



SAML 2 pour le SP

Éléments de fonctionnement d'un SP dans la
Fédération Education Recherche et au-delà.

Sommaire

Une visite guidée

Les métadonnées

La FER

En pratique

Installation

Debug

Visite guidée

Que voit-on !

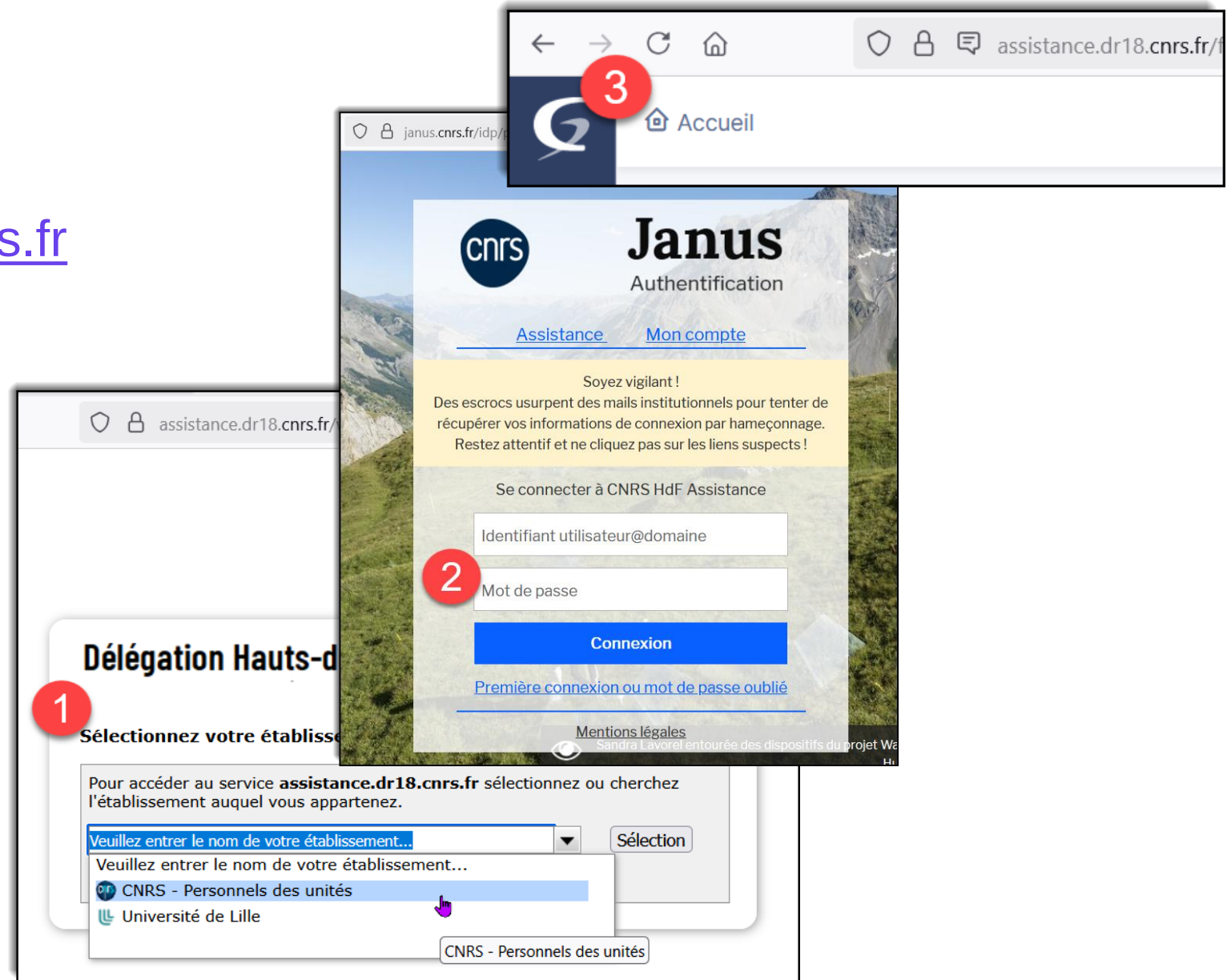
- Navigation vers :
<https://assistance.dr18.cnrs.fr>

1. Sélection IdP
2. Authentification
3. Contenu

- Navigation vers :
<https://aide.core-cloud.net/>

1. Sélection IdP
3. Contenu

- Délégation AuthN
- SSO



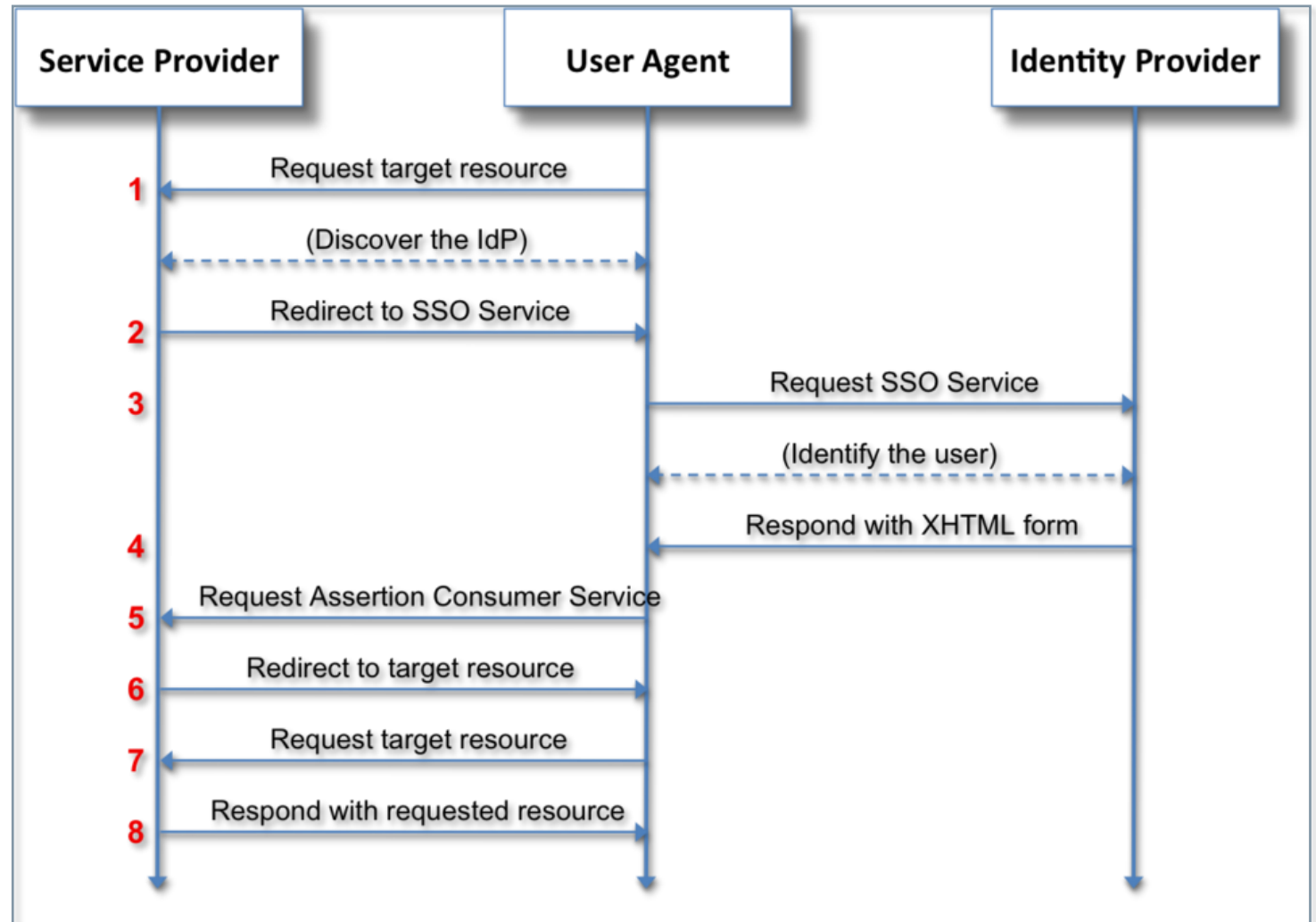
- CC-BY-NC Jean Marie THIA 03 mars 2026

café MIN2RIEN : Fédération Education Recherches

5

Ce qui se passe...

- Protocole SAML 2
- SP initiated Flow



[SAML 2.0 Web Browser SSO \(SP Redirect Bind/ IdP POST Response\)](#)

Oui mais...

- Comment savoir où renvoyer le user-agent ?
- Comment sécuriser les échanges ?
- Comment décrire ce qui est demandé ?
- Comment décrire ce qui est transmis ?
- ...

Les métadonnées

IdP metadata

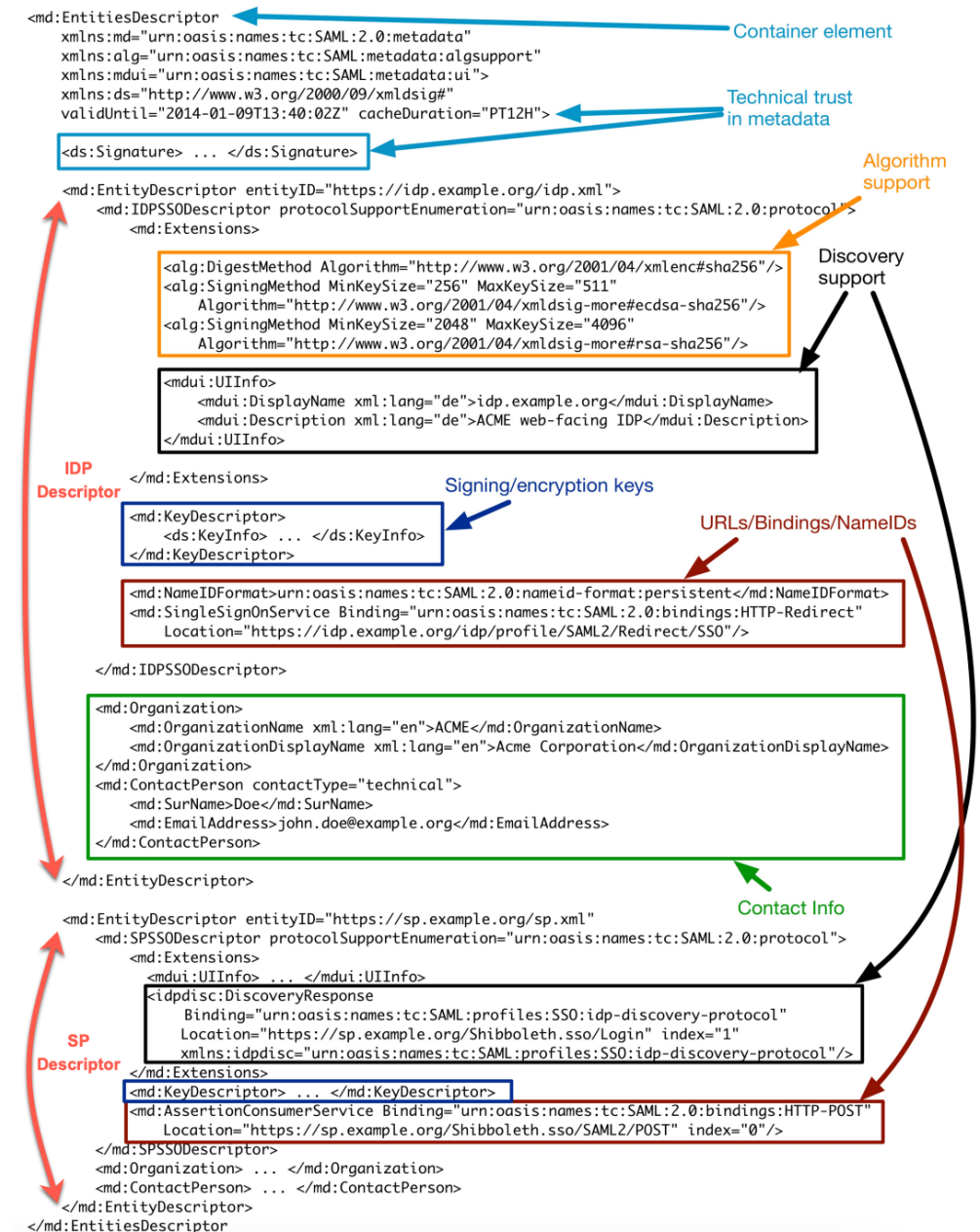
```
<md:EntityDescriptor entityID="http://auth.chu-limoges.fr/adfs/services/trust">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="https://federation.renater.fr/" registrat
      <mdrpi:RegistrationPolicy xml:lang="en">https://services.renater.fr/federation/en/do
    </mdrpi:RegistrationInfo>
    <mdattr:EntityAttributes>
  </md:Extensions>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <shibmd:Scope regexp="false">chu.fr</shibmd:Scope>
      <mdui:UIInfo>
    </md:Extensions>
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <!-- 56:F6:50:4B:C5:6A:3D:90:43:3A:DA:12:16:96:6A:08 -->
          <ds:X509Certificate>MIIC4jCCAcqgAwIBAgIQVvZQS8VqPZBDotoSFpZqCDANBgkqhkiG9w0B
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Loc
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Locatio
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Loc
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Locatio
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Loc
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Locatio
  </md:IDPSSODescriptor>
  <md:Organization>
  <md:ContactPerson contactType="technical">
  <md:ContactPerson contactType="other" remd:contactType="http://refeds.org/metadata/contactTy
</md:EntityDescriptor>
```

SP / Relaying Party metadata

```
<md:EntityDescriptor entityID="http://elgg.test.entrouvert.org/simplesamlphp/module.php/saml/sp/metadata.php/default-sp">
  <md:Extensions>
  <md:SPSSODescriptor SP protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol"
    <md:Extensions>
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
          <ds:X509Data>
            <!-- 93:F2:EC:35:3D:22:3B:5D -->
            <ds:X509Certificate>MIID4zCCAsugAwIBAgIJAJPY7DU9IjtdMA0GCSqGSIb3DQEBAQUAMIGHMQswCQYDVQGEwJGUjEMMAoGA1UECAwDSURGMQ4wDAYD
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:X509Data>
              <!-- 93:F2:EC:35:3D:22:3B:5D -->
              <ds:X509Certificate>MIID4zCCAsugAwIBAgIJAJPY7DU9IjtdMA0GCSqGSIb3DQEBAQUAMIGHMQswCQYDVQGEwJGUjEMMAoGA1UECAwDSURGMQ4wDAYD
              </ds:X509Data>
            </ds:KeyInfo>
          </md:KeyDescriptor>
          <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://elgg.test.entrouvert.org/simplesamlphp/module.php/saml/acs"
          <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" Location="http://elgg.test.entrouvert.org/simplesamlphp/module.php/saml/acs"
          <md:AttributeConsumingService index="0">
            <md:ServiceName xml:lang="fr">Elgg de test</md:ServiceName>
            <md:ServiceDescription xml:lang="fr">Service elgg de test</md:ServiceDescription>
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:0.9.2342.19200300.100.1.3" FriendlyName="cn"
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.16.840.1.113730.3.1.241" FriendlyName="sn"
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.5.4.3" FriendlyName="cn"
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.5.4.4" FriendlyName="sn"
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.5.4.42" FriendlyName="givenName"
          </md:AttributeConsumingService>
        </md:SPSSODescriptor>
        <md:ContactPerson contactType="technical">
          <md:ContactInfo email="mailto:contact@elgg.test.entrouvert.org">
            <md:Name xml:lang="fr">Elgg de test</md:Name>
          </md:ContactInfo>
        </md:ContactPerson>
      </md:EntityDescriptor>
```

Protocole

- SAML 2.0 (Security Assertion ML)
 - XML
 - XML Schema
 - XML Signature
 - XML Encryption
 - Metadata exchange
 - Profile
 - Endpoint
 - Signing, encryption certificates
 - Transport
 - HTTP
- OASIS 2005



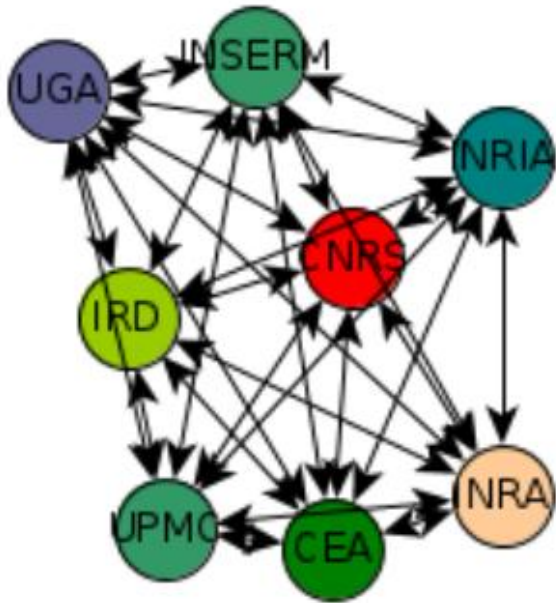
Oui mais...

- Comment échanger facilement avec tous
 - Les IdPs
 - Les SPs
- En France
- En Europe
- Dans le monde

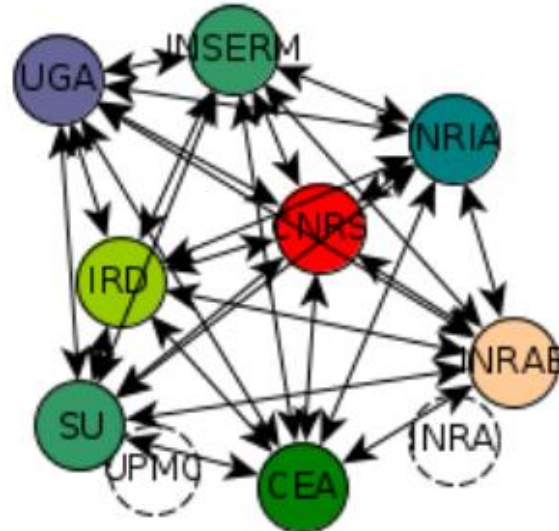
la Fédération Education Recherche

Mettons en commun

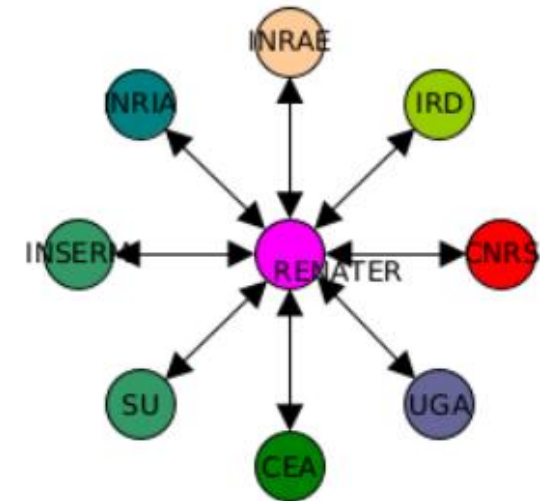
Environnement complexe



Environnement mouvant



Mise en place d'un rôle pivot



[Tutoriel RENATER : tronc commun.pdf](#)

- Service RENATER
- Le cadre de confiance national
- Métadonnées FER
 - Déclaration des IdP
 - Déclaration des SP
- Fédérations
 - Production
 - Test



SERVICES RENATER

Réseau et connectivité ▾ Sécurité ▾ Identité ▾ Collaboration ▾ Mobilité ▾ Documentation ▾

Rechercher

FÉDÉRATION

- Accueil
- A propos de la fédération d'identité ▾
- Rejoindre la Fédération Éducation-Recherche ▾
- Outils à disposition ▾
- Documentation ▾
- Evènements et Formations ▾
- Contact et support ▾

[Click here for the english version](#)

LA FÉDÉRATION ÉDUCATION-RECHERCHE (FER)

Bienvenue sur le site de la Fédération Éducation-Recherche.

[La Fédération Éducation-Recherche](#) met en relation des organismes proposant [des ressources web](#) (applications, portail, etc.) avec d'autres organismes gérant les identités d'utilisateurs accédant à ces ressources, [les fournisseurs d'identité](#).

Via les mécanismes de fédération d'identité, elle permet aux utilisateurs de réduire le nombre de mots de passe à retenir, étend les bénéfices de *Single Sign On* jusqu'à des applications hébergées en dehors de leurs institutions et offre à ces dernières une meilleure maîtrise de la diffusion de données à caractère personnel.

Sur ce site vous découvrirez [les concepts de base et principe de fonctionnement d'une fédération d'identité](#), [ses intérêts et limites](#), ainsi que [des exemples concrets d'utilisation](#).

Un organisme peut rejoindre la Fédération Éducation-Recherche en tant que membre ou partenaire (voir la page [Comment rejoindre la Fédération Éducation-Recherche ?](#)). Son fonctionnement est régie par [deux chartes](#) et par [un cadre technique](#).

[Une fédération de test](#) et [un ensemble d'outils de test](#) permettent de comprendre, tester et valider l'installation et la configuration des principales briques et logiciels de fédération.

Un ensemble de documents (guides d'installation, fiches techniques, recommandations, etc.) est mis à disposition au travers de la rubrique [Documentation](#). [Un glossaire](#) est également disponible et décrit les principaux termes utilisés.

N'hésitez pas au besoin à [contacter les administrateurs de la Fédération Éducation-Recherche](#).

📅 Dernière modification : 2024/04/17 09:37

[S'identifier](#)

 © RENATER 2023 - www.renater.fr

[La Fédération Éducation-Recherche \(FER\)](#)

Le registre



Guichet de la fédération

Fédérations | Attributs | Catégories de service

Liste des fédérations

Afficher entrées

Précédente **1** Suivante

Rechercher :

Affichage de 1 à 6 sur 6 entrées

IDENTIFIANT	NOM	ORGANISME	ACTIONS
https://federation.renater.fr/test/	Fédération de Test	GIP RENATER	
https://federation.renater.fr/	Fédération Education-Recherche	GIP RENATER	
https://federation.renater.fr/edugain/	eduGAIN	GIP RENATER	
https://federation.renater.fr/qualif/	Fédération de qualification	GIP RENATER	
https://federation.renater.fr/partage	Partage	GIP RENATER	
https://federation.renater.fr/proconnect	ProConnect	GIP RENATER	

<https://registry.federation.renater.fr/>



RENATER - Tous droits réservés

Réseau National de télécommunications
pour la Technologie l'Enseignement et la Recherche.



[Aide](#) | [CGU](#) | [Politique de confidentialité](#) | [À propos](#) | [Support](#) | [www.renater.fr](#)

Les métadonnées de la FER

Portail des services RENATER

Vous êtes ici / [La Fédération Éducation-Recherche \(FER\)](#) / [Documentation](#) / [Documentation générale](#) / [Métadonnées SAML](#)

FÉDÉRATION

- [Accueil](#)
- A propos de la fédération d'identité
- Rejoindre la Fédération Éducation-Recherche
- Outils à disposition
- Documentation
- Evènements et Formations
- Contact et support

[Click here for the english version](#)

MÉTADONNÉES SAML

RENATER publie des métadonnées SAML dans le cadre de son infrastructure de fédération d'identité. Ces métadonnées recensent les informations techniques sur les fournisseurs d'identité (IdP) et les fournisseurs de service (SP) renseignées au travers du guichet de la fédération.

Ces métadonnées sont indispensable au fonctionnement d'une fédération d'identité, puisque les entités SAML doivent se connaître mutuellement avant d'échanger le moindre message. L'authentification réciproque, par exemple, nécessite que chacun connaisse le certificat de signature de l'autre. En conséquence, pour pouvoir communiquer avec une autre entité enregistrée dans une fédération d'identité, une entité doit:

- être enregistrée dans cette fédération d'identité, de façon à être présent dans les métadonnées chargées par les autres
- charger les métadonnées de cette même fédération d'identité, de façon à connaître les autres

```
graph TD
    User((User)) -- "déclaration et enregistrement (metadata.xml)" --> Pub[publication des métadonnées]
    Pub -- "chargement des métadonnées" --> SP_a[SP urn:sp:a]
    Pub <--> IdP_a[IdP urn:idp:a]
    Pub <--> IdP_b[IdP urn:idp:b]
    Pub <--> IdP_c[IdP urn:idp:c]
```

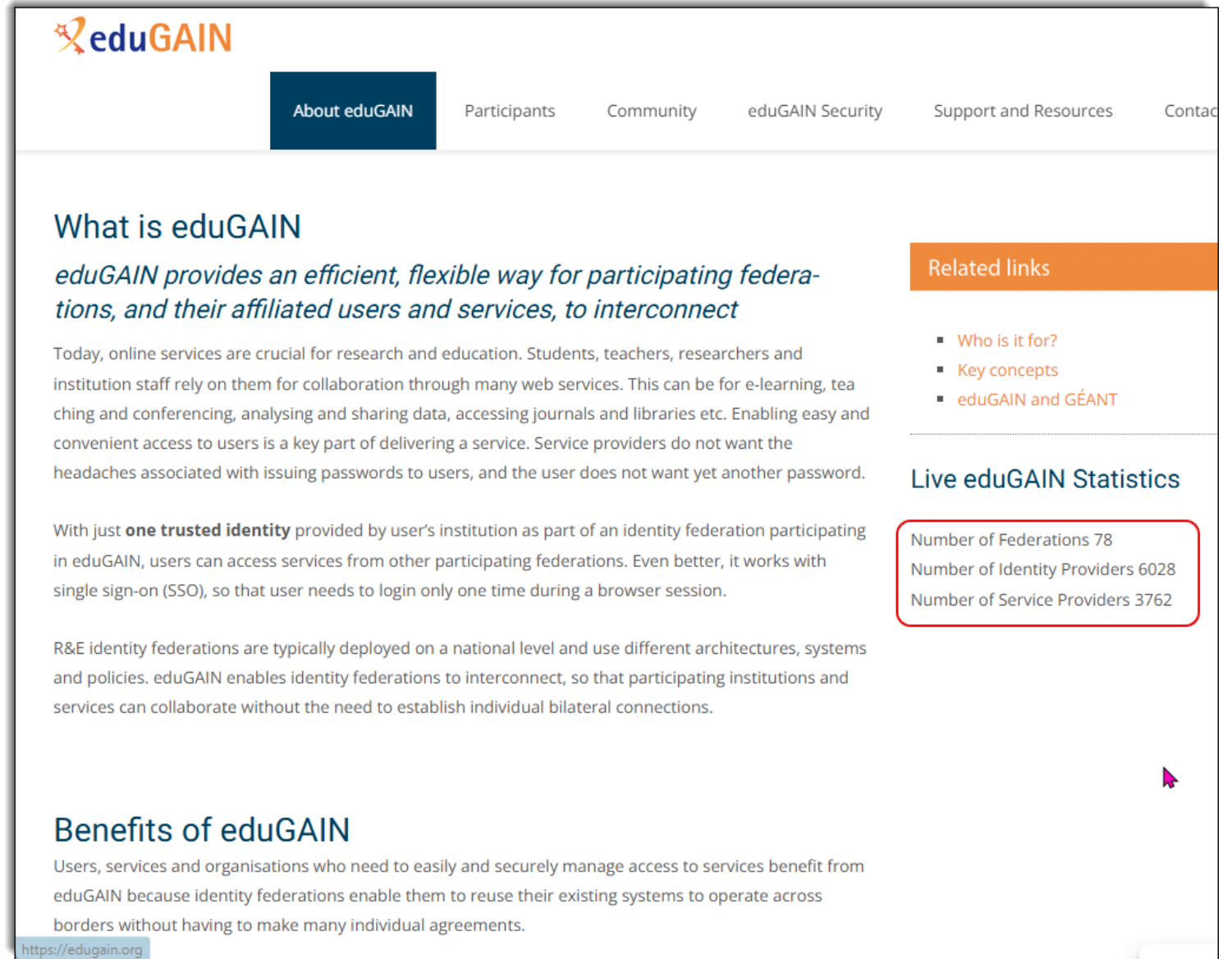
Table des matières

- [Métadonnées SAML](#)
- [Fédérations et métadonnées](#)
- [Mise à jour](#)
- [Intégrité](#)
- [Distribution](#)

<https://services.renater.fr/federation/documentation/generale/metadata/index>
<https://pub.federation.renater.fr/metadata/>

Au delà

- eduGain
 - Méta fédération
 - Service de Géant
 - OptIn depuis la FER
- ProConnect
 - Passerelle OIDC



The screenshot shows the homepage of the eduGAIN website. At the top is the eduGAIN logo and a navigation bar with links: About eduGAIN, Participants, Community, eduGAIN Security, Support and Resources, and Contact. The main content area is titled 'What is eduGAIN' and includes a sub-header: 'eduGAIN provides an efficient, flexible way for participating federations, and their affiliated users and services, to interconnect'. Below this is a paragraph explaining the importance of online services for research and education. To the right, there is a 'Related links' section with links to 'Who is it for?', 'Key concepts', and 'eduGAIN and GÉANT'. Below that is a 'Live eduGAIN Statistics' section with a red border, displaying: 'Number of Federations 78', 'Number of Identity Providers 6028', and 'Number of Service Providers 3762'. At the bottom, there is a 'Benefits of eduGAIN' section. A URL bar at the bottom left shows 'https://edugain.org'.

What is eduGAIN

eduGAIN provides an efficient, flexible way for participating federations, and their affiliated users and services, to interconnect

Today, online services are crucial for research and education. Students, teachers, researchers and institution staff rely on them for collaboration through many web services. This can be for e-learning, teaching and conferencing, analysing and sharing data, accessing journals and libraries etc. Enabling easy and convenient access to users is a key part of delivering a service. Service providers do not want the headaches associated with issuing passwords to users, and the user does not want yet another password.

With just **one trusted identity** provided by user's institution as part of an identity federation participating in eduGAIN, users can access services from other participating federations. Even better, it works with single sign-on (SSO), so that user needs to login only one time during a browser session.

R&E identity federations are typically deployed on a national level and use different architectures, systems and policies. eduGAIN enables identity federations to interconnect, so that participating institutions and services can collaborate without the need to establish individual bilateral connections.

Benefits of eduGAIN

Users, services and organisations who need to easily and securely manage access to services benefit from eduGAIN because identity federations enable them to reuse their existing systems to operate across borders without having to make many individual agreements.

<https://edugain.org>

Related links

- [Who is it for?](#)
- [Key concepts](#)
- [eduGAIN and GÉANT](#)

Live eduGAIN Statistics

Number of Federations 78
Number of Identity Providers 6028
Number of Service Providers 3762

[What is eduGAIN – eduGAIN](#)

Oui mais...

- Il faut faire confiance pour
 - La véracité de l'identifiant
 - La qualité des données

En pratique

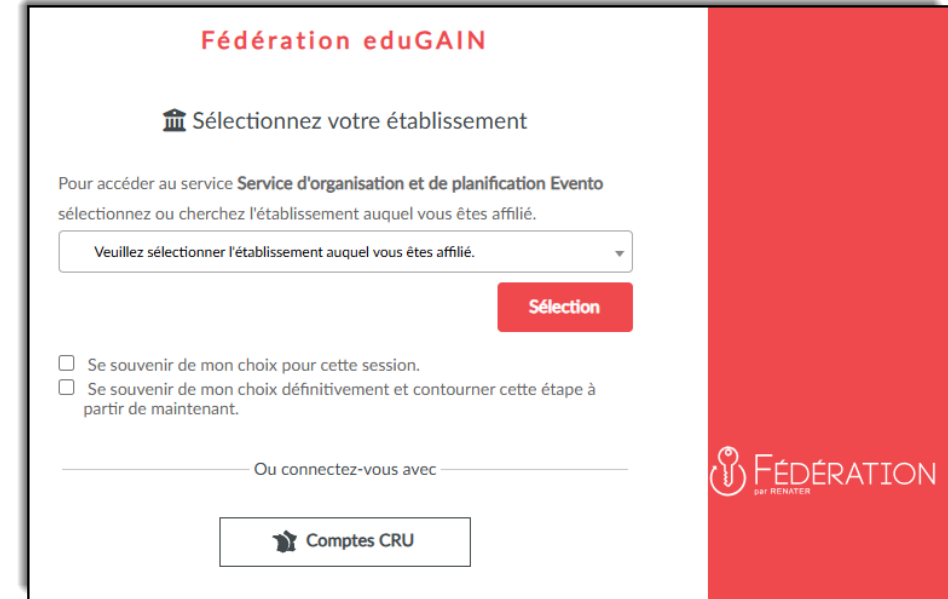
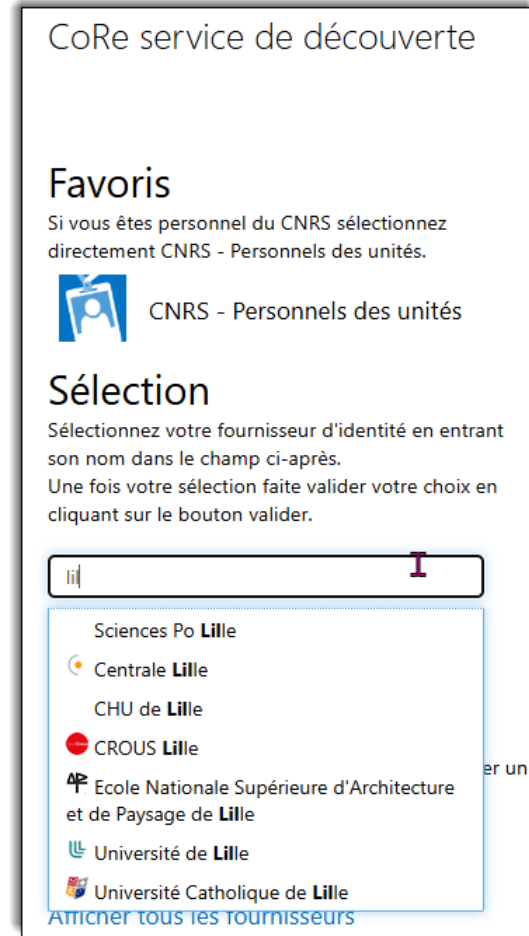
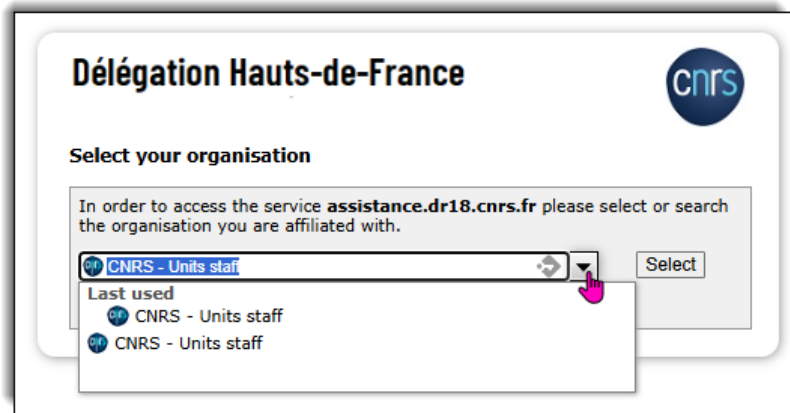
Logiciels

- Shibboleth SP (module Apache + démon)
- LemonLDAP::NG (Perl)
- Keycloak (Java)
- SimpleSAMLPhp (Php)
- AD FS (.Net)
- Auth0
- Etc.

WAYF / RHD / HD

Where Are You From
Realm Home Discovery
Home Discovery

- Vers quel IdP envoyer de la personne ?
 - Domaine du login ?
- Comment filtrer les IdP ?
- Trouver
Adapter le bon logiciel



Métadonnées FER / eduGAIN

- Rechargement régulier
 - Durée de vie limitée
 - Cycle de vie des IdP / SP
 - Cycle de vie des certificats
- Pas toujours natif
 - AS FS
 - SimpleSAMLphp dans Moodle

```
<?xml version='1.0' encoding='UTF-8'>
<md:EntitiesDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
  xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xrd="http://docs.oasis-open.org/ns/xri/xrd-1.0"
  xmlns:pyff="http://pyff.io/NS" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ser="http://eid.europe.eu/metadata/servicelist" xmlns:eidas="http://eid.europe.eu/saml-
  extensions" xmlns:remd="http://refeds.org/metadata" xmlns:renater="https://federation.renater.fr/metadata" Name="https://federation.renater.fr/"
  cacheDuration="PT1H" validUntil="2025-05-28T16:00:02Z" ID="_20250519T160002Z">
  <ds:Signature>
    ...
  </ds:Signature>
  <md:Extensions>
    <mdrpi:PublicationInfo publisher="https://federation.renater.fr/" creationInstant="2025-05-19T16:00:02Z">
      <mdrpi:UsagePolicy xml:lang="en">http://www.edugain.org/policy/metadata-tou_1_0.txt</mdrpi:UsagePolicy>
    </mdrpi:PublicationInfo>
    </md:Extensions>
    <md:EntityDescriptor entityID="http://accesnoto.deboecksuperieur.com">
      <md:Extensions>
        <mdrpi:RegistrationInfo registrationAuthority="https://federation.renater.fr/" registrationInstant="2014-12-09T14:12:55Z">
          <mdrpi:RegistrationPolicy xml:lang="en">https://services.renater.fr/federation/en/documentation/engagement-
            conforme/metadata_registration_practice_statement</mdrpi:RegistrationPolicy>
          </mdrpi:RegistrationInfo>
          <mdattr:EntityAttributes>
            <saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue>https://federation.renater.fr/category/elearning</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="https://federation.renater.fr/member-of" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue>https://federation.renater.fr/</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="urn:oasis:names:tc:SAML:profiles:subject-id:req" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue>none</saml:AttributeValue>
            </saml:Attribute>
          </mdattr:EntityAttributes>
        </md:Extensions>
      </md:EntityDescriptor>
    <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:2.0:protocol">
      <md:Extensions>
        <mdui:UIInfo>
          <mdui:DisplayName xml:lang="fr">De Boeck Supérieur License Desk</mdui:DisplayName>
          <mdui:DisplayName xml:lang="en">De Boeck Supérieur License Desk</mdui:DisplayName>
          <mdui:Description xml:lang="fr">Environnement sur lequel les clients de Noto et NotoBib peuvent utiliser les ressources éducatives de De Boeck
            Supérieur</mdui:Description>
          <mdui:Description xml:lang="en">Environment on which Noto and NotoBib customers can use educational resources of De Boeck
            Supérieur</mdui:Description>
          <mdui:InformationURL xml:lang="fr">http://accesnoto.deboecksuperieur.com</mdui:InformationURL>
        </mdui:UIInfo>
      </md:Extensions>
    </md:SPSSODescriptor>
  </md:KeyDescriptor use="signing">
    <ds:KeyInfo>
      <ds:X509Data>
```

<https://pub.federation.renater.fr/metadata/>

3 Certificats

- Service
 - Accès via le navigateur
 - Certificat Harica
- Signature / Chiffrement
 - Certificat autosigné
 - Généré par
/usr/sbin/shib-keygen
 - Valable en général 10 ans

```
</md:Extensions>
▼<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  ▼<md:Extensions>
    <shibmd:Scope regexp="false">devinci.fr</shibmd:Scope>
    <shibmd:Scope regexp="false">edu.devinci.fr</shibmd:Scope>
    <shibmd:Scope regexp="false">ext.devinci.fr</shibmd:Scope>
    ▼<mdui:UIInfo>
      <mdui:DisplayName xml:lang="fr">Pole de Vinci</mdui:DisplayName>
      <mdui:DisplayName xml:lang="en">Pole de Vinci</mdui:DisplayName>
      <mdui:Description xml:lang="fr">ADFS Pole de Vinci</mdui:Description>
      <mdui:Description xml:lang="en">ADFS Pole de Vinci</mdui:Description>
    </mdui:UIInfo>
  </md:Extensions>
  ▼<md:KeyDescriptor use="signing">
    ▼<ds:KeyInfo>
      ▼<ds:X509Data>
        <!-- 33:4C:E8:D1:BE:5F:7A:BA:48:CA:30:D3:74:25:6E:C5 -->
        <ds:X509Certificate>MIIC2jCCAcKgAwIBAgIQM0zr0b5ferLyjDTdCVuxTANBgkqhkiG9w0BAQsFADApMScwJQYDVQQDEx5BREZTIFNpZ25pbm
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  ▼<md:KeyDescriptor use="encryption">
    ▼<ds:KeyInfo>
      ▼<ds:X509Data>
        <!-- 48:6F:04:5D:84:03:9D:BE:4C:78:91:03:56:CE:71:66 -->
        <ds:X509Certificate>MIIC4DCCAcigAwIBAgIQSG8EXYQDnb5MeJEDVs5xZjANBgkqhkiG9w0BAQsFADAsMSowKAYDVQQDEyFBREZTIEVudY3J5ch
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://adfs.devinci.fr/
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://adfs.devinci.fr/adfs
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://adfs.devinci.fr/
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://adfs.devinci.fr/adfs
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://adfs.devinci.fr/
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://adfs.devinci.fr/adfs
  </md:IDPSSODescriptor>
  ▼<md:Organization>
```

Attribute / Claim

- Le SP demande
- L'IdP peut ne pas répondre a tout
 - Attribut standard
 - Mail
 - Cn,
 - Sn
 - displayname
 - Demander à l'IdP
 - Voir les contacts techniques

```
</ds:Signature>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<saml:Assertion xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75" Version="2.0" IssueInstant
="2014-07-17T01:01:48Z">
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <saml:Subject>
    <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="
urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
      _ce3d2948b4cf20146dee0a0b3dd6f69b6cf86f62d7</saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="2024-01-18T06:21:48Z" Recipient="
http://sp.example.com/demo1/index.php?acs" InResponseTo="
ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" />
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
    <saml:AudienceRestriction>
      <saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z" SessionNotOnOrAfter="
2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:
AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
>
      <saml:AttributeValue xsi:type="xs:string">testuser</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
">
      <saml:AttributeValue xsi:type="xs:string">testuser@example.com</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="eduPersonAffiliation" NameFormat="
urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

[SAML 2.0 Explained in Simple Words - Part II](#)

Attribute / Claim

- Utilisé par l'application
 - AuthZ
 - OU
 - EduPersonAffiliation
 - Présentation
 - Name
 - Mail
 - EPPN
 - Intégration application
 - http header (shib sp)

3

Installation

Shib SP

- Mod-shib pour Apache (Linux, Windows)
 - /etc/shibboleth/shibboleth2.xml, attribute-policy.xml, attribute-filter.xml
- Les tutos / guides
 - Service Provider - Guides - SWITCHaai - SWITCH Help
 - Installation d'un SP Shibboleth et Shibbolisation d'application
- Attributs SAML mis à disposition dans les variables d'environnement du serveur (php = \$_SERVER['mail'])
- Difficultés
 - Transformation des attributs
 - Usage pour authZ

Le fichier Attribute-policy.xml est commenté par défaut

Shib ProxySP

- Guides
 - [Portail des services RENATER] - Utiliser un reverse-proxy SAML en frontal d'un serveur hébergeant une application
- Apache mod-Proxy + Shib SP
- Configuration du WAYF est unique

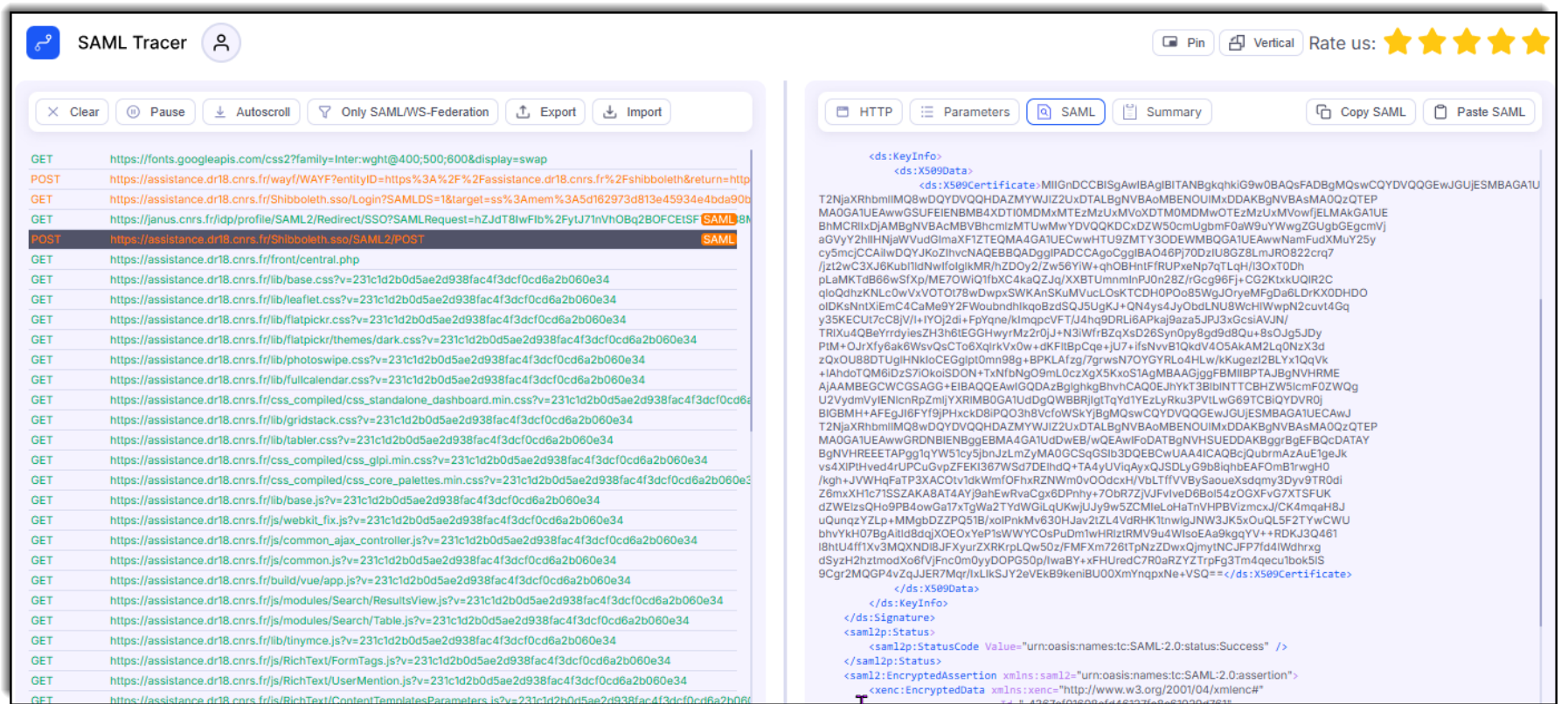
Intégration application web

- Récupérer les variables d'environnement du serveur
 - `php = $_SERVER['mail']`
- Pour affichage (nom, prénom)
- Pour autorisation
 - CoRe
 - Accès rôle dans une unité (tout les du, DU UMR)
 - Moodle
 - Affectation à une cohorte

Debug

SAML Tracer

- Extension Chrome
- Visibilité des échanges SAML



Fiddler

- Proxy http
- Permet de voir les requêtes http / https
 - Entêtes
 - Contenu
- [Web Debugging Proxy and Troubleshooting Tools | Fiddler](#)

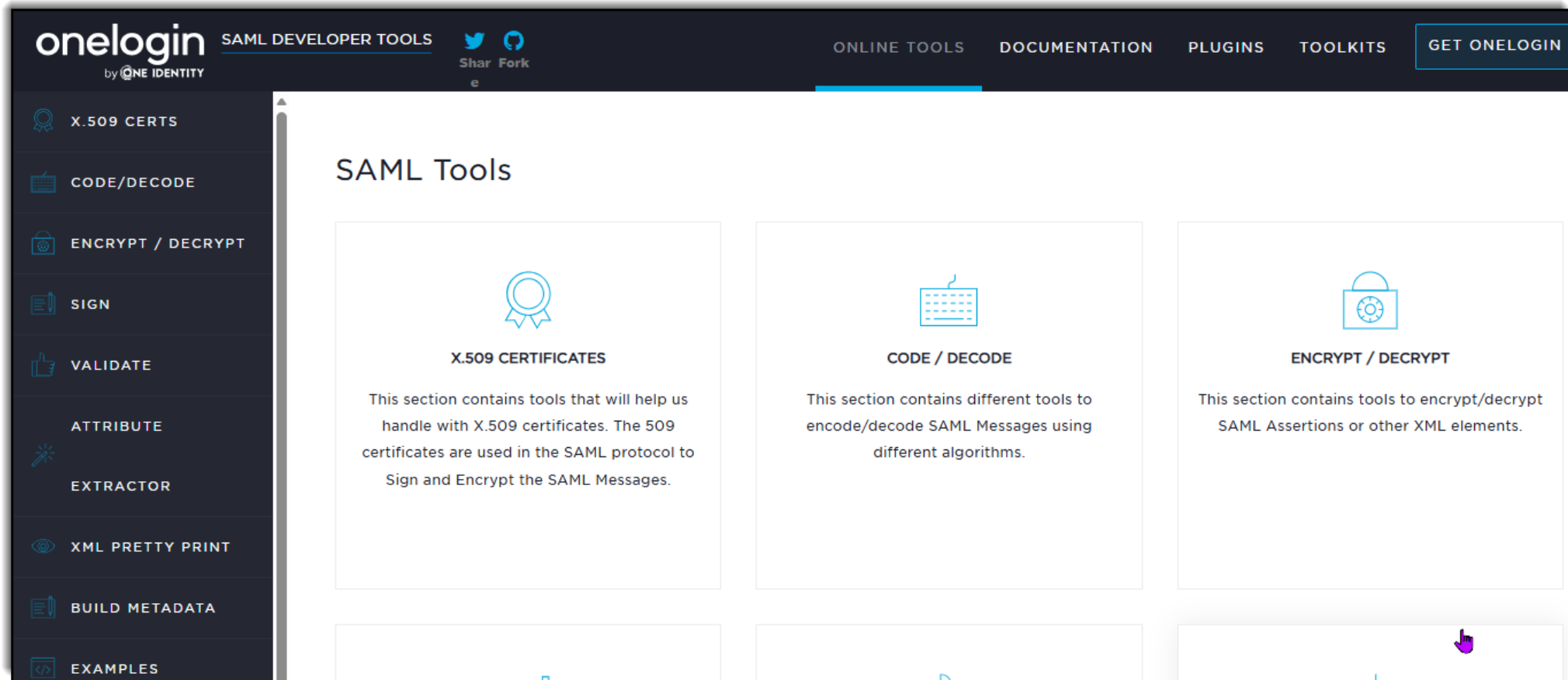
Handler Secure ShibSP

- Affichage des attributs transmis

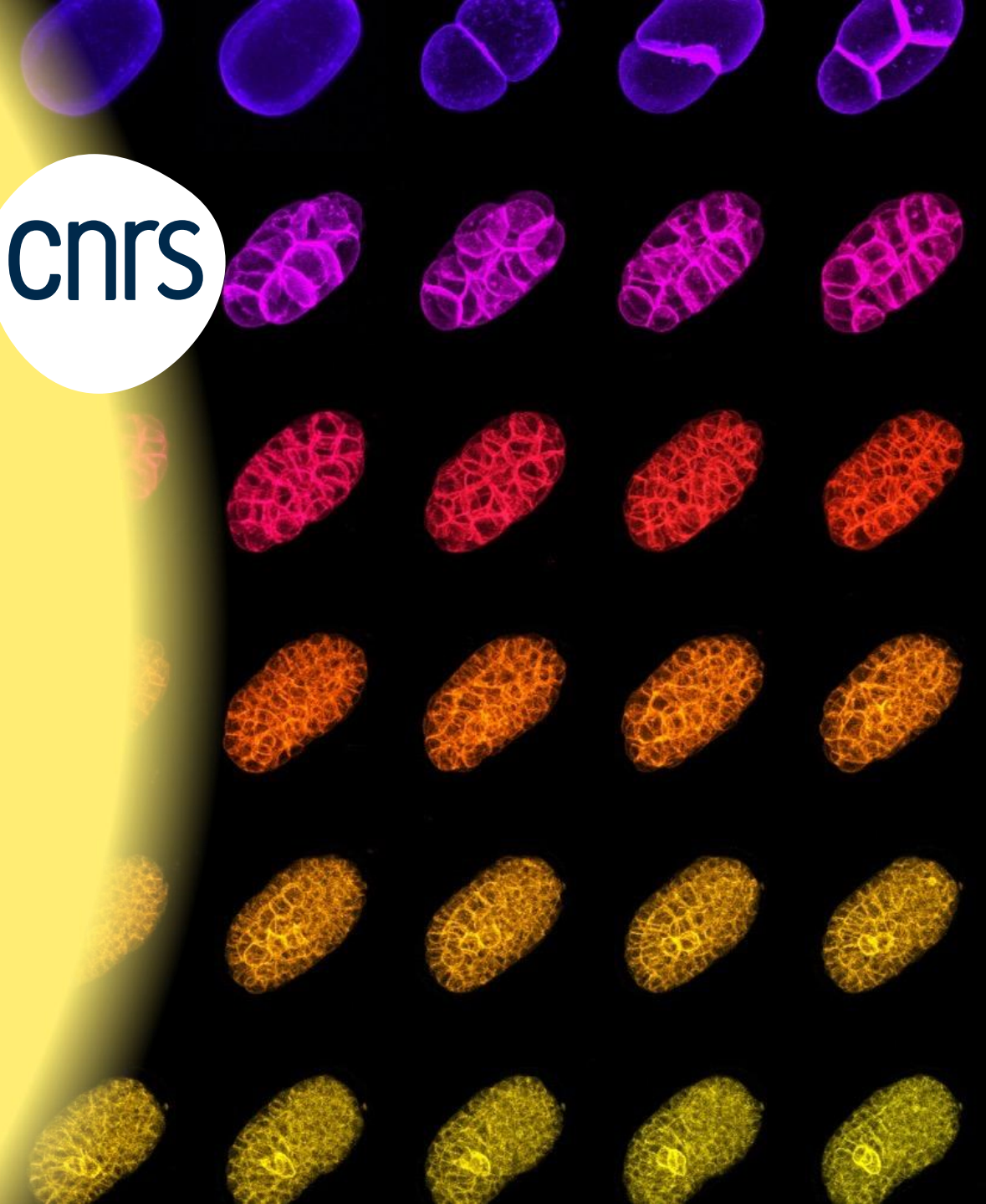
SCRIPT_URL	/secure/
SCRIPT_URI	https://[REDACTED]
Shib-Handler	https://[REDACTED]
Shib-Application-ID	default
Shib-Session-ID	_e636a7cb069e9c1d910d4d3921648527
Shib-Identity-Provider	https://janus.cnrs.fr/idp
Shib-Authentication-Instant	2025-05-19T15:22:10.027Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	_5bccd4fd9c4209025c760f68cf4410f0
Shib-Session-Expires	1747696884
Shib-Session-Inactivity	1747671693
displayName	THIA SONG FAT Jean Marie
eppn	jean.marie.thia.song.fat.2@cnrs.fr
givenName	Jean Marie
mail	jean-marie.thia@cnrs.fr
o	CNRS
ou	MOY1800
sn	THIA SONG FAT
supannEtablissement	{CNRS}MOY1800
unscoped-affiliation	member;employee;staff
HTTPS	on

HTTP_SHIB_COOKIE_NAME	
HTTP_SHIB_SESSION_ID	_e636a7cb069e9c1d910d4d3921648527
HTTP_SHIB_SESSION_INDEX	_5bccd4fd9c4209025c760f68cf4410f0
HTTP_SHIB_SESSION_EXPIRES	1747696884
HTTP_SHIB_SESSION_INACTIVITY	1747671693
HTTP_SHIB_IDENTITY_PROVIDER	https://janus.cnrs.fr/idp
HTTP_SHIB_AUTHENTICATION_METHOD	urn:oasis:names:tc:SAML:2.0:ac:classes:Pass
HTTP_SHIB_AUTHENTICATION_INSTANT	2025-05-19T15:22:10.027Z
HTTP_SHIB_AUTHNCONTEXT_CLASS	urn:oasis:names:tc:SAML:2.0:ac:classes:Pass
HTTP_SHIB_AUTHNCONTEXT_DECL	
HTTP_SHIB_ASSERTION_COUNT	
HTTP_SHIB_HANDLER	https://assistance.dr18.cnrs.fr/Shibboleth.sso
HTTP_TARGETED_ID	
HTTP_PERSISTENT_ID	
HTTP_EPPN	jean.marie.thia.song.fat.2@cnrs.fr
HTTP_AFFILIATION	
HTTP_UNSCOPED_AFFILIATION	member;employee;staff
HTTP_PRIMARY_AFFILIATION	
HTTP_ENTITLEMENT	
HTTP_NICKNAME	
HTTP_PRIMARY_ORGUNIT_DN	
HTTP_ORGUNIT_DN	
HTTP_ORG_DN	
HTTP_SUPANNACTIVITE	
HTTP_SUPANNAUTRETELEPHONE	
HTTP_SUPANNCIVILITE	
HTTP_SUPANNEMPID	
HTTP_SUPANNENTITEAFFECTATION	
HTTP_SUPANNENTITEAFFECTATIONPRINCIPALE	
HTTP_SUPANNETABLISSEMENT	{CNRS}MOY1800
HTTP_SUPANNROLEENTITE	
HTTP_SUPANNROLEGENERIQUE	
HTTP_SUPANNCODEINE	
HTTP_SUPANNETUANNEEINSCRIPTION	
HTTP_SUPANNETUCURSUSANNEE	
HTTP_SUPANNETUDIPLOME	

samltool



[SAML Tools | SAMLTool.com](https://samltool.com)



cnrs

Merci pour votre attention

Des questions ?

→ 02/03/2026

Sources

- [SAML 2.0 Explained in Simple Words - Part I](#)
- [What is SAML and how does SAML Authentication Work | Auth0](#)
- [Security Assertion Markup Language – Wikipedia](#)
- [SAML 2.0 – Wikipedia](#)
- [Download A Guide to Claims-Based Identity and Access Control, Second Edition - Book Download from Official Microsoft Download Center](#)
- [SAML Documentation & Tools - Learn SAML | SAMLTool.com](#)

Références

- [Portail des services RENATER] - La Fédération Éducation-Recherche (FER)
 - <https://services.renater.fr/federation/index>
- SWITCHaai - SWITCH Help
 - <https://help.switch.ch/aai/>
- Spaces – Confluence
 - <https://shibboleth.atlassian.net/wiki/spaces>