A Security Incident Response Trust Framework for Federated Identity (Sir-T-Fi)

Editor: David Kelsey, STFC Rutherford Appleton Laboratory, UK.
DRAFT DOCUMENT (not yet approved or adopted)

Abstract
The Security for Collaborating Infrastructures (SCI) group is a collaborative activity of information security officers from several large-scale distributed IT infrastructures (DITIs), including EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE. SCI is developing a framework to enable interoperation of collaborating DITIs with the aim of managing cross-infrastructure operational security risks, to build trust and develop policy standards for collaboration especially in cases where we cannot just share identical security policy documents.

Audience
This document is intended for use by the operational-security personnel responsible for developing and maintaining security policies and procedures for their DITI.

Table of Contents

1 Sir-T-Fi

To get started we will identify a number of IdPs at willing key Universities or Labs for the research community to implement this trust framework in its draft form and signal such adoption in metadata.

- At this time, only address security incident response
- Needs to be light-weight
- IdPs self assert
- Federation Operators act as conduits of information from IdP
- Use eduPersonAssurance or "SAMLAuthenticatonContextClassRef" in assertions from IdP http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
- Agree to use a separate profile of this for IdPs
- Would be useful to have a filtered metadata aggregator
- There is no defined security contact in metadata so we could use abuse@idp.example.com or just use the technical contact or abuse@scope or
    - https://spaces.internet2.edu/display/InCFederation/Contacts+in+Metadata

Need to clearly define the scope, is it IdP or also AA? What about metadata handlers?

2 Introduction

In recent years we have seen the implementation of a variety of infrastructures supporting distributed computing environments and sharing of resources. Each such infrastructure consists of distributed computing and data resources, users (who may be organised into separate user communities), and a set of policies and procedures. Examples of such infrastructures include computing grids and/or clouds, as well as cooperating computing facilities managed by different organisations.

Even when such an infrastructure considers itself to be decoupled from other infrastructures, it is in fact subject to many of the same threats and vulnerabilities as other infrastructures because of the use of common software and technologies. Moreover, there may be users who take part in more than one infrastructure and are thus potential vectors that can spread infection from one infrastructure to another. Finally, one infrastructure may want to extend rights to use its resources to users who are enrolled in a different infrastructure. In each of these situations, the infrastructures can benefit from working together and sharing information on security issues.

Security in a distributed collaborative environment is governed by the same principles that apply to a local centrally managed system, but complicated by the diversity of sites (both in terms of hardware and software systems and in terms of local policies and practices that apply), and by the lack of a centralised management hierarchy that can "order" certain operations to be performed in specific ways.

Governing principles include:

- The management of risk; both to mitigate the most likely occurring and dangerous risks, and to take counter measures that are commensurate with the scale of the involved risks
- Containing the impact of a security incident while keeping services operational, but in certain cases this may require identifying and fixing a security vulnerability before re-enabling user access
- Identifying the cause of incidents and understanding what measures must be taken to prevent them from re-occurring
- Identifying users, hosts and services, and controlling their access to resources, all of which must be sufficiently robust and commensurate to the value of the resources and the level of risk and must comply with the regulatory environment
- Active monitoring to detect and reduce the impact of security incidents

In this document we lay out a series of numbered requirements in six areas (operational security, incident response, traceability, participant responsibilities, legalities, and data protection) that each DITI should address as part of promoting trust between DITIs.

To evaluate the extent to which the requirements described in this document are met, we recommend that each DITI assess the maturity of its implementation according to the following levels:

Level 0: Function or feature not implemented

Level 1: Function or feature exists, is operationally implemented but not consistently documented

Level 2: Function or feature is comprehensively (and up to date) documented and operationally implemented

Level 3: Function or feature implemented, documented, and reviewed by an independent external body

We encourage openness and transparency in the documentation and for Levels 2 and 3 we recommend that wherever possible such documents should be made available to collaborating DITIs as a way of promoting trust.

2.1 Glossary

The following terms are defined for use in the SCI 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 (DITI)	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	A means of delivering access to, information about or controling *resources.*
Resource Provider	The smallest *resource* administration domain in a DITI. 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.

3 Operational Security [OS]

Retaining operational availability and integrity is the most urgent and visible aspect of security. Each of the collaborating DITIs must 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
- [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 verified, recorded and communicated to the appropriate contacts
- [OS3] A process to manage vulnerabilities (including reporting and disclosure) in any software distributed within the infrastructure.
- [OS4] Mechanisms deployed to detect possible intrusions and protect the infrastructure against significant and immediate threats on the infrastructure
- [OS5] The capability to suspend, modify or terminate the access rights of a client, e.g. a user, a portal or of a collection of users, in a timely manner
- [OS6] The capability to identify and contact clients, e.g. authenticated users or portals, and Service Operators
- [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

4 Incident Response [IR]

A security incident is the act of violating an explicit or implied information security policy.

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.

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

We need general intro for IdP

Each Claims Processor must:

- [IR1] Provide security contact information who will respond in a timely manner according to current best practice, e.g. one working day.
- [IR2] Have an established Incident Response procedure. This must address: roles, authority, and responsibilities; identification and assessment of an incident; minimising damage, response and recovery strategies;

- [IR3] The ability and the willingness to collaborate in the handling of a security incident with affected Claims Processors;
- [IR4] Respect and should use the TLP (ref) information disclosure policy.

5 Traceability (or Logging) [TR]

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 at least the following events: connect, authenticate, authorise (including identity changes) and disconnect.

Each Claims Processor must have the following:

- [TR1] Mechanisms deployed to provide the traceability of the service usage, by the production, retention, and protection of appropriate logging data, to identify the source of all actions as defined above
- [TR2] A specification of the logging data retention period, consistent with local, national and international regulations and policies (for users to which this applies?). Do we want to define the times?) or turn on tracing when requested? To be revisited.
- [TR3] The capability to identify and contact subjects, e.g. authenticated users

6 Participant Responsibilities [PR]

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

- Individual users
- Collections of users
- Resource Providers and Service Operators

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

6.1 Individual Users

Each DITI must have:

- [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 for non-compliance.
  - *Need some examples*
- [PRU2] A process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.
- [PRU3] Mechanisms deployed to communicate to their users any additional restrictions or requirements on acceptable use that arise out of new collaborative partnerships

6.2 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 that 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 DITIs.

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

Each DITI 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 user lifecycle management by the body granting access to services. At a minimum these must address the accuracy of user contact information both for initial collection and periodic renewal

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[2] 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

6.3 Resource Providers and Service Operators

The DITI must have policies and procedures in place to ensure that Service Operators understand and agree to abide by expected security standards as defined by the DITI, including:

- [PRR1] Vulnerability patching
- [PRR2] Incident reporting
- [PRR3] Physical and network security
- [PRR4] Confidentiality, integrity, and availability of services
- [PRR5] Retention and protection of appropriate logs

7 Legal Issues and Management procedures [LI]

DITIs, Resource Providers, Service Operators 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

[2] Examples include but are not limited to: Registration or renewal in a membership system, dynamic authorisation such as acquisition of VOMS attributes, authentication to a Science Gateway or portal, job submission or file transfer initiated by the Collection on behalf of an individual user

- [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

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

DITIs, Resource Providers, Service Operators 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

9 Copyright Notice