GÉANT
Networks • Services • People

Trust & Identity services: eduroam, Identity Federations and eduGAIN

V2.0

Mario Reale
GÉANT
RESEARCH ENGAGEMENT AND SUPPORT TEAM

Diginar-2: Progress and Challenges In Introducing Eduroam and Federated Identity
under Asi@Connect/Geant
December 18, 2019

www.geant.org

Agenda

- GÉANT and the GÉANT Network
- GÉANT Trust and Identity Services
  - 1. Identity Federations and eduGAIN
  - 2. eduroam

Provides an open, innovative and trusted information infrastructure for the European knowledge economy and to the benefit of society worldwide

GÉANT
Networks • Services • People

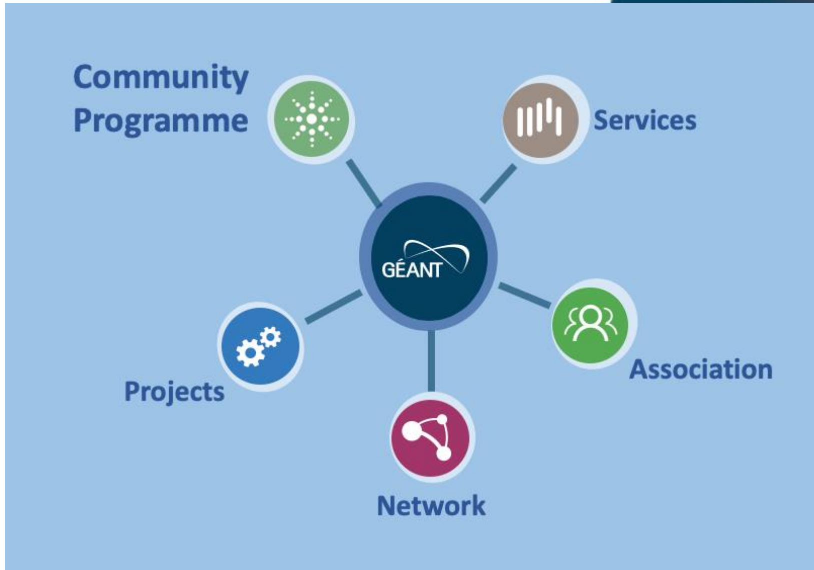
A membership Association for Europe's National Research & Education Networks (NRENs)
GÉANT Association

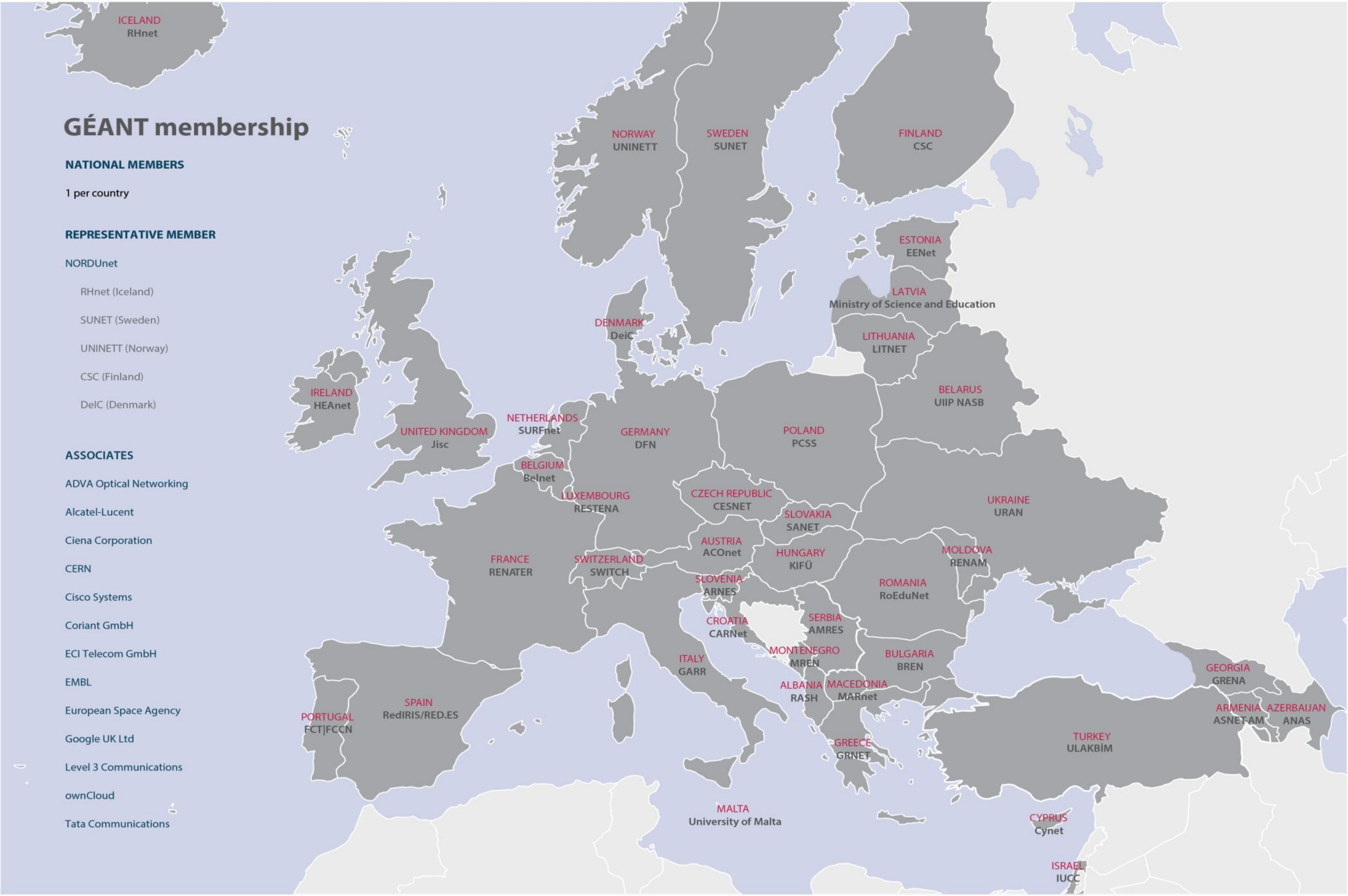
Coordinates and participates in EC-funded projects
Under Horizon 2020 the financial instrument for implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness

Operates a pan-European e-infrastructure with connections to all regions of the world
GÉANT network

Manages a portfolio of services for research & education
EduX

Organises and runs community events & working groups
TNC, task forces & special interest groups





GÉANT membership

NATIONAL MEMBERS

1 per country

REPRESENTATIVE MEMBER

NORDUnet

- RHnet (Iceland)
- SUNET (Sweden)
- UNINETT (Norway)
- CSC (Finland)
- DeIC (Denmark)

ASSOCIATES

ADVA Optical Networking

Alcatel-Lucent

Ciena Corporation

CERN

Cisco Systems

Coriant GmbH

ECI Telecom GmbH

EMBL

European Space Agency

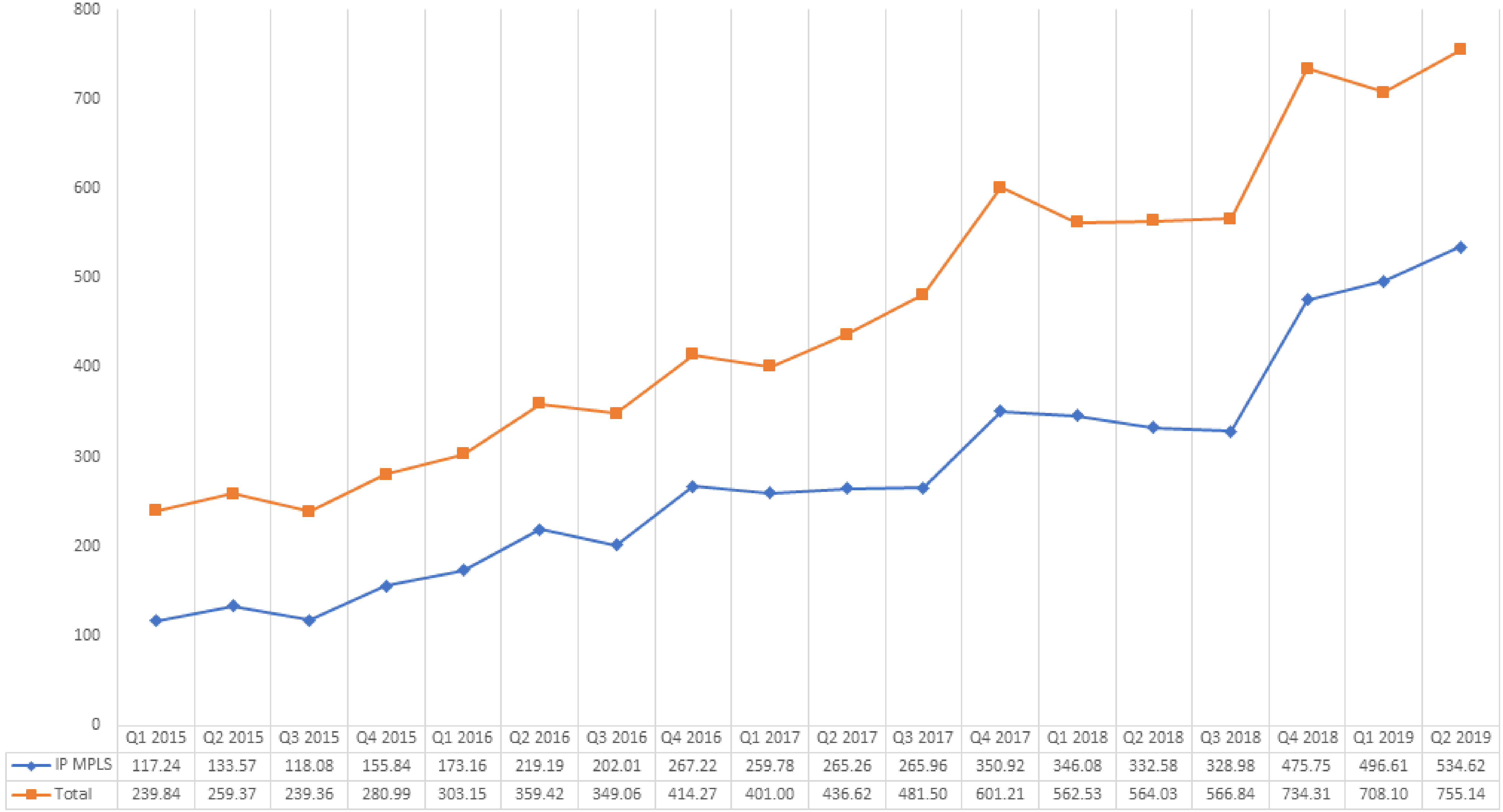
Google UK Ltd

Level 3 Communications

ownCloud

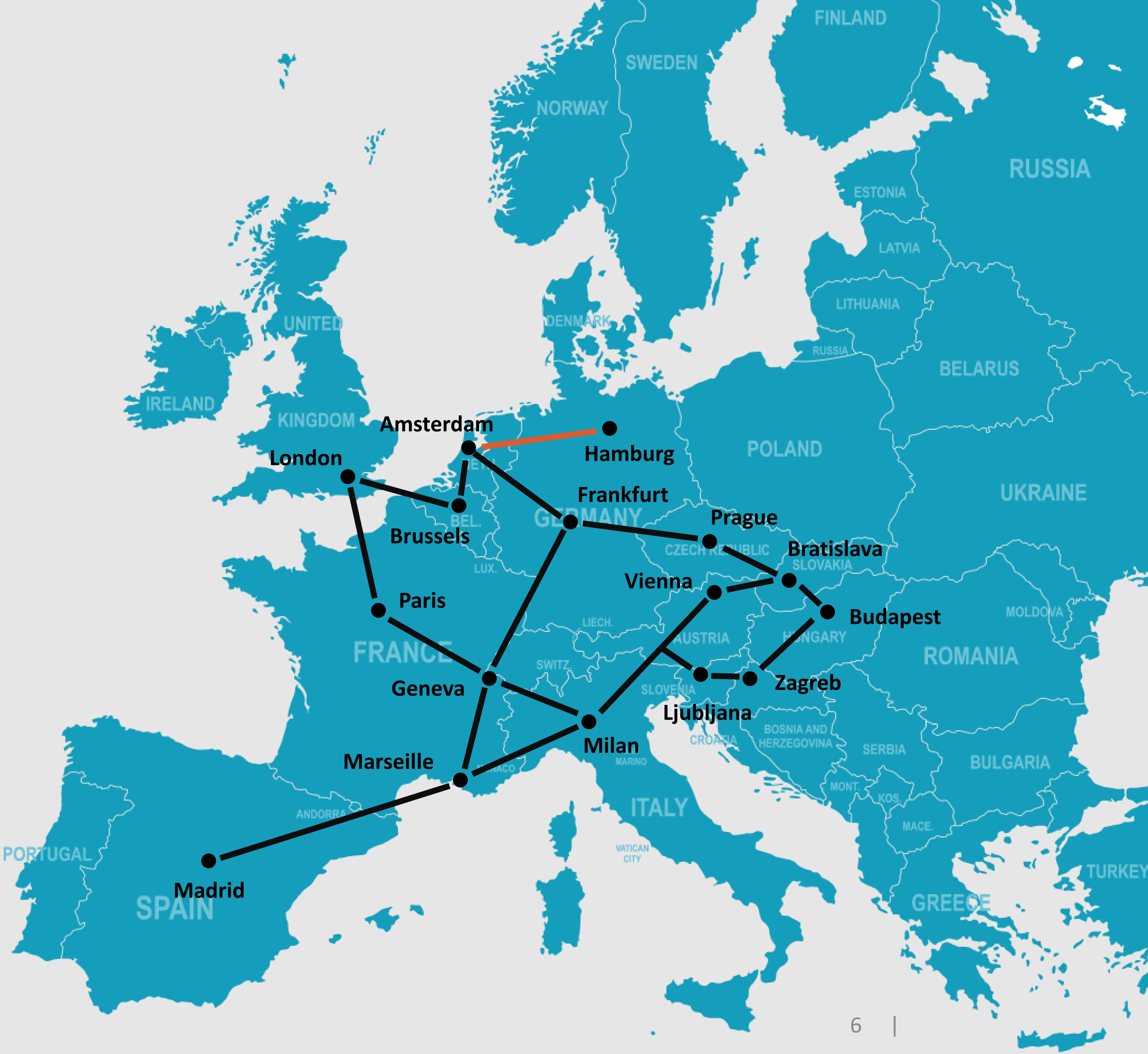
Tata Communications

QUARTERLY VIEW PB OF DATA RECEIVED BY GÉANT



	Q1 2015	Q2 2015	Q3 2015	Q4 2015	Q1 2016	Q2 2016	Q3 2016	Q4 2016	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018	Q3 2018	Q4 2018	Q1 2019	Q2 2019
◆ IP MPLS	117.24	133.57	118.08	155.84	173.16	219.19	202.01	267.22	259.78	265.26	265.96	350.92	346.08	332.58	328.98	475.75	496.61	534.62
■ Total	239.84	259.37	239.36	280.99	303.15	359.42	349.06	414.27	401.00	436.62	481.50	601.21	562.53	564.03	566.84	734.31	708.10	755.14

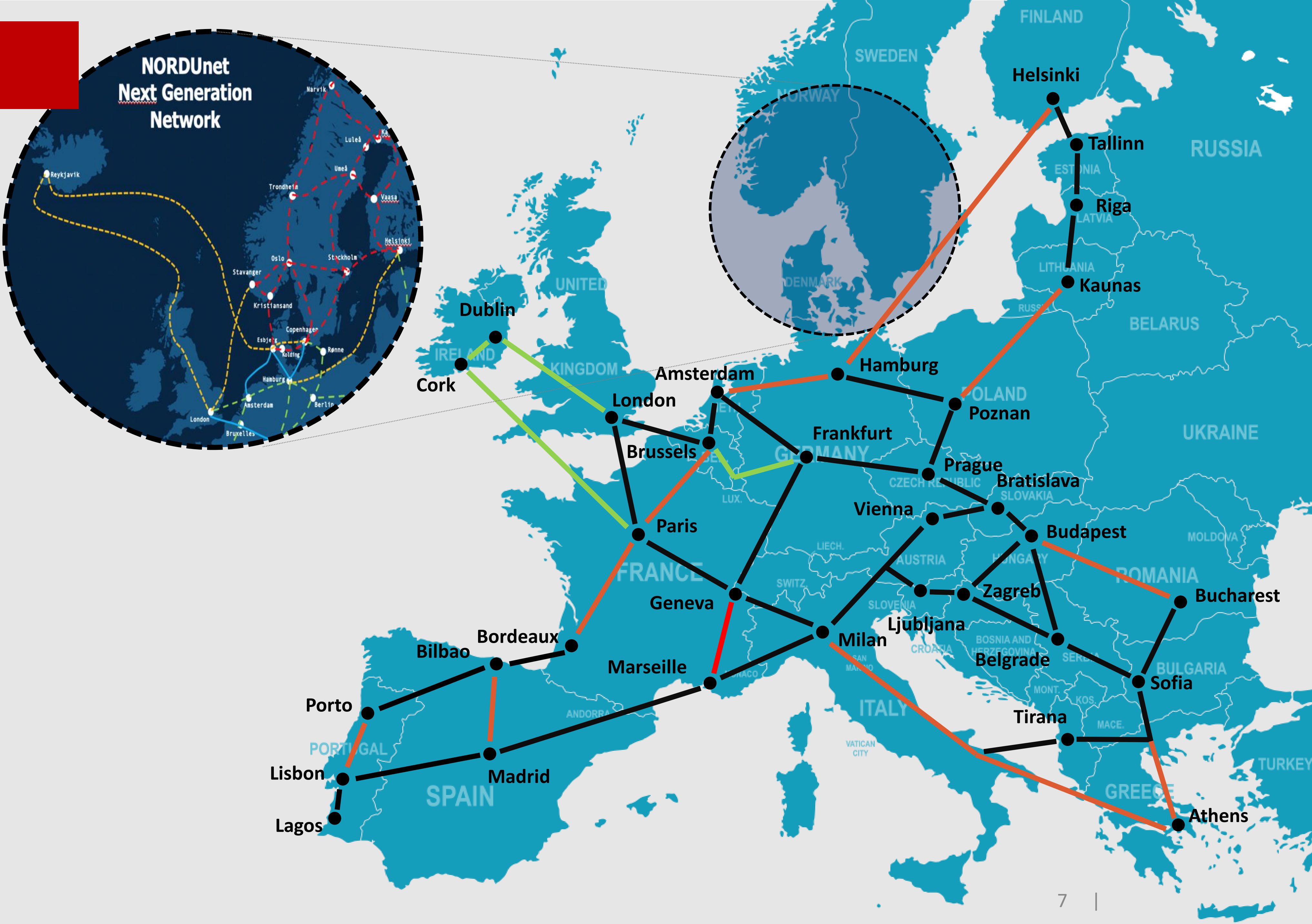
CURRENT FIBRE NETWORK



▬ Commercial Dark Fibre

▬ NREN Spectrum

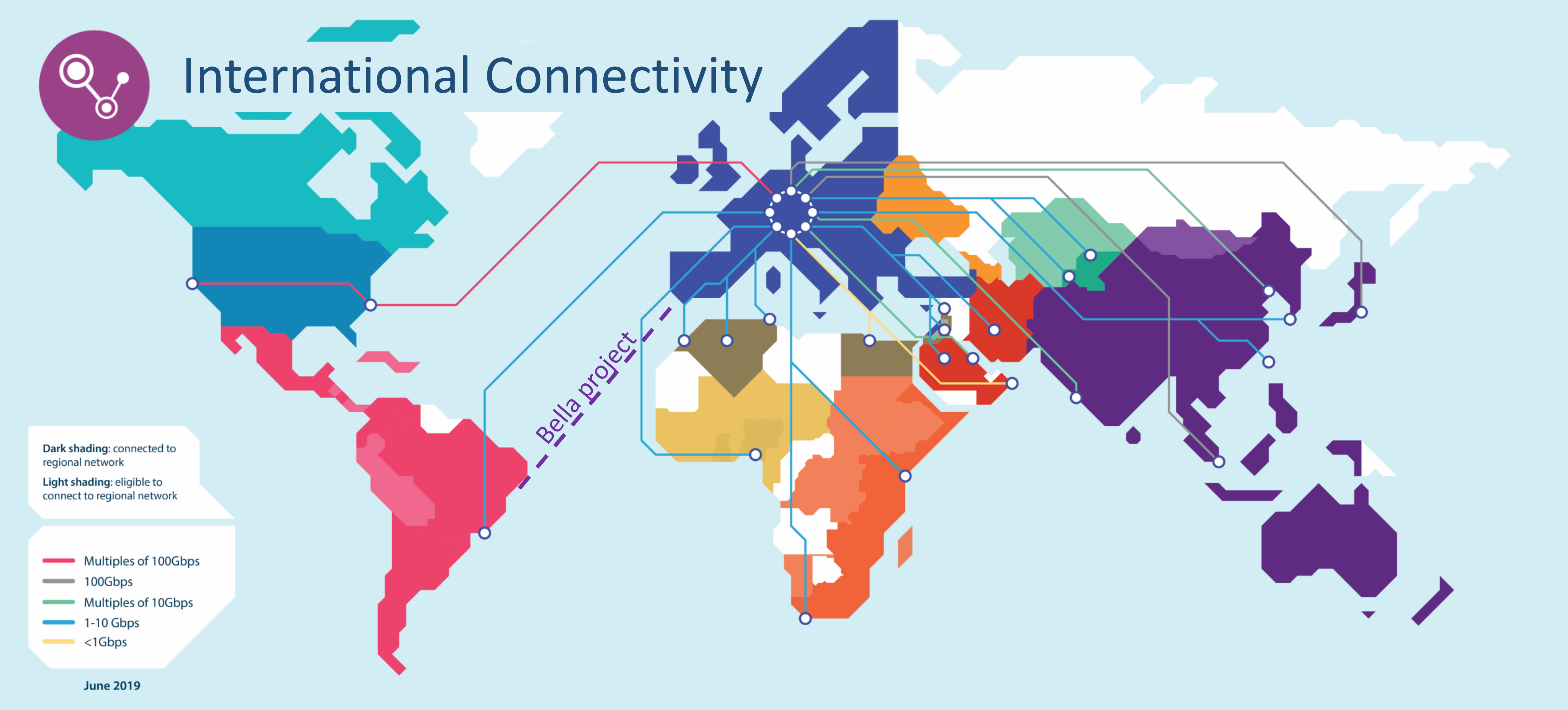
Planned network (not definite!)



Commercial Dark Fibre

NREN Spectrum

International Connectivity



Dark shading: connected to regional network

Light shading: eligible to connect to regional network

Multiples of 100Gbps

100Gbps

Multiples of 10Gbps

1-10 Gbps

<1Gbps

June 2019

Canada & USA

canarie ESnet INTERNET2

Latin America

RedCLARA

Europe

GÉANT EaPConnect

North Africa & Eastern Mediterranean

ASREN AfricaConnect2

West & Central Africa

WACREN AfricaConnect2

Eastern & Southern Africa

UbuntuNet Alliance AfricaConnect2

Central Asia

CAREN

Asia-Pacific

TEIN

Other R&E Networks

GÉANT Services: Secure Trust & Identity services

Protecting privacy and enabling secure access to services

eduroam - secure global roaming access service ***250+ million authentications per month*** in 101 territories. This is a federated service

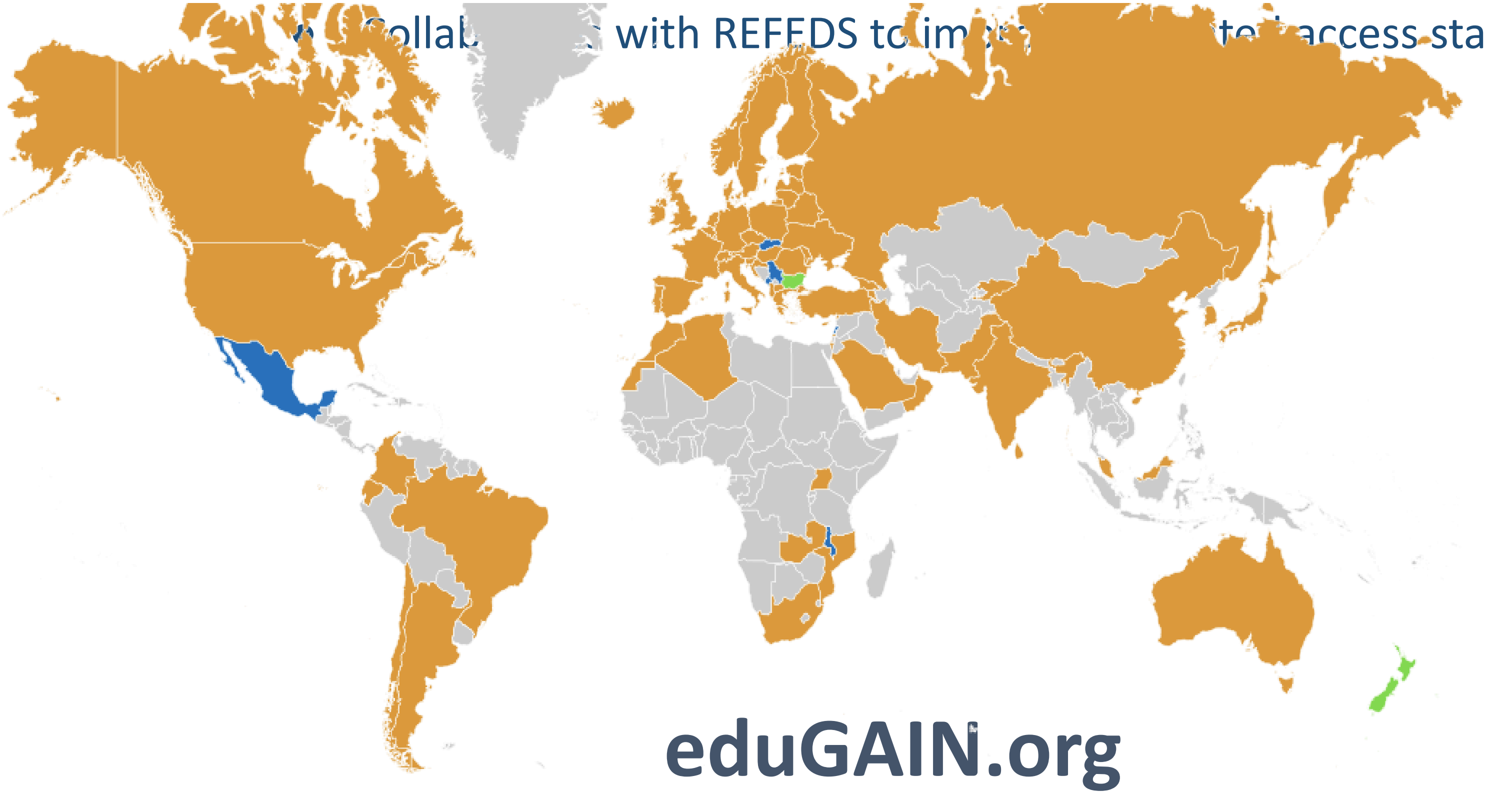
eduGAIN - interconnects identity federations around the world, simplifying access to content, services and resources ~ 3500 identity providers accessing services

eduGAIN

The inter-federation service

eduGAIN inter-connects Identity Federations enabling Identity Providers and Service Providers of different federations to authenticate users worldwide:

- Expands the user base to tens of millions.
- Enables national service providers to offer their service worldwide without per-county agreements
- Enables secure Single Sign On services to global research and educational resources
- Collab[illegible] with REFEDS to im[illegible] [illegible]te[illegible] access standards and security



November 2019:

* 68 Active Federations

* 7 Candidate Federations

* 5790 entities

eduGAIN.org

Identity Providers, Service Providers and Discovery Service

Identity Provider

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

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

The Discovery Service service, also known as "Where Are You From (WAYF)" 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.

The key benefits of eduGAIN

Enabling secure Single Sign On services to global research and educational resources

eduGAIN

Institutions

eduGAIN enables Institutions to support access to thousands of services globally.

Service Providers

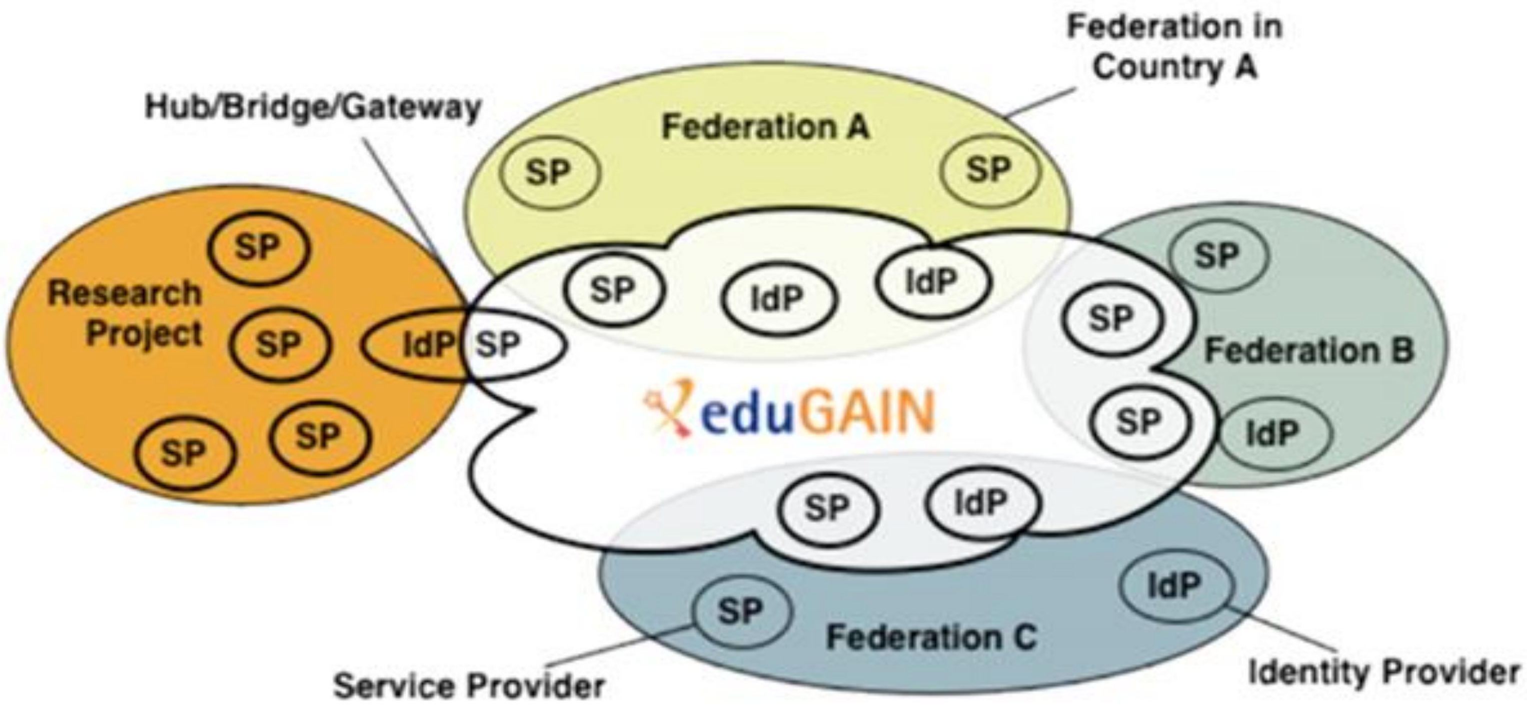
Publishers, Research infrastructures and Cloud service providers can leverage a worldwide authentication service.

Students and Researchers

eduGAIN lets Students, Researchers and Staff access online services and resources using their Home Institution account, improving the user experience and security and reducing the costs and complexity.

The big picture about eduGAIN

eduGAIN



The **eduGAIN inter-federation** service connects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN comprises over 60 participant federations connecting more than 5,000 Identity and Service Providers.

Full Mesh Federations

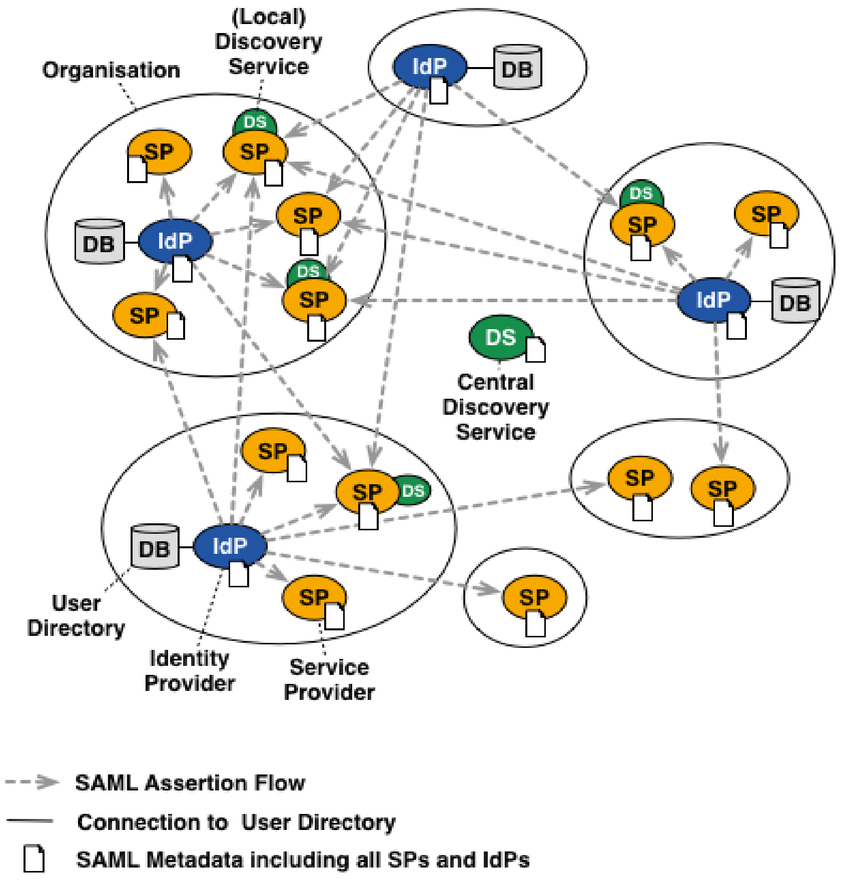
Full mesh federations are the most common and straight forward to implement federations because everything is distributed and there is **no need for a central component** that has to be protected specifically against failover (that duty is distributed as well).

Every organisation in mesh federations (IdP) connected to a local user data**operates their own Identity Provider** base and an arbitrary number of Service Providers (SP).

All these **entities are listed in a centrally distributed SAML metadata file**, which is consumed by all entities.

Full Mesh Federation

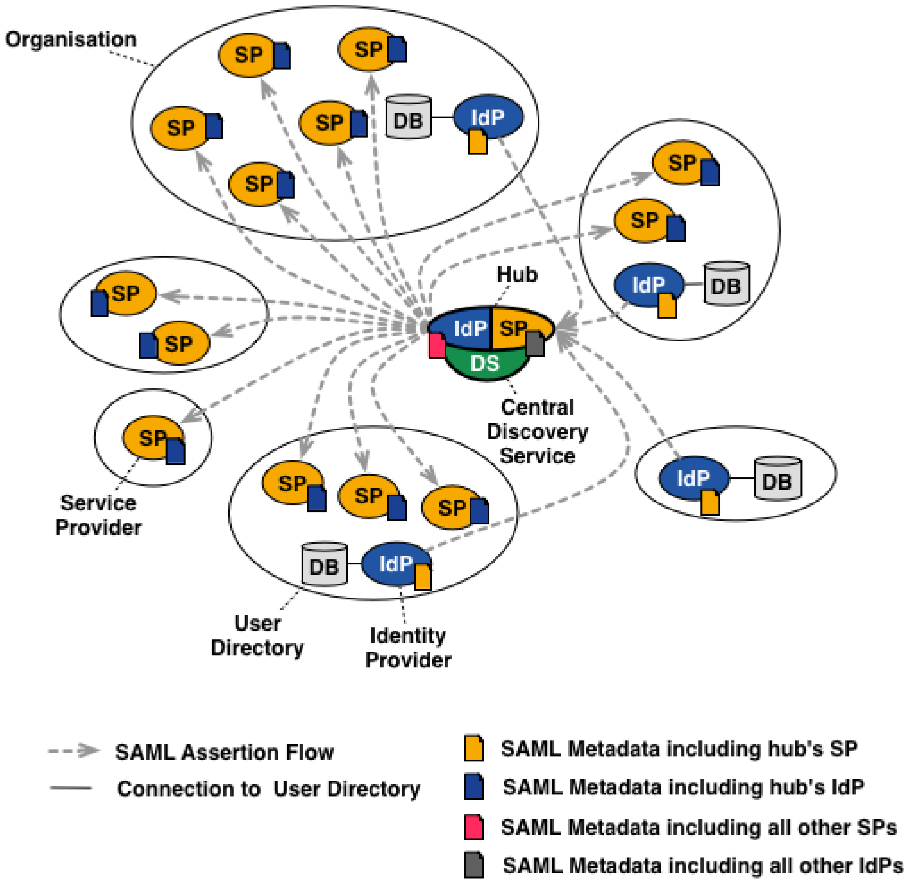
~80% of all NREN Federations (June 2013)
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF


Organisation
(Local) Discovery Service
IdP
DB
SP
DS
Central Discovery Service
User Directory
Identity Provider
Service Provider
SAML Assertion Flow
Connection to User Directory
SAML Metadata including all SPs and IdPs

Hub and Spoke Federations

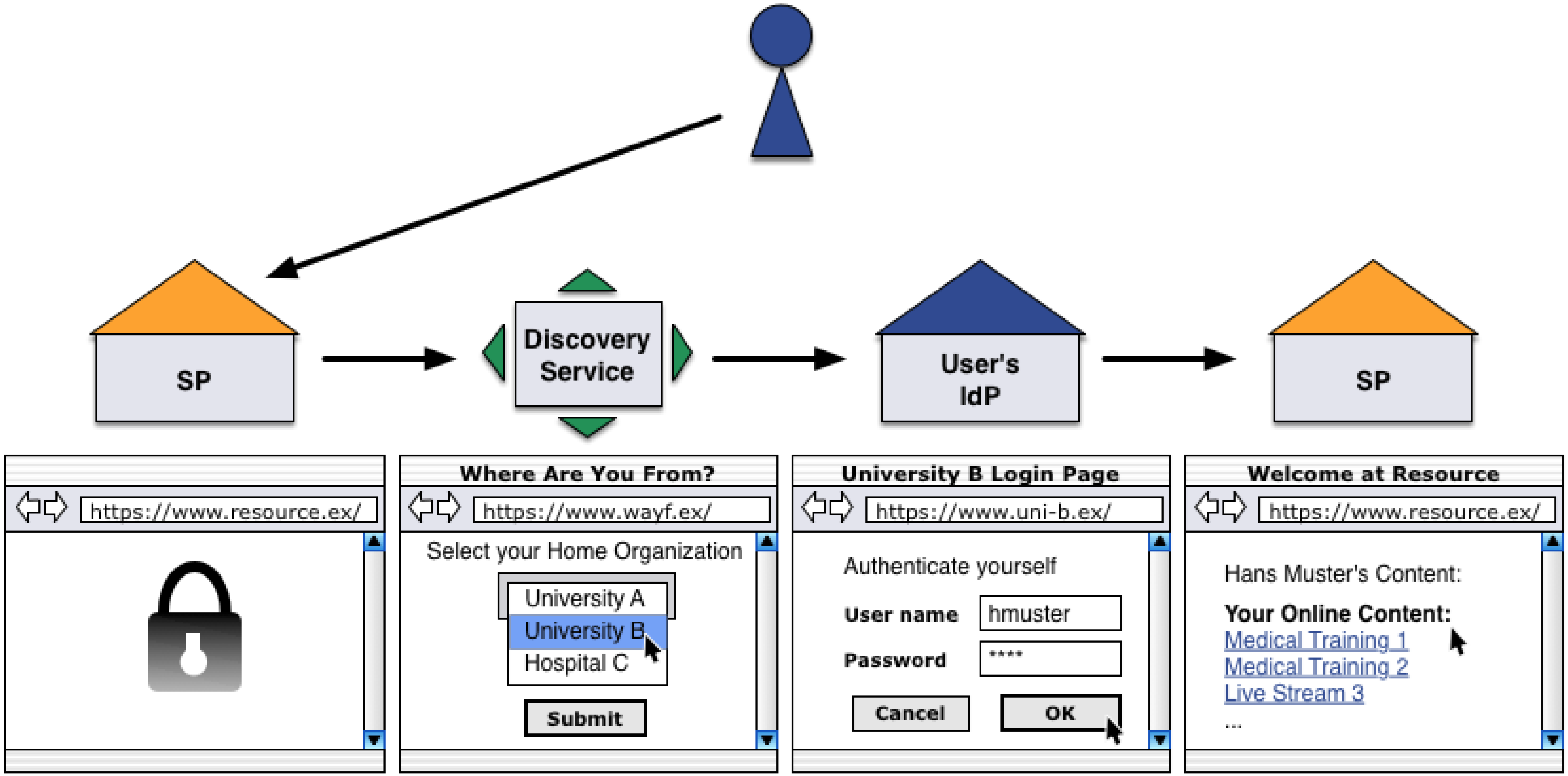
Hub-and-Spoke Federation with Distributed Login

~15% of all NREN Federations (June 2013)
SURFconext, WAYF.dk, SIR, TAAT, Confia


Organisation
SP
SP
SP
SP
DB
IdP
SP
SP
SP
SP
IdP
DB
Hub
SP
SP
IdP
SP
DS
Central
Discovery
Service
SP
Service
Provider
SP
SP
SP
IdP
DB
DB
IdP
User
Directory
Identity
Provider
SAML Assertion Flow
Connection to User Directory
SAML Metadata including hub's SP
SAML Metadata including hub's IdP
SAML Metadata including all other SPs
SAML Metadata including all other IdPs

- Hub & Spoke federations with distributed login rely on a central hub or proxy via which all SAML assertions are sent.
- The hub serves as a Service Provider versus the Identity Providers and as an Identity Provider versus the Service Providers in the federation.
- Each organisation still operates their own Identity Provider connected to a local user database but the Identity Provider only needs metadata of the hub.
- Vice versa the Service Providers only need metadata for the hub.
- On the hub there is a central Discovery Service for all users.
- Because the hub is a single-point of failure, it has to be carefully secured and protected.

A simple flow



Where Are You From?

Select your Home Organization

- University A
- University B
- Hospital C

University B Login Page

Authenticate yourself

User name hmuster

Password ****

Welcome at Resource

Hans Muster's Content:

Your Online Content:

Medical Training 1
Medical Training 2
Live Stream 3
...

Access Service | **Choose Home Organisation** | **Provide credentials** | **Use Service**

Entities, metadata and Identity Federation

Entities register metadata

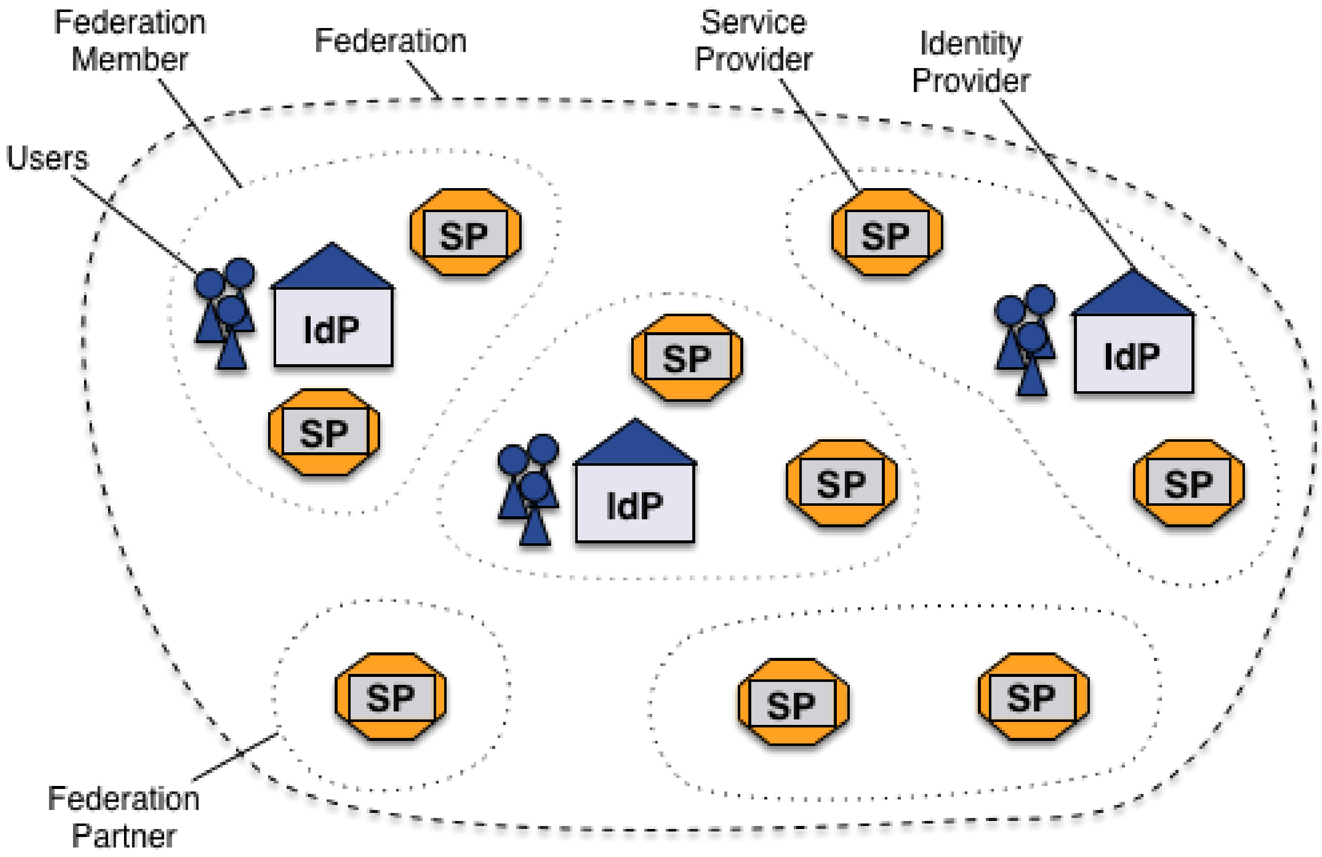
Participating Entities register their metadata into the Federation

The Federation feed

The Federation validates and aggregates all the entites metadata creating one or more federation feed

Signing & Distribution

The Federation feed(s) is signed with the Federation key and distributed through an MDS (Metadata Distribution System)



eduGAIN MDS, how does it work?

Federations' upstream feed

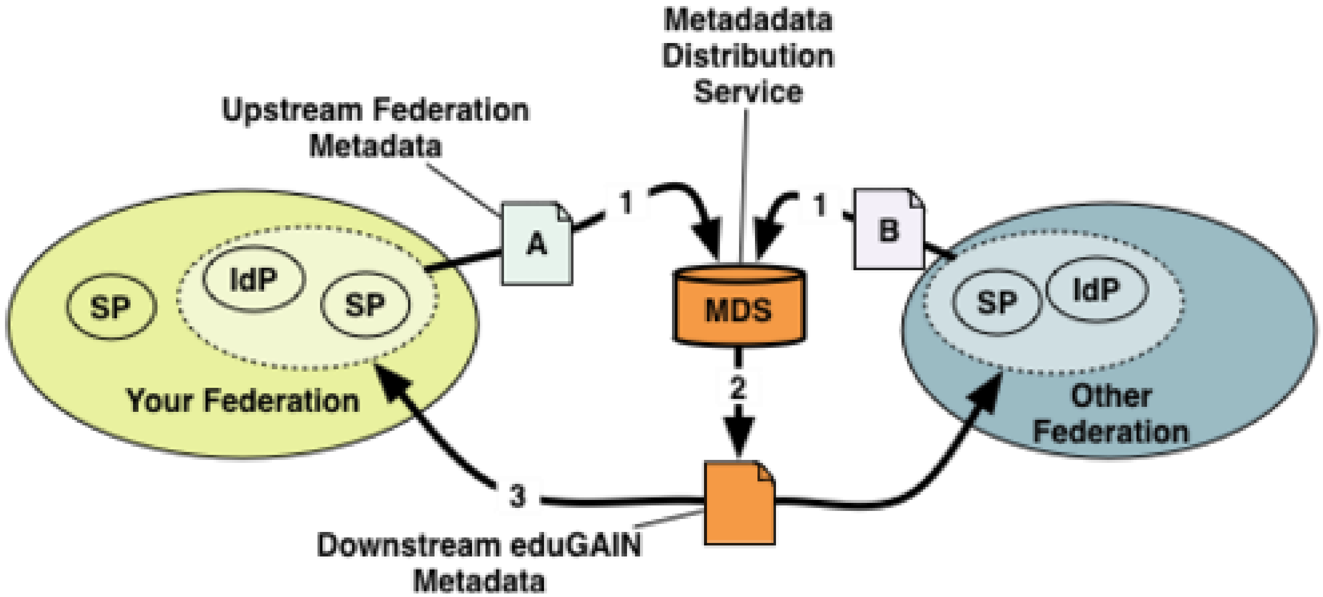
Participating Federations provide a metadata aggregate of entities to be exported to eduGAIN

The eduGAIN feed

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

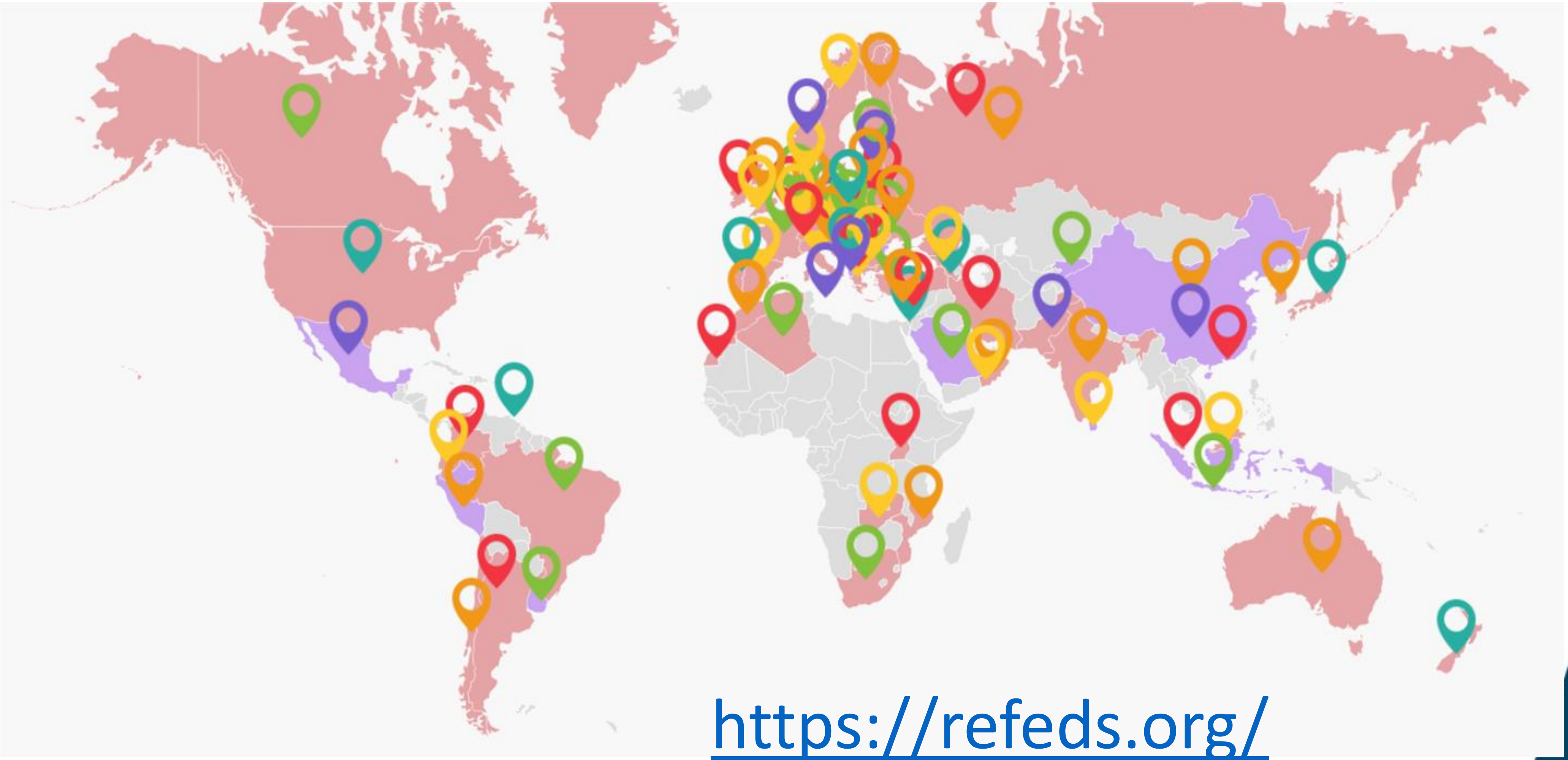
Signing & Distribution

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


Metadadata Distribution Service
Upstream Federation Metadata
A
1
1
B
SP
IdP
SP
Your Federation
MDS
2
SP
IdP
Other Federation
3
Downstream eduGAIN Metadata

http://mds.edugain.org/edugain-v1.xml

REFEDS Production Federation Map



https://refeds.org/

eduGAIN and federated services

https://technical.edugain.org

Security

eduGAIN Support

eduGAIN Security Incident Response

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)

eduGAIN Code of Conduct Monitor (ECOCM) monitor

Sirtfi contact check service

F-Ticks based eduGAIN statistics collection and presentation service

Deploy

Campus IdP Toolkit (ansible playbook to install an IdP)

Federation-as-a-Service (FaaS)

The GEANT IdP Ansible toolkit

Deploy

- GN4-2/GN4-3 developed a toolkit based on **Ansible** to ease the spawning of Shibboleth 3.4+ Identity Providers
- It makes spawning IdPs easy
  - Minimal set of mandatory configuration
  - Wrapper script to generate customized playbook
  - Supports Entity Categories R&S, CoCo
  - Fully eduGAIN compliant (privacy policy pages, logos..)

  - https://github.com/GEANT/ansible-shibboleth

ANSIBLE

eduGAIN

Service outreach options:

- Local Deployment
- Capacity Building / Training
- Sharing of Best Practices
- Marketing Material

How to join eduGAIN as a Federation:

- In order to join eduGAIN, Federations need to provide information to edugain@geant.org via a signed email
  - **Contact email**
- **Signing declaration**
  - https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf
- **Printed Declaration** must be signed by a person authorized to represent the Federation
  - Signed Declaration should be sent to the postal address of the eduGAIN Team:

    eduGAIN c/- GÉANT, 6B, Nieuw Amsterdam
    Hoekenrode 3
    1102 BR Amsterdam-Zuidoost
    The Netherlands
- Please also send a scan of the declaration to the eduGAIN Team mail: edugain@geant.org
- **Metatada source and signing certificate**
-

How to join eduGAIN as a Federation

- **Governance delegate and deputy**
  - eduGAIN is governed by the Steering Group. Each partcipating federation must delegate two members - a delegate and a deputy. Please send names and e-mail addresses to the edugain@geant.org
- **Federation page**
  - Provide a URL pointing to the main (English if exists) page of your Federation
- **Policy**
  - Provide a URL pointing to the English version of your Federation Policy
- **Registration practice statement**
  - Provide a URL pointing to the English version of Metadata Registration practice statement for your federation. This document shall describe rules and procedures used for registering entities which get exposed to inter-federation

eduGAIN and federated services

https://technical.edugain.org

Security

eduGAIN Support

eduGAIN Security Incident Response

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)

eduGAIN Code of Conduct Monitor (ECOCM) monitor

Sirtfi contact check service

F-Ticks based eduGAIN statistics collection and presentation service

Deploy

Campus IdP Toolkit (ansible playbook to install an IdP)

Federation-as-a-Service (FaaS)

The GEANT IdP Ansible toolkit

Deploy

- GN4-2/GN4-3 developed a toolkit based on **Ansible** to ease the spawning of Shibboleth 3.4+ Identity Providers
- It makes spawning IdPs easy
  - Minimal set of mandatory configuration
  - Wrapper script to generate customized playbook
  - Supports Entity Categories R&S, CoCo
  - Fully eduGAIN compliant (privacy policy pages, logos..)

  - https://github.com/GEANT/ansible-shibboleth

eduroam

eduroam

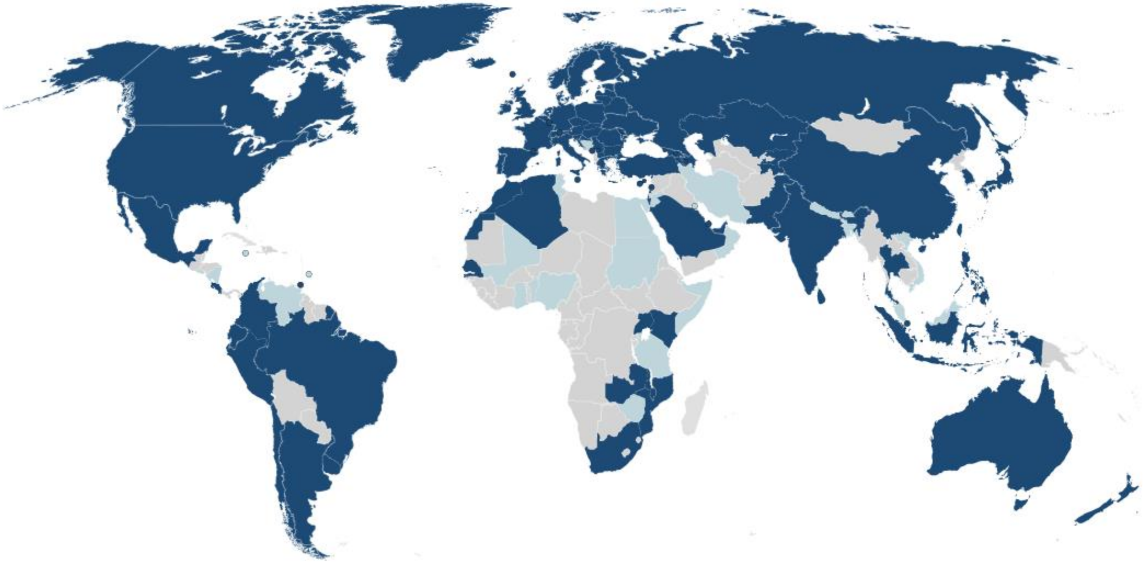
Linking students to the global community

A secure global roaming infrastructure for research and education:
users **authenticate locally** and
get online in eduroam-enabled locations

A global network of users across 101 territories.
More than 2 billion international authentications and counting

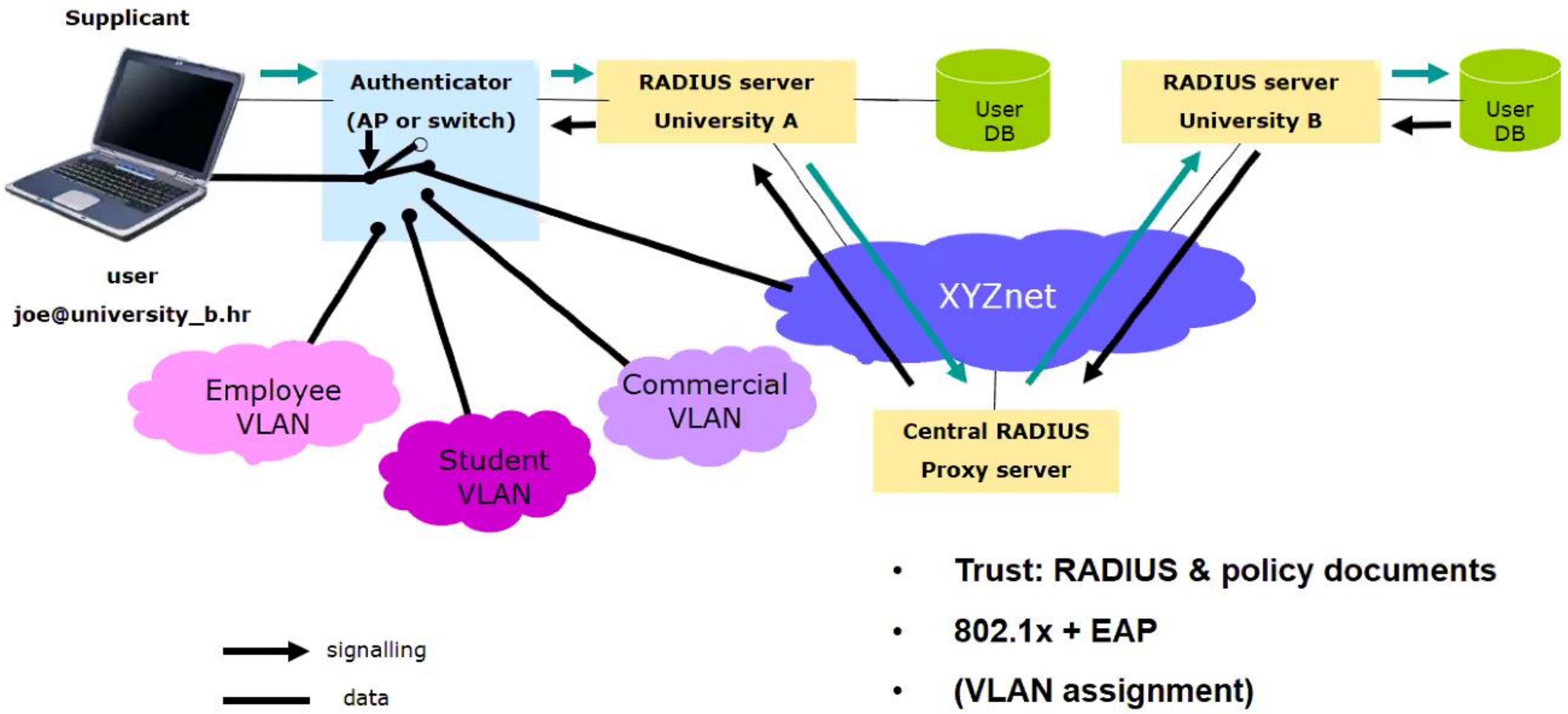
A worldwide success story :

Millions of users in more than 100 territories worldwide, eduroam has been an amazing success story and an example of research and education collaboration.



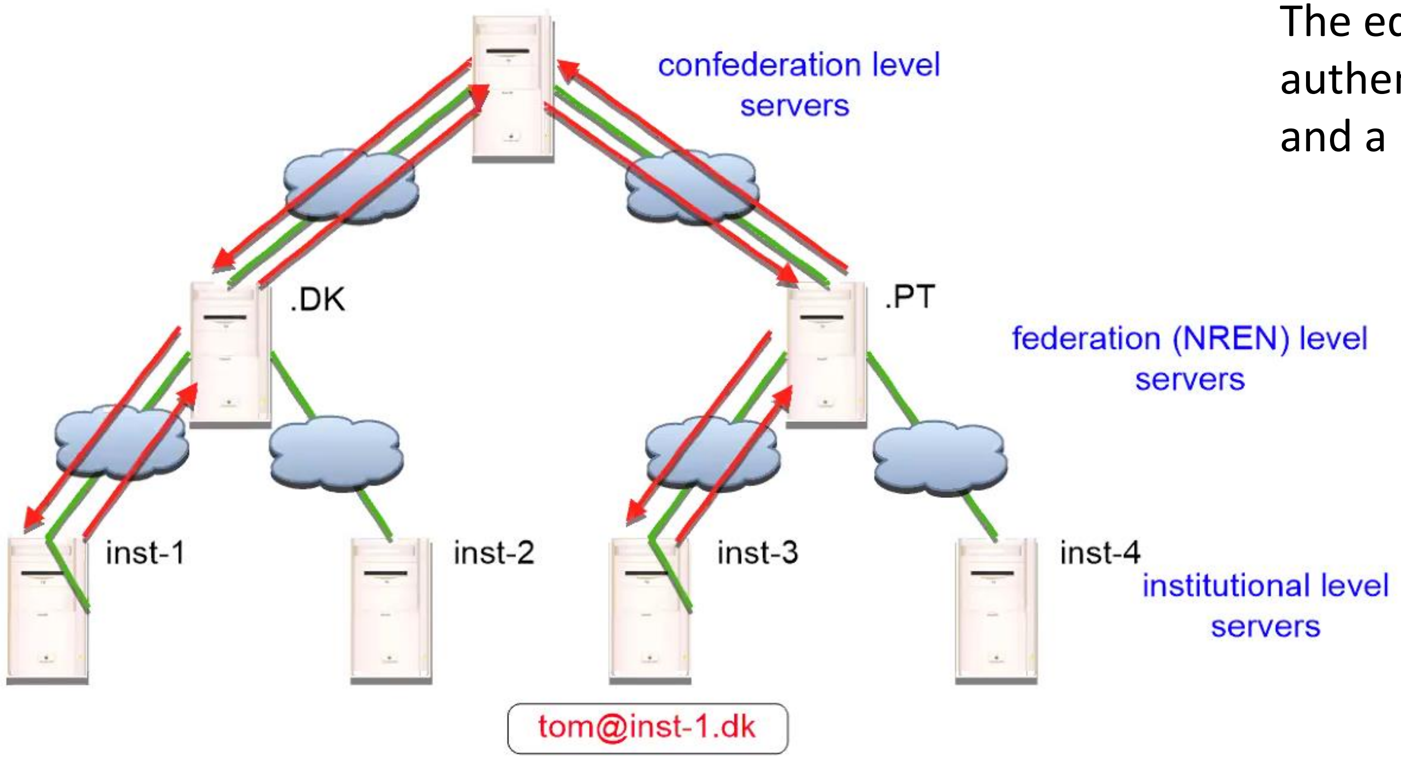
eduroam.org **@eduroam**

The eduroam™



- Trust: RADIUS & policy documents
- 802.1x + EAP
- (VLAN assignment)

Hierarchical RADIUS-based authentication infrastructure



confederation level servers
.DK
.PT
federation (NREN) level servers
inst-1
inst-2
inst-3
inst-4
institutional level servers
tom@inst-1.dk

The eduroam service uses IEEE 802.1X as the authentication method
and a hierarchical system of RADIUS servers

CAT: Configure your mobile device to use eduroam:
https://cat.eduroam.org/

NEW

eduroam Managed IdP service to simplify onboarding of smaller institutions

Open for Institutes worldwide

eduroam monitor:
Monitor the status of the RADIUS servers and related infrastructure:
https://monitor.eduroam.org/

How to join eduroam

- Ensure NRENs act as NRO for eduroam
  - Sign the eduroam policy documents
    - Done. (Signed in March 2018 by Bangladesh)
  - Need to publish XML information on the eduroam DB

- Start by setting up national FLR server and national eduroam infrastructure
  - Set up eduroam IdPs at individual institutions or make us of eduroam managed IdP (contact the eduroam-ot@lists.geant.org or help@eduroam.org)
  - Set up beta service providers (SPs)
- Contact eduroam operational teams to configure the international branches
  - ASIA-Pacific Top Level Radius servers operated by Univ. Honk Kong and AARNET/Australia

How to set up the national eduroam infrastructure

- Becoming a Roaming Operator (RO)
  - Administrative requirements / Information management requirements
- Operating a Federation Level RADIUS server (FLR)
- Gauging your federation's performance
  - Monitoring
    - Federation monitoring in Europe: the eduroam Operational Team
    - Monitoring inside the federation
    - Nagios/Icinga: EAP Login check : Preparatory work , Implementing the checks
    - Nagios/Icinga: RADIUS/TLS certificate validity checks
  - Statistics
- RADIUS/TLS: Obtaining and managing certificates
  - The eduroam server certificate trust model: eduPKI PMA and the eduroam Trust Profile
  - Managing accredited CAs in eduroam servers
  - Updating CRLs on your server

- https://wiki.geant.org/pages/viewpage.action?pageId=121346324

eduroam in Bangladesh

- Bangladesh (BdREN) is an accepted member of the eduroam service
- Signed eduroam compliance statement in March 2018
- Need to set up information for the eduroam DB
  - Need to publish information on the web site on https://www.eduroam.bd/general/realm.xml
    - **Schema and related information:** https://monitor.eduroam.org/eduroam-database/v2/docs/eduroam-database-ver17102017.pdf
- Inform eduroam-ot@lists.geant.org and miro@srce.hr
- After that access to the eduroam central DB and the CAT tool can be granted

eduroam related services

- eduroam Managed IdP
  - Focusing on smaller organisations that lack technical capabilities to have deploy IdP
  - Outsources the technical setup of eduroam IdP functions to the eduroam Operations Team
  - Already available in 20 countries; no charge to Roaming Operators.
- eduroam CAT
  - Configuration tool
- eduroam Companion App
  - Where’s the nearest eduroam access point?
- eduroam Visitor Access
  - Service from Dutch NREN, SURFnet
  - Enables institutions to provide temporary eduroam access for visitors

To provide an open, innovative and trusted information infrastructure for the European knowledge economy and to the benefit of society worldwide

Thank you

mario.reale@geant.org

Acknowledgements:
GEANT and GN4-3 eduGAIN, eduroam Teams,
GEANT Partner Relations Team,
GEANT Research Engagement and Support Team

www.geant.org

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).