

SEE Identity Federation Training

Best Current Practice :
Entity Categories

Content

- **Definition** of Entity Category (EC)
- **Why** have Entity Categories been introduced
- Entity Category R&S - **Research and Scholarship**
- Entity Category GEANT **CoCo v1 and v2**
- Entity Category **Hide from Discovery**
- **How** are Entity Categories implemented in practice
- **SIRTFI** : a framework to handle security
 - SIRTFI for Identity Providers (IdPs)
 - SIRTFI for Service Providers (SPs)
- References

What Entity Categories are

Entity Categories are a way to group entities together according to their membership in categories defined primarily to ensure

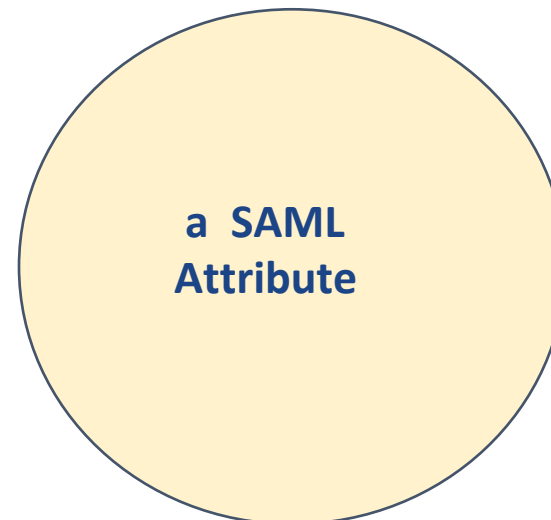
- **inter-operation** with other entities
- compliance to specific policy/security standards.

Entity Categories group federation entities that share common criteria.

The intent is that all entities in a given entity category are obliged to conform to the characteristics set out in the definition of that category.

From a **technical** point of view, ECs are a **SAML attribute** (*entity category attribute*), the values of which represent entity types or categories .

`<saml:Attribute>` is here a a TAG inside the entity Metadata.



What are Entity Categories for

When used with the [SAML V2.0 Metadata Extension for Entity Attributes](#) each such entity category attribute value represents a claim that the entity thus labeled meets the requirements of the indicated category

The entity is therefore asserted to be a member of that category

These category membership claims **MAY be used by a relying party** to

- provision policy for release of attributes from an identity provider
- influence user interface decisions (e.g.: identity provider discovery)

or for **any other purpose**.

In general, the intended uses of any claim of membership in a given category will depend on the details of the category's definition, and will often be included as part of that definition.

Entity Categories: a **Best Practice** for Federations

- The Entity Category best practice is managed by **REFEDS** through an open consultation among all the Federation Operators:
<https://wiki.refeds.org/display/ENT/Entity-Categories+Home>
- The produced simplification consists in a federation **service categorization of homogeneous services**
- Another important goal of Entity Category is that the **attribute release policy will not be configured for each SP but only once-for the whole category**
- Each category will contain a set of homogeneous entities (in our case a set of SPs) that meet the requirements of the category itself - SPs become members of that category
- IdPs can configure a rule for the category that will remains unchanged (scalable) even if further SPs become member of that category in the future.

How to introduce Entity Categories in practice

A federation agrees with its members to:

1. **Introduce** one or more Entity Category for its federated IdP and SP
2. **Define a set of criteria** to belong to the category
3. **Establish procedures**, both for SPs and IdPs, to be a member
4. **Membership** to a category is reported **in the entity metadata**

Entity Categories to ease and support releasing attributes

- SPs must satisfy a set of specific requirements
- Federation Operator verifies that those requirements are compliant and satisfied
- Federation or the Registration Authority accepted the SP in a category



The IdP can trust every SP in that category, and be sure that all the requirements are satisfied and certified by the Registration Authority, or by the Federation

ENTITY CATEGORIES EASE THE RELEASE OF ATTRIBUTES FROM IDPs to SPs

Entity Category attribute

To obtain the entity category attribute a SP **MUST** satisfy the requirements for the category and needs to **ASK** for the certification to the Registrar

To certify that a SP is member of a category the Registrar (after any necessary control) **adds a fragment to the SP entity metadata like this:**

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">  
    <saml:AttributeValue>  
      http://refeds.org/category/research-and-scholarship  
    </saml:AttributeValue>  
    <saml:AttributeValue>  
      http://www.geant.net/uri/dataprotection-code-of-conduct/v1  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```


The Entity Category support attribute

It is fundamental for SPs to know which IdPs support the category, in order to **enable interoperation**

IdPs are asked to claim explicitly that they are supporting the category, by inserting a proper tag in their entity metadata:

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category-support"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">  
    <saml:AttributeValue>  
      http://refeds.org/category/research-and-scholarship  
    </saml:AttributeValue>  
    <saml:AttributeValue>  
      http://www.geant.net/uri/dataprotection-code-of-conduct/v1  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

Why have Entity Categories been introduced ?

One of the main reasons to introduce ECs has been to **ease the process of attribute release by Identity Providers to Service Providers**:

- **Tagging an IdP** as being part of a given Entity Category which specifies policies by means the IdP is managed (ensuring appropriate level of security, allowing LoA to be associated to released IDentifiers)
- **Tagging a Service Provider** as being part of a given Entity Category to reassure IdPs about the usage that the SP will make of the provided IDs and associated attributes
 - According to a given generally accepted policy on Privacy and Confidentiality of data
 - According to specific, well identified, agreed data processing purposes, implying expressed user consent and information

Research and Scholarship

The **Research and Scholarship Entity Category** has been introduced to characterize the corresponding member entities as **entity primarily devoted to the Research and Academic world**. It is applicable to :

- Service Providers - **Directly**
- Identity Providers - As an **expression of Support** to the Entity Category itself

Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part.

For more information please see [REFEDS Entity Category Research and Scholarship](https://refeds.org/category/research-and-scholarship)

<https://refeds.org/category/research-and-scholarship>

Research and Scholarship EC

- The **REFEDS Research and Scholarship Entity Category** (R&S) has been designed as a **simple** and **scalable** way for Identity Providers to release minimal amounts of required personal data to Service Providers serving the Research and Scholarship Community.

Research and Scholarship Entity Category **formal definition**

Candidates for the Research and Scholarship (R&S) Category are Service Providers that are **operated for the purpose of supporting research and scholarship interaction, collaboration or management**, at least in part.

Example Service Providers may include *(but are not limited to)* collaborative tools and services that require some personal information about users to work effectively:

- wikis / blogs / project and grant management tools

This Entity Category **should not be used for access to licensed content such as e-journals.**

Identity Providers may indicate support for **Service Providers in this category** to facilitate discovery and improve the user experience at Service Providers.

How to assert R&S EC

- According to R&S specs the registrar **MUST** perform at least the following check:
- *The service enhances the research and scholarship activities of some subset of the user community.*
- So **SPs should not self-assert this**. Federation operators must make a judgement call on whether the SP is in the category
- **Self-assertion is the typical approach** used for IdPs

Research and Scholarship in practice:

(1 / 2)

R&S is used in the eduGAIN interfederation to make services available to users of the higher education institution around the world

The R&S makes it possible to **automatically release mostly harmless attributes to Service Providers within the higher educational sector**

The expected IdP behaviour is to release the Service Provider required subset of the R&S Category Attributes:

- **ePTID**
- **ePPN**
- **email**
- **displayName**
- **surname**
- **given name**
- **ePSA (scoped affiliation)**

- The requested subset of attributes for a specific service is defined in metadata
- There is furthermore an **Identity Provider entity support category** that should be registered for all IdP supporting the R&S Category that **can be used for filter purpose in a discovery service**
- [The Service Provider requests attributes needed by the service/s through the metadata <RequestedAttribute> tag]



THE IDP DISCOVERY PROCESS CAN LEVERAGE ENTITY CATEGORIES

Research and Scholarship: Requirements for **Service Providers**

- The service enhances the research and scholarship activities of some subset of the user community.
- Service metadata has been submitted to the registrar for publication.
- The service meets the following technical requirements:
 - The Service Provider is a production SAML deployment that supports SAML V2.0 HTTP-POST binding
 - The Service Provider claims to refresh federation metadata at least daily.
 - The Service Provider provides an mdui:DisplayName and mdui:InformationURL in metadata
- The service enhances the research and scholarship activities of some subset of the user community
- The Service Provider provides one or more technical contacts in metadata

Research and Scholarship attribute

An SP part of R&S category has to

- Claim that **it will not use attributes for purpose that fall outside of the service definition**
- Request a minimal subset of R&S attributes that represent only those attributes that the SP requires to operate its service - **R&S relies on the legitimate interest approach**

Metadata example for an R&S SP

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
    <saml:AttributeValue>  
      http://refeds.org/category/research-and-scholarship  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

WATCH OUT:

Strictly-speaking, you must not have white spaces around the URI for the attribute value, even though it makes it clearer in the display.

Research & Scholarship (V1.3) IdP support attribute

An IdP that support R&S entity category **MUST** release the following attributes to the SPs in this category

- **eduPersonPrincipalName (if not reassigned)**
- **eduPersonTargetedID + eduPersonPrincipalName (if reassigned)**
- **displayName OR (givenName + sn)**
- **mail**

Populate the user directory with the attributes to release

An IdP that support R&S entity category is **STRONGLY ENCOURAGED** to release:

- **eduPersonScopedAffiliation**

<https://refeds.org/category/research-and-scholarship>

Research & Scholarship IdP metadata

After the IdP configured its attribute-filter file for R&S it has to explicitly claim its support to the category, by **inserting this fragment in its metadata:**

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category-support"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
    <saml:AttributeValue>  
      http://refeds.org/category/research-and-scholarship  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

Automatic Attribute Release based on EC for Shibboleth Research & Scholarship IdP filter

Example of attribute-filter.xml file for an IdP supporting R&S

```
<AttributeFilterPolicy id="releaseDynamicSubsetRandSAttributeBundle">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <AttributeRule attributeID="eduPersonPrincipalName"> </AttributeRule>
  <AttributeRule attributeID="email"> </AttributeRule>
  [...]
</AttributeFilterPolicy>
```

Examples:

<http://www.garr.it/idem-conf/attribute-filter-v3-rs.xml>

<https://wiki.refeds.org/display/ENT/Research+and+Scholarship+IdP+Config>

GÉANT Data Protection Code of Conduct Entity Category

GÉANT Data Protection Code of Conduct (DP_CoCo)

- Created to meet the requirements of the EU Data Protection Directive in federated identity management
- Fundamental agreement on how user data will be managed and processed in order to respect user privacy
- Home Organisations are more keen to release attributes to Service Providers who comply with Data protection Code of Conduct

Context and goals of DP CoCo

The **Data protection Code of Conduct** describes an approach to meet the requirements of the **EU Data Protection Directive** in federated identity management

The **Data protection Code of Conduct** defines behavioral rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organizations.

It is expected that **Home Organizations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct.**

What is DP CoCo for ?

GEANT Code of Conduct contributes to

- permitted use
- data minimisation
- transparency
- further release to a 3rd party/country
- data retention
- security practices and incidents

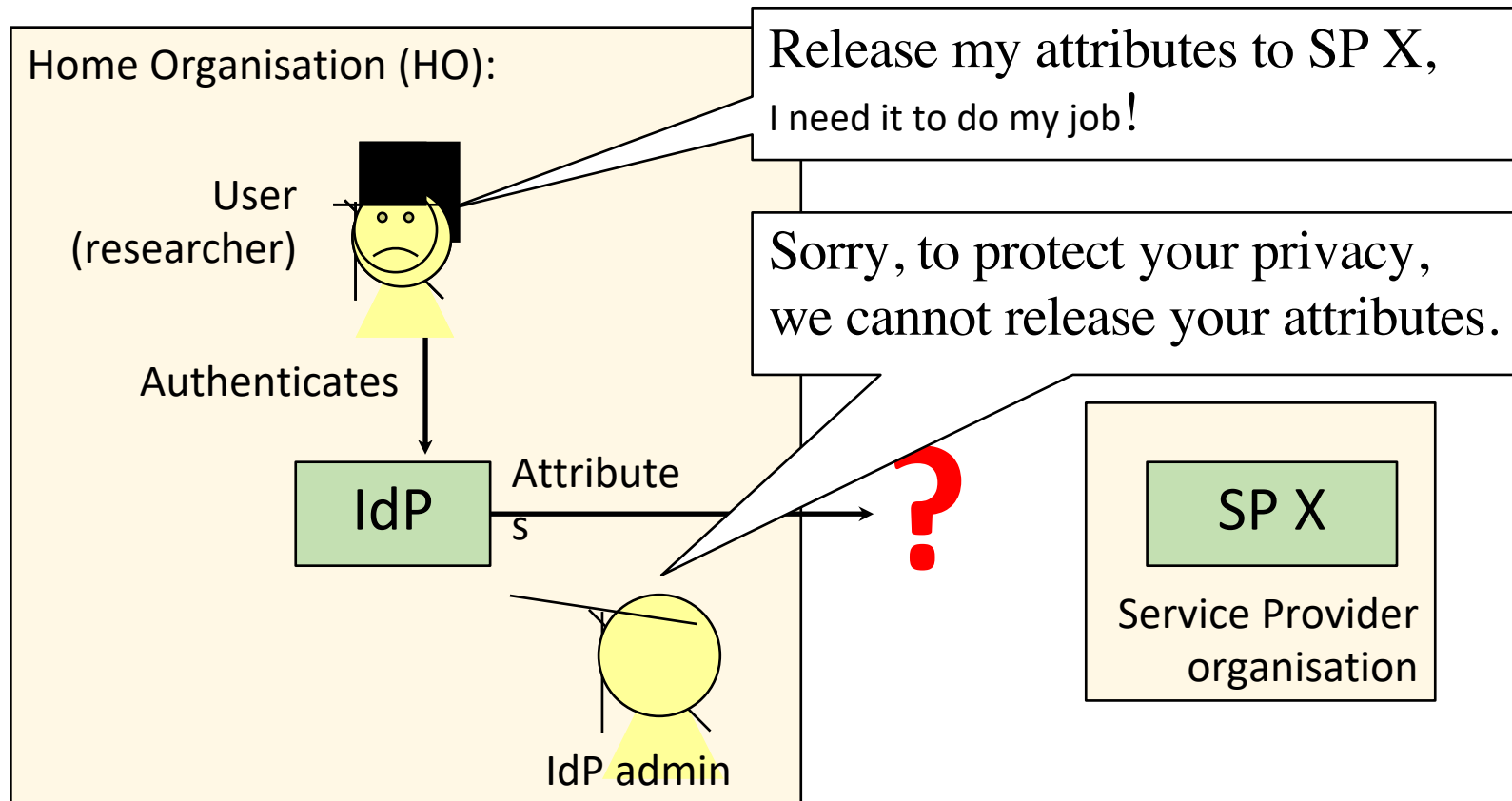
of the attributes the **Home Organization** has released to a **Service Provider**

DP_CoCo attribute - **Service Providers**

To be member of **DP_CoCo** entity category a SP (Service Provider) has to:

- Be located in EU/EEA and obey to EU laws
 - It is not allowed to send the user data to third parties
 - It must ask only for the minimal set of required attributes
- Ask its necessary attributes in its RequestedAttribute statement as «isRequired="true"»
- **Inform the user about the processing his personal data in a Privacy Policy page** linked to its primary service page

The attribute release challenge: Why a DP Code of Conduct is needed



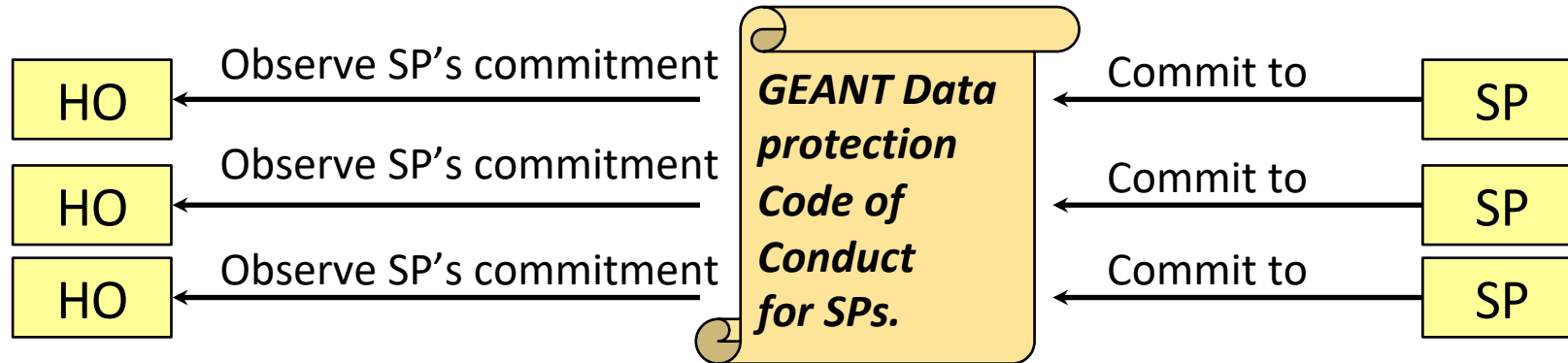
Observations:

- username and password not exposed to SP
- only necessary attributes exposed to SP
- HO knows its users and delivers them credentials

Typical user attributes:

- name
- e-mail address
- unique user identifier
- role and affiliation
(“student@universityx.org”)
- dedicated permissions to use the service

GEANT Code of Conduct



- Service Providers (SP) commits to the CoCo
- Identity federations (and eduGAIN) relays SPs' commitment to Home Organizations (HO)
- HO decides if it feels confident to release attributes to the SP

GEANT CoCo version 1.0

- published 2013
- 199 SPs committed to it
- 360 HOs recognise it

GEANT CoCo version 2.0

- work started 2016
- stabile draft
- proceeding to submit to Dutch DPA

DP_CoCo IdP support attribute

To support DP_CoCo entity category an IdP has to:

- Release **only the requested attributes with the «isRequired="true"»** value
- If the SP requires a particular value for multivalue attribute the IdP has to release **only that value**
- Inform the user about the treatment for every single attribute in its **PrivacyStatementURL**
- To support **DP_CoCo EntityCategory**, the IdP has to **explicitly claim it** in its **metadata** by adding:

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category-support"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
    <saml:AttributeValue>  
      http://www.geant.net/uri/dataprotection-code-of-conduct/v1  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

Automatic Attribute Release based on EC for Shibboleth DP_CoCo IdP – **attribute-filter.xml**

```
<AttributeFilterPolicy id="releaseToCoCo">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1"/>

    <AttributeRule attributeID="sn">
      <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
    </AttributeRule>

    <AttributeRule attributeID="givenName">
      <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
    </AttributeRule>

  [...]
</AttributeFilterPolicy>
```

Examples:

<http://www.garr.it/idem-conf/attribute-filter-v3-coco.xml>

<https://portal.nordu.net/display/SWAMID/Example+of+a+standard+attribute+filter+for+Shibboleth+IdP>

DP_CoCo: Notes for IdP Managers

- **Release only Attributes** that are **adequate, relevant and not excessive** for the Service Provider flagged as mandatory in SAML metadata (see SAML 2 Profile for the Code of Conduct for details on how this is done)
- If the Service Provider requests only a **particular Attribute value**, release only that value and no other values for instance, if the Service Provider requests only `eduPersonAffiliation="member"`, do not release `eduPersonAffiliation="faculty"`
- **Inform the end user** on the Attribute
 - for each Attribute, the Attribute name, description and value an easily understood label can be displayed instead of displaying several closely related Attributes (eg the various name Attributes)
- If use the **data controller's legitimate interests** as the legal grounds for attribute release, release only attributes that are flagged as **NECESSARY**

How will I know **how the SP manages my attributes?**

- The SP provides the End User a **privacy notice**
- **Concise, transparent, intelligible** and provided in an **easily accessible form**
- It is further suggested that the **HO presents a link to the privacy notice** to the user before the attributes are released

PRIVACY NOTICE TEMPLATE	
Name of the Service	SHOULD be the same as <u>mdui:DisplayName</u> <i><u>WebLicht</u></i>
Description of the Service	SHOULD be the same as <u>mdui:Description</u> <i><u>WebLicht</u> is a service for language research. It provides an environment for automatic annotation of text corpora.</i>
Data controller and a contact person	<i><u>Tübingen</u> university, Institute for language research Laboratory manager Bob Smith, bob.smith@example.org</i>
Data controller's data protection officer, if applicable	If the controller has a data protection officer (GDPR Section 25) <i>Chief Security Officer bill.smith@example.org</i>

In which countries SPs can commit to the CoCo

- **SPs in EU and EEA**
(EU28 + Norway, Iceland, Liechtenstein)
- **SPs in EC whitelist countries** and international organisations
("providing adequate protection")
- SPs in other countries and international organisations
(Art. 46.2(e): "together with binding and enforceable commitments")

Service Provider	In EU/EEA or EC whitelist	Outside EU/EEA or EC whitelist
Home Organisation		
In EU/EEA or EC whitelist	Yes	Yes (with binding and enforceable commitments)
Outside EU/EEA or EC whitelist	Yes	(Yes)

For what purpose **my attributes can be used?**

Which of my attributes an SP can request?

- The Service Provider must use the attributes only for **enabling the end user access to the Service.**
- for other purpose only on user's prior consent
- The Service Provider must request only Attributes that are **adequate, relevant and not excessive** for enabling the end user access the service

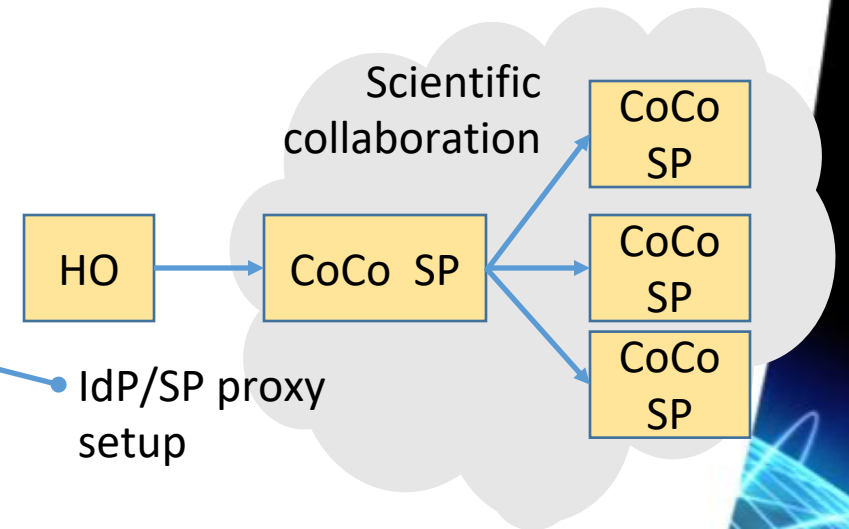
Examples of enabling access

Authorisation	User's role and affiliation used for deciding if they can access
Identification	Service needs personal identifier to separate users' files, datasets, pages, postings, ...
Transferring real-world trust online	User's name can be released if the user community knows each other by name in real world
Researcher unambiguity	Associating scientific contribution to proper person
Accounting and billing	Monitoring consumption of resources e.g. compute capacity
Information security	Ensuring service integrity, confidentiality and availability (e.g. incident response)

Can the SP relay my attributes to a **third party**?

SP can transfer attributes to **3rd parties** if

- 3rd party is a **data processor for the SP**, or
- 3rd party is **committed to the CoCo**, or
- **User consents to the transfer**



SP can transfer attributes to **3rd countries** if

- The receiver is **committed to an approved CoCo**, or
- other **appropriate measures** (e.g. **EC model contracts, consent**)

How long can the SP keep my attributes?

- The SP shall delete or anonymise attributes **when no longer needed** for enabling access to the service
 - if the user no more wishes to use the service
 - if the user does not show up for **18 months**
- there may be reasons to extend the 18 month rule of thumb
 - attributing researchers for their scientific contribution
 - assessing the provenance of a contribution
 - maintaining source code in a git...

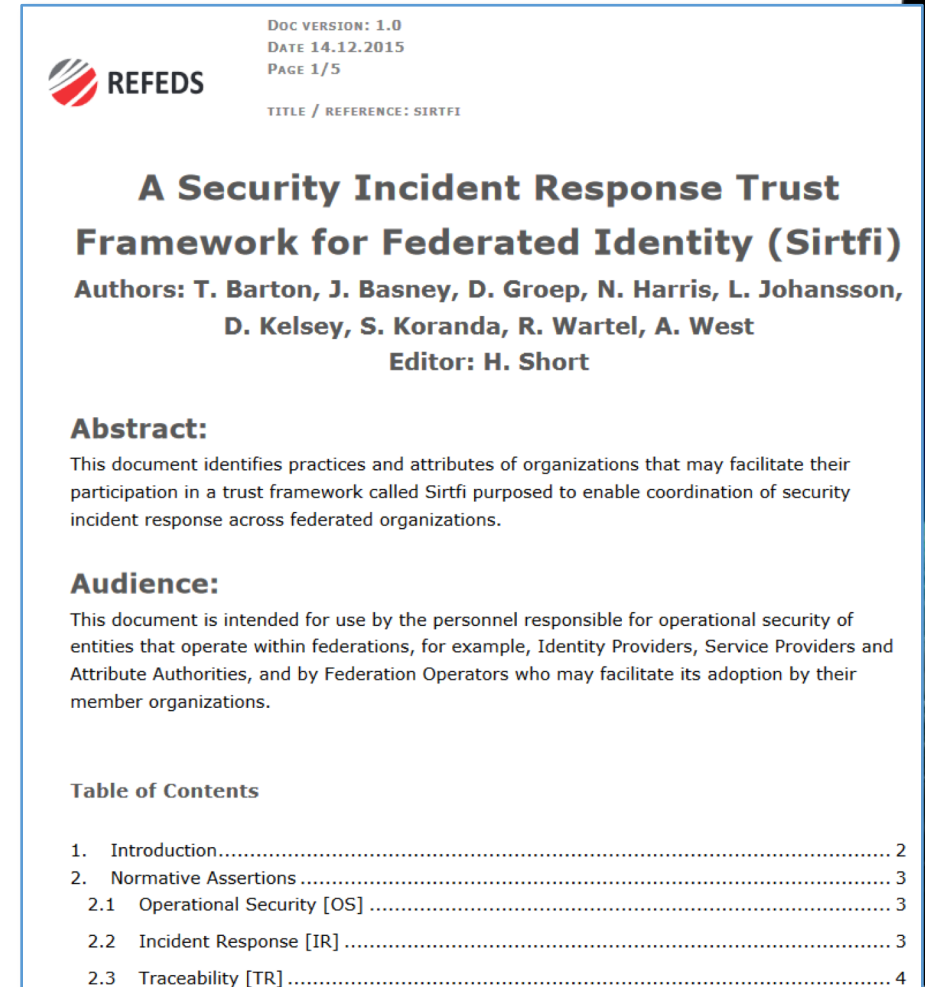
How will the SP protect my attributes?

Security measures


- SP takes proper care of information security
- **SIRTFI as a well-established community practice**

Security breaches

- normal GDPR obligations apply
- The SP report suspected privacy or security breaches also to **Home Organisation**



DOC VERSION: 1.0
DATE 14.12.2015
PAGE 1/5

 REFEDS

TITLE / REFERENCE: SIRTFI

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)
Authors: T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West
Editor: H. Short

Abstract:
This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations.

Audience:
This document is intended for use by the personnel responsible for operational security of entities that operate within federations, for example, Identity Providers, Service Providers and Attribute Authorities, and by Federation Operators who may facilitate its adoption by their member organizations.

Table of Contents

1. Introduction.....	2
2. Normative Assertions	3
2.1 Operational Security [OS]	3
2.2 Incident Response [IR]	3
2.3 Traceability [TR]	4

What if I think an **SP** is *misbehaving*?

If an End User suspects an SP non-compliance:

1. Contact **the SP** and them to check and correct
2. Contact **the SP's Home identity federation** and ask them to contact the SP
3. Contact **the CoCo monitoring body**
4. Lodge a complaint with the **competent supervisory authority**

Data subject rights

- Obtain transparent information on data processing
 - **SP's privacy notice on-line**
 - HO is encouraged to **present SP's privacy notice link to user at login**
 - (HO's privacy notice)

The Privacy Notice describes data subject rights:

- e.g. access their personal data

PRIVACY NOTICE TEMPLATE

Name of the Service	SHOULD be the same as <u>mdui:DisplayName</u> <i><u>WebLicht</u></i>
Description of the Service	SHOULD be the same as <u>mdui:Description</u> <i><u>WebLicht</u> is a service for language research. It provides an environment for automatic annotation of text corpora.</i>
Data controller and a contact person	<i><u>Tübingen</u> university, Institute for language research Laboratory manager Bob Smith, bob.smith@example.org</i>
Data controller's data protection officer, if applicable	If the controller has a data protection officer (GDPR Section 25) <i>Chief Security Officer bill.smith@example.org</i>

DP_CoCo SP metadata

The SP is member of DP_CoCo category if the Registrar certifies it (after any necessary control) by adding this fragment to the SP entity metadata

```
<mdattr:EntityAttributes>  
  <saml:Attribute Name="http://macedir.org/entity-category"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
    <saml:AttributeValue>  
      http://www.geant.net/uri/dataprotection-code-of-conduct/v1  
    </saml:AttributeValue>  
  </saml:Attribute>  
</mdattr:EntityAttributes>
```

CoCo version 2

Commonalities of CoCo 1.0 and 2.0

- Both are binding agreements for the Service Provider who has committed to it.
- They both consist of 17-18 clauses which express what the service provider is committing to. The reader can observe many similarities in the clauses.
- They both use similar SAML metadata constructs

(Entity category, RequestedAttributes, mdui:PrivacyStatementURL, mdui:DisplayName, mdui:Description)

(See <https://wiki.refeds.org/display/CODE/CoCo+v1+vs+v2>)

CoCo version 2

Differences between CoCo 1.0 and 2.0 (1 / 2)

- CoCo 1.0 is based on the Data protection directive and CoCo 2.0 on the **GDPR** which replaced the directive in 25 May 2018.
- **CoCo 2.0 is more descriptive**, it explains how the law should be interpreted in the context of attribute release in an R&E identity federation (e.g. what the attributes can be used for, how long they can be stored, etc)
- CoCo 2.0, after approved by the data protection authorities, **justifies attribute release out of EU, if the SP has committed to do it properly. This means also non-EU/EEA SPs can commit to it.**

CoCo version 2

Differences between CoCo 1.0 and 2.0 (2 / 2)

- CoCo 2.0 covers better the needs of **international organisations** (such as CERN and EMBL)
- CoCo 2.0 introduces a **CoCo monitoring body**, as required by GDPR
- **CoCo 2.0 requires the SP to commit to SIRTFI**, too
- Some of the material that is non-normative in CoCo 1.0 is made normative in CoCo 2.0, as suggested by the authorities (e.g. Privacy Policy template, handling non-compliance)
- **SPs can make use of the CoCo also for receiving attributes from Attribute Providers**

Entity Category **Hide From Discovery**

- The **HfD** EC has been introduced to mark in an unambiguous way those **Identity Providers which need for specific reasons to be hidden from the Discovery process**
 - e.g. Test IdPs, Internal ones, which are not meant for the general Fed or eduGAIN user
- It applies to **Identity Providers**
- More information on <https://refeds.org/category/hidden-from-discovery>

Example code to assert **Hide From Discovery** in an IdP

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://institution.example.com/idp">
<Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Attribute
Name="http://macedir.org/entity-category"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue>http://refeds.org/category/hide-from-discovery</saml:AttributeValue>
</saml:Attribute>
</mdattr:EntityAttributes>
</Extensions>
...
</EntityDescriptor>
```



SIRTFI

The **Security Incident Response Trust Framework for Federated Identity (SIRTFI)** aims to enable **the coordination of incident response** across federated organisations

The SIRTFI assurance framework comprises a **list of assertions** which an organisation can attest in order to be declared SIRTFI compliant

SIRTFI specifies a set of compliance rules for entities to be able to assert it



A Security Incident Response Trust Framework

Security
Incident
Response
Trust Framework for
Federated
Intity

This framework has been approved by the REFEDS Community and registered as an assurance profile by the Internet Assigned Numbers Authority (IANA)

<https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml>

What is SIRTFI about ?

Operational Security

- Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

Traceability

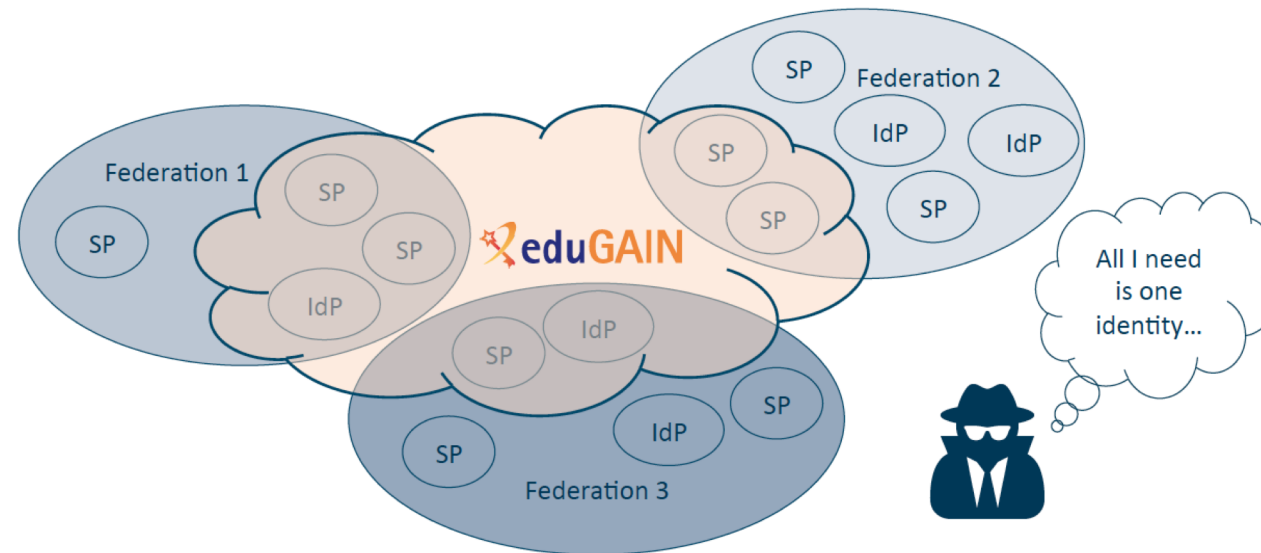
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

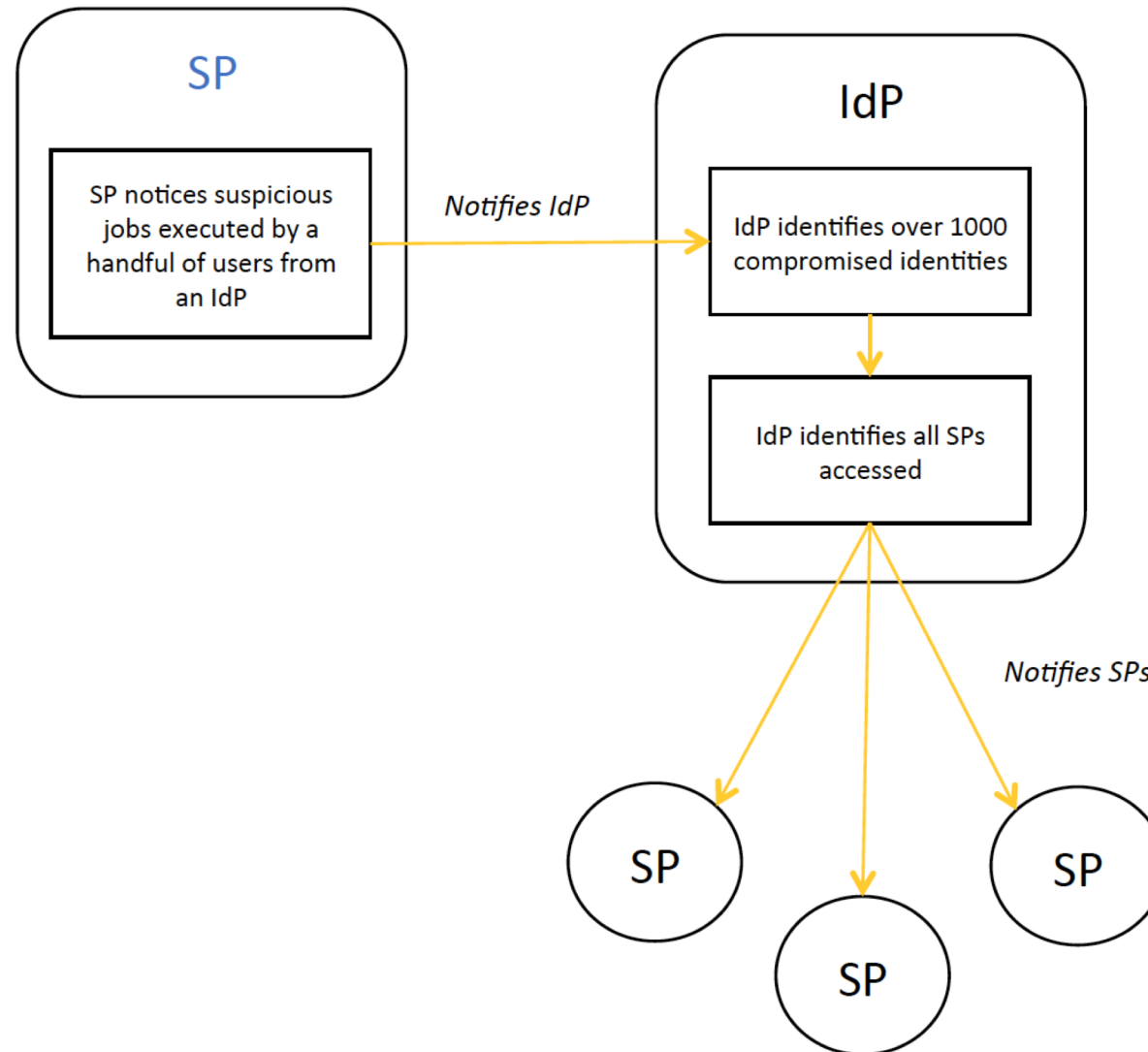
- Confirm that end users are aware of an appropriate AUP

Why do we need **Federated Security Incident Response** ?

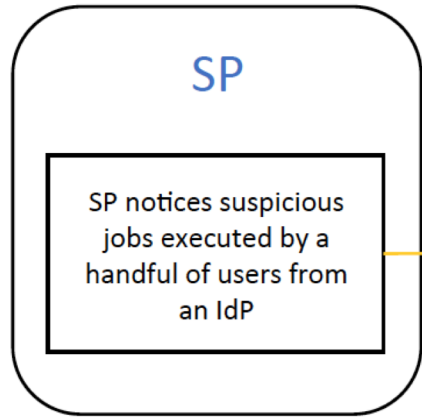
- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need participants to collaborate during incident response – this may be outside their remit



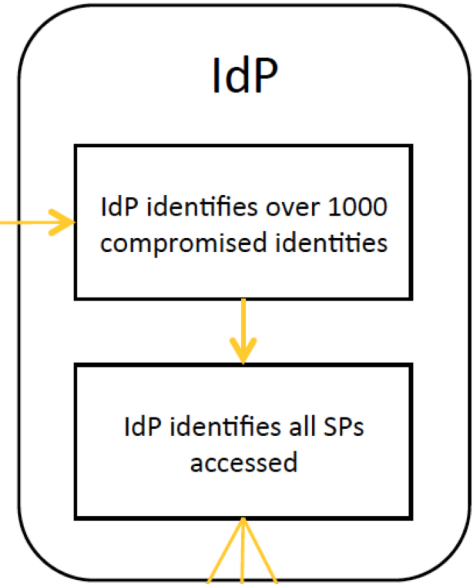
Common sense would imply....



But in practice....



Notifies IdP



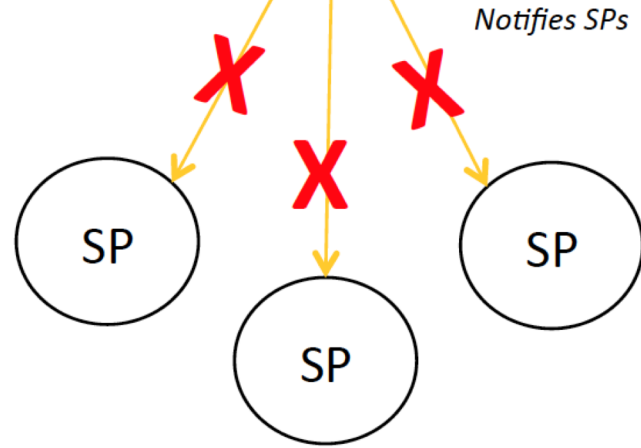
Small IdP may not have capability to block users, or trace their usage



Large SP does not share details of compromise, for fear of damage to reputation



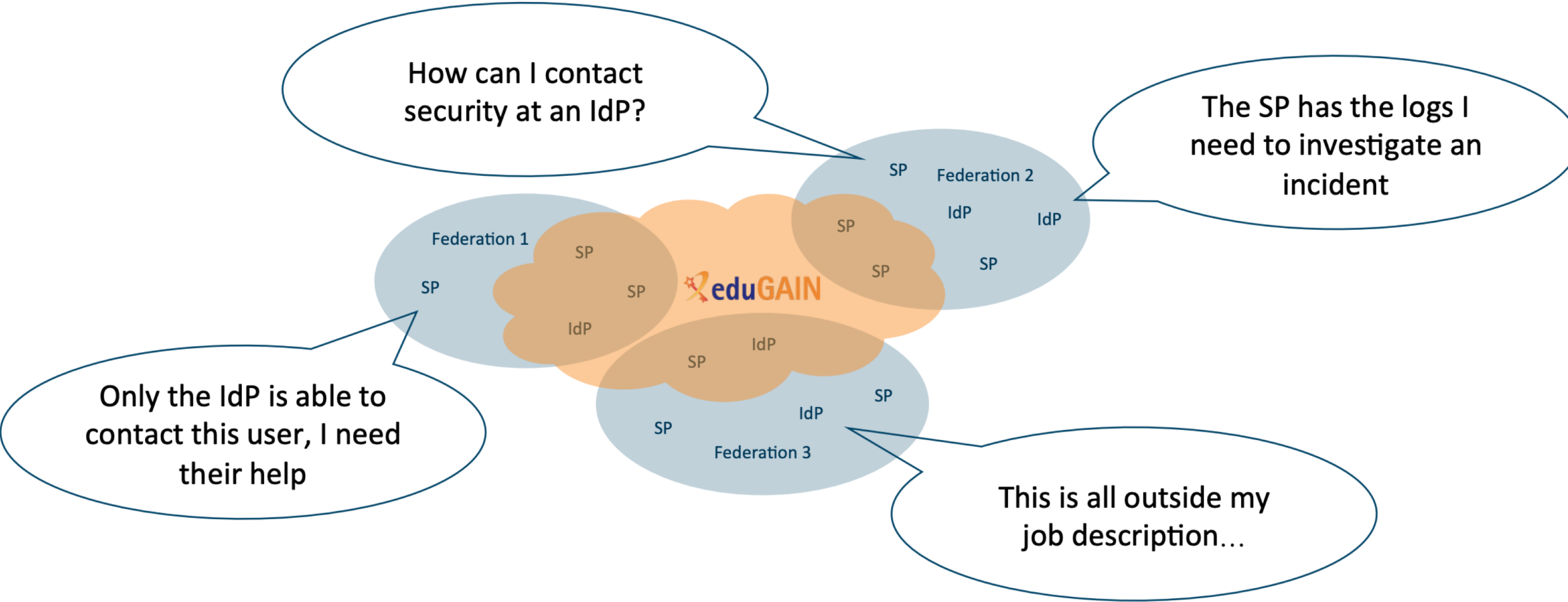
SPs are not bound to abide by confidentiality protocol and disclose sensitive information



No security contact details!



Why is security incident response difficult in identity federations ?



SIRTFI self assessment based assertions for Organizations

SIRTFI consists in practice of a **set of assertions that each organisation shall self-attest** to so that they may participate in the SIRTFI trust framework.

These are divided into four areas:

- **Operational Security [OS]**
- **Incident Response [IR]**
- **Traceability [TR]**
- **Participant Responsibilities [PR]**



SIRTFI Operational Security [OS] Self-Assertions

- **[OS1]** Security patches in operating system and application software are applied in a timely manner
- **[OS2]** A process is used to **manage vulnerabilities** in software operated by the organisation
- **[OS3]** Mechanisms are deployed to **detect possible intrusions** and protect information systems from significant and immediate threats
- **[OS4]** A user's access rights can be suspended, modified or terminated in a timely manner
- **[OS5]** Users and Service Owners (as defined by ITIL) within the organisation can be contacted
- **[OS6]** A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

SIRTFI Incident Response [IR] Self-Assertions

- **[IR1]** Provide **security incident response contact information** as may be requested by an R&E federation to which your organization belongs
- **[IR2]** **Respond** to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework **in a timely manner**
- **[IR3]** Be able and willing to **collaborate in the management of a security incident** with affected organisations that participate in the SIRTFI framework
- **[IR4]** **Follow security incident response procedures** established for the organisation
- **[IR5]** **Respect user privacy** as determined by the organisations policies or legal counsel
- **[IR6]** **Respect and use the Traffic Light Protocol [TLP]** information disclosure policy

The Benefits of SIRTFI

IdPs

Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs

SPs

Gain **users** whose home organisations only allow authentication at Sirtfi compliant SPs

Guarantee an efficient and effective **response** from partner organisations during incident response

Raise the bar in operational **security** across eduGAIN

Why should SPs and IdP adopt SIRTFI ?

As a Service Provider:

I should adopt Sirtfi to advertise that I am a secure service (to encourage IdPs to trust me), and to broadcast my security contact information

Why should IdPs adopt Sirtfi?

I would like IdPs to adopt Sirtfi so that I can identify trustworthy sources of identity to grant access to my critical infrastructure, and to provide a contact point for incident handling

SIRTFI in practice: Step 1: Perform Self assessment of IdP

Step 1: Self Assessment

Complete a self assessment of your organisation following the [SIRTFI Framework](https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf)
(<https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf>)

If you are able to agree with each and every statement included in the framework, **your organisation is SIRTFI compliant.**

To assert this compliance, two extensions must be added to your SP/IdP's federation metadata.

Your local federation may manage all metadata extensions centrally.

In this case, ask your federation operator to perform the following steps.

SIRTFI Step 2: **Add Security Contact** to your Metadata

Add relevant security contact details to your entity metadata,

following the established process of your local federation on updating metadata.

Consult the guide on [Choosing a SIRTFI Contact](#) for recommendations on the most appropriate contact point for your entity.

An example of a Contact Person element can be seen below:

REFEDS security contact

Refer to the REFEDS Standards and Specification Wiki for full details: [Security Contact Metadata Extension Schema](#)

SIRTFI Step 2: Add Security Contact to your Metadata

```
<md:ContactPerson xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  contactType="other"
  remd:contactType="http://refeds.org/metadata/contactType/security"
  xmlns:remd="http://refeds.org/metadata">
  <md:GivenName>Security Response Team</md:GivenName>
  <md:EmailAddress>mailto:security@xxxxxxxxxxxxxxxx</md:EmailAddress>
</md:ContactPerson>
```

Step 3: Provide the Assurance-certification Entity Attribute

Sirtfi compliance is expressed with the use of the Entity Attribute “urn:oasis:names:tc:SAML:attribute:assurance-certification”

holding the value <https://refeds.org/sirtfi> in an entity’s metadata :

SIRTFI Entity Attribute in the metadata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...>
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
        <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
</md:EntityDescriptor>
```



Find out more about SIRTIFI

Call us : +31(0)20 5304488

Mail us : contact@refeds.org



[Home](#)

[Blog](#)

[Wiki](#)

[Meetings](#)

[Sponsor](#)

[Federations](#)

[Our Work](#)

[Specifications](#)

[About](#)



SIRTIFI

<https://refeds.org/sirtfi>

[REFEDS > SIRTIFI](#)

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. Visit our [Wiki](#) to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

REFEDS' [Sirtfi Working Group](#) has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the [AARC Project](#).



Benefits

Why should I join? What are the [Benefits?](#)



Sirtfi v 1.0

View the [Sirtfi Framework](#)



FAQs

Need [help?](#)



Implement

[Sirtfi Identity Assurance Certification Description](#)

New Entity categories: Anonymous Authorization

- [Anonymous Authorization](#)
- <https://refeds.org/category/anonymous>
- Candidates for the Anonymous Authorization Entity Category are Service Providers that grant service access based on proof of successful authentication, which make authorization decisions based on affiliation, and which do not require any additional user attributes.
- Example Service Providers may include (but are not limited to) services such as licensed e-resource providers, retailers, vendors, platform providers, services providing access to research data sets, and collaborative tools and services such as wikis, project, and grant management tools that require enough information to make authorization decisions based on affiliation.

New Entity Categories: Pseudoanonymous Authorization

- <https://refeds.org/category/pseudonymous>
- Candidates for the Pseudonymous Authorization Entity Category are Service Providers that grant service access based on proof of successful authentication, and which offer personalization based on a pseudonymous user identifier and which do not require any other user attributes. These service providers do not qualify for the REFEDS Research and Scholarship Entity Category [R&S].
- Example Service Providers may include (but are not limited to) services that support research and scholarship such as licensed e-resource providers, retailers, vendors, platform providers to support access to online content, inter-library loan services, services providing access to research data sets, and collaborative tools and services such as wikis, project, and grant management tools that require some personal information about users to work effectively.

References

- <https://tools.ietf.org/id/draft-young-entity-category-07.html>
- <https://wiki.refeds.org/display/ENT/Entity-Categories+Home>
- Latest CoCo document: <https://tinyurl.com/s8hdg5v>
- <https://refeds.org/sirtfi>
- <https://aarc-project.eu/wp-content/uploads/2016/06/TF-CSIRT-Sirtfi-Introduction-20160513.pdf>

Credits - Some slides have been provided by:

- Mikael Linden CSC
- Hannah Short CERN
- Marco Malavolti GARR
- The AARC project

66



Thank you

Any questions?

www.geant.org

