24 May 2017

GN4-2: SIRTFI Interview Survey Report

Supporting Documentation

Task Item:	GN4-2-JRA3-T1
Dissemination Level:	PU (Public)
Authors:	Tangui Coulouarn, Jule Ziegler, Brook Schofield, Pål Axelsson

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Interview Survey Report

This report syntheses the results of a series of short informal interviews with federation operators from March to May 2017. The main goal of the survey was to understand how they perceive the **Security Incident Response Trust Framework for Federated Identity (SIRTFI)**[1].

On the basis of the survey, three main recommendations can be made:

- Overwhelming priority should be adoption of the existing framework rather than further significant development (except a few minor adjustments around its scope);
- Self-assertion has to be completed with some degree of compliance checking. For this purpose, some tools have to be developed; GÉANT should deliver these tools, compliant to eduGAIN BCP recommendations, and make them available on the eduGAIN technical portal;
- There should be an outreach efforts towards IdPs and SPs. GÉANT and AARC should cooperate on outreach effort. GÉANT in particular should support federations in their engagement with IdPs. It would help if some major eInfrastructures or projects (such as EUDAT or Elixir) indicated their support for SIRTFI (without mandating it, at least for a period of 12 months).

The survey

The interviews were structured around the following questions:
Q1. Why do you think about SIRTFI?
Q2. Any enquiries from your IdPs or SPs?
Q3. Are you building any tool - do you envision central tools or will you build them?
Q4. Self-asserted? Drawn from their own metadata or will you augment the metadata centrally?
Q5. Incident Response Readiness testing? How? Who?

Interviews were carried out with representatives of the federation of the following countries:

- Canada;
- Denmark;
- Germany;
- Greece;
- Italy;
- Sweden;
- Switzerland;
- The United Kingdom;
- USA.

[1] https://refeds.org/sirtfi

Results

Generally there is an agreement that **SIRTFI is a positive development** and it is therefore recommended by all interviewed federation operators to their constituents. It is needed by SPs who provide access to sensitive data (and **it will be a requirement in the second version of the Data Protection Code of Conduct (CoCo) so that CoCo meets the expectations of GDPR**). It is also useful for other reasons: because it makes federation people speak with security people (a limit of this comes from the fact that these two groups deal with different concepts: security people see IP addresses while federation people see entities); because it helps federation operators solve the issue of data which is not updated (e.g. in the case they plan to do periodic checks of the security contact).

The level of adoption of SIRTFI is generally very low at this early stage. The need to access resources at CERN has played an obvious major role in getting these early adopters to comply with SIRTFI. The tool sending an email to IdP administrators is generally considered as useful (as long as emails are not sent to security contacts) but some federation operators criticised the process (incl. the unilateral decision by CERN to impose SIRTFI before the specification was final).

There is a recognized **need for federation operators to play an active role to incite IdPs/SPs to adopt SIRTFI.** The problem of SIRTFI is that the benefits are not always obvious. Webinars are mentioned as a strategy as well as mentions in newsletters, user meetings, etc. For that purpose, it has been mentioned several times that "good stories", probably anonymised, where the use of SIRTFI actually helps would be very welcome. On another level, there are some expectations that the **self-assessment tool currently developed within GÉANT JRA3T2 is going to help** as well as the central support for interfederation issues (as recommended in https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf Appendix 1).

It would also **help if other major eInfrastructures such as Elixir or EUDAT recommended SIRTFI** (or to convince an SP who opted out of eduGAIN for security reasons to join because of SIRTFI).

Most interviewees however do not want to "push too hard" for adoption. It was mentioned several times that the role of a federation is to support rather than force federation members with varying resources and abilities into compliance.

Evolution of SIRTFI: most interviewees agree **that SIRTFI should not be changed in the short term, except if it can ease adoption.** However, some **minor amendments could be made around the scope of SIRTFI** (In particular it was questioned whether compliant institutions should be expected to use TLP for everything) and **whether SIRTFI incidents should be tagged as such in communications**.

Self-assertion raises questions for all interviewees. Some federations are small enough for federation operators to check the validity of the asserted information thanks to their knowledge of people. In larger federations, when there is self-assertion (as opposed to a process by which the metadata is augmented by the federation operators with an ex-ante control), there is a hope that there will some kind of **"community policing" (ex post control as opposed to an ex ante control) and that there will be improvements in quality as shared experience grows**. It has also been asked whether it would help to demand a signed document asserting formally SIRTFI compliance (so there is ownership at the local institution).

"eduGAIN incident response readiness testing": **A tool or a set of tools to check compliance would be welcome in the future.** As mentioned by interviewees, an easy way to start would be to send an email to the security contact and see how fast they answer. As most interviewees don't want to "push too hard" (cf. above) and sometimes even fear some form of backlash from IdPs if they do, it seems that it could help to let some time pass before a third party checks the validity of the information which has been asserted. As mentioned above, several federation operators have chosen to augment themselves the metadata for institutions and want some mechanisms in place so to guarantee that SIRTFI is taken seriously.

As a first step, it would help to formalize the process for checking compliance, for example a document explaining the different steps to be taken in order to assess compliance.

Ownership: **REFEDS is perceived as the right owner for SIRTFI.** A mentioned problem is that most IdP admins don't know REFEDS; it is an extra reason to state the responsibility of the federation to introduce SIRTFI into their trust framework. **GÉANT has also been mentioned as a major player** (the reasoning being that the most common use case for SIRTFI is interfederation, GÉANT is maintaining eduGAIN and should therefore maintain SIRTFI). However, GÉANT will concentrate on operational implementation in eduGAIN and in contributing to SIRTFI at REFEDS.

Notes:

- Subsidiarily it was noted that SIRTFI contributed to making KALMAR obsolete.
- In Sweden, there is already assurance level (AL1 and AL2): 50% of IdPs already work with AL and therefore comply with some the requirements of SIRTFI.
- In Greece, there are serious issues with staffing and other resources in institutions, which make it difficult to comply to SIRTFI. This is reinforced by the conclusions of the 2015/2016 REFEDS survey which shows significant inequalities in staffing and resource of federations throughout Europe.