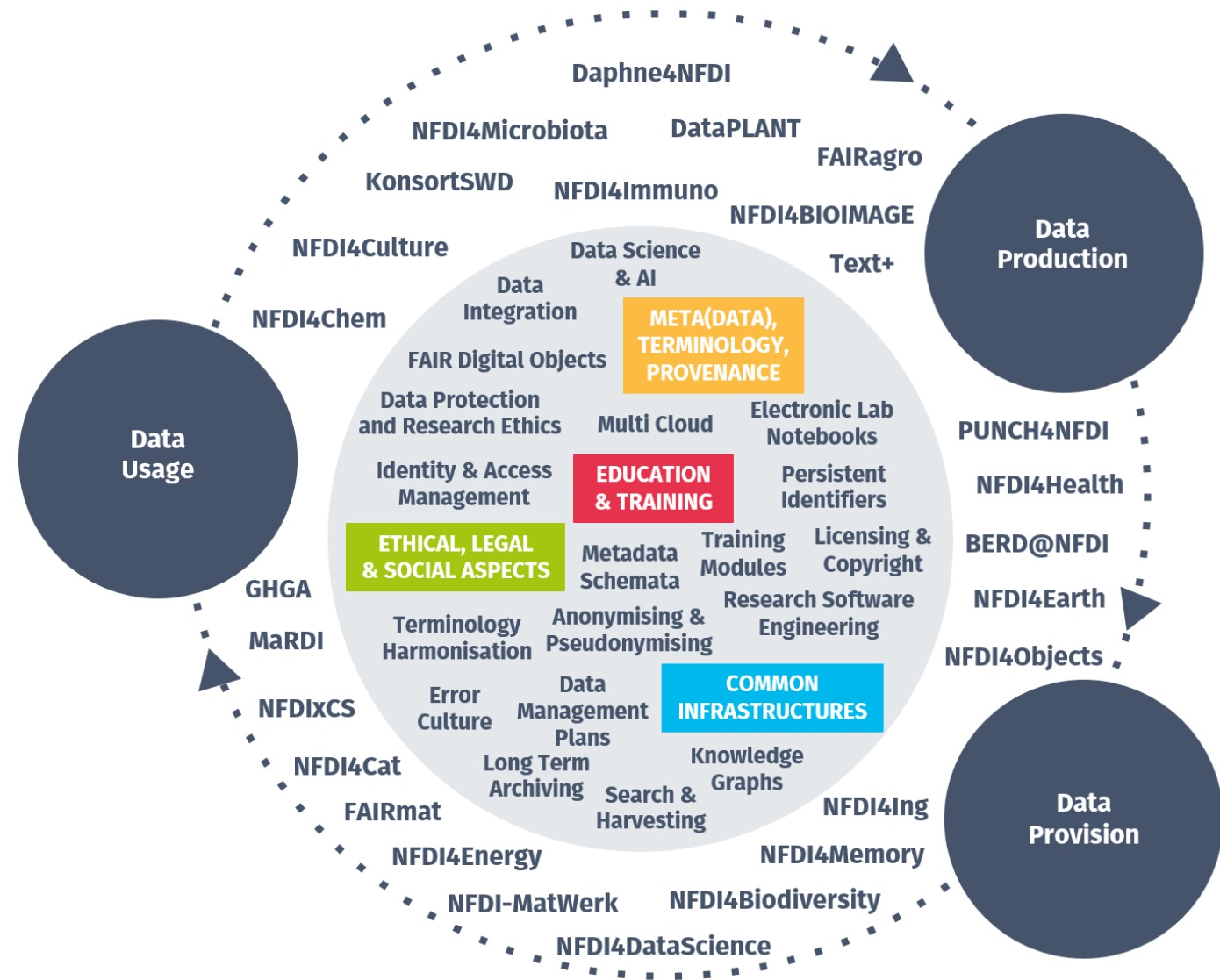


IAM4NFDI Infoshare Policy Framework 2023-10-12

Wolfgang Pempe (pempe@dfn.de)



Contents

- Overview
NFDI Policy Framework
- Proxies and Trust
- Snctfi + AARC PDK
- Data Protection
Code of Conduct
- Security and Incident
Response

IAM4nfdi

Identity and Access Management
for the German National Research
Data Infrastructure



NFDI-AAI Policy Framework

Overview

- <https://doc.nfdi-aai.de/documents/policies-v0.9/>
- Based on the Policy Framework of the Helmholtz AAI, successfully in use for 5 years
 - Based on the AARC Policy Development Kit and the Snctfi Framework
- Adapted, modernized and extended to meet the requirements of the NFDI-AAI
 - Attribute Profiles: Research & Scholarship -> Personalized Access Entity Category
 - Security: Sirtfi v1 -> Sirtfi v2
 - Data Protection: CoCo v1 -> CoCo v2

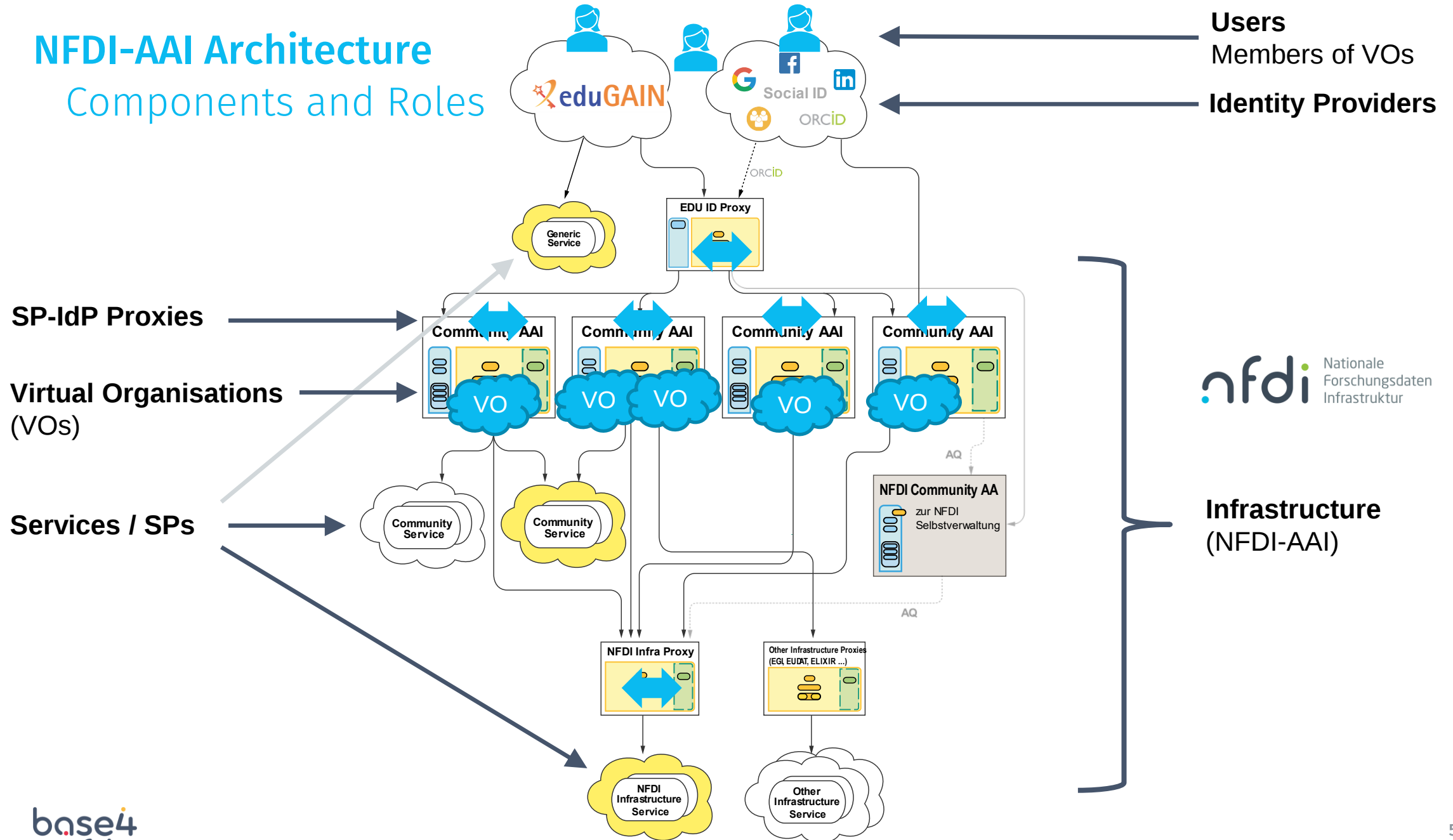
The Concept of Virtual Organisations

NFDI-AAI Top-Level Policy:

„A Virtual Organisation (VO) is a group of one or more Users, not necessarily bound to a single institution, **organised with a common purpose, jointly granted access to one or more Services**. In many cases, a Virtual Organisation **unites the users of a specific research community** represented by one or more of the NFDI consortia. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Virtual Organisation will not need to separately negotiate access with Service Providers. A User can be a member of multiple Virtual Organisations.”

NFDI-AAI Architecture

Components and Roles



NFDI-AAI Policy Documents

- Top Level Infrastructure Policy
- Virtual Organisation Membership Management Policy (VOMMP)
 - VO Lifecycle Management – *a checklist*
 - Service Access Policy Template (SAP) - *optional*
- Policy on the Processing of Personal Data (PPPD)
- Security Incident Response Procedure (SIRP)
- Infrastructure Attribute Profiles (IAP)
- Acceptable Use Policy Template (AUP) → Services (SAUP), VO (VO AUP)
- Privacy Policy Template → Services (SPP), VO (VO PP), SP-IdP Proxy (Proxy PP)
- (Template Records of Processing Activities/Verzeichnis der Verarbeitungstätigkeiten)

Top Level Infrastructure Policy

- „Mother“ Document
- Definition of key terms, concepts and responsibilities
 - Infrastructure, Virtual Organisation, Participant, ...
 - Technical components (Service Provider, Identity Provider, SP-IdP proxy, ...)
- Explanation of how the policy documents are related
- Reference to external but mandatory frameworks and standards in terms of trust, data protection and security
 - REFEDS Assurance Framework
 - Data Protection Code of Conduct
 - Sirtfi (Security Incident Response Trust Framework for Federated Identity)

Virtual Organisation Membership Management Policy

- Establish trust between VO and Infrastructure and other VOs
- Binding rules for managing a VO within the NFDI
- Roles and Responsibilities
- Supplementary Documents / Templates
 - VO Lifecycle Management – *a checklist*
 - Service Access Policy Template (SAP) - *optional*
for Services with special requirements towards a VO, e.g. in terms of user management or attributes

SIRP, PPPD and IAP

- Security Incident Response Policy (SIRP)
 - Best Practices with reference to Sirtfi
- Policy on Processing of Personal Data (PPPD)
 - GDPR-based list of principles of processing of personal data
 - Reference to REFEDS Code of Conduct for Service Providers
- Infrastructure Attribute Profiles (IAP)
 - Mandatory attribute profiles for the NFDI-AAI

NFDI-AAI Policy Documents

complies with policy

defines policy

	Infrastructure Management	Infrastructure Security Contact	VO Management	Service Provider	SP-IdP Proxy	Identity Provider	User
Infrastructure Management	Top Level Infrastructure Policy						
		SIRP					
			PPPD				
				IAP			
			VOMMP				
VO Management			VO PP				VO AUP
SP-IdP Proxy					Proxy PP		
Service Provider			SAP	SPP	SAP		SAUP

Roles

Infrastructure

- Management
- Security Contact
- Virtual Organisation Supervisor (e.g. approval of VOs)

Virtual Organisation

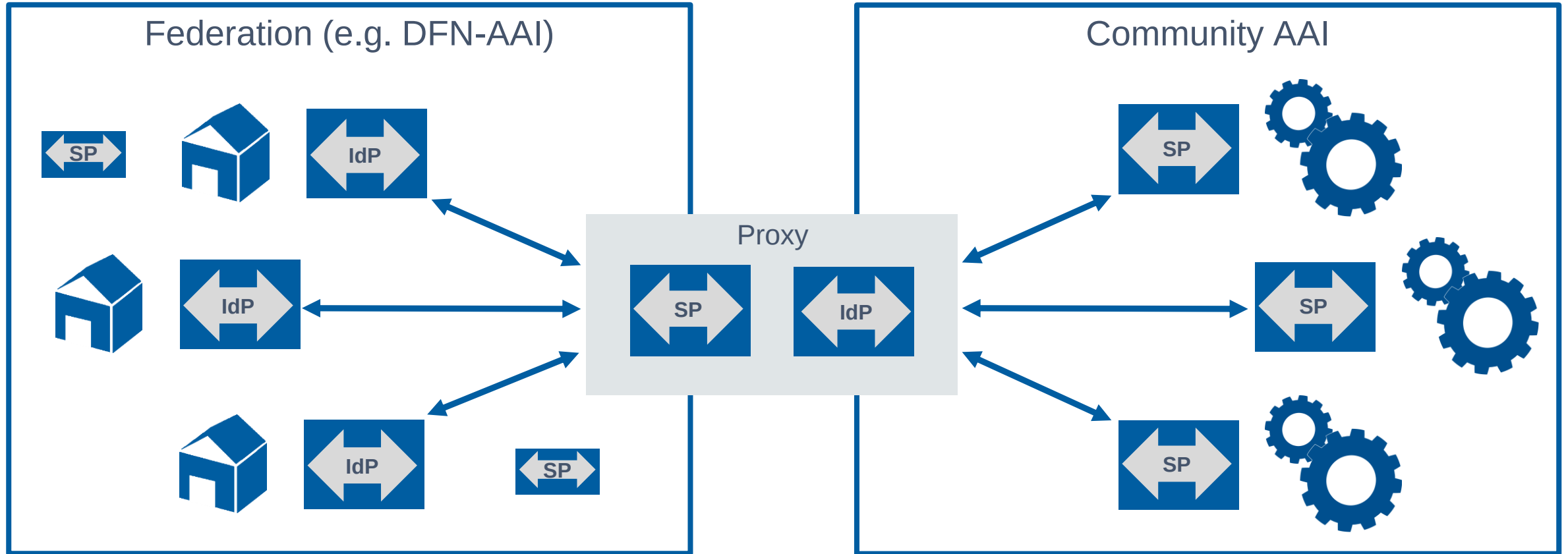
- Management
- Security Contact
- Data Protection Contact
- User

Service

- Security Contact
- Data Protection Contact

Proxies and Trust

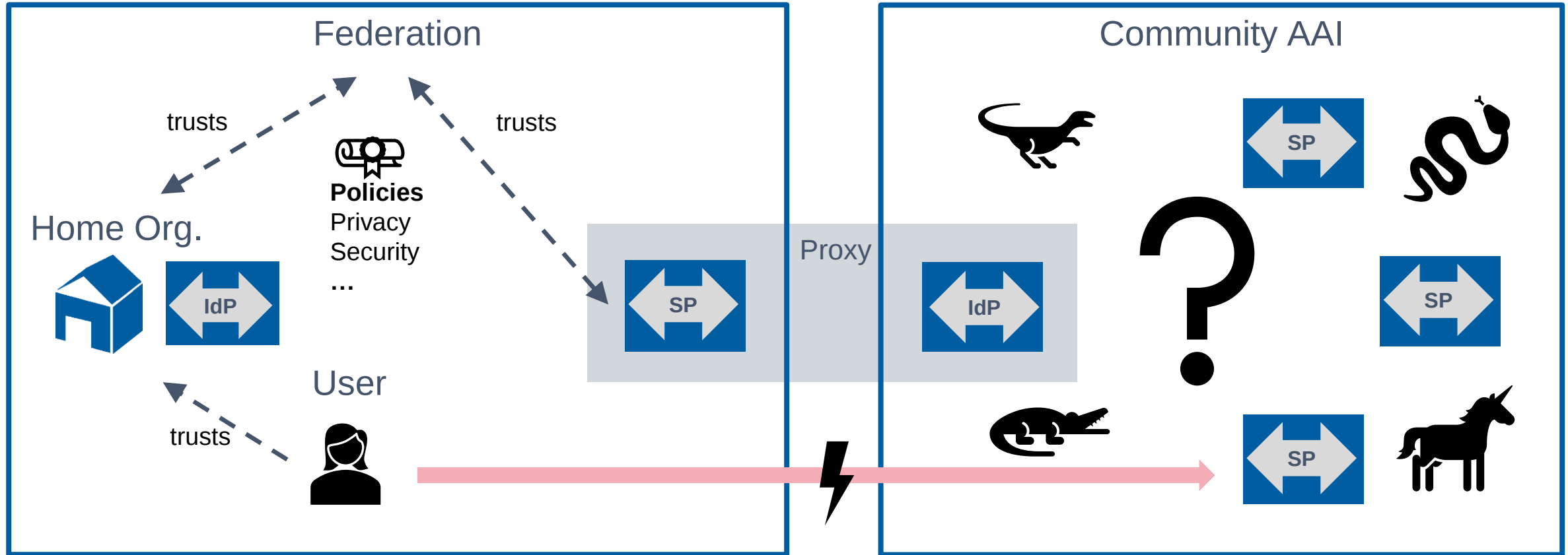
The Technical View



Proxies and Trust

Trust – the Federation's Perspective

A Federation is a framework of mutual trust – but what's behind the SP part of the Proxy?

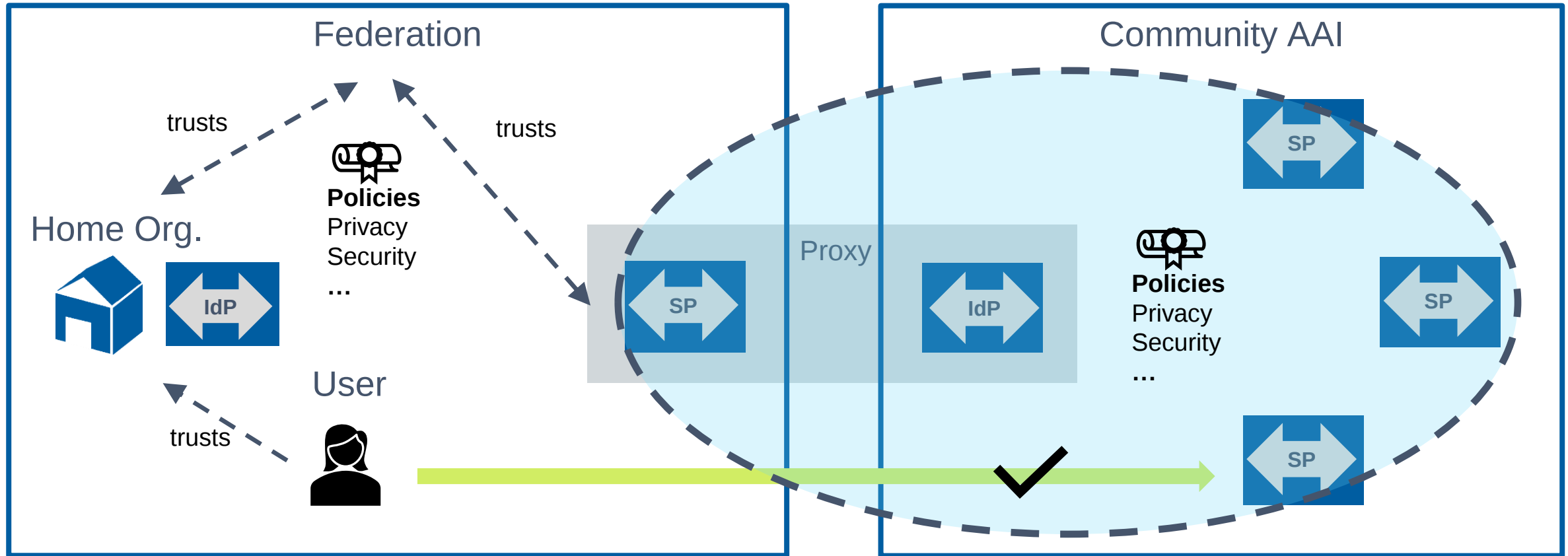


The user usually doesn't know about the SP part of the proxy, but wants to access a Service *behind* the proxy

Proxies and Trust

Trust – the Federation's Perspective

We need a **Trust Framework** where all services abide by the same policies as the Proxy SP



Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures



- Built on the structures of the Security for Collaboration among Infrastructures (SCI) framework -> EGI, EUDAT, WLCG, PRACE, XSEDE ...
- Compliant infrastructures commit themselves to **an internally consistent policy set** covering critical areas of best practice such as the **protection of personal data** (-> PPPD) and **security incident handling** (-> SIRP) capabilities. As for NFDI-AAI:
 - REFEDS Code of Conduct for Service Providers (CoCo v2)
 - Security Incident Response Trust Framework for Federated Identity (Sirtfi)
- Part of the **AARC Policy Development Kit** (next slide)



- A set of policy documents (sample texts, templates) to **facilitate trust** between users, resource providers, and infrastructures (ideally including identities and IdPs)
- Outline the **operational measures** undertaken by an infrastructure to properly provide services
- Policies basically cover **security** measures, **data protection** and **user management**
- **User management** brings in further aspect:
 - **Virtual Organisation:** rights and roles for users committed to domain-specific research
-> Access management for community-specific resources and services
 - **Identity Assurance:** REFEDS Assurance Framework

Data Protection Code of Conduct for Service Providers (CoCo)

- Version 1 (2013): GÉANT Code of Conduct for Service Providers in in EU/EEA
 - Based on the EU Data Protection Directive (95/46/EC)
- Version 2 (2022): REFEDS Data Protection Code of Conduct
 - Based on the GDPR
- Commitment of Service Providers to European data protection jurisdiction
 - Indicated via an Entity Category / Trust Mark in Federation Metadata
- Trust-building measure designed to encourage Home Organisations / IdP Operators to release required attributes to Service Providers

CoCo v2: Best Practices

Principles of the Processing of Attributes

- Legal compliance
- Purpose Limitation
- Data Minimisation
- Information Duty Towards End Users
- Information Duty Towards Home Organisation
- Data Retention
- Security Measures
- ... and more

<https://refeds.org/wp-content/uploads/2022/05/REFEDS-CoCo-Best-Practicev2.pdf>

Policies – Next Steps

- Current versions (0.9) of the Policy documents are available online
- Consultation with Base4NFDI about process for approval of policy docs
- Develop and establish a sustainable governance structure (together with Base4NFDI and the Directorate)
 - Who takes over which role? *OK, 'user' is simple...*
 - Who decides who takes over which role?
 - Best Practices for operating Virtual Organisations
 - Concepts for rights and role management - Interoperability?

REFERENCES

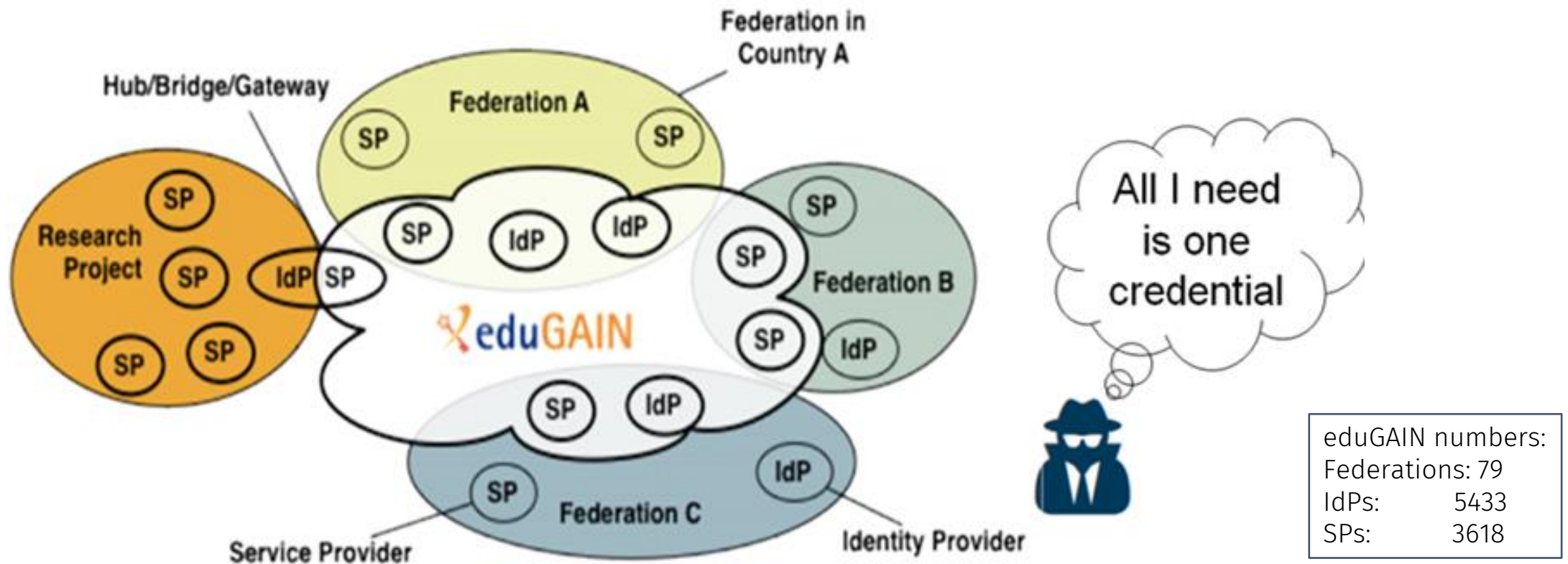
- AARC Policy Development Kit
<https://aarc-community.org/policies/policy-development-kit/>
- NFDI-AAI Policy Framework - <https://doc.nfdi-aai.de/policies/>
- REFEDS Assurance Framework (RAF) - <https://refeds.org/assurance>
- REFEDS Code of Conduct for Service Providers (CoCo v2) -
<https://refeds.org/category/code-of-conduct>
- Snctfi - Scalable Negotiator for a Community Trust Framework in Federated Infrastructures - <https://aarc-community.org/policies/snctfi/>

Security & Incident Response

- Dangers of Identity Theft in Federated Contexts
- Sirtfi Framework
- NFDI and Sirtfi

What if...

... an incident spread throughout the federated Research & Education community via a single compromised identity?



Picture/ideas courtesy of Ann Harding (SWITCH), Hannah Short (CERN)

What if...

- An incident with one compromised user account has the potential to cause damage to thousands of services
- What to do?
 - **Identify** - develop an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities
 - **Protect** - ability to limit or contain the impact of a potential cybersecurity event
 - **Detect** - timely discovery of cybersecurity events
 - **Respond** - contain the impact of a potential cybersecurity incident
 - **Recover** - timely recovery to normal operations to reduce the impact from an incident

<https://www.nist.gov/cyberframework/online-learning/five-functions>

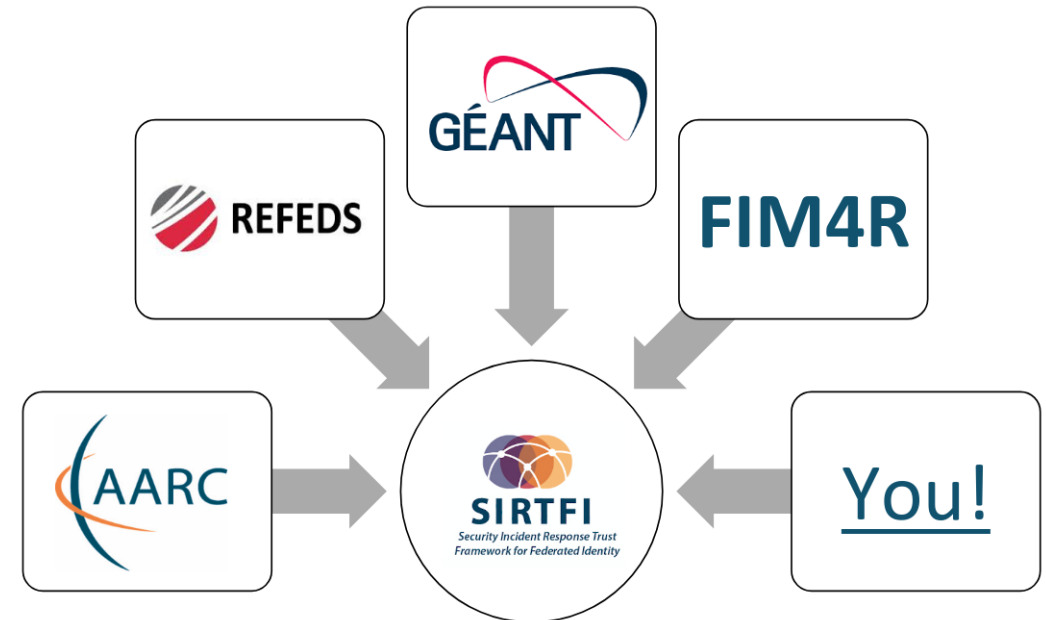
Respond...

Incident Response is the way...

... to contain the impact of an incident in a federated environment:

Sirtfi - Security Incident Response Trust Framework for Federated Identity

- Driven by research communities
- Developed in AARC project (2015)
- Specifications (v1 + v2) hosted by REFEDS
- Supported by GÉANT (make eduGAIN a safe place)
- First implemented by CERN: Only Sirtfi-compliant IdPs allowed to access CERN resources



Credit: Hannah Short, CERN

Srtfi - Components in a Nutshell

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 security contacts
- Guarantee a response during collaboration

Traceability

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

Participant Responsibilities | User Rules and Conditions

- Confirm that end users are aware of an appropriate AUP

Sirtfi - Practicalities in a Nutshell

Apply basic operational security protections to your federated entities in line with your organisation's policies and priorities



Patch, manage vulnerabilities, detect intrusions, manage access, log events

Be willing to collaborate in responding to a federated security incident *and notify others when you realise that an incident impacts them*



Respect user privacy and use the Traffic Light Protocol (TLP) with other Sirtfi participants

Publish security contact and apply for the Sirtfi Entity Category so that others will know to trust this about you

```
<EntityDescriptor  
  ...  
  Sirtfi EC  
  ...  
  security contact  
  ...  
</EntityDescriptor>
```

Coordinate with your Federation Operator to publish in federation metadata

Credit: Tom Barton, Internet2

Sirtfi and NFDI-AAI

- Sirtfi is anchored in the NFDI-AAI Policy Framework:
 - Security Incident Response Procedure (SIRP) + others
 - Please note: security@nfdi.de doesn't work yet! Use security@aai.dfn.de instead
- Supporting Sirtfi is mandatory for all participants/roles
 - Infrastructure (Security Contact takes over the coordination)
 - Virtual Organisations
 - Identity and Service Providers, SP-IdP Proxies
- Security Contacts play a crucial role
 - **Never appoint a single person as Security Contact!**

BTW: Entities participating in DFN-AAI and eduGAIN are entitled to get support by the DFN-CERT Incident Response Team and the eduGAIN Security Team. Cf. <https://doku.tid.dfn.de/de:aai:incidentresponse>

References

- Overview and Best Practices - <https://doku.tid.dfn.de/de:aai:incidentresponse>
- AARC Deliverable I051: Guide to Federated Security Incident Response for Research Collaboration - <https://wiki.geant.org/display/AARC/Generic+Security+Incident+Response+Procedure>
- Sirtfi v1 & v2 Specifications - <https://refeds.org/sirtfi>
- Traffic Light Protocol - <https://www.first.org/tlp/>
- New Service DFN.Security: Advertising on our (DFN) own behalf - <https://www.dfn.de/dfn-security-aktuell/>

Thanks for your attention!

Questions?

Contact: aai-kernteam@lists.kit.edu

