THIS IS VERSION 0.2 (DRAFT)

Start with words from SCI document version 1

A Trust Framework for Security Collaboration among Infrastructures

http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

Old Workplan (July 2016)

Start with the part related to Incident Response.
Then move to Data Protection.
Afterwards - add behaviour of the Proxy itself, the Community Attribute Authority and credential stores.

BUT - 1 Dec 2016 - start with participant responsibilities

Must allow for contracts.MoUs, SLAs, policy sets

Audience is the SP federation (or data controller of the proxy) not individual SPs
And/or the Data Controller of the Proxy

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

- AARC NA3 Task 3.4 Draft Document - version 0.2

Need an Introduction explaining the aims of the document etc etc. Framework binds together the SPs belonging to a Research Community sitting behind an IdP/SP Proxy. Enables eduGAIN federations and IdPs to trust the IdP/SP Proxy (which needs to assert R&S, Sirtfi, DP CoCo **on behalf** of the whole SP community). Snctfi enables the Proxy to do the assertions.

1. Glossary

The following terms are defined for use in the ~~SCI~~ Snctfi document:

Infrastructure	All of the IT hardware, software, networks, data, facilities, processes etc. that are required to develop, test, deliver, monitor, control or support *services*.
Distributed IT Infrastructure (DII)	An *Infrastructure* together with its management, *Resource Providers* and *Service Operators*. It provides, manages and operates (directly or indirectly) all the *services* required by the *Resource Providers* and their collections of *users*.
Resource	The equipment (CPU, disk, tape, network), software, middleware and data required to run a *service*.
Service	Any computing, storage, preservation, or software system which provides access to, information about or controls *resources.*
Resource Provider	The smallest *resource* administration domain in a DII. It can be either localised or geographically distributed.
Service Operator	An entity responsible for the management, deployment and operation of a *service*.
Participant	Any entity providing, using, managing, operating, supporting or coordinating one or more *service(s).*
User	An individual or an organisation who has been given authority to access and use *resources*.

~~computing grids and/or clouds, as well as cooperating computing facilities managed by di~~

ADD sections on behaviour of Proxy/Gateway and associated AA and credential store?

Address Sirtfi, DP CoCo, new AARC DNA3.5 Data Protection policy guidance, REFEDS R&S. R&S first to be mentioned?

What about AA addtional attributes that are more sensitive

V1.0 restricted to R&S bundle.

Snctfi requires R&S SPs and Sirtfi and "CoCo/DNA3.5"

Comment [1]: for just one SP behind the proxy? majority? all?

What do we call the "infrastructure/set of SPs"?
Could we add a template "contract" to be adopted by internal SPs? (TomB)
Should the SP Proxy then publish its Snctfi status/policies etc?

2. Operational Security [OS] and Sirtfi

Retaining operational availability and integrity is the most urgent and visible aspect of security. ~~Each of the collaborating infrastructures~~ Each of the SPs in the "Community" and the Proxy must meet all of the requirements specified in Sirtfi V1.0 ~~therefore have the following:~~

- ~~[OS1] A security model addressing issues such as authentication, authorisation, access control, confidentiality, integrity and availability, together with compliance mechanisms ensuring its implementation~~

Comment [2]: keep in Snctfi

We need the binding mechanism from OS1 somewhere else

- ~~[OS2] A process that ensures that security patches in operating system and application software are applied in a timely manner, and that patch application is recorded and communicated to the appropriate contacts~~
- ~~[OS3] A process to manage vulnerabilities (including reporting and disclosure) in any software distributed within the infrastructure. This process must be sufficiently dynamic to respond to changing threat environments~~

- ~~[OS4] The capability to detect possible intrusions and protect the infrastructure against significant and immediate threats on the infrastructure~~
- ~~[OS5] The capability to regulate the access of authenticated users~~
- ~~[OS6] The capability to identify and contact authenticated users, service providers and resource providers~~
- ~~[OS7] The capability to enforce the implementation of the security policies, including an escalation procedure, and the powers to require actions as deemed necessary to protect resources from or contain the spread of an incident~~

3. Incident Response [IR]

The management of risk is fundamental to the operation of any Infrastructure. Identifying the cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.

Meet requirements of Sirtfi version 1 - single section

~~It is imperative that every infrastructure has an organized approach to addressing and managing events that threaten the security of resources, data and overall project integrity.~~

~~Each infrastructure must have the following:~~

- ~~[IR1] Security contact information for all service providers, resource providers and communities together with expected response times for critical situations~~
- ~~[IR2] A formal Incident Response procedure. This must address: roles and responsibilities, identification and assessment of an incident, minimizing damage, response & recovery strategies, communication tools and procedures~~
- ~~[IR3] The capability to collaborate in the handling of a security incident with affected service and resource providers, communities, and infrastructures~~
- ~~[IR4] Assurance of compliance with information sharing restrictions on incident data obtained during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with site-specific security teams on a need to know basis, and will not be redistributed further without prior approval~~

4. Traceability [TR]

The minimum level of traceability for the Infrastructure is to be able to identify the source of all actions (executables, file transfer, etc.) together with the individual initiating the actions. In addition, sufficiently fine-grained controls, such as blocking the originating user, system or service and monitoring to detect abnormal behaviour, are necessary for keeping services operational. It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.

Sirtfi Version1

~~The aim is to be able to answer the basic questions "who, what, where, when and how" concerning any incident. This requires retaining all relevant information, including accurate timestamps and the digital identity of the initiator, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorise (including identity changes) and disconnect.~~

~~Each infrastructure must provide the following:~~

- ~~[TR1] Traceability of service usage, by the production and retention of appropriate logging data, to identify the source of all actions as defined above~~
- ~~[TR2] A specification of the data retention period, consistent with local, national and international regulations and policies~~
- ~~[TR3] A specification of the controls that the resource provider implements to achieve the goals of [TR1]~~

5. Participant Responsibilities [PR]

All participants in a ~~group of collaborating infrastructures~~ community of SPs need to rely on appropriate behavior by various actors in both their own and other infrastructures. We separate these responsibilities into behavior expected of:

- Individual users
- Collections of users
- Resource providers and service operators

Each infrastructure must ensure that the various participants are aware that they have these responsibilities.

5.1 Individual Users

Each ~~infrastructure~~ SP or the Community must provide:

- [PRU1] An Acceptable Use Policy (AUP). The AUP must at least address the following areas: defined acceptable use, non-acceptable use, user registration, protection and use of credentials, data protection and privacy, Intellectual Property Rights (IPR), disclaimers, liability and sanctions
- [PRU2] A process to ensure that all users are aware of, and accept the requirement to abide by, the AUP
- [PRU3] Communication to their users of any additional restrictions or requirements on acceptable use that arise out of new collaborative partnerships

5.2 Collections of Users

A Collection of users is a group of individuals organised around a common purpose jointly granted access to the Infrastructure. It may serve as an entity which acts as the interface between the individual users and each Infrastructure. In general the members of the Collection will not need to separately negotiate with Resource Providers or Infrastructures.

Examples of Collections of users include: User groups, Virtual Organisations, Research Communities, Virtual Research Communities, Projects, Science gateways, and geographically organised communities.

Each infrastructure must have:

- [PRC1] A process to ensure that all Collections of users using their infrastructure are aware of, and accept the need to abide by, various policy requirements
- [PRC2] Policies and procedures regulating the individual user registration and membership management (registration, renewal, suspensions, removal, and banning). At a minimum these must address the accuracy of contact information both for initial collection and periodic renewal

Do we need to address data protection issues

Collections of users must:

- [PRC3] be aware that they will be held responsible for actions by an individual member of the collection which in turn may reflect on the ability of other members to utilise the infrastructure
- [PRC4] ensure a way of identifying the individual user responsible for an action
- [PRC5] keep appropriate logs of membership management actions sufficient to participate in security incident response
- [PRC6] define their common aims and purposes and make this available to the Infrastructure and/or Resource Providers to allow them to make decisions on resource allocation

5.3 SP Resource Providers and Service Operators

The Infrastructure must have policies and procedures in place to ensure that Resource Providers and Service Operators understand and agree to abide by expected standards of behaviour, including:

- [PRR1] vulnerability patching
- [PRR2] incident reporting
- [PRR3] physical and network security
- [PRR4] confidentiality and integrity of data
- [PRR5] retention of appropriate logs

6. Legal Issues and Management procedures [LI]

Infrastructures, resource providers, service providers and collections of users must have policies and procedures, appropriately communicated to all participants, that address legal issues including but not limited to the following:

- [LI1] Intellectual Property Rights clarifying the rights and obligations of the participants
- [LI2] Liability responsibilities and disclaimers to make the participants aware of their obligations
- [LI3] Software licensing clarifying the rights and obligations of the participants
- [LI4] Dispute handling and escalation procedures
- [LI5] Data Protection responsibilities (also see the next section)
- [LI6] Any additional regulations such as export controls, ethical use, externally imposed data protection and/or access control requirements

7. Protection and processing of Personal Data/Personally Identifiable Information [DP]

Separating out the various types of attribute - here or a separate document

Infrastructures, resource providers, service providers and collections of users must have policies and procedures addressing the protection of individuals with regard to the processing of their personal data (PII) collected as a result of their participation in the infrastructure, including but not limited to:

- [DP1] Accounting Data
- [DP2] User Registration Data
- [DP3] Monitoring Data
- [DP4] Logging Data
- [DP5] ~~Data owned by or produced by Users or Collections of Users~~

The Community of SPs and the Proxy must have a Data Protection Policy binding all participants to a single framework (as recommended in AARC DNA3.5)

Comment [3]: should be published somewhere permanent, e.g. arxiv, conference proceedings, somewhere else

Comment [4]: by FIM4R