|  |  |
| --- | --- |
| **World Meteorological Organization****COMMISSION FOR BASIC SYSTEMS****Task Team on Evolution of WIS**21-23 November 2017, Geneva | **TT-eWIS2017/Doc -XX** |
| Submitted by:José Mauro de Rezende 01.11.2017 |

# FEDERATION INITIATIVE AT GISC BRASILIA

## References

[1] <https://www.rnp.br/servicos/servicos-avancados/cafe>

[2] <https://www.switch.ch/aai/demo/>

[3] <https://www.switch.ch/aai/>

## Recommended Text

\_\_\_\_\_\_\_\_\_\_\_\_

# Action and Decision Summary

## Actions

[**A1** \_](#_Toc388521070)To take note

## Decisions

[**D1** \_](#_Toc388521074)Which RFC will is recommended for the metadata?

\_\_\_\_\_\_\_\_\_\_\_\_

## background

1. Since the introduction of WIS, providing access among its GISC´s is quite a big problem. The various services provided requires database with information about its users, and users need to register themselves to have access. One possibility to overcome this difficulty is to implement an authentication technology known a “Federation Identification”. It is a standard way to provide security and identification intermediation. If an organization has such “Identification Service” in place, it can offer “services” for those users who are “authorized” by its original institution.
2. After the meeting in Australia, Dave asked me to try it in Brazil and look for the possibility to use a federation schema on a WIS environment.

## federation

1. In practice, on a federation environment, it is possible to log in from a profile created locally, to be able to connect with other system in other networks and get access to the services provided remotely.
2. To be part of a Federation, the activities should comply:
* Unique Login (Single Sign On)
* Arrangement of organizations forming a Circle of Trust
* Intermediation and control of user data
1. Every organization has to follow some protocols and implement their authentication and security process. Each federation has an Authentication and Authorization Infrastructure. It defines the communication model between the parties.
2. Among the technologies used, the most important is the use of directory services, such as, LDAP, to store and organize the users’ information.
3. When the user access a particular service provider, the discovery services redirects him to a page that presents a list of identity providers. He chooses, then, his home institution and his browser is redirected to the identity provider of that institution. After authenticating the user, the identity provider passes the result of this authentication to the service provider and creates a user session associated with the user, so that access to new services within a certain time interval does not generate new authentication requests.

## GISC Brasilia

1. In Brazil there is an academic federation community called CAFe, which provides identification management for the research and education institutions in the country. RNP (National Education and Research Network) implemented it. Today most of the universities and researches organizations are part of the federation (https://www.rnp.br/servicos/servicos-avancados/cafe).
2. I started working with them in order to include INMET as part of their federation and to verify whether we could add the GISC Brasilia as a service provider.
3. We had several meetings and conversation until we get to the conclusion it would not be possible at this stage. We needed to do some extra work in order to take the correct way to go on. In our case, the authentication procedure were not robust and reliable. Therefore, we step back and now we are in the process to review and reconstruct it again. This time we have in mind to consider a possible WIS federation and include some metadata to allow such identification.
4. We got all the support from the RNP experts and they are willing to help us to construct our own Identity Provider Service. After that, we can go back and start again the process to enter the CAFe federation. RNP has a list of Best Practices, which they recommended us to follow.

## CONCLUSION

1. The use of the “Federation” on WIS environment could be an alternative for the identity management. If that is the case, what type of service the GISCs centres should provide?

## FEDERATION cafe and SWITCHaai

1. CAFe (Comunidade Acadêmica Federada) is an identity federation that brings together Brazilian teaching and research institutions. It was built based on the SWITCH, from Switzerland. The protocol WAYF (Where Are You From) at CAFe uses a PHP implementation developed by Switch. (<https://www.switch.ch/aai/support/tools/wayf/>). The SWITCHwayf code is published under a BSD license and provided "**as-is**".
2. I found a lot´s of useful information on <https://www.switch.ch/export/sites/default/edu-id/.galleries/files/SWITCH_edu-ID_Update_2017_all.pdf>
3. Their demo pages explain very well how the Authetication and Autorization Infrastructure (AAI) works <https://www.switch.ch/aai/demo/>.
4. The diagram bellow shows the organizations who participate on the SWITCHaai network.

