Evaluation of REEP

REEP was launched a few years ago with the aim to offer an external registry for federations. It had some clear use-cases in the beginning, but later due to eduGAIN offering more features it was parked and operated as best effort.

Over the last time, the insterest in REEP is renewed, mostly in light of the discussing in the Sirtfi WG to look for a registry to host Sirtfi-ed entities.

We are at a point where a decision is needed as to whether improve REEP or to slowly fade it out. It would be very useful if we had a clear understanding of REEP requirements/use-cases as well as of what is currently not working.

Based on the information collected a decision can be made on how to proceed.

Use Cases / Technical Requirements

Requirement	**Bug**	**Community /federations /services** **the needs come from**	**Does REEP support this already?**
The ExLibris Alma library system reportedly creates one IDP-specific SAML SP for every customer/institution, i.e., thousands of virtual SPs, each one only usable by a single IDP. We're not convinced we should register these in the federation, as federations are about scaling things. (Multi-tenancy is the opposite, in many ways.) Maybe having someone stuff those entities (for n IDPs register n × Alma SP) into REEP and having the federation aggregate entities from there would be beneficial.		ACOnet, but possibly library consortia/networks acting on behalf of their Alma customers the world over	✅
Improve DCV approach to reflect up to date processes.			
Support for entity categories - is this there?			
invite friend says: "$name has invited you to the Terena PEER site." Needs cleaning.			
what to do with existing domains? REEP "clear out"			
DCV methods: HTTP/S, DNS, email -- not all are covered in REEP policy. Need to update policy.			
I can extract the certificate for validation of the metadata signature from the XML, no problem, but if we want people to actually validate the metadata signature we should publish the cert prominently (plus how often one should refresh, validUntil, etc.)			
what about the security officers mentioned in the past? (i.e., once the private key for signing is in the HSM do we want a procedure to reconstruct it, in exceptional circumstances? (I'm OK with "no", though REEP's potentially wordl-wide and unknown to us metadata consumer communtiy may not be reached easily. so a re-keying will be rather disruptive, I think.)			
Is the key from the key signing party (of many years ago, TNC Dublin, IIRC?) already being used?			
The exported metadata XML lacks a meaningful name/ID - currently it's `Name="http://127.0.0.1:8080/entities"` . It would be useful when processing/aggregating the metadata.	Yes		