DNE-GAR

ERAM – Functional, technical and security reference

Support document for resource providers
ERAM release 7.0 – March 2023

gar.education.fr

Revision history

Date	ERAM Version	Description
23/01/2019	V1.0	Creation of the document
26/05/2020	V4.0	New features and changes to ERAM v4.0 Extension of the scope of ERAM to non-teaching staff Insensitivity to breakage and accents for certain identifiers
05/02/2021	V4.1	Reorganization of the documentation New features and changes to ERAM v4.1 Addition of the title of the resource in the assignment report Addition of a notification in case of activation or deactivation of resources
12/05/2021	V5.1	New features and changes to ERAM v5.1
02/02/2022	V6.0	New features and changes to ERAM v6.0
11/04/2022	V6.1	New features and changes to ERAM v6.1
09/09/2022	V6.1	New features and changes to ScoLOMFR 8.0
23/11/2022	V6.2	New features and changes to ERAM v6.2
20/03/2022	V7.0	New features and changes to ERAM v7.0

Table 1 - Document revision history

Table of contents

Table of illustrations: diagrams and tables

1 Organisation of the documentation

The ERAM technical, functional and security reference documentation for ERAM partners, both resource providers and VLE operators, is organized into two levels and a package of supporting documents and examples:

1.1 General presentation

This document provides existing and future partners with general information on legal aspects, IT security, the main functional and technical points and the support available.

1.2 Technical reference

This document provides comprehensive technical, functional and security information enabling providers to interface their resources with ERAM and ensure ERAM compatibility. The hooking parameters on the ERAM platform are transmitted at the initialization of the hooking phase.

1.3 Support document and examples

The package of support documents and examples is a zip file comprising a set of documents:
- grammar of the identity data archives;
- examples;
- XSD or XML files mentioned in the reference documents listed above;
- the SSO interface contract for resource providers;
- a completed version of the registration file;
- the ERAM contract.

2 Abbreviations and definitions

Assignment manager
ERAM-specific term
Person within an education establishment responsible for assigning digital resources to relevant users (students, teachers or other staff).

Access Token (AT)
The Access Token is a token issued under the OAuth 2.0/OpenID Connect protocols that allows, in the context of the ERAM, a web or native application to access information related to the user for whom it has been generated.
Within the framework of ERAM, it is also possible to obtain an Access Token via the CAS and SAML protocols.

Authorization Code Flow
Access mode proposed by the OAuth 2.0 and OpenId Connect protocols by which a client will obtain an authorization code to be exchanged for tokens.

Public CA
Public certification authority.
A certifying authority is a trusted third party responsible for creating, issuing and managing electronic certificates. Web actors maintain a list of recognized public certification authorities whose certificates are accepted by browsers and other services.

BCN
A Central basis of nomenclatures (*Base centrale des nomenclatures*).
Basis for nomenclatures used by the information system of the ministries responsible for national education, higher education and research.
(http://infocentre.pleiade.education.fr/bcn/).

CAS
Central authentication service.
CAS is a single sign on (SSO) web authentication system developed by Yale University and widely implemented in organizations around the world. The implementation of CAS is monitored by Apereo Foundation (https://www.apereo.org/content/about).

Cipher
Encryption algorithm.

Conformance
ERAM-specific term
A Set of rules that any resource must conform to in order to validate its linkage to ERAM.

CSR
Certificate signing request.
A Certificate Signature Request (CSR for) is a message sent by the requester to a Certifying Authority to request a Digital Identity Certificate.

DCP (PD)
Personal data.

DCR (CDR)
Commercial distributor of resources (*Distributeur commercial de ressources).

ERAM role: managing subscriptions for the resource provider.

DTR (TDR)

Technical distributor of resources (*Distributeur technique de ressources).*

ERAM role: technical responsibility for exploitation of resources for the resource provider.

EIM (PMD)

Personal mobile device

ENT (VLE)

Virtual Learning Environment (*Espace numérique de travail*).

An integrated set of digital services selected and made available to all actors in the education community of one or more schools within a trusted framework defined by a master plan for VLEs (SDET).

FQDN

Full qualified domain name.

An address giving the exact position of a machine within the DNS tree. The FQDN is required to apply for a certificate. It must be built from areas regularly reported in the DNS organization

GAR (ERAM)

Educational Resource Access Manager (*Gestionnaire d'Accès aux Ressources*).

A project initiated by the French Ministry of Education and implemented by RENATER, a public interest group (GIP). The aim of ERAM is to provide a secure access service to digital resources for school users, in compliance with the principles of personal data protection.

The use of resources in the context of the ERAM is the subject of specific data processing, known as 'ERAM Processing', entered in the Ministry's Processing Register and under the responsibility of the Minister. School principals (secondary education) and Academic directors for education services (primary education) are thus removed from the obligations relating to the status of controller, which are generally carried out at national level.

GIP RENATER

RENATER is a public interest group (GIP) set up in 1993, which acts as the contracting authority for the national electronic communications network for technology, education and research.

The members of RENATER are the Ministry of National Education and Youth, the Ministry of Higher Education, Research and Innovation, as well as research organizations (such as CNRS, CPU, CEA, Inria, CNES, INRA, Inserm, ONERA, Cirad, IRSTEA, IRD and BRGM).

RENATER offers a portfolio of services (mobility, telephony, videoconferencing, security, identity federation, messaging, anti-spam), as well as efficient collaborative services tailored to the needs of the community.

The GIP RENATER implements and operates the Educational Resources Access Manager (GAR).

ID

Identifier.

IDP

Identity provider.

IETF

Internet engineering task force.

An open standardization body, which produces most of the new Internet standards. The IETF specifications are in the form of 'request for comments' (RFC) documents.

ISNI

International standard name identifier.

A unique identifier for entities that have contributed to the media such as books, television programs, press articles, etc. ISNI is defined by the International Organization for Standardization (ISO) and published under reference ISO 27729: 2012. The ISNI is managed by the International Agency. The BNF manages it for France.

MEF_STAT

A set of identifiers used by the Central Nomenclature Base (BCN) to describe the basic training modules (*Modules élémentaires de formation,* MEF). These codes are defined for statistical purposes.

MENJS (MEN)

Ministry of National Education, Youth and Sport. Ministry of National Education.

Native Application

A native application is an application that is not only accessible from a web browser and that requires an installation on the user's device (PMD, computer ...).

OAI-PMH

Open archives initiative; protocol of metadata harvesting.

OAI-PMH makes it possible to set up and automatically update centralized warehouses where metadata from various sources can be interviewed simultaneously. Particularly used by open archives and institutional warehouses, it has now become widely used in institutions such as libraries.

OASIS

Organization for the advancement of structured information standards.

An international consortium of standardization of open file formats. OASIS is the source of the SAML standard.

OpenID Connect (OIDC)

OpenID Connect is a protocol implementing an identification layer in addition to the OAuth 2.0 protocol.

Its goal is to allow the authentication of a user, as well as the propagation of identity attributes. The exchange of tokens and attributes is done through REST webservices calls and http redirections on defined entry points.

OP

OpenId Provider - identity provider.

In the OIDC protocol, the OP is the identity provider to which the user authenticates.

OpenSSL

A software generally provided with most operating systems, constituting a encryption toolbox. Open SSL is used in particular to produce the encryption keys used by the certificates.

OU

Organization unit.

In a certificate, designates the holding organization, and possibly the unit concerned within the organization.

PD

Personal data.

PKCE

Proof Key for Code Exchange.

A code created at the OIDC authorization request, and then used when exchanging the authorization code for an access token, to ensure that the client requesting the token is the one that made the authorization request.

RGAA

General repository for improving accessibility (*Référentiel général d'amélioration de l'accessibilité.)*

The RGAA is edited by the Interministerial Directorate for Digitalization to facilitate the implementation of digital accessibility.

RGS

General security repository (*Référentiel Général de sécurité*).

The RGS is the regulatory framework for building trust in the exchanges within the administration and with citizens. It is under the responsibility of the ANSSI.

RP

Relying Party.

In the OIDC protocol, an RP refers to a client application that requests user authentication from an identity provider.

RTC (STR)

Shared Technical Resource

A third-party component of a native and/or web application that allows information to be shared (stored, exchanged) between multiple ERAM resources. A shared technical resource is a specific resource that is not subject to subscription, not assignable by an assignment manager and cannot be displayed. It is characterized by a service type authorization (OIDC or OAuth2) and references to resources that can authorize it to request PD from ERAM.

SAML

A security assertion markup language.

XML based IT Single Authentication Standard (SSO) developed by OASIS defining a protocol to exchange security-related information.

ScoLOMFR

ScoLOMFR is the application profile of the LOMFR standard for school education.

Lom (learning object model) is the IEEE international standard, from which the AFNOR NF Z7640 (LOMFR) standard is derived.

SDET

A Virtual Learning Environments Master Plan (*Schéma directeur des environnements de travail*).

The SDET is published by the Ministry in charge of education. It defines the reference architecture and the target services in Virtual Learning Environments (VLEs), and formalizes the associated organizational, functional and technical recommendations (https://eduscol.education.fr/1559/schema-directeur-des-ent-sdet-version-en-vigueur).

SIREN

A business register identification system. The unique code, assigned by INSEE, identifies a company, body or association active in France. Sirens are referenced in the SIRENE register.

ERAM uses SIREN to identify the business name of the partners, their distributors or service providers.

SLO

Single log out.

An acronym used in SSO protocols to denote a single disconnection process.

SP

Service provider.

An SP refers to the client software in a client-server protocol.

SSL

Secure sockets layer.

A Netscape Internet security protocol, renamed Transport Layer Security (TLS) by IETF in 1999.

SSO

Single sign on.

A method allowing a user to access multiple IT applications (or secured websites) with only one authentication.

TLS

Transport layer security.

A security profile for IT exchanges derived from SSL. Developments in TLS are managed by IETF since 1999 (TLS v1.0 in 1999, TLS v1.1 in 2006, TLS v1.2 in 2008 and TLS v1.3 in 2018).

UAI

Registered administrative unit (*Unité administrative immatriculée*).

A 7-digit and 1-letter identifier, attributed to all private and public educational establishments in France.

URI

Uniform resource identifier.

A character chain identifying a resource on a network. URIs are defined by RFC 3986. Unlike URLs, URIs must provide permanent information.

URL

Uniform resource locator.

A uniform chain that makes it possible to locate a resource on the web, indicating its access procolm and its DNS location. URL syntax is defined by RFC 3986 (IETF).

UUID

Universally unique identifier

UUIDs are specified in RFC 4122.

VCARD

Visit card

VCard is an open standard format for the exchange of personal data, in the form of business cards. The current version (version 4.0) is defined by RFC 6350 and 6868.

WAYF

Where are you from - Discovery service.

A web interface that allows the user to select their profile and institution so that the ERAM can redirect them to the correct identity provider for authentication.

Web Service

A computer interface protocol of the web technology family enabling communication and data exchange between heterogeneous applications and systems in distributed environments.

Wildcard (certificat)

An omni-domain certificate *or* wildcard makes part of the certified domain name generic. It covers the certification of all machinery in the relevant sub-domain.

XML

Extensible Markup Language.

A mark-up metalanguage derived from SGML to produce structured data, in a predefined format via a schematic diagram.

XSD

XML Scheme, published as a recommendation by W3C in May 2001, is an XML document format description language to define the structure and content type of an XML document. That definition makes it possible, in particular, to verify the validity of that document.

ZIP

A file format allowing archiving (use of a single file to store multiple files) and compression of data without loss of quality. Examples and support documents for the Technical, Functional and Security Reference are proposed in the form of a zip file.

3   New features in latest ERAM versions

Each version of ERAM contains a set of improvements for users, VLE operators or resource providers. The present document presents only the new features concerning resource providers.

3.1   New features of ERAM release 7.0

In Addition to the information codeProjetResource (Resource project code) in the « Subscription » object

- ▶ Integration of native applications into ERAM's trust framework
- ▶ ERAM architecture allows resources available as native applications to operate within a reinforced trust framework based on the OpenId Connect protocol.

3.2   New features of ERAM release 6.2

Subscriptions Webservice

- ▶ A verification of the education cycle (primary or secondary) is performed when creating and modifying a subscription. The target audience can now include teacher-documentalists for a subscription for a primary school establishment, but the corresponding number of licenses must not be filled in (tag present without value or tag absent).

3.3   News features of ERAM release 6.1

Assignment Report Webservice

- ▶ The Assignment Report webservice allows a technical resource distributor known to ERAM to retrieve delta and complete assignment reports and the indication that they have been taken into account without having to connect to the ERAM portal.

Adding the idENT information to the "establishment" object accessible through the Subscriptions Webservice

- ▶ In the export file of the institutions' list, the identifier of the VLE to which each institution belongs is transmitted via the "idENT" tag.

Removal of irrelevant teaching areas from the records

- All the teaching field concepts are deleted during the post-missing, for each record added or modified, that contains a number of teaching fields corresponding to the ScoLOMFR-BCN vocabulary that exceeds a configurable threshold set at 5.

New accessor profile added

- A new ERAM access profile "national_aca" has been created for academic staff (non-teaching staff from the rectorate, DRAF, DSDEN, and districts).
- These are essentially educational inspectors or certain academic trainers who will benefit from the same VLE and resources.
- This profile completes the profiles of school management staff for secondary schools (National_dir), academic life staff working in the school (National_evs), administrative, technical or supervisory staff working in the school (National_eta) and local authority staff (National_col).

Implementation of ScoLOMFR version 8.

4 Native Application

4.1 Presentation

4.1.1 Context

Digital resources for schools are available in several "variants" (e.g. web applications, mobile applications - IOS, Android or other, desktop applications - Windows, MacOS, Linux, etc.).
In the following, we will refer to any application that is not only accessible from a web browser and must require an installation on the user's device (PMD, computer etc.) as a "native application".
The distribution and installation of this type of application on personal or company owned devices such as PMD, computer, etc. is on the responsibility of their owner's user.

ERAM allows to link the access of a user to a resource, through a native application, in the same framework of trust as for web resources.
It should be noted that the publisher can only protect a subset of the native application it provides with a valid ERAM session, especially when it processes personal data (PD as defined by ERAM).
The connection to ERAM within the application will have to be done through an ERAM connection button, easily identifiable by the user. In the rest of the document, we will refer to this button as the "ERAM Access Button".

4.1.2 Mixed user resource (web and native)

Some ERAM resources are accessible both in a web browser and through native applications specific to the OS on which they run.
This type of resource is called a mixed user resource and the different usage modes are called variants. A mixed user resource must contain 1 web variant and 0 to n native variants.
Although technically, a single digital resource can correspond to several applications, it is nevertheless managed as a single ERAM resource. It is described in a single record. Its subscriptions are valid for all its variants, it is only to be assigned once to a user and is presented in a unique way by the List of resources Webservice.
The information necessary for the proper functioning of native applications with ERAM must be provided by the resource providers to ERAM through new information in the resource records. These elements are described in §6.3.

4.1.3 Authentication modes via ERAM

A resource accessible via ERAM can be opened in several modes:
▸ The user has the option to launch the resource directly in a native application. The native application can then contact the RAG directly to authenticate the user to the

resource, using the OpenId Connect (OIDC) and OAuth2 protocols. This direct access mode will be referred to here as "application first".

 ▶ The user can launch the resource in web mode from his Mediacenter. The web page provided by the publisher can then decide on the access strategy to the corresponding native application (direct call to the installed application, link to an installation page, etc.).

This chapter presents the different ways a user can access an ERAM resource in a native application. The technical implementation details are detailed in §4.2.

4.1.3.1   Authentication from the application

Access to the resource from a native application by a user

There are five steps to access a resource :
1- The user clicks on a resource protected by ERAM in the native application
2- The ERAM receives the request to access the resource
3- Authentication of the user in his VLE or Authentication desk
4- Authorization of access to the resource and transmission of PD to the native application
5- Display of the resource in the native application

Figure 1 - Accessing a resource from a native application

ERAM access button
When accessing in "Application First" mode, the ERAM access button is necessary that the user must easily authenticate himself to access the functionalities of the resource protected by ERAM.
The native application should include a button to connect to ERAM. It is mandatory to use the provided button and no other visual.
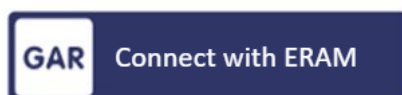
Figure 2 - ERAM access button

The sources of ERAM Access Button are available in the accompanying documents and examples:

GAR-RTFS_V7.0_DocumentsAccompagnement_FR/Protocoles_SSO/Bouton GAR

In order to delegate the authentication to the VLE or to the authentication desk, ERAM needs information about the user's profile and their institution.

Several implementations of this button are possible depending on the information held by the application on its user. The different possibilities are described in §4.2.2.1.

Authentication via the discovery service (WAYF)

If the application does not have all the information required to create the access URL (UAI, possibly Identity provider and/or profile), a click on the ERAM access button must provide this data.

The user is then redirected to a discovery service (WAYF) to choose their institution and profile via a form. The WAYF then redirects to the resource access module with the parameters entered by the user to continue the authentication process.

In order to make the user's experience smoother, WAYF also offers a function to memorize the choice of institution and profile in the browser used by the native application. The user will then have access to a favorite page the next time they access the application through the same browser.

Authentication via information retrieved from a previous connection

Following a first successful connection, the native application can retrieve the connection parameters defined by the user in the attributes provided by ERAM after the authentication process.

The call forged by the native application via the ERAM access button can then specify via the "profile" and "idEtab" parameters the information with which the user wishes to connect, in addition to the ResourceId: in this case ERAM Resource Access service continues the authentication process without presenting the WAYF interface for the establishment and profile selection.

The retrieval and use of these parameters by the application is not mandatory. If they are used, special attention must be paid to partitioning sessions between users.

4.1.3.2   Authentication from an ERAM access URL

In the case where the user accesses the resource from their media center, ERAM redirects them to the access URL for the web resource, defined in the record.

It is then up to the resource provider to choose the behavior to adopt:
- ▸ propose to the user to open the resource in the native application if it is installed on the user's device
- ▸ propose to the user to download it (without third-party identification),
- ▸ propose to the user to continue in web mode
- ▸ etc.

If the user chooses to use their resource within the native application, there are several implementation options available to the resource provider for requesting access from the application.

Requesting access without an open ERAM session

The Resource Provider may decide to launch the native application directly, before having requested an ERAM authentication. In this case, the user will have to authenticate to ERAM in their native application to access the features of their ERAM protected resource.
Access request on ERAM session opened in web mode.
The resource provider can also request ERAM authentication in CAS or SAML via the resource access service before proposing to the user to open the application.

Requesting access via an existing ERAM authentication by Access Token

In order to improve the user experience, especially to avoid the need to re-authenticate, ERAM proposes to provide an Access Token on web accesses in CAS and SAML. The resource provider can use this Access Token (AT) when opening the native application to obtain the user's PD. No additional authentication from the user will be required to view the resource in their native application by accessing it through this means.

4.1.4   Common technical resources

A shared technical resource (RTC) is a particular resource that allows storing and sharing data produced by other authorized resources. It cannot receive attributes provided by ERAM from another resource (identity and education data), but it can collect its own from behalf of a linked user resource. The list of user resources authorized to share data authorization with the RTC is specified in its record via a list of ark identifiers.
An RTC has the ability to retrieve its own ERAM attributes upon presentation to ERAM of a valid Access Token obtained from an authorized user resource. ERAM attributes are declared in the record of the RTC, and the RTC must be declared in the declaration of conformity of the calling user resource, whether it is web or mixed.
This type of resource cannot be subscribed to, or assigned by an Assignment Manager and will not be displayed in the Mediacenter.
Note that data exchanges, including the Access Token, with authorized resources are the responsibility of the resource provider who is in charge for their security.
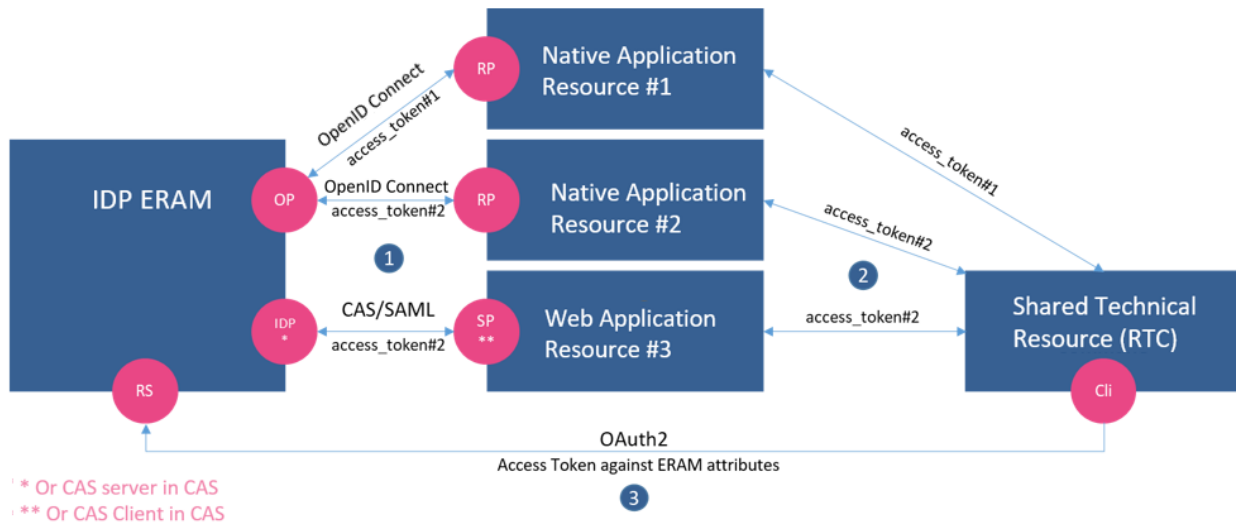
Figure 3 - Schematic diagram of Access Token exchange between RTC and user resources

Elements used to create an RTC record are described in §6.3.2.

4.2 Technical linkage guide

4.2.1 OpenID Connect Protocol

OpenID Connect protocol is an identification overlay to the OAuth 2.0 protocol.
It allows RPs ("Relying Party", aka the resource provider) to obtain user information (ERAM attributes) through an OP ("OpenId Provider", here ERAM).

There are several possible implementations of OpenId Connect (called flows). In order to interconnect with ERAM, native applications must use the *authorization code flow with PKCE* (Proof Key for Code Exchange).
In the standard authorization code flow, the exchange of access tokens is based on the presentation of the authorization code obtained from the OP and an "OIDC secret". The secret is a character string known only to the OP and the RP to ensure that the RP is legitimate to receive information from the user.
Since a native application cannot guarantee the security of this "OIDC secret", it cannot be used. The native application therefore does not provide the secret but a verification key (PKCE). This key does not allow the identification of the application but ensures that it is the same application that requests authentication and receives the tokens.

According to this mode, the authentication proceeds as follows:
- The native application prepares and sends an authentication request to ERAM;
- ERAM delegates the authentication to the VLE/the counter;
- ERAM redirects the user (or browser) to the native application with an authorization code;
- The native application exchanges the previously obtained code for tokens (ID Token, Access Token and Refresh Token) with ERAM;
- The application can then exchange the obtained Access Token for the PD.
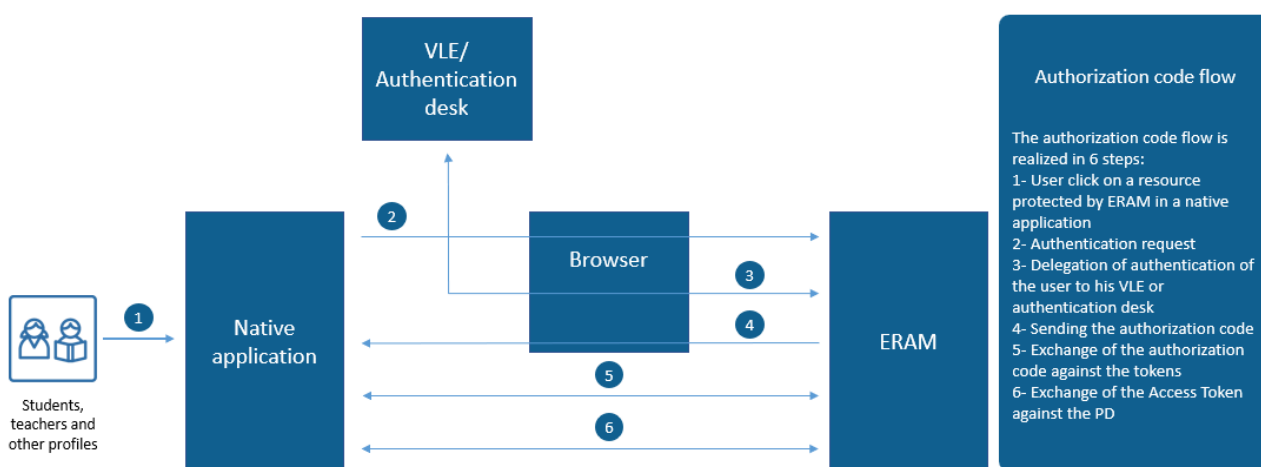
Figure 4 - Authorization code flow

RPs must be declared to ERAM. This declaration is done through the notice describing the resource (see §6.3).

It requires the following information:
- The "clientId": allows the application to be identified within ERAM. It must correspond to a UUIDv4 ("Universally unique identifier version 4");
- The "redirecUri": the redirection URI to which ERAM must redirect following the authentication request;
- The "clientName": a name (text without spaces) allowing to easily identify the native application.

Once declared to the OP (i.e. ERAM), the RPs can contact it using the configuration information exposed in the "well-known" file, the interface contract exposed by the OP (also called discovery).

For more details on the OpenId Connect protocol, you can consult the protocol specifications available at :

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

4.2.2 Specificities of OIDC implementation by ERAM

To interconnect to ERAM, the OpenId Connect implementation must comply with a set of specifications. The details of the endpoints and associated parameters are available in the SSO-FR interface contract available in the accompanying documents and examples:

GAR-RTFS_V7.0_DocumentsAccompagnement_FR/Protocoles_SSO/ERAM_SSO_Contract.pdf

4.2.2.1 Authentication and retrieval of ERAM attributes

Calls to some endpoints must include some additional parameters:

- "authorization endpoint":
- "idRessource" (required): ark identifier of the accessed resource;
- idEtab" (optional): UAI identifier of the user's establishment. It can be retrieved from a previous call if the UAI attribute is requested in the resource record;
- profile" (optional): user's profile. It can be retrieved on a previous call if the PRO attribute is requested in the resource record.

The "idEtab" and "profile" parameters are used to redirect the user to the VLE or the authentication desk. If they are not filled in, the user will be redirected to the WAYF described in chapter 4.1.3.1.

- "userinfo endpoint":
- "idRessource" (required): ark identifier of the accessed resource;
- access_mode" (required): access mode:
  o Access in web mode: " access_mode=web ".
  o Access in native application mode: " access_mode=appnat ".
  o Access from a RTC: " access_mode=rtc ".

The "access_mode" parameter is used by ERAM for statistical purposes to determine which type of access is requested when the PD is requested on the userinfo endpoint. Indeed, we allow to obtain an Access Token by other means than the OpenId Connect protocol for different use cases (see chapter 4.2.5).

4.2.2.2 Logout

For a web access, ERAM receives the logout from the VLE/Mediacentre to invalidate the user's active session and the associated tokens and propagate the logout to the resources to which the user is connected in web mode.

In a native application, the user initiates the logout from the application and not from their VLE/Mediacentre, in particular to allow operation without an open IDP session. The native application must transmit this logout request to ERAM on the "end_session_endpoint" exposed in the "well-known" in the front channel. ERAM uses the session cookie to identify the user's session to be invalidated and then propagates the logout to the identity provider that was used for the authentication.

If the latter does not implement the logout, ERAM displays an informative message inviting the user to logout with their VLE/authentication desk, provided that the browser displays it to the user.
In both cases, ERAM invalidates the authentication cookie and the associated tokens and then deletes the information stored for the session.
If passed, the post_logout_redirect_uri parameter is ignored. No redirection to the application is performed after logout.

After the logout, the user is redirected to ERAM information page or to the VLE/authentication desk page indicating that he/she has been correctly logged out, provided that the browser is displayed to the user. To return to the application, the user can close that page.

4.2.3   Granular access

Granular access is possible for a resource that is accessible by a native application to access a precise sub-part of the resource ("grain"). To do this, the redirectUri declared in the record must be suffixed by the grain at the time of the authentication request.

For example, for a redirectUri "my.app:/my-ressource/ " declared in the record, the grain can be defined in the redirectUri positioned in the authentication request, as follows:

-   "my.app:/my-ressource/part1"
-   "my.app:/my-ressource/?grain=part1".

Thus, the redirection to the application at the time of the transmission of the authorization code will be done on the grain requested during the authentication request.

4.2.4   Opening and authentication modes

4.2.4.1   Authentication from the application

The two authentication modes described in §4.1.3, via the WAYF or via information retrieved from a previous connection, are explained in the following sequence diagram:

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS
Liberté
Égalité
Fraternité
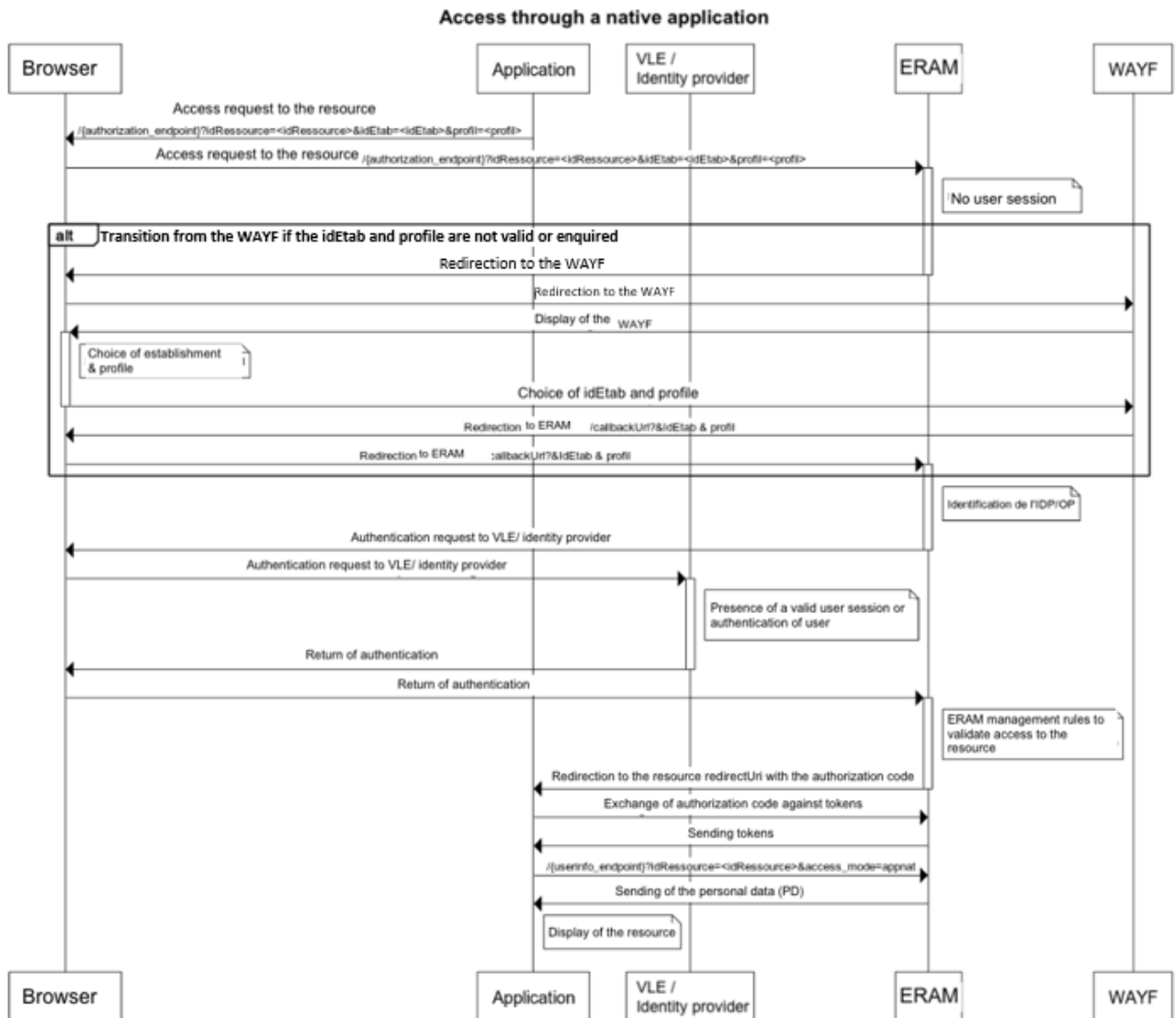
Figure 5 - Sequence diagram - Access by native application

4.2.4.2   Authentication from ERAM access URL

Request access without an open ERAM session

To access without an open ERAM session, the resource provider redirects to the application without having requested authentication from ERAM for the web variant. The native application requests authentication from ERAM as described in section 4.2.4.1.
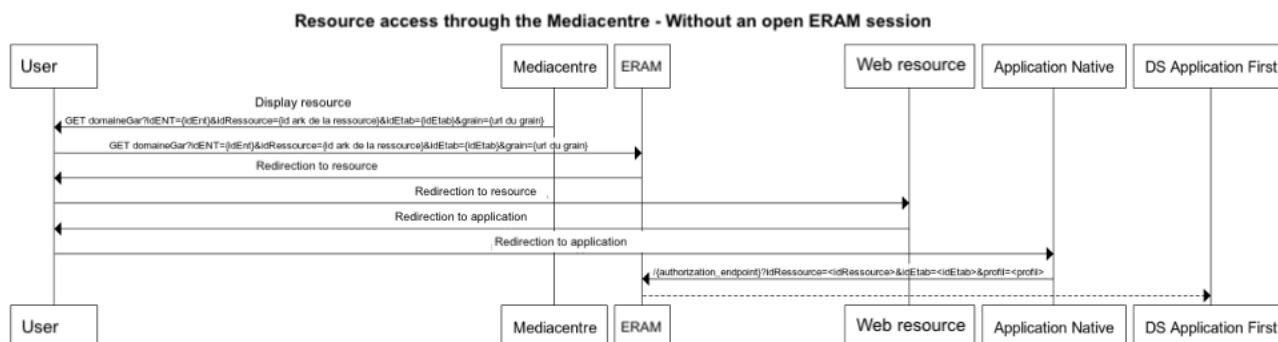
Figure 6 - Access from the Mediacenter without an open ERAM session

Request access based on an open ERAM session

The resource provider can also choose to authenticate the user for the web variant. After authentication, the partner can offer the user to either open the native application or to continue in the web browser.
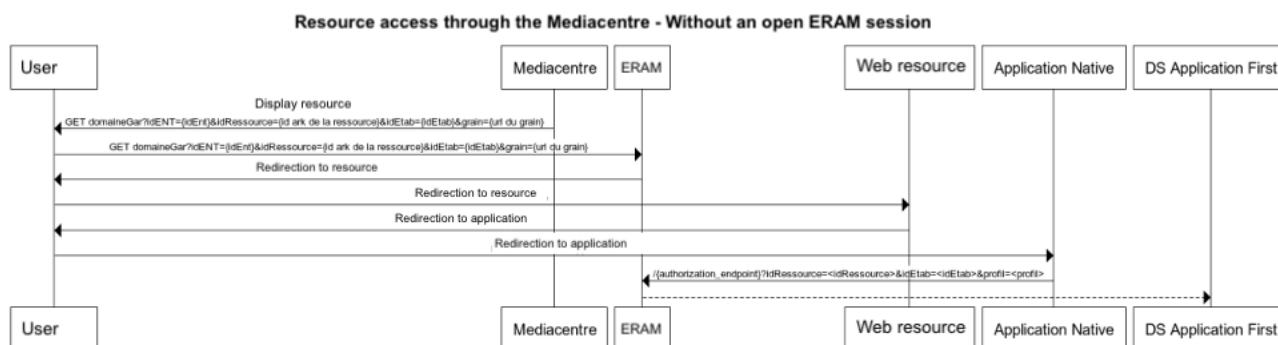
Figure 7 - Access from the Mediacenter with an open ERAM session

With this access mode, the user may have to re-authenticate within the native application if the browser used by the native application is not the one used by the user.

For example, if the resource provider uses Chrome Custom Tabs (for Android) or Safari View Controllers (for IOS) to implement OpenID Connect in the native application, cookie sharing can occur between the application's browser and the user's browser, if the user is using a browser that supports the solution (e.g. Chrome or Safari). In this case, the web browser session will be reused within the native application and authentication will be transparent to the user.

However, if these conditions are not met, the user will have to re-authenticate from his native application.

Request access via an existing ERAM authentication by the Access Token

ERAM proposes to provide an Access Token for web accesses using the CAS and SAML protocols (more details on the use of Access Tokens in chapter 4.2.5). This Access Token obtained through a web access can be passed on to the native application to obtain the user's PD without requesting a new authentication. The resource provider must then request authentication from the user during the web access request to obtain the Access Token to be transmitted to the native application.
The transmission of the Access Token to the native application must be done in a secure way. We recommend the use of an intermediate token with a low lifetime to exchange the Access Token.
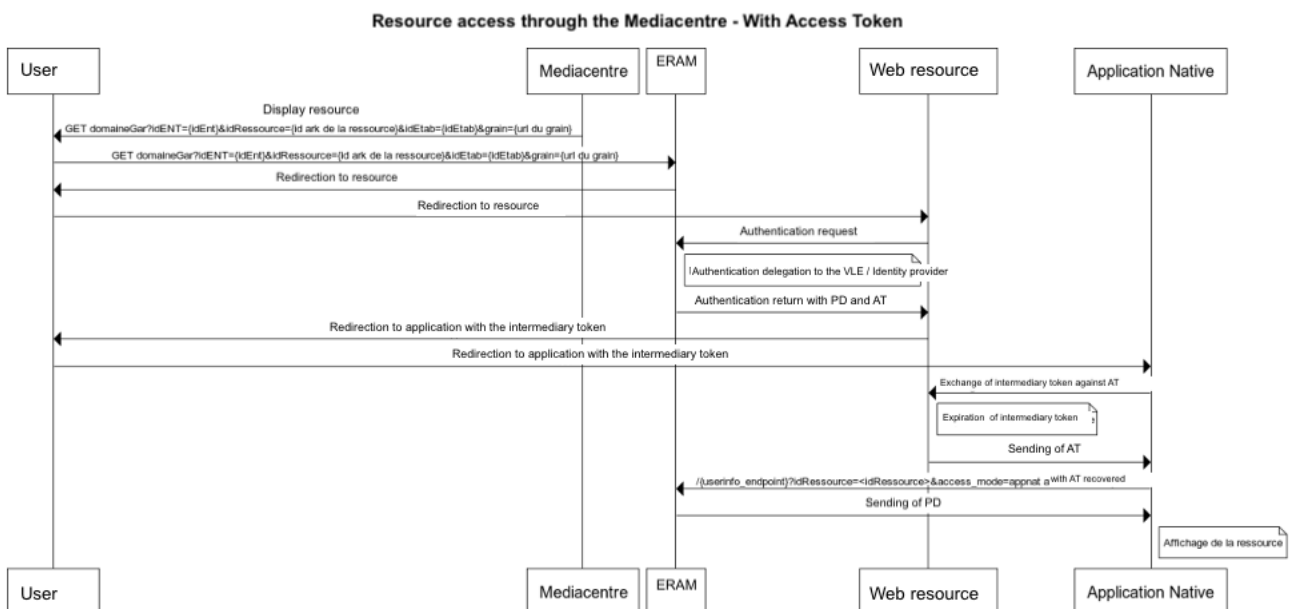
Figure 8 - Access from the media center with Access Token

4.2.5   Use of the Access Token

Access Token is a token issued under the OAuth 2.0/OpenID Connect protocols that allows, in the context of ERAM, a web or native application to access information related to the user for whom it was generated. This token is issued in OpenID Connect resource accesses, for native variants and on the call to the token_endpoint.
In CAS and SAML accesses, ERAM also provides the ability to obtain a "non-protocol" Access Token for resource accesses via web variants.

As described above, the Access Token obtained allows the resource provider to retrieve the user's ERAM attributes.

The different possible cases of usage are described below.

Sharing the Access Token between the web and the native variants of a mixed user resource

The transmission can be done from the web variant to the native variant, in a secure way as explained in §4.2.4.2, or from the native variant to the web variant.
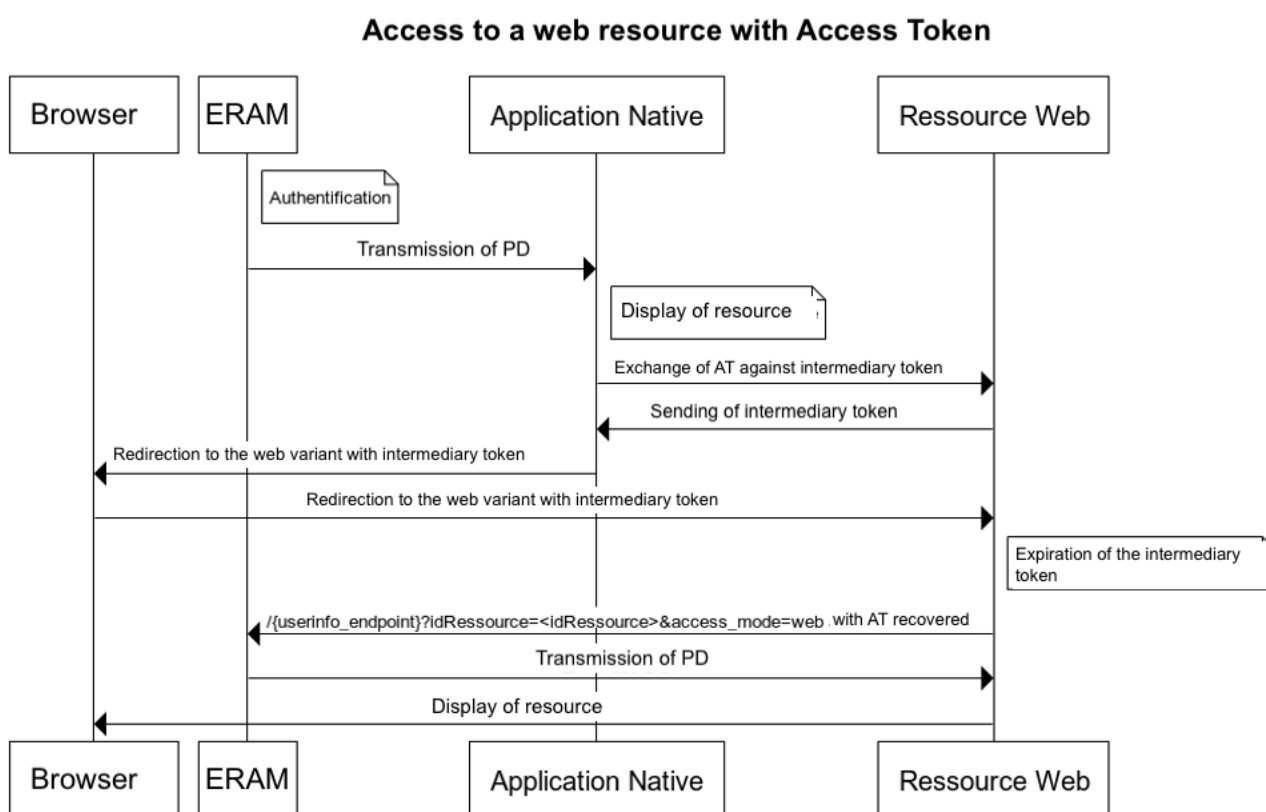
Figure 9 - Web access via an Access Token

Sharing the Access Token between a user resource and a shared technical resource (RTC)

This case of usage allows the RTC to retrieve its own attributes from ERAM (which may differ from those of the user resource), via the TA of the user resource requesting it. This retrieval is only possible if the user resource that obtained the Access Token is linked to the common technical resource by means of a declaration in the RTC record (see §6.4). The common technical resource will retrieve its own PDs, not the PDs of the resource initially accessed.

Personal Data retrieval via a Shared Technical Resource (RTC)
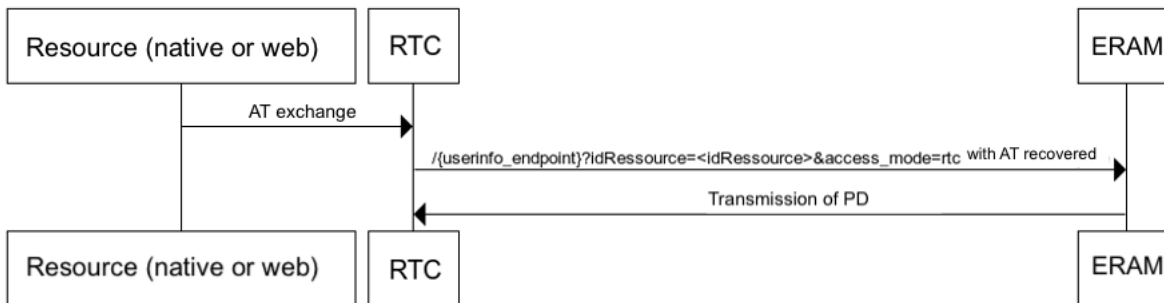
Figure 10 - PD retrieval by an RTC

Sharing the Access Token between two resources of the same TDR platform

For two resources accessible via a given TDR platform, it is possible to transmit the Access Token of an initially accessed resource A to a resource B. Resource B will then be able to obtain its own ERAM attributes thanks to the Access Token obtained on the access to resource A, without making a new authentication request.

Personal Data retrieval for two resources of the same TDR platform
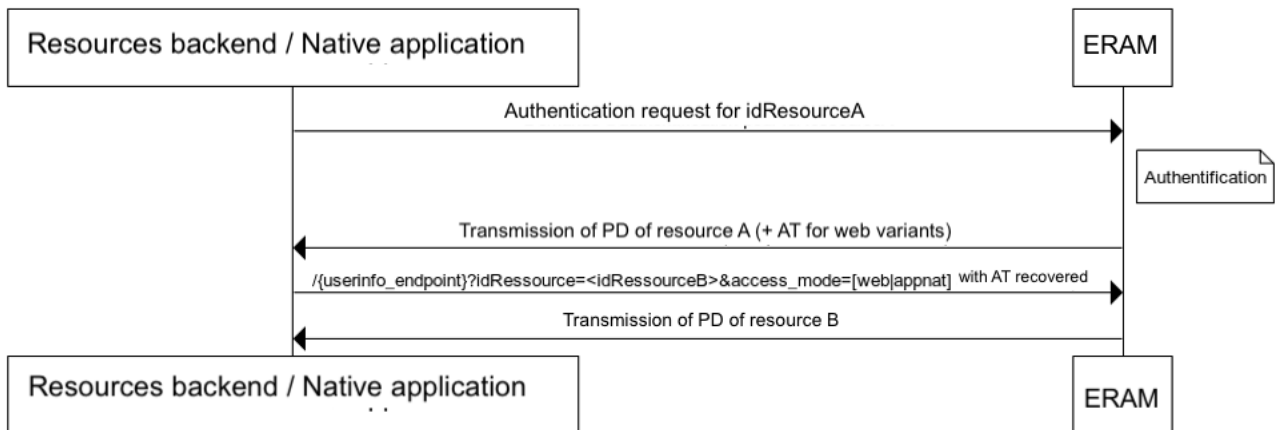
Figure 11 - PD retrieval for two resources of the same TDR platform

Comments

The validity of the Access Token is equal to the session duration of the ERAM.
In terms of accesses from a native application in OpenID Connect ("application first"), it is possible to renew the Access Token through the Refresh Token obtained with the Access Token when calling the token_endpoint. If the renewal is requested, a new Access Token is provided

with a new validity equal to the session duration of ERAM. The Refresh Token has a lifetime equal to the maximum ERAM session duration (see SSO-FR interface contract).

When the Access Token is obtained through the CAS and SAML protocols for web variants, no Refresh Token is transmitted. Thus, it cannot be renewed as for the native variants. However, the resource provider can request a new Access Token by requesting a new authentication request.

The extension of the user's ERAM session for the access to the same resource as a new resource does not extend the validity of the current Access Token.
The end of an ERAM session, on a logout request or by expiration of the session, will cause the expiration of the valid Access Tokens linked to this session.

4.2.6   Offline mode

ERAM allows native applications to implement an "offline ERAM" or "offline" mode for a specific period of time.
This "offline ERAM" or "offline" mode allows the user to access, for a limited time, the protected content of the resource without being authenticated to ERAM. This mode can be used in two cases: the momentary loss of network access (offline) or the end of ERAM session (offline).
The use of this mode MUST BE limited in time: a "maximum offline access time" MUST BE set in the mobile application, but the setting of this time falls under the responsibility of the resource provider.

ERAM session protection

ERAM protection applied to native applications that implement the OIDC protocol is technically guaranteed by the ERAM session.
In general, the ERAM session mechanism has the following characteristics:

- ERAM protection is no longer guaranteed beyond the ERAM session (6 h max);
- It is not possible to request ERAM PD beyond the ERAM session;
- The user must re-authenticate with his VLE or counter, to continue ERAM protection and request PD on a session basis.

ERAM out-of-session mode

For native applications, beyond ERAM session, it is possible to explicitly propose to the user to use "offline ERAM" for a given time (determined by the "maximum offline access time"). This operation also applies to the "offline" mode (in case of loss of internet connection during a valid ERAM session).

This mode of use MUST BE restricted by the following rules:

- The user can remain identified and use the protected part of the resource in nominal mode up to the "maximum offline access time"; the native application MUST NOT contact or exchange with third party services for its ERAM protected part.
- After the "maximum offline access time", the user is no longer allowed to access the resource protected by ERAM: the user is therefore no longer identified in the application.

Examples of "out of session ERAM" mode implementation

Use case 1: Internet is not accessible from the device

The Internet becomes inaccessible on the device while a valid ERAM session is in progress. The following operation is given as an example:

- If the native application goes into "offline" mode: the user still has access to the ERAM protected content as long as the duration of the "offline" mode is not exceeded;
- If the Internet becomes accessible again before the end of the maximum "offline" access time while using the native application,
  - The native application checks if the session is still active and can therefore be renewed. Once the session is renewed, the status changes to "online";
- If the session is no longer active and cannot be renewed :
  - The native application proposes to reconnect to ERAM;
- If the session is refused, the application remains in "offline" mode until the end of the maximum "offline" access time;
- If the Internet is still inaccessible at the end of the maximum "offline" access time, the user no longer has access to the content protected by the ERAM and goes into "offline" mode. The native application displays an information popup to the user to notify them that they are logged out of ERAM.

Use case 2: Internet is accessible from the terminal but ERAM session expired

When an ERAM session has expired (after 6 hours), it cannot be renewed. The following examples are given:

- The native application displays a popup to the user, offering them to reconnect or to stay offline;
- The user can reconnect; the mobile application then initiates a new connection request to ERAM (with the same profile and institution, registered during the first connection);
- If the user decides to stay offline, the native application goes into "offline" mode: the user still has access to the content protected by the ERAM as long as the "maximum offline access time" is not exceeded;

- ▶ Once the "maximum offline access time" has been exceeded, the native application switches to "offline" mode: a popup is displayed and informs the user that they no longer have access to the content protected by ERAM and that they switches to "anonymous" mode;
- ▶ The user can then click on one of the ERAM access buttons to log back in.

ERAM variable	Value
Session validity	Defined by ERAM: 1h00
Maximum session length	Defined by ERAM: 6h00
Access Token validity (OIDC)	Defined by ERAM: 1h00
Maximum Access Token duration (OIDC)	Defined by ERAM: 6h00
Refresh Token Lifetime (OIDC)	Defined by ERAM: 6h00
Maximum offline access time	Defined by the resource provider

Table 2 – Duration of the ERAM sessions
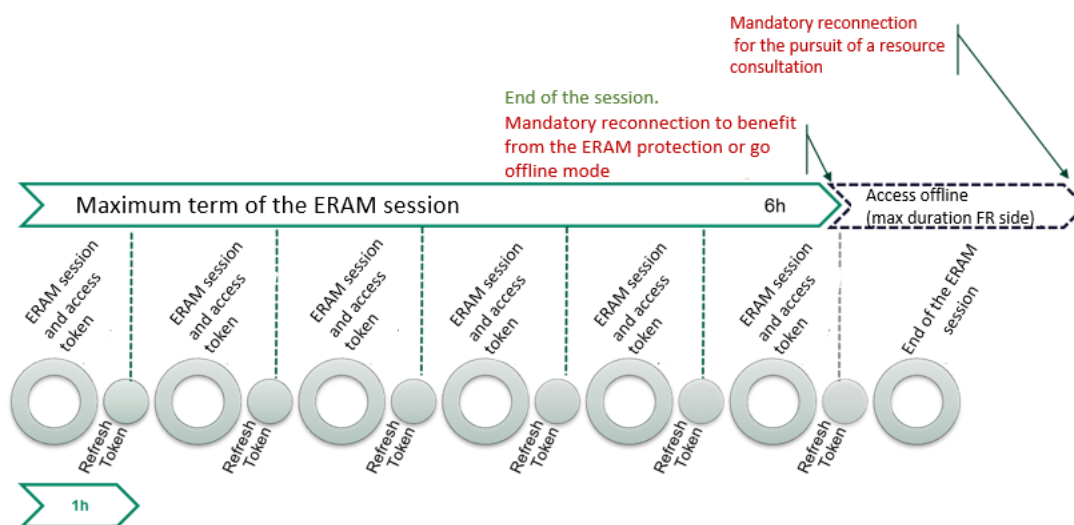
Figure 12 - Mechanism of the sessions and the ERAM protection

5 ERAM security protocols

In its security policy, ERAM only allows protocols and cipher suites that provide a sufficient level of security.

Protocol : TLSv1.2 ;

Cipher :

- ECDHE-ECDSA-CHACHA20-POLY1305,
- ECDHE-RSA-CHACHA20-POLY1305,
- ECDHE-ECDSA-AES128-GCM-SHA256,
- ECDHE-RSA-AES128-GCM-SHA256,
- ECDHE-ECDSA-AES256-GCM-SHA384,
- ECDHE-RSA-AES256-GCM-SHA384,
- DHE-RSA-AES128-GCM-SHA256,
- DHE-RSA-AES256-GCM-SHA384,
- ECDHE-ECDSA-AES128-SHA256,
- ECDHE-RSA-AES128-SHA256,
- ECDHE-ECDSA-AES128-SHA,
- ECDHE-RSA-AES256-SHA384,
- ECDHE-RSA-AES128-SHA,
- ECDHE-ECDSA-AES256-SHA384,
- ECDHE-ECDSA-AES256-SHA,
- ECDHE-RSA-AES256-SHA,
- DHE-RSA-AES128-SHA256,
- DHE-RSA-AES128-SHA,
- DHE-RSA-AES256-SHA256,
- DHE-RSA-AES256-SHA,
- ECDHE-RSA-DES-CBC3-SHA,
- AES128-GCM-SHA256,
- AES256-GCM-SHA384,
- AES128-SHA256,
- AES256-SHA256,
- AES128-SHA,
- AES256-SHA,
- !DSS.

6 Resource description

ERAM operates with resource description records.

These records are in ScoLOMFR format. They are placed in an OAI-PMH data repository (see below, Chapter 7- Harvestable warehouses), where they are harvested to be registered in the ERAM resource repository.

This chapter provides all specifications for using ScoLOMFR to create the resource description records within the ERAM framework.

It specifies all the elements of the record that must meet specifications to allow ERAM to work.

However, it does not revisit the general ScoLOMFR specifications, for which the documentation is available on the official ScoLOMFR website.

Examples of records in ScoLOMFR 7.0 format are provided in the accompanying annexed documents (see below for the list of example records).

ScoLOMFR records are XML files that conform to the structure defined by the XSD schemas of the ScoLOMFR version used.

The records provided in the examples package are validated according to the "lax" XSD scheme of ScoLOMFR version 8.0.

ScoLOMFR version

> *This "lax" scheme ensures backward compatibility in terms of XSD validation from version 3.0 to 8.0.*

The XSD of the ScoLOMFR 8.0 version are available on the following links

for download

https://www.reseau-canope.fr/scolomfr/telecharger-tous-les-fichiers

Within ERAM, a ScoLOMFR record represents a user resource or a shared technical resource (RTC).

A user resource can be:

- ▶ A web access only resource
- ▶ A mixed resource, with web access and one or more native variants (definition §4.1.2). For more details on records describing mixed resources, see §6.3.

A user resource can be autonomous, or linked "mother of family", or "family member". For more details on records describing linked resources, see §6.2.

For more details on records describing RTCs, see §6.4.
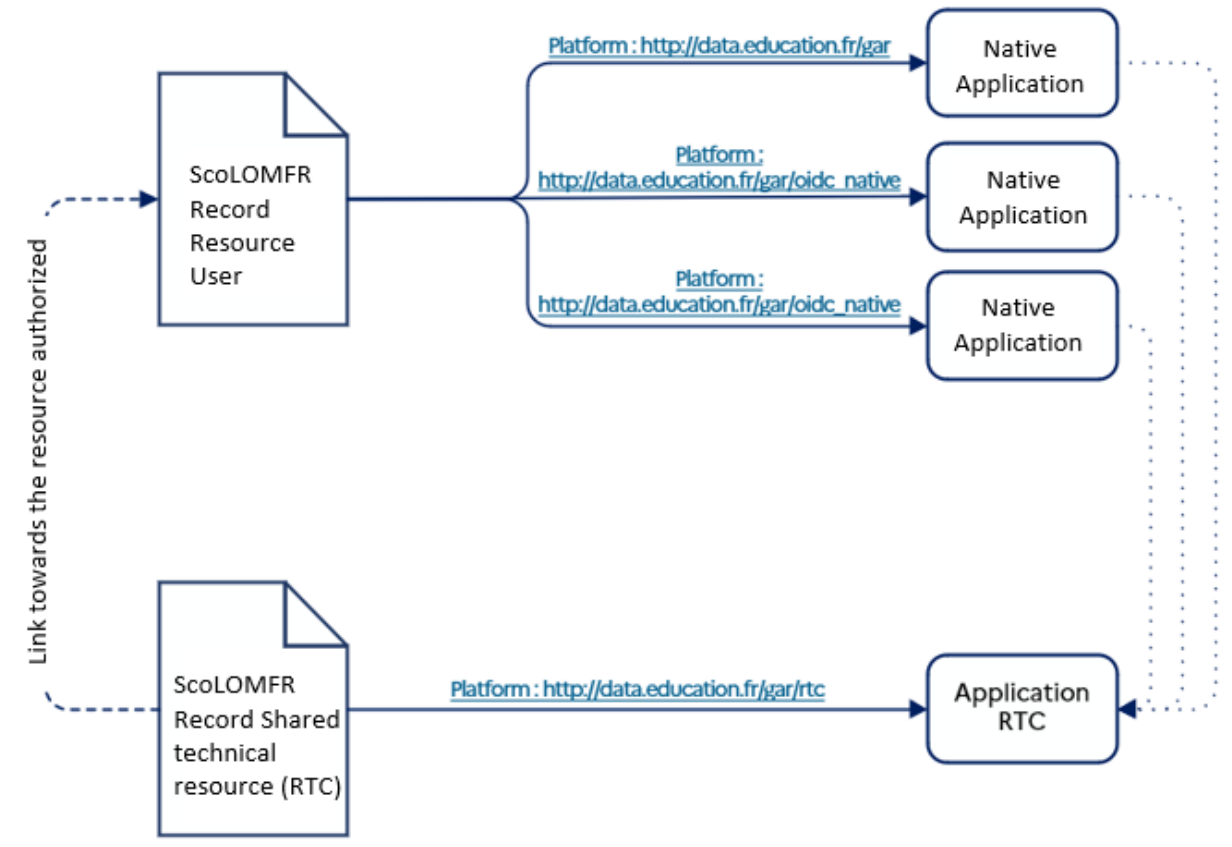
Figure 13 -Diagram showing the types of resources and their different implementation variants

6.1 Record elements

The rules for the use of ScoLOMFR elements are defined by the ScoLOMFR Reference Manual, available online at https://www.reseau-canope.fr/scolomfr/.
The following specifications provide details on the use of ScoLOMFR elements specifically used for the ERAM operation.
The elements are presented according to the order of presentation in the ScoLOMFR reference manual, which is strictly enforced in the records provided as examples.

The set of examples includes a stand-alone resource record, three records describing a family of resources (two member resources, and a "mother" of resources), a manual with native variants, a shared technical resource manual (RTC), as well as a prototyping record, which can be used as a guide for making a first resource record:

- NoticeExemple_Autonome_p.xml
  Sample record for an autonomous resource, subject: German, level: *classe de cinquième*, equivalent to seventh grad.
- NoticeExemple_FamilleLesArts_cirque_p.xml
  sample record for a resource member of the family *Les Arts*, about circus arts.
- NoticeExemple_FamilleLesArts_musique_p.xml
  Example record for a resource member of the family *Les Arts*, about music.
- NoticeExemple_FamilleLesArts-MFV_galerieArts_p.xml
  sample record for "mother of the family" resource, for the family *Les Arts*.
- NoticeExemple_Autonome_OIDCNative_p.xml
  sample record for a user resource with a native variant
- NoticeExemple_rtc_p.xml
  sample record for an RTC resource linked to a user resource
- Maquette_prototypage_notice_p.xml
  Mask for the creation of a new record, including comments to help with the input of all the significant elements.

The different elements detailed in the following paragraphs refer to the presentation adopted in the prototyping record. Links to specific portions of the code are presented by anchors of the form "# + anchorName"; these same anchors are present in the prototyping record, which allows one to go directly to the sections concerned by a keyword search.

Example

In the following section 6.1.1, you will find the tag "#identifier", this tag is also present in the prototyping record in the accompanying documents.

6.1.1 Identifier

ScoLOMFR Element

1.1 – Identifier

ScoLOMFR vocabulary

Not controlled.

XML element

lom.general.identifier.catalog
lom.general.identifier.entry

Example

Sample record: #identifier

```
<lom:identifier>
   <lom:catalog>ark</lom:catalog>
   <lom:entry>ark:/49591/AmanAll5.p</lom:entry>
</lom:identifier>
```

Comments

The title is used as a label for user resources, and will appear in the VLE media center used by the users. In the case of a shared technical resource (RTC), it is not displayable and will not appear in a media center.

ERAM constraints

> *The title MUST be filled in and unique;*
>
> *Its size MUST be less than 255 characters;*
>
> *In the case of a "mother" resource (see below, Chapter 5.2 - Creating a family), the title MUST contain "parent".*
>
> *In the case of a common technical resource, the title MUST begin exactly with "[RTC]".*

6.1.2   Resource title

ScoLOMFR element

1.2 – Title

ScoLOMFR Vocabulary

Not controlled

XML element

lom.general.title.string

Example

Sample record : #title

```
<lom:title>
   <lom:string>Visiter le château de Moulinsart</lom:string>
</lom:title>
```

Comments

The title is used as a label and will appear in the VLE media center accessed by users.

ERAM constraints

> *The title MUST be filled in and unique ;*
>
> *Its size MUST be less than 255 characters ;*

6.1.3 Description

<u>ScoLOMFR element</u>

1.3 – Description

<u>ScoLOMFR Vocabulary</u>

<u>Not controlled</u>

<u>XML element</u>

lom.general.description.string

<u>Example</u>

Sample record: #description

```
<lom:description>
  <lom:string>
    Description de la ressource, affichée dans la console d'affectation (détail
des ressources).
  </lom:string>
</lom:description>
```

<u>Comments</u>

Element "1.4 description" contains the description of the resource. It is used in ERAM as information on the nature of the resource and presented as such to the assignment managers. It is an informative summary, providing all the necessary information for relevant assignments by the assignment managers.

In order to retain formatting elements (line breaks in particular), it is advisable to place the content of the element <string> in a CDATA block.

<u>ERAM Constraints</u>

The description element MUST be filled in.

6.1.4 Documentary Type

<u>ScoLOMFR element</u>

1.9 – Documentary Type DC

<u>ScoLOMFR Vocabulary</u>

ScoLOMFR controlled vocabulary voc-004[2]

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

XML element

lom.general.documentType

Example

Example record : #document type

```
<lomfr:documentType>
   <lomfr:source uniqueElementName="source">SCOLOMFRv8.0 </lomfr:source>
   <lomfr:value uniqueElementName="value">
     http://url.org/dc/dcmitype/Text
   </lomfr:value>
   <lomfr:label>texte</lomfr:label>
</lomfr:documentType>
<lomfr:documentType>
   <lomfr:source uniqueElementName="source">SCOLOMFRv8.0 </lomfr:source>
   <lomfr:value uniqueElementName="value">
     http://url.org/dc/dcmitype/Service
   </lomfr:value>
   <lomfr:label>service</lomfr:label>
</lomfr:documentType>
```

Comments

Possibility of assigning several values.

ERAM constraints

> *The "Documentary Type" element MUST contain the documentary type of the resource.*

6.1.5 Resource Provision Roles

ScoLOMFR element

2.3 - Contribution

ScoLOMFR Vocabulary

ScoLOMFR controlled vocabulary voc-003

Élément XML

lom.lifeCycle.contribute

Example

Sample record: #role

```
<lom:contribute>
   <lom:role uniqueElementName="role">
     <lom:source uniqueElementName="source">LOMv1.0</lom:source>
     <lom:value uniqueElementName="value">
         http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-003-num-026
     </lom:value>
     <lom:label>distributeur technique</lom:label>
   </lom:role>
```

```
    <lom:entity>
<![CDATA[
BEGIN:VCARD
VERSION:4.0
KIND:org
ORG:EFFIOS
FN:EFFIOS
TEL:(33)6-19-35-68-55
LOGO:http://
EMAIL:dtr@effios.fr
NOTE:SIREN=511083743
NOTE:ISNI=0000000073624720
NOTE:X-PLATEFORME-ID=00
URL:http://www.effios.fr
REV:2021-01-01
END:VCARD
]]>
    </lom:entity>
    <lom:date uniqueElementName="date">
        <lom:dateTime uniqueElementName="dateTime">2016-07-01</lom:dateTime>
        <lom:description uniqueElementName="description">
            <lom:string>GAR : distributeur technique</lom:string>
        </lom:description>
    </lom:date>
</lom:contribute>
```

Comments

All the roles (publisher, technical distributor, commercial distributor, technical validator) ensuring access to the resource via the ERAM are identified in the record through VCARDs.

ERAM constraints

> *The roles "Éditeur", "Distributeur technique", "Distributeur commercial" and "Valideur technique" MUST be filled in.*

6.1.6   Using VCARDs

ScoLOMFR element

2.3.2 - Entity

ScoLOMFR Vocabulary

Use of the VCARD format, RFC 6350

XML element

lom/lifeCycle.contribute.entity

Example

Sample record: #vcard
```
<![CDATA[
```

```
BEGIN:VCARD
VERSION:4.0
KIND:org
FN:MonFournisseurDeRessources
TEL:(33) 0-00-00-00-00
LOGO:http://monUrl.com.logo.png
EMAIL:moi@MonFournisseurDeRessources.com
NOTE:SIREN=000000000
NOTE:ISNI=0000000000000000
ORG:MonFournisseurDeRessources
REV:2020-09-25
END:VCARD
]]>
```

Comments

List of VCARD elements, cardinality and obligation.

Element	VCARD Required Y/N	Card	ERAM Required Y/N	Comments
BEGIN:VCARD	Y	1	Y	Start of VCARD
VERSION:4.0	Y	1	Y	Immediately after the element BEGIN. Version information.
FN	Y	1-N	Y	Name of the object described by the VCARD (max 255 characters)
ADR	N	0-N	N	Address, structured string; ADR:[POBox];;[ext. Adr];;[street and N°];;[ville];;[region];;[postalcode];;[country]eg : ADR:;;22 rue de la Source.;Paris;;75001;France
TEL	N	0-N	Y	Phone number text or URI (URI SchemeTEL, RFC 3966)
EMAIL	N	0-N	Y	Mandatory for TDR, CDR and TV Max 255 characters
NOTE:SIREN=	N	1	Y	Mandatory. Entity's SIREN number for French companies, and DUNS number for foreign ones A vCard NOTE field, starting with SIREN=, is used to describe the entity's identifier. 9 characters, no spaces.
NOTE:ISNI=	N	1	N	Entity's ISNI number. Optional, if the SIREN is not used by several registered entities. If the ISNI is missing, it will be coded in the form: 0000-0000-0000-0000
NOTE:X-PLATEFORME-ID	N	1	N	TDR's platform (if applicable) By default, 00
ORG	N	0-1	Y	Name of organization. ERAM uses the field ORG for TDRs and CDRs (mandatory for these roles).
REV	N	0-1	N	vCard revision date (timestamp). Ex REV:2021-01-01
END:VCARD	Y	1	Y	End of VCARD

Table 3 -Description of VCARD elements

ERAM constraints

The VCARDs of the roles used by ERAM MUST respect the presence of the mandatory ERAM elements (see the table above);

The VCARDs MUST be compliant with version 4.0 or higher (RFC 6350)[2];

VCARDs MUST be placed in a CDATA tag (which indicates textual content, not parsed for format validation);

Elements MUST be separated by a CRLF line break;

VCARDs MUST NOT contain tabs and other special characters not specified in the format.

6.1.7   Publisher Role

ScoLOMFR Element

2.3.1 - Role

ScoLOMFR Vocabulary

ScoLOMFR controlled vocabulary voc-003[1]

XML element

lom.lifeCycle.contribute.role[publisher]

Example

Sample record : #editeur

Comments

The "*éditeur*" role is used by the ERAM to identify the signatory of the contract (legal entity identified by its SIREN (or DUNS) and possibly its ISNI).

ERAM constraints

The VCARD MUST contain the elements necessary for the GARERAM, following a precise syntax;

The FN field MUST contain the publisher's corporate name, as declared for the ERAM initialization process;

The ORG field MUST contain the publisher's brand name, as declared for the initialization of the ERAM;

The TEL and EMAIL fields are required;

The SIREN field MUST be filled in, with the value declared during the initialization process and mentioned in the contract;

The ISNI MUST be filled in if the SIREN of the signatory of the contract corresponds to several publishing brands. The ISNI can be requested from the local managing entity;

The LOGO and URL fields MAY be filled in;

---

[1]   Available at:
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-003 (ScoLOMFR vocabulary 6.0).

The REVISION field SHOULD be filled in (update date, version);

The VCARD SHOULD be placed in a CDATA block (which ensures the correct management of textual elements);

The "publisher" role MUST have only one instance with a note SIREN belonging to the list of ERAM agreement signatories.

6.1.8   Technical Distributor Role

<u>ScoLOMFR element</u>

2.3.1 - Role

<u>ScoLOMFR Vocabulary</u>

ScoLOMFR controlled vocabulary voc-003 [2]

<u>XML element</u>

lom.lifeCycle.contribute.role[distributeur technique]

<u>Example</u>

Sample record: #DTR

```
<lom:contribute>
  <lom:role>
  …
  </lom:role>
  <lom:entity>
<![CDATA[
BEGIN:VCARD
…
END:VCARD
]]>
  </lom:entity>
  <lom:date uniqueElementName="date">
    <lom:dateTime uniqueElementName="dateTime">2016-07-01</lom:dateTime>
    <lom:description uniqueElementName="description">
        <lom:string>GAR : distributeur technique</lom:string>
    </lom:description>
  </lom:date>
<lom:contribute>
```

<u>Comments</u>

The "*GAR : distributeur technique*" role is used by ERAM for technical liaison and support.

---

[2]   Available at:
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-003 (ScoLOMFR vocabulary 6.0).

> *The VCARD MUST contain the elements required by ERAM, following a precise syntax;*
>
> *The FN field MUST contain the company name of the TDR, as declared during the ERAM initialization process;*
>
> *The TEL and EMAIL fields are mandatory. The email will be used for repository harvest notifications;*
>
> *The SIREN field MUST be filled in, with the value declared during the initialization process;*
>
> *The LOGO and URL fields MAY be filled in;*
>
> *The REVISION field SHOULD be filled in (update timestamp, version);*
>
> *The VCARD SHOULD be placed in a CDATA block (which ensures the correct management of textual elements);*
>
> *The TDR MUST be unique;*
>
> *In case the TDR uses a platform different from the default one (00), the NOTE:X-PLATEFORME-ID= element specifying the technical platform must be added. The platform number used is provided by ERAM, according to the platforms initialization.*
> *The value of this element is coded on two numeric characters:*
>
> - *this element is missing, platform 00 is used.*
>
> - *If the value does not conform or if the field is multivalued, the record is rejected.*
>
> *The date.description element associated with the entity must contain the mention "GAR : distributeur technique".*

6.1.9 Commercial Distributor Role

<u>ScoLOMFR element</u>

2.3.1 - Role

<u>ScoLOMFR vocabulary</u>

ScoLOMFR controlled vocabulary ScoLOMFR voc-003[3]

<u>XML element</u>

lom.lifeCycle.contribute.role[diffuseur/distributeur]

<u>Example</u>

Example record: #DCR

```
<lom:contribute>
```

---

[3] Available at:
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-003 (ScoLOMFR vocabulary 6.0).

```
   <lom:role>
     <lom:source uniqueElementName="source">LOMv1.0</lom:source>
     <lom:value uniqueElementName="value">
         http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-003-num-017
     </lom:value>
     <lom:label>diffuseur / distributeur</lom:label>
   </lom:role>
   <lom:entity>
<![CDATA[
BEGIN:VCARD
…
END:VCARD
]]>
   </lom:entity>
   <lom:date uniqueElementName="date">
     <lom:dateTime uniqueElementName="dateTime">2016-07-01</lom:dateTime>
     <lom:description uniqueElementName="description">
         <lom:string>GAR : distributeur commercial</lom:string>
     </lom:description>
   </lom:date>
<lom:contribute>
```

Comments

The "*GAR : distributeur commercial*" role is used by ERAM for the subscription management web service.

ERAM constraints

The VCARD MUST contain the elements required by ERAM, following a precise syntax;

The FN field MUST contain the corporate name of the CDR, as declared for the initialization of ERAM

The TEL and EMAIL fields are mandatory;

The SIREN field MUST be filled in, with the value declared during initialization process;

LOGO and URL fields CAN be filled in;

The REVISION field SHOULD be filled in (update timestamp, version);

The VCARD SHOULD be placed in a CDATA block (which ensures the correct management of textual elements);

The record MAY contain several CDRs;

Only the CDRs mentioned in the record will be able to use the web service to communicate subscriptions on this resource;

The date.description element associated with the entity must include the mention "GAR: distributeur technique".

6.1.10 Technical Validator Role

ScoLOMFR element

2.3.1 – Role

ScoLOMFR vocabulary

 ScoLOMFR controlled vocabulary voc-003[4]

 XML element

lom.lifeCycle.contribute.role[valideur technique]

Example

Sample record: #valideur

```
<lom:contribute>
   <lom:role>
     <lom:source uniqueElementName="source">LOMv1.0</lom:source>
     <lom:value uniqueElementName="value">
         http://data.education.fr/voc/scolomfr/concept/technical_validator
   <lom:label>valideur technique</lom:label>
   </lom:role>
   <lom:entity>
<![CDATA[
BEGIN:VCARD
…
END:VCARD
]]>
   </lom:entity>
   <lom:date uniqueElementName="date">
     <lom:dateTime uniqueElementName="dateTime">2016-07-01</lom:dateTime>
     <lom:description uniqueElementName="description">
         <lom:string>GAR : validation technique</lom:string>
     </lom:description>
   </lom:date>
<lom:contribute>
```

Comments

The "GAR : validation technique" role is used by ERAM to define the validation date of the resource.
This validation date is initially set at the date of the conformance assessment. It must be renewed at the end of the two-year validity period.
By renewing this date, the publisher certifies that it has verified that the record still matches the current state of the resource, and that the resource still complies with the terms of the ERAM contract.

---

[4]   Available at :
     https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-003 (ScoLOMFR vocabulary 6.0).

> *The VCARD MUST contain the elements necessary for ERAM, following a precise syntax;*
>
> *The FN field MUST contain the company name of the technical validator;*
>
> *The TEL and EMAIL fields are mandatory;*
>
> *The SIREN field MUST be filled in;*
>
> *The LOGO and URL fields MAY be filled in;*
>
> *The REVISION field SHOULD be filled in (update timestamp, version);*
>
> *The VCARD SHOULD be placed in a CDATA block (which ensures the correct management of textual elements);*
>
> *In production, the record MUST have a validation date of less than two years:*
>
> *The validity period is two years. If the date is invalid or missing, the record is not harvested;*
>
> *Records used by the partner platform MUST NOT have a validation date.*

6.1.11   Extended Location

ScoLOMFR element

4.3.1 – Extended Location

ScoLOMFR vocabulary

Complex element, containing several sub-elements (see below).

XML element

lom.technical.extendedLocation

Example

Sample record: #localisationEtendue

```
<scolomfr:extendedLocation>
  <scolomfr:location>
    https://www.effios.fr/cas_gar/allemand5.php
  </scolomfr:location>
  <scolomfr:platform>http://data.education.fr/gar</scolomfr:platform>
  <scolomfr:personalDataProcessType>
    <scolomfr:source uniqueElementName="source">
        SCOLOMFRv2.1
    </scolomfr:source>
    <scolomfr:value uniqueElementName="value">
        http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-044-num-003
    </scolomfr:value>
    <scolomfr:label>
        personnalisation moyenne : les donnÈes transférÈés ne permettent pas
        d'identifier directement l'utilisateur </scolomfr:label>
  </scolomfr:personalDataProcessType>
```

```
    <lom:description uniqueElementName="description">
      <lom:string>
          Attributs GAR : [UAI] Code Ètablissement ; [IDO] Id opaque ;
           [PRO] Profil
      </lom:string>
    </lom:description> …
</scolomfr:extendedLocation>
```

Comments

The "extendedLocation" element contains the elements related to the resource's access terms and the attributes required by the resource to operate within the ERAM framework:

▶ SSO access URL;
▶ requested attributes;
▶ reference to the resource's declaration of conformance.

ERAM constraints

A complete "extended location" element MUST be present for ERAM operation.

In the case of a user resource with a web variant only, the record MUST contain ONLY ONE "extended location" element related to the ERAM, whose platform is that of a web access (see §6.1.13).

In the case of a mixed user resource with a web variant and native variant(s), the record MUST contain ONLY ONE "extended location" element relating to the web variant AND at least ONE "extended location" element relating to a "native application" variant.

In the case of a common technical resource, the record MUST contain ONLY ONE "extended localization" element for an RTC.

6.1.12   URL Access

ScoLOMFR element

4.3.1.1 - Localisation

ScoLOMFR vocabulary

URL. Not part of a controlled vocabulary.

Élément XML element

lom.technical.extendedLocation.location

Example

Sample record: #URL

```
<scolomfr:location>
   https://www.effios.fr/cas_gar/allemand5.php
</scolomfr:location>
```

Comments

The lom.technical.extendedLocation.location element contains the URL to access the resource in the publisher's domain.
ERAM redirects access requests to this URL, which validates the access on the ERAM's Identity Server (IDP) by initiating the SSO transaction.
In the case of a common technical resource, the latter not being accessible via web access, the access URL is ignored.

ERAM constraints

> *This element MUST provide the address to access the resource on the provider's servers that will be used by ERAM.*
>
> *This access URL MUST be unique.*

6.1.13 Platform

ScoLOMFR element

4.3.1.2 - Platform

ScoLOMFR vocabulary

URI of the platform for which the information in the lom.technical.extendedLocation element is defined.

XML element

lom.technical.extendedLocation.platform

Example

Sample record: #UriGar

```
<scolomfr:platform>http://data.education.fr/gar</scolomfr:platform>
```

Comments

ERAM's URI is http://data.education.fr/gar

Comments

> *The platform element takes the value of one of the URI defined for the ERAM, depending on the nature of the resource and/or the variants described. In the case of the description of the web variant of a user resource, this element MUST have the value http://data.education.fr/gar.*
>
> *In the case of the description of the native variant of a user resource, this element MUST have the value " http://data.education.fr/gar/oidc_native ".*
>
> *In the case of a common technical resource, this element MUST be set to " http://data.education.fr/gar/rtc".*

6.1.14 Personal Data (PD) Processing

<u>ScoLOMFR element</u>

4.3.1.3 –Type of personal data required to operate the resource

<u>ScoLOMFR vocabulary</u>

ScoLOMFR controlled vocabulary voc-044

<u>XML element</u>

lom.technical.extendedLocation. personalDataProcessType

<u>Example</u>

Sample record: #typeTraitement

```
<scolomfr:personalDataProcessType>
  <scolomfr:source uniqueElementName="source">SCOLOMFRv8.0 </scolomfr:source>
  <scolomfr:value uniqueElementName="value">
    http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-044-num-003
  </scolomfr:value>
  <scolomfr:label>personnalisation moyenne : les données transférées
  ne permettent pas d'identifier directement l'utilisateur
  </scolomfr:label>
</scolomfr:personalDataProcessType>
```

<u>Comments</u>

In ERAM's functional framework, all accesses are individualized, so it is always possible to indirectly identify a user via the ERAM manager. All resources accessed by ERAM therefore fall into personal data types 3 and 4 of (average or strong personalization), depending on the attributes transmitted.

Type	Personalization level	URL
Type 3	Average personalization: the data transferred cannot be used to directly identify the user	http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-044-num-003
Type 4	Strong personalization: the data transferred can be used to directly identify the person and/or includes details of their civil status or private life	http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-044-num-004

Table 4 - Personal data processing types under ERAM

<u>ERAM constraints</u>

> *The extendedLocation. personalDataProcessType element MUST have a value of Type 3 or Type 4.*

This value MUST be in line with the attributes requested in the next element. If this value is not in line or is missing, the record is rejected.

6.1.15 Description (attributes)

<u>ScoLOMFR element</u>

4.3.1.4 - Description

<u>ScoLOMFR vocabulary</u>

Text field

<u>XML element</u>

lom.technical.extendedLocation.description

<u>Example</u>

Sample record: #DCP

```
<lom:description uniqueElementName="description">
  <lom:string>
    Attributs GAR : [UAI] Code établissement ; [IDO] Id opaque ; [PRO] Profil
  </lom:string>
</lom :description>
```

<u>Comments</u>

The attributes requested are described in the "description" element associated with the "extendedLocation" block describing ERAM access. As this is a text field used by ERAM to collect specific information (the list of attributes requested), it must follow a specific syntax:

  ▸   « Attributs GAR : » as a prefix,
  ▸   followed by the ";" separated list of requested attributes, with their identifying code in square brackets ("[code]") followed by the wording for each attribute.

In case the resources belong to a family, the family-specific attributes must be described in the "GAR:Famille" element (see below, chapter 6.2 - Records describing a family of resources).

The attributes are classified into categories that define the way in which they are sent to the resource provider. Any request for a category 3 or 4 attributes requires using the value http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-044-num-004for PD processing type (strong personalization) (see above).

Code	Title	Multivalued	Category	1D/2D	Description
UAI	School code	N	1	1D/2D	UAI (i.e., Registered Administrative Unit)
idENT	VLE project code	N	1	1D/2D	VLE Project code, encoded in base

IDO	Opaque ID	N	1	1D/2D	Resource-specific user Id, guaranteeing that no personal information can be accessed
PRO	Profile	N	2	1D/2D	Accessor profile Id(s) (PROFIL_NATIONAL: "National_elv" [i.e., national for pupils], "National_ens" [i.e., national for teachers], "National_doc" [i.e., national for librarians], National_aca, etc.)
DIV	Division(s)	Y	3	1D/2D	Code of the division(s) and title of the division(s)
GRO	Group(s)	Y	3	1D/2D	Code of the group(s),and title of the group(s)
DIV_APP	Division(s) of affiliation	Y	3	1D/2D	Code of the group(s), code of the division(s) of affiliation of the group(s), title of the division(s) of affiliation of the group(s),. The attribute DIV_APP does not need to be requested. It is automatically transmitted if the attribute GRO is requested.
E_MS1	Level of education (student)	N	3	1D/2D	Education level code(s) (N_MEF_STAT_1)
E_MS2	Education cycle (student)	N	3	1D/2D	Education cycle code(s) (N_MEF_STAT_2)
E_MS3	Training system (student)	N	3	1D/2D	Training system code(s) (N_MEF_STAT_3)
E_MS4	Training level (student)	N	3	1D/2D	Training level code(s) (N_MEF_STAT_4)
E_MS5	Stream (student	N	3	2D	Stream code(s) (N_MEF_STAT_5)
E_MAT	Courses followed (student)	Y	3	2D	Codes of courses followed, as in the source repositories, + title
P_MAT	Subjects taught (teacher)	Y	3	2D	Codes of subjects taught, as in the source repositories, + title
P_MS1	Level(s) of education (teacher)	Y	3	1D/2D	Teaching level code(s) (N_MEF_STAT_1)
P_MS2	Education cycle(s) (teacher)	Y	3	1D/2D	Education cycle code(s) (N_MEF_STAT_2)
P_MS3	Training system(s) (teacher)	Y	3	1D/2D	Training system code(s) (N_MEF_STAT_3)

P_MS4	Training level(s) (teacher)	Y	3	1D/2D	Training level code(s) (N_MEF_STAT_4)
P_MS5	Stream(s) (teacher)	Y	3	2D	Stream code(s) (N_MEF_STAT_5)
P_MEL	Email address (NOT for students)	Y	4	1D/2D	Email address of teacher or other personnel
CIV	Title	N	4	1D/2D	Mr or Mrs
NOM	Surname	N	4	1D/2D	Last name
PRE	Given name	N	4	1D/2D	First name

Table 5 - List of possible ERAM attributes for an autonomous resource

Every EMS_x and PMS-x contains MS_ values from 1 to x (e.g., E_MS4 contains E_MS1, E_MS2, E_MS3 and E_MS4). As a result, only the highest MS code should be requested. The possible profiles for ERAM users are detailed in Table 13 - Different profiles covered by the target audiences of ERAM subscriptions.

ERAM constraints

The "description" element of "extendedLocation" MUST include the list of requested attributes.

This list MUST strictly conform to the required syntax.

The requested attributes MUST be consistent with the Personal Data Type specified.

Note that the request and transmission of these attributes is subject to rules described in the legal and administrative reference document, and to a functional justification provided in the declaration of conformance.

6.1.16 Description (declaration of conformance)

ScoLOMFR Element

4.3.1.4 - Description

ScoLOMFR Vocabulary

Text field.

XML element

lom.technical.extendedLocation.description

Example

Sample record: #DC

```
<lom:description>
  <lom:string>
GAR : Déclaration de conformité=ARK:/49591/GARcnf#511083743#1575186080287
  </lom:string>
</lom:description>
```

Comments

The declaration of conformance is identified by a specific ark identifier, assigned when the declaration is created on the dedicated online platform.

This reference is linked to the resource(s) it applies to via its entry in the resource(s)'s record. It must be mentioned in the "description" element associated with the "extended location" element. Because this is a text field, it must respect the following syntax:

▶ a prefix "GAR: déclaration de conformité ",
▶ followed by the ARK identifier of the declaration of conformance.

ERAM constraints

The ARK identifier of the declaration of conformance MUST be present in the element lom.technical.extendedLocation.description.string.

6.1.17 Rights

ScoLOMFR Element

6 - Rights

ScoLOMFR Vocabulary

Complex element, containing several sub-components:

▶ *Coût* [Cost] (ScoLOMFR 7.0 element)
controlled vocabulary ScoLOMFR voc-026[5]
▶ *Droits* [Rights] (ScoLOMFR 7.0 element)
controlled vocabulary ScoLOMFR voc-027[6]
▶ *Description* (ScoLOMFR 7.0 element)
Text element.

XML element

lom.rights

lom.rights.cost
lom.rights.copyrightandotherrestrictions
lom.rights.description

Example

Sample record: #droits

```
<lom:rights uniqueElementName="rights">
  <lom:cost uniqueElementName="cost">
```

---

[5] Available at :
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-026 (ScoLOMFR vocabulary 6.0).

[6] Available at :
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-027 (ScoLOMFR vocabulary 6.0).

```
        <lom:source uniqueElementName="source">SCOLOMFRv8.0</lom:source>
        <lom:value uniqueElementName="value">
            http://data.education.fr/voc/scolomfr/concept/no
        </lom:value>
        <lom:label>gratuit</lom:label>
    </lom:cost>
    <lom:copyrightAndOtherRestrictions
uniqueElementName="copyrightAndOtherRestrictions">
        <lom:source uniqueElementName="source">SCOLOMFRv8.0</lom:source>
        <lom:value uniqueElementName="value">
            http://data.education.fr/voc/scolomfr/concept/yes_2</lom:value>
        <lom:label>oui</lom:label>
    </lom:copyrightAndOtherRestrictions>
        <lom:description>
            <lom:string>
            <![CDATA[
Effios, certains droits réservés
Cette création est mise à disposition selon les termes de la licence CC BY SA
version 3
Mentions légales : https://www.effios.fr/ressources/mentions_legales
Mentions d'information RGPD : http://www.effios.fr/ressources/mentions_rgpd
Mentions d'accessibilité : http://www.effios.fr/ressources/accessibilite
Conditions d'utilisation : http://www.effios.fr/ressources/CGU-CGV
]]>
            </lom:string>
        </lom:description>
</lom:rights>
```

Comments

The "rights" element provides all the information on the legal and contractual conditions for using the resource.
It contains three types of information:
- « Coûts (gratuit/payant) » [*Cost (free/paid)]:* this information indicates whether the resource is fee-based or free to the institution/school. Resources made available by the ministry are considered free, even if the resource is publicly funded.
- Droits [*Rights*]: always set to OUI [YES].
- Description:
  - The description contains the following text: « [publisher], all rights reserved/some rights reserved » ;
  - An indication of mandatory/recommended legal information pages: link to the legal information, GDPR information pages, General Terms & Conditions of Use, Accessibility page, etc.

ERAM constraints

The element "Coûts" [i.e., fees] MUST be set to "payant" (paid) for paid resources or "gratuit" (free) for free resources.

The element « Droits » MUST always be set to OUI (YES).

6.1.18   Relationship « Thumbnail »

<u>ScoLOMFR Element</u>

7 - Relation

<u>ScoLOMFR Vocabulary</u>

ScoLOMFR voc-009[7] controlled vocabulary
We use the value « a pour vignette:
http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-009-num-021

<u>XML Element</u>

lom.relation[a pour vignette]

<u>Example</u>

Sample record: #vignette

```
<lom:relation>
  <lom:kind>
    <lom:source>SCOLOMFRv8.0</lom:source>
    <lom:value>
        http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-009-num-021
    </lom:value>
    <lom:label>a pour vignette</lom:label>
  </lom:kind>
  <lom:resource>
    <lom:identifier>
        <lom:catalog>URI</lom:catalog>
        <lom:entry uniqueElementName="entry">
           https://pfv-simulateur-dtr.gar.renater.fr/vignette/vign4.png
        </lom:entry>
    </lom:identifier>
    <lom:description uniqueElementName="description">
        <lom:string>Vignette 300X300</lom:string>
    </lom:description>
  </lom:resource>
</lom:relation>
```

---

[7]   Available at :
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-009 (ScoLOMFR vocabulary 6.0).

Comments

This element specifies the URL used to access the thumbnail (picture associated with this resource and stored by the publisher). The thumbnail is used to represent the resource in the media centre, in combination with the title.

During harvesting, the harvesting module retrieves the URL of the thumbnail proposed by the publisher. ERAM loads the picture, adjusts it to the correct size by inserting it into a 250x250-pixel square (maintaining the proportions), embeds an ERAM "label" into it and stores it in a PNG format.
This prepared thumbnail will be sent to ERAM for display and for no other purposes outside ERAM.
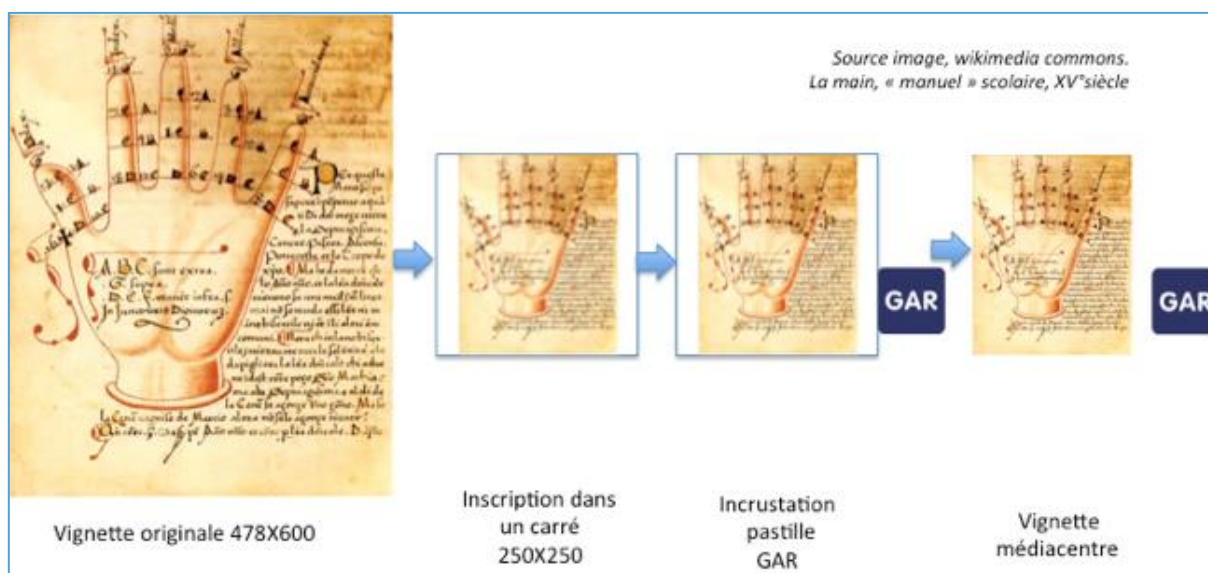
Figure 14 - Example of thumbnail processing

ERAM constraints

The element « relation / a pour vignette » [thumbnail] SHOULD be filled in, with a link to a thumbnail that will be used for display in the media center.

Thumbnails MUST be in PNG, GIF or JPEG format

The URL of the thumbnail MUST be valid and allow for downloading.

If there is no URL or the thumbnail cannot be downloaded, the record will still be accepted. The TDR will receive a notification alert. The resource displayed in the media centre will not contain a thumbnail.

6.1.19 Education field

ScoLOMFR Element

9 - Classification

9.1 - Objectif
9.1.2.6 – Domaine d'enseignement

<u>ScoLOMFR Vocabulary</u>

ScoLOMFR voc-015A controlled vocabulary for agricultural education[8].
Vocabulaire contrôlé ScoLOMFR voc-015GTPX controlled vocabulary for general, technological, vocational and other education[9].

<u>XML Element</u>

lom.classification[domaine d'enseignement]

<u>Example</u>

Sample record: #domaineEnseignement

```
<lom:classification>
  <lom:purpose uniqueElementName="purpose">
    <lom:source uniqueElementName="source">SCOLOMFRv8.0</lom:source>
    <lom:value uniqueElementName="value">
        http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-028-num-003
    </lom:value>
        <lom :label>domaine d'enseignement</lom :label>
  </lom:purpose>
  <lom:taxonPath>
        <lom:source uniqueElementName="source">
          <lom:string>
            SCOLOMFRv3.0 ; scolomfr-voc-015 ; Enseignement
          </lom:string>
        </lom:source>
        <lom:taxon>
          <lom:id uniqueElementName="id">
        http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-015-num-1623
          </lom:id>
          <lom:entry uniqueElementName="entry">
            <lom:string>allemand (LVER)</lom:string>
          </lom:entry>
        </lom:taxon>
        <lom:taxon>
          <lom:id uniqueElementName="id">
        http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-015-num-1460
          </lom:id>
          <lom:entry uniqueElementName="entry">
            <lom:string>
              langues vivantes étrangères ou régionales (cycle 4)
            </lom:string>
          </lom:entry>
```

---

[8] Available at :
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-015A (ScoLOMFR vocabulary 6.0)

[9] Available at :
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-015GTPX (ScoLOMFR vocabulary 6.0).

```
            </lom:taxon>
        </lom:taxonPath>
    </lom:classification>
```

Comments

This information is used to pre-assign the resource. It is sent to ERAM for display in the media centre. This information is also transmitted to VLE operators.

This information is carried by ScoLOMFR elements of the type "classification", with the objective http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-028-num-003 (domaine d'enseignement).
The pre-assignment process offers assignment managers "assignment suggestions", based on the existence of an equivalence between the BCN codes "subjects taught" present in VLE identity data and the ScoLOMFR concepts present in the resource's record.

The ScoLOMFR concepts describing the education fields can be found in the vocabularies voc-015GTPX (general, technical, professional and various other education) and voc-015A (agricultural education). Within these vocabularies, the concepts corresponding to the education fields are grouped under the headings "enseignements par discipline".

Recommendations

The education field concepts are used by the assignment interface to help the assignment managers perform their work, and are also represented in the various media centers, often with search filter functions.
As a general rule, it is recommended to limit the number of concepts indicated in the record.
In addition, only concepts designating subjects can be effectively matched with the "subjects taught" indications provided by VLEs.

Therefore, the index « Domaine d'enseignement » is only for teaching areas that have a BCN "Subject" equivalent in the ScoLOMFR-BCN alignment vocabulary.

The index « Domaine d'enseignement »

- MUST contain only teaching area uri present in the BCN/SCOLOM-FR alignment vocabulary " Domaine d'enseignement / Code matière >voc-015 " ;

- MUST NOT contain more than five concepts with a BCN " Matière " equivalence in the ScoLOMFR-BCN alignment vocabulary. In the event that this number is exceeded, all additional subject area concepts will be ignored and the indexing will be considered non-existent;

- *SHOULD ONLY contain concepts designating subjects (« disciplines »)[10] or subject families (« Familles matières[11] ») in the case of vocational education.*

ERAM Constraints

The record MUST contain at least one value for « Domaine d'enseignement ».

The education field (domaine d'enseignement) SHOULD use ScoLOMFR concepts identified as "enseignement par discipline". Non-subject concepts will not be considered by the pre-assignment process.

6.1.20 Detailed education level

ScoLOMFR Element

9 - Classification
> 9.1 - Objectif
>> 9.1.2.11 - Niveau éducatif détaillé

ScoLOMFR Vocabulary

ScoLOMFR voc-022[12] controlled vocabulary

XML Element

lom.classification[niveau éducatif détaillé]

Example

Sample record: #niveauEducatif

```
<lom:classification>
  <lom:purpose uniqueElementName="purpose">
    <lom:source uniqueElementName="source">SCOLOMFRv8.0</lom:source>
    <lom:value uniqueElementName="value">
        http://data.education.fr/voc/scolomfr/concept/educational_level
    </lom:value>
    <lom:label>niveau éducatif détaillé</lom:label>
  </lom:purpose>
  <lom:taxonPath>
    <lom:source uniqueElementName="source">
        <lom:string>
           SCOLOMFRv8.0 ; scolomfr-voc-021 ; Niveau éducatif détaillé
        </lom:string>
```

---

[10] ScoLOMFR Vocaulary 15, « enseignements par disciplines » (http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-015-num-1835)

[11] ScoLOMFR Vocaulary 15, « domaines d'neseignement professionnels par familles de matières » (http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-015-num-100)

[12] Available at https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-022 (vocabulaire de la v6.0 de ScoLOMFR, en attendant la mise à jour du navigateur d'ontologie).

```
        </lom:source>
    <lom:taxon>
        <lom:id uniqueElementName="id">
    http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-022-num-020
        </lom:id>
        <lom:entry uniqueElementName="entry">
            <lom:string>5e</lom:string>
        </lom:entry>
    </lom:taxon>
  </lom:taxonPath>
</lom:classification>
```

Comments

The element « niveau éducatif détaillé » (detailed education level) is used by ERAM in the pre-assignment process. This information is also transmitted to VLE operators.

This information is carried by ScoLOMFR elements of the type "classification", with the objective http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-028-num-003 (domaine d'enseignement).

The pre-assignment process offers assignment managers "assignment suggestions", based on the existence of an equivalence between the BCN codes "subjects taught" present in VLE identity data and the ScoLOMFR concepts present in the resource's record.

These equivalencies are available only for grade level information per year:
▶ Elementary school [*école élémentaire*] : CP, CE1, CE2, CM1, CM2 ;
▶ Middle school [*collège*] : 6°, 5°, 4°, 3° ;
▶ Vocational middle school [*collège professionnel*] : 4° pro, 3° pro ;
▶ General and technological high school [*lycée général et technologique*] : 2° GT, 1° GT, T GT
▶ Vocational high school [*lycée professionnel*] : 2° pro, 1° pro, T pro, voie BEP, BMA 1° année, BMA 2°année, BP 1° année, BP 2°année, BT 1°, BT T, BTM 1° année, BTM 2°année, CAP 1° année, CAP 2° année ;
▶ Higher education in high school [*enseignement supérieur en lycée*] : BTS 1° année, BTS 2° année, DUT 1° année, DUT 2° année, CPGE 1° année, CPGE 2° année.

Generic mentions (college, high school, …) and cycle information are not taken into account.

ERAM constraints

The record MUST have at least one value for « Niveau éducatif détaillé ».

The detailed educational level SHOULD use the ScoLOMFR concepts identified as grade level by year. Concepts other than grade level by year will not be taken into account by the pre-assignment process.

6.1.21 ERAM Label

<u>ScoLOMFR Element</u>

9 - Classification
    9.1 - Objectif
        9.1.2.8 – Label de la ressource

<u>ScoLOMFR vocabulary</u>

Vocabulaire contrôlé ScoLOMFR voc-045[13]

<u>XML Element</u>

lom.classification[label]

<u>Example</u>

Sample record : #label

```
<lom:classification>
  <lom:purpose uniqueElementName="purpose">
    <lom:source uniqueElementName="source">SCOLOMFRv8.0 </lom:source>
    <lom:value uniqueElementName="value">
    http://data.education.fr/voc/scolomfr/concept/scolomfr-voc-028-num-013
    </lom:value>
    <lom:label>label</lom:label>
  </lom:purpose>
  <lom:taxonPath>
    <lom:source uniqueElementName="source">
        <lom:string>SCOLOMFRv8.0 ; scolomfr-voc-043 ; Label</lom:string>
    </lom:source>
    <lom:taxon>
        <lom:id uniqueElementName="id">
           http://data.education.fr/gar
        </lom:id>
        <lom:entry uniqueElementName="entry">
           <lom:string>GAR</lom:string>
        </lom:entry>
    </lom:taxon>
  </lom:taxonPath>
  <lom:description uniqueElementName="description">
    <lom:string>GAR_Présentation : [MAN] manuels numÈriques</lom:string>
  </lom:description>
</lom:classification>
```

<u>Comments</u>

The ERAM label is used as a selector for the OAI harvesting datasets. It is mandatory and is checked by the harvesting module.

---

[13] Consultable à l'adresse
https://www.reseau-canope.fr/scolomfr/data/scolomfr-6-0/fr/page/?uri=http%3A%2F%2Fdata.education.fr%2Fvoc%2Fscolomfr%2Fscolomfr-voc-045 (vocabulaire de la v6.0 de ScoLOMFR, en attendant la mise à jour du navigateur d'ontologie).

In order to be labeled "ERAM", the record must contain the "Classification" element as presented in the sample record.

In this element, and in order to facilitate the implementation of the display process in the VLE media center, the "description" tag associated with the ERAM label MUST mention the resource's "presentation type", in the form of a unique value from the list provided below.

Code	Description
[DIC]	reference resources, dictionaries and encyclopaedias
[DOC]	Documentary and press resources
[MAN]	Digital textbooks
[MUL]	Multimedia resources
[ORI]	Professional guidance resources
[PRO]	Pedagogical production resources
[ACC]	School training and tutoring resources

Table 6 - Resource presentation types

One of the following syntaxes must be used:
- GAR_presentation: [value]
- GAR_présentation: [value]

ERAM constraints

> *The "description" element of the "label" classification objective MUST contain the presentation type, which MUST be a single value from the table above.*
>
> *If the value is missing, or if several values are indicated, the record will be rejected.*

6.2 Records describing resources part of a Family of resources

6.2.1 Family of resources

In certain cases (depending on editorial choices), several resources can be combined into a consistent whole that can share certain information in order to offer specific services to users accessing these resources.
For example:
- A unified search portal using a defined set of content resources
- A "personal workspace" service covering several digital content resources, for storing the work of a pupil or teacher and/or usage data
- A storage environment shared by several versions of a resource (e.g., a background service shared by different versions of a digital manual (Web, Android, iOS, etc.)
- A dictionary for use in a set of manuals.

The constitution of a "family" allows these transfers of information, by providing two specific attributes:

▸ The complementary identifier: IDC
▸ The list of designated resources: LRA.

> *The constitution of a family, and in particular the attribution of the IDC, MUST meet a functional need, in accordance with the CNIL's recommendation on this subject.*
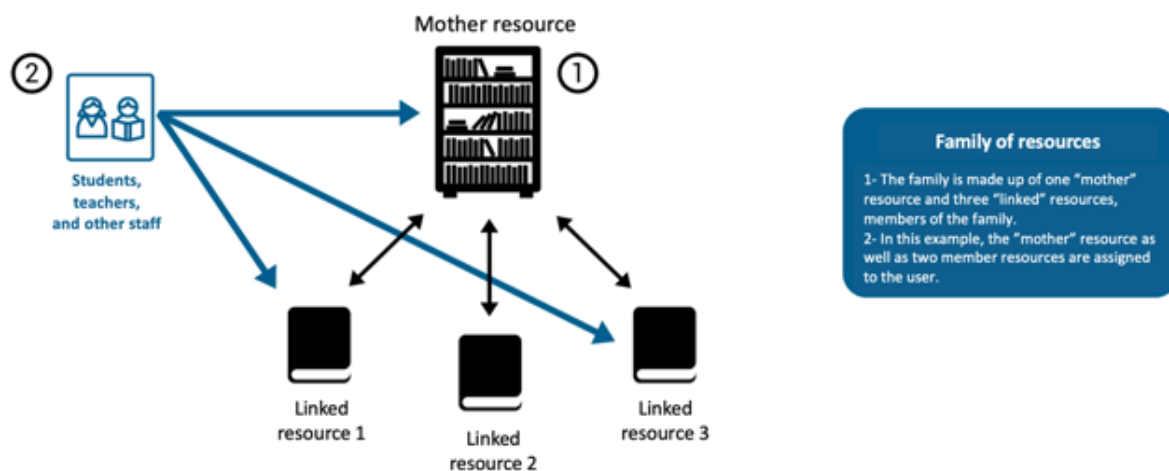
Figure 15 - Families of resources and assignment processes

6.2.2   Definitions

Family of resources

The term "family of resources" is used to designate a set of resources that share a common set of information or services and are organized as such through a specific ScoLOMFR description.

Autonomous resource

The term « autonomous resource » is used to designate resources without any links between each other, that do not belong to any family of resources.

Linked resource

The term « linked resource » is used to designate any resource belonging to at least one family. Resources belonging to the same family are said to be « linked » between one another, as they can share a certain amount of information.

« Mother of family » resource

Every family relies on a resource called « Mother of family », which provides the composition of the family.

Family-specific attributes

In addition to attributes specific to each resource (cf below, paragraphe 5.2.6.3 et suivants, DCP), a family of resources can request two family-specific attributes:

▶ The complementary ID (IDC): it is communicated as an attribute during SSO access to every resource of the family ; it is unique for a user and a family of resources ; it can be requested only in the record of the "mother of family" resource, but is transmitted whenever one of the linked resources is accessed.

▶ The list of called resources (LRA): this attribute contains the call URL of every family resource that can be called from the resource during a session. These URLs are filtered so that only the resources assigned to the user are displayed.

Code	Title	Description
IDC	Identifiant complémentaire (Complementary ID)	[Family_ID][Mother of family IDO]
LRA	Liste des ressources appelées (List of called resources)	List of URLs of other resources in the family that are « called » by the resource and assigned to the user.

Table 7 - Family-specific attributes

Case study

In figure 2 above, when accessing linked resource 1, the following attributes are transmitted :

▶ Attributes requested for linked resource 1,
▶ The family IDC, if it has been requested in the "mother of family" resource's record,
▶ The URL of other linked resources that can be called by resource 1 (in this example, the mother of family and linked resource 3).

Display or Non-display Nature of the Resource

Linked resources are primarily intended to offer services that provide or simplify the use of the content within their scope. Some of these services run in the background in the form of exchanges between applications.

If these resources do not possess a UI, they are said to be "non-display" resources. They do not appear in the user's media center.

6.2.3 Describing a family of resources

The declaration of a family is done through ScoLOMFR records which describe a family's linked resources and the 'mother of family' resource.

These records are similar to that of independent resources described in the previous chapters, but include a set of supplementary elements in a specific 'ERAM : Family' field (« GAR : Famille »), defined in a « description » of the element « localisation étendue » .

ScoLOMFR Element

4.3.1.4 - Description

ScoLOMFR Vocabulary

Text field

XML Element

lom.technical.extendedLocation.description

Example

Sample record: #famille

```
<lom:string>GAR:Famille
GAR:RessourceAffichable = true
GAR:MembresFamille = ark:/49591/FArtsMFVGa.p ; ark:/49591/FartsFFMus.p ;
ark:/49591/FartsFFCirq.p
GAR:AttributsFamille = [IDC] Identifiant complémentaire ; [LRA] Liste des
ressources appelées ;
GAR:IdRessourcesAppelantes = ark:/49591/FartsFFMus.p ;ark:/49591/FartsFFCirq.p
GAR:IdRessourcesAppelees = ark:/49591/FartsFFMus.p ;ark:/49591/FartsFFCirq.p
</lom:string>
```

A set of records describing a family is provided in the accompanying documents.

Comments

The family-specific information is located in the element extendedLocation »
(lien_chapitre_notice) of the ScoLOMFR record, after the description of ERAM attributes.
The text block 'GAR : Famille' contains the following information:

Property	Description	Expected value	Default value
GAR:RessourceAffichable	Indicates whether the resource is displayable	true ou false	false
GAR:MembresFamille	IDs of the family's members. The presence of this property indicates that the resource is a 'mother of family'.	List of Ids separated by semicolons (« ; »)	Empty list
GAR:AttributsFamille	Family attributes. Only the 'mother of family' can contain the IDC attribute.	List of attributes separated by semicolons (« ; »)	Empty list
GAR:IdRessourcesAppelantes	IDs of the calling resources	List of resource IDs separated by semicolons (« ; »)	Empty list
GAR:IdRessourcesAppelees	IDs of the called resources	List of resource IDs separated by semicolons (« ; »)	Empty lsit

Table 8- « GAR:Famille » text block structure

6.2.4 Declaration of the 'Mother of family' resource

▸ It is the presence of the text element « GAR :MembresFamille » that defines a resource as a « Mother of family ».
▸ The IDC attribute can be requested only for the « Mother of family » resource. It will be communicated for each SSO access to any member resource.
▸ The title of the resource must contain "Mère de famille" [Mother of family]
▸ The elements « GAR :IdRessourcesAppelantes » (Calling resources IDs) et « GAR :IdRessourcesAppelées » (Called resources IDs) must be present, as for member resources.

6.2.5 Declaration of a linked resource

▸ The record of a linked resource must contain the following elements:
  • GAR:AttributsFamille
  • GAR:IdRessourcesAppelantes
  • GAR:IdRessourcesAppelees
▸ GAR:RessourceAffichable is optionnal. If it is absent, the default value « false » will be applied.

6.2.6 Constraints

Structure of the family

In order for a family of resources to operate correctly, there must be coherence between different lists:
▸ The list of family member resources, present in the record of the 'mother of family' resource, must be strictly equivalent to the list of resources linked to the mother of family (list of calling / called resources).
▸ Each link to a calling resource must match a reciprocal link 'called resource' in the corresponding record.
▸ Each linked to a called resource must match a reciprocal link 'calling resource' in the corresponding record.

Assignments

The "mother of family" resource must in all cases be subscribed and assigned.
This resource is in fact the one that concentrates the most important exploitation and conservation of personal data. It must therefore be the subject of an informed choice for the institution/school.

Compliance with the CNIL record

The use of a family, and in particular the assignment of the complementary identifier (IDC), is a major point of application compliance. CNIL deliberation No. 2017-253 of September 21, 2017

sets out the principles for the existence of a complementary identifier common to several resources.

> *"[...]The Commission considers that it would then be up to the Administrative Manager to complete its analysis of the proportionality of requests for access to personal data for an assessment, for each group of resources, of the appropriateness of using an "opaque identifier" common to a group of resources rather than an "opaque identifier" specific to each resource. The Commission notes the Ministry's commitment to carry out such a review and to allow the same "opaque identifier" only if there is a proven need, such as, for example, the provision of highly personalized services to the student or teacher, for the duration of the subscription only.*
> *In any case, the Commission considers that the use of an "opaque identifier" identical for all providers should not be allowed insofar as it could lead to the creation of a unique identifier for the student that would be available to private organizations. It notes the Ministry's commitment on this point. [...]. "*

Any request for the constitution of a family MUST therefore be accompanied by a justification of the aforementioned need for a common identifier for the family's resources, included in the declaration of conformance, in accordance with the terms of the CNIL's opinion and in compliance with the principle of proportionality of data.

6.3 User resource records with native variants

6.3.1   Description

A mixed user resource is an ERAM resource accessible via a web browser and via one or more native applications (see detailed description in §4.1.3). The declaration of access to these native applications is made in the resource record.

6.3.2   Declaration

The declaration of a native variant of a mixed user resource is made by adding an extendedLocation element, whose platform element takes the value http://data.education.fr/gar/oidc_native, and whose description element includes a text field "GAR:OIDC_Native".

ScoLOMFR element
4.3.1 - Extended Location

ScoLOMFR vocabulary

Complex element, containing several sub-elements.

<u>XML element</u>
lom.technical.extendedLocation

<u>Example</u>
Record example : #native

```
<scolomfr:extendedLocation>
  <scolomfr:location>

  </scolomfr:location>
  <scolomfr:platform>

  </scolomfr:platform>
  <scolomfr:personalDataProcessType>
    <scolomfr:source uniqueElementName="source">SCOLOMFRv2.1</scolomfr:source>
    <scolomfr:value uniqueElementName="value">

    </scolomfr:value>
    <scolomfr:label>
        personnalisation moyenne : les données transférées ne permettent pas
d'identifier directement l'utilisateur
    </scolomfr:label>
  </scolomfr:personalDataProcessType>
  <lom:description uniqueElementName="description">
    <lom:string>Attributs GAR : [UAI] Code établissement ; [IDO] Id opaque ;
[PRO] Profil</lom:string>
    <lom:string>GAR:OIDC_Native
        GAR:RedirectUri = apptest://openid/oauthredirect/AmanAll5
        GAR:ClientId = f95b7651-9abc-4451-bc1d-2323acfc2a1e
        GAR:ClientName = AppNatClientName
    </lom:string>
  </lom:description>
</scolomfr:extendedLocation>
```

A record describing a native variant is provided in the accompanying zip of examples associated.

<u>Comments</u>
The elements of the native variant are located in the "extendedLocation" element (cf.6.1.11) of the ScolomFR record, after the declaration of the attributes.

The "GAR:OIDC_Native" text block includes the following data, all of which are mandatory and unique in ERAM :

Property	Description	Expected value	Default value

	Unique URI to access the native variant, this is also the callback URI used during the authentication process	URI	Empty
GAR:RedirectUri			
GAR:ClientId	Unique identifier of the native variant	UUID version 4	Empty
GAR:ClientName	Unique name identifying the native variant	Text without spaces	Empty

Table 9 -Components of the "GAR:OIDC_Native" text field

6.4 Records describing common technical resources

6.4.1 Description

A shared technical resource (RTC) is a specific ERAM resource whose description is detailed in § 4.1.4.

6.4.2 Declaration

The declaration of an RTC resource is made by adding an extendedLocation element, whose platform element takes the value http://data.education.fr/gar/rtc.

ScoLOMFR element
4.3.1 - Extended Location

ScoLOMFR vocabulary
Complex element, containing several sub-elements.

XML element
lom.technical.extendedLocation

Declaration of the link between an RTC and a user resource
The declaration of the link between an RTC and one or more user resources is made through a text field " GAR:IdRessourcesAppellants ", carried by a "description" element of the "extended location" element of the record describing the RTC, following the declaration of the ERAM attributes.
The text field "GAR:CallingResourceId" includes the list of user resource identifiers (ark) separated by ";".

Example
```
Record example : #rtc<scolomfr:extendedLocation>
```

```
    <scolomfr:location>

    </scolomfr:location>
    <scolomfr:platform>.education.fr/gar/rtc</scolomfr:platform>
    <scolomfr:personalDataProcessType>
       <scolomfr:source uniqueElementName="source">SCOLOMFRv7.0 </scolomfr:source>
       <scolomfr:value uniqueElementName="value">

       </scolomfr:value>
       <scolomfr:label>
            personnalisation moyenne: les données transférées ne permettent pas
d'identifier directement l'utilisateur
       </scolomfr:label>
    </scolomfr:personalDataProcessType>
    <lom:description uniqueElementName="description">
       <lom:string>
            Attributs GAR: [UAI] Code établissement ; [IDO] Id opaque ; [PRO]
Profil
       </lom:string>
       <lom:string>GAR:IdRessourcesAppelantes = ark:/49591/AmanAll5.p</lom:string>
    </lom:description>
</scolomfr:extendedLocation>
```

A record describing an RTC is provided in the accompanying zip of examples.

6.4.3   Constraints

Extended location
A record describing an RTC must contain only one "extendedLocation" element relating to ERAM (see §6.1.11).
An RTC cannot be a member of a family. Only one GAR:CallingResourceId tag is allowed.

Link between RTC and user resource
The user resource(s) linked to an RTC must all exist in the ERAM.

Title of the record
The title of an RTC record must begin exactly with "[RTC]" (see §6.1.2).

ERAM label
The value of the "description" element of the "label" classification objective of an RTC resource must be "[PRO] educational production resources" (cf. 6.1.21).

6.5 Naming and identification of records on different platforms

Once the integration with ERAM is complete, a resource provider partner has access to two environments and therefore two types of records:
▶   the record of the resource accessible on the production platform;

▸ the record(s) of the resource(s) accessible on the partner testing platform.

6.5.1 Nominal record: Publisher production version and ERAM production platform

When a resource is in production, its record must:
- ▸ include the validation date (date of the [technical validator] role element);
- ▸ point to an extendedLocation.location URL address providing access to the resource and, therefore, using the ERAM production platform's authentication server to validate all access.

6.5.2 Support and monitoring record: Publisher Production version and ERAM Partner Platform

Version	Record	Identifier (ark)
Publisher production /ERAM production platform (PFPROD)	[publisher][title or Id].xml	Ark:/49591/f54x54g11
Publisher production /ERAM partner testing platform (PFPART)	[publisher][title or Id]_p.xml	Ark:/49591/f54x54g11.p
Publisher pre-production / ERAM partner testing platform (PFPART)	[publisher][title or Id]pp.xml	Ark:/49591/f54x54g11.pp

Table 10 - Identification of record variants

Another record must be kept throughout the ERAM linkage phase, in order to allow access to the publisher's production version of the resource on ERAM's partner testing platform. This is important in particularly to test the resource's conformance with ERAM constraints prior to its validation, but also to provide support during the operating phase.

This record provides access to the publisher's production version via the ERAM partner testing platform.

- ▸ it does not have a validation date;
- ▸ it points to an extendedLocation.location URL address that provides PFPART access to the resource and so uses the ERAM partner platform's authentication server to validate all access.
- ▸ it has the same ark identifier as the production resource, but with a ".p" suffix;
- ▸ the file name has a suffix " _p ";
- ▸ the title also has a "_p" suffix.

6.5.3 Upgrade record: Publisher pre-production version and ERAM partner testing platform

Partners can optionally set up another record providing partner platform access to a publisher pre-production version, notably for development and upgrade testing.

This record gives access to the publisher's pre-production version of the resource from ERAM's partner testing platform.

▶ it does not have a validation date;
▶ it points to an extendedLocation.location URL address that provides PFPART access to the pre-production resource and so uses the ERAM partner platform's authentication server to validate all access;
▶ It has the same ark identifier as the production resource, but with a ".pp" suffix;
▶ the file name has a suffix " _pp " ;
▶ the title also has an "_pp" suffix.

6.5.4 Identifying the different records describing the resource during hanging

The warehouse used is currently configured so that the name of the .xml file is used to construct the record's OAI. identifier of the record. It is proposed to use a standardized naming scheme when managing the different records required for a resource. It is also recommended that standardized identifiers be used for records.

▶ Records pointing to the partner testing platform (publisher production or pre-production) are in fact specific versions of the nominal record;
▶ these records are distinguished by a suffix appended to the file name (_p or _pp);
▶ the identifier also has a suffix, in accordance with the ark syntax if this identification system is used (.p or .pp, the separator "." indicating an ark variant).

Only the nominal record [publisher][title or Id].xml can enter production use. It is the only one that MUST have a valid validation date once the tests carried out on the partner testing platforms are complete.

The " _p " and " _pp " records MUST NOT have a validation date.

7 Harvestable warehouse

In order to be integrated with ERAM, the records produced in ScoLOMFR format must be deposited on a warehouse that will be harvested periodically by ERAM.
TDRs can ask to benefit from the shared warehouse proposed by ERAM or set up their own warehouse and ask for direct harvesting by ERAM.
The harvesting is done according to the OAI-PMH protocol.

7.1 Shared warehouse

ERAM provides a shared warehouse hosted by the Polytechnic University of Hauts-de-France (Valenciennes) for resource providers who wish to use it. To benefit from this service, TDRs can provide their records via a ticket on the ERAM linkage support tool (Mantis), addressed to the administrative manager, who will be responsible for integrating them into the warehouse.

7.2 Using third-party warehouses managed by resource providers

It is possible for ERAM to set up a third-party harvesting warehouse managed directly by a resource provider.
This requires the resource provider to provide the data needed for the warehouse data to be harvested and to designate a data warehouse manager.
The data warehouse manager receives notifications regarding the harvesting of the OAI-PMH warehouse itself (notably, if any records are rejected by the OAI-PMH harvester); the TDR receives all harvesting and record processing notifications.
Warehouses set up by resource providers (usually TDRs) can have two different organizations:
- a single warehouse with two "sets," one for the PFPART, the other for the PFPROD ;
- two different warehouses, one for PFPART records, the other for PFPROD records.

The linkage of a third-party warehouse must be conducted in partnership between the TDR and the ERAM technical manager.

Data required to declare a third-party warehouse

To declare a warehouse, the resource provider must provide the ERAM technical manager with the information detailed below.

Data	Observations
Entity hosting the warehouse - Short code	Administrative information used to identify a warehouse during record harvesting. Maximum 50 characters.
Entity hosting the warehouse - Name	Administrative information indicating the OAI-PMH name of the warehouse.
Warehouse URL	Warehouse access URL used for harvesting.
Record format	Value to use for the OAI warehouse request's "metadataPrefix" parameter. Regardless of which value is used, the records must conform to the supported ScoLOMFR schemas. Example: 'Lom', 'oai_scolomfr'.
Granularity type	Type of granularity used by the warehouse for the management of the versions of the records. date : daily version management (YYYY-MM-DD) dateTime : version management by time stamp (YYYY-MM-DDThh:mm:ssZ)
Harvesting type	Full or partial harvesting Full harvesting: harvesting retrieves all records in the warehouse. Partial harvesting: harvesting only retrieves records updated since the last harvesting.
Set for ERAM	Optional set parameter of the OAI allowing to filter on the records. Example "ERAM".
Technical contact Civility Last name First name Email address Phone number	Information about the technical manager of the warehouse. The first name and last name can be used for notifications. The email address will be used to create the user account on the ERAM portal. The phone number must be provided in international format.

Table 11- Data Required to Report a Third-Party Warehouse

Applicable Principles

> *Each repository manager MUST ensure the quality of the service provided for metadata exposure.*

> *Each resource provider MUST ensure the quality of the records they place in the defined data warehouse for harvesting by ERAM.*

8 Subscriptions Web Service

8.1 Overview

ERAM's Subscriptions web service allows the CDR to distribute its user resources to the institutions/schools that have ordered them.

The user resources are distributed by informing ERAM of the subscriptions concluded with the institutions/schools, via a specific web service, the Subscriptions web service.

The entity in charge of placing the subscriptions is the CDR mentioned in the record, in line with that declared in the ERAM registration file.

Principles of the Subscription Webservice

Commercial distributors of resources can manage their ERAM subscriptions through the Subscriptions webservice, which allows to:
- Add subscriptions,
- Modify subscriptions,
- Delete subscriptions.
CDRs can also recover the list of establishments connected to ERAM. They are informed directly in the response to their calls for each action.

Figure 16 - Principles of the subscriptions web service

Via the web service, the CDR communicates to ERAM the information needed to distribute the resource:

▶ subscription duration;
▶ institutions/schools involved
▶ type of assignment;
▶ number of licenses;
▶ etc.

The Subscriptions web service provides several functions necessary for managing subscriptions:

▶ add a subscription;
▶ modify a subscription;
▶ delete a subscription;
▶ retrieve information on existing subscriptions;
▶ consult the list of institutions/schools connected to ERAM.

8.2 Main parameters of the Subscriptions web service

8.2.1 Subscription duration

All dates must be in accordance with the ISO 8601 standard.
The start date of the subscription is a mandatory parameter.
For the end of the subscription, there are two options:
- ▸ a fixed date (ISO 8601) ;
- ▸ an expiration date at the end of the school year.

In the latter case, the subscription will expire on the end date of the school year for which it was made.
This date is configured in ERAM. It is set to August 15, 23:59:59 to take into account the different school calendars of Metropolitan France and overseas territories.
When a subscription expires, accesses are immediately cut for all users.
For subscriptions covering multiple school years (up to a maximum of ten), when the school year changes, all digital copies used become available again and can be assigned to new users, regardless of the subscription's assignment category.
The duration of a subscription can be extended at any time, up to a maximum of ten school years from the beginning of the subscription.

> *Choosing a date-based subscription can lead to loss of assignments during the year, which is a serious disruption to the use of resources and a significant burden on support and resource assignment staff.*
>
> *It is strongly recommended that, wherever possible, subscriptions be defined by school year(s).*
>
> *If date-based subscriptions are maintained, the CDR is encouraged to modify the existing subscription (extension) rather than issue a new subscription. This method avoids the need for the institution to reassign resources during the school year.*

8.2.2 Transferability

In the latest versions of ERAM, only the **transferable** category is available for subscriptions. With this category, changes in resource assignments can be made freely by the institution/school, in accordance with the subscription made, for instance in the case of a student changing classes at the beginning of the school year.

8.2.3 Schools involved

A subscription can be created for a school or a list of schools, defined by their UAI codes.

8.2.4 Type of assignment

It is possible to create subscriptions according to two types of assignment:
- ▶ **Individual:** In this case, the school will be able to distribute the copies individually;
- ▶ **Institutional:** In this case, the institution/school will be able to distribute copies to all members of an audience, but will not be able to manage access individually.

In the case of an institutional assignment, all new students/teachers will be automatically assigned the resource.
In the case of an individual assignment, new students/teachers will receive a suggested assignment, but the assignment will need to be made by the school's assignment manager.

> *The use of "institutional" assignments must be strictly limited to general purpose resources. Indeed, many complaints have been received that when specific resources are distributed using institutional assignments, the users' media centers are cluttered with unnecessary resources.*

8.2.5 Number of copies and target audience

The ERAM subscriptions are defined on the basis of audiences. When accessing resources, the user presents himself with a "profile" transmitted during the SSO transaction in the attributes (PRO attribute). The profile information is provided to the ERAM by the VLE, based on the definition of profiles in the SDET.

The commercial resource distributor can create a subscription that addresses any target audience managed in ERAM:
- ▶ students;
- ▶ teachers ;
- ▶ documentalists,
- ▶ Other school staff (school management staff; administrative, technical, supervisory or service staff working in the school; local authority staff, etc.).

Public (subscription)	Type of public	User profile (SSO attribute [PRO])	Type of profile
STUDENT	Student	National_elv	Student
TEACHER	Teacher	National_ens	Teacher
DOCUMENTALIST	Documentalist	National_doc	Documentalist, documentalist teacher (not available in 1D)

OTHER STAFF	Management staff	National_dir	Head of school, management team
	School life staff	National_evs	Educational advisor, principal educational advisor
	Administrative, technical and service staff	National_eta	Administrative and laboratory personnel, AED, AVS, AESH, etc.
	Community staff	National_col	Community staff working in a facility
	Academic Staff	National_aca	Staff in charge of an academic support mission, not attached to an educational institution.

Table 12 -Different profiles covered by the target audiences of ERAM subscriptions

The commercial distributor may define:
- ▶ a specific number of copies for each of the target audiences defined in the subscription (nbLicenceEnseignant [number of licenses for teachers], nbLicenceEleve [number of licenses for students], nbLicenceProfDoc [number of licenses for documentalists], nbLicenceAutrePersonnel [number of licenses for other staff]) ;
- ▶ or a common number of copies for all target audiences (nbLicenceGlobal). In this case, the copies are shared between the different target audiences.

It is possible to increase the number of copies of a subscription at any time, by modifying the subscription.

The number of copies can be set to UNLIMITED for resources distributed under a license valid for the entire school.

8.2.5.1 Access for non-teaching staff

Non-teaching personnel are referred to generically as "OTHER PERSONNEL." The DTR is responsible for the implementation of the OTHER PERSONNEL accesses. The DTR will work with the publisher to develop specific functionality for each profile.

To allow access to non-teaching staff, it is necessary to:
- provide a subscription with the OTHER PEOPLE audience;
- open access to the resource when the user has a National_dir, National_evs, National_eta, National_col, National_aca profile.

For reasons of simplicity, resource providers have sometimes chosen to provide Teacher access whenever the profile is different from National_elv.

However, it may be appropriate to define specific functionalities for certain profiles, for example functions for designating the person responsible for the administration of the resource or for authorizing publication by the head teacher.

8.2.5.2 Special case of multi-profile users

Generally, staff are associated with a single profile, within an UAI.
However, in specific situations, some staff may have several profiles, corresponding to several specific functions. If these profiles correspond to different UAI, only the profile associated with the UAI will be provided. If, on the other hand, the user has several functions within the institution (for example, a teacher may also have an academic mission, a librarian may have a teaching mission, etc.), the ERAM attributes provided at the time of the SSO session may include several profiles.

This is an exceptional situation in public education, but it may be more frequent in private schools, for example with the combination of management and teaching, teaching and school life, etc.
In order to respond to this type of situation, it is essential to define a policy for managing cases of multi-profile users.

If the resource does not have any special features for OTHER PEOPLE, it may be possible to grant teacher access whenever the content of the profiles is different from National_elv (students).
On the other hand, if the resource offers differentiated functionality based on the profile, it will be necessary to define an order of priority to determine the version offered.
   ▸ In the most general case, it will be necessary to distinguish between student monitoring functions for the teacher profile, and access to the resource without student monitoring for the others. it will then be appropriate to open the teacher version as soon as the National_ens profile is present in the [PRO] attribute.]
   ▸ In more complex situations, for example if the management staff are required to perform specific functions (e.g. authorize publication for a given content, or designate other staff to administer the resource), it may be necessary to propose a profile choice at the time of access.

8.2.6 Reusing IDs from deleted subscriptions

When a subscription is deleted or expired, it is assigned a new automatically generated subscription ID prefixed with the character "_". This allows resource providers to reuse the same deleted/expired subscription IDs when creating new subscriptions.
At the ERAM portal and Subscription web service level, expired or deleted subscriptions are recognizable by the "_" prefix in their subscription ID.

8.2.7 Resource project code associated with a subscription

Resource providers can create or modify subscriptions by indicating the "Resource Project" code to which that Subscription is attached.
This "resource project" code is defined by the "Resource Project Sponsor", for example, in the context of a public resource contract. The project owner must then communicate this code to the ERAM team (dne-gar@education.gouv.fr). After validation by the ERAM team, the resource project owner asks the distributors of each resource project to integrate this project code into their subscriptions.

In this case, the XML flow of subscription will evolve to integrate the resource project code information relevant to the subscription. However, the resource project code information remains optional and does not affect the creation or modification of subscriptions that do not contain this data.
Note: Resource project holders will have access to this information via the ERAM portal as of ERAM since 6.1 (June 2022).

8.3 Authentication of access to the Subscriptions web service (certificate)

In order to use the subscriptions web service, resource providers must present a certificate issued by the certification authority of the Ministry of Education, in order to guarantee the traceability of the client/server authentication.
This certificate must be requested from the technical manager of ERAM, via the transmission of a CSR (Certificate Signing Request).
The certificate request procedure is described in Chapter 14 (Provision of Technical Information).

8.4 Description of the Subscriptions web service

8.4.1 Subscription object

The data describing the subscriptions exchanged via the web service must be in XML format.
The "subscription" object is used to create, modify or delete a subscription.

Fields	Description	Format	Required	Mult.
idAbonnement	The Subscription-id MUST be unique.	String (45 max.)	yes(RG14)	no
commentaireAbonnement	Subscription detail Free wording for the CDR	Character string (255 max.)	no	no
idDistriuteurCom	Identifier of the commercial	Character string	yes(RG3)	no

Fields	Description	Format	Required	Mult.
	distributor for ERAM. It is composed from the SIREN and ISNI data of the CDR.	(26) The format is [SIREN]_[ISNI]		
idRessource	Identifier of a publisher's resource given by the naming authority (id contained in the ScoLOMFR record).	String (1024 max.)	yes	No
typeIdRessource	Type of resource identifier (ark)	String (50 max.)	yes	No
libelleRessource	Title of the resource of a publisher subject of the subscription (title element of the ScoLOMFR record).	String (255 max.)	yes	No
debutValidite	Start date of the validity of the license.	Date, au format ISO 8601. AAAA-MM-DD	yes(RG7)	No
finValidite	Date of the end of validity of the license.	Date, au format ISO 8601 AAAA-MM-DD	non(RG7, RG9)	No
anneeFinValidite	School year in which the validity of the license ends.	String (45)	no(RG7, RG9)	No
uaiEtab	UAI of the institution or school. In the case of a list of institutions/schools, the uaiEtab element is repeated.	String in upper case without accents (45 max.)	no (RG2)	yes
codeNatureUAI	Code of the nature of the UAI (nomenclature N_NATURE_UAI). Values separated by ",".	String (45)	no (RG2)	yes
categorieAffectation	Category of assignment in ERAM: "transferable"	String (45 max.)	yes	No
typeAffectation	Type of assignment in ERAM ETABL : for Institution/School INDIV : for Individual	String (45 max.)	yes	No
nbLicenceEnseignant	Number of teacher licenses. Possible values: Number or "UNLIMITED"	String (8 max.)	no (RG1)	No
nbLicenceEleve	Number of student licenses. Possible values: Number or "UNLIMITED"	String (8 max.)	no (RG1)	No

Fields	Description	Format	Required	Mult.
nbLicenceProfDoc	Number of teacher-documentalist licenses. Possible values: Number or "UNLIMITED	String	no (RG1)	No
nbLicenceAutrePersonnel	Number of other personnel licenses. Possible values: Number or "UNLIMITED	String	no (RG1)	No
nbLicenceGlobal	Number of global licenses. Possible values: Number or "UNLIMITED	String	no (RG1)	No
publicCible	Target audience of the assignment Possible values: TEACHER STUDENT DOCUMENTALIST OTHER STAFF	String	yes	yes
codeProjetRessource	Resource project code	String (50)	No	no

Table 13-- Subscriptions Web Service - Description of the "subscription" object

8.4.2 Management rules

Rule	Description
RG1	To define the number of licenses for a subscription, two types of configurations are possible: - Either only the field "nbLicenceGlobal" is filled in, providing licenses applicable to all the audiences mentioned in PublicCible (in this case, the fields nbLicenceEnseignant, nbLicenceEleve, nbLicenceProfDoc and nbLicenceAutrePersonnel are absent). Either the "nbLicenceGlobal" field is missing and at least one of the following four fields is/are filled in: nbLicenceEnseignant, nbLicenceEleve, nbLicenceProfDoc and nbLicenceAutrePersonnel These specific licenses are only applicable to their nominal audience. The corresponding target audience must be declared in publicCible.
RG2	Only one of the 2 fields "uaiEtab" or "codeNatureUAI" must be filled in (OR exclusive).
RG3	Identifier of the commercial distributor (cf. field idDistriuteurCom) The SIREN is mandatory. If the commercial distributor has a SIREN and ISNI, in this case the identifier will be of the form: [SIREN]_[ISNI].

	If the commercial distributor does not have an ISNI code, in this case the identifier will be of the form: [SIREN]_0000000000000000 The separator between the SIREN code and the ISNI code is the character " _ ". No space between the characters.
RG4	The value filled in the field categorieAffectation must be filled in with "transferable". The value filled in the field typeAffectation must be filled in with "ETABL" or "INDIV".
RG5	If a number of licenses per audience is entered: then the target audience field (publicCible) must contain the audience(s) for which the number of licenses is defined. Only the audience designated by the license type can be addressed. For instance: If the field "nbLicenceEleve" is provided (with the value > or = 0) then publicCible must contain ELEVE If the field " nbLicenceEnseignant " is provided (with the value > or = to 0) then publicCible must contain ENSEIGNANT If the field " nbLicenceProfDoc " is provided (with the value > or = to 0) then publicCible must contain DOCUMENTALISTE If the field "nbLicenceAutrePersonnel" is provided (with the value > or = to 0) then publicCible must contain AUTRE PERSONNEL
RG6	A subscription with an assignment of type "establishment" (value "ETABL") does not have a number of licenses defined by audience, but only a number of global licenses with the value "UNLIMITED". If a number of licenses is provided for an audience or if the number of global licenses is not "UNLIMITED", the subscription action will return an error.
RG7	The validity period of a subscription cannot exceed 10 school years.
RG8	The start date of the validity of a subscription cannot exceed 10 years after the date the subscription was created.
RG9	One or the other of the fields "finValidite" or "anneeFinValidite" must be present. Only one of the two fields "finValidite" or "anneeFinValidite" must be filled in (mutually exclusive fields).
RG10	The "anneeFinValidite" field is of the form "[4 digit year]-[4 digit year]". Example: 2017-2018
RG11	A check regarding the level of the institution/school (primary education, secondary education) is made when a subscription if created or modified. If the subscription is for a primary school, the number of licenses for documentalists must not be filled in (tag present without value or tag absent). or tag absent.
RG12	The subscription ID must be unique. Prohibited values: "abonnements" [subscriptions], "catégorie" [category]
RG13	When creating a subscription, its "idAbonnement" field must not begin with the character "_". This character is used as a prefix to the "idAbonnement" field generated for deleted or expired subscriptions.

Table 14 -Subscriptions Web Service - Management rules

8.4.3 Subscription web service requests

This paragraph presents the information common to all requests of the subscription web service.

8.4.3.1 Structure of requests

The web service requests are presented in the form of a standard HTTP/REST request.
The following table describes each part of the request.

Parts of the request	Description
HTTP command	Command line for the HTTP request.
Headers	The HTTP headers of the request.
Body	The body of the request.

Table 15 - Web Service Subscriptions - Description of parts of the HTTP request

The structure of a web service request is composed of :
▸ The HTTP command, which refers to the operation to be performed;
▸ The HTTP URI, which defines the object to which this operation is linked;
▸ The HTTP version, which MUST be 1.1.
The available requests are:
▸ PUT: used to create an object ;
▸ POST: used to update an object;
▸ DELETE: used to delete an object;
▸ GET: used to retrieve an object.

In the case of PUT and POST requests, the body of the request must be in XML format and must respect the grammar defined in this document.
Otherwise, an error will be returned.

8.4.3.2 HTTP headers for different requests

Header	Description	Required
Content-Type	Defines the type of content passed in the request body. The default value is "application/xml". For PUT and POST requests, the value should be: "application/xml;charset=utf-8" in case extended characters are present in the request body.	No
Content-Length	Request size (without headers)	No
Date	The current date and time	No
Host	Allows to specify the web service concerned by the request.	Yes

	This header can be used to specify the format of the response. Accepted values: - application/xml - application/json The default value is "application/xml".	
Accepta		No

Table 16 - Web Service Subscriptions - Description of common HTTP request headers

8.4.3.3 Example of a request

```
POST / HTTP/1.1
Host: domain.com
Date: Mon, 10 Dec 2015 14:25:01 GMT
Content-Type: application/xml;charset=utf-8
Content-Length: 3495
Accept: application/xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<abonnement xmlns="http://www.atosworldline.com/wsabonnement/v1.0/">
   <idAbonnement>abonnement1</idAbonnement>
   <commentaireAbonnement>commentaire1</commentaireAbonnement>
   <idDistributeurCom>000000000_0000000000000000</idDistributeurCom>
   <idRessource>ark:/ressource1</idRessource>
   <typeIdRessource>ark</typeIdRessource>
   <libelleRessource>ressource1</libelleRessource>
   <debutValidite>2015-09-01T09:00:00</debutValidite>
   <finValidite>2016-08-16T23:59:59</finValidite>
   <uaiEtab>01200000X</uaiEtab>
   <uaiEtab>03400000Y</uaiEtab>
   <categorieAffectation>non transferable</categorieAffectation>
   <typeAffectation>INDIV</typeAffectation>
   <nbLicenceEnseignant>10</nbLicenceEnseignant>
   <nbLicenceEleve>100</nbLicenceEleve>
   <nbLicenceProfDoc>2</nbLicenceProfDoc>
   <nbLicenceAutrePersonnel>4</nbLicenceAutrePersonnel>
   <!--<nbLicenceGlobale>0</nbLicenceGlobale>-->
   <publicCible>ELEVE</publicCible>
   <publicCible>ENSEIGNANT</publicCible>
   <publicCible>DOCUMENTALISTE</publicCible>
   <publicCible>AUTRE PERSONNEL</publicCible>
   <codeProjetRessource>SA2021</codeProjetRessource>
</abonnement>
```

Header	Description
Content-Length	The size of the response in bytes.
Content-Type	The type of content returned in the body of the response.
Date	The date and time of the response.
Server	The server that returned the response.

Table 17 - Subscriptions Web Service - Description of common response headers

8.4.4 Web Service response

This paragraph describes the responses of the Subscriptions web service.

8.4.4.1 Structure of the response

The response is in standard HTTP format. The following table describes each part of the response.

Parts of the response	Description
Status of the response	It is composed of the protocol (always "HTTP/1.1"), followed by the HTTP response code and then the HTTP message.
Headers	HTTP headers of the response.
Body	The body of the response.

Table 18- Subscriptions web service - Description of parts of the response

8.4.4.2 Common HTTP headers for responses

HTTP Code	HTTP Message	Description
200	OK	The request has been successfully processed
201	Created	The object has been created
202	Accepted	The request has been taken into account, but it is not completely finished
204	No content	There is no content (mainly used in case of object deletion)
206	Partial Content	Only a part of the request has been successfully processed
304	No Changed	The requested object has not changed

Table 19 - Subscriptions web service - Description of HTTP return codes in case of success

8.4.4.3 resource listhttp

HTTP Code	HTTP Message	Description
400	Bad Request	The request failed because of an invalid format or a missing parameter.
401	Unauthorized Request	The request failed because of an invalid or missing authentication parameter.
401	Unauthorized Request	SSL error / No required SSL certificate was sent The client certificate is missing from the request
401	Unauthorized Request	SSL error / Invalid client certificate The client certificate is not valid (wrong CA, expired, revoked)
403	Forbidden Request	Request failed due to invalid access rights
404	Not Found	The request failed because the requested object does not exist.
405	Method not allowed	The requested method does not exist.
406	Content not acceptable	The "content-type" header is not present
406	Content not acceptable	The "Accept" header does not contain a valid data.
409	Conflict	The request could not be completed because there is a conflict on the requested object.
409	Conflict	The value given in the "idSubscription" field is forbidden
500	Internal Server	A technical error has occurred
503	Service Unavailable	The service is temporarily unavailable

Table 20 - Subscriptions Web Service - Description of HTTP return codes in case of failure

8.4.4.4 Response body

The body of the response, when it exists, may contain an object in either JSON or XML format. The "Accept" header must contain:
> either "application/xml" for a response in XML format;
> or "application/json" for a response in JSON format.

If the "Accept" header is not provided, the response will be in XML format by default.
If the "Accept" header contains a value other than those expected, an HTTP 406 error code will be returned.

8.4.5 Adding a subscription

8.4.5.1 Request

Method	URL	Protocol
PUT	/{idAbonnement}	HTTP/1.1

Table 21 - Subscriptions web service - Method and structure - Adding a subscription

```
PUT /{idAbonnement} HTTP/1.1
Content-type: application/xml;charset=utf-8
Accept: application/xml
```

Request parameters

There are no request parameters to provide.

Request headers

There are no specific headers to provide in addition to the common headers.

Request body

A "subscription" XML document is expected for this call.

Example:

```
Request :
PUT /0560010G_FBJ_2018-08-31

Body :
<?xml version="1.0" encoding="UTF-8"?>
<abonnement xmlns="http://www.atosworldline.com/wsabonnement/v1.0/">
   <idAbonnement>0560010G_FBJ_2018-08-31</idAbonnement>
   <commentaireAbonnement>Abonnement à  FBJ jusqu'en 2021</commentaireAbonnement>
   <idDistributeurCom>123448915_0000000122425488</idDistributeurCom>
   <idRessource>ark:/34885/ytfy/wr000hghj0002</idRessource>
   <typeIdRessource>ark</typeIdRessource>
   <libelleRessource>Fleury et Bott Junior</libelleRessource>
   <debutValidite>2018-08-16T00:00:00</debutValidite>
   <anneeFinValidite>2020-2021</anneeFinValidite>
   <uaiEtab>0560010G</uaiEtab>
   <categorieAffectation>transferable</categorieAffectation>
   <typeAffectation>ETABL</typeAffectation>
   <nbLicenceGlobale>ILLIMITE</nbLicenceGlobale>
   <publicCible>ELEVE</publicCible>
  <codeProjetRessource>SA2021</codeProjetRessource>
</abonnement>

Réponse :
201 Created
```

8.4.5.2 Response

Response in case of success

If the action was successful,

- ▶ there is no body in the response,
- ▶ an HTTP code "201 Created" is returned.

In case some of the institutions/schools in the subscription are not known to ERAM, an HTTP code "206 Partial Content" is returned. The response includes a body (in XML or JSON format)

providing details on the schools not known to ERAM. This return code is obtained if at least one institution/school in the list is known to ERAM.

List of possible success return codes specific to this method:

Code HTTP	Message HTTP	Message
201	Created	
206	PartialContent	The subscription for the following establishment has not been created: "... ".

Table 22 -Subscriptions Web Service - Description of success return codes - Adding a subscription

Response in case of failure

In case of a failure of the request, the web service returns:
- ▶ an error code selected in accordance with the cause of the error ;
- ▶ a response body (in XML or JSON format) that provides details about the error.

Example of a response:

```
HTTP/1.1 409 Conflict
Date: Tue, 19 Aug 2016 15:13:55 GMT
Content-Type: application/xml
Content-Length : 42
Server : monserveur

<?xml version="1.0" encoding="UTF-8"?>
<Erreur>
<Code>Conflit</Code>
<Message>Les données sont inexactes : debutValidite, finValidite</Message>
<Resource>/idAbonnement</Resource>
</Erreur>
```

List of possible error codes specific to this method:

Code HTTP	Message HTTP	Message
400	Bad Request	One of the two following fields must be filled in: uaiEtab or codeNatureUAI
400	Bad Request	The object does not correspond to an object of type subscription
400	Bad Request	One of the following two fields must be filled in: anneeFinValidite or finValidite
400	Bad Request	The year filled for "anneeFinValidite" is not correct
409	Conflict	The data is inaccurate: "... ".
409	Conflict	The data is incompatible: " ... "
409	Conflict	The subscription identifier " ... " already exists.
409	Conflict	The resource " ... " is unknown.
409	Conflict	The institution " ... " is unknown.
409	Conflict	The data regarding the number of licenses is inaccurate: "

Code HTTP	Message HTTP	Message
		... "
409	Conflict	No correspondence between categorieAffectation and typeAffectation.
409	Conflict	The number of licenses " ... " does not correspond to the target audience " ... ".
409	Conflict	The start date of the subscription is later than the end date
409	Conflict	Conflict with another subscription of a different assignment category
409	Conflict	The number of licenses must be GLOBAL and ILLIMITE if the assignment type is ETABL
409	Conflict	The resource is not distributable.
409	Conflict	For primary schools, the target audience must not contain documentalist teachers and the number of linked licenses must either be 0 or not filled in.
409	Conflict	The value entered in the " idAbonnement " field is forbidden
415	UnsupportedMediaType	The subscription format must be in XML format

Table 23 -Subscriptions web service - Description of return codes in case of error - Adding a subscription

8.4.6 Deleting a subscription

> *Deleting a subscription to a resource that has already been assigned to users is forbidden. The web service will return an error in this case.*

Deleting is an emergency maneuver allowing for example to delete an erroneous subscription just after its transmission.
It is not intended to delete a subscription with at least one valid assignment.
A subscription is the result of a contractual arrangement between the CDR and the institution; it cannot therefore be deleted unilaterally.

> *Any particular case must be reported to ERAM's technical manager, so that any necessary technical actions can be taken.*

8.4.6.1 Requête

Method	URL	Protocol
DELETE	/{ idSubscription}	HTTP/1.1

Table 24 - Subscriptions Web Service - Method and structure - Deleting a subscription

Syntax

```
DELETE /{idAbonnement} HTTP/1.1
```

```
Content-type: application/xml;charset=utf-8
Accept: application/xml
```

Example
Example in the accompanying documents and examples:
GAR_RTFS_V7.0_SupportDocument_EN/ SubscriptionWS/Deleting_subscription.xml

Parameters of the request
There are no request parameters to provide.

Request headers
There are no headers specific to this request to provide in addition to the common headers.

Request body
There is no body to provide for this request.

8.4.6.2 Response

Response in case of success
If the action was successful,
  ▸ There is no body in the response,
  ▸ An HTTP code "204 No Content" is returned.
Response in case of failure
In case of failure, the web service returns:
  ▸ an error code selected in accordance with the cause of the error;
  ▸ a response body (in XML or JSON format) that provides details about the error.

List of possible error codes when deleting a subscription:

HTTP Code	HTTP Message	Message	Comment
400	Bad Request	The subscription identifier does not exist.	
400	Bad Request	The data is not valid	Deletion of a subscription with a record that no longer has an associated CDR.
409	Conflict	The resource is already assigned.	

Table 1 - Subscriptions Web Service - Description of return codes in case of error – Deleting a subscription

Table 25 -Subscriptions Webservice - Description of return codes in case of error - subscription deletion

8.4.7 Modifying a subscription

Subscription modification is only possible for specific parameters, according to the indications given in the management rules (see 8.4.7.3). The subscription object used must be strictly identical to the one used for the initial subscription, apart from the modified parameters.

8.4.7.1 Request

Method	URL	Protocol
POST	/{ idSubscription }	HTTP/1.1

Table 26 - Subscriptions Web Service - Method and structure - Modifying a subscription

<u>Syntax</u>

```
POST /{idAbonnement} HTTP/1.1
Content-type: application/xml;charset=utf-8
Accept: application/xml
```

<u>Example :</u>

```
Request :
POST /0560010G_FBJ_2018-08-31

Body :
<?xml version="1.0" encoding="UTF-8"?>
<abonnement xmlns="http://www.atosworldline.com/wsabonnement/v1.0/">
   <idAbonnement>0560010G_FBJ_2018-08-31</idAbonnement>
   <commentaireAbonnement>Abonnement à  FBJ jusqu'en 2021</commentaireAbonnement>
   <idDistributeurCom>123448915_0000000122425488</idDistributeurCom>
   <idRessource>ark:/34885/ytfy/wr000hghj0002</idRessource>
   <typeIdRessource>ark</typeIdRessource>
   <libelleRessource>Fleury et Bott Junior</libelleRessource>
   <debutValidite>2018-09-01T09:00:00</debutValidite>
   <finValidite>2022-07-15T23:00:00</finValidite>
   <categorieAffectation>transferable</categorieAffectation>
   <typeAffectation>INDIV</typeAffectation>
   <nbLicenceGlobale>8</nbLicenceGlobale>
   <publicCible>ENSEIGNANT</publicCible>
   <publicCible>DOCUMENTALISTE</publicCible>
  <codeProjetRessource>SA2022</codeProjetRessource>
</abonnement>

Réponse : 200 OK
```

<u>Request parameters</u>
There are no request parameters to provide.

<u>Request headers</u>
There are no specific headers to provide to this request, only the common headers must be provided.

Request body
A "subscription" XML object is expected for this call.
The uaiEtab field must be absent from the subscription object as part of the modification.

Fields	Required	Modifiable	Not allowed in the query body
idAbonnement	Yes	No	
commentaireAbonnement	No	Yes	
idDistributeurCom	Yes	No	
idRessource	Yes	No	
typeIdRessource	Yes	No	
libelleRessource	Yes	Yes	
debutValidite	Yes	Yes	
finValidite	No	Yes (cf. RG_M_01)	
anneeFinValidite	No	Yes (cf. RG_M_01)	
uaiEtab			Yes
codeNatureUAI			Yes
categorieAffectation	Yes	Yes (cf. RG12)	
typeAffectation	Yes	Yes	
nbLicenceEnseignant	No (cf. RG1)	Yes (cf. RG_M_01)	
nbLicenceEleve	No (cf. RG1)	Yes (cf. RG_M_01)	
nbLicenceProfDoc	No (cf. RG1)	Yes (cf. RG_M_01)	
nbLicenceAutrePersonnel	No (cf. RG1)	YES (cf. RG_M_01)	
nbLicenceGlobale	No (cf. RG1)	Yes (cf. RG_M_01)	
publicCible	Yes	YES	
codeProjetRessource	No	CF (cf. RG_M_01)	

Table 27 - Subscriptions Web Service - Subscription object elements – Modifying a Subscription

8.4.7.2 Response

Response in case of success
If the action was successful:
- ▶ there is no body in the response;
- ▶ an http code "200 OK" is returned.

Response in the case of a failure
In case of failure, the web service returns:
- ▶ an error code selected in accordance with the cause of the error;
- ▶ a response body (in XML or JSON format) that provides details about the error.

List of possible error codes specific to this method:

HTTP Code	HTTP Message	Message	Commen

400	Bad Request	Subscription ID does not exist	
400	Bad Request	The object does not correspond to a subscription object	The received subscription element does not respect the XSD
400	Bad Request		The received element is not known in the XSD
400	Bad Request	One of the 2 following fields must be filled in: dateFinValidite or finValidite	
400	Bad Request	The year entered for anneeFinValidite is not correct	
409	Conflict	No correspondence between categorieAffectation and typeAffectation	
409	Conflict	Unauthorized modification attempt	UaiCode or uaiEtab is present in the request
409	Conflict	The start date of the subscription is greater than the end date	
409	Conflict	Conflict with another subscription of a different assignment category	
409	Conflict	For primary schools, the target audience must not contain a documentalist teacher and the number of linked licenses must either be 0 or not be filled in.	
415	UnsupportedMediaType	The subscription format must be in XML format	

Table 28 -Subscriptions web service - Description of error codes - Modifying a subscription

8.4.7.3 Management rules

RG_M_01: Modifying the subscription of a resource that has already been assigned to users is only allowed in order to extend the subscription's end date or to increase the number of licenses.

Consequently, if the subscription is already assigned, only the following fields can be modified, as described above:

- ▶ commentaireAbonnement
- ▶ finValidite
- ▶ dateFinValidite
- ▶ nbLicenceEnseignant
- ▶ nbLicenceEleve

- ▸ nbLicenceProfDoc
- ▸ nbLicenceAutrePersonnel
- ▸ nbLicenceGlobal

The subscription object used for the modification must have all the unmodified fields exactly the same as the original subscription, except for the UAI field, which must not be present.

8.4.8 Retrieving information about subscriptions

This function allows you to retrieve information from one or more subscriptions according to defined filters, for a given CDR.

8.4.8.1 "Filters" object

The requested information is defined by using filters (by date, by name or value, etc.).

List and syntax of the filters that can be used:

Field	Description	Format	Mandatory
List\<filter>	List of "filter" type objects defined below. If no value is submitted, all subscriptions of the commercial distributor will be returned Filters on different attributes will add up (logical AND) Filters on identical attributes will add up (logical OR)	List of filter type objects	No
List\<filtreParDate>	List of filtre_par_date" objects defined below. Filters on different date types will add up (logical AND) Filters on identical date types will add up (logical OR)		No

triPar	Sort on the specified attribute Here is the list of available values: idAbonnement idRessource typeIdRessource libelleRessource debutValidite finValidity categorieAffectation typeAffectation publicCible codeProjetResource Default value is: idAbonnement	String	No
Tri	Sorting order Here is the list of available values: ASC: for an ascending order DSC: for a descending order The default value is: ASC	String	No
aboSuppr	true to include active and inactive subscriptions in the list false to include only active subscriptions in the list Default value: false	Boolean	No
filtreNom	Defines the field on which you want to filter. Here is the list of available values: idDistributeurCom: identifier of the commercial distributor uaiEtab: identifier of an establishment idAbonnement: identifier of the subscription typeAffectation: Type of assignment in ERAM categorieAffectation: Category of assignment in ERAM publicCIble: target audience codeProjetRessource: resource project code associated to the subscription Note: the filter on idDistributeurCom is useful if the extracted OR allows access to several commercial distributors.	String	No
filtreValeur	Defines the value of the field to filter on	String	No

Table 29 - Subscriptions Web Service - Description of the "filters" object

Description of filters per date

Field	Description	Format	Mandatory
dateName	Defines the date field on which you want to filter Here is the list of available values: dateCreation: date of creation of the subscription dateModification: date of modification of the subscription debutValidite: start date of the subscription finValidite: end date of validity of the subscription	String	No
dateBefore	Defines the end date of the period on which to filter	Date	No
dateAfter	Defines the start date of the period on which to filter	Date	No

Table 30 - Subscriptions Web Service - Description of the filters by date object

8.4.8.2   Request

Method	URL	Protocol
GET	/subscriptions{?start=XX&end=XX}	HTTP/1.1

Table 31 - Subscriptions Web Service - Method and structure - retrieving subscription information

<u>Syntax</u>

```
GET /abonnements{?debut=XX&fin=XX} HTTP/1.1
Content-type: application/xml
Accept: application/xml
```

<u>Example</u>

```
Request :
GET /abonnements

Body :
<?xml version="1.0" encoding="UTF-8"?>
<filtres xmlns="http://www.atosworldline.com/wsabonnement/v1.0/">
  <filtre>
    <filtreNom>idDistributeurCom</filtreNom>
    <filtreValeur>123448915_0000000122425488</filtreValeur>
  </filtre>
  <filtre>
    <filtreNom>codeProjetRessource</filtreNom>
    <filtreValeur>SA2021</filtreValeur>
  </filtre>
  <filtre>
```

```
        <filtreNom>uaiEtab</filtreNom>
        <filtreValeur>0560010G</filtreValeur>
    </filtre>
    <filtreParDate>
          <dateName>debutValidite</dateName>
          <dateAvant>2018-08-15T00:00:00</dateAvant>
          <dateApres>2017-09-01T09:00:00</dateApres>
    </filtreParDate>
    <filtreParDate>
          <dateName>finValidite</dateName>
          <dateAvant>2018-08-15T00:00:00</dateAvant>
          <dateApres>2017-09-01T09:00:00</dateApres>
    </filtreParDate>
</filtres>


Response :

200 OK

Body :

<abonnements>
   <abonnement xmlns="http://www.atosworldline.com/wsabonnement/v1.0/">
     <idAbonnement>0560010G_FBJ_2018-08-31</idAbonnement>
     <commentaireAbonnement>
          Abonnement à  FBJ jusqu'en 2021
     </commentaireAbonnement>
     <idDistributeurCom>123448915_0000000122425488</idDistributeurCom>
     <idRessource>ark:/34885/ytfy/wr000hghj0002</idRessource>
     <typeIdRessource>ark</typeIdRessource>
     <libelleRessource>Fleury et Bott Junior</libelleRessource>
     <debutValidite>2017-09-01T09:00:00</debutValidite>
     <finValidite>2018-07-15T23:00:00</finValidite>
     <uaiEtab>0560010G</uaiEtab>
     <categorieAffectation>transferable</categorieAffectation>
     <typeAffectation>INDIV</typeAffectation>
     <nbLicenceGlobale>5</nbLicenceGlobale>
     <publicCible>ENSEIGNANT</publicCible>
     <publicCible>DOCUMENTALISTE</publicCible>
     <codeProjetRessource>SA2021</codeProjetRessource>
   </abonnement>
</abonnements>
```

Request parameters

In order to limit the number of elements in the returned list, the two parameters described below allow to specify the number of elements to be returned as well as a notion of pagination. The maximum number of subscriptions returned is 5000.

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

Parameter	Description	Mandatory
Debut	Element number for the beginning of the selection Default: 0	No
Fin	Element number for the end of the selection Default: Debut + 5000	No

Table 32 - Subscriptions Web Service - Subscription Information Retrieval Settings

<u>Request headers</u>

<u>There are no specific headers to provide to this request, only common headers must be provided.</u>

<u>Request body</u>
A "filter" XML document is expected for this call.

8.4.8.3 Response

Response in the case of a success
If the action was successful, the web service returns :
- ▶ An HTTP code "200 OK NoContent" is returned;
- ▶ A list of "subscription" objects.

Applied grammar
The file provided in return is in accordance with the XSD wsabonnement.xsd, available in the examples zip.
- ▶ File name: wsabonnement.xsd
- ▶ Location: in the accompanying documents and examples:
GAR_RTFS_V7.0_SupportDocument_EN/ SubscriptionWS/ws_subscription.xml

Response in case of failure
In case of failure, the web service returns :

- ▶ An error code selected in accordance with the cause of the error ;
- ▶ A response body (in XML or JSON format) that provides details about the error.

List of possible error codes specific to this method:

HTTP Code	HTTP Message	Message
400		The difference between the beginning and the end cannot be greater than 5000
400		The object does not correspond to "filter" object
400		The received element is not known in the xsd
409	Conflict	The data is/are inaccurate: "…".
409	Conflict	The data on the number of licenses is/are inaccurate: "…".
415	UnsupportedMediaType	The format of the filter must be in XML format.
415	UnsupportedMediaType	The object does not correspond to an object of type filters.

Table 33 - Subscriptions Web Service - Error codes - Subscription information retrieval

8.4.9 Retrieving the list of institutions

This command allows you to download a file in XML format containing the list of institutions known to ERAM.
The list of known institutions is generated daily.

8.4.9.1 "Établissement" object

Description of the "établissement" [*establishment*] object:

8.4.9.2 Request

Field	Description	Format
uai	registered administrative unit. Identifier of the establishment	String in upper case without accent (255 max.)
nature_uai	Coded nature of the establishment	String (255 max.)
nature_uai_libe	Nature of the establishment in text format	String (255 max.)
type_uai	Coded type of establishment	String (255 max.)
type_uai_libe	Type of the establishment in text format	String (255 max.)
commune	Postal code of the municipality of the establishment	String (255 max.)
commune_libe	Name of the municipality of the establishment	String (255 max.)
academie	Identifier of the academy	String (255 max.)
academie_libe	Name of the academy	String (255 max.)
departement_insee_3	Department number	String (255 max.)
departement_insee_3_libe	Name of the department	String (255 max.)
appellation_officielle	Name of the establishment	String (255 max.)
patronyme_uai	Name of the establishment	String (255 max.)
code_postal_uai	Postal code of the municipality where the establishment is located	String (255 max.)
localite_acheminement_uai	Municipality of postal delivery of the establishment	String (255 max.)
idENT	Identifier of the VLE to which the institution is attached encoded in base 64	String (255 max.)

Table 34 - Subscriptions Web Service – Description of the "Etablissement" object

Method	URL	Protocol
GET	/establishments/establishments.xml	HTTP/1.1

Table 35 -Subscriptions Web Service - Method and Structure - List of Institutions

Syntax

```
GET /etablissements/etablissements.xml HTTP/1.1
Content-type: application/xml
Accept: application/xml
```

Example

Example in the accompanying documents and examples:

GAR_RTFS_V7.0_SupportDocument_EN/ SubscriptionWS/Etablishment_List.xml

Parameters of the request

There are no request parameters to provide.

Request headers

There are no specific headers to provide for this request, only the common headers must be provided.

Request body

There is no request body for this call for this call.

8.4.9.3 Response

The web service returns:

▸ An HTTP code "200 OK" ;
▸ A list of "establishment" objects.

Example

```
Request :
GET /etablissements/etablissements.xml

Response :
200 OK

Body :
<listEtablissement xmlns="http://www.gar.education.fr/listEtablissement/v1.0/">
  <etablissement>
    <numero_uai>0010428K</numero_uai>
    <nature_uai>151</nature_uai>
    <nature_uai_libe>Ecole élémentaire</nature_uai_libe>
    <type_uai>1ORD</type_uai>
    <type_uai_libe>Ecoles du premier degré ordinaires</type_uai_libe>
```

```
      <commune>1083</commune>
      <commune_libe>Chaneins</commune_libe>
      <academie>10</academie>
      <academie_libe>Lyon</academie_libe>
      <departement_insee_3>01</departement_insee_3>
      <departement_insee_3_libe>Ain</departement_insee_3_libe>
      <appellation_officielle>Ecole primaire</appellation_officielle>
      <patronyme_uai></patronyme_uai>
      <code_postal_uai>01110</code_postal_uai>
      <localite_acheminement_uai>CHANEINS</localite_acheminement_uai>
   </etablissement>
   <etablissement>
      <numero_uai>2050032W</numero_uai>
      <nature_uai>304</nature_uai>
      <nature_uai_libe>Lycée français à l'étranger</nature_uai_libe>
      <type_uai>ETRA</type_uai>
      <type_uai_libe>Etablissements français à l'étranger</type_uai_libe>
      <commune>99205</commune>
      <commune_libe></commune_libe>
      <academie></academie>
      <academie_libe></academie_libe>
      <departement_insee_3></departement_insee_3>
      <departement_insee_3_libe></departement_insee_3_libe>
      <appellation_officielle>College Elite de TYR</appellation_officielle>
      <patronyme_uai>COLLEGE ELITE DE TYR (M,E,C,L)</patronyme_uai>
      <code_postal_uai></code_postal_uai>
      <localite_acheminement_uai>TYR</localite_acheminement_uai>
   </etablissement>
</listEtablissement>
```

Applied grammar

The file provided in response is in accordance with the XSD establishment available in the zip of examples.
File name: Establishment_List.xsd.

9 Resource access module

9.1 Presentation of the resource access module

The resource access module allows ERAM users to access the resources assigned to them.
This module manages:

- resource access authorizations;
- the supply of attributes requested in the resource record and, where applicable, validated by the administrative manager;
- the propagation of logout requests in the event of the end of an ERAM session, and in particular in the event of the end of a VLE session.

The module allows the use of SAML v2.0 and CAS v3.0 or higher authentication protocols for web access and OIDC for native application access.
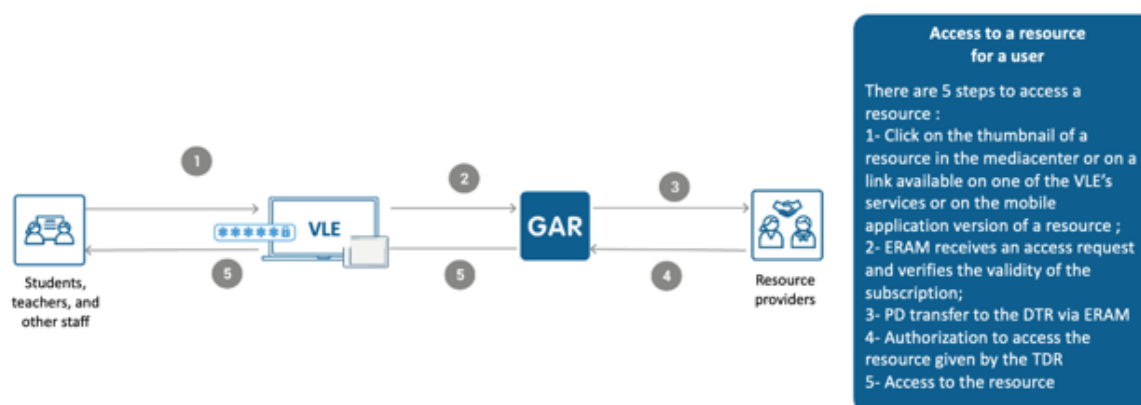
Figure 17 - Resource access module

The operation of the resource access module in OIDC for native applications is described in §4. The following diagram describes the different steps required to authenticate a user to a resource through ERAM.

```
        ┌──────────────────────────┐
        │  Access to the URL of the │
        │ resource at the ERAM level│
        └────────────┬─────────────┘
                     │
        ┌────────────▼─────────────┐
        │ Extraction of idRessource, idEtab │
        │ and profi/idHint parameters│
        └────────────┬─────────────┘
                     │
              ◇ Available resource? ◇ ── no ──▶ ( Case of error )
                     │ yes
        ┌────────────▼─────────────┐
        │ redirection to the resource│
        │     at the publisher       │
        └────────────┬─────────────┘
                     │
         ◇ existing session on the TDR side ◇ ── yes ──▶ ( user's access to the resource )
                     │ no
        ┌────────────▼─────────────┐
        │ ERAM authentication request│
        └────────────┬─────────────┘
                     │
┌────────────────────────────────┐
│ identification of the institution│ ◀── no ── ◇ profile and idEtab present? ◇
│ and the profile through the WAYF │
└──────────────┬─────────────────┘                  │ yes
               │                                     │
        ┌──────▼──────────────────────────────────────▼┐
        │ redirection to the identity                   │
        │ provider for authentication                   │
        └────────────┬─────────────┘
                     │
  no ◀── ◇ Recovery of the user's identifier OK ? ◇
                     │ yes
  ( Case of error ) ◀── no ── ◇ "Valid ERAM" Control ? ◇
                     │ yes
        ┌────────────▼─────────────┐
        │ supply of user's attributes│
        │      to the resource       │
        └──────────────────────────┘
```

Figure 18 - Diagram of authentication of a user to a resource by ERAM

9.2 Using the resource access module

To be able to take into account access requests, the TDR needs to:
- ▶ set up an SSO access 'door' to the resource dedicated to ERAM, ensuring the processing of the access session;
- ▶ indicate the URL of this 'door' in the resource description record.

9.2.1   Choice of protocol

When registering with ERAM, the TDR chooses a resource access protocol, for web access, SAML2.0 or CAS 3.0 or above.
This protocol is associated with the TDR's default platform.
The TDR may request the creation of other platforms, either to operate multiple protocols or to be able to use more than one SSO client on different URLs.
In the case of access via a native application, the protocol used is OIDC.
DTR platforms are created with the Access Token enabled by default.

If using SAML protocol

The TDR shall provide ERAM with the SAML metadata access URL of its Service Provider (SP) for its platform.

If using CAS protocol

The TDR shall provide the logout URL, to which the ERAM will transmit the logout propagation requests.
The combination of a resource and a platform is made in the record, via the elements provided by the VCARD of the "technical distributor" role.
The TDR identifier is composed in the form [SIREN]_[ISNI]. If there is no ISNI, it is replaced by 16 characters "0".
The TDR identification can be complemented, if needed, by a platform number (X-PLATEFORME-ID parameter). If this information is missing, ERAM uses the default platform (00).

9.2.2   SAML access to resources

Access Protocol

The resource access protocol is SAML 2.0 in SP-Initiated mode.
The ERAM resource access module acts as an identity provider (IDP).
The SAML client set up by the TDR to protect its resources acts as Service Provider (SP).
When ERAM receives the authentication request for a resource:
- ▶ it validates the authorization to access the resource;
- ▶ it returns the user attributes available for the resource.

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS

Liberté
Égalité
Fraternité

Sequence diagram

The diagram below describes the exchanges between the ERAM resource access module and the resources.
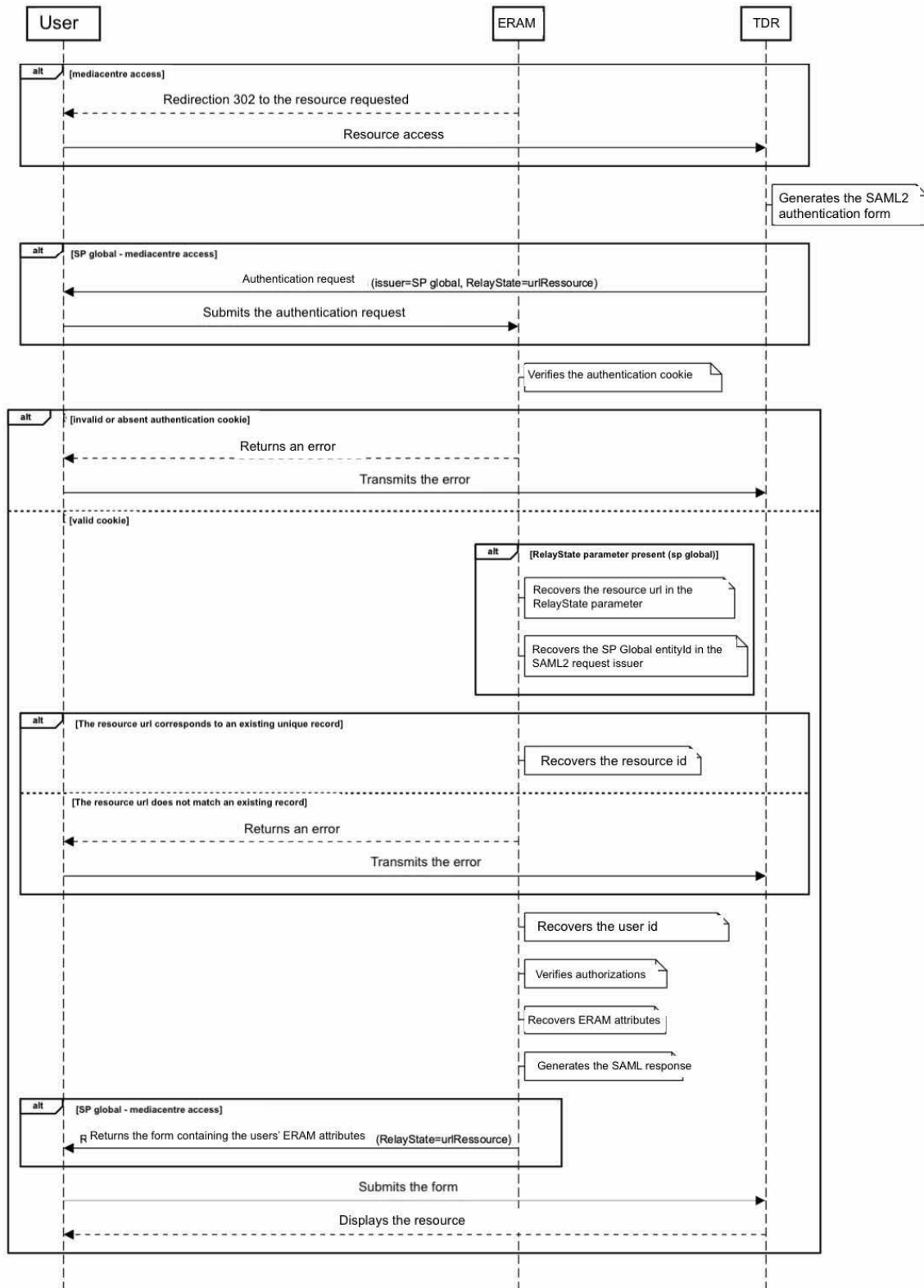
Figure 19 - Sequence diagram of a SAML 2.0 access to a resource

ERAM uses SAML in 'SP Global' mode (a common SP for several resources). The 'relaystate' parameter provided by the resource when sending the authentication request must contain the resource URL.

Management of errors

If access fails, the following errors are possible:
- ▸ user not authenticated to ERAM;
- ▸ resource unknow to ERAM;
- ▸ resource not assigned to the user;
- ▸ subscription expired;
- ▸ SAML incident.

In this case, ERAM returns a page indicating the nature of the error.

Provision of SAML metadata

The operation of the SAML protocol is based on the principle of metadata exchange between the identity provider (IDP) and the resource provider (SP, service provider).
It is necessary for the resource provider to makes available its SAML metadata for ERAM (available via HEAD and GET methods).
This is done through a TLS (HTTPS) encrypted flow.
To encrypt this flow, the server providing the metadata must have an x509 certificate issued by a publicly recognized certification authority. The partner is free to choose the issuing authority.
The SAML metadata of the TDR are cached by ERAM in order to minimize the volume of exchanges and minimize the impact of possible access errors. As a result, the spread of updates is not instantaneous; metadata are updated at least once a day.

Requirements for metadata provision

- ▸ The partner's server making the metadata available must:
  - • be accessible via the Internet;
  - • have a valid domain name and server name.
- ▸ The certificate must be issued by a public certificate authority.
- ▸ The certificate must support TLS encryption. The partner is free to choose either Standard SSL or Extended Validation (EV) SSL. Only TLS encryption is required, so the partner may choose the most appropriate option for their environment.
- ▸ The partner is free to choose the number of certificates they need (unit, wildcard, etc.). They shall select a certificate appropriate to the architecture of their information system.

SP SAML configurations

SP SAML (SAML service provider) here refers to the SAML client software module installed by the TDR to protect access to resources.
To limit the number of SAML SPs to be configured, resource providers must use the principle of a global SP, which enables the protection of access to several resources from a single SAML SP provider configuration point (= a single entityID).

When accessing the resource in SP initiated mode, this global SP will generate a request for an SAML token to ERAM's IDP. This request is accompanied by a relayState parameter which must contain the URL of the requested target resource.

With a value in accordance with the desired SP configuration:

- ▸ EntityID = URL of the metadata SAML = SAML Issuer ;
- ▸ RelayState = URL of the resource;
- ▸ Name id : the transient mode must be accepted by the TDR's SAML service provider. In this mode, the NameID is different for each authentication.

The SP metadata must therefore contain an element in the following form:

```
<md:NameIDFormat>
   urn:oasis:names:tc:SAML:2.0:nameid-format:transient
</md:NameIDFormat>
```

The ERAM response during authentication will then contain the NameID element of the following form:

```
<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:Subject>
```

9.2.3   CAS access to resources

Access Protocol

The protocol for accessing resources is CAS version 3.0 or above.
When ERAM receives the authentication request from a resource:

- ▸ it validates the authorization to access the resource;
- ▸ it returns a service ticket to the resource.

The resource must validate this ticket to ERAM in server-server mode in order to obtain the user's attributes.

Sequence diagram

The diagram below describes the exchanges between the ERAM resource access module and the resources.
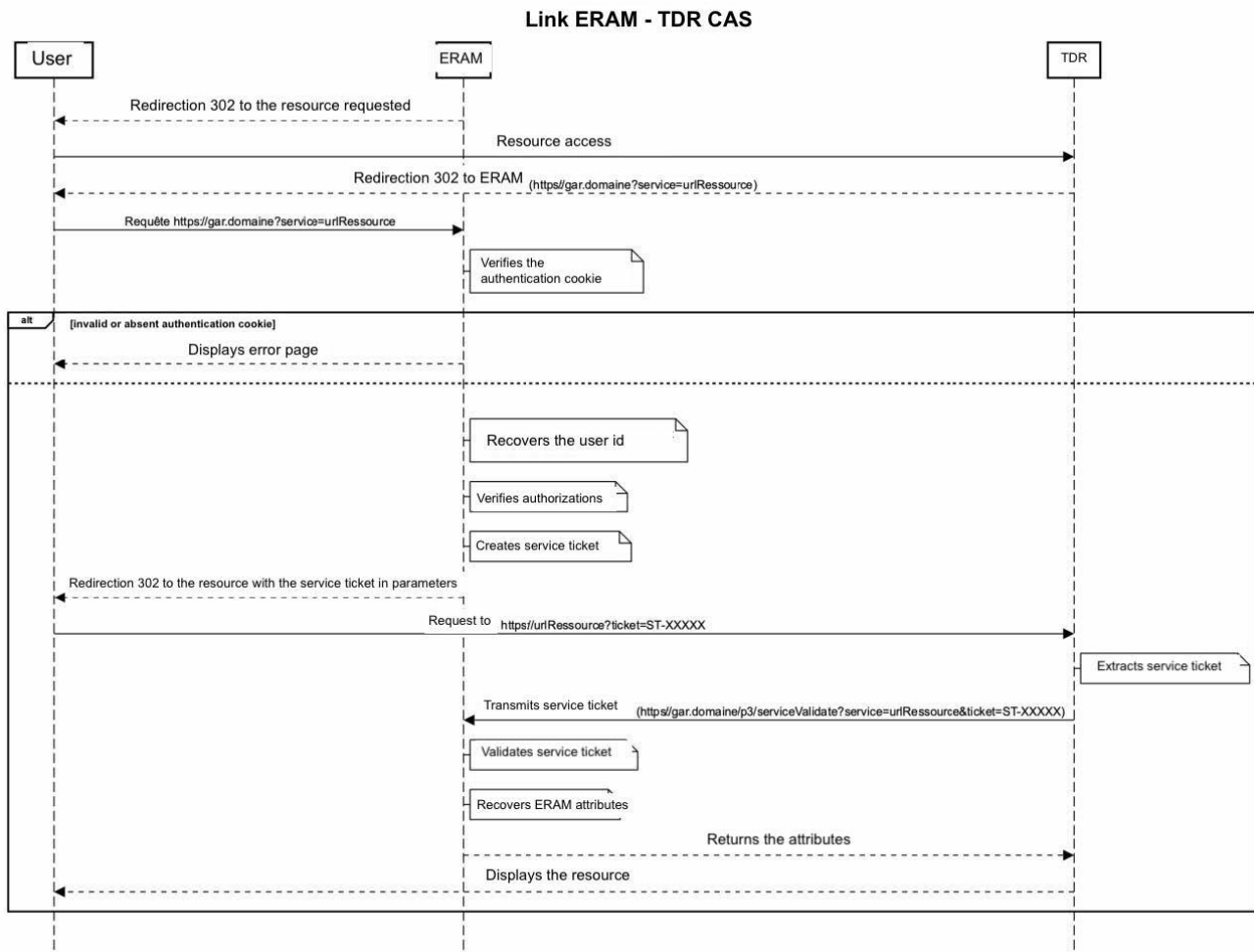
*Figure 20 - - Sequence diagram of a CAS 3.0 (or above) access to a resource*

When a resource receives an access request, it redirects the user to ERAM (through an HTTP 302 redirect via the accessor's browser) by adding a "service" parameter to the request.
This parameter contains the URL of the resource identified at ERAM level and will be used to redirect the user to the resource once authentication is complete. In addition to the URL of the resource, the value of the "service" parameter can contain a grain parameter (see below, granular access).

▶ ERAM validates the user's authentication and access authorization.
▶ ERAM generates a service ticket and redirects the user to the resource by adding the service ticket to the request (ST parameter) and the value of the service received at the time of the authentication request (access URL to the resource and optionally the grain parameter).
▶ The resource retrieves the service ticket and validates it with ERAM in order to obtain the user's attributes. The request sent to ERAM contains the service ticket and a "service" parameter containing the URL that received the service ticket (resource access URL and optionally the grain parameter).

Management of errors

If access fails, the following errors are possible:
- user not authenticated to ERAM;
- resource unknow to ERAM;
- resource not assigned to the user;
- subscription expired;
- technical error.

In this case, ERAM returns a page indicating the nature of the error.
The following errors are possible when calling the server to validate the service ticket:
- invalid service ticket;
- technical error.

In this case, ERAM returns an error stream to the resource.

9.2.4 OIDC access to resources

Access to OIDC resources via ERAM is reserved for native applications. The authentication mechanism in OIDC is described in §4.2.

9.2.5 Logout management from VLE/authentication desk

The implementation of logout is essential to avoid cases of identity theft on shared equipment.

General description

When a VLE sends a logout request to ERAM, ERAM sends a logout request to each web resource to which the user is connected. ERAM then invalidates the authentication cookie, associated tokens, and deletes the stored information for the session.
The propagation by ERAM of logout to resources is performed asynchronously in server-server mode.
The resources are responsible for managing their session after receiving the logout request.
However, the logout is not propagated to native applications.

Sequence diagram

The diagram below describes the exchanges between ERAM's resource access module and the resources in case of a logout request.

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS
Liberté
Égalité
Fraternité
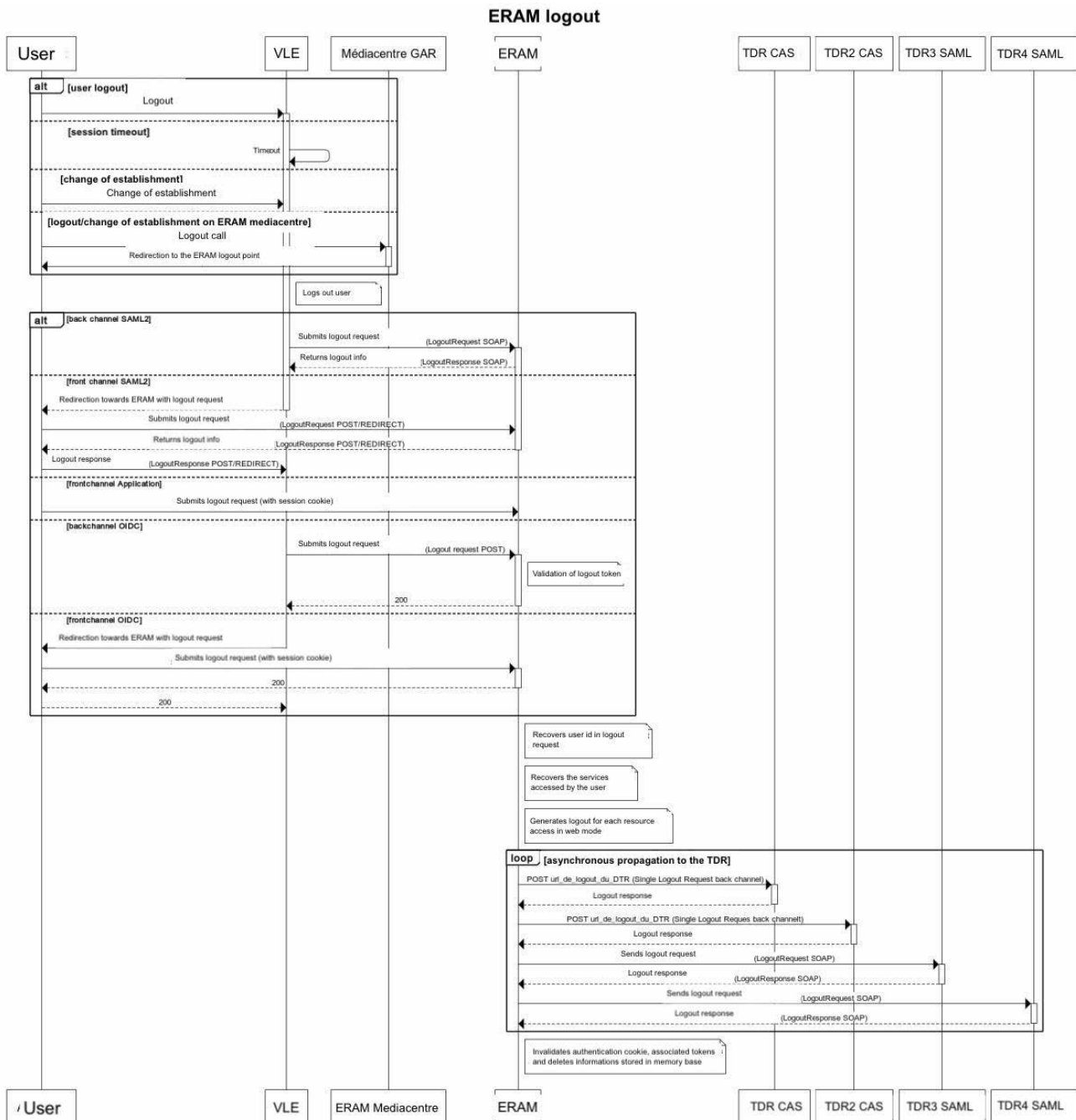
Figure 21 - Sequence diagram for the propagation of the logout to resources

Logout Propagation - SAML Protocol

The resource logout URL must be available via the metadata (SingleLogoutService Binding).
Logout requests will be submitted by ERAM in server/server mode (SOAP). The SOAP Binding
must therefore be available in the provider's metadata.
ERAM sends a logout request to each SP to which the user is connected.

The session identification key for logout takes the value of the NameId provided by ERAM during the connection.

Example

The ZIP of examples contains an example of a logout propagation request

(4-GAR_RTFS_V7.0_SupportDocuments_FR/Logout/slo_request_SAML.xml).

Logout propagation - CAS protocol

The logout URL (endPoint/logout) is provided by the TDR in the initialization data. Logout requests are transmitted by ERAM in server/server mode (back channel).
The call to the endPoint/logout provides the service ticket that enabled authentication with ERAM when accessing the resource.

Example

The ZIP of examples contains an example of a logout propagation request (4-GAR_RTFS_V6.0_SupportDocuments_EN/Logout/slo_request_CAS.xml).

9.2.6 Logout management from a native application in OIDC

The logout propagation in OIDC in the case of native applications is described in §4.2.2.

Example

The example ZIP contains an example of a logout request in front channel from the mobile application to the GAR (4- GAR-RTFS_7.0_DocumentsAccompaniment_FR/Protocols/Deconnexion/slo_request_OIDC.txt).

9.3 Granular access to resources

9.3.1 General presentation

Many of the resources accessible via ERAM are presented as a collection of "grains", which can be defined as an editorial unit of pedagogical use for the resource (article, media, exercise, etc.).
Granular access allows access to a "grain" of the resource, via an "ERAM GRAIN URL". This URL is composed of ERAM's access URL to the resource used by the VLE mediacenters (ERAM RESOURCE URL) and a parameter containing the PUBLISHER GRAIN URL.
Subscription and assignment remain defined on the entire resource, but accesses can be made directly on the grains defined in advance for this purpose by the publisher.
The grain call is formatted as a call to the resource's home page, with the grain's URL as a parameter.
The granular resource receives the call on its home page (ie SSO gate) and forwards it to the grain URL.
Grain indexing and grain searching are outside the scope of ERAM.

For resource providers, granular access is organized into two types of functionalities:

- ▶ provide access to granular contents: content resources;
- ▶ implement access to granular contents.

Access to granular contents can be implemented by resources offering a service for using these contents and/or by functional modules of VLEs (courses, textbooks, etc.). Most granular resources combine the provision of granular contents and the implementation of granular contents' access.

Content resource providers:

- ▶ Decide whether to provide granular access;
- ▶ Define the granules that will be accessible;
- ▶ Implement, according to their approach, the tools to enable discovery, indexing, identification, etc. of the granules (outside of ERAM's scope);
- ▶ Implement a routine to exploit the received granular ERAM URLs.

Service resource providers:

- ▶ Decide how to operate granular accesses on resources that provide such accesses;
- ▶ Define one or more ways to retrieve bookmarks;
- ▶ Implement, depending on their approach, tools for managing granular identifications (bookmark management, federated or propagated search base, etc.);
- ▶ Implement an ERAM granular URL composition routine.

ERAM access to a grain operates in three phases:

1. Request ERAM access to the Grain, via a specific ERAM URL containing a GRAIN parameter.

2. Redirects the user to the resource, with the PUBLISHER GRAIN URL as a parameter. The TDR validates the user's access to the resource, and retrieves the user's attributes.

3. The TDR redirects to the grain using the URL parameter PUBLISHER GRAIN URL.

In the case of granular access, the GRAIN parameter must be provided to ERAM when requesting access:

- ▶ For the CAS protocol, in the parameter "service";
- ▶ For the SAML protocol, in the parameter "relayState".

9.3.2 Grain access cinematics for web access
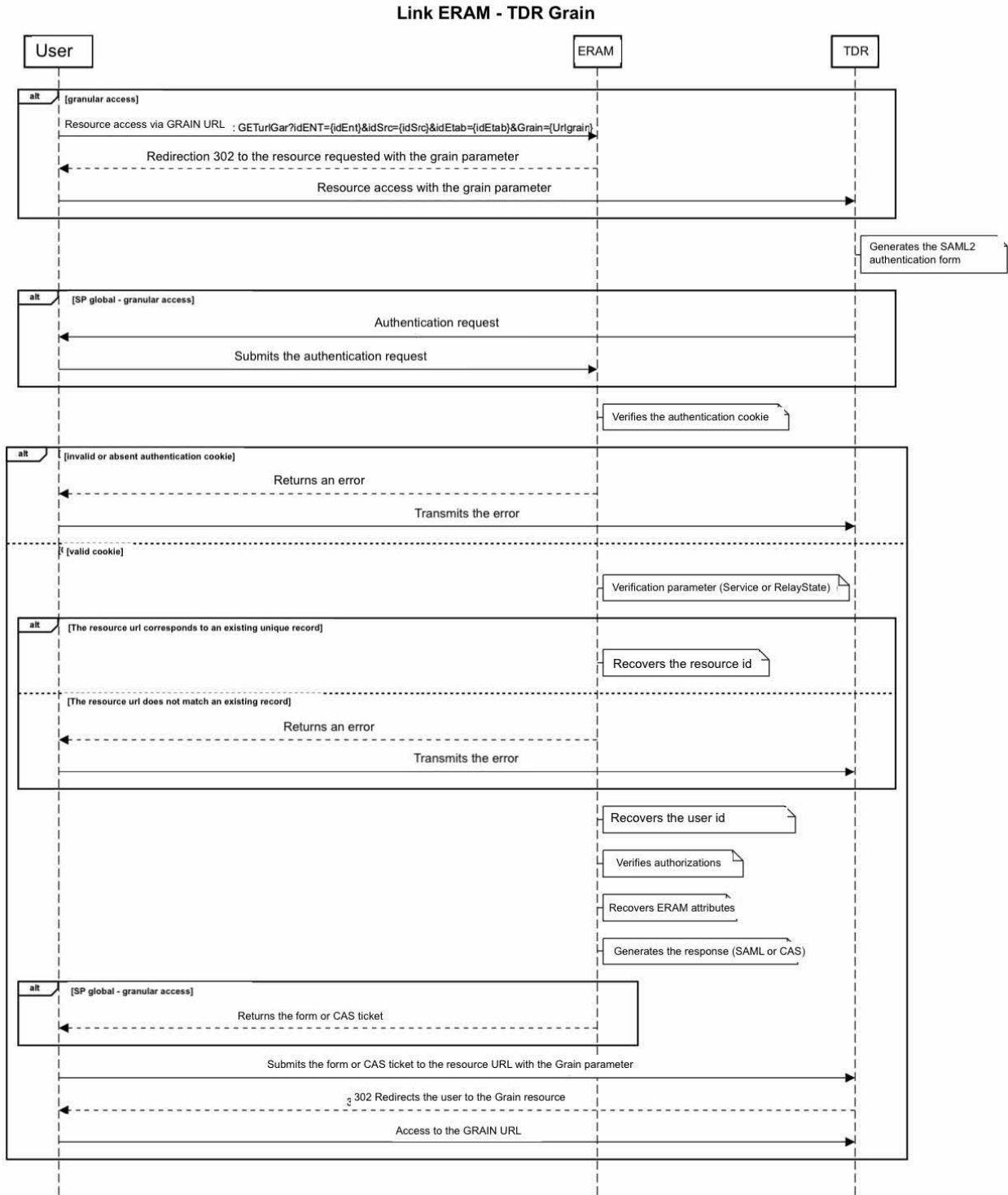
Figure 22 - Sequence diagram for accessing a grain

If the grain parameter is supplied to ERAM, then:

- ▸ the GRAIN parameter is added to the resource URL with the value provided;
- ▸ the user is redirected to this URL containing the GRAIN parameter;
- ▸ it is then up to the resource to route the user to the grain URL.

URL	Function	Remarks
ERAM GRAIN URL	Incorporates the ERAM RESSOURCE URL (URL used by the media center, including parameters UAI and idENT) and the PUBLISHER GRAIN URL	ERAM checks the resource's subscription and assignment, and forwards the request to the PUBLISHER RESOURCE URL
PUBLISHER RESOURCE URL via ERAM	ERAM forwards the PUBLISHER RESOURCE URL, with the PUBLISHER GRAIN URL as a parameter	The PUBLISHER RESOURCE URL initiates the SSO transaction with ERAM, keeping the PUBLISHER GRAIN URL as a parameter
PUBLISHER RESOURCE URL	Retrieves the access "Success SSO" with the PUBLISHER GRAIN URL as a parameter	The resource forwards the access to the PUBLISHER GRAIN URL

Table 36 - Granular Access - Details of URLs used

Example

Identifier of the used resource: ark:/54037/jlnd9g5g37m1.p/InaEdu06508

Access URL to the resource (PUBLISHER RESOURCE URL) :

Granular call

```
https://sp-auth.partenaire.test-
gar.education.fr/domaineGar?idENT=WjA=&idEtab=MDU2MTkzMVY=&idRessource=ark%3A%2F5
4037%2Fjlnd9g5g37m1.p%2FInaEdu06508&grain=https%3A%2F%2Ffresques.ina.fr%2Fjalons%
2Ffiche-media%2FInaEdu06508%2Fla-reforme-des-bourses-etudiantes.html
```

ERAM redirects the user to the PUBLISHER RESOURCE URL to which the Grain parameter is added:

```
https://fresques.ina.fr/jalons/?grain=https%3A%2F%2Ffresques.ina.fr%2Fjalons%2Ffi
che-media%2FInaEdu06508%2Fla-reforme-des-bourses-etudiantes.html" \h
```

Once the access is validated, the resource redirects the user to the PUBLISHER GRAIN URL.

```
https://fresques.ina.fr/jalons/fiche-media/InaEdu06508//la-reforme-des-bourses-
etudiantes
```

If the Grain parameter is missing, the user is redirected to the URL of the resource.

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

```
https://fresques.ina.fr/jalons
```

Parameter	Value	Mandatory	Comment
idENT	VLE project code, base64 encoded	yes	The value can be retrieved by the resources via the PD idENT.
idRessource	Resource ARK identifier, base64 encoded	yes	ark identifier defined by the ScoLOMFR record
idEtab	UAI of the institution from which the access is carried out, base64 encoded	yes	The value can be retrieved by the resources via the PD UAI.
Grain	Publisher's grain identification	no	Outside of ERAM's scope

9.3.3 Formation of the ERAM URL to access a Grain in web mode (ERAM GRAIN URL)

Table 37 - Parameters of the ERAM URL for calling a grain (ERAM GRAIN URL)

The URL for accessing the grain of a resource via ERAM is formed as follows:

```
https://domaineGar?idENT={idENT}&[idRessource={id de la
ressource}]&idEtab={idEtab}[&Grain={URL du Grain}]
```

9.4 Access through WAYF

Access to resources requires knowing the identity provider to be requested. This information is deduced from the user's establishment ("idEtab" parameter) and profile ("profile" parameter). The access URL to the forged resource (by ERAMor by the FR) can contain this information.
In case the URL forged by the FR does not contain this information, ERAM redirects the user to the WAYF so that he can select his profile and his institution. For more details, see §4.1.3.1.

10 Attributes returned during authentication

10.1 Principles

When accessing the resources, ERAM sends the TDR the attributes requested in the ScoLOMFR record as well as the technical attributes DIV_APP and ACCESS_TOKEN which do not need to be explicitly requested.
Attributes are transmitted on the basis of the information provided by VLE operators.

10.2 Attributes returned to the TDR by ERAM

▶ The UAI, Opaque ID, title, first name and last name and email address attributes ([UAI], [IDO], [CIV], [PRE], [NOM], [P_MEL] codes) are provided "in clear".
▶ The Division(s) and Group(s) attributes ([DIV] and [GRO] codes) are provided in the form of the code used in VLE followed by the label, separated by a '##' separator ([code]##[label]).
▶ The division of affiliation attribute ([DIV_APP]) is provided with a specific coding to identify the group, code and label of the division: (GroupCode||DivisionCode##DivisionLabel).
▶ The E_MSx, P_MSx (x from 1 to 5), E_MAT and P_MAT attributes are provided as codes from the Central Nomenclature Database (BCN, available online at: http://infocentre.pleiade.education.fr/bcn/). Attributes beginning with E_ relate to students; those beginning with P_ relate to teachers.

10.2.1 Format of the DIV_APP attribute

The DIV_APP attribute is issued for all records that request the GRO attribute.
The DIV_APP attribute is delivered in the attribute stream.
For each value of the GRO attribute delivered, there are as many values of the DIV_APP attribute as there are group membership divisions.
DIV_APP includes three pieces of information:
▶ group code (the corresponding label is provided in the GRO attribute);
▶ the division code;
▶ the division label.
The "||" separator is used for the DIV_APP attributes to separate group codes from parent division codes and the "##" separator is used to separate codes from labels.
GroupCode||DivisionCodeBelonging##DivisionLabelBelonging

Example
For the group (code: grp_code1, label "group1") belonging to two membership divisions:

Attribute	Code	Label
Division of affiliation 1	div_code1	division1 label
Division of affiliation 2	div_code2	division2 label

Table 38 - Examples of the coding of divisions of affiliation

The following information is returned:

```
GRO
GRP_CODE1##groupe1

DIV_APP
GRP_CODE1||DIV_CODE1##division1
GRP_CODE1||DIV_CODE2##division2
```

10.2.2 DIV attribute in primary level education

In the case of primary-level education access, the information about divisions may not be present for teachers. This situation is due to the specific use of the Onde software in primary schools. This division information may be completed by the VLE, if the local administrator has entered it. It is therefore not always possible to establish direct correspondence between the student's division and that of the teacher.

In this case, it is therefore necessary to populate all divisions of the school when the students connect to the resource, and to ask the teacher which division he/she wishes to work with.

Note that this lack of information does not concern groups, as the GRO attribute is regularly provided for primary school teachers and students. The divisions of affiliation (DIV_APP) are also provided.

10.2.3 E_MSx and P_MSx attributes

The E_MS and P_MS attributes are based on nomenclatures MEF_STAT_1 to MEF_STAT_5 (available online at: http://infocentre.pleiade.education.fr/bcn/workspace/viewTable/n/N_MEF_STAT_x, where x is a value from 1 to 5).

The MEF_STAT_x codes are hierarchical: the more characters are read, the more detailed the information:

- 1st character: MEF_STAT_1, level of education (primary education, secondary education, higher education);
- 2nd character: MEF_STAT_2, educational cycle[14] (lower secondary, upper secondary, General & Technological, etc.);

---

[14] Note: this is the French education cycle ("college": lower level of secondary education; "high school": upper level of secondary education), not to be confused with the *learning cycles* first introduced in 2013, i.e., cycle 1: preschool cycle (first, second and third years of preschool), cycle 2: fundamental learning cycle (first, second and third years of primary school), cycle 3: consolidation cycle (fourth and fifth years of primary school and first year of secondary school) and cycle 4: further learning cycle (second, third and fourth years of secondary school).

- 3rd character: MEF_STAT_3, training system (one-year vocational qualification, two-year vocational qualification, two-year advanced technician's certificate, etc.);
- 4th character : MEF_STAT_4, grade (first year of secondary, second year, …, fifth year Pro, …, sixth year General & Technological, etc.);
- 5th character: MEF_STAT_5, General & Technological upper secondary school stream (General stream, technological stream, technical stream, etc.)

Given this organization, only one E_MSx attribute and one P_MSx attribute (those corresponding to the highest index required) are required

10.2.4 P_MEL Attribute

A "teacher email address" attribute [P_MEL] is available, only for teachers, documentalists (school librairians) and other school staff.
Its use is subject to specific legal rules; it must be justified by a pedagogical need of the resource.

10.2.5 ACCESS_TOKEN attribute

When accessing resources in CAS or SAML, if the TDR platform allows it, an "ACCESS_TOKEN" attribute is returned in addition to the ERAM attributes requested in the record.
By default, the sending of this attribute is activated for all new TDR platforms.
The details of the use of the Access Token thus obtained are described in chapter 4.2.5.

11 Accessor's Assigned Resources (RAA) Web Service

11.1 Overview

The RAA web service provides the list of resource IDs that a given TDR known to ERAM distributes, and that have been assigned to an accessor.

This list is provided based on an IDO assigned to the accessor for one of the resources distributed by the TDR, for a given UAI. It can be filtered by publisher or by CDR.

The TDR requests ERAM to obtain the list of resources they distribute that have been assigned to a given user for a given UAI.

Figure 23- Principles of the RAA web service

In particular, the RAA web service can be used for the deployment of the alternative to using family of resources and specifically for displaying to the user the list of the TDR resources assigned to them.

The use of the WS RAA is limited to the management of an ongoing ERAM session to identify resources assigned to the user in the session. Any out-of-session use to collect data on a set of users is inconsistent with the personal data management principles of ERAM Processing.

11.2 Main parameters of the RAA web service

11.2.1 IDO

The call to the RAA web service operates based on an opaque identifier (IDO) assigned to the accessor for which one wants to receive the list of resources assigned to them. This list is limited to the resources distributed by the TDR calling the web service.

As a reminder, the IDO is defined for one user and one given resource.

The call can be made with any IDO assigned to the accessor for any resource distributed by the TDR calling the web service.

11.2.2 UAI

The list of resources assigned to the accessor is defined for the UAI defined as a parameter. When the accessor is linked to several institutions, the list of resources returned includes only those assigned within the institution defined by the UAI.

11.2.3 Publisher

Optional parameter, allowing to limit the list of resources returned to a given list of publishers.

11.2.4 CDR

Optional parameter, allowing to limit the list of resources returned to the specified CDR.

11.3 Authentication of the access to the RAA web service

The authentication required to use the RAA web service is performed by presenting a certificate, issued by the certification authority of the Ministry of Education, in order to guarantee the traceability of the client/server authentication.
This certificate must be requested from ERAM's technical manager, via the transmission of a CSR (Certificate Signing Request).
The certificate request procedure is described in Chapter 14 (Providing Technical Information).

11.4 Description of the RAA Web Service

The access to this web service must be performed via HTTPS protocol with the use of X.509 certificates (see above).

11.4.1 RAA Web Service Requests

This section presents all the information common to all the command lines of the subscription management web service.

11.4.1.1 Structure of the requests

The web service commands are presented in the form of a standard HTTP/REST request.
The following table describes each part of the request.

Parts of the request	Description
HTTP Command	Command line of the HTTP request.
Headers	HTTP request headers.
Body	The request body.

Table 39 - RAA Subscriptions - Description of HTTP request components

The structure of a web service call is composed of:
▸ The HTTP command, which refers to the operation to be performed;
▸ The HTTP URI, which defines to which object this operation is linked;
▸ The HTTP version, which MUST be 1.1.

Only one command is available:
▸ POST: used to update an object.

In the case of a POST request, the body of the request must be in JSON format and must respect the grammar defined in this document.

Otherwise, an error will be returned.

11.4.1.2 Url request

Method	URL	Protocol
POST	/ressources?uai=0650499P &ido= c780677ff8337d8530d85faaf0a8091825cae158409ea3f4fc2f8022604 4ce2a337d65fee5eefb50e1ebecce0471ecb4c228d3826a96ea957366 f45b01bdaed1	HTTP/1.1

Table 40 - RAA Web Service - Call - URL format to access the web service

Request url parameters

Parameter	Type	Description	Required
Ido	String (128)	The opaque identifier of an accessor for a resource	Yes
Uai	String (8)	The identifier of the accessing institution (UAI access)	Yes

Table 41 - RAA Web Service - Web service access parameters

11.4.1.3 HTTP header

Header	Description	Required
Content-Length	Size of the request (without headers)	No
Date	The current date and time	Yes
Host	Allows to specify the web service concerned by the request.	Yes
Accept	This header is used to specify the format of the response. Accepted value: application/json	No

Table 42 - RAA Web Service - Header Description

11.4.1.4 Request body parameters

Parameter	Type	Description	Required	Multi.
editeurs	List of strings	Resource Publishers.	No	Yes

Parameter	Type	Description	Required	Multi.
	(SIREN_ISNI) ([0-9]{9}_[0-9]{15}[0-9,X]{1})	If the structure does not have an ISNI code, in this case the identifier will be in the form: [SIREN]_0000000000000000		
dcr	String ([0-9]{9}_[0-9]{15}[0-9,X]{1})	Identifier of the Commercial Distributor of Resources	No	No

Table 43 - RAA Web Service - Call - list of parameters passed via the request body

11.4.1.5 Example of a request

```
POST
/ressources?uai=0650499P&ido=c780677ff8337d8530d85faaf0a8091825cae158409ea3f4fc2f
80226044ce2a337d65fee5eefb50e1ebecce0471ecb4c228d3826a96ea957366f45b01bdaed1
HTTP/1.1
Host: domain.com
Date: Tue, 09 Feb 2021 12:48:09 GMT
Content-Length: 1234
Accept: application/json
{
  "filtre": {
    "editeurs": [
  "123006766_0000000000000000",
  "123456789_1234567891237777",
  "280345678_1194567891230528"
    ] ,
    "dcr" : "378901946_0000000000000088"
  }
}
```

Indications :

▸ uai: identifier of the accessing institution (UAI access)
▸ ido: opaque identifier of the accessor for a resource distributed by the requester

11.4.2 Processing

Upon the reception of the request, ERAM performs the following processes:
▸ control of the authorizations associated with the TDR site;
▸ control that all mandatory parameters have been filled in;
▸ control that the identifier of the accessor identified from the IDO parameter exists;
▸ control that the resource retrieved from the IDO parameter is distributed by the TDR making the call;
▸ control that the parameter UAI corresponds to a valid institution in ERAM;
▸ control that the accessor belongs to the UAI;
▸ retrieve the ark IDs of each of the assigned resources, with the following filters:

- filter on the resources distributed by the TDR;
- filter on distributable resources ;
- for resources linked to a "mère de famille" resource, filter on displayable resources;
- if the "éditeur" filter is set, filter on resources belonging to one of the publishers in the list of set as a parameter;
- if the "dcr" filter is set, filter on the resources distributed by the CDR;
▸ Return the recovered data in json format.

The URL and body parameters other than those defined will be ignored by the service

11.4.3 Web Service response

This paragraph describes the responses of the RAA web service.

11.4.3.1 Structure of the response

The response is in standard HTTP format. The following table describes each part of the response.

Part of Response	Description
Status of the response	It consists of the protocol (always "HTTP/1.1"), followed by the HTTP response code then the HTTP message.
Headers	The HTTP headers of the response.
Body	The body of the response.

Table 44 - RAA Web Service - Description of Response Parts

11.4.3.2 Response header

Header	Description
Content-Length	The size in bytes of the response
Content-Type	The type of content returned in the body of the response
Date	The date and time of the response
Server	The server that returned the response

Table 45 - RAA Web Service - Response Header Description

11.4.3.3 List of HTTP returns

HTTP code	HTTP message	Description
200	OK	Request successfully processed
400	Bad Request	The request failed because of a missing parameter.
401	Unauthorized Request / SSL error	The client certificate is missing from the request.
401	Unauthorized Request / SSL error	The client certificate is not valid (wrong CA, expired, revoked).
401	Unauthorized Request	The request failed because of an invalid or missing authentication parameter.
403	Accès refusé	[Access Refused] The request failed because of invalid access rights.
403	Accès refusé	[Access Refused] Unauthorized client certificate for the TDR's site entered as a parameter.
403	Forbidden Request	The value of the "nom_parametre" [*parameter_name*] parameter provided does not allow to access the resource.
404	Resource Not Found	The value of one of the parameters of the request is not known by ERAM.
405	Method not allowed	The requested method does not exist. Technical error managed by the application server, so the message cannot be personalized.
406	Content not acceptable	The "Accept" header does not contain valid data. Technical error managed by the application server, so the message cannot be personalized.
500	Internal Server	A technical error has occurred. Technical error managed by the application server, so the message cannot be personalized.
503	Service Unavailable	The service is temporarily unavailable. Technical error managed by the application server, so the message cannot be personalized.

Table 46 - Subscriptions Web Service - Return Code Description

11.4.4 WS RAA Response

11.4.4.1 Response in case of success

If the action was successful,
- an HTTP code "200 OK" is returned;

> ▶ if the user has resources assigned to him, the response body provides the ark identifiers of the resources assigned to the user.

With a result:

```
HTTP/1.1 200 OK
Date: Tue, 09 Aug 2016 12:48:49 GMT
Content-Type: application/json
Content-Length: 542
Server: monserveur
{
 "ressources":
    [
    "ark:/99999/r166xxxxxxxx",
    "ark:/99999/r160xxxxxxxx"
    ]
}
```

Without a result:

```
HTTP/1.1 200 OK
Date: Tue, 09 Aug 2016 12:48:49 GMT
Content-Type: application/json
Content-Length: 542
Server: monserveur
{
 "ressources":
    [

    ]
}
```

11.4.4.2 Response in case of failure

In case of failure, the web service returns:
> ▶ an error code in accordance with the error ;
> ▶ a message returned by the web service to give an indication of the cause of the error.

Response example:

```
HTTP/1.1 400 Bad Request
Date: Tue, 09 Feb 2021 12:48:09 GMT
Content-Type: application/json
Content-Length : 123
Server : monserveur
{
  "erreur": {
    "Code": "Bad Request",
    "Message": "Le paramètre UAI n'est pas renseigné",
  }
}
```

12   Assignment Report Webservice

12.1 Presentation

The Assignment Report web service allows a technical resource distributor to obtain the list of its delta and full assignment reports based on its idDistributeur.
This web service also allows a TDR to change the status of a delta report and to download a delta or full assignment report in xml format in a zip file, via the name of the report, or to download the latest delta report without specifying the report name.

Figure 24 - Principle of the Assignment Report webservice

12.2 Main parameters of the Assignment Report webservice (WS AssignmentReport)

12.2.1   idDistributeur

The call to the AssignmentReport WS is made on the basis of a technical identifier of the distributor assigned to each TDR.
A TDR can only access information from its own assignment reports. The consistency between this parameter and the technical identifier retrieved from the certificate presented by the distributor is checked to access the different methods of the webservice.

12.2.2 Status of delta reports

The delta assignment reports contain a status that indicates their status. The possible values are :
- TAKEN_INTO_ACCOUNT
- NOT_TAKEN_INTO_ACCOUNT
The TDR can change the status of a delta report via the "changeStatus" verb.

12.2.3 Report name

This parameter is the name of the assignment report. Calls to the change status and report upload methods are made based on this name.
For a delta report, the name is composed of the idDistributeur, a separator "_", the dateCreation parameter, then ".zip" (idDistributeur _dateCreation.zip).
For a complete report, the name is composed of the word "Export", a separator "_", the idDistributeur, then ".zip" (Export_ idDistributeur.zip).
For the report download, it is also possible to indicate the keyword LAST DELTA in this parameter, to obtain the last delta report without specifying its name.

12.3 Authentication of access to the RapportAffectation webservice

The authentication required to use the RapportAffectation webservice is done by presenting a certificate issued by the certification authority of the Ministry of National Education, in order to guarantee the traceability of the client/server authentication.
This certificate must be requested from the technical manager of the ERAM, via the transmission of a CSR (Certificate Signing Request).
The certificate request procedure is described in Chapter 15 (Provision of Technical Information).

12.4 Description of the AssignmentReport web service

The access to this web service will be done via the HTTPS protocol with the use of X.509 certificates
To be able to use the web service reportAssignment, the TDR must first :

- ▶ Have been declared in the ERAM
- ▶ Have a valid X509 certificate
- ▶ Have the certificate identifier filled in at the ERAM level

12.4.1 Webservice requests

This section contains all the information common to all the requests made to this web service.

12.4.1.1 Structure of the requests

The requests are standard http requests. The following table describes each part of the request

Part of the request	Description
Command	This is the command line of the HTTP request
Headers	The http headers of the request
Body	The body of the request

Table 47 -AssignmentReport webservice - Description of the parts of the http request

The structure of a webservice call is composed of:
- The HTTP command, which refers to the operation to be performed;
- The HTTP URI, which defines to which object this operation is linked;
- The HTTP version, which must be 1.1.
The available commands are:
- GET : used for read actions only ;
- PUT: used to update an object.

12.4.1.2 Common request headers

Here is the list of common headers for each request:

Header	Description	Required
Content-Type	Defines the type of content passed in the request body. The default value is "application/xml". The charset used must be "UTF-8". (If the encoding used is not UTF-8, there is no error and the request is processed as is)	No
Content-Length	Size of the request (without headers)	No
Date	The current date	No
Host	Allows to specify the web service concerned by the request.	Yes
Accept	This header can be used to specify the format of the response. Accepted values: application/xml application/json The default value is "application/xml".	No

Table 48 - Webservice rapportAffectation - Description des entêtes communs aux requêtes http

12.4.1.3 Example of the query

Here is an example of a query:

```
[GET|PUT /[type d'appel] HTTP/1.1

Host: domain.com
Date: Mon, 13 Déc. 2021 16:35:01 GMT
Content-Type: application/xml
Content-Length: 3495
Accept: application/xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
[Objet XML correspondant au type d'appel]
```

12.4.2 Web service response

The technical distributor of the resources is instantly informed of the success or failure of the operation (List and update) via the return flow of the web service. The http code returned identifies whether there was an error, and in the event of an error the return flow contains the error description.

12.4.2.1 Structure of the response

The response is a standard HTTP response. The following table describes each part of the response.

Part of the answer	Description
Status of the response	It is composed of the protocol (always "HTTP/1.1"), then the HTTP response code.
Headers	The http headers of the request
Body	The body of the response

Table 49 - AssignmentReport Webservice - Description of HTTP response parts

12.4.2.2 Headers common to responses

Here is the list of headers common to each response:

Header	Description
Content-Length	The size in bytes of the response
Content-Type	The type of content returned in the body of the response
Date	The date and time of the response
Server	The server that returned the response

Table 50 - Webservice reportAssignment - Description of common headers for HTTP responses

12.4.2.3 List of http returns

In the case of a success

HTTP status code	Description
200 OK	Request processed successfully
204 No content	There is no content (mainly used in case of object deletion)
304 No changed	The requested object has not changed

Table 51 - Webservice Assignment report - Description of return codes in case of success

In the case of a failure :

HTTP status code	Description
400 Bad Request	The request failed because of an invalid format or a missing parameter.
401 Unauthorized Request	The request failed because of an invalid or missing authentication parameter.
401 Unauthorized Request	The SSL error / No required SSL certificate was sent The client certificate is missing from the request
401 Unauthorized Request	SSL error / Invalid client certificate The client certificate is not valid (wrong CA, expired, revoked)
403 Forbidden Request	Request failed due to invalid access rights
404 Not found	The request failed because the requested object does not exist.
405 Method not allowed	The requested method does not exist.
406 Content not acceptable	The "content-type" header is not present
406 Content not acceptable	The "Accept" header does not contain a valid data.
409 Conflict	The request could not be completed because there is a conflict on the requested object.
500 Internal Server	A technical error has occurred
503 Service unavailable	The service is temporarily unavailable

Table 52 -AssignmentReport Webservice - Failure Return Code Description

12.4.2.4 Response body

The body of the response may contain an object in JSON/XML format.
In order for the body of the response to be in JSON/XML format, the "Accept" header must contain :

- Either "application/xml" for a response in XML format
- Or "application/json" for a response in JSON format
If the "Accept" header is not provided, the XML format will be used by default.
If the "Accept" header contains a value other than those allowed, an http 406 error code will be returned.

12.4.2.5 Example of a response

Here is an example of a response in XML format:

```
HTTP/1.1 200 OK
Date: Mon, 06 Déc. 2021 09:59:59 UTC
Content-Type: application/xml
Content-Length : 321
Server : monserveur
```

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rapportsAffectation>
     <rapportAffectation>
         <idDistributeur>130006042_0000000106379136</idDistributeur>
         <nomRapport>130006042_0000000106379136_2021-12-05.zip</nomRapport>
         <dateCreation>05/12/2021</dateCreation>
         <taille>32 ko</taille>
         <statut>PRIS_EN_COMPTE</statut>
     </rapportAffectation>
     <rapportAffectation>
         <idDistributeur>130006042_0000000106379136</idDistributeur>
         <nomRapport>Export_130006042_0000000106379136.zip</nomRapport>
         <dateCreation>05/12/2021</dateCreation>
         <taille>152 Mo</taille>
     </rapportAffectation>
</rapportsAffectation>
```

12.4.3 Display the list of delta and complete assignment reports

This verb allows to retrieve, from a technical idDistributeur, a list of delta and complete assignment reports allowing to have information on the creation dates or the size of the documents.
The list of assignment reports is returned in the form of an xml containing a list of "AssignmentReport" objects with the characteristics of each delta or complete report for a technical distributor.

12.4.3.1 "AssignmentReport" object

Each "AssignmentReport" object is composed of the following fields:

Field	Format	Description
idDistributeur	String (1024 max)	Technical identifier of a TDR
nomRapport	String (1024 max)	Name of the report
dateCreation	Date	Report generation date
Size	String (10 max)	The size of the file
Status	Possible values: TAKEN_INTO_ACCOUNT NOT_IN_ACCOUNT	Only for a delta report, its status

12.4.3.2 Management rules

RG_RAPPORTAFFECTATION_1 : if the report is of type complete then the status field is not provided.

RG_RAPPORTAFFECTATION_2 : the list in delta mode is sorted in chronological order (date of report generation).

RG_RAPPORTAFFECTATION_3 : for a delta report, the name is composed of the idDistributeur, a separator "_", the parameter dateCreation, then ".zip" (idDistributeur_dateCreation.zip).

RG_RAPPORTAFFECTATION_4 : for a complete report, the name is composed of the word " Export ", a separator "_", the idDistributeur, then ".zip" (Export_idDistributeur.zip).

RG_REPORT_5 :

▶ If status = 'TAKEN_IN', the list contains the characteristics of the delta reports taken into account and the characteristics of the complete report

▶ If status = 'NOT_TAKEN_IN', the list contains the characteristics of the delta reports not taken into account and the characteristics of the complete report.

▶ If status = 'ALL', the list contains the characteristics of all the existing delta reports and the characteristics of the complete report.

RG_RAPPORTAFFECTATION_6: the characteristics of the full report are displayed at the end of the list.

12.4.3.3 Request

Method	URL	Protocol
GET	/rapportsAffectation/{idDistributeur}/{statut}	HTTP/1.1

Table 54 - Webservice reportAssignment - Method and structure - List reports

Syntax

```
GET /rapportsAffectation/{idDistributeur}/{statut} HTTP/1.1

Host: value
Date: date
Content-length: value
Content-type : value
Accept : value
```

Request parameter

Field	Description	Required
idDistributeur	Identifier of a technical distributor	Yes
status	Status of desired delta reports Allowed values: TAKEN_INTO_ACCOUNT NOT_ACCOUNTED_FOR ALL	Yes

Table 55 - AssignmentReport Webservice - Description of request parameters - List reports

Request headers

There are no headers specific to this request to provide in addition to the common headers.
Request body
No objects are expected in the request body.

12.4.3.4 Response

Response in case of success
If the action was successful, an http code "200 OK" is returned as well as a list of
"reportAssignment" objects
Example of a request

```
GET /rapportsAffectation/130006042_000001063136/PRIS_EN_COMPTE HTTP/1.1

Host : domain.com
Date : Tue, 02 Déc. 2021 15:13:47 GMT
Content-length : 567
Content-type : application/xml
Accept : application/xml
```

Example of a response

```
HTTP/1.1 200 OK
Date : Tue, 02 Déc. 2021 11 :04:09 GMT
Content-Type : application/xml
Content-Length : 42
Server : monserveur

<rapportsAffectation>
  <rapportAffectation>
        <idDistributeur>130006042_0000000106379136</idDistributeur>
        <nomRapport>130006042_0000000106379136_2021-10-02.zip</nomRapport>
        <dateCreation>02/10/2021</dateCreation>
        <taille>12 ko</taille>
        <statut>PRIS_EN_COMPTE</statut>
 </rapportAffectation>
        <rapportAffectation>
        <idDistributeur>130006042_0000000106379136</idDistributeur>
        <nomRapport>130006042_0000000106379136_2021-12-03.zip</nomRapport>
```

```
            <dateCreation>03/12/2021</dateCreation>
            <taille>28 ko</taille>
            <statut>PRIS_EN_COMPTE</statut>
 </rapportAffectation>
        <rapportAffectation>
            <idDistributeur>130006042_0000000106379136</idDistributeur>
            <nomRapport>130006042_0000000106370010_2021-12-05.zip</nomRapport>
            <dateCreation>05/12/2021</dateCreation>
            <taille>32 ko</taille>
            <statut>PRIS_EN_COMPTE</statut>
 </rapportAffectation>
        <rapportAffectation>
            <idDistributeur>130006042_0000000106379136</idDistributeur>
            <nomRapport>Export_130006042_0000000106379136.zip</nomRapport>
            <dateCreation>05/12/2021</dateCreation>
            <taille>152 Mo</taille>
        </rapportAffectation>
</rapportsAffectation>
```

Response in case of failure

In the case of an error, the selected error code will be in accordance with the cause of the error and the body of the response (in XML format) will provide details about the error.

Example of a request

```
GET /rapportsAffectation/13/PRIS_EN_COMPTE HTTP/1.1

Host : domain.com
Date : Tue, 02 Dec. 2021 15:13:47 GMT
Content-length : 567
Content-type : application
```

Example of a response

```
HTTP/1.1 400 Bad Request
Date : Tue, 02 Dec. 2021 15 :14:47 GMT
Content-Type : application/xml
Content-Length : 125
Server : monserveur

<?xml version="1.0" encoding="UTF-8"?>
<Erreur>
<Code>Paramètre invalide</Code>
<Message>Le paramètre de requête «idDistributeur» est incorrect</Message>
<Resource>/rapportsAffectation/13/PRIS_EN_COMPTE</Resource>
</Erreur>
```

Here is the list of possible error codes specific to this method:

HTTP Error Code	Code	Message
400 Bad Request	Incorrect parameter	The request parameter " idDistributeur " is incorrect
409 Bad Request	Incorrect parameter	The mandatory parameters are not all filled in: " idDistributeur"/"status".
400 Bad Request	Incorrect parameter	The "status" parameter is incorrect. The authorized values are: "TAKEN_IN", "NOT_TAKEN_IN", "ALL".

Table 56 - AssignmentReport Webservice - Description of specific error codes - List reports

12.4.4 Change the status of a delta report

This verb allows you to change the status of a delta report from taken into account to not taken into account and vice versa.

12.4.4.1 "ModificationReportStatus" object

Here is the description of the "modificationAssignmentReportStatus" object

Field	Description	Required	Multivalued
idDistributeur	String (1024 max)	Yes	No
nomRapport	String (1024 max)	Yes	No
statusAction	Allowed values: - TAKE_INTO_ACCOUNT - REMOVE_FROM_ACCOUNT	Yes	No

Table 57 - AssignmentReport Webservice - Description of the "modificationAssignmentStatus" object

12.4.4.2 Management rules

RG_VERIFICATION_1 : idDistributeur must exist in ERAM
RG_VERIFICATION_2 : the report name must exist in ERAM
RG_VERIFICATION_3 : A consistency check between the idDistributeur and the report name is performed.
RG_VERIFICATION_4 : the report must be of type delta.
RG_VERIFICATION_5 : the status must have an authorized value.
RG_MODIFICATIONSTATUT_1 : the delta reports taken into account can only be modified in NON_PRISED_IN_COMPT
RG_MODIFICATIONSTATUT_2: delta reports that are not taken into account can only be modified to TAKE_IN_COUNT

12.4.4.3 Request

Method	URL	Protocol
PUT	rapportAffectation/modificationStatut	HTTP/1.1

Table 58 - AssignmentReport Webservice - Method and Structure - Change Status

Syntax

```
PUT  /rapportAffectation/modificationStatut HTTP/1.1

Host: value
Date: date
Content-length: value
Content-type: value
Accept: value
```

Request parameters
There are no request parameters to provide.

Request headers
There are no headers specific to this request to provide in addition to the common headers.

Request body
An XML object of type "modificationStatusAssignment" is expected for this call.

Field	Description	Required
idDistribut eur	Identifier of a technical distributor	Yes
nomRappo rt	Name of a delta report	Yes
statusActio n	Take into account or withdraw the consideration of a delta report	Yes

Table 59 - AssignmentReport Webservice - Request body description - Change status

12.4.4.4 Response

Response in case of success
If the action was successful, then there is no body in the response, an http code "200 OK" is returned.
Example of a request

```
PUT /rapportAffectation/modificationStatut/130006042_0000000106379136/
130006042_0000000106379136_2021-12-02/RETIRER_PRISE_EN_COMPTE HTTP/1.1

Host: domain.com
Date: Sun, 05 Dec 2021 12:13:47 GMT
Content-length: 567
Content-type: application/xml
Accept: application/xml
<modificationStatutRapportAffectation>
    <idDistributeur>130006042_0000000106379136</idDistributeur>
```

```
        <nomRapport>130006042_0000000106379136_2021-12-02</nomRapport>
        <statutAction>RETIRER_PRISE_EN_COMPTE</statutAction>
    </modificationStatutRapportAffectation>
```

Example of a response

```
HTTP/1.1 200 OK
Date: Sun, 05 Dec 2021 12:15:47 GMT

Content-Type: application/xml
Content-Length : 42
Server : monserveur
```

Response in case of failure
In the case of an error, the selected error code will be in accordance with the cause of the error
and the body of the response (in XML format) will provide details about the error.

Example of a request

```
PUT
/rapportAffectation/modificationStatut/130006042_0000000106379136/130006042_00000
00106379136_2021-12-02/PRENDRE_EN_COMPTE  HTTP/1.1

Host: domain.com
Date: Sun, 05 Dec 2021 12:15:57 GMT

Content-length: 567
Content-type: application/xml
Accept: application/xml

<modificationStatutRapportAffectation>
    <idDistributeur>130006042_0000000106379136</idDistributeur>
    <nomRapport>130006042_0000000106379136_2021-12-02</nomRapport>
    <statutAction>PRENDRE_EN_COMPTE</statutAction>
 </modificationStatutRapportAffectation>


Exemple de réponse
HTTP/1.1 400 Bad Request
Date: Sun, 05 Dec 2021 12:43:09 GMT
Content-Type: application/xml
Content-Length : 42
Server : monserveur

<?xml version="1.0" encoding="UTF-8"?>
<Erreur>
<Code>Objet avec données incorrectes</Code>
<Message>Le rapport d'affectation est déjà pris en compte</Message>
<Resource>/rapportAffectation/modificationStatut
        /130006042_0000000106379136/130006042_0000000106379136_2021-12-
        02/PRENDRE_EN_COMPTE
     </Resource>
```

```
</Erreur>
```

Here is the list of possible error codes specific to this method:

HTTP Error Code	Code	Message
400 Bad Request	Invalid object	The object must match an object of type "modificationStatusAssignment
409 Conflict	Object with incorrect data	The data "..." is incorrect
400 Bad Request	Incorrect parameter	The parameter " idDistributeur" is incorrect
400 Bad Request	Incorrect parameter	The report name does not exist in ERAM
409 Conflit	Object with incorrect data	The name of the report is not attached to the idDistributeur.
409 Conflict	Object with incorrect data	The assignment report is already taken into account
409 Conflict	Object with incorrect data	The assignment report is already ignored
409 Conflict	Object with incorrect data	The complete report object has no status
400 Bad Request	Incorrect parameter	The "ActionStatus" parameter is incorrect. Allowed values are: "TAKE_IN", "TAKE_OUT".
415 UnsupportedMediaType	Unsupprted Format	The format of the object must be in XML format

Table 60 - AssignmentReport Webservice - Description of specific error codes - Change status

12.4.5 Download an assignment report

This verb allows the downloading of a delta or full xml assignment report in a zip file from its name, or directly the downloading of the latest delta report, via the keyword LAST_DELTA.
The full assignment report is an xml file containing all assignments for the resources of a TDR for all institutions of the ERAM.
The delta assignment report is an xml file containing only the assignments created or modified (any change in status) for a TDR's resources for all ERAM schools since the last file generation except in the case of the change of school year.

12.4.5.1 "ERAM-Assignments" object

The "ERAM-Assignments" object is composed of the following fields:

Field	Format
idDistributeur	String of characters
dateGeneration	Date
idResource	String of characters
typeResouce	String of characters
titleResource	String of characters
idSubscription	String of characters
finValidite	Date
UAI	String of characters
dateLastModif	Date
idOpaque	String of characters

Table 61 - AssignmentReport Webservice - "ERAM-Assignments" object description

12.4.5.2 Request

Method	URL	Protocol
GET	GAR-Affectations/{idDistributeur}/{nomRapport}	HTTP/1.1

Table 62 - AssignmentReport Webservice - Method and Structure - Download Report

Syntax

```
GET /GAR-Affectations/{idDistributeur}/{nomRapport} HTTP/1.1

Host: value
Date: date
Content-length: value
Content-type : value
Accept : value
```

Request parameters

Method	URL	Required
idDistributeur	Identifier of a technical distributor	Yes
nomRapport	Name of a delta or full report This parameter can contain : either a report name in the format defined in RG_RAPPORTAFFECTATION_3 and RG_RAPPORTAFFECTATION_4 or the keyword "LAST_DELTA"	Yes

Table 63 -ReportAssignment webservice - Description of request parameters - Download a report

Request headers
There are no headers specific to this request to provide in addition to the common headers.

Request body

No objects are expected in the request body.

12.4.5.3 Response

Response in case of success
If the action was successful, an http code "200 OK" is returned as well as a zip file containing the assignment report in xml format.

Examples of downloaded zip files are provided in the accompanying documents:
Full report: GAR-RTFS_7.0_DocumentsAccompagnement_FR/WS Rapport Affectation/Export_000000000_0000000000000001.zip

Delta report : GAR-RTFS_7.0_DocumentsAccompaniment_FR/WS Report Assignment/000000000_0000000000000001_2021-06-01.zip

Example of request with report name
```
GET /GAR-Affectations/010101010_0000000000000000/010101010_0000000000000000_2021-
02-06.zip HTTP/1.1

Host : domain.com
Date : Tue, 02 Déc. 2021 15:13:47 GMT
Content-length : 567
Content-type : application/xml
Accept : application/xml


Exemple de requête avec mot clé
GET /GAR-Affectations/010101010_0000000000000000/DERNIER_DELTA HTTP/1.1

Host : domain.com
Date : Tue, 02 Déc. 2021 15:13:47 GMT
Content-length : 567
Content-type : application/xml
Accept : application/xml
```

Example of a response
```
HTTP/1.1 200 OK
Date : Sun, 05 Dec 2021 11 :04:09 GMT
Content-Type : application/xml
Content-Length : 42
Server : monserveur
```

Response in case of failure

In the case of an error, the selected error code will be in accordance with the cause of the error and the body of the response (in XML format) will provide details about the error.

Example of a request
```
GET /GAR-Affectations/130006042_000001063136/130006042_000001063136_ HTTP/1.1
```

```
Host : domain.com
Date : Tue, 02 Dec. 2021 15:13:47 GMT
Content-length : 567
Content-type : application
```

Example of a response

```
HTTP/1.1 400 Bad Request
Date : Sun, 05 Dec. 2021 15 :14:47 GMT
Content-Type : application/xml
Content-Length : 125
Server : monserveur

<?xml version="1.0" encoding="UTF-8"?>
<Erreur>
   <Code>Paramètre invalide</Code>
   <Message>Le paramètre de requête «nomRapport» est incorrect. Les valeurs
autorisées sont : le nom d'un rapport existant ou «DERNIER_DELTA»</Message>
   <Resource>/GAR-Affectations/130006042_000001063136/130006042_000001063136_
   </Resource>
</Erreur>
```

Here is the list of possible error codes specific to this method:

HTTP Error Code	Code	Message
400 Bad Request	Request Invalid parameter	The request parameter " idDistributeur " is incorrect
400 Bad Request	Request Invalid parameter	The request parameter "reportname" is invalid. Allowed values are: the name of an existing report or "LAST_DELTA
400 Bad Request	Request Invalid parameter	Not all mandatory parameters are filled in: " idDistributeur "/"report name
409 Conflict	String (10 max)	The name of the report is not attached to the idDistributeur.

Table 64 - AssignmentReport Webservice - Description of Specific Error Codes - Download Report

13 Consent to leave the confidence framework

Resources linked to ERAM must be in cnformance with ERAM's principles. As such, they must not collect personal data during their operation other than the data securely transmitted via ERAM (ERAM attributes).
In some cases, however, and for staff only (teachers, documentalists and other staff), it may be necessary to request additional information – for instance, in order for them to register for an event/or a contest/etc.
This type of data collection and/or processing must be placed outside ERAM's confidence framework.
The consent module aims to provide a common framework for such exits from the confidence framework. This principle received a positive opinion from the Cnil in 2018.

13.1 Presentation of the confidence framework exit module

The notion of "confidence framework exit" refers to any link to a page in a resource or functionality that requires data collection and/or processing not provided for by the publisher in the declaration of conformance of the resource.
When browsing the resource leads to a "confidence framework exit", the resource must call ERAM's "consent module" service. This module displays a standardized warning requesting the user's consent before redirecting the user to the page outside ERAM's confidence framework. This module keeps a history of user consents.

13.2 Using the confidence framework exit module

13.2.1 Modality of the call

An ERAM resource requesting an exit from the confidence framework to a destination page must redirect the user to the URL of the ERAM web page consenting to exit the ERAM confidence framework.
This can be done by opening a link in a new tab or window.

13.2.2 Parameters of the call

The URL to ERAM's "consent module" service must include three parameters:
- idRessource=ark identifier of the resource requesting the exit;
- IDO=opaque identifier of the user exiting the resource;
- urlDest=URL of the destination page.

The parameters are provided as a request string embedded in the URL, encoded in "URL Encode".
The "urlDest" parameter is mandatory.

Example

For:

- A resource in in the ERAM confidence framework with the id
  ark:/12345/ft4w10060w/s3 ;
- A destination page outside ERAM's confidence framework with the URL
  https://monsite.editeur.fr/contact.html?from=gar&sortie=ok ;
- A user with the opaque ID for the resource:
  cad8d33f82565f8bdb4b0aaacb5a26e2.

To exit the confidence framework of the resource to the destination page outside ERAM, the resource must therefore redirect the user to the following URL

```
https://sortie-
confiance.gar.education.fr?idRessource=ark%3A%2F12345%2Fft4w10060w%2Fs3&IDO=cad8d
33f82565f8bdb4b0aaacb5a26e2&urlDest=https%3A%2F%2Fmonsite.editeur.fr%2Fcontact.ht
ml%3Ffrom%3Dgar%26sortie%3Dok
```

13.2.3 User journey

With the ERAM's "consent module" service, the user is asked to validate the exit from the ERAM confidence framework.
- If the user chooses to remain within the ERAM confidence framework, the resources (source and destination) are not informed.
- If the user chooses to exit the ERAM confidence framework, they are redirected to the URL of the destination page provided during the call.

14 Summary of notifications sent by ERAM

14.1 Harvesting module

Notification	Frequency	TDR	Warehouse Manager
List of records in error concerning the partner	Daily	X	X
Harvest report	Daily		X

Table 65 -Notifications - Harvesting Module

14.2 Post-harvest module

Notification	Frequency	TDR	Warehouse Manager
Report of consistency problems in the declaration of linked resources	Daily	X	
Report of problems with downloading resource thumbnails	Daily	X	

Table 66 - - Notifications - Post-Harvest Module

In the event that the post-harvest module identifies inconsistencies in the declaration of linked resources (family), a notification is sent to the TDR indicating the problems on the resource concerned.

The following checks are carried out:
- ▶ the consistency of the list of family members;
- ▶ the consistency between calling resources and resources called within a family of resources.

14.3 Assignment Report

This notification contains a link to a page on the ERAM portal containing:
- ▶ a zip archive in XML format containing all assignments made for a partner's resource(s) for all educational establishments connected to ERAM;
- ▶ delta files in XML format, generated over the last 30 days, containing only the changes in assignments occurred since the last file generation.

Notifications	Frequency	DTR	Warehouse Manager
Report on resource assignments and deletions as an XML file.	Daily	X	

Table 67 - Notifications - Availability of assignment reports

Management rules related to the use of assignment reports:

Rule	Description
RG01	The notification uses the format of ERAM notifications, contains a fixed introductory text and a link to the relevant page on the ERAM portal.
RG02	To access the portal, the user must authenticate himself.
RG03	The delta file and the complete file are updated daily if one of these actions is performed on the resource: assignment (by the automatic assignment batch or the assignment HMI) ; withdrawal of an assignment or reassignment to the same user via the assignment HMI; purge of expired subscriptions; change in assignment status performed by the VLE import batch.
RG04	Following the file update, a notification is sent to the Technical Resource Distributor (TDR)'s email address.
RG05	The complete XML file is unique for a technical distributor and is invariant. Therefore, it is not possible to upload an older version of the file.
RG06	The complete XML file contains, for a technical distributor and for each of its resources, all the opaque identifiers grouped by subscription and then by establishment.
RG11	The delta XML file contains, for a technical distributor and for each of its resources, only the IDO grouped by subscription and then by establishment for assignments that have been created or whose status has changed (withdrawn, deleted, assigned) since the last generation of the complete report.
RG07	For each IDO, the update date is available as well as the deactivation date (where necessary). The update date corresponds to the date of the status update.
RG08	The deactivation date corresponds to the date the status was removed or deleted. For other statuses, the deactivation date is not present.
RG10	Assignments that are permanently deleted at the end of the school year do not appear in the XML file.
RG12	Delta XML files are deleted after 30 days
RG13	Delta XML files have a name that enables them to be identified
RG14	A complete report is generated following the following events: change of school year for VLE projects change of school year for subscriptions In these cases, the corresponding delta file is not generated.

Table 68 -Management rules for using assignment reports

<u>Examples</u>

Examples are provided in the zip of support documents:

GAR_RTFS_V7.0_SupportDocuments_FR/AssignmentReport /Complete_123448915_0000000122425488.xml

GAR_RTFS_V7.0_SupportDocuments_FR/AssignmentReport/Delta_123448915_0000000122425 488

15 Linkage to ERAM

15.1 Partner Platform

During the linkage phase, all operations are carried out on ERAM partner testing platform (PFPART).
This platform, similar to the one used in production, is entirely dedicated to partner testing. It includes a VLE simulator and a user base.
This user database is populated with anonymized data generated by the Académie of Rennes in accordance with GDPR recommendations, providing educational structures in line with those that will be encountered in production.
Once the resource has been validated on the partner testing platform, it is transferred into production, and is subject to end-to-end validation before being distributed.
Once the resource has linked to ERAM, it is necessary for the resource provider to have an environment that is accessible from the PFPART for testing, support and management of changes, in an environment that is free from the constraints of personal data management.

15.2 Phases of linkage to ERAM

Phase	Description	Comment
1 - Initialization of the linkage project	Transmission of the resource provider's registration file, initialization of accounts	Following an information session, the resource provider sends a duly completed registration file. This file does not include any contractual commitment, which will be materialized by the signature of the contract, before the resource is put into production.
2 - Technical linkage	2.1 - Development of the ScoLOMFR record	Realization of the ScoLOMFR description of the resource, including all information necessary for the operation of the resource in ERAM.
	2.2 - Resource access module	Once the record is regularly harvested without any errors, the resource provider may access the PFPART environment to perform the SSO configuration work to allow access to the resource. The propagation of the logout from the VLE shall be set up during this phase.
	2.3 - Subscription management module	The resource provider shall develop a module to provide subscription information to ERAM via a "Subscribing to ERAM" web service. This function can be achieved by implementing standard tools or developed using the publisher's information system. These developments are validated for all resources

		that will may be linked to ERAM later on.
	2.4 – Conformance	The resource shall be adapted to ensure full conformance with applicable rules: centralization of authentication processes and personal data management, GDPR compliance, conformance to the Education Code, etc.
3 – Conformance validation	3.1 Validation of conformance in the partner testing platform	Once the resource provider has conducted its internal qualification of the resource on the partner testing platform, it creates subscriptions for its resource on two test establishments used by the Ministry of Education team. The ERAM team within the Ministry of Education validates the conformance of the resource. The resource provider shall make the necessary adaptations, where applicable.
	3.2 - Membership Agreement	Transmission and receipt of the signed membership agreement.
4 – Production roll-out	4.1 - Initialization in production	Initialization of accounts on the production platform
	4.2 – Production roll-out	The resource validated in the partner testing platform is authorized for production roll-out. This requires the resource provider to transmit the production platform record for its resource(s).
	4.3 - End-to-end validation	As soon as the resource has a distributable status in production, an end-to-end validation test is carried out to validate access to the resource in a real school chosen by the Ministry of Education.
5 - Distribution	Distribution of the resource	Once the validation is positive, the resource provider can distribute subscriptions to its client establishments. The resource is released into production.
	Assignment of the ERAM brand	The resource provider receives the "ERAM brand", which it can use in its communication.

Table 69 - The phases of linking a resource to ERAM

16 Providing technical information

A set of technical data is required for the initialization of the resource provider's accounts on the different platforms, in addition to the administrative data provided at the time of registration with ERAM.

16.1 Technical elements to be provided by resource providers

16.1.1 For the Commercial Distributor of Resources (CDR)

Field name	Comment
CSR[15] to the Ministry of Education's CA[16]	The procedure for creating the CSR is described in the "Subscriptions WebService" chapter.
OU[17] value from the CSR	The OU must start with 'GAR' (ERAM). It is recommended to have the following structure: GAR, followed by the company name (possibly abbreviated) and any additional information. The use of extended characters is not recommended.

Table 70- Items to be provided by the CDR

16.1.2 For the Technical Distributor of Resources (TDR)

Field name	Comment
SAML metadata URL per platform	If using SAML protocol. Not necessary if using CAS. The metadata must contain the elements necessary for authentication as well as the SingleLogout profile if logout is implemented.
EntityID by platform	If using the SAML protocol. Not necessary if using CAS.
Certificate with a public CA	If using SAML protocol. Not necessary if using CAS.
Logout URL by platform	If the disconnection is implemented and the CAS protocol is used. Not necessary if SAML is used.

Table 71 - Items to be provided by the TDR

---

[15] See 'Abbreviations and definitions'

[16] See 'Abbreviations and definitions'

[17] See 'Abbreviations and definitions'

16.2 Elements provided by RENATER

16.2.1 SAML metadata URL

ERAM authentication server provides SAML access validation services.

Platform	Designation	URL	IP
Partner testing platform	SAML Metadata	https://idp-auth.partenaire.test-gar.education.fr/idp/metadata	195.221.81.197
Production platform	SAML Metadata	https://idp-auth.gar.education.fr/idp/metadata	195.221.81.4

Table 72 - - SAML metadata URLs

16.2.2 CAS login URL

ERAM authentication server provides CAS access validation services.

Platform	Designation	URL	IP
Partner testing platform	CAS Login	https://idp-auth.partenaire.test-gar.education.fr/	195.221.81.197
Production platform	CAS Login	https://idp-auth.gar.education.fr/login	195.221.81.4

Table 73 - CAS login URLs

16.2.3 Well-known OIDC URL

Platform	Designation	URL	IP
Partner testing platform	well-known OIDC	https://idp-auth.partenaire.test-gar.education.fr/oidc/.well-known/openid-configuration	195.221.81.197
Production	well-known OIDC	https://idp-auth.gar.education.fr/oidc/.well-known/openid-configuration	195.221.81.4

Table 74 - Well-known OIDC URLs

16.2.4 VLE Simulator

The partner testing platform is based on an VLE simulator, which allows to simulate the access of different user profiles.

Platform	Designation	URL	IP
Partner testing platform	VLE simulator	https://simulent.partenaire.test-gar.education.fr	195.221.81.204

Table 75 -- URL of the VLE simulator

The login credentials dataset for the resource access test accounts shall be communicated by the administrative manager as soon as the resource provider's configuration is effective on the partner testing platform.

To activate the resource access test accounts on the VLE simulator, the partner must have:

▶ the dataset transmitted by the ERAM administrative manager;
▶ an email address.

16.2.5 Subscriptions Web Service

Platform	Designation	URL	IP
Partner testing platform	Subscriptions web service	https://abonnement.partenaire.test-gar.education.fr	195.221.81.198
Production platform	Subscriptions web service	https://abonnement.gar.education.fr	195.221.81.6

Table 76 -Subscriptions web service URLs

16.2.6 Resources Assigned to the User (RAA) Web Service

Platform	Designation	URL	IP
Partner testing platform	RAA Web Service	https://ws-raa.partenaire.test-gar.education.fr/ressources	195.221.81.208
Production platform	RAA Web Service	https://ws-raa.gar.education.fr/ressources	195.221.81.18

Table 77 - RAA web service URLs

16.2.7 Assignment Report Webservice (AssignmentReport)

Platform	Designation	URL	IP
Partner test	webservice rapportAffectation	https://ws-rapports-affectation.partenaire.test-gar.education.fr	195.221.81.213
Production	webservice rapportAffectation	https://ws-rapports-affectation.gar.education.fr	195.221.81.23

Table 78 - AssignmentReport webservice URLs

16.2.8 ERAM Portal

Platform	Designation	URL	IP
Partner testing platform	ERAM Portal	https://portail.partenaire.test-gar.education.fr	195.221.81.201
Production platform	ERAM Portal	https://portail.gar.education.fr	195.221.81.9

Table 79 - ERAM portal URLs

16.2.9 Exit page of the confidence framework

Platform	Designation	URL	IP
Partner testing platform	Exit of the confidence framework Page	https://sortie-confiance.partenaire.test-gar.education.fr	195.221.81.206
Production platform	Exit of the confidence framework Page	https://sortie-confiance.gar.education.fr	195.221.81.14

Table 80 - Exit of the confidence Framework page URLs

16.2.10 OAI Warehouse

The operation of ERAM relies on data provided via the harvesting of the warehouse designated by the TDR.
ERAM partners may request the harvesting of their own warehouse. They are then responsible for its operation.
They can also use the shared OAI-PMH warehouse made available by the Ministry of Education, in partnership with the Polytechnic University of Hauts-de-France (Valenciennes).
The operation is identical on the Partner testing and Production platforms.
Only the warehouse manager can add or modify records.

Platform	Designation	URL	IP
Partner testing platform	OAI-PMH Warehouse	http://scolomfr.univ-valenciennes.fr/ori-oai-repository	Records must be sent to the Administrative Manager via support.gar.renater.fr. The latter will be responsible for checking them and upload them into the warehouse. The date element of the technical validator role should be absent (or indicated as a comment) for the partner testing platform record.

Table 81- Shared OAI-PMH Warehouse made available by the Ministry of Education

16.2.11 Provision of certificates for web service access

16.2.11.1 Description

The authentication required to use ERAM's web services (Subscriptions, RAA Web Services, reportAssignment) is carried out on presentation of a certificate issued by the certification authority of the Ministry of Education, to guarantee the traceability of client/server authentication.

This certificate must be requested from the ERAM technical manager, via the transmission of a CSR (Certificate Signing Request).

16.2.11.2 Certificate request

> *The procedure for requesting a certificate is based on the use of OpenSSL software and is described below[18].*
>
> *The commands are to be adapted according to the encryption tool available to each partner.*

16.2.11.3 Steps

▸ Identify the instance/station/machine requiring a client certificate. This is the machine on which the client web service is installed. As a reminder, this instance/machine unit must be identifiable via an FQDN[19], and must therefore be named DNS[20];
▸ if necessary, install OpenSSL if it is not present on the machine requiring the client certificate;
▸ generate the CSR and the private key by following the steps described below;
▸ keep the private key, which should not be transmitted;
▸ send the generated CSR to the ERAM technical manager;
▸ Upon receipt of the certificate, install it on the chosen workstation/machine unit.

16.2.11.4 Generating the CSR

▸ Execute the command :

```
openssl req -nodes -newkey rsa:2048 -sha256 -keyout monserveur.key -out
nomfichier.csr
```

The two files genered by the command are named "monserveur.key and "nomfichier.csr".
The names given to these files are free, only extensions must be kept as described.
The naming suggestions below can help manage certificate requests more effectively:

▸ monserveur.key: replace "monserveur" with the name of the machine that requires a certificate;
▸ nomfichier.csr: replace "nomfichier" with your publisher's name followed by "_" and the name of the machine, without any spaces or special characters (publishername_machinename).

OpenSSL command will run, requesting for input a set of parameters detailed below. OpenSSL generates the files [monserveur].key (private key) and [nomfichier].csr (csr file)

> *Note: it is essential to keep the CSR and, above all, the private key.*

---

[18] See "abbreviations and definitions".

[19] See "abbreviations and definitions".

[20] See "abbreviations and definitions".

The elements to be provided in the CSR are described in the table below.

16.2.12 Certificate protection perimeter

Field	Value
Country Name (2 letter code) [AU]:	FR for an establishment in France (if the establishment is not in France, enter the country code)
State or Province Name (full name) [Some-State]:	Enter a "." (full point) to leave the field empty.
Locality Name (eg, city) :	To be filled in with the city of the publisher's headquarters
Organization Name (eg, company) [Internet Widgits Pty Ltd]:	Enter a "." (full point) to leave the field empty.
Organizational Unit Name :	ERAM [DCR|DTR] [organization name] [indication [optional indication of department within organization] It is recommended that no characters other than letters be used (no "-" or "_" in particular) The DCR|DTR indication is mandatory for partners who have both functions.
Common Name (eg, YOUR name) :	To be filled in with the FQDN of the machine The FQDN is of the form <host name>.<main DNS suffix>. The DNS must be in an identified domain.
Email Address :	For a production environment, put: "isr@education.gouv.fr" For a test environment, put: " isr-test@education.gouv.fr "
A challenge password :	Enter a "." (full point) to leave the field empty.
An optional company name :	Enter a "." (full point) to leave the field empty.

Table 82 - Certificate Application - CSR Parameter Details

16.2.12.1 Holder

Certificates for the Subscriptions Werbservice are issued to commercial distributors.
Certificates for the RAA Web Service are issued to technical distributors.
For partners who perform both technical and commercial distributor roles, it is necessary to apply for both certificates.

16.2.12.2 Platform

Each certificate issued is valid either on the partner testing platform or on the production platform.
At the start of the ERAM linkage operations, a CSR is sent to obtain the certificate for use in PFPART.

Before the production roll-out phase, it is necessary to apply for a new certificate, running on ERAM's production platform.