Technical Information on the EMREX-Network

June 2020

Further resources:
https://emrex.eu/
https://emrex.eu/wp-content/uploads/2020/01/Technical-Guide-to-EMREX.pdf

During a data transfer in the EMREX network, a user interacts with two systems.

The first one is the so-called SMP (Student Mobility Plugin, also described as the Emrex-Import-Interface), into which the data should be imported.
The SMP leads the user to the second system, the NCP (National Contact Point, also described as the Emrex-Export-Interface), from which data can be exported.
The NCP brings a user and their data back to the first system (the SMP) at the end of the process.
A step-by-step description is provided below:

1. The user authenticates himself in the SMP (e.g. student information system, Standalone-SMP, PIM).
2. Every export service in the EMREX-Network is registered in the EMREG-Register. In order to offer the user a list with available organisations owning an export interface. SMP application retrieves the list (in json format) through the central EMREG web service and displays it to the user.
   https://fsweb-demo.uio.no/emreg/list/test
3. The user chooses an NCP.
4. At this point, the NCP URL represents the significant information offered by the register. The public key of the NCP has to be kept in memory for later verification of the data.
5. A request with two parameters is prepared: The first one is a session-Id. It needs to be generated and has to be kept in memory of the SMP application. It is used later to identify and assign the export data package. The NCP will only use the sessionId to provide it back together with its own answer. As a second parameter, the SMP provides a return-URL, which is basically the SMP address itself, to which the export data (the ELMO file) should be sent.
6. By selecting an NCP in the frontend, the user triggers a request to the NCP in the following format:

   ```
   <form action="https://url_to_ncp" method="POST">
   <input type="hidden" name="sessionId" value="mysessionid12345">
   <input type="hidden" name="returnUrlvalue="https://url_smp"> </form>
   ```

7. The „url_to_ncp“ forwards to the login-site of the NCP, which is most probably integrated into a student information system (sis) or similar portal. The user should own an account on this portal.

8. After logging in, the user can select which data should be exported at course level.
9. The data available in an internal format is converted into the ELMO format.
10. A summary of achievements in pdf-format is integrated as Base64 String in the ELMO tag <Attachment>
11. The Elmo file is signed with a certificate.
12. The Elmo file is compressed by Gzip.
13. The Gzip is coded as Base64 String.
14. The data is inserted in a form with the following structure:

```
<form action="https://url_smp" method="POST">
<input type="hidden" name="sessionId" value="mysessionid12345">
<input type="hidden" name="returnCode" value="NCP_OK">
<input type="hidden" name="returnMessage" value="">
<input type="hidden" name="elmo" value="H4sIAJSMFI...AAAA==">
</form>
```

15. The delivery-URL of this request is the ReturnURL, that was sent together with the request to the NCP. The same applies to the sessionId.
16. The NCP Server embeds the form in the html-response to the client browser. The user can then decide to confirm sending it or not. A delivery of the request (meaning, the export data package to the SMP) can be then initiated by a click, or it can be stopped. The export data package is not sent directly by the NCP.
17. When the data arrives at the SMP, they can be assigned correctly with the sessionId that was sent originally to the NCP and that is sent back at this point. Additionally, an existing htttp-session of the browser can be used at the SMP.
18. The data is extracted, by Base64decode, unzip ...
19. The data is verified. For this, the Public Key for the document issuer that was retrieved from the EMREG register is used and the signature is verified.
20. The user name and the user birth date in the ELMO are compared with the ones of the person that logged in to the SMP system.
21. The user can view the extracted data.
22. The user can decide again if he wishes to save the data in the SMP system.

A weakness of the authentication is the login in two systems.
A user could try to log in to the NCP system with a different account. In this case, the data belonging to the different account is sent back to the SMP. The only verification is the comparison of the name and of the birth date of the NCP account contained in the ELMO with those in the SMP account.