Contribution ID: **97** Type: **Long Talk**

Incident Response (IR) on credentials provided through a global federated AAI service.

Access to EGI services is also provided through Federated AAI, as for example eduGAIN (https://edugain.org/)i. In particular egi-checkin, our IdP/SP proxy is part of this infrastructure and allows users from around the globe to authenticate with their home institutions IdP and receive credentials that could be used to access to EGI services.
Our IR procedure therefore also have to cover the aspect to be able to deal with compromised accounts provided through the eduGAIN service.

In this workshop we want to raise awareness of the complexity of IR where we have to coordinate our IT security activities with a global service managing the authentication of users.

The focus is on the inter federation aspect of IR, and what the key players in IR can do, to deal with an incident requiring the collaboration of the operators (Federation, IdP, SP) contributing to the eduGAIN service and the coordination with eduGAIN CSIRT and EGI CSIRT.

The participants will get an introduction to eduGAIN, the relevant security policies, the key security roles, and the IR supporting frameworks like SIRTFI.

After that, the participants will have to deal with an artificial incident and apply the IR concepts presented before in a Table Top Exercise (TTX) set-up. Although it's a "made up" scenario, it consists of real world incidents we had to deal with.

Each of the security roles will be taken by a group, in which the possible reaction to the developing incident response situation needs to be discussed and the found reaction fed back to the incident coordinator.
The goal here is to identify the organisational obstacles we may run into during IR, and check if the existing procedures are clear enough.

The enabled learning objectives (what the participants should learn) include:
* IdP/SP logfile analysis (check for/find a reported ID)
* know SIRTFI v2, and understand applying it
* Know how eduGAIN is organised, role of Federations, eduGAIN and eduGAIN CSIRT
* Name the risks of federated Identity Management.

Topic

Trust and Security: Access control

Primary authors: KOURIL, Daniel (CESNET); GROEP, David (Nikhef); KELSEY, David (STFC); DUSSA, Tobias (DFN-CERT)

Presenter: GABRIEL, Sven (NIKHEF)

Session Classification: Trust & Security