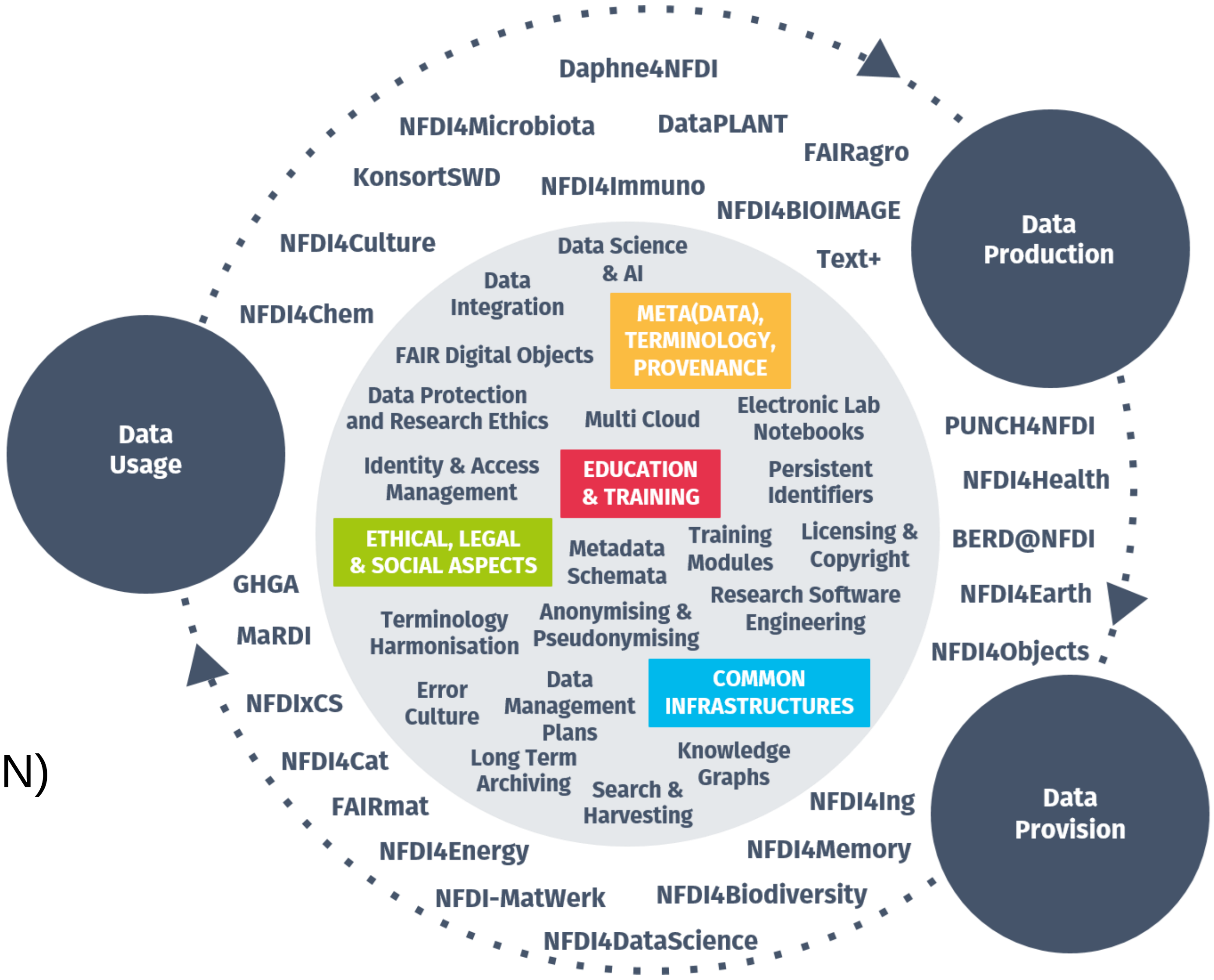
Basic Services for NFDI

IAM4NFDI
Policy Framework

Marcus Hardt (KIT), Wolfgang Pempe (DFN)



Data Production

Data Provision

Data Usage

Daphne4NFDI
NFDI4Microbiota
DataPLANT
FAIRagro
KonsortSWD
NFDI4Immuno
NFDI4BIOIMAGE
NFDI4Culture
Text+
NFDI4Chem
PUNCH4NFDI
NFDI4Health
BERD@NFDI
NFDI4Earth
NFDI4Objects
GHGA
MaRDI
NFDIxCS
NFDI4Cat
FAIRmat
NFDI4Energy
NFDI-MatWerk
NFDI4DataScience
NFDI4Biodiversity
NFDI4Memory
NFDI4Ing

Data Science & AI
Data Integration
META(DATA), TERMINOLOGY, PROVENANCE
FAIR Digital Objects
Data Protection and Research Ethics
Multi Cloud
Electronic Lab Notebooks
Identity & Access Management
EDUCATION & TRAINING
Persistent Identifiers
ETHICAL, LEGAL & SOCIAL ASPECTS
Metadata Schemata
Training Modules
Licensing & Copyright
Research Software Engineering
Terminology Harmonisation
Anonymising & Pseudonymising
Error Culture
Data Management Plans
COMMON INFRASTRUCTURES
Long Term Archiving
Search & Harvesting
Knowledge Graphs

Funded by **DFG** as part of **NFDI**.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

Contents

- Overview
  NFDI Policy Framework
- Virtual Organisations
- Data Protection
- Incident Response
- ... and the rest

IAM4nfdi

Identity and Access Management for the German National Research Data Infrastructure

NFDI-AAI Policy Framework
Overview

- https://doc.nfdi-aai.de/policies/
- 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
  - Interoperable with international research infrastructures

NFDI-AAI Architecture

Components and Roles

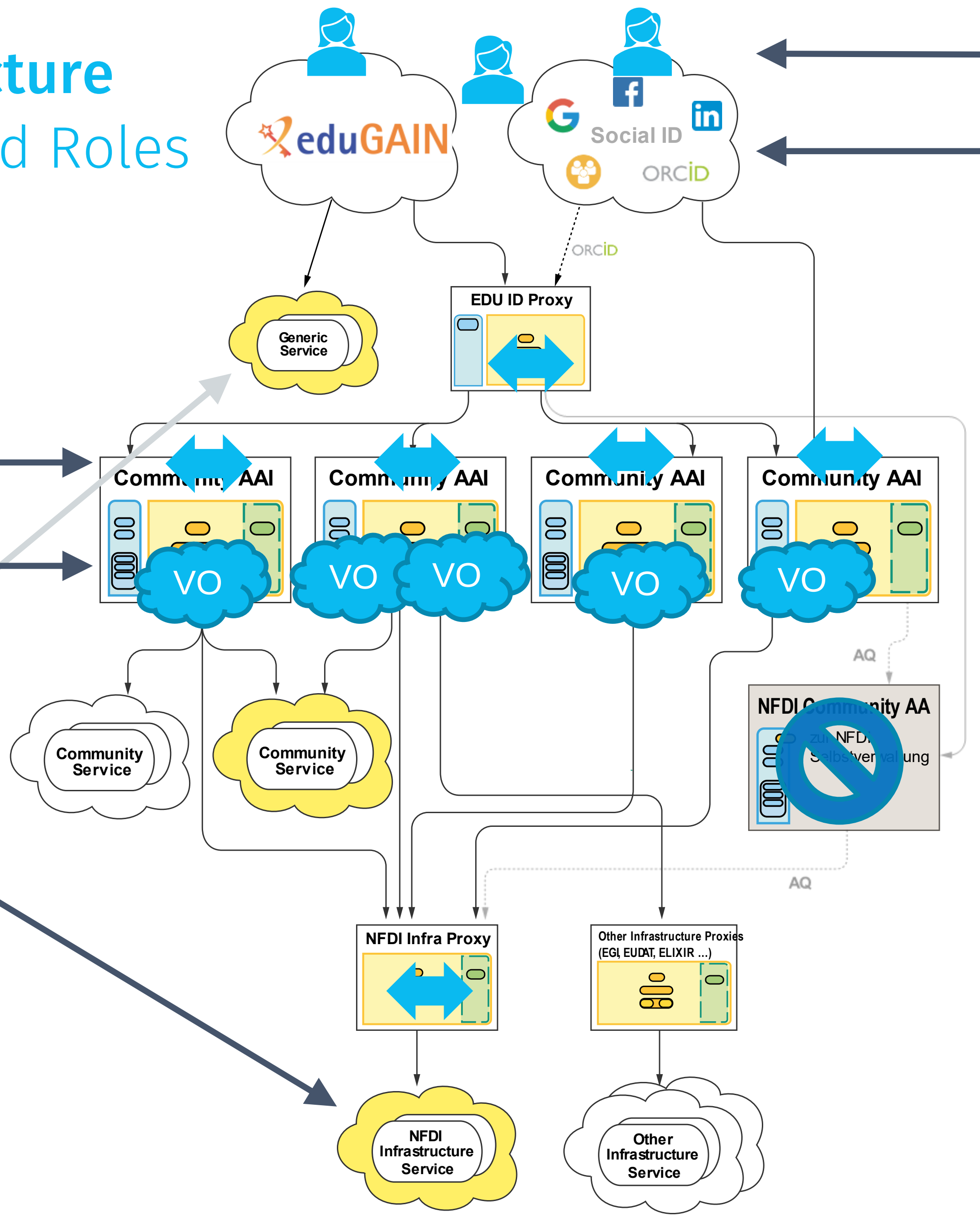
Users
Members of VOs

Identity Providers

SP-IdP Proxies

Virtual Organisations
(VOs)

Services / SPs



Nationale
Forschungsdaten
Infrastruktur

Infrastructure
(NFDI-AAI)

NFDI-AAI Policy Documents

NFDI-AAI

- Top Level Infrastructure Policy
    - Infrastructure Attribute Profiles (IAP)
    - Policy on the Processing of Personal Data (PPPD)
    - Security Incident Response Procedure (SIRP)

Community AAI

- Community Acceptable Use Policy Template (CAAI-AUP)

Virtual Organisation

- Virtual Organisation Membership Management Policy (VOMMP)
- VO Lifecycle Management – a checklist
- VO Acceptable Use Policy Template (VO-AUP) - optional

NFDI-AAI Policy Documents

Services

- Service Access Policy Template (SAP) - optional
- Service Acceptable Use Policy Template (SAUP) - optional

Data Protection

- Privacy Statement Template
  - Services (SPP)
  - SP-IdP Proxy (Proxy PP)
  - VO (VO PP)
- Template for 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, …)
  - Governance: *Infrastructure Management* -> appoints *Infrastructure Security Contact*
- 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 -> GDPR
  - Sirtfi (Security Incident Response Trust Framework for Federated Identity)

Virtual Organisation Membership Management Policy (VOMMP)

- Establish trust between VO and Infrastructure (NFDI-AAI) 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

Acceptable Use Policies (AUP)

- AUP can be defined by every single service in the infrastructure
  - This is difficult for users to digest
- WISE have distilled the so-called Baseline AUP, most commonly used on **existing, global** infrastructures -> Basis for the NFDI-AAI (and Helmholtz) AUP templates
  - Community AAI AUP
- Available as a template / default
  - Can **optionally** be modified if needed (not recommended)
    - By a VO
    - By a Service
- Usually, only contact details, names and dates need to be added to the template(s)

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 the current version of the REFEDS Code of Conduct for Service Providers
- Infrastructure Attribute Profiles (IAP)
  - Mandatory attribute profiles for the NFDI-AAI

Technical filters exist to express and check compliance with these Frameworks

Privacy Policies
(VO PP, Proxy PP, SPP)

- Required by law (GDPR)
- Each service MUST specify
  - A set of responsible people and contacts (data controller and – if applicable - data processors)
  - The set of processed and stored data
- A template exists
  - To make it easier to have a compliant policy
- Pain point?
  - Each and every service **must do it by themselves**
  - Otherwise **can not** be part of NFDI

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			🟦 CAAI AUP
			🟦 VOMMP				
VO Management			🟨 VO PP				🟪 VO AUP
SP-IdP Proxy (CAAI)					🟨 Proxy PP		
Service Provider			🟩 SAP	🟨 **SPP**	🟩 SAP		🟩 SAUP

Key:

🟦 Existing Policy (Modifications are **not** encouraged)
🟩 Optional Policy (Template available)
🟪 Existing Policy (Few Modifications necessary)
🟨 Required Policy (Template available)

Policies – Next Steps

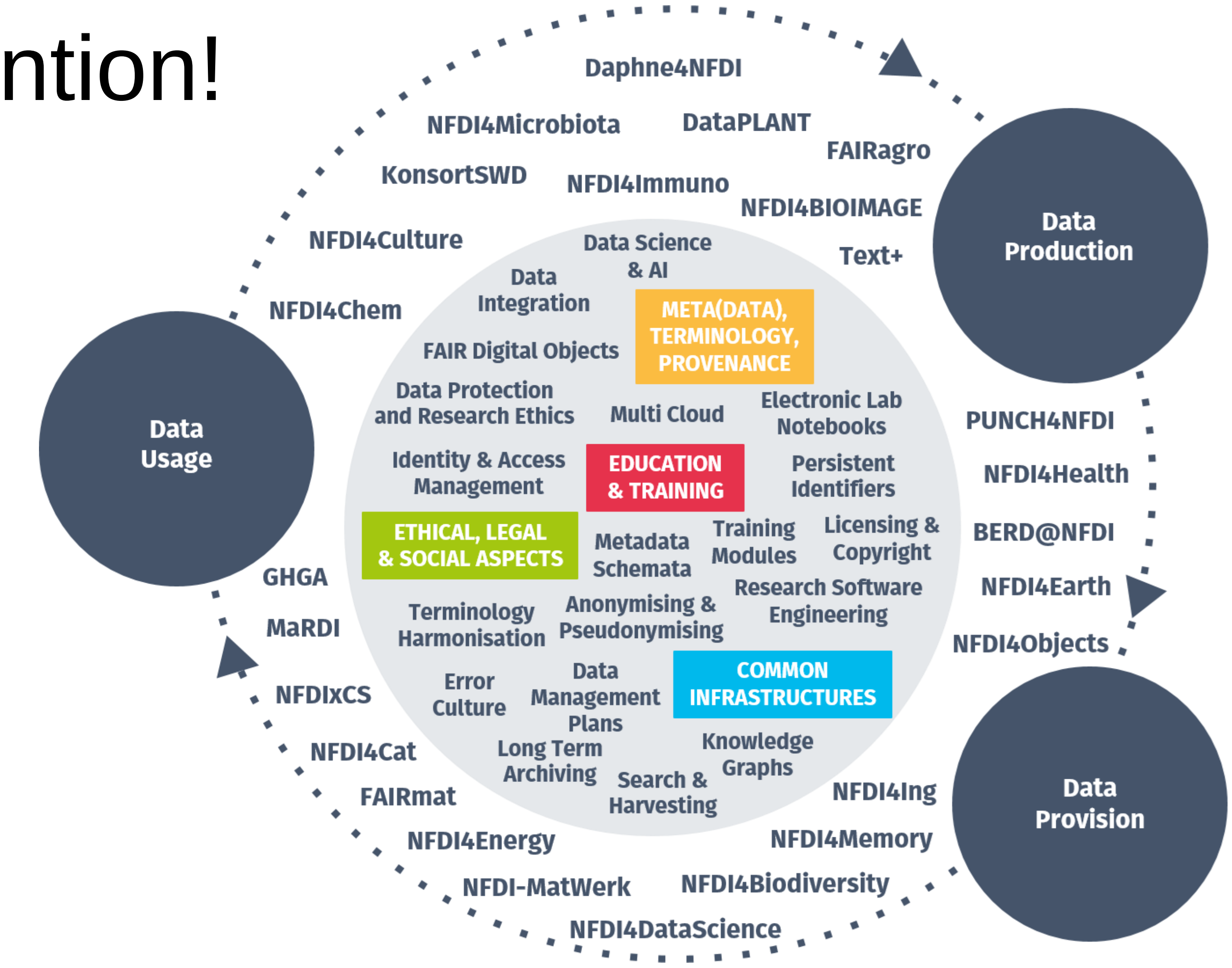
- Current versions (0.9.x) of the policy documents are available online
- Consultation with Base4NFDI about process for approval of future versions of policy docs -> will be based on the consultation procedures of the REFEDS community
- Develop and establish a sustainable governance structure (together with Base4NFDI and the Directorate)
  - Who takes over which role? *e.g. who will represent the (top-level) Infrastructure?*
  - Who decides who takes over which role?
  - Best Practices for operating Virtual Organisations

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 Personalized Access Entity Category - https://refeds.org/category/personalized
- 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/
- WISE Baseline AUP and Conditions of Use - https://wise-community.org/wise-baseline-aup/

Thanks for your attention!

Questions?



Contact: aai-kernteam@lists.kit.edu

base4 nfdi

Funded by **DFG** as part of **NFDI**.

Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

Backup slides

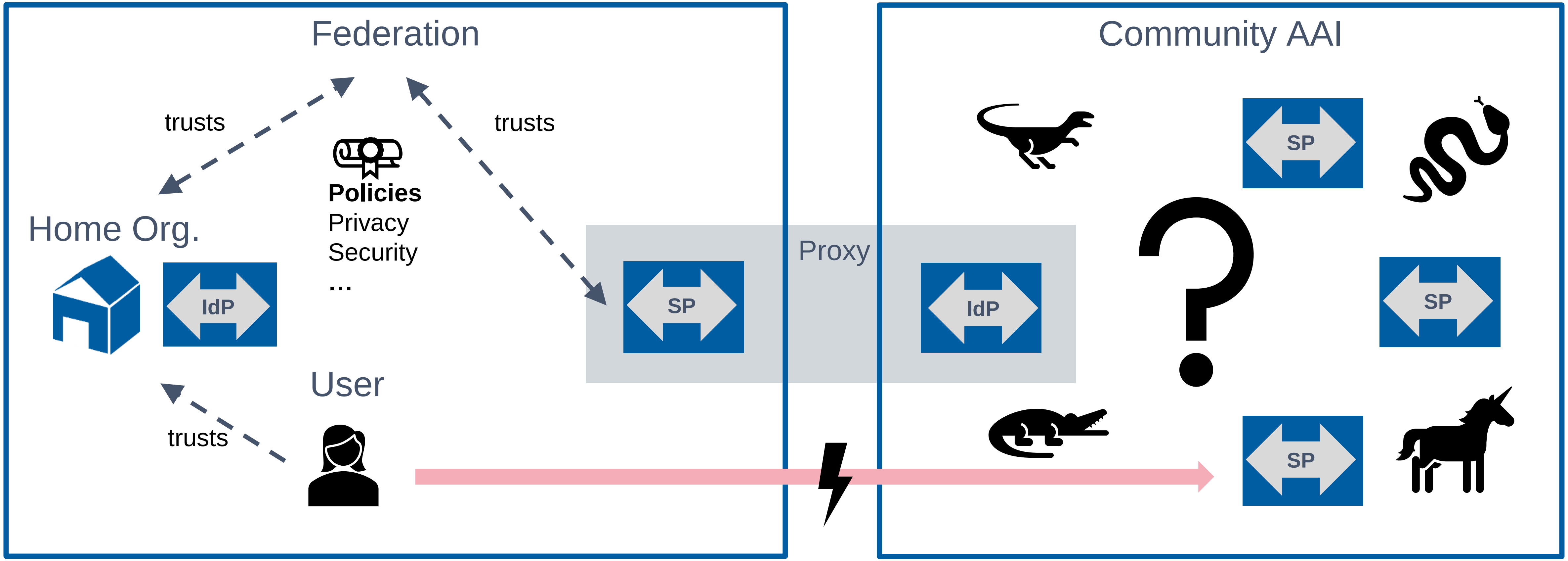
AARC Policy Development KIT

- 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

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?

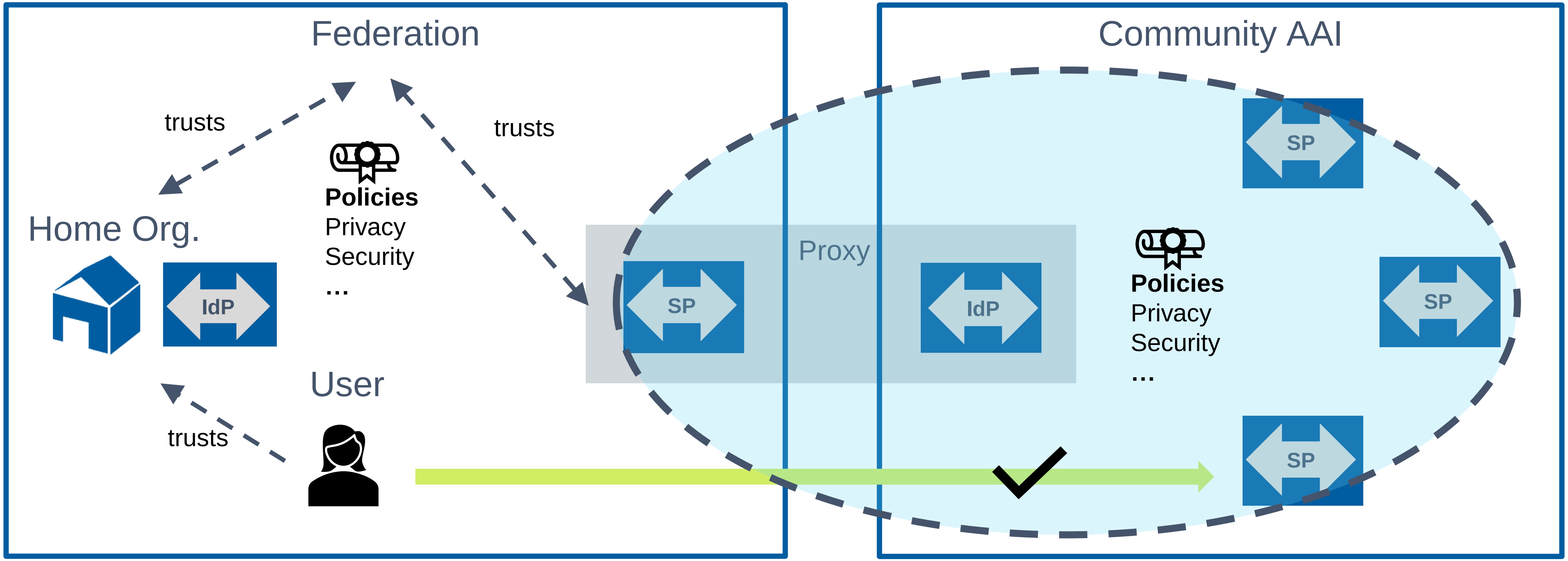


The user usually doesn‘t know about the SP part of the proxy, but wants to access a Service *behind* the proxy

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)

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

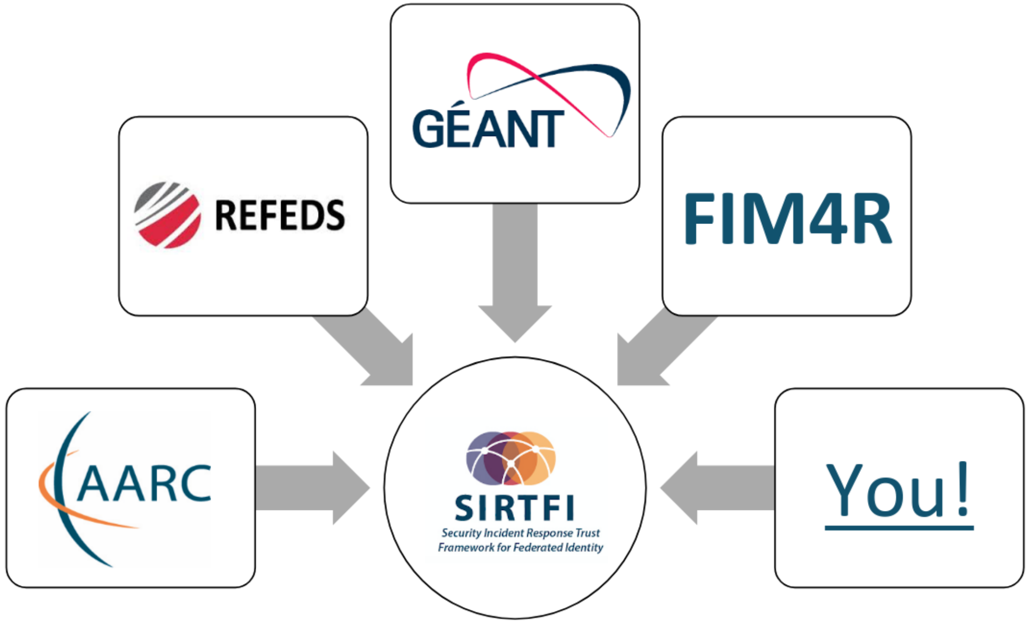
Incident Response

The Sirtfi Framework

SIRTFI
Security Incident Response Trust
Framework for Federated Identity

Sirtfi - Security Incident Response Trust Framework for Federated Identity

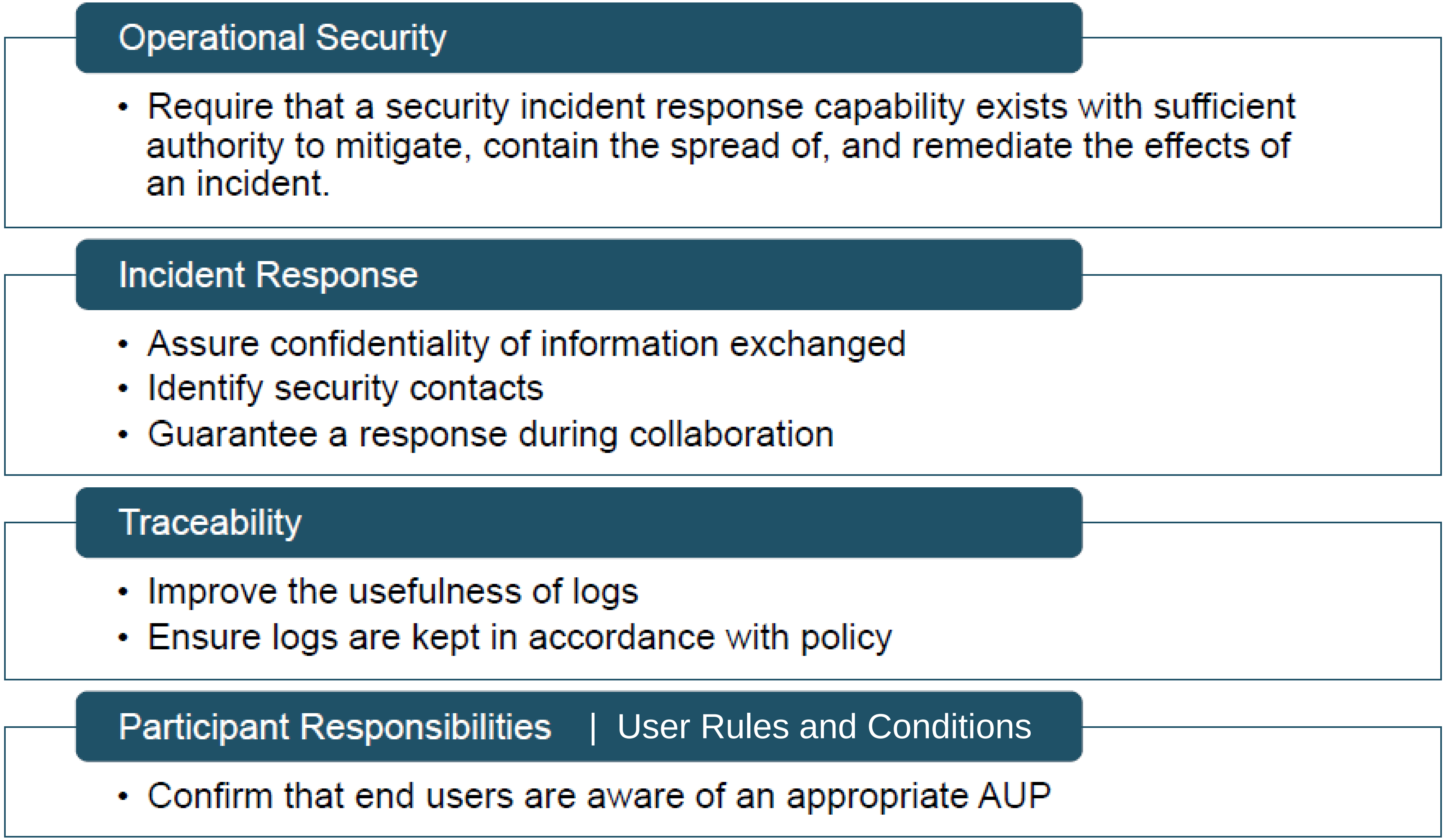
- Driven by research communities
- Developed in AARC project (2015)
- Specifications (v1 + v2) hosted by REFEDS
- Supported by GÉANT
  (make eduGAIN a safe place)
- First implemented by CERN:
  Only Sirfti-compliant IdPs allowed
  to access CERN resources


GÉANT
REFEDS
FIM4R
AARC
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
You!

Credit: Hannah Short, CERN

cf. also https://doku.tid.dfn.de/de:aai:incidentresponse

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

Credit: Hannah Short, CERN

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