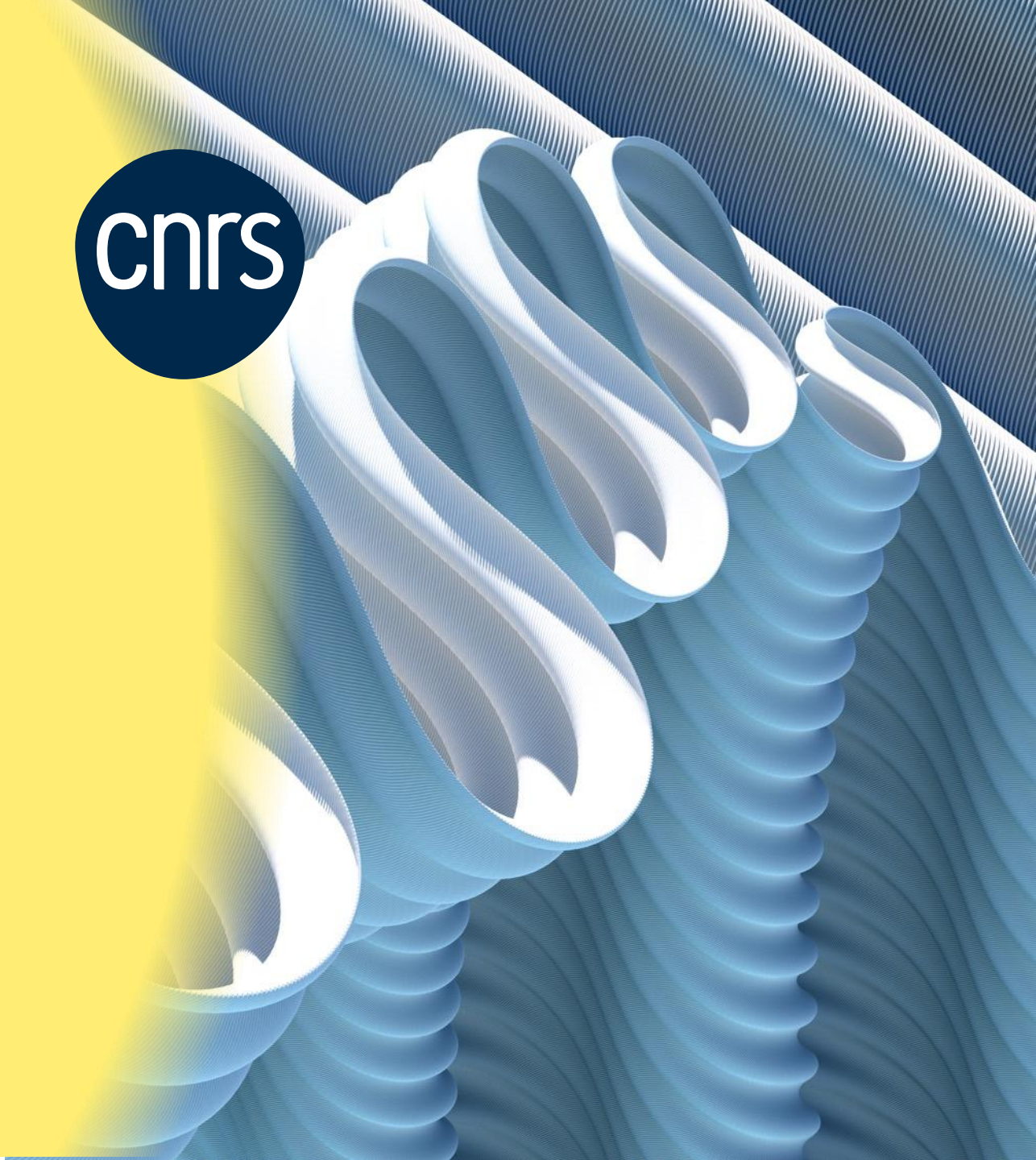
SAML 2
pour le SP

Eléments de fonctionnement d’un SP dans la Fédération Education Recherche et au-delà.



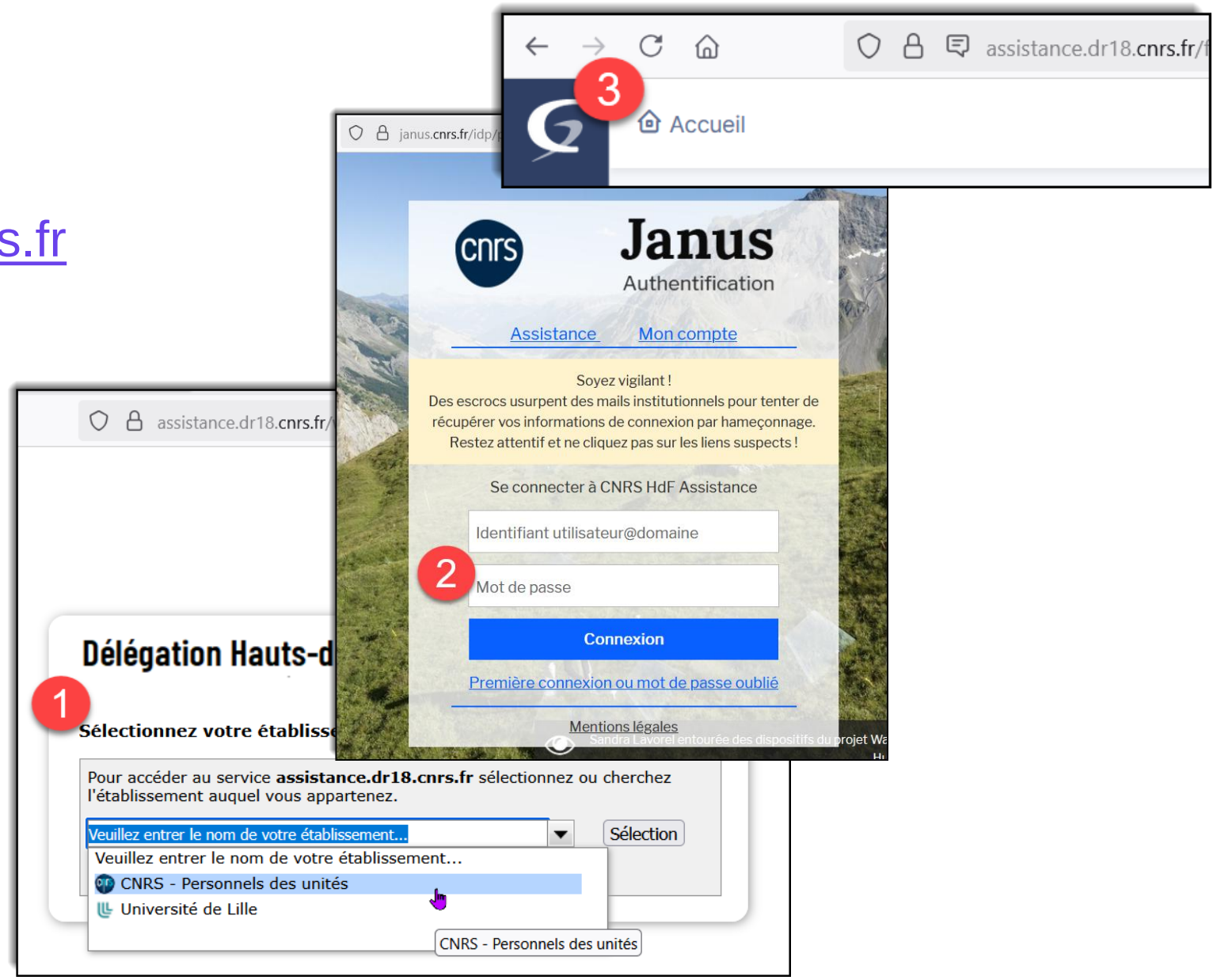
Sommaire

Visite guidée

Que voit-on !

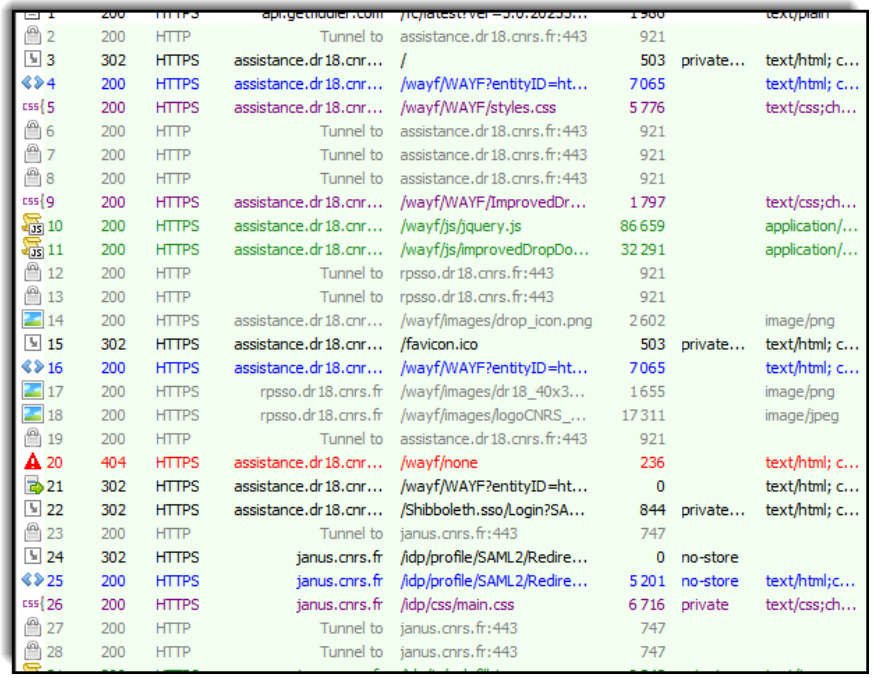
- Navigation vers : Https://assistance.dr18.cnrs.fr
  1. Sélection IdP
  2. Authentification
  3. Contenu
- Navigation vers : https://aide.core-cloud.net/
  1. Sélection IdP
  3. Contenu

- Délégation AuthN
- SSO

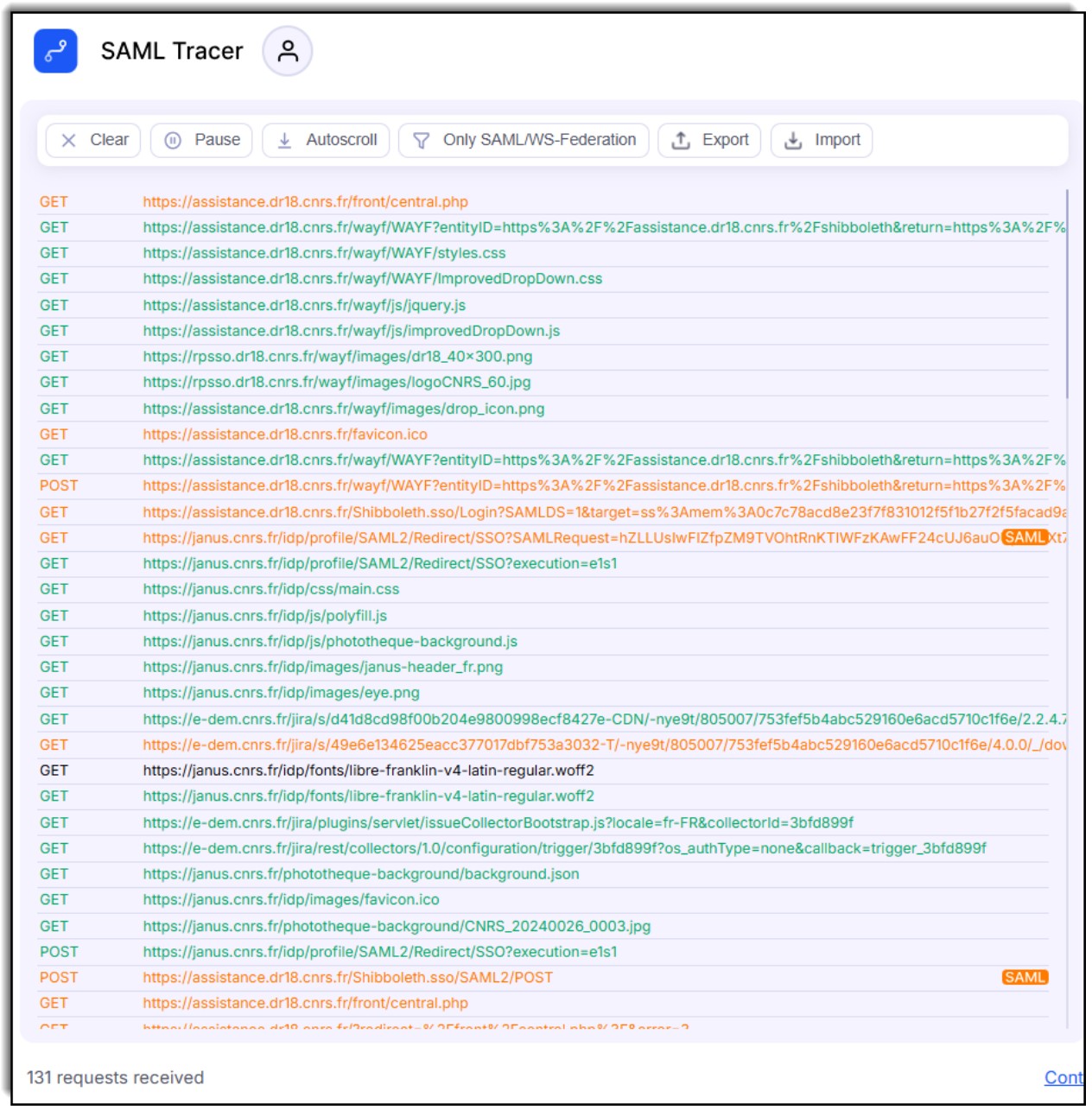


Mais encore

- Le navigateur (UA) est redirigé
  - Pour choisir son IdP
  - Pour authentifier l'utilisateur
  - Et accéder à la ressource s'il y est autorisé

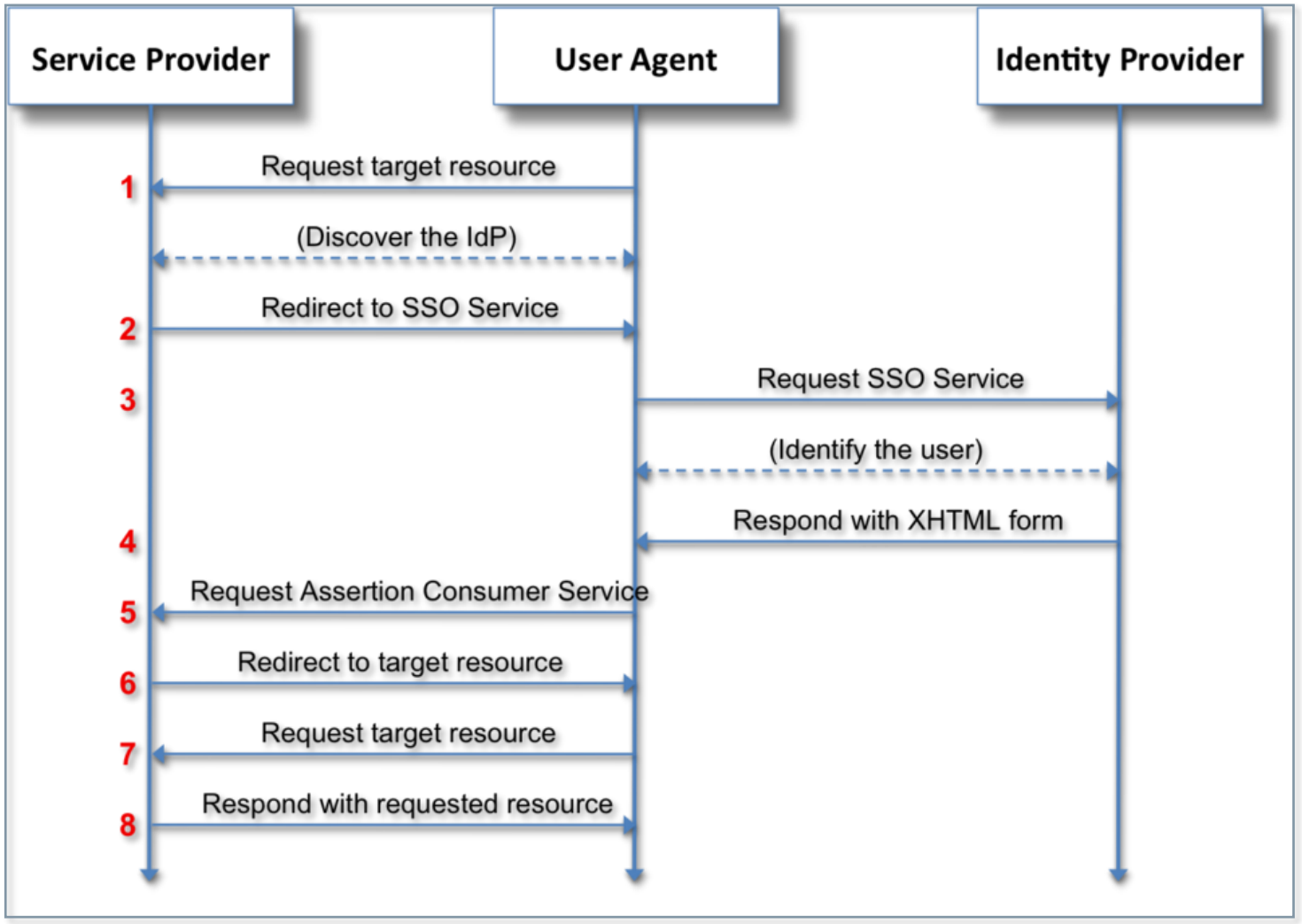


2	200	HTTP	Tunnel to	assistance.dr18.cnrs.fr:443	921		
3	302	HTTPS	assistance.dr18.cnr…	/	503	private…	text/html; c…
4	200	HTTPS	assistance.dr18.cnr…	/wayf/WAYF?entityID=ht…	7 065		text/html; c…
5	200	HTTPS	assistance.dr18.cnr…	/wayf/WAYF/styles.css	5 776		text/css;ch…
6	200	HTTP	Tunnel to	assistance.dr18.cnrs.fr:443	921		
7	200	HTTP	Tunnel to	assistance.dr18.cnrs.fr:443	921		
8	200	HTTP	Tunnel to	assistance.dr18.cnrs.fr:443	921		
9	200	HTTPS	assistance.dr18.cnr…	/wayf/WAYF/ImprovedDr…	1 797		text/css;ch…
10	200	HTTPS	assistance.dr18.cnr…	/wayf/js/jquery.js	86 659		application/…
11	200	HTTPS	assistance.dr18.cnr…	/wayf/js/improvedDropDo…	32 291		application/…
12	200	HTTP	Tunnel to	rpsso.dr18.cnrs.fr:443	921		
13	200	HTTP	Tunnel to	rpsso.dr18.cnrs.fr:443	921		
14	200	HTTPS	assistance.dr18.cnr…	/wayf/images/drop_icon.png	2 602		image/png
15	302	HTTPS	assistance.dr18.cnr…	/favicon.ico	503	private…	text/html; c…
16	200	HTTPS	assistance.dr18.cnr…	/wayf/WAYF?entityID=ht…	7 065		text/html; c…
17	200	HTTPS	rpsso.dr18.cnrs.fr	/wayf/images/dr18_40x3…	1 655		image/png
18	200	HTTPS	rpsso.dr18.cnrs.fr	/wayf/images/logoCNRS_…	17 311		image/jpeg
19	200	HTTP	Tunnel to	assistance.dr18.cnrs.fr:443	921		
20	404	HTTPS	assistance.dr18.cnr…	/wayf/none	236		text/html; c…
21	302	HTTPS	assistance.dr18.cnr…	/wayf/WAYF?entityID=ht…	0		text/html; c…
22	302	HTTPS	assistance.dr18.cnr…	/Shibboleth.sso/Login?SA…	844	private…	text/html; c…
23	200	HTTP	Tunnel to	janus.cnrs.fr:443	747		
24	302	HTTPS	janus.cnrs.fr	/idp/profile/SAML2/Redire…	0	no-store	
25	200	HTTPS	janus.cnrs.fr	/idp/profile/SAML2/Redire…	5 201	no-store	text/html;c…
26	200	HTTPS	janus.cnrs.fr	/idp/css/main.css	6 716	private	text/css;ch…
27	200	HTTP	Tunnel to	janus.cnrs.fr:443	747		
28	200	HTTP	Tunnel to	janus.cnrs.fr:443	747		



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>
```

IdP

signing certificate

endpoint

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 protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:nam
        <md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <!-- 93:F2:EC:35:3D:22:3B:5D -->
                    <ds:X509Certificate>MIID4zCCAsugAwIBAgIJAJPy7DU9IjtdMA0GCSqGSIb3DQEBBQUAMIGHMQswCQYDVQQGEwJGUjEMMAoGA1UECAwDSURGMQ4wDAY
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
            <ds:KeyInfo>
                <ds:X509Data>
                    <!-- 93:F2:EC:35:3D:22:3B:5D -->
                    <ds:X509Certificate>MIID4zCCAsugAwIBAgIJAJPy7DU9IjtdMA0GCSqGSIb3DQEBBQUAMIGHMQswCQYDVQQGEwJGUjEMMAoGA1UECAwDSURGMQ4wDAY
                </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/sim
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" Location="http://elgg.test.entrouvert.org/
        <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" Fr
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-forma e="urn:oid:2.16.840.1.113730.3.1.241" Fr
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format me="urn:oid:2.5.4.3" FriendlyName="cn" re
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.5.4.4" FriendlyName="sn" re
            <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:2.5.4.42" FriendlyName="given
        </md:AttributeConsumingService>
    </md:SPSSODescriptor>
    <md:ContactPerson contactType="technical">
</md:EntityDescriptor>
```

SP

siging certificate

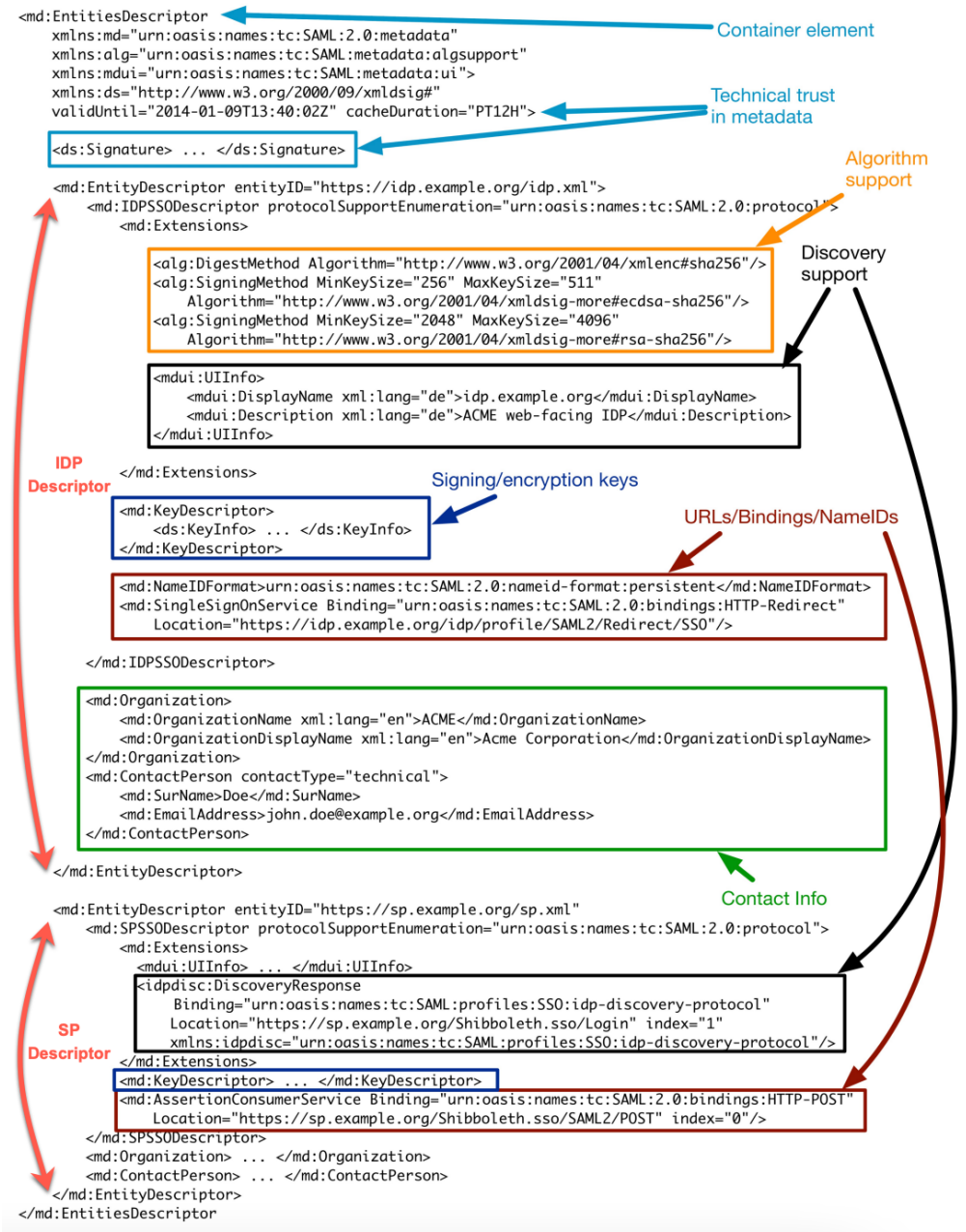
encryption certificate

endpoint

requested attribute

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



SAML 2.0 Explained in Simple Words - Part I

Oui mais…

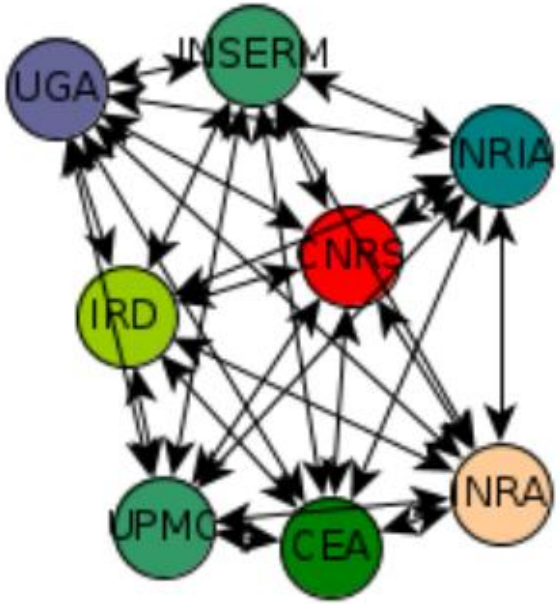
- Comment échanger facilement avec tous
  - Les IdPs
  - Les SPs

  - En France
  - En Europe
  - Dans le monde

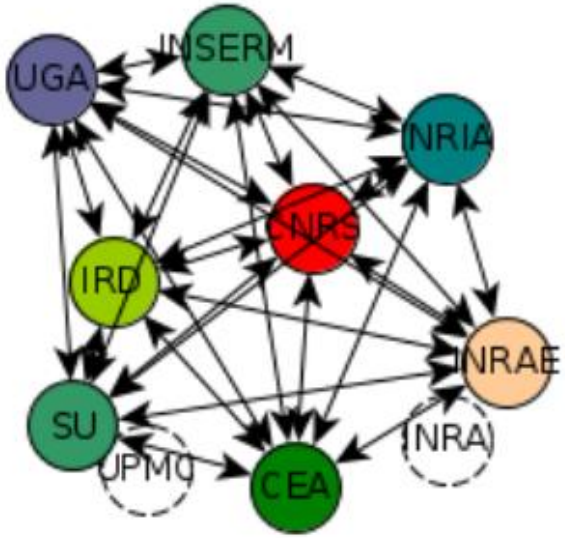
la
Fédéretion
Education
Recherche

Mettons en commun

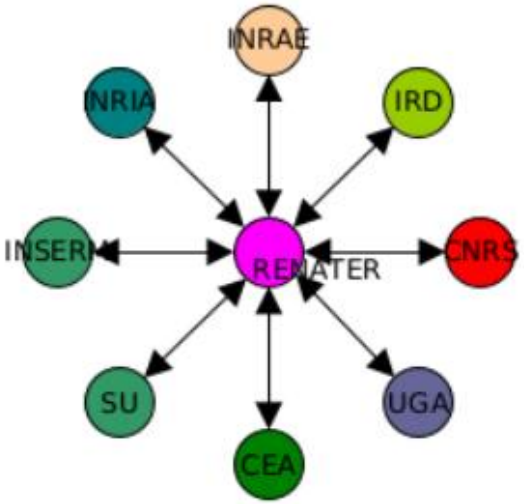
Environnement complexe



Environnement mouvant



Mise en place d'un rôle pivôt



[Tutoriel RENATER : tronc_commun.pdf]

FER

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

La Fédération Éducation-Recherche (FER)

Le registre


FÉDÉRATION
par RENATER
Guichet de la fédération
Fédérations
Attributs
Catégories de service
Liste des fédérations
Afficher 50 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
Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche.
RENATER - Tous droits réservés
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

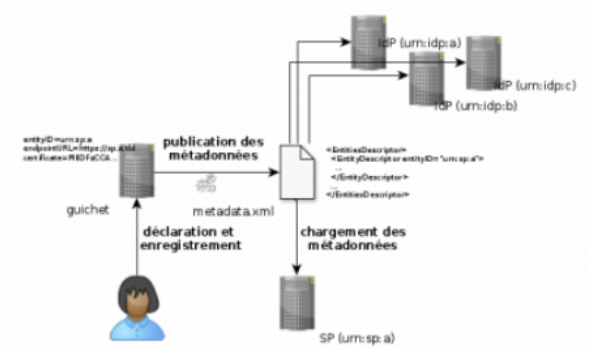
Table des matières
- Métadonnées SAML
  - Fédérations et métadonnées
  - Mise à jour
  - Intégrité
  - Distribution

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 connaitre 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:

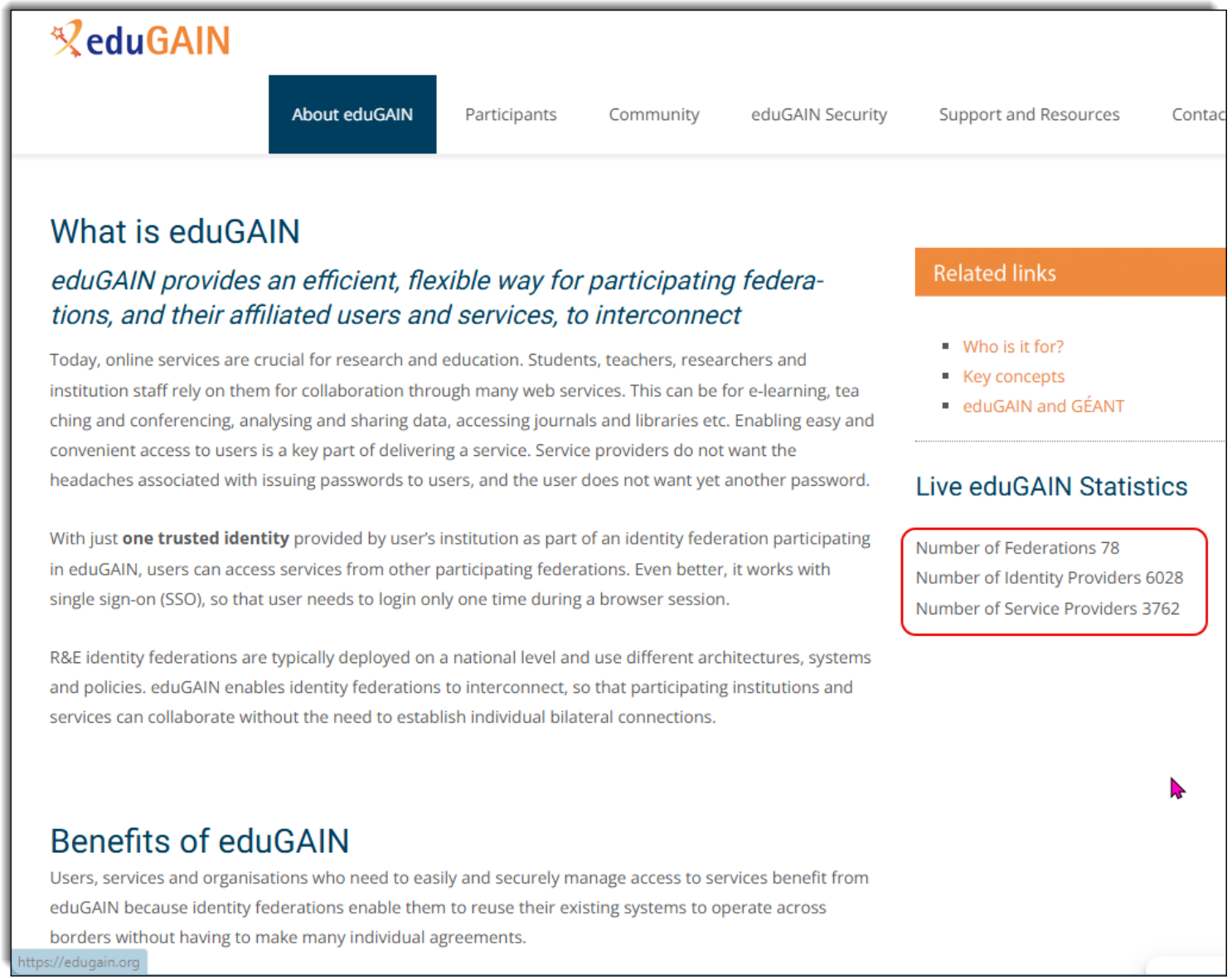
- être enregistrée dans cette fédération d'identité, de façon à être présent dans les métadonnées chargées par les autres
- charger les métadonnées de cette même fédération d'identité, de façon à connaitre les autres



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



What is eduGAIN – eduGAIN

Oui mais...

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

En pratique

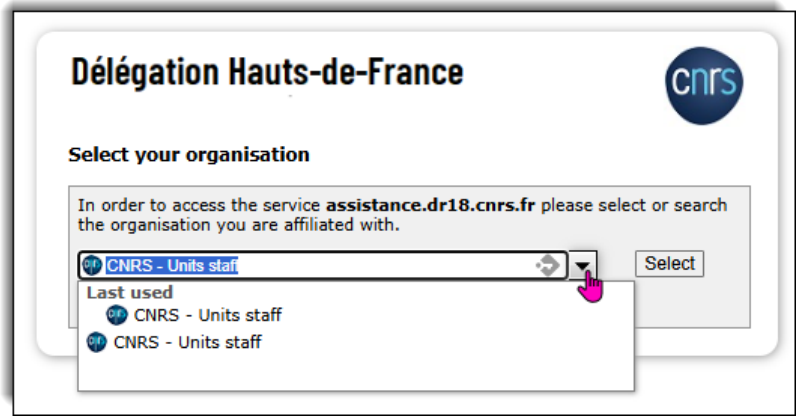
Logiciels

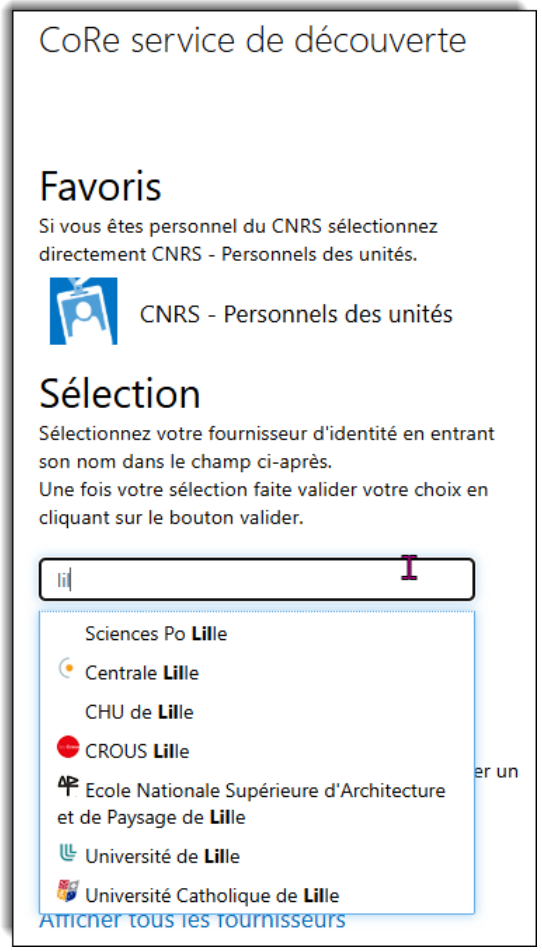
- Shibboleth SP (module Apache + démon)
- LemonLDAP::NG (Perl)
- Keycloak (Java)
- SimpleSAMLPhp (Php)
- AD FS (.Net)
- Auth0
- Etc.

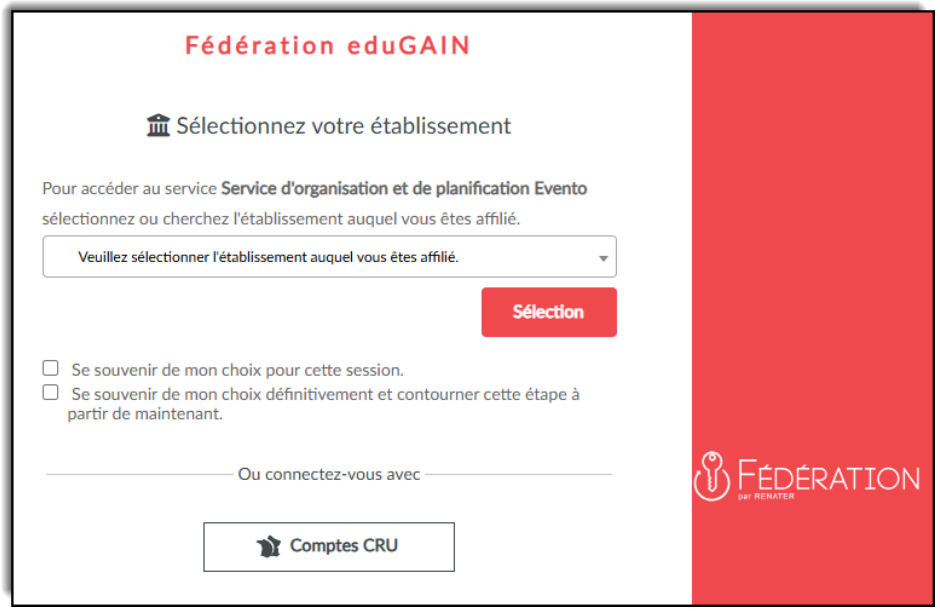
WAYF / RHD / HD

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



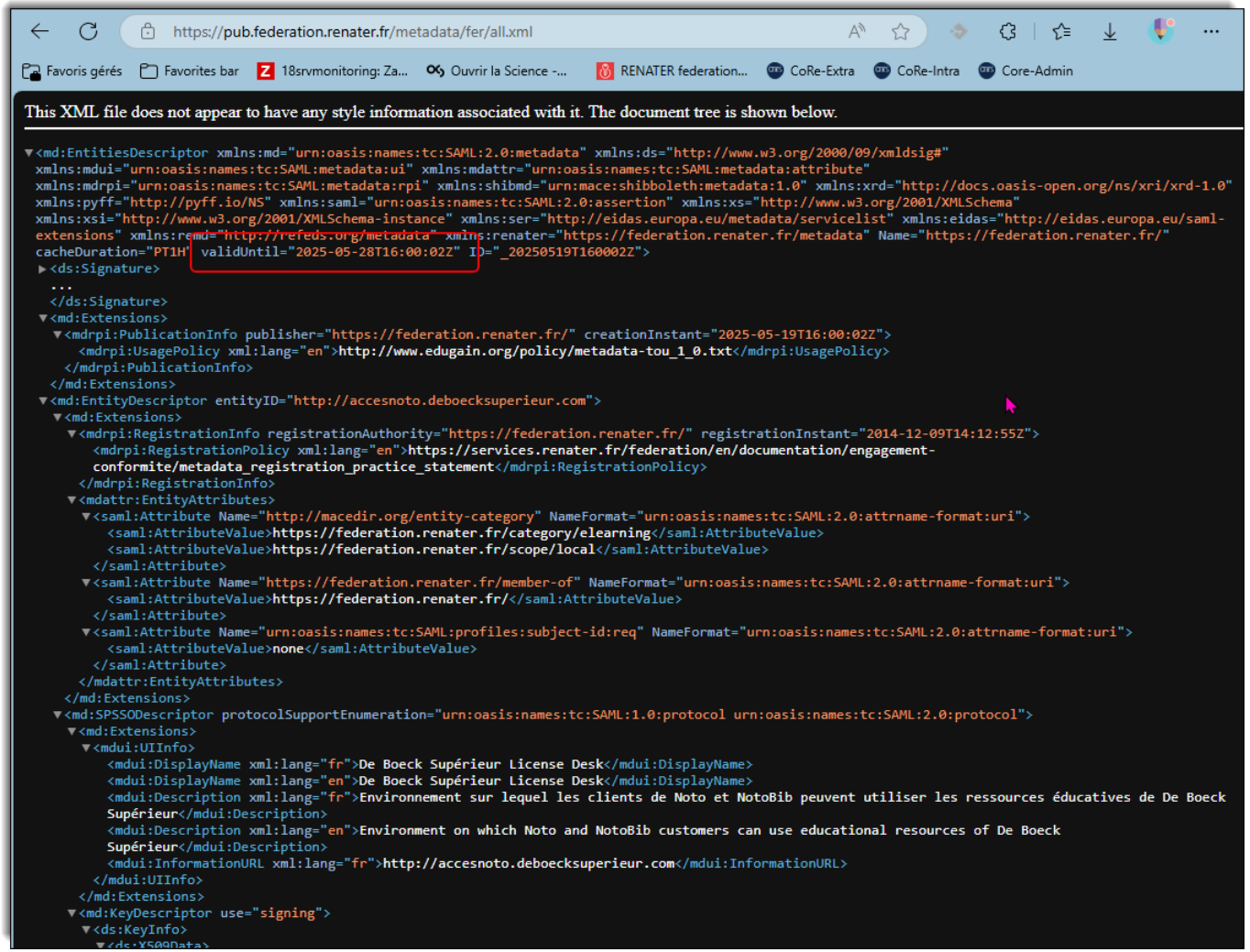




Métadonnées FER / eduGAIN

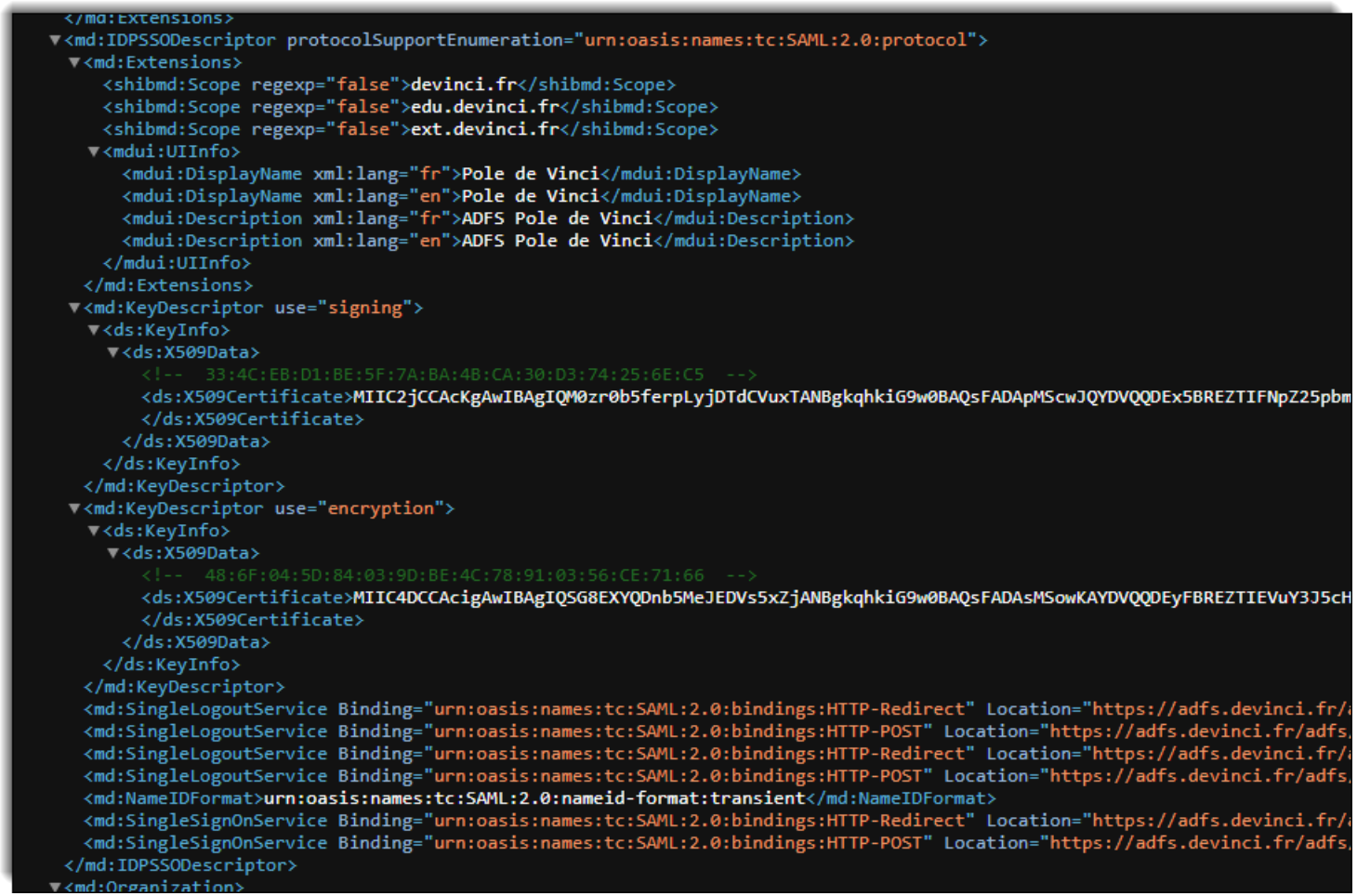
- Rechargement régulier
  - Durée de vie limitée
  - Cycle de vie des IdP / SP
  - Cycle de vie des certificats

- Pas toujours natif
  - AS FS
  - SimpleSAMLphp dans Moodle



3 Certificats

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



Attribute / Claim

- Le SP demande
- L'IdP peut ne pas répondre a tout
  - Attribut standard
    - Mail
    - Cn,
    - Sn
    - displayname
  - Démander 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>
Assertion   <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

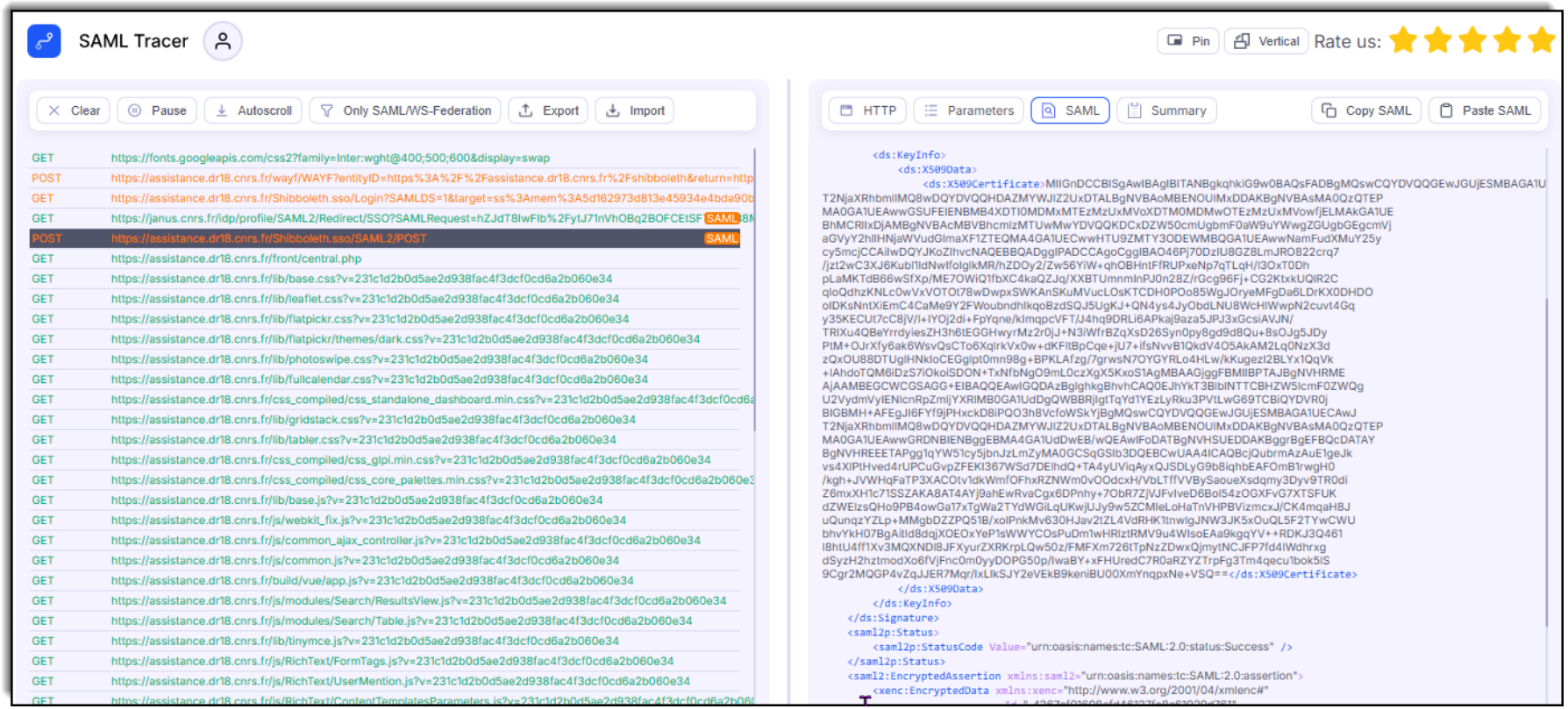
Intégration application web

- 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

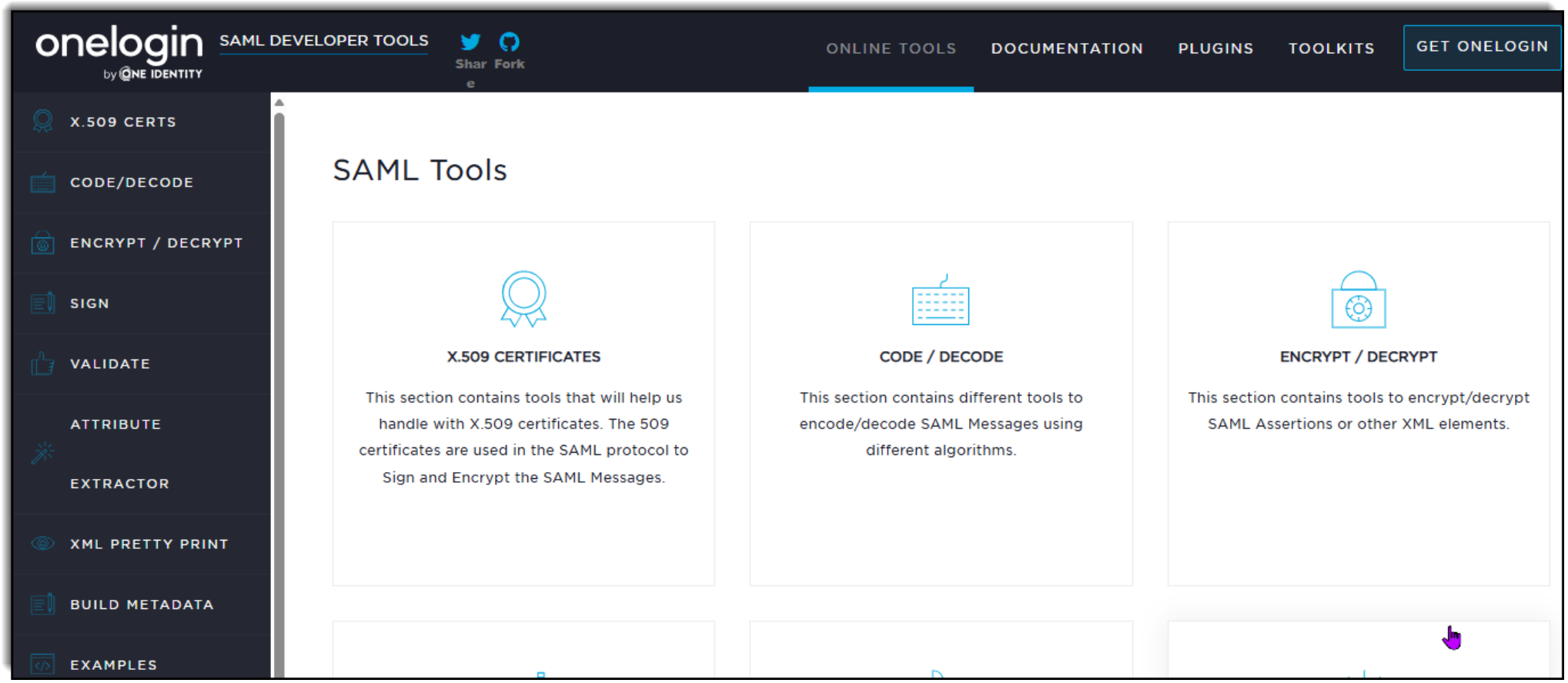
Handler Secure ShibSP

- Affichage des attributs transmis

SCRIPT_URL	/secure/
SCRIPT_URI	https://
Shib-Handler	https://
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	_5bcdd4fd9c4209025c760f68cf4410f0
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	_5bcdd4fd9c4209025c760f68cf4410f0
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

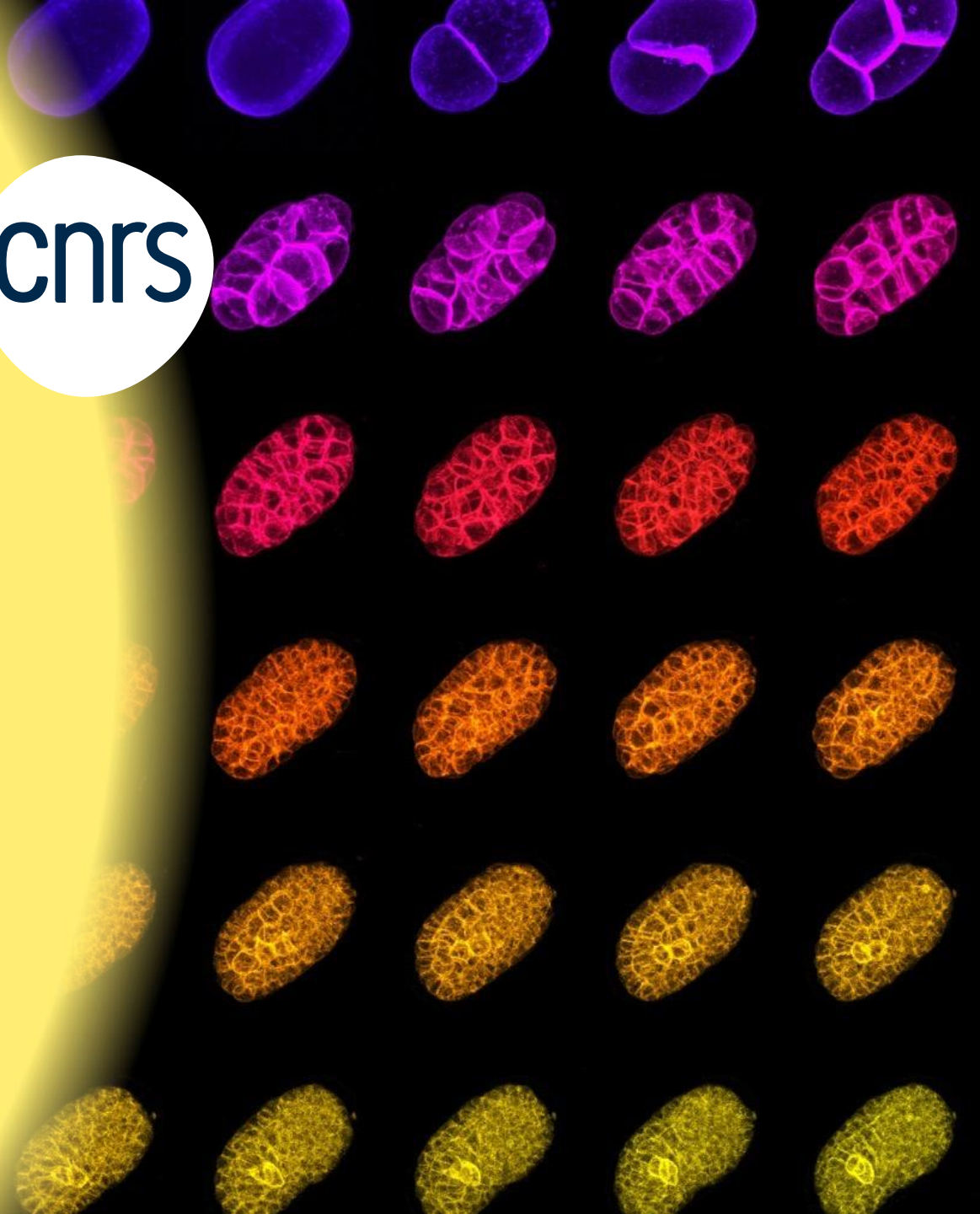


[SAML Tools | SAMLTool.com]

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