
EAS User Documentation

Release 0.9b1

Javier Quinteros and Andres Heinloo

May 16, 2019

Contents

1	Objective	1
2	The EIDA Authentication System	2
3	B2ACCESS: A proxy to the user home institution	2
3.1	New accounts via eduGAIN	3
3.2	New local accounts on B2ACCESS	5
4	Get a token from EAS	5
5	Users: Testing the whole workflow	7
6	Contributors	8

Warning: The only way to improve this service for our users is to receive continuous and constructive feedback. Please, read first very carefully this documentation and the provided examples to get (meta)data. If you have problems requesting (meta)data and you cannot find there the solution, please contact us reporting an issue at <https://github.com/EIDA/userfeedback/issues>

1 Objective

EIDA is formed by many seismological data centres along Europe. Most of the seismic waveforms archived at these data centres are open data, which could be anonymously downloaded. But for

some embargoed data it is necessary to be authenticated, and the user must be properly authorized by the network operator in order to access them.

The EIDA Authentication System (EAS) is a system designed to let users log in and request a “token”, which can be used as credentials for many EIDA services. From its conception, the EAS was designed to make use of the discovery service provided by eduGAIN (GEANT initiative), so that a user could login at EIDA by authenticating at his/her home institution, not with EIDA.

2 The EIDA Authentication System

A simple web page was designed to provide a way to request a token (expiring maximum in one month time) to be later presented to the EIDA services. This web page will redirect the user to a service called B2ACCESS and, after a successful login, will provide him/her a digitally signed human-readable file with all the attributes present in the user profile.

The web page also includes the possibility to upload a token to check the validity of its signature. This can be useful in case of problems using the token with an EIDA service.

All information needed for a user requesting a token is also present in the web page in the form of Questions and Answers. Technically, a “token” is a text file, which you will need to send along with your data request. Below is an example of what you will receive from the system:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

{"valid_until": "2019-05-08T10:21:26.269027Z", "cn": "John Doe",
"memberof": "/epos/experiment2;/epos;/", "sn": "Doe",
"issued": "2019-04-08T10:21:26.269034Z", "mail": "john.doe@gfz-potsdam.
→de",
"givenName": "John", "expiration": "1m"}
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcbAEBAgAGBQJcQyCmAAoJEEFpZp0AlwdXaBQIAL9I7lUriWaoWMDPAnUTLUVE
uA5iQfLwnkano8d18MSjP7ztGx/EO5+NUoutdXCpQFqDXmnk94HbxoOkSkzPPyHO
Tl4FTVsa0/wjdNDG/Gsua jZ9zAr0qRTYHGhU1EfcwrhZ/RCYAp9xUzQ4tS6jb0w=
=8kex
-----END PGP SIGNATURE-----
```

3 B2ACCESS: A proxy to the user home institution

B2ACCESS is a service provided by EUDAT and hosted at the Forschungszentrum Jülich. It acts as a proxy/hub to the home institutions of the users, but also allowing to create local accounts in case that the home institution does not take part in the eduGAIN approach. The possibility to login

using home credentials is available only in the case that the institution takes part in the eduGAIN initiative.

In order to know whether this is the case, a list of institutions is included in the block “Login with your institutional ID” and, due to the length of the list, a search field is also provided to allow for a quick search.

A new user must register itself by means of any of the following two methods:

1. Login at home institution: this is only available if the institution is found in the list at the main page of B2ACCESS.
2. Creation of a local account at B2ACCESS: if the user organization does not take part in eduGAIN, then a local B2ACCESS account can be created.

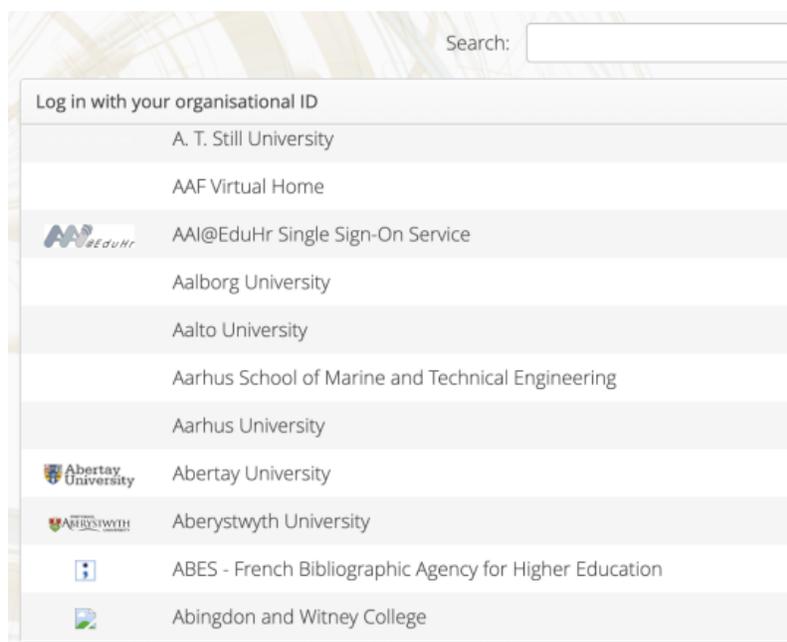


Fig. 1: List of eduGAINED Universities and Research Institutes present in the B2ACCESS main page

3.1 New accounts via eduGAIN

When the user finds its home institution, this can be selected and the user will be redirected to log in there with a message explaining that the login will be used by B2ACCESS for authentication purposes.

Once the user is successfully authenticated at their institution, it is sent back to B2ACCESS to finish the registration, which is usually just the confirmation of the data provided by the home institution. But before sending the information, **there is a checkbox available to request being part of EPOS. It is mandatory to check it.**

Welcome to ETH Zurich user authentication

You have requested access to a service that requires your authentication.

You are about to access the service:

EUDAT B2ACCESS of [e234](#)

Description as provided by this service:

AAI for EUDAT B2-Services

Please fill the fields with your nethz username and password (case sensitive) and click on the 'Login' button.

Username

Password

Disable 'single sign-on' (on public or shared computers)

Clear prior granting of permission for release of your information to this service.

[Login](#)

Fig. 2: Redirection to the user's home institution.

Fig. 3: Registration form including the EPOS checkbox, which is **mandatory** to check.

After sending the information a message will be sent to the email address informed to finalize the registration process.

3.2 New local accounts on B2ACCESS

Any user can access the B2ACCESS portal and register to have an account in the system. On the upper right corner of the main page, there is a link for this purpose (“Register a new account”). There are different technical ways to create this account, being the “Create B2ACCESS account (username only)” the recommended one due to its simplicity.

The user will need to fill a form with basic contact details (e.g. name, email). In this form, **there is a checkbox available to request being part of EPOS. It is mandatory to check it.** When the form is submitted, the email address will be validated with a message to the user containing a link for the validation.

4 Get a token from EAS

On the user side, once the user has been registered, a token to access data (or services) from EIDA can be requested at the following production server URL: <https://geofon.gfz-potsdam.de/eas>

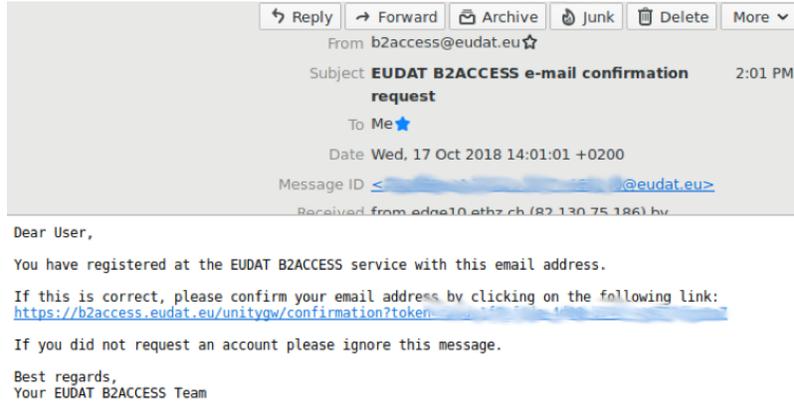


Fig. 4: Message received from the system to validate the e-mail account.

A registration form titled 'Registration form' with a '+' icon in the top right. The form contains several input fields: 'User name: *', 'Password credential: *', 'Repeat the password: *', 'Email *', 'Organisation Name *', 'Given name: *', and 'Surname: *'. Below these is a section 'Apply for membership' with a checkbox labeled 'EPOS'. At the bottom right are 'Submit' and 'Cancel' buttons.

Fig. 5: Registration form to create a local account including the EPOS checkbox, which is **mandatory** to check.

The user has to select how long the token will be valid (e.g. 1 day, 1 week, 1 month) and click on the button to request it. The first time, the user will be redirected to the B2ACCESS login page (from there it could be the home institution login page, in the hypothetical case of an eduGAIN approach), where the user has to login successfully. After the first login your browser could remember you in the same way as Google/Facebook and others do. Of course, you can always log out at any time. After the successful login, the token will be automatically downloaded and all the attributes related to him will be included.

Before the user information is being sent to EAS, a detail of these attributes would be presented to the user to confirm that they can be released. The user has at this point the capability to select/deselect different attributes to be included/excluded from the “token”. By default, everything is included.

If you plan to access a particular restricted dataset, you should be aware that you need to be first authorized by the network operator, so you must contact the operator before trying to access the data. If you are authorized after you download a “token”, the authorization will not be reflected there and you will have no access to the data. The solution is simply to request a new token, which will include the latest information about the datasets you are authorized to access.

5 Users: Testing the whole workflow

Once a user profile has been setup and is included in the Access Control List of the restricted dataset, you will need to follow the next steps to check that the whole workflow is valid:

- Request a token from <http://geofon.gfz-potsdam.de/eas> .
- Check with a normal text editor that the attributes in the token look reasonable. Do not modify it!
- Option 1: Use the `fdsnws_fetch` client to request data from the restricted stations archived at any data centre. At the moment of this test all data centres include updates to support this workflow. This client is included in the `fdsnwsscripts` package, which can be installed via `pip`. [See full example](#) .
- Option 2: clients provided by Obspy (version 1.1.1 or later¹) that support the automatic internal routing and token for EIDA (i.e. `RoutingClient`). [See full example](#).
- Option 3: Use <http://eida.gfz-potsdam.de/webdc3/> and `fdsnws` authentication, loading token.
- If some other tool has to be used, this should be taken into account on the client-side. Routing Service should be contacted to see where data is archived, and the `auth` method transforming a token into a short-live user/password at each data centre must be called.

¹ In some previous Obspy version there is a bug which you can patch for it to work. See <https://github.com/obspy/obspy/issues/2297>

6 Contributors

This documentation was written by [Javier Quinteros](#), Stefan Heimers, Philipp Kaestli, John Clinton, Jonathan Schaeffer, Helle Pedersen and others.