Introduction to best current practices

Click to edit subtitle

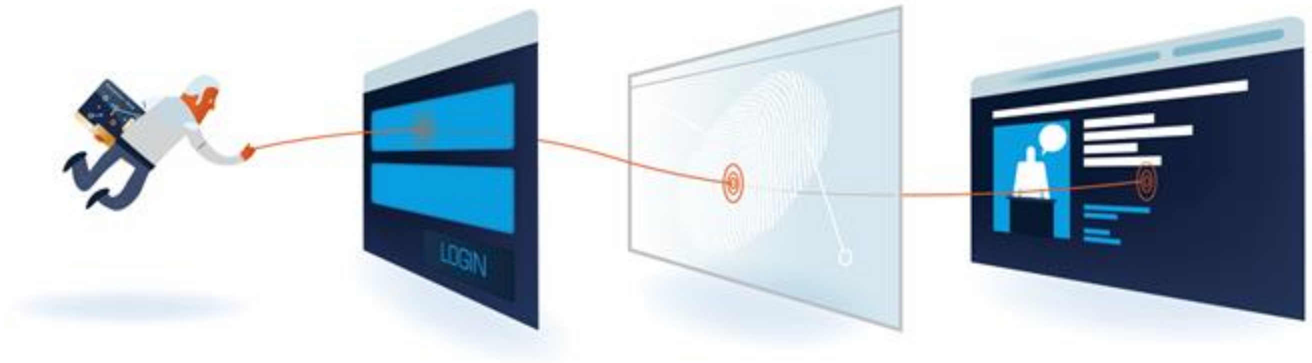
eduGAIN Training Team

GÉANT GN5-2

eduGAIN training for ngREN
April 2025

<Click to edit label> Public (PU) / Project Participants Sensitive (SEN)

Learning Objectives



01 What Entity Categories are

02 How are Entity Categories implemented

03 Examples of the most important 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 (throughout the presentation)
- SIRTFI : a framework to handle security
  - SIRTFI for Identity Providers (IdPs)
  - SIRTFI for Service Providers (SPs)
- SIRTFI v2 – and what has changed
- References

What Entity Categories are

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

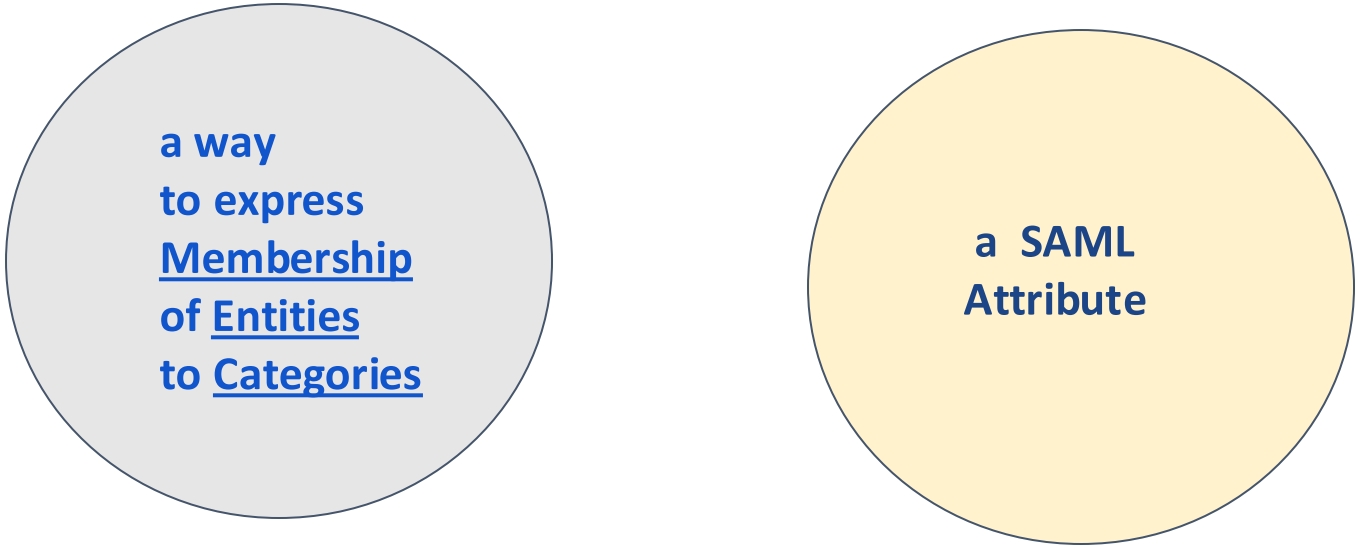
- **inter-operation** with other entities
- compliance to specific policy/security standards.

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 attributes** (*entity category attribute*), the values of which represent entity types or categories .

In what follows: <saml:Attribute> is a TAG inside the entity Metadata.



a way to express Membership of Entities to Categories

a SAML Attribute

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 remain 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 requirement 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/v2
        </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/v2
       </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**:

- **by Tagging an IdP** as being part of a given EC specifying policies by means the IdP is managed (ensuring appropriate level of security, allowing LoA to be associated to released IDentifiers)
  "SP guys, listen I am a good IdP! You can trust my users!"

- **by Tagging a Service Provider** as being part of a given EC 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, implyi expressed user consent and information

  "IdP guys, listen: I am a good SP! You can trust my services!"

The Research and Scholarship (R&S) Entity Category

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

The Research and Scholarship (R&S) EC: in other words:

- 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 behavior is to release the Service Provider a minimal required subset of the R&S Category Attributes:

ePTID	*eduPersonTargetedID*
ePPN	*eduPersonPrincipalName*
email	*email*
displayName	*displayName*
surname	*surname*
givenName	*givenName*
ePSA (scoped affiliation)	*eduPersonScopedAffiliation*

Tip about getting

- Thanks to SWITCH (CH) : L

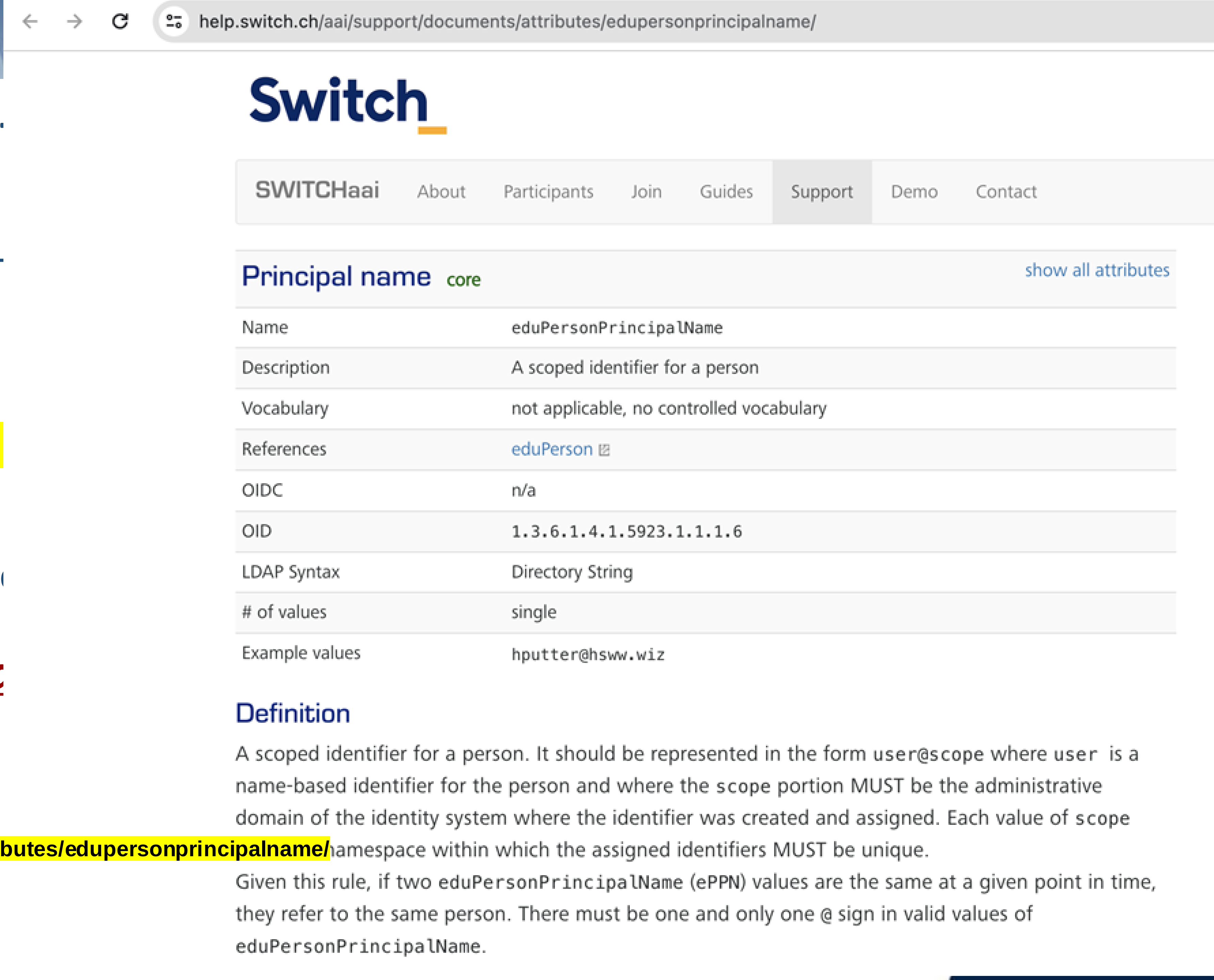
Switch

- https://help.switch.ch/aa

- Example: What is exactly

eduPersonPrincipalNa

https://help.switch.ch/aai/support/documents/attributes/edupersonprincipalname/



Principal name core

Name	`eduPersonPrincipalName`
Description	A scoped identifier for a person
Vocabulary	not applicable, no controlled vocabulary
References	eduPerson
OIDC	n/a
OID	`1.3.6.1.4.1.5923.1.1.1.6`
LDAP Syntax	Directory String
# of values	single
Example values	`hputter@hsww.wiz`

Definition

A scoped identifier for a person. It should be represented in the form `user@scope` where `user` is a name-based identifier for the person and where the `scope` portion MUST be the administrative domain of the identity system where the identifier was created and assigned. Each value of `scope`

amespace within which the assigned identifiers MUST be unique.

Given this rule, if two `eduPersonPrincipalName` (ePPN) values are the same at a given point in time, they refer to the same person. There must be one and only one `@` sign in valid values of `eduPersonPrincipalName`.

Research and Scholarship in practice: (2 / 2)

- 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

See https://refeds.org/category/research-and-scholarship

Research and Scholarship attribute

A Service Provider who is part of the R&S Entity 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 + surname (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

Data Protection Code of Conduct (CoCo) v1 and v2

GÉANT Data Protection Code of Conduct Entity Category

GÉANT Data Protection Code of Conduct (DP_CoCo) (aka: **CoCo version 1**)

- Created to meet the requirements of the EU Data Protection Directive in federated identity management (1995)
- Fundamental agreement on how user data will be managed and processed in order to respect user privacy
- Home Organizations are keener **to release attributes to Service Providers who comply with Data protection Code of Conduct**

Historical developments of the CoCo Entity Category

- Started as DP_CoCo version 1
  - **2013** – based on EU regulation from 1995 **(95/46/EG - Data Protection Directive)**

- Updated to DP_CoCo version 2
  - **2022** – based on EU regulation from 2018 **("GDPR")**

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 minimization
- 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:

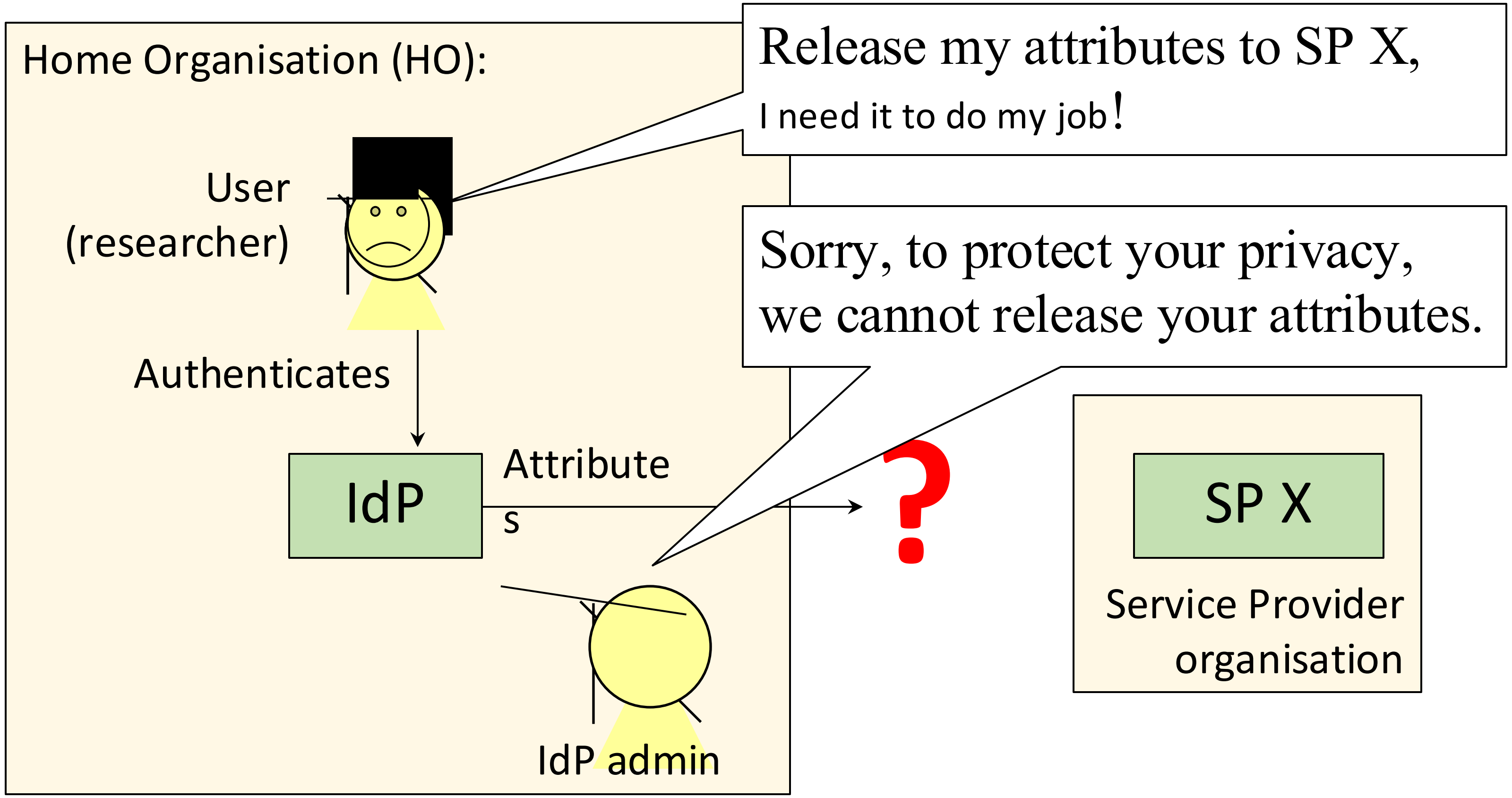
- Be located in EU/EEA and obey to EU laws
  - It is not allowed to send the user data to third parties
  - It must ask only for the minimal set of required attributes

- 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


Home Organisation (HO):
User (researcher)
Release my attributes to SP X, I need it to do my job!
Authenticates
IdP
Attributes
Sorry, to protect your privacy, we cannot release your attributes.
?
IdP admin
SP X
Service Provider organisation

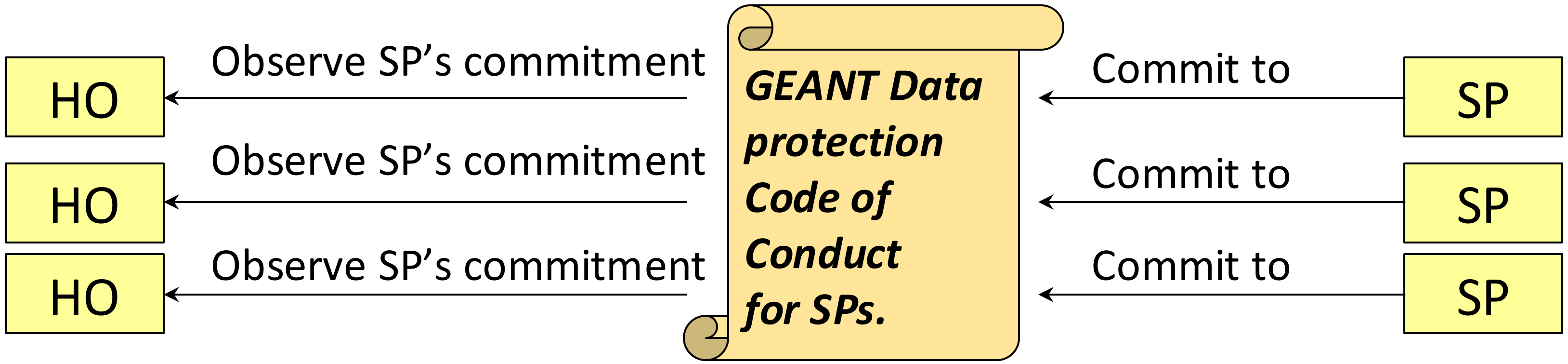
Observations:
- username and password not exposed to SP
- only necessary attributes exposed to SP
- HO knows its users and delivers them credentials

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

el Linden, mikael.lin n@csc.fi

Webinar for end users 17 December 2019
Slides: https://tinyurl.com/rby5rmp

GEANT Code of Conduct



GEANT CoCo version 1.0
- published 2013

GEANT CoCo version 2.0
- work started 2016
- stabile draft 2018
- Adopted: March 2022

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

Webinar for end users 17 December 2019
Slides: https://tinyurl.com/rby5rmp

DP_CoCo v2 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/v2
        </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

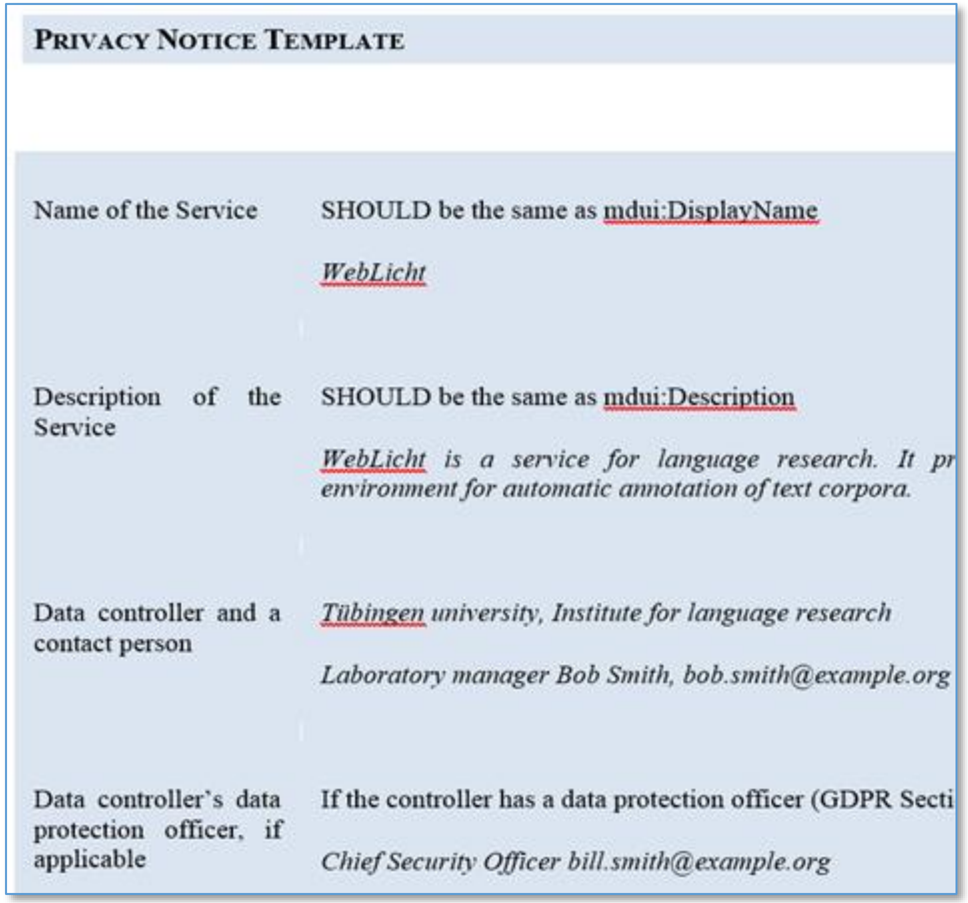
https://portal.nordu.net/display/SWAMID/Example+of+a+standard+attribute+filter+for+Shibboleth+IdP

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

Webinar for end users 17 December 2019
Slides: https://tinyurl.com/rby5rmp

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)

From: Mikael Linden, mikael.linden@csc.fi

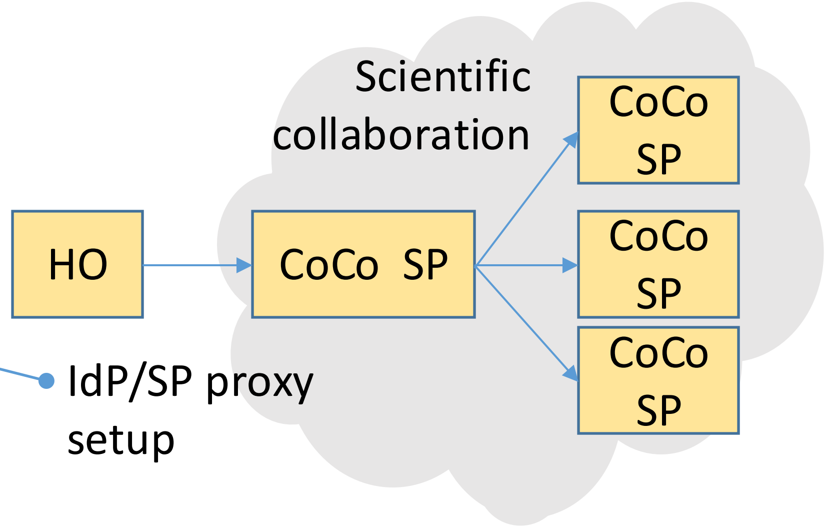
Webinar for end users 17 December 2019

Slides: https://tinyurl.com/rby5rmp

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...

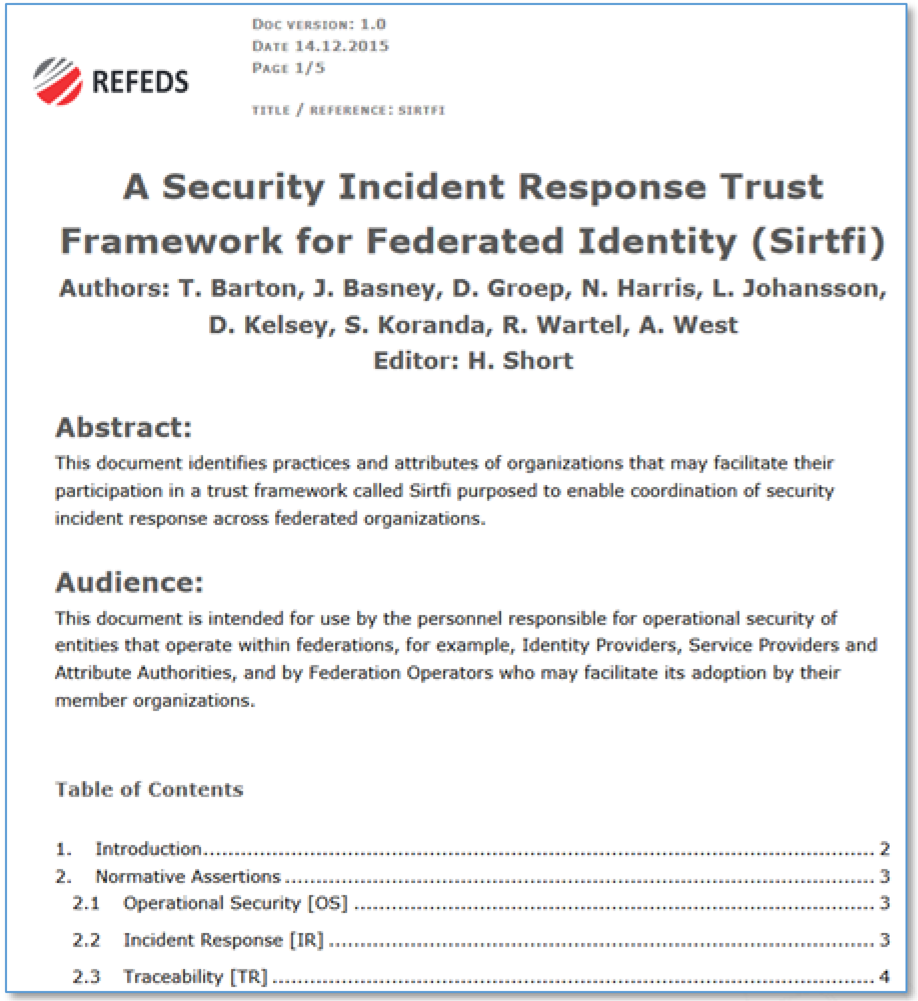
How will the SP protect my attributes?

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**



REFEDS

Doc version: 1.0
Date 14.12.2015
Page 1/5

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

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**

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>
```

```
Version 2
http://www.geant.net/uri/dataprotection-code-of-conduct/v2
```

CoCo v2 : Definition

Candidates for the Code of Conduct Entity Category are Service Provider Organisations that are willing to support and implement **the REFEDS Data Protection Code of Conduct Best Practice guidelines**

https://refeds.org/category/code-of-conduct
https://refeds.org/wp-content/uploads/2022/05/REFEDS-CoCo-Best-Practicev2.pdf

This Code of Conduct is addressed to any Service Provider Organisation established in any of the Member States of the European Union and in any other countries belonging to the European Economic Area (Iceland, Liechtenstein and Norway).

Furthermore, Service Provider Organizations established in any **third country or International organization offering:**

- An **adequate level of data protection** in the terms of Article 45 of the GDPR, **or**
- Appropriate safeguards in the terms of Article 46 of the GDPR can also subscribe to this Code of Conduct.

CoCo v2: meaning

By asserting a Service Provider to be a member of this Entity Category, a Registrar claims that:

- The Service Provider has applied for membership in the Category and complies with this entity category's registration criteria.
- The Service Provider's application for using the Code of Conduct Entity Category has been reviewed against the registration criteria and approved by the Registrar.

In possessing the Entity Category Attribute with the above value, a Service Provider claims that it is bound by:

- The data protection laws in the European Union or European Economic Area,

or can demonstrate:

- an adequate level of data protection in the terms of Article 45 of the GDPR;
- appropriate safeguards in the terms of Article 46 of the GDPR;
- that it has committed to the REFEDS Data Protection Code of Conduct
- that it conforms to the Metadata Requirements for Service Providers - (See section 5 on https://refeds.org/category/code-of-conduct/v2)
- that it informs the Registrar about any material changes that may influence their ability to commit to the REFEDS Data Protection Code of Conduct

- The Service Provider is responsible for the service it offers and its legal compliance with the Code of Conduct. The Service Provider is regarded as authoritative about its Privacy Notice and the attributes the service requests.
- By asserting the Entity Category support attribute, an Identity Provider claims that **it releases the requested attributes to a Code of Conduct committed Service Provider** without administrative involvement.

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 (95/46/EC Oct 1995) 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 introduce to mark in a unambiguous way those **Identity Providers which need for specific reasons to the 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/hide-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

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

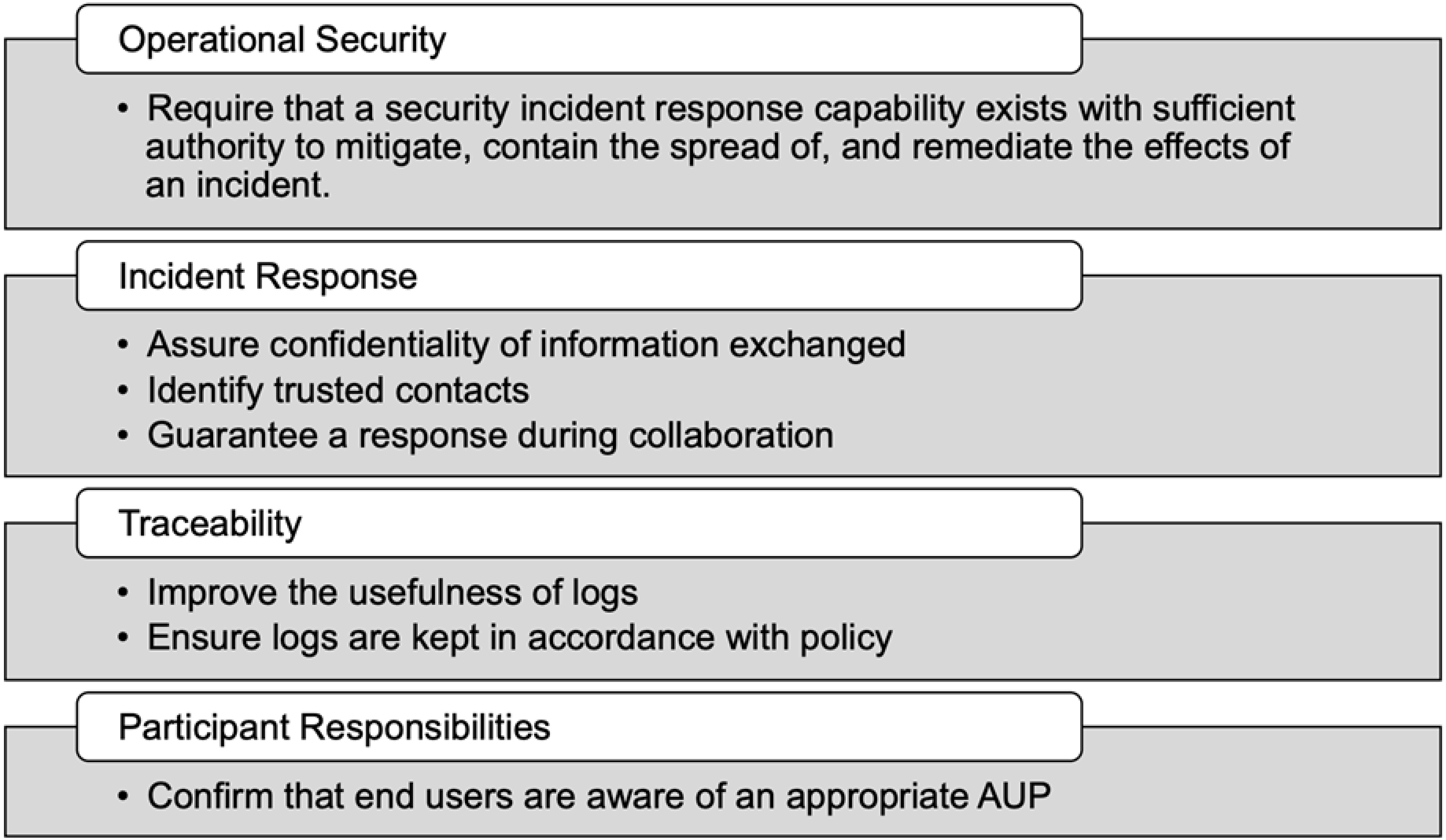
SIRTFI specifies a set of compliance rules for entities to be able to assert it

A Security Incident Response Trust Framework

Security
Incident
Response
Trust Framework for
Federated
Identity

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

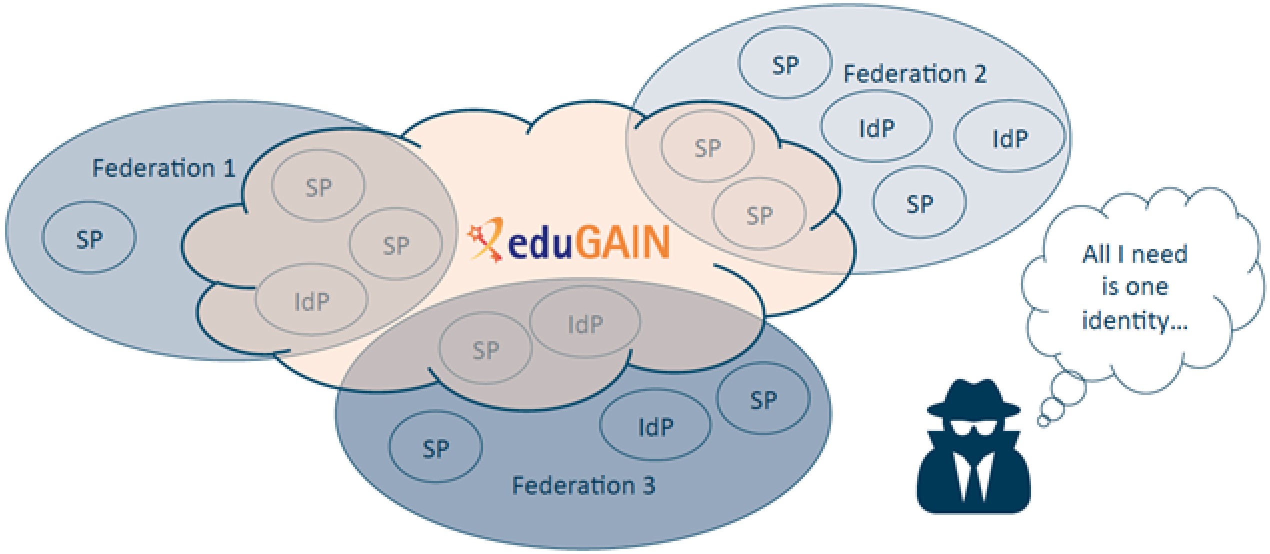
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

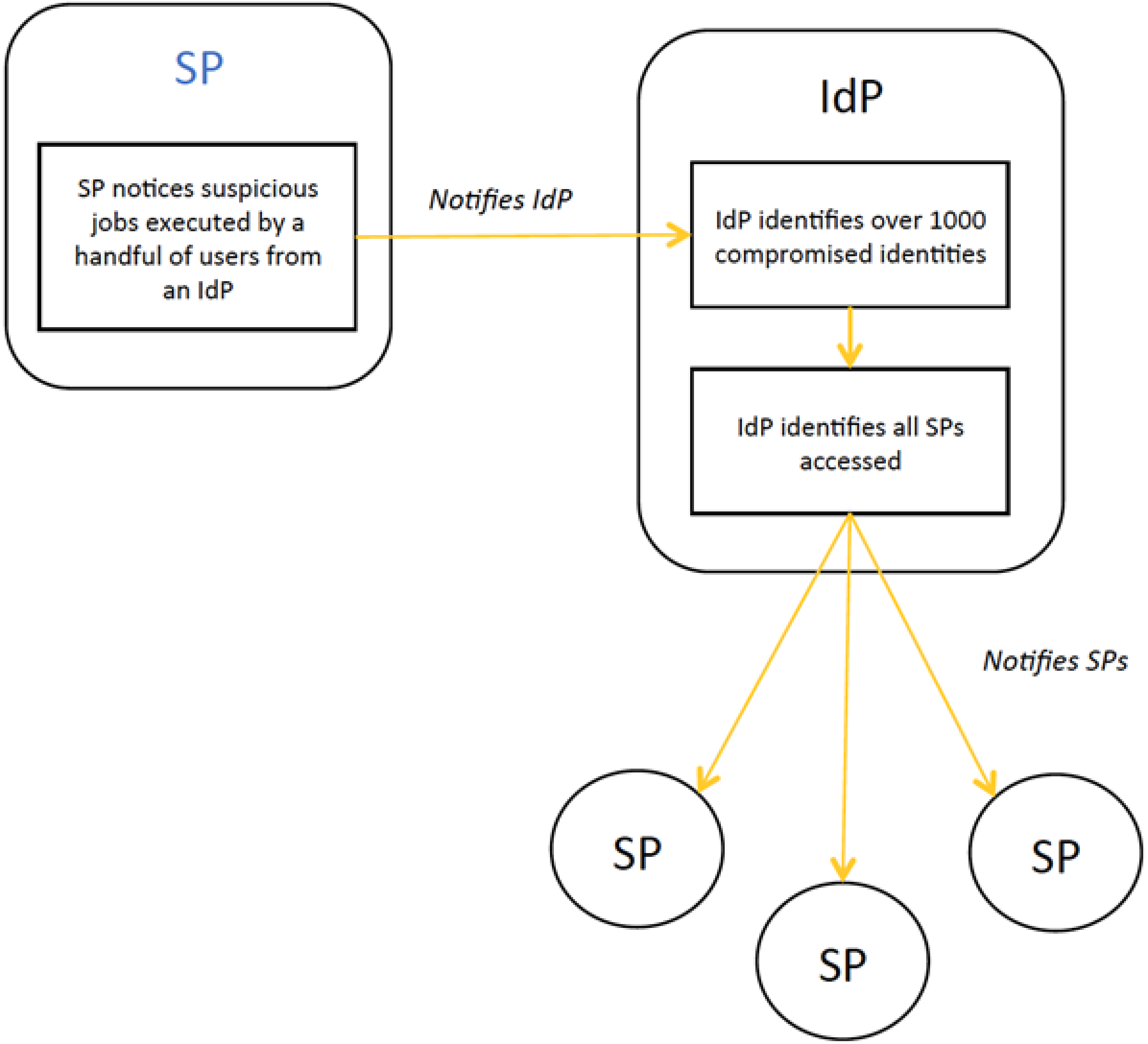
- Confirm that end users are aware of an appropriate AUP

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

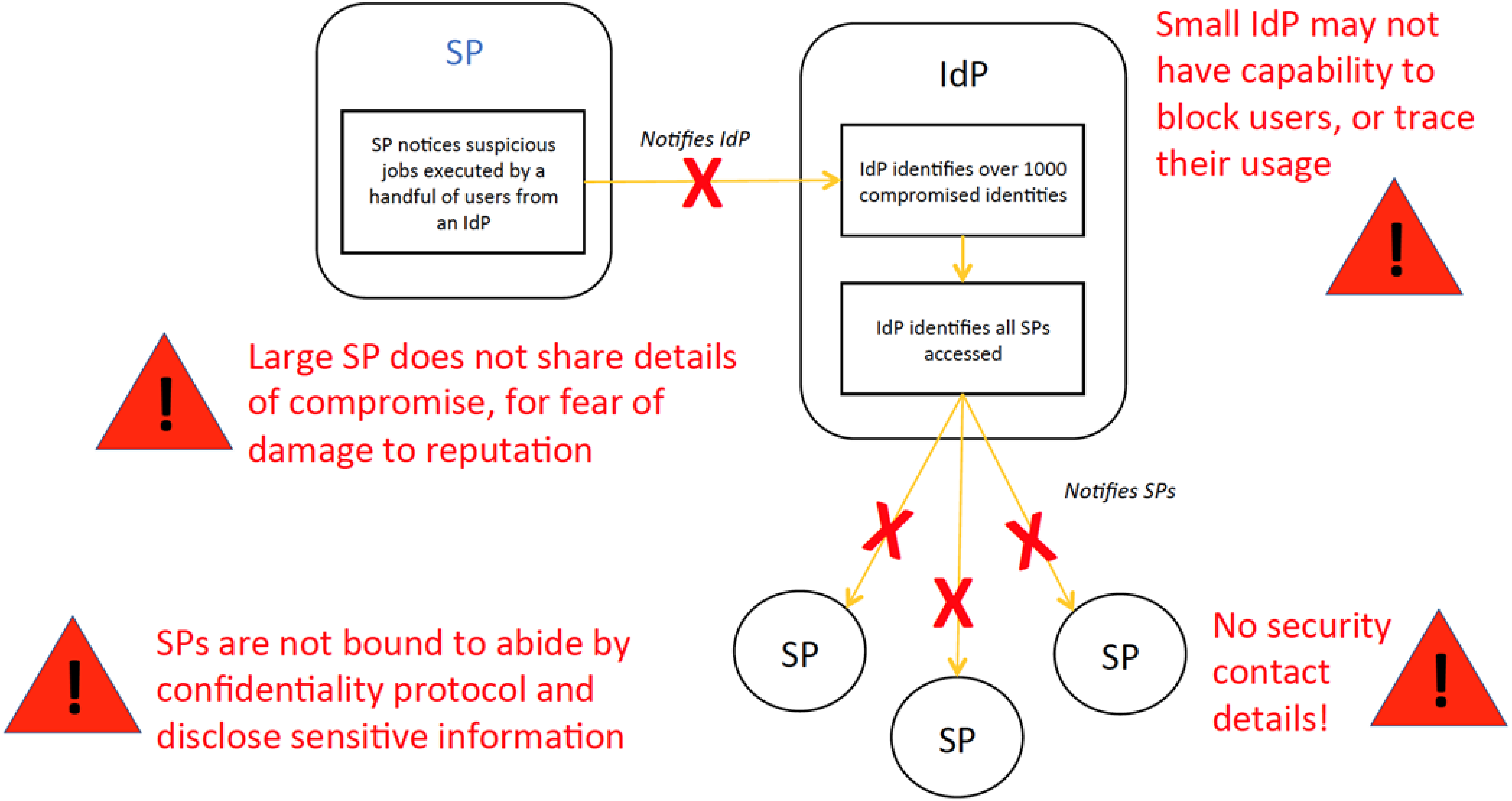


Common sense would imply….



SP
SP notices suspicious jobs executed by a handful of users from an IdP
Notifies IdP
IdP
IdP identifies over 1000 compromised identities
IdP identifies all SPs accessed
Notifies SPs
SP
SP
SP

But in practice….



SP

SP notices suspicious jobs executed by a handful of users from an IdP

Notifies IdP

IdP

IdP identifies over 1000 compromised identities

IdP identifies all SPs accessed

Notifies SPs

SP

SP

SP

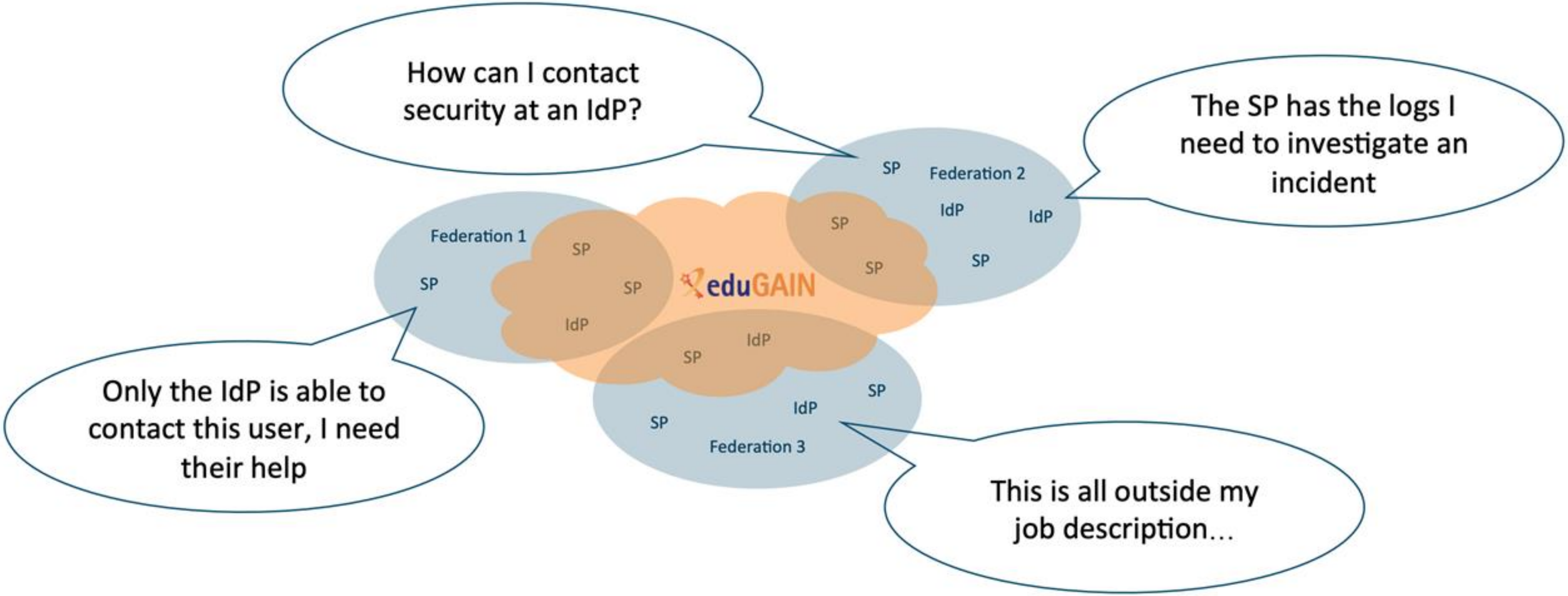
Small IdP may not have capability to block users, or trace their usage

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 ?



How can I contact security at an IdP?

The SP has the logs I need to investigate an incident

Only the IdP is able to contact this user, I need their help

This is all outside my job description…

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]**

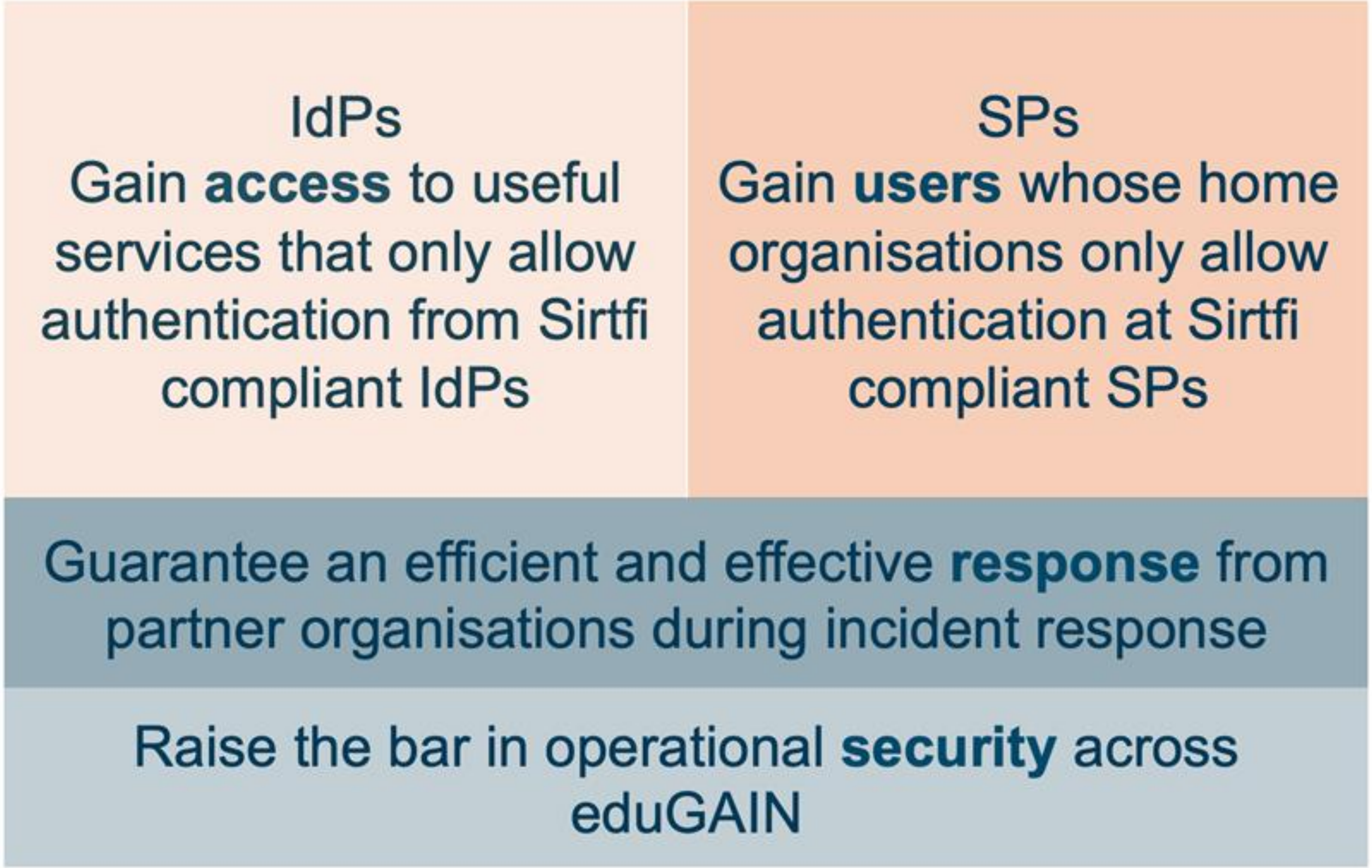
SIRTFI Operational Security [OS] Self-Assertions

- [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

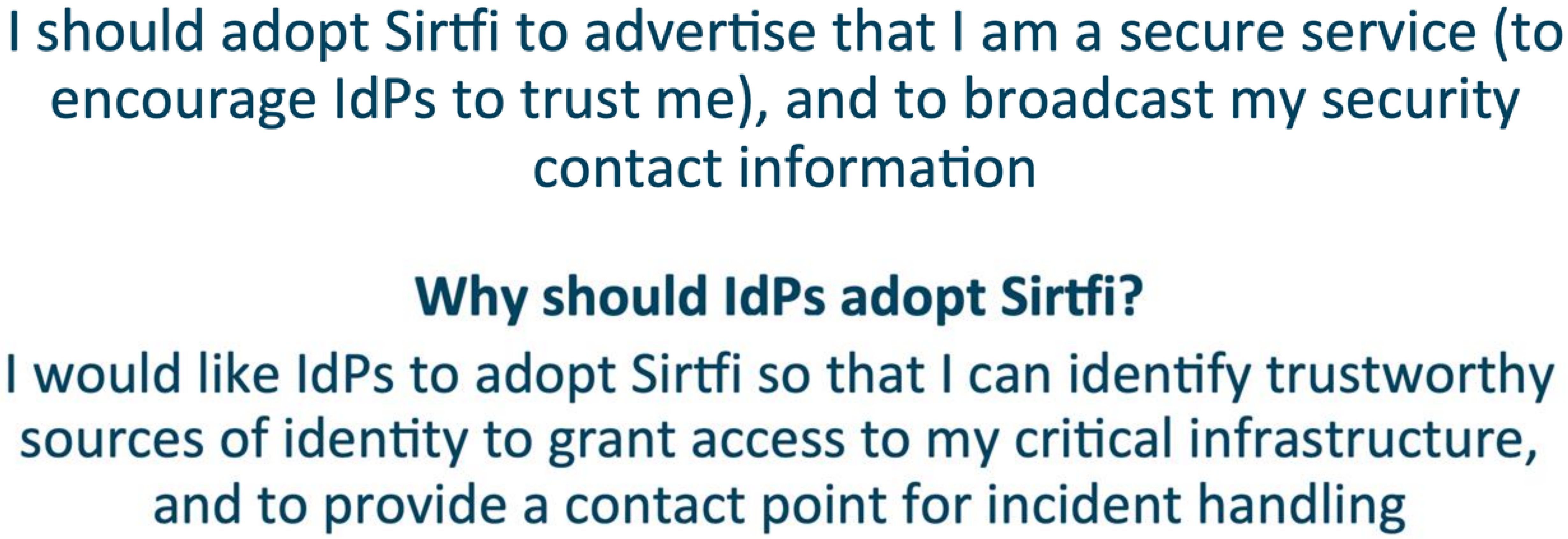
SPs
Gain **users** whose home organisations only allow authentication at Sirtfi compliant SPs

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)

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@xxxxxxxxxxxxxxx</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

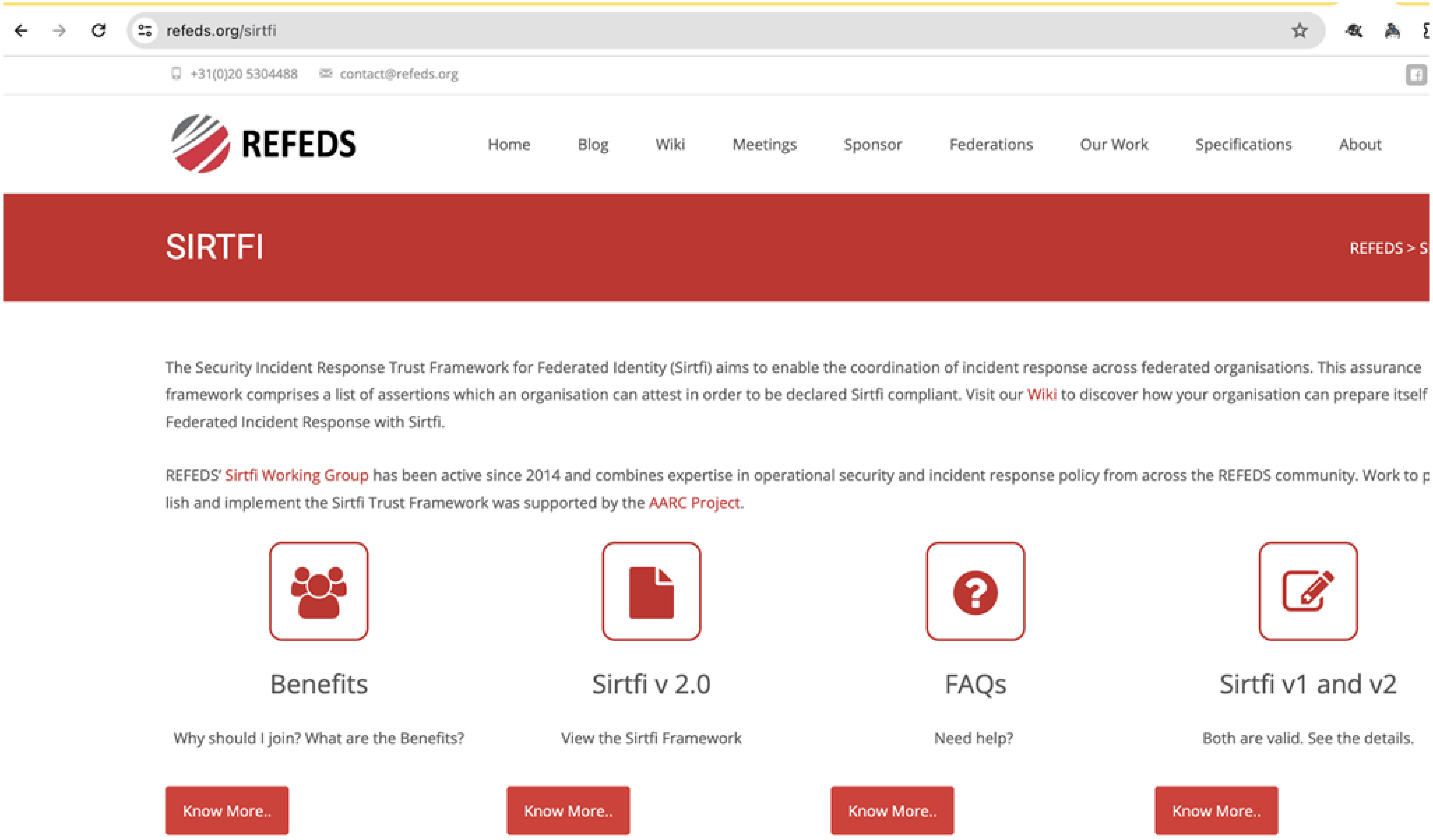
```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...>
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            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>
```

SIRTFI v2.0

- A new version of SIRTFI has been produced in 2022, to enhance the benefical outcome of the adoption of the whole Entity Category
- Among others, the main difference is in incident response procedures: **the obligation to notify entities involved**

  https://refeds.org/wp-content/uploads/2022/08/Sirtfi-v2.pdf

Find out more about SIRTIFI



SIRTFI

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 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 p lish and implement the Sirtfi Trust Framework was supported by the AARC Project.

Benefits

Why should I join? What are the Benefits?

Sirtfi v 2.0

View the Sirtfi Framework

FAQs

Need help?

Sirtfi v1 and v2

Both are valid. See the details.

Operational Security in SIRTFIv2

Operational Security [OS]

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security

- [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] Means are implemented to **detect and act on possible intrusions** using threat intelligence information in a timely manner.
- [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 [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.**

Incident Response in SIRTFIv2

- [IR1] **Provide security incident response contact information** as may be requested by any federation to which your organisation belongs.
- [IR2] Respond to requests for assistance with a security incident from other organisations participating in Sirtfi in a **timely manner.**
- **[IR3] Notify security contacts of entities participating in Sirtfi when a security incident investigation suggests that those entities are involved in the incident. Notification should also follow the security procedures of any federations to which your organisation belongs.**
- [IR4] Be able and willing to **collaborate in the management of a security incident** with affected organisations that participate in Sirtfi.
- [IR5] **Respect user privacy as determined by the organisation's policies or legal counsel.**
- [IR6] Respect the **Traffic Light Protocol [TLP]** information disclosure policy and use it during incident response communications with federation participants.

Traceability in SIRTFIv2

Traceability [TR] To be able to answer the basic questions **"who, what, where, and when"** concerning a security incident requires retaining relevant system generated information, including accurate timestamps and identifiers of system components and actors, for a period of time

- [TR1] **Relevant system generated information**, including accurate timestamps and identifiers of system components and actors, **are retained and available for use in security incident response procedures.**
- [TR2] Information attested to in [TR1] is retained **in conformance with the organisation's security incident response policy or practices.**

User Rules and Conditions [UR] in SIRTFIv2

- Identity Providers and Service Providers (participants) have a responsibility **to notify users** that **their access may be controlled following unauthorised use, such as during a security incident**

  The definition of authorised use may be communicated to the user via an Acceptable Usage policy, terms and conditions, contract or other agreement

  This may be done directly between the participant and the user, or between a third party and the user in the case that operation of a system has been delegated

  - [UR1] The participant has defined rules and conditions of use
  - [UR2] There is a process to notify all users of these rules and conditions of use

Security contact in incident response in SIRTFIv2

Security Contact *(normative section)*

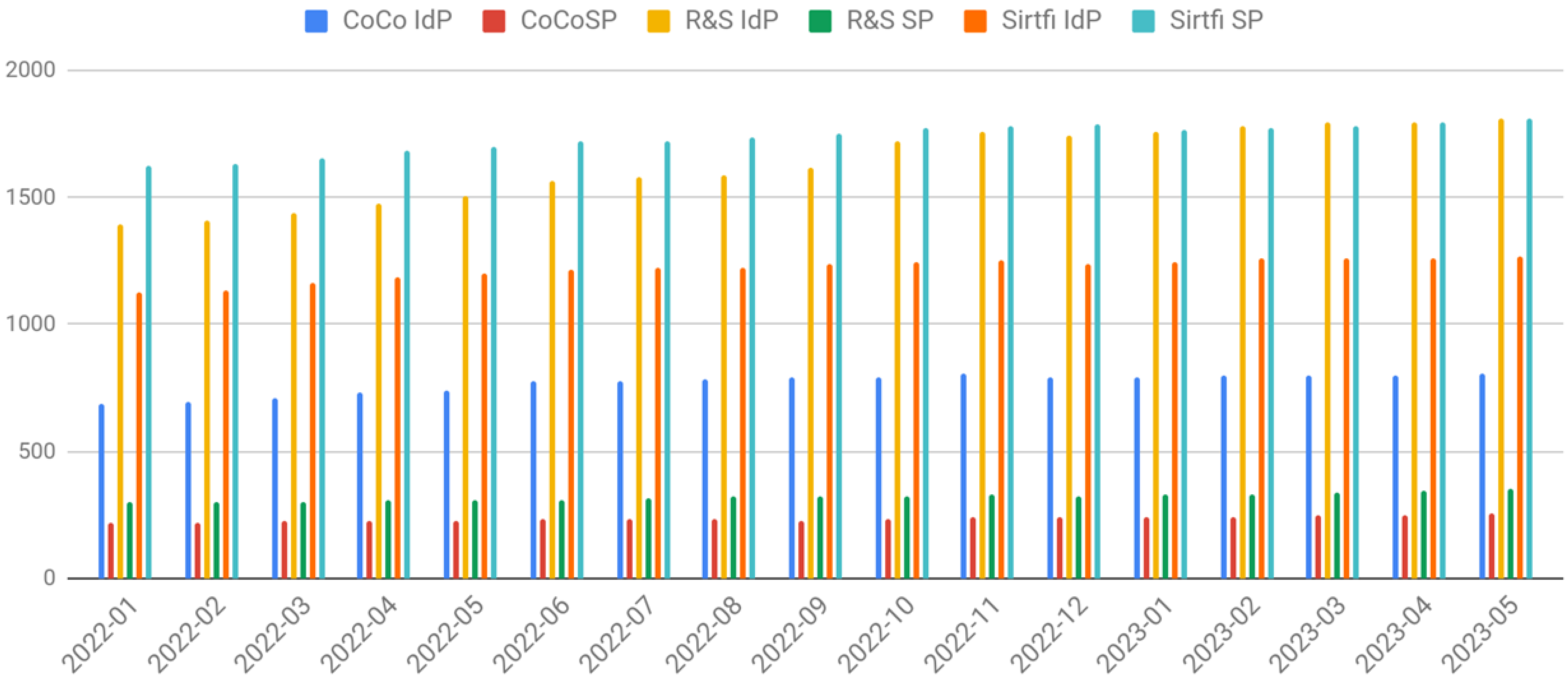
The entity operator, or party providing incident response support on behalf of the entity, **MUST:**

- **Provide a security contact [CONTACT] containing:**
  - Name, included as a GivenName element (this MAY be the name of a service function, such as "Security Operations")
  - Email, included as an EmailAddress element
  - OPTIONAL additional fields from the SAML Standard for contactPerson [SCHEMA]
- **Ensure that communication sent to the security contact is not publicly archived.**
- If the entity removes the security contact [CONTACT] from metadata, it MUST also remove the corresponding Sirtfi Attribute

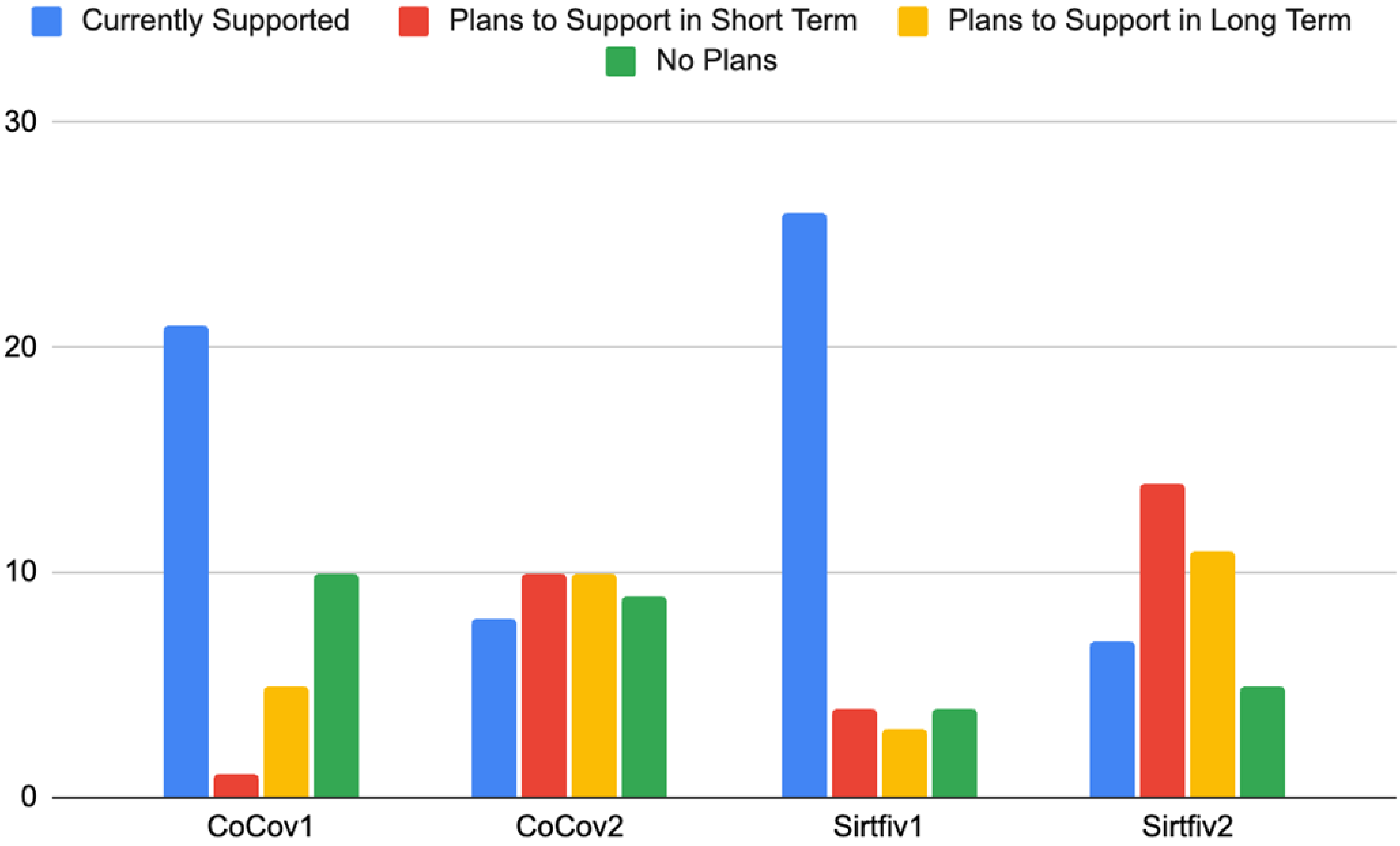
The registrar MAY perform, or facilitate, a **periodic check for responsiveness of the security contact**.

Entities' Compliance to Standards (2022):

EC adoption evolution with time

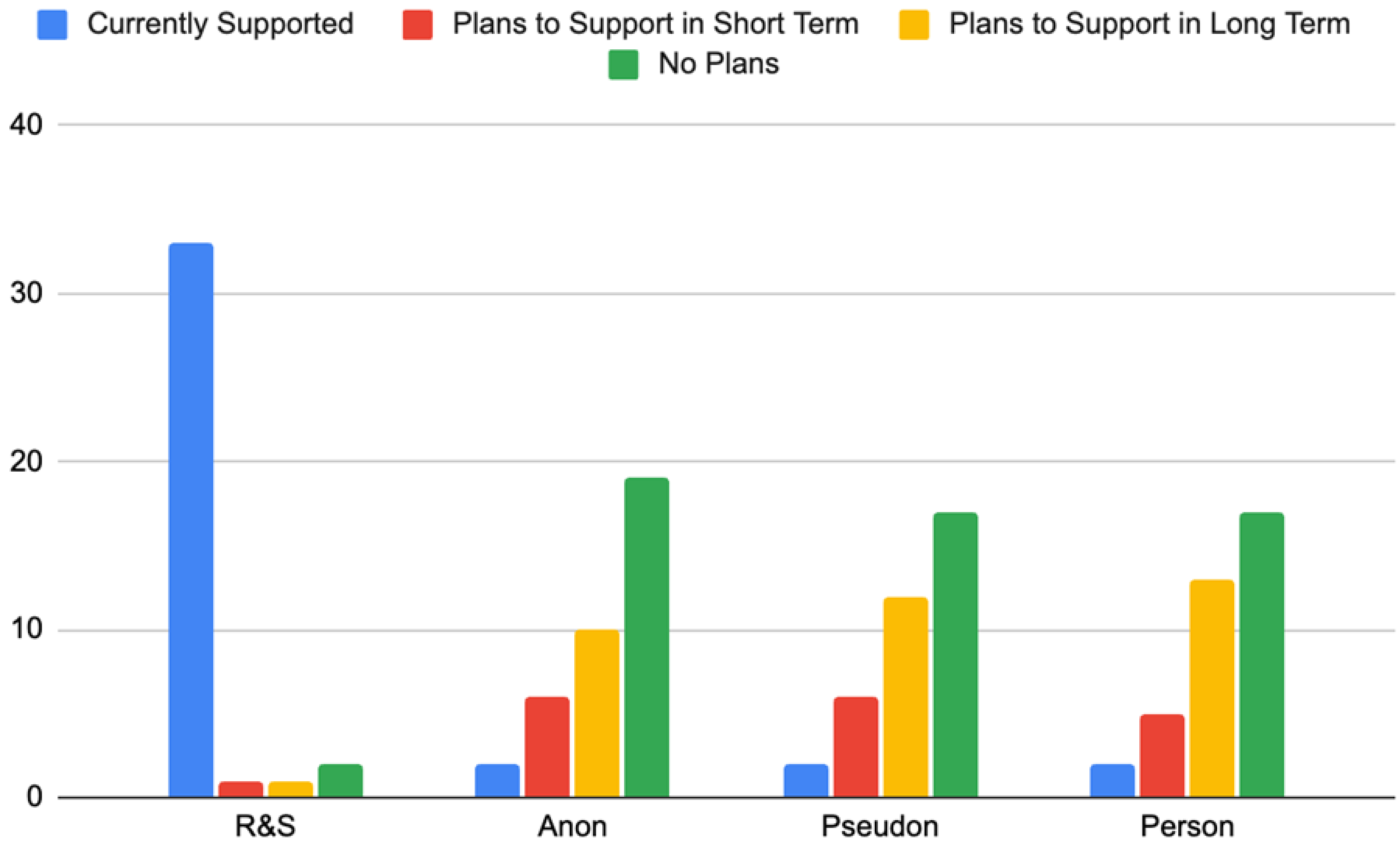


Plans for adoption of Entity Categories within the REFEDS community



Source:
REFEDS
SURVEY
2022

Plans for adoption of Entity Categories within the REFEDS community



Source:
REFEDS
SURVEY
2022

Additional – more recent - Entity Categories:

- https://refeds.org/category/anonymous **Anonymous Access**
  *By asserting this entity category, Service Providers are signalling **that they do not wish to receive personalized data.***

- https://refeds.org/category/pseudonymous **Pseudonymous Access**
  *Candidates for the Pseudonymous Access Entity Category are Service Providers that offer a level of service based on proof of successful authentication **and offer personalization based on a pseudonymous user identifier**.*

- https://refeds.org/category/personalized **Personalised Access**
  - *The service has a proven and documented need for the personally identifiable information that forms the attribute bundle for this entity category.*
  - *The Service Provider has committed to data minimisation and will not use the attributes for purposes other than as described in their request.*

Thank You

www.geant.org

Co-funded by
the European Union