Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Current/Recent Tasks

Who	What	When	Status
Romain	Add Act-Inform diagram to the eduGAIN security wiki when it gets created		Done
Shannon	Generate list of contacts Tool link to the right. This python tool will generate a CSV of contacts in the order of precedence that we decided on. Should properly handle multi-valued contacts.		Link to a tool to generate contact info from an XML aggregate
Shannon/Tom	List here the FOs that prefer to send the survey invite themselves: KAFE, SWAMID, AAF, TENET, SURFconext, LEAF	April 29	In progress

Older tasks are at the bottom of running Sirtfi call notes document.

April 22, 2021

Attending: Alan B, Sven G, Uros S, Daniela P, Tom B, David G, Hannah S

Regrets: Pål A, Dave K, David C, Romain W

Agenda:

1. Update on the survey.
2. Revisit the Sirtfi through proxies discussion and decide if something should be added to Sirtfi v2 to address this need.
3. AOB

Tom is recording those federations that prefer to send the survey invite themselves in the bottom row of the task table at the top of this doc.

The WG discussed the “Sirtfi through proxies” problem for most of the hour. Several things were noted:

Members rejected the idea that Sirtfi IdPs should also send something like an eduPersonAssurance value with the semantic that the assertion is from a Sirtfi compliant IdP. This approach imposes the cost of solving the problem on those who are not a party to it. Also, it is a very costly approach since it would require a great deal of change management across the world.

Members also noted that, in the constrained use case of an e-infrastructure consisting of a proxy and its registered RPs, none of which is another proxy, the problem can be addressed by amending RP registration procedures to note when an RP requires the origin IdP to be Sirtfi compliant. This data would enable the proxy operator to implement that policy on behalf of the RP.

However, there can be chains of proxies between the origin IdP and ultimate RP. For this the WG recognized that the first proxy in the chain, ie, that which directly interacts with the origin IdP, can insert in a suitable attribute (to be created, perhaps in the voPerson schema) indicating whether or not the origin IdP has the Sirtfi tag in its entity metadata. That way each successive proxy in the chain can pass this information along in whatever formats are native to their e-infrastructures. The ultimate RP can then apply its policy itself, or the e-infrastructure within which it is registered might provide a service to their RPs of managing that at the proxy - only passing an assertion when the origin IdP is Sirtfi compliant.

Members noted that the idea of passing Sirtfi status in a voPerson attribute to downstream parties is generalizable to any entity attribute, providing a way for RPs that are not direct federation participants (including proxies) to have a view of that sort of metadata about the origin IdP.

Members also noted that the idea of registration information about whether an RP's access policy includes a requirement for origin-IdP Sirtfi compliance can be expressed among eduGAIN SPs if a new "Sirtfi support entity category" was introduced. However, this is not needed in R&E federation (SPs can look at the metadata themselves and simply apply their access policy).

The WG also discussed whether it is ok for a proxy, on its upstream or SP side, to assert Sirtfi compliance without concern for the compliance status of its registered RPs. It was observed that the proxy operator can always disable access through the proxy by a specified federated identity, and in other regards implement all of the specifications. Likewise, it is the proxy's operation, alone, that determines whether it can express Sirtfi compliance on its downstream interface (its IdP interface).

The WG further distinguished between two types of RP access policies: the first in which the RP requires the immediately upstream IdP (the proxy's) to be Sirtfi compliant, and the second, in which the RP's access policy is to require the origin IdP to be Sirtfi compliant. It is only the second of these that poses a problem addressable along the lines noted above.

None of the above appears to be hindered by Sirtfi as it stands, and no enhancement to Sirtfi would further enable solutions like those mentioned above. None of this appears to be work that the Sirtfi WG should undertake.

Where to start on a solution, since it‘s not Sirtfi’s to do? The AARC Architecture Committee (appint list), under the aegis of AEGIS, seems an appropriate venue. David G or Uros S will work out between them who will raise this there, relay our discussion and conclusions, and offer the WG to consult with them as they may wish.