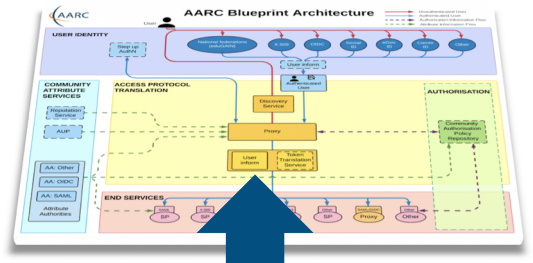
eduGAIN overview

Marina Adomeit, SUNET

SUNETdagarna, October 2020

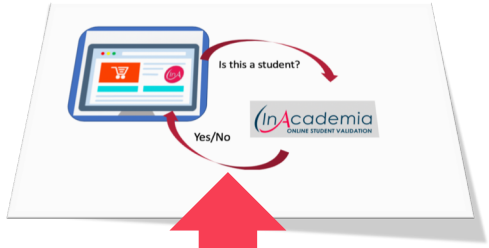
Global T&I service portfolio

eduTEAMS



Support virtual teams and share resources

InAcademia
ONLINE STUDENT VALIDATION



Offering a validation service based on the “studentness”

SUNET

Widening scope with OpenRoaming

eduGAIN

eduroam

haka
SWITCHaai
cafe
grnet
SWAMID
COFRe Comunidad Federada REUNA
The UK Access Management Federation FOR EDUCATION AND RESEARCH
confia
arnes
GakuNin
TAAT
Carsi
RCTSaai
MiNGA
FEIDE
WAYF Where are you from
SURF CONEXT
Belnet RGE Federation
edu ID
SIFULAN
InCommon
aconet
TAIFE
RENATER CONNECTEUR DE SAVOIRS
AUSTRALIAN ACCESS FEDERATION
idem garr aai
Tuakiri
DFN-AAI
Colfire
Edugate
AFIRE
@EduHr
edu ID cz
SIR

Key Benefits of eduGAIN

SUNET

- Enabling secure Single Sign On services to national and global R&E resources

Institutions

Enables institutions to support access to thousands of services within identity federation they participate and globally.

Service Providers

Education, Publishers, Research infrastructures and Cloud service providers can leverage a worldwide authentication service for R&E.

Students and Researchers

Students, Researchers and Staff access online services and resources using their Institution identity, improving the user experience, security and privacy and reducing the costs and complexity.

GÉANT

Identity Federation

R&E Institution

User

eduGAIN

Global Metadata Service

Supporting Tools

Global Policy

National Metadata Service

National Policy

SAML Auth Infrastructure

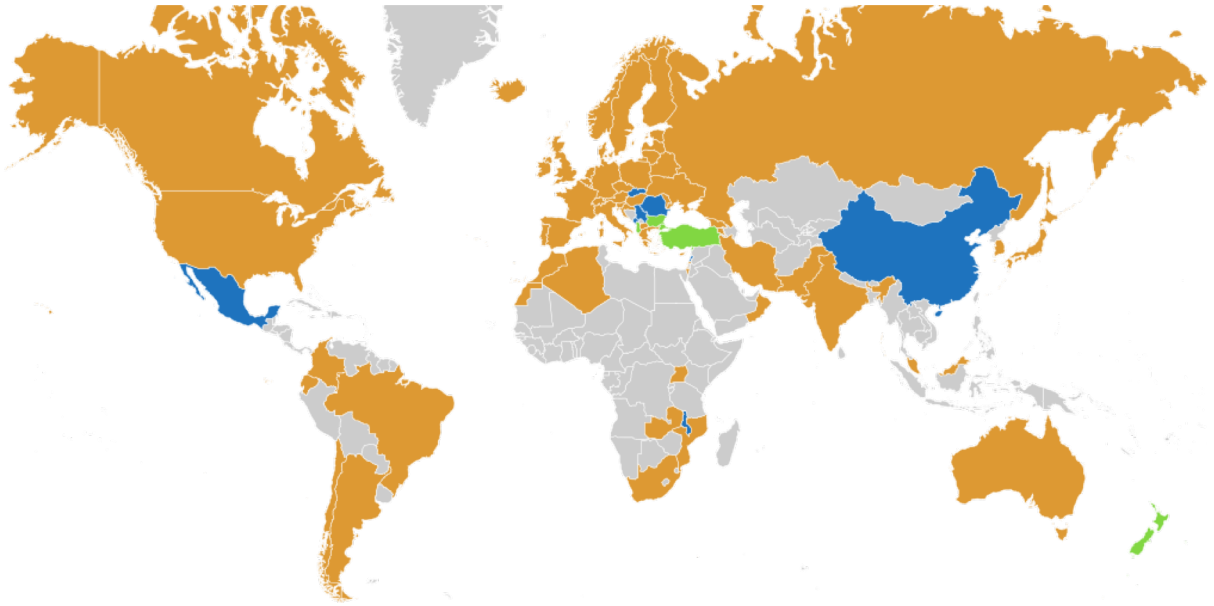
Identity Management

Web Service

Can use over 2900 Web services

SUNET

Access to thousands of WebSSO services available via eduGAIN, with R&E institutional identity



eduGAIN Entities and Discovery Service

SUNET

Identity Provider - IdP

The system component that **authenticates a user** (e.g. with username and passwords) and issues identity assertions on behalf of the user who wants to access a service protected by a Service Provider.

Service Provider - SP

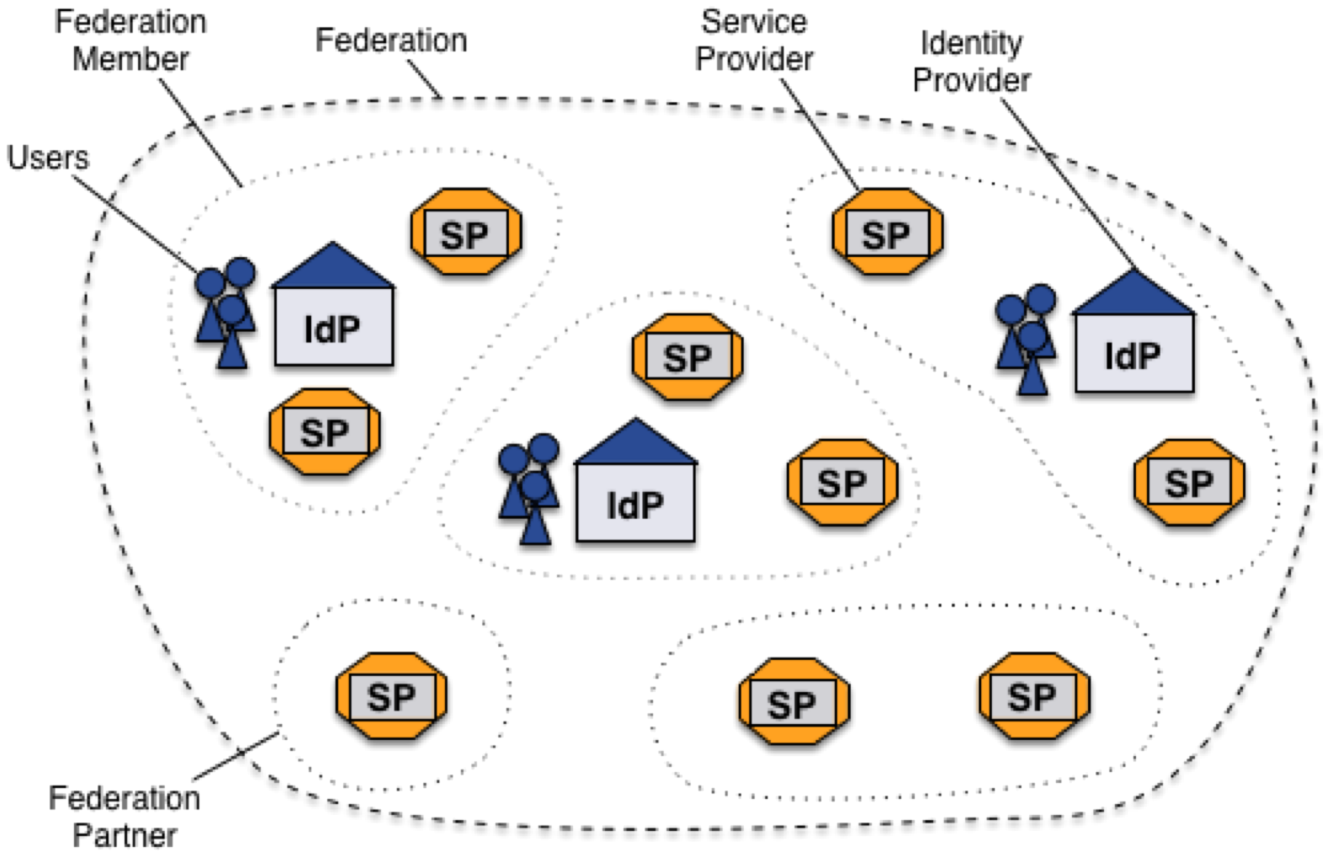
The system component that **evaluates identity assertions from an Identity Provider and uses the information from the assertion for controlling access to protected services.**

Discovery Service - DS

The Discovery Service service, **lets the user choose his home institution from a list and then redirects the user to the login page** of the selected institution for authentication. Can be integrated within SP site, or used as an external service.

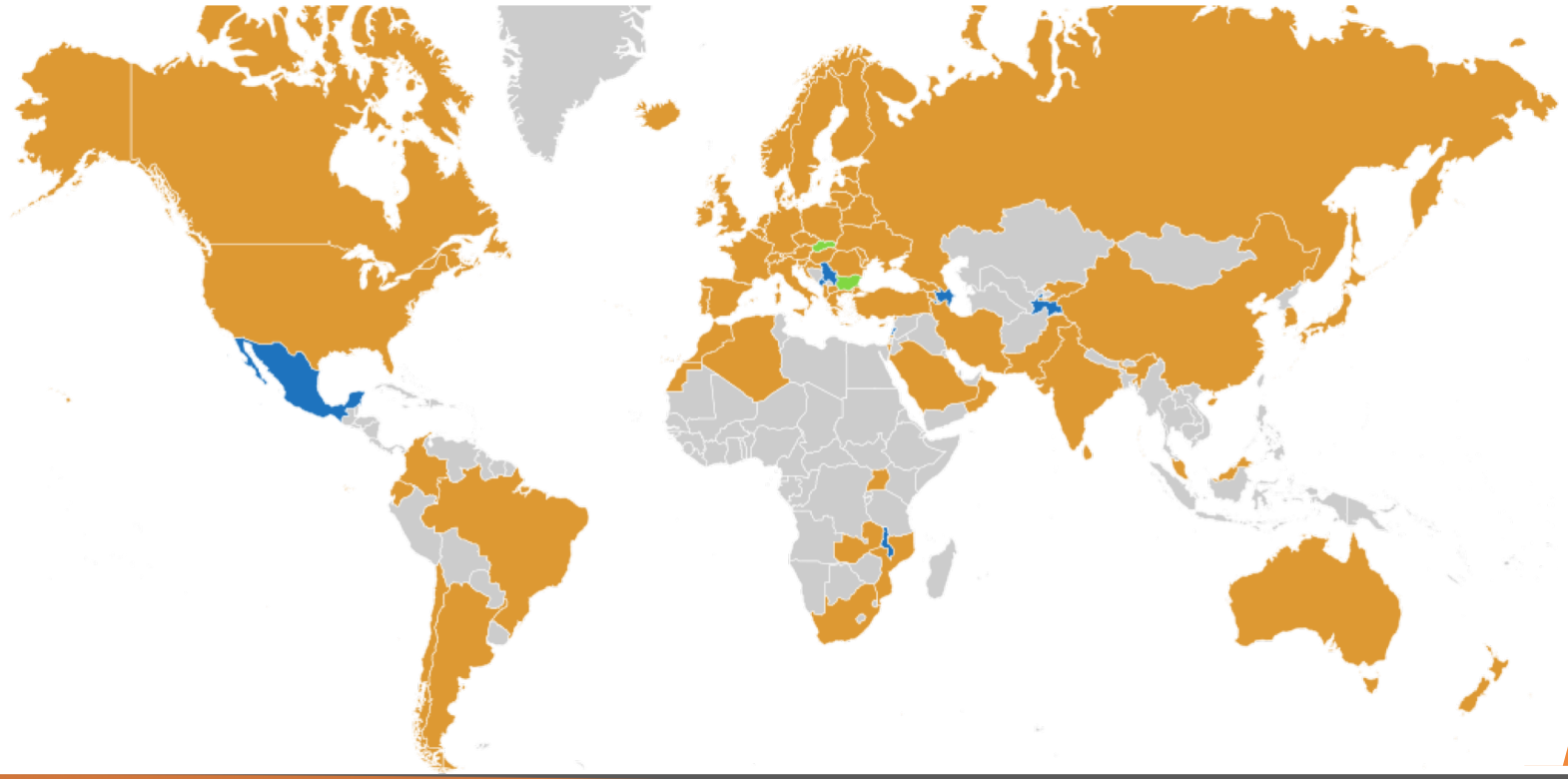
Identity Federation

- An Identity federation is a collection of organizations that agree to interoperate under a certain rule set.
- This rule set typically consists of **legal frameworks**, **policies** and **technical profiles** and standards.
- It provides the necessary **trust** and **security** to exchange home organizations' **identity** information to **access services** within the federation.



eduGAIN in Numbers

- 5th October 2020 from https://technical.edugain.org

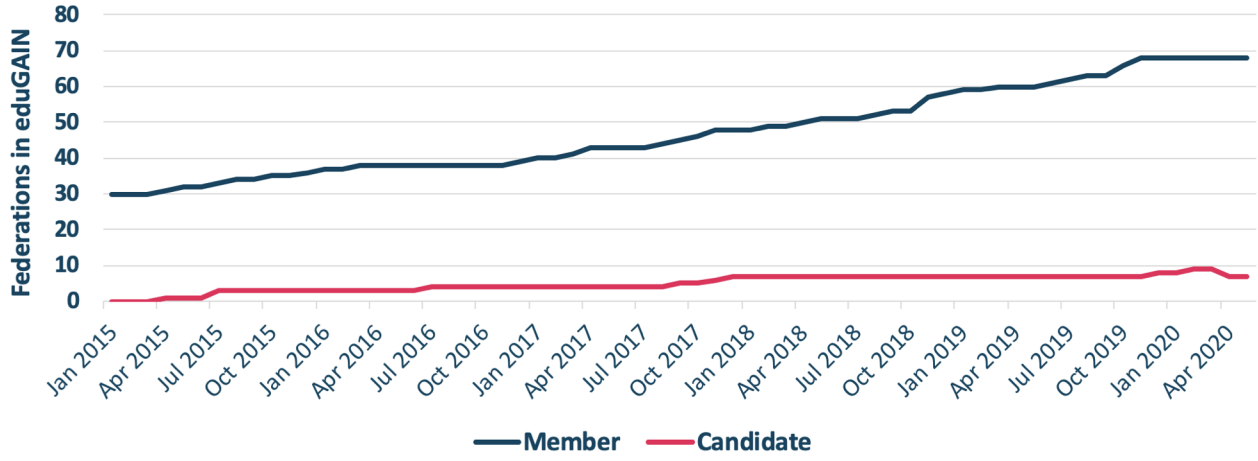


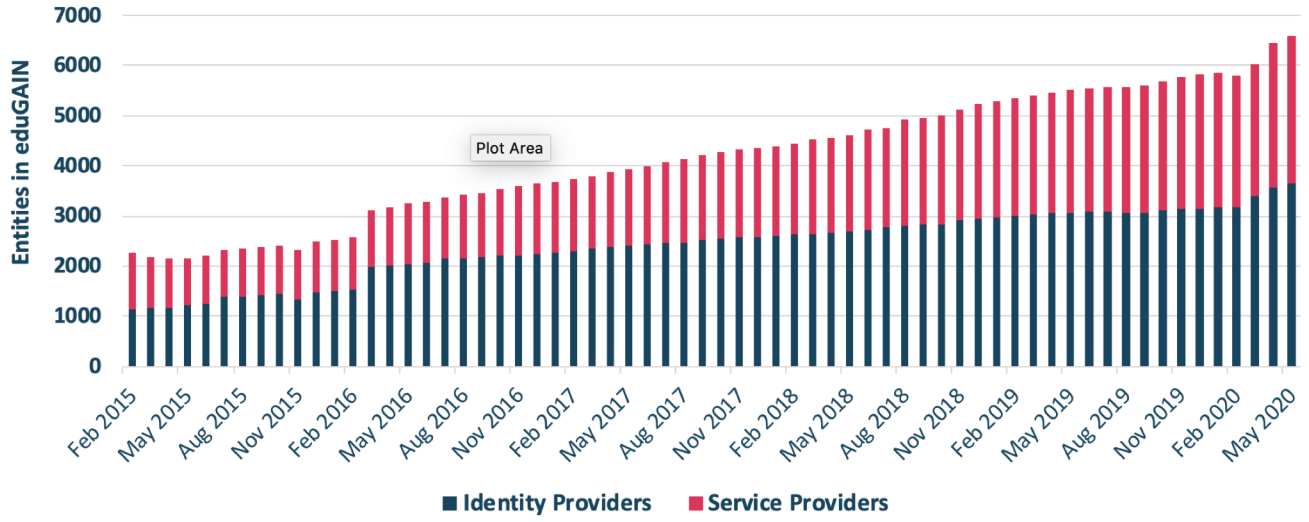
69
Identity Federations

4015
Identity Providers

3090
Service Providers

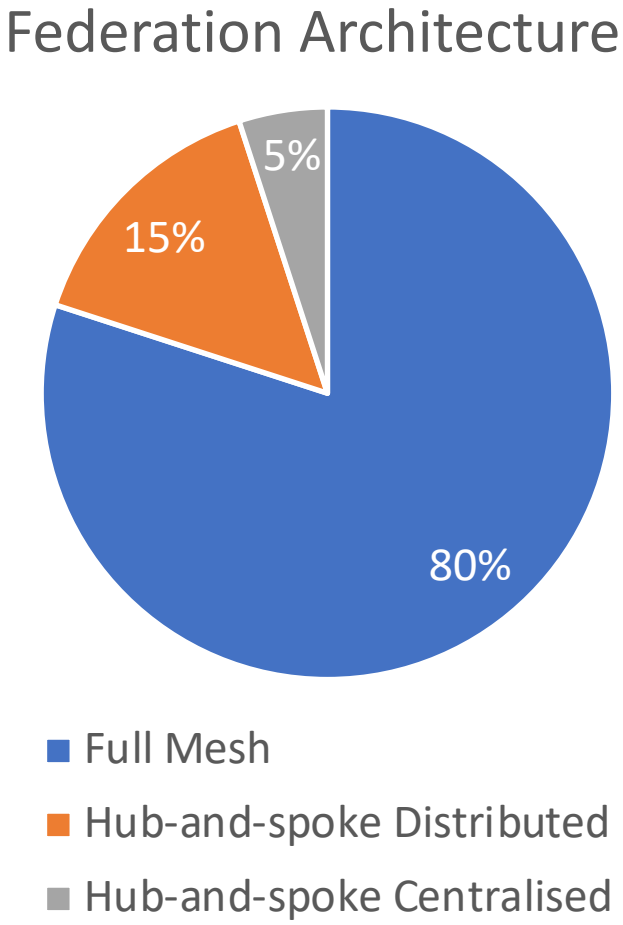
eduGAIN Growth in Numbers





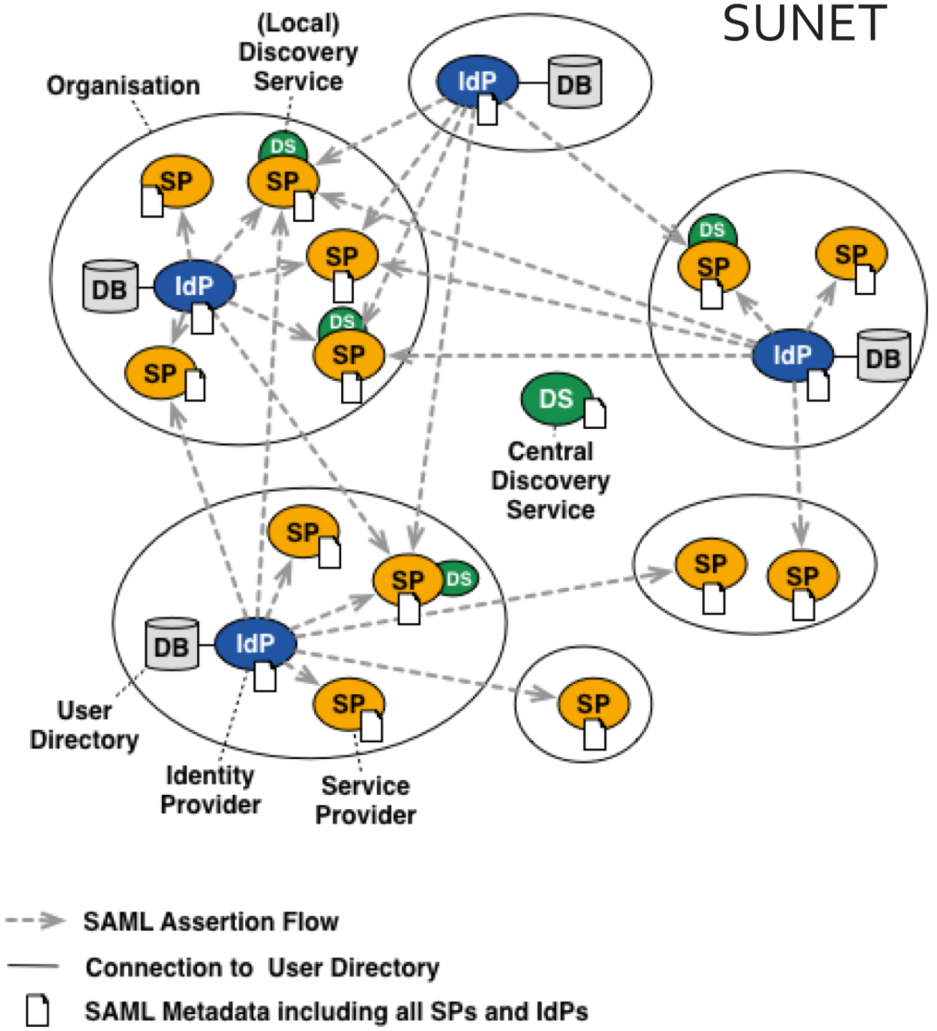
Common Federation Architectures

- **Full Mesh:** Full mesh federations are the most common and straight forward to implement federations because everything is distributed and there is no need for a central component that has to be protected specifically against failover.
- **Hub-and-spoke Distributed:** Hub-and-Spoke federations with distributed login rely on a central hub or proxy via which all SAML assertions are sent.
- **Hub-and-Spoke Centralized:** Hub-and-Spoke federations with central login are a special case in the sense as there is only one single Identity Provider in the federation.



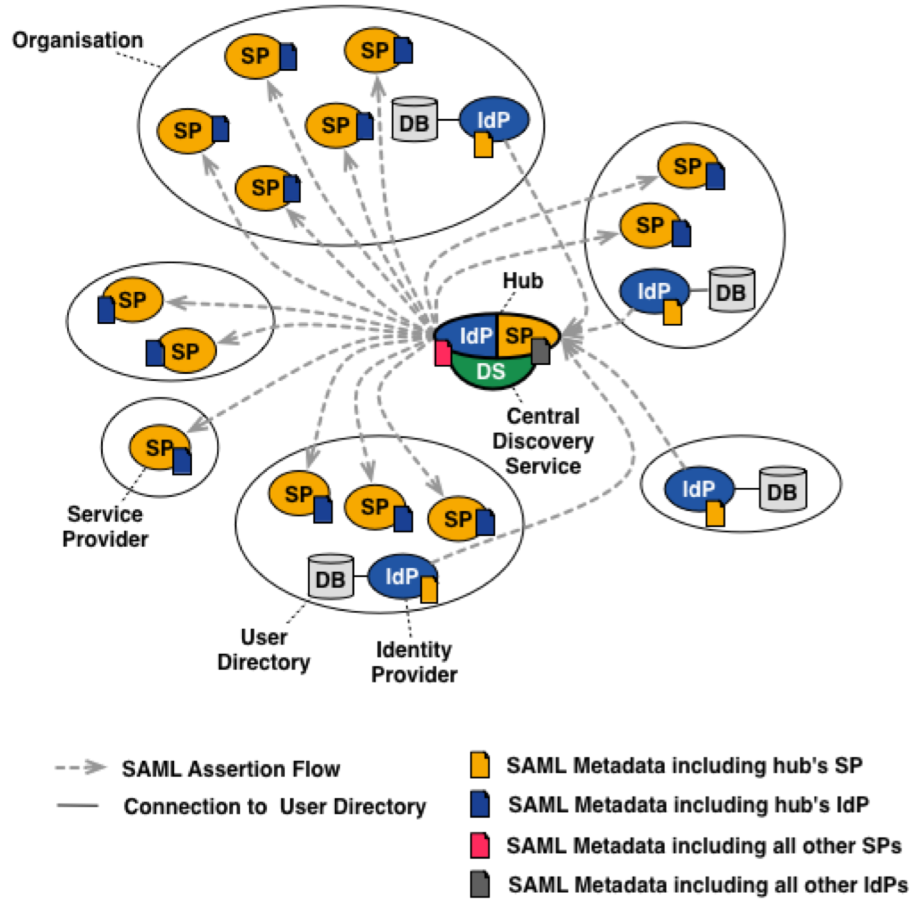
Full Mesh Federation

- Every organisation in federation operates their own IdP connected to a local identity management solution and/or an arbitrary number of SPs.
- Federation operator is anchor of trust that registers entities metadata according to its policy. This metadata is aggregated, signed and published as Federation metadata.
- Consequently, all entities are listed in Federation metadata that is consumed by all entities in the federation.



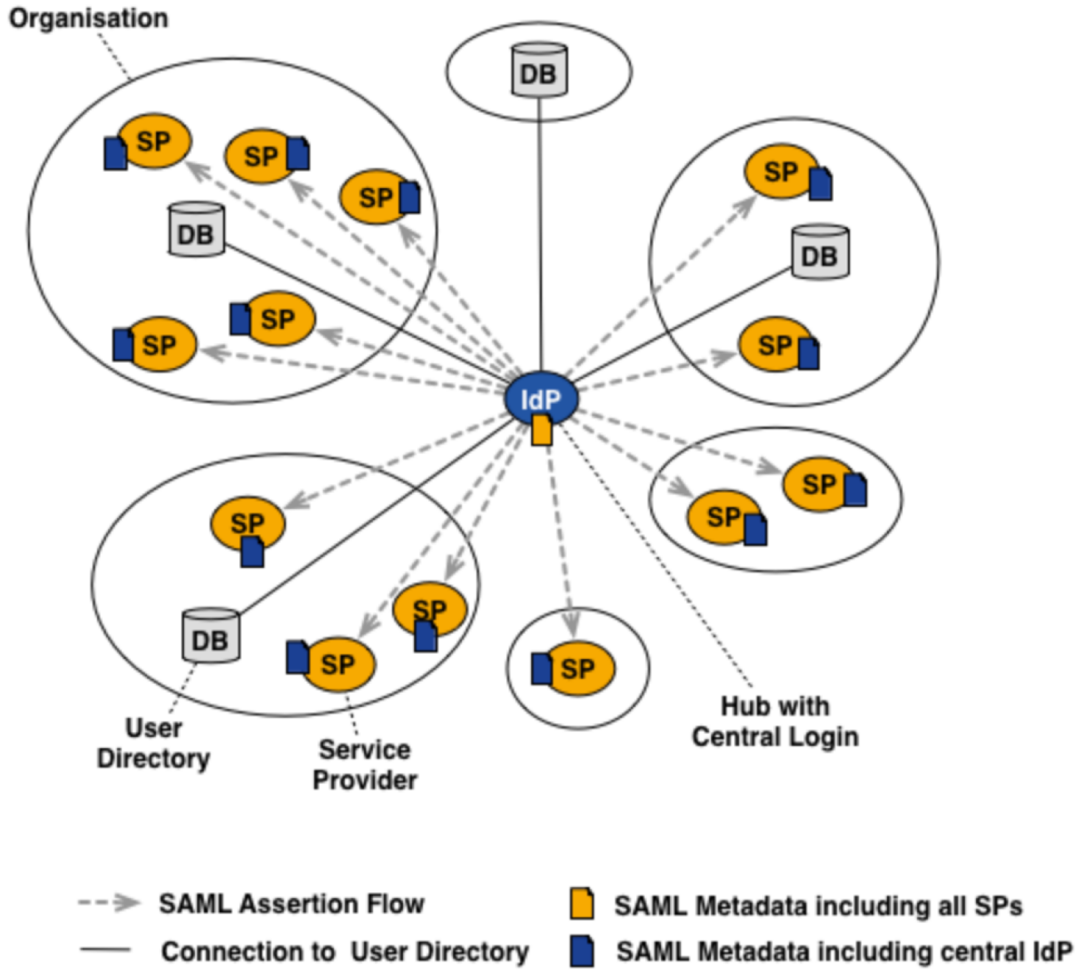
Hub-and-Spoke Distributed Federation

- Each organisation still operates their own IdP connected to a local Identity management system, but IdP is only connected to central hub.
- Vice versa the SPs are also connected to the hub.
- IdPs and SPs only consume metadata of hub.
- The hub serves as a SP versus the IdPs and as an IdP versus the SPs in the federation.
- Hub typically also offers a number of services such as central DS, managing attribute release policies etc.
- Because the hub is a single-point of failure, it has to be carefully secured and protected.



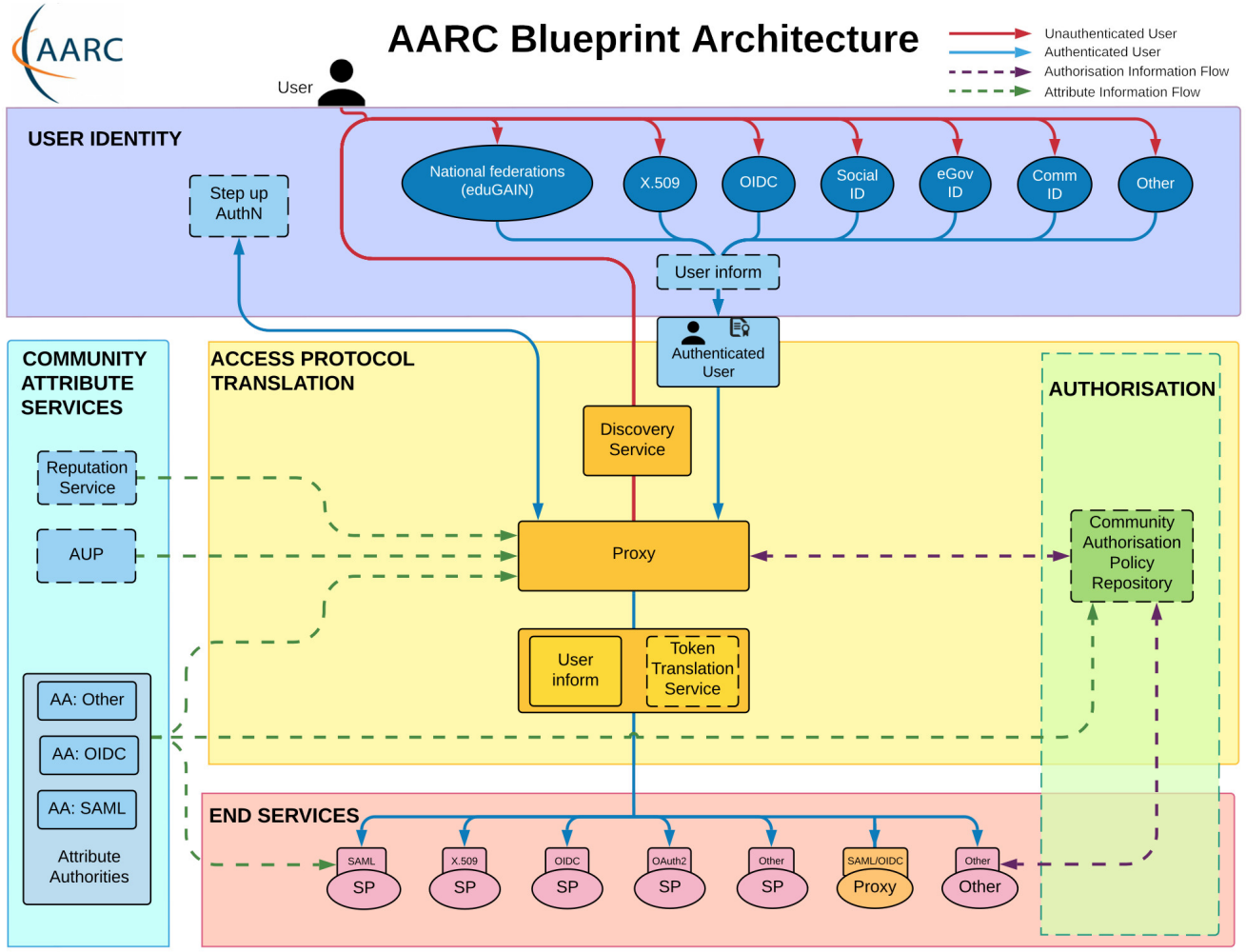
Hub-and-Spoke Centralised Federation

- There is only one single IdPs in the federation.
- Instead of operating individual IdPs at each organisation, in this architecture all organization's identity management databases are connected to a central IdP.
- The organisation operating central IdPs needs to be especially trusted by all organisations.
- Central IdP is a single point of failure and it must be highly available.
- On the other side, it is very easy to support new authentication protocols on the hub thanks to the central login.



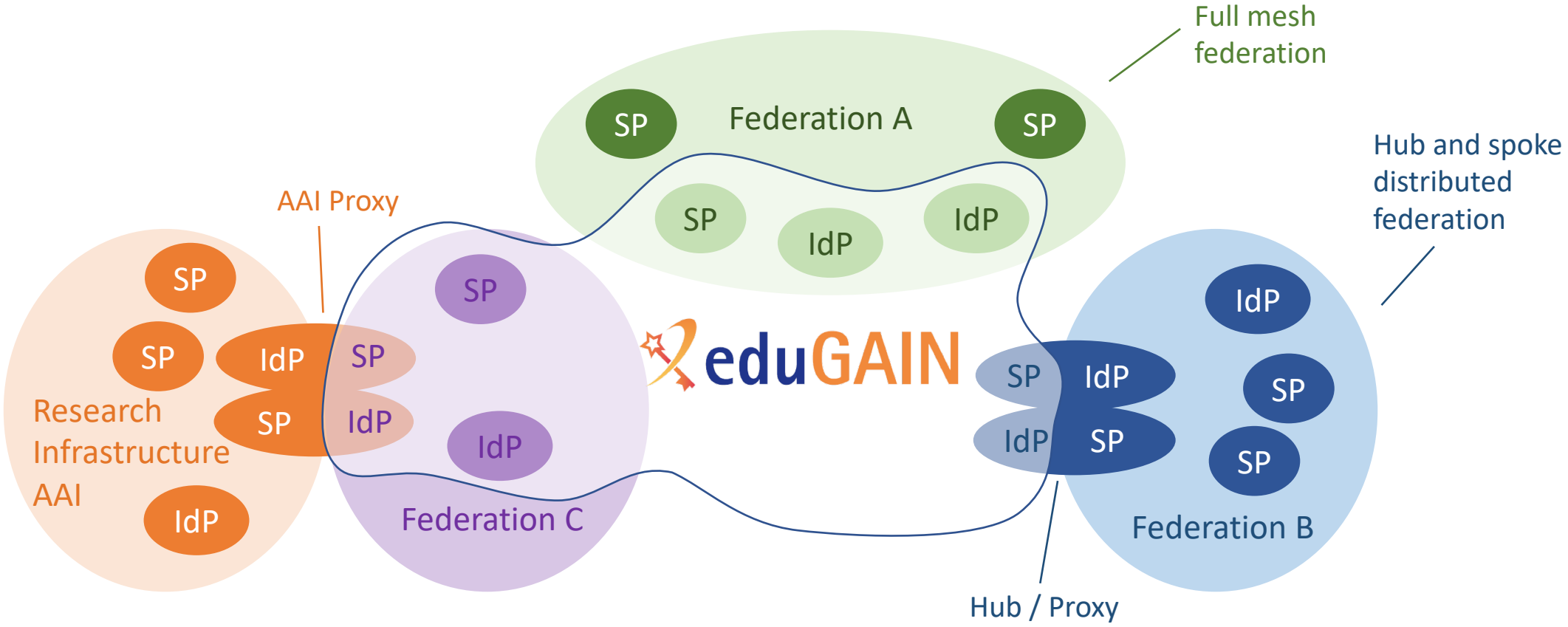
AARC Blueprint Architecture - BPA

- Blueprint for Research Infrastructure (RI) AAIs
- RI AAI Specifics:
  - Manage roles and membership attributes that are in context of that research project
  - Connect specific SPs in context of that collaboration via one AAI Proxy
  - Integrate IdPs not available in context of eduGAIN



The big picture of eduGAIN

- Complex eduGAIN ecosystem of different R&E Federations and Research infrastructures



eduGAIN MDS, how does it work?

- **1. Federations' upstream feed**

Participating Federations provide an upstream federation metadata aggregate of entities to be exported to eduGAIN

- **2. The eduGAIN metadata feed**

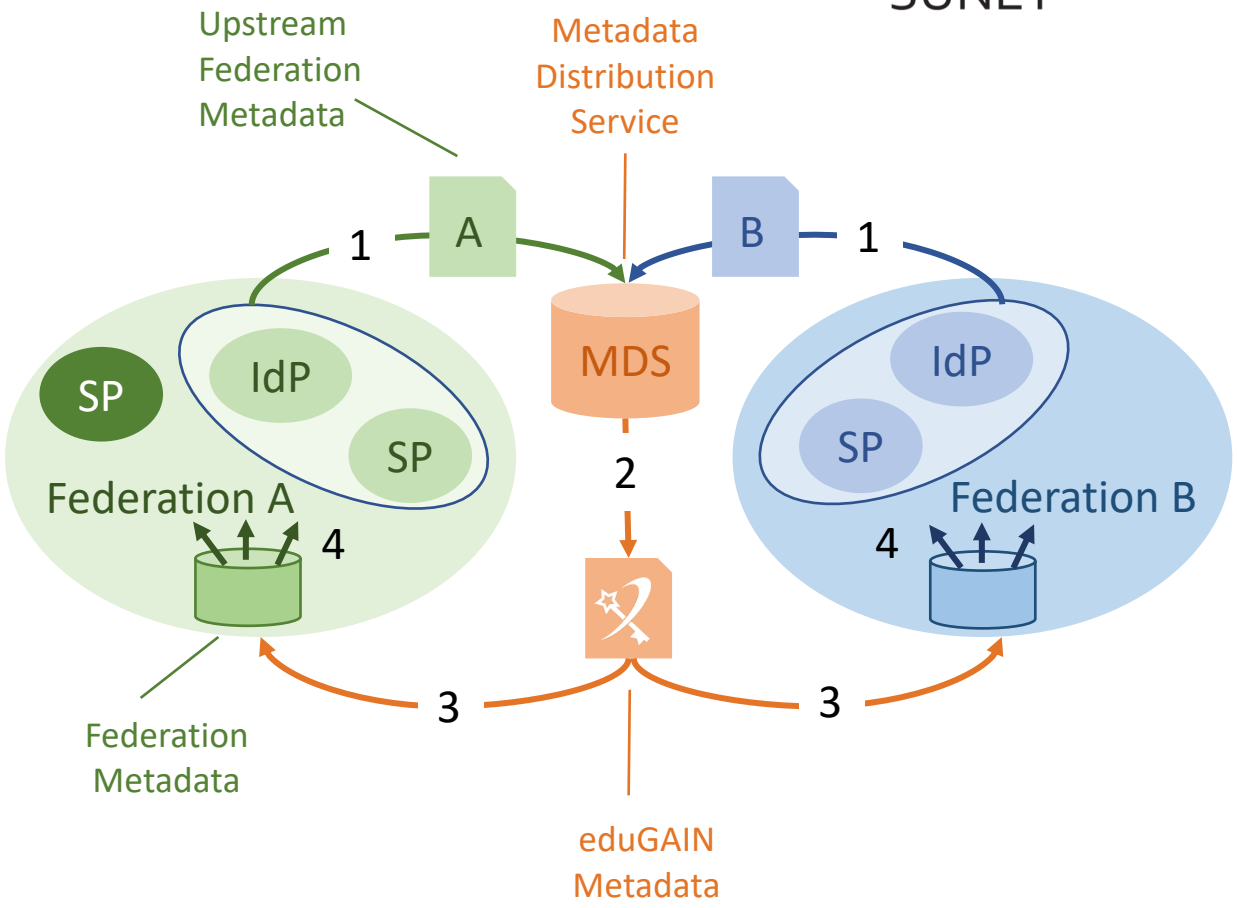
Federations' metadata aggregates are picked up, validated and aggregated in the so called eduGAIN metadata feed

- **3. Signing & Distribution**

The eduGAIN feed is signed with the eduGAIN key and distributed to Federations through the eduGAIN MDS

- **4. Federations redistribute eduGAIN metadata feed**

Federation pulls eduGAIN metadata, aggregates, signs and publishes in federation metadata for its members



eduGAIN supporting tools

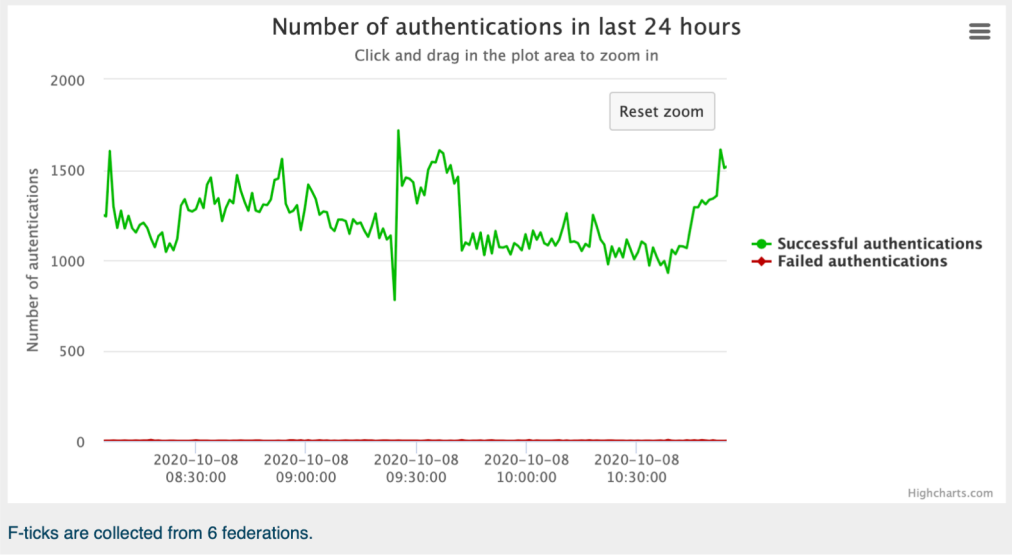
SUNET

Metadata

eduGAIN Metadata Distribution Service (MDS)
eduGAIN Validator
eduGAIN Entities Database
eduGAIN Technical site (and APIs)

Attribute Release

eduGAIN Connectivity Check (ECC)
eduGAIN isFederated Check (EIFC)
eduGAIN Access Check (EAC)
eduGAIN Attribute Release Check (EARC) ->
Use the one prepared by SWAMID
eduGAIN Code of Conduct Monitor (ECOCM) monitor



F-ticks are collected from 6 federations.

https://technical.edugain.org

https://f-ticks.edugain.org

eduGAIN Challenges

SUNET

- Too few federations participate
  - Solved as more then 85% known R&E federations participate
- Too few organisations participate
  - Addressed with recommendations for opt-in/opt-out approach
- Process to address interfederated security incidents
  - eduGAIN Security team and SIRTFI Entity Category
- Too few attributes get released
  - Addressed with Entity Categories – R&S and CoCo

eduGAIN Challenges that lead to Complexity

SUNET

- Still too complex to end users
  - Improvement for discovery service -> Seamless Access
- Complex environment for profit SPs that need to check students
  - InAcademia service
- Complex environment for Research Infrastructures
  - eduTEAMS service for international research projects and national solutions for national context based on AARC BPA
- Different technical and policy federation rules
  - Upcomming REFEDS Baseline expectations

REFEDS Entity Categories

- Entity Categories used within eduGAIN are managed by **REFEDS** through an open consultation among all the Federation Operators

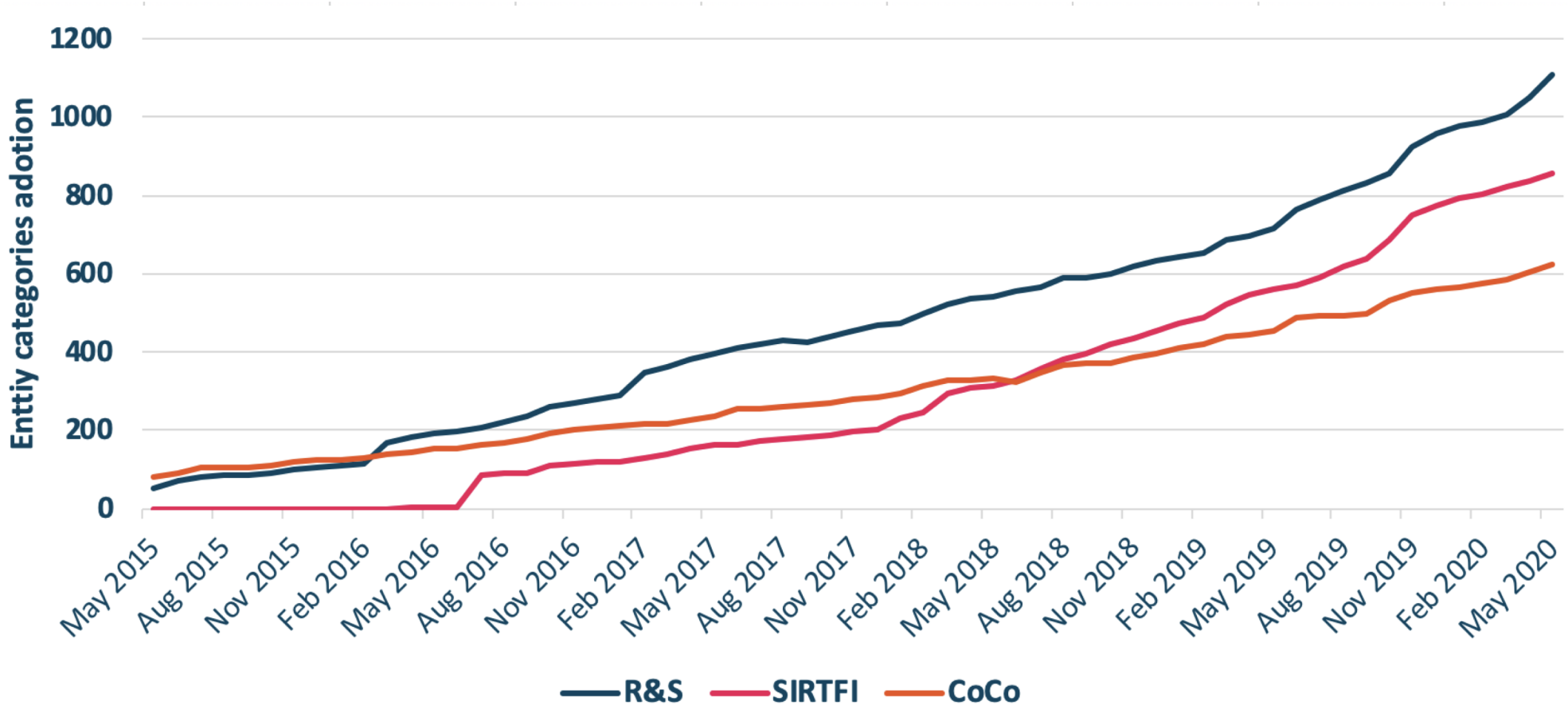
  https://wiki.refeds.org/display/ENT/Entity-Categories+Home

- Enitity Categories are used to express that an entity is following characteristics set out in the definition of that category
- They add another layer enabling entities to express additional capabilities with aim of enabling trust establishment between entitles in international context
- Trust enables IdPs to better form attribute release decisions

  https://wiki.sunet.se/display/SWAMID/Entity+Category+attribute+release+in+SWAMID

REFEDS Entity Categories Adoption

SUNET



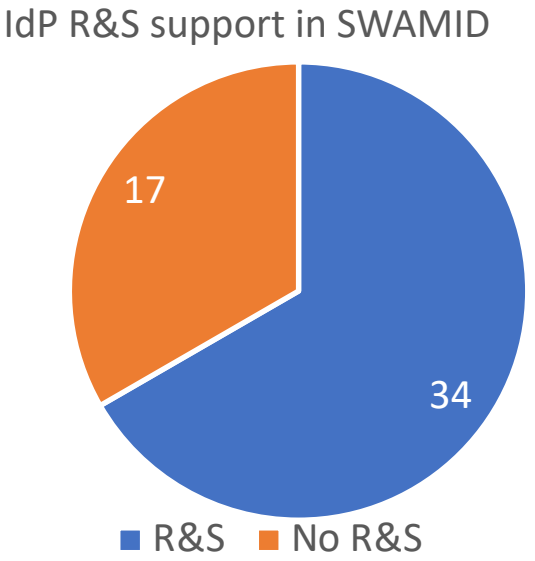
REFEDS Research and Scholarship - R&S

SUNET

- Designed as a simple and scalable way for IdPs to release minimal amounts of required personal data to SP serving the Research and Scholarship Community
- Services are tagged by federation operators that have briefly audited the SPs to ensure they meet R&S criteria
- Once tagged, IdPs can safely release a small set of data to these providers with the knowledge it meets minimal requirements and privacy requirements
- SWAMID process for applying for R&S Entity Category

https://wiki.sunet.se/display/SWAMID/4.1+Entity+Categories+for+Service+Providers

https://wiki.sunet.se/display/SWAMID/Entity+Support+Categories+for+Identity+Providers



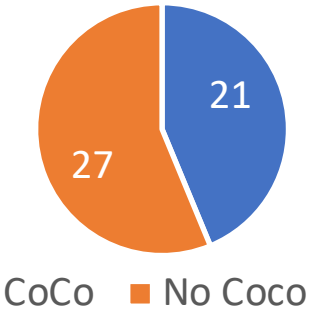
GÉANT Code of Conduct - CoCo

- Describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management
- Defines behavioral rules following EU DPD for SPs which want to receive user attributes from the IdPs
- It is expected that IdPs are more willing to release attributes to SPs who manifest conformance to the GÉANT CoCo
- SWAMID process for applying for GÉANT CoCo Entity Category

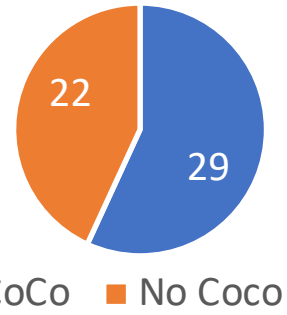
https://wiki.sunet.se/display/SWAMID/4.1+Entity+Categories+for+Service+Providers

https://wiki.sunet.se/display/SWAMID/Entity+Support+Categories+for+Identity+Providers

SP support for CoCo in SWAMID

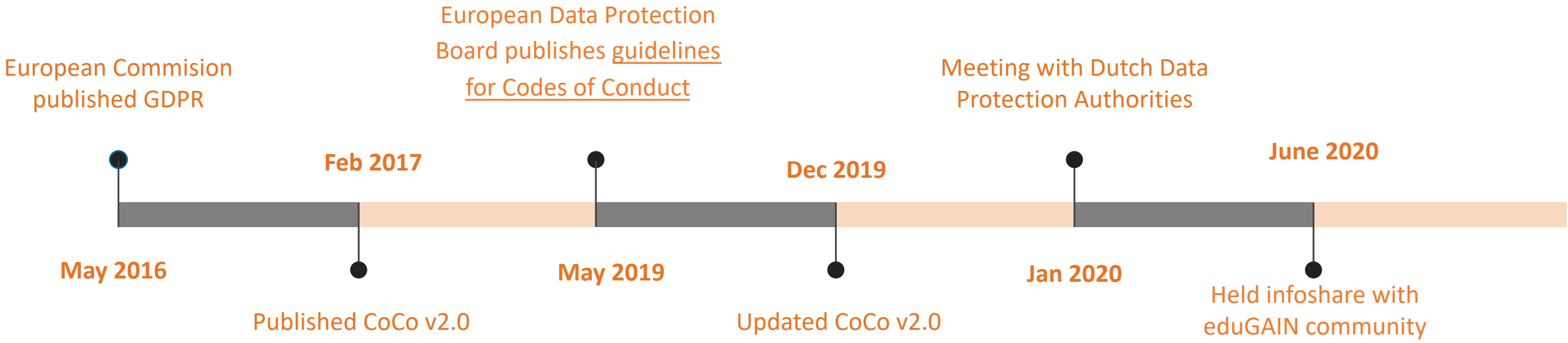


IdP support for CoCo in SWAMID



GÉANT CoCo

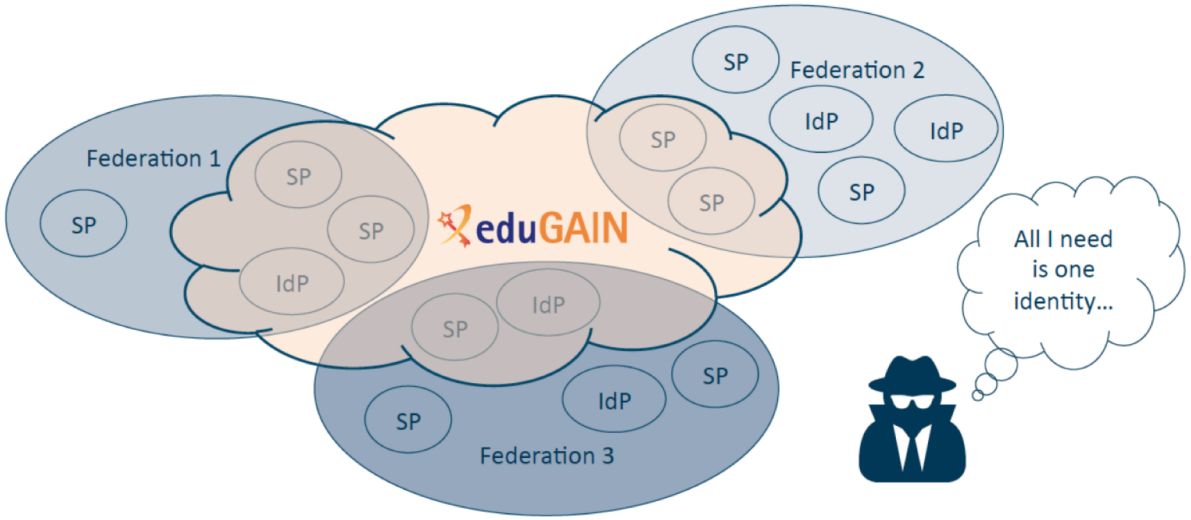
- V2.0 was created to reflect GDPR requirements and also include international data transfer
- In order to be legally valid, GÉANT CoCo needs to be registered by a national data protection authority
- After meetings with Dutch Data Protection Authorities, conclusion was that v2.0 cannot be registered as current European Data Protection Board guidelines do not address international transfer of personal data
- After community consultations, decision was to continue working on CoCo v 2.0 limiting it to European personal information transfer
- https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project



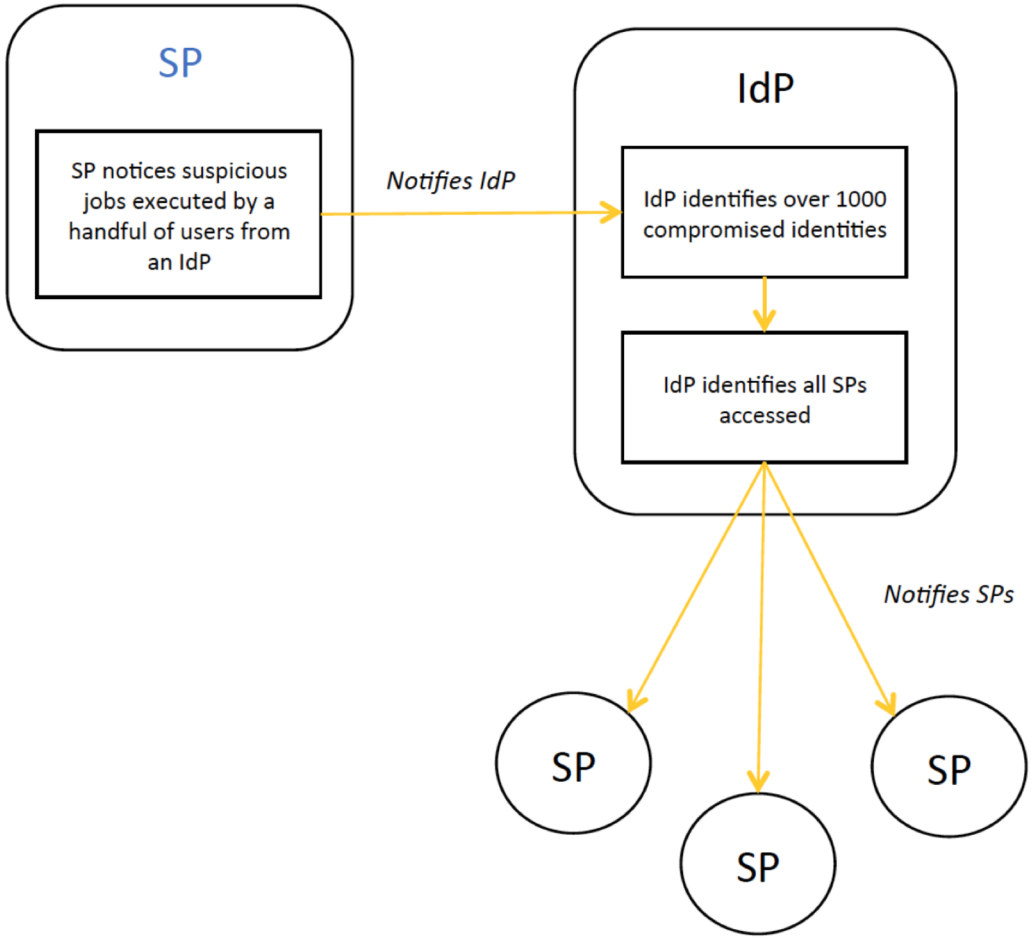
Why do we need Federated Security Incident Response

SUNET

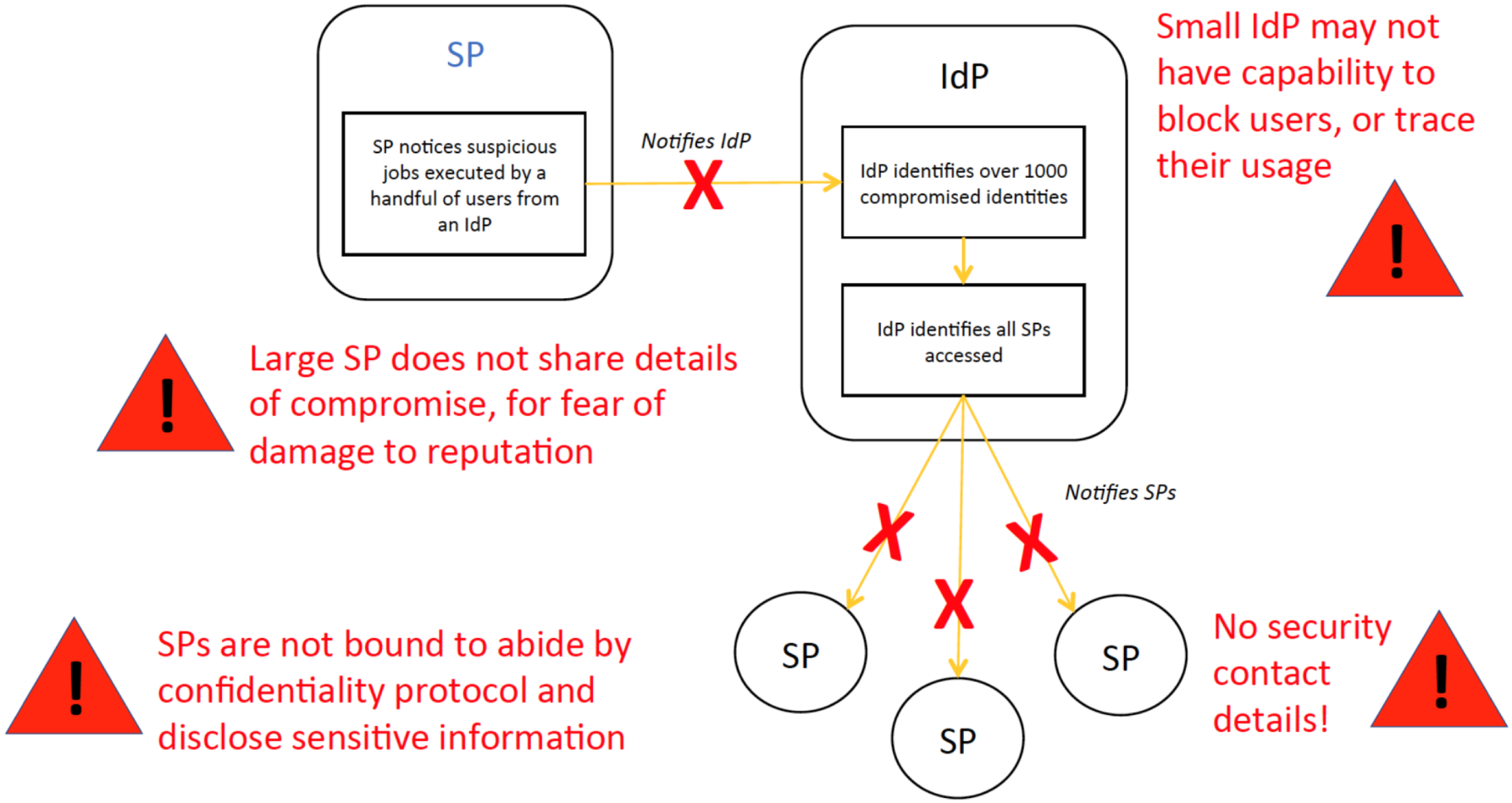
- Clearly an inviting vector of attack
- The lack of centralized support system for security incident response was identified risk to the success of eduGAIN
- Participant will need to collaborate during incident response



Common sense would imply…



But in practice…



REFEDS SIRTFI – Security Incident Response Trust Framework for Federated Identity

SUNET

- Aims to enable the coordination of incident response across federated organisations
- SIRTFI specifies a set of compliance rules for entities to be able to assert it

Operational Security

Security incident response capability exists with sufficient authority to mitigate, contain spread of, and remediate the effects of an incident

Incident Response

Assure confidentiality of information exchanged
Provide security incident response contacts
Guarantee a response during collaborations

Tracebility

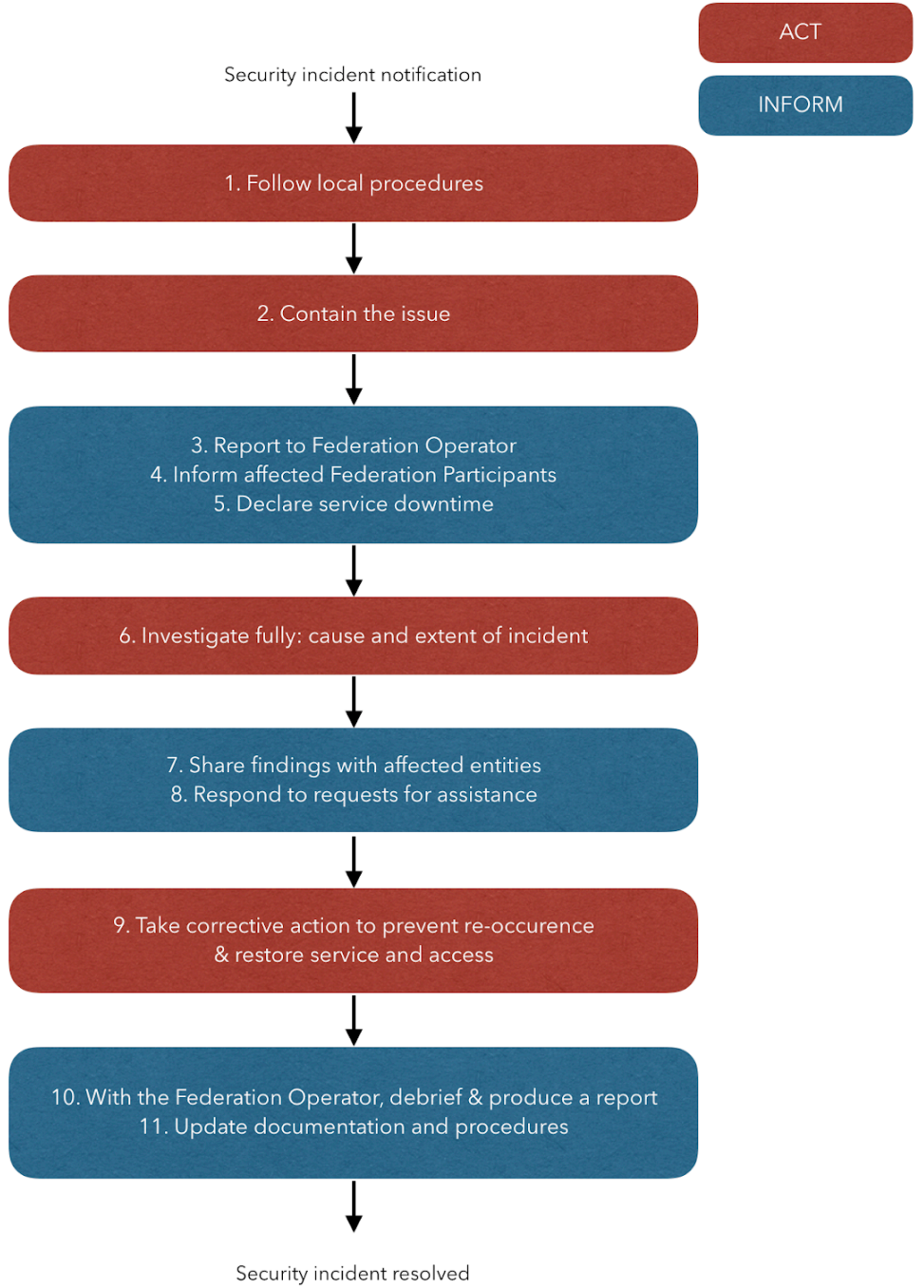
Improve usefulness of logs
Ensure logs are kept in accordance with policy

Participants Responsibilities

Confirm that end users are aware of an appropriate AUP

eduGAIN Incident Response Procedure

- Goes in hand with SIRTFI extending it by defining roles, responsibilities and processes for handling incidents
- Introduces eduGAIN security support as a central coordinating party
- Currently under consultation !



eduGAIN Baseline Expectations

SUNET

- To improve the interoperation among entities, the eduGAIN community is **currently working** in the definition of **Baseline Expectations for eduGAIN**, classifying them in groups targeting:
  - Identity Providers
  - Service Providers
  - Federation Operators
- Aim is to improve user experience, interoperability and quality of the eduGAIN Metadata

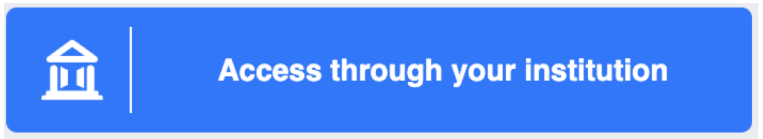
https://wiki.refeds.org/display/GROUPS/Baseline+Expectations+Working+Group

Seamless Access

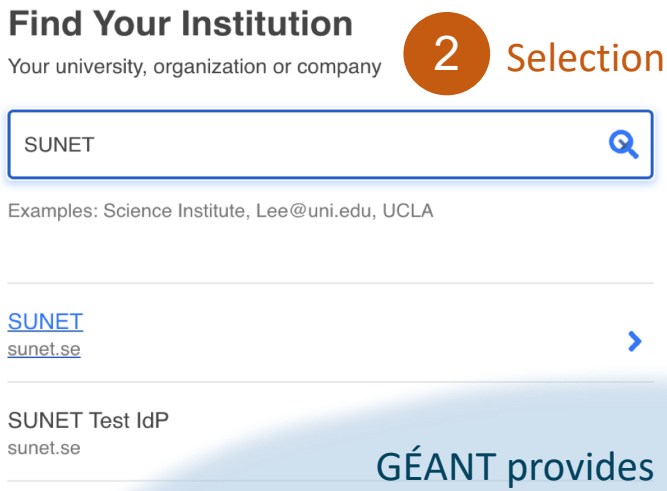
3600+ IdPs in eduGAIN

Challenge to properly implement IdP discovery

Many SPs, such as publishers, still rely on IP-based authorisation



1 SA Button



2 Selection of IdP

3 IdP Selection saved in SA button

UX experts proven design

Retains user's IdP choice and presents it next time

Privacy by design

Delivered via coalition: NISO, Internet2, GÉANT and STM

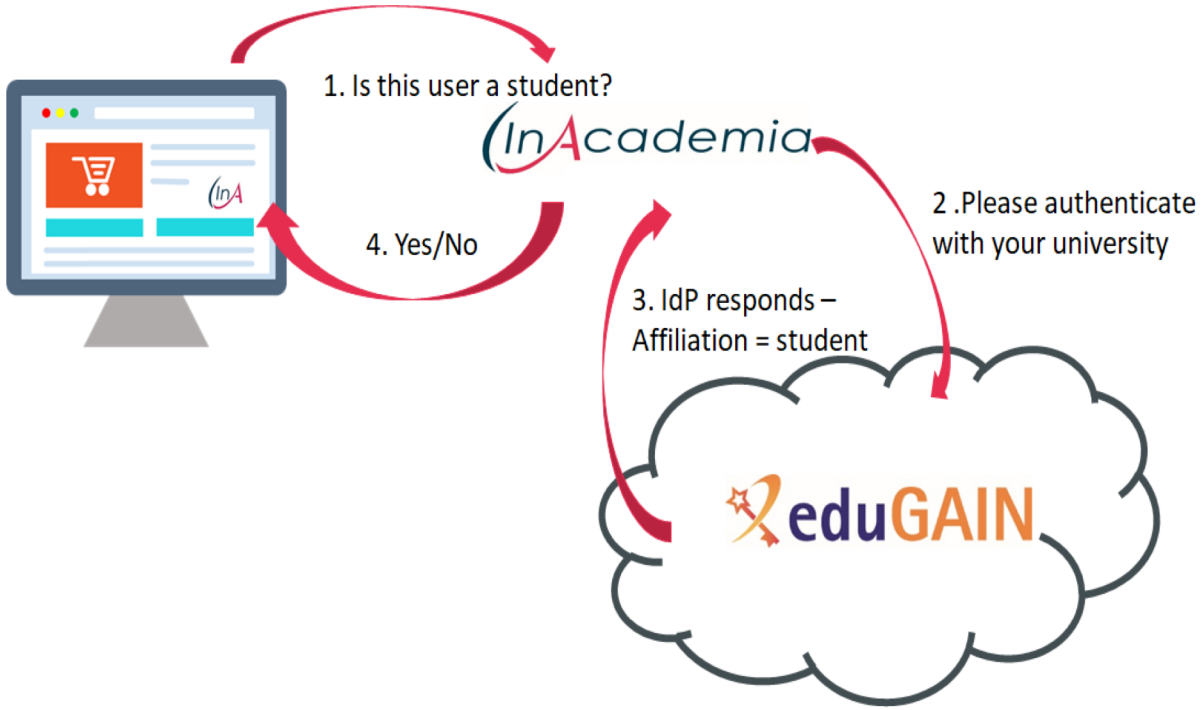
GÉANT provides beta service operations

Robust infrastructure for mission critical service

Beta service since July 2019

Delivered production grade service in P1

InAcademia



Reduces burden for IdPs and identity federations

Support and connect merchants

Lighter-weight option for service providers (SPs)

Quick, reliable and secure way to verify academic identities

Source of income for T&I

Designed to support Identity Federations and eduGAIN to achieve sustainability

Privacy by design to protect end users

Helps with GDPR compliance

SUNET

Thank you

Questions?

marina@sunet.se