX6UaXIaeJ7ZLWA
wTdwW28uy5sKG7sDSh83rGNEPNhhRNvfBPi49S9UNrdmz99IDwswvXslZK6yARfG2ZLErrczfmmg
CQIpkwzH+ySYf1ODG/Q+WF4CTw3jX5yXkVbwS//9qNhYhII0IBFyppDfcLqv/BGekonfrV3Bor94
QlpdxSkY7Yy42whqWb698c7qnWX5IOBHbWCBfi4mFs051Bg+JRN15GjOeWoX93sjnJtw8oFReCVd
RIPcW9Gg6LE99Tk2GvPtU/wfscMT+Wj+3wpwigBpeWbpN5nXUIzqGs+grVT+uBQX8ZCdayyAwFaC
zJPZdtg=</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
```

```
    </ds:Signature>
    <saml2:EncryptedID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                            Id="_e9179bcc2aa6297a690e4eb3095516ae"
                            Type="http://www.w3.org/2001/04/xmlenc#Element"
                            >
            <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
                                   />
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                   Id="_e5f6bf88626ef97ead729724921d1da8"
                                   Recipient="urn:gar:ihmAffectation:seclin"
                                   >
                    <xenc:EncryptionMethod
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"
                                              >
                        <ds:DigestMethod
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
                                             />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:X509Data>

<ds:X509Certificate>MIIDPjCCAiYCCQCQPJzNuh7k1zANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGE
wJGUjENMAsGA1UE
CAwETm9yZDEPMA0GA1UEBwwGU2VjbGluMQ0wCwYDVQQKDARBVE9TMRIwEAYDVQQLDAlXb3JsZGxp
bmUxDzANBgNVBAMMBmFwb2xsbzAeFw0xNzA4MDkwODMxNDRaFw0xODA4MDkwODMxNDRaMGExCzAJ
BgNVBAYTAkZSMQ0wCwYDVQQIDAROb3JkMQ8wDQYDVQQHDAZTZWNsaW4xDTALBgNVBAoMBEFUT1Mx
EjAQBgNVBAsMCVdvcmxkbGluZTEPMA0GA1UEAwwGYXBvbGxvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAv0tolhk6KlRWaIxsUc2Nv+OE2qLIGB4Z/jtailLvEqVQvNyP26kX7yoN9/hM
zMP0cqsQOmUgtodhReYZ5ZzVt30OuGkWl1GKUMXktVAq8BYWGzJkw+pJyKy5YZjkKmxf1iaRXBIF
mHG1QuMkpYAjMPyOWdHUSsfKauUUTo/lHGyoUhO7XR9jqT5mGt2iyvJHfjZ1pFHyKk/RcEBYezLM
0xJ2JU16j3OgjcshZH5PJF+eihyfzTYwT3K5EW6nA929zLikOGA0jx32CIbGS/r6P/1rU2AMS6YO
ooxjnQKdA85cPgiIB206soEX9V5p8GELNey/DR5s4Y5tklBaozgRlQIDAQABMA0GCSqGSIb3DQEB
BQUAA4IBAQAfACKI9CPNCFKKV1eca9iwtqxF461GKpc5TUL5Wtd4IdwvopeQHgQYyGHom65vX3N+
QHkPorKKUffmaOiiXWNESQBgDxhVfn/GSrw0cSDK9qK/gLoCHC0flT9fYP94F4mAdfgK8AoV7smr
xcWfhCA6tKSp3A5BdBPWIpNg4ghbK586Us7H55uwwhsS9HE/hLHnn74NjuqV83pTLtaG1X0YZmuy
hvDmX/n4AHVefApDIA7cWImQ7djQFtM9ZggZvga8D5t0hLcy6K/P1bcNXRgkARTZ/OQ9gfjLmrNh
1MXEZNbijgl0fa82Q7SVlNQUVfQ41KcejRZaC5ipBEB91gjl</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                    <xenc:CipherData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
```

```
<xenc:CipherValue>W0n1m4+0kE7Ka+isXmoukip95ZBM+D0zdbrumvSD4yUAENS8FCRYkv2L+jXDQey
BcLz94QhEd5fo
83DaXX4robf85x9kT0DnKSbpvX02Ix0elEzw+/LUhfRlELCtkBXYJxZzTQb67QMxXzRFlxyjCyz2
1ydD7kGM/dcMRaSP5XPAo8ihLlmwcZm2YfeUqfwLi96GGyDFEjn5varyqv6GY+KWrlilbycIUQ9p
UY7O6XVtLWMXcZ9WPeeWbuZ1AvpNoNckWanW0eL8yZNnfYgb+j9bdzldgDLJkO9KVO9qCN9wUyCG
+v0Q0pAsJ3VTHEsI79OIncmRZU6N91jRYz2jig==</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedKey>
            </ds:KeyInfo>
            <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

<xenc:CipherValue>SaBB7FocY5s7nke8qRAkjDae1o0/dgeCtShCT3dPACsJmUH5JrUKxMxmI4s+cK3
4XrJ3DeD1nF0j
MoSQ7usKl1RXU9Q8ainrYgnyOUK02Abc61+qelswiX6CF1S59fKQTpBeGxT1K/xoWMbGmB7e/6gn
Y4mswXis2VnH/209RvfaKyaLHhjy02jQKV7vMPI6yhxbSRV/aiV207VHtUJdZf6u87ahFysqmBvA
EhHZTA6rf/141SGgvQF+LXKYl4eyLDC1y/ud4eaGMqAUcNs64y0xGjLoBVA2ftVvu8doPJpXIVXV
sHj/1ZSfFozdptDHi1SiqTRQR273/2giOrcZBkH+K9EQ4h8/5WcIsofhZU0IKLcCJfY9/CejdOcA
JIFnxuhG6Bz8c/eFjOYodhyE/JhoCR7tXuSSLZW1NdKrjvHoA/dA0IeGg2z9Frz28bVQcqELu7W8
unUTRkKn2Fv/9aNIlQsD2jMA+gf4S3GCL2u7W5M2MKYt0dCjAI7CN48S8Cx2D/jPhDL51Xcfo9xl
6+Afll6uYCvwG6fguZ5zsGcGQqt+TQTeG7WMKl3pL5I5</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml2:EncryptedID>
    <saml2p:SessionIndex>_398b3a8f4135bc7be57e728b6e79cf8d</saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

Description

Balise	Attribut	Description
LogoutRequest	Destination	Adresse du point d'accès auquel 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 de l'ENT
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

Balise	Attribut	Description
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
LogoutRequest > Subject > NameID	NameQualifier	entytiID de l'ENT
LogoutRequest > Subject > NameID	SPNameQualifier	entytiID du GAR
LogoutRequest > Subject > NameID		Obligatoire. Valeur du nameId correspondant au format/utilisateur
LogoutRequest	SessionIndex	Identifiant de session fournit dans l'Auth Response

Tableau 8 – Description de la Logout Request

2.3. Description SSO en OIDC

Pour les ENT utilisant le protocole OpenId Connect, la demande d'authentification est initiée par le RP (Relying Party).

Les modules *d'accès aux ressources* ou le *SSO des IHMs du GAR* tiennent respectivement le rôle de RP.

Le rôle d'OP (OpenId Provider) vis-à-vis de ces deux services du GAR est tenu par le projet ENT.

Le mode d'échange implémenté est l'authorization code flow sans PKCE.

Pour les deux services, 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 : {URL_Accès_aux_Ressources}/login/{{CODE_ENT}}
- à l'IHM d'affectation via le SSO des IHMs : {URL_SSO}/authenticateoidcent?idEnt={code_ENT}

On notera bien ici que L'ENT doit lui-même forger son URL d'accès aux SSO des IHMs du GAR en renseignant son code ENT en paramètre, afin que le SSO puisse identifier le client à utiliser pour la délégation d'authentification.

L'OIDC s'appuie ensuite sur les métadonnées exposées par l'ENT via le endpoint du *well-known* pour initialiser les échanges techniques entre l'ENT et les SSOs du GAR. A l'issue des échanges, le service du GAR concerné réalise un appel au endpoint */userinfo* mis à disposition par l'OP (ici l'ENT) afin de récupérer les données d'authentification de l'utilisateur (*GPID, idENT*), à des fins d'identification de l'utilisateur dans le GAR.

Les projets ENT qui s'accrochent au GAR doivent mettre préalablement à disposition du GAR les éléments techniques suivants, utilisés pour les services GAR d'accès aux ressources et d'accès à l'interface d'affectation :

Nom du champ	Commentaire	Contenu du champ
ClientID	identifiant du client OIDC du projet ENT	A fournir par l'ENT
secret	"mot de passe" entre l'ENT et le GAR	A fournir par l'ENT

scope	scope des informations autorisées pour le service d'accès aux ressources.	{
		idEnt:<ident>,
		GARPersonIdentifiant:<GPID>
		}

URL de well-known	Cette URL doit être accessible via Internet	A fournir par l'ENT

Tableau 9- Éléments techniques à fournir par les projets ENT utilisant OIDC

2.3.1 Métadonnées ENT

Contrairement au SAML2.0, les métadonnées exposées par l'ENT sont les mêmes pour les deux services du GAR qui délèguent leur authentification.

Les métadonnées OIDC des ENT sont mises en cache par le GAR afin de minimiser le volume d'échanges et de minimiser l'impact d'éventuelles erreurs d'accès. De ce fait, la propagation des mises à jour des ENT au GAR n'est pas instantanée ; les métadonnées sont actualisées et contrôlées deux fois par jour (début de matinée et début d'après-midi).

2.3.1.1 Description

La description détaillée de tous les champs techniques de l'endpoint well-known (metadata) sont présents sur le lien de la documentation §2.1.2.

A noter que, si une URL de déconnexion est fournie par l'ENT dans le well-known, elle ne sera utilisée par le GAR que si l'ENT a demandé l'activation de la propagation de la déconnexion.

2.3.1.2 Exemple

Les metadata en OIDC sont récupérables sur l'endpoint /.well-known sous format json :

Dans le dossier : Protocoles/OIDC.

Fichier : well-known.json

Le well-known expose les informations techniques nécessaires aux échanges à venir et les informations correspondant au mode d'utilisation d'OIDC telles qu'explicitées précédemment :

```
"grant_types_supported":[
      "authorization_code"
   ],
[…]
   "token_endpoint_auth_methods_supported":[
      "client_secret_basic"
   ],
[…]
   "userinfo_endpoint":"url_serveur_oidc/oidcProfile",
[…]
```

En particulier, on y retrouve les informations métier GAR nécessaires suivantes :

```
   "claims_supported":[
      "GARPersonIdentifiant",
      "idEnt"
   ]
```

A noter que les algorithmes d'encryption seront dynamiquement choisis par le RP (les services du GAR) sur la base de la liste des algorithmes supportés communiqués par l'OP (l'ENT). Tous les algorithmes listés dans l'exemple ne sont pas nécessaires pour le bon fonctionnement de l'interconnexion, il s'agit ici de tous ceux embarqués par défaut par une solution implémentant OIDC en particulier.

2.3.2 URL des endpoints pour l'Accès aux ressources en OIDC

Le GAR met à disposition des ENT utilisant protocole OIDC les endpoints suivants pour l'accès aux ressources :

	Plate-forme	Contenu du champ	IP
URL Login	Tests partenaires	https://idp-auth.partenaire.test-gar.education.fr/login/{{CODE_ENT}}	195.221.81.197
	Production	https://idp-auth.gar.education.fr/login/{{CODE_ENT}}	195.221.81.5
URL Logout	Tests partenaires	https://idp-auth.partenaire.test-gar.education.fr/login?client_name={{CODE_ENT}} &logoutendpoint=true	195.221.81.197
	Production	https://idp-auth.gar.education.fr/login?client_name={{CODE_ENT}} &logoutendpoint=true	195.221.81.5

Tableau 10 - URL des endpoints mis à disposition par le GAR pour l'interconnexion en OIDC avec le service d'accès aux ressources

2.3.3 URL des endpoints pour le SSO des IHMs du GAR

Le GAR met à disposition des ENT utilisant protocole OIDC les endpoints suivants pour l'interface d'Affectation :

Nom du champ	Plate-forme	Contenu du champ	IP
URL d'accès au SSO provoquant la demande de délégation d'authentification vers l'ENT	Tests partenaires	https://sso-portail.partenaire.test-gar.education.fr /authenticateoidcent?idEnt={code_ENT}	195.221.81.202
	Production	https://sso-portail.gar.education.fr /authenticateoidcent?idEnt={code_ENT}	195.221.81.10
URL de redirection	Tests partenaires	https://sso-portail.partenaire.test-gar.education.fr/ login/{CODE_ENT}	195.221.81.202
	Production	https://sso-portail.gar.education.fr/login/{CODE_ENT}	195.221.81.10
URL du logout	Tests partenaires	https://sso-portail.partenaire.test-gar.education.fr/logout	195.221.81.202
	Production	https://sso-portail.gar.education.fr/logout	195.221.81.10

Tableau 11– URL des endpoints mis à disposition par le GAR pour l'interconnexion en OIDC avec son SSO des IHMs