Table of Contents

Proposed EMIR Deployment for National Grid Infrastructures (NGI)

EMIR is a federated service endpoint registry, enables deployment of registries in an hierarchy as well as in a P2P fashion. Following figure depicts an example of EMIR deployment at the NGIs (Germany and Hungary) and at the federation level (e.g. EGI).

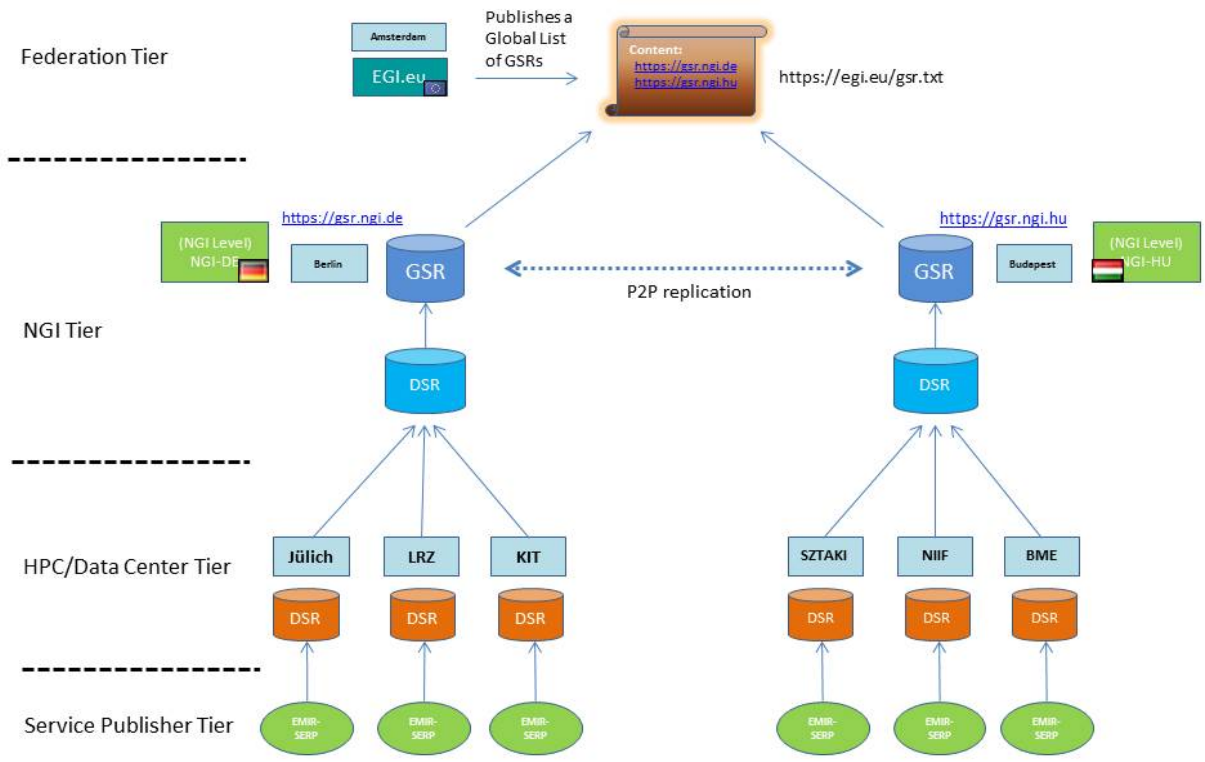

Figure 1: Deployment of EMIR in EGI and NGIs

Service Publisher Tier

EMIR's Service Endpoint Record publishers (EMIR-SERP) are deployed at this tier. They are responsible for making the endpoint information available to the Domain Service Registry (DSR) of HPC/Data Center Tier. The endpoint information should be a valid JSON document with all the mandatory attributes defined.

HPC/Data Center Tier

The Domain Service Registries (DSR) are deployed at this tier. It receives the requests from EMIR-SERP containing the endpoints information (which gets registered(or modified)). The administrator of the DSR make sure that the authentication (SSL/TLS) and authorization (ACL or XACML) settings are properly configured.

There are three mandatory configuration options (in the **emir.config** file) to enable the secure deployment of HPC/Data Center tier

- Configure trust anchors and credentials
- Enable authorisation (using ACL) while adding DN of all the relevant EMIR-SERPs into the *emir.acl* file.
- Set parent Address to the NGI tier DSR

NGI Tier

The NGI Tier deploys DSR and GSR, the DSR only aggregates the information from DSRs below its hierarchy. However, for the GSR publishes the information two different sources: children DSRs (at HPC/DC tier) and GSR from other NGIs.

There are three mandatory configuration options (in the **emir.config** file) to enable the secure deployment of NGI tier (DSR)

- Configure trust anchors and credentials,
- Enable authorisation (using ACL) while adding DN of all the relevant HPC tier DSRs into the *emir.acl* file,
- Set it's parent Address to the NGI (same) tier's GSR

For the GSR:

- Configure trust anchors and credentials,
- Enable authorisation (using ACL) while adding DN of all the relevant NGI tier DSRs into the *emir.acl* file,
- Set provider list to URL of the **Global List**, which resides at the Federation tier
- Set global flag to **TRUE**

Federation Tier

The Global List containing a list of participating GSR URLs. It has to be published by a central body (e.g. EGI), where all the participating (or peer) GSRs can access to build a P2P network at the federation tier.

This topic: EMI > EMIRFORNGI
Topic revision: r4 - 2012-07-17 - IvanMartonExCern