HEAnet

LIR group

Shibboleth Access

Glenn Wearen

NDP National Development Plan Transforming Ireland

4 May 2011

Agenda

- **Overview of HEAnet**
  - Who we are, what we do
- **Introduction to Shibboleth federated access**
  - History, current status, future outlook
- **Edugate**
  - Why HEAnet, how it works, benefits
  - Who's a member, what it takes to join
  - Technical information
  - Implementation options

HEAnet's Mission

HEAnet is committed to delivering and supporting advanced network and associated ICT services in furtherance of national and international objectives for Irish education and research.

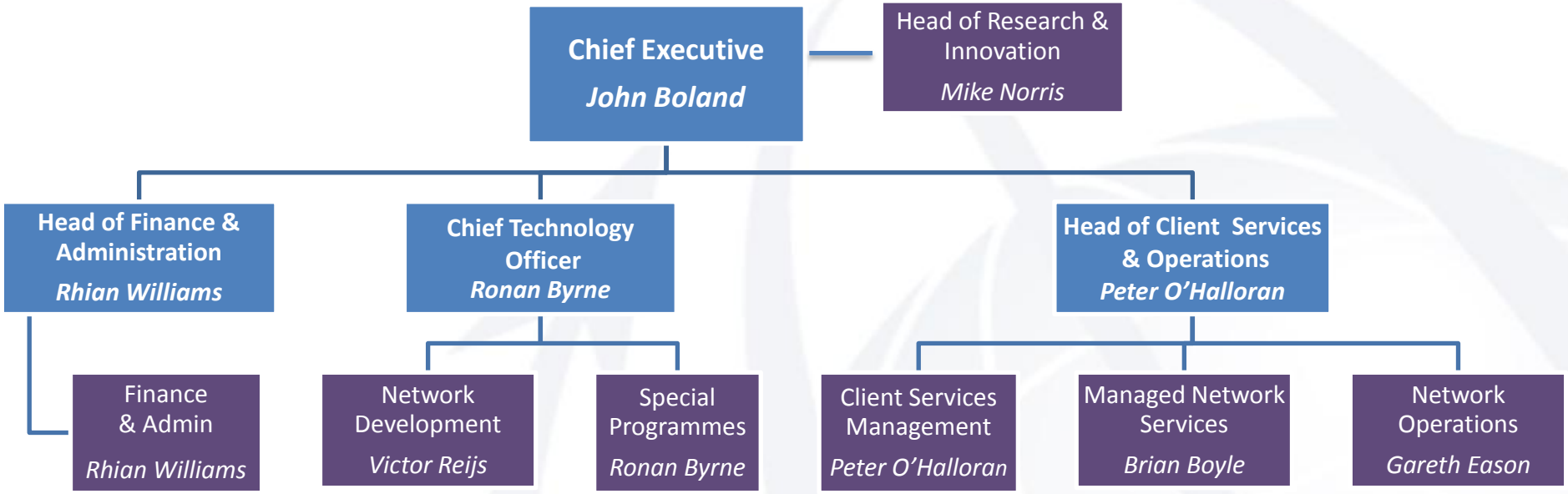
Source: HEAnet Strategic Plan 2008 -2013 "Lighting the Future"

Who We Are

- HEAnet is Ireland's National Education and Research Network
- Set up in 1983 as a collaborative body by the seven Irish Universities & The Higher Education Authority
- Became a non-profit, Limited company in 1997
- Approx. 50 staff members whose areas of expertise lie in:

Shared Services Infrastructure	Advanced ICT Services
Network Operations	Services management
Leading Edge Internet Engineering	Telecommunications

Who We Are: Management Structure



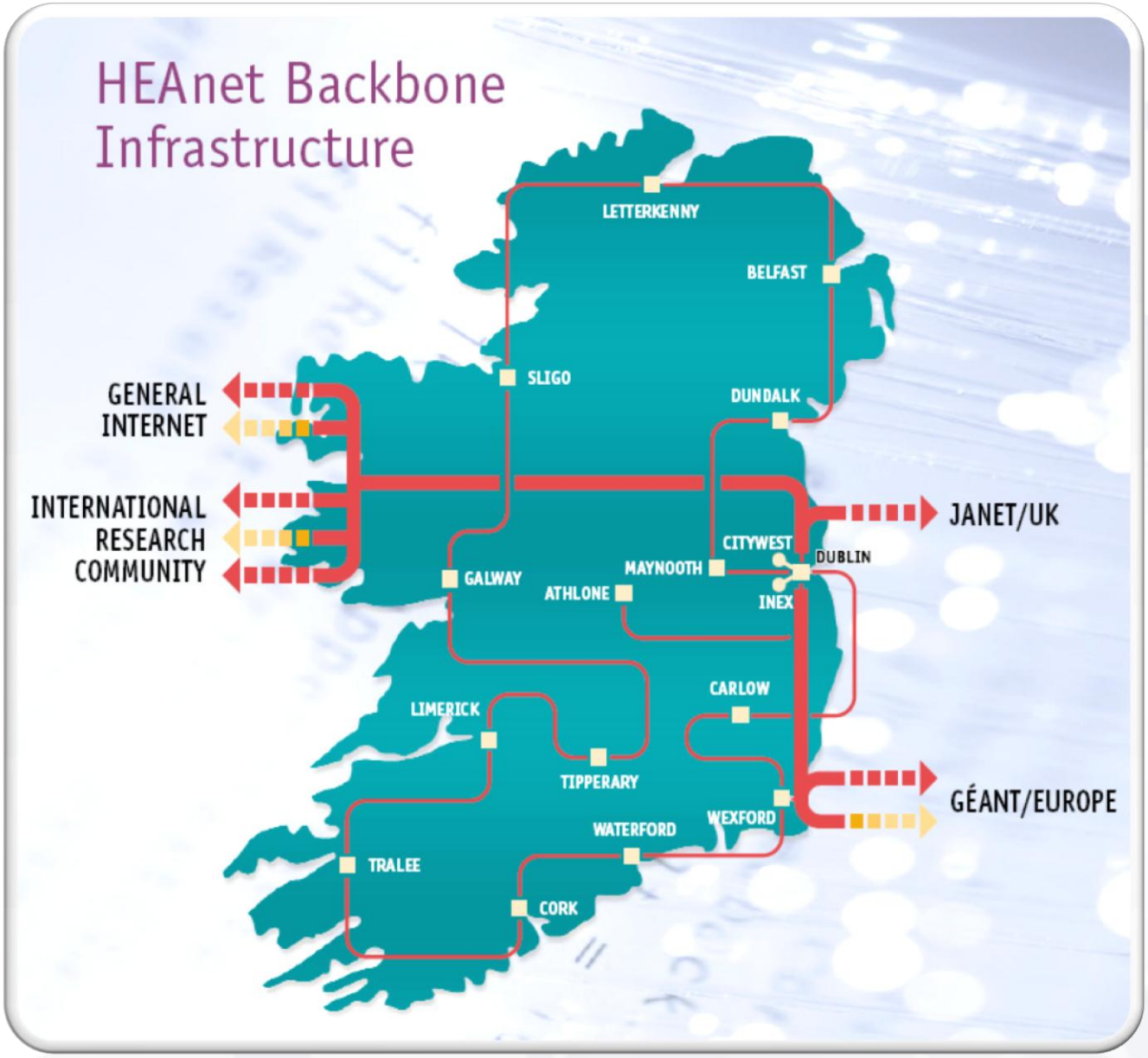
Who We Are: Network Members

- 7 Universities & DIT
- 13 Institutes of Technology
- 16 Third Level Colleges and VECs
- 24 Non-profit Education and Research organisations
- Government agencies / Administrative bodies
- In excess of 180,000 end user community
- 4,000 primary and post-primary schools, through DES

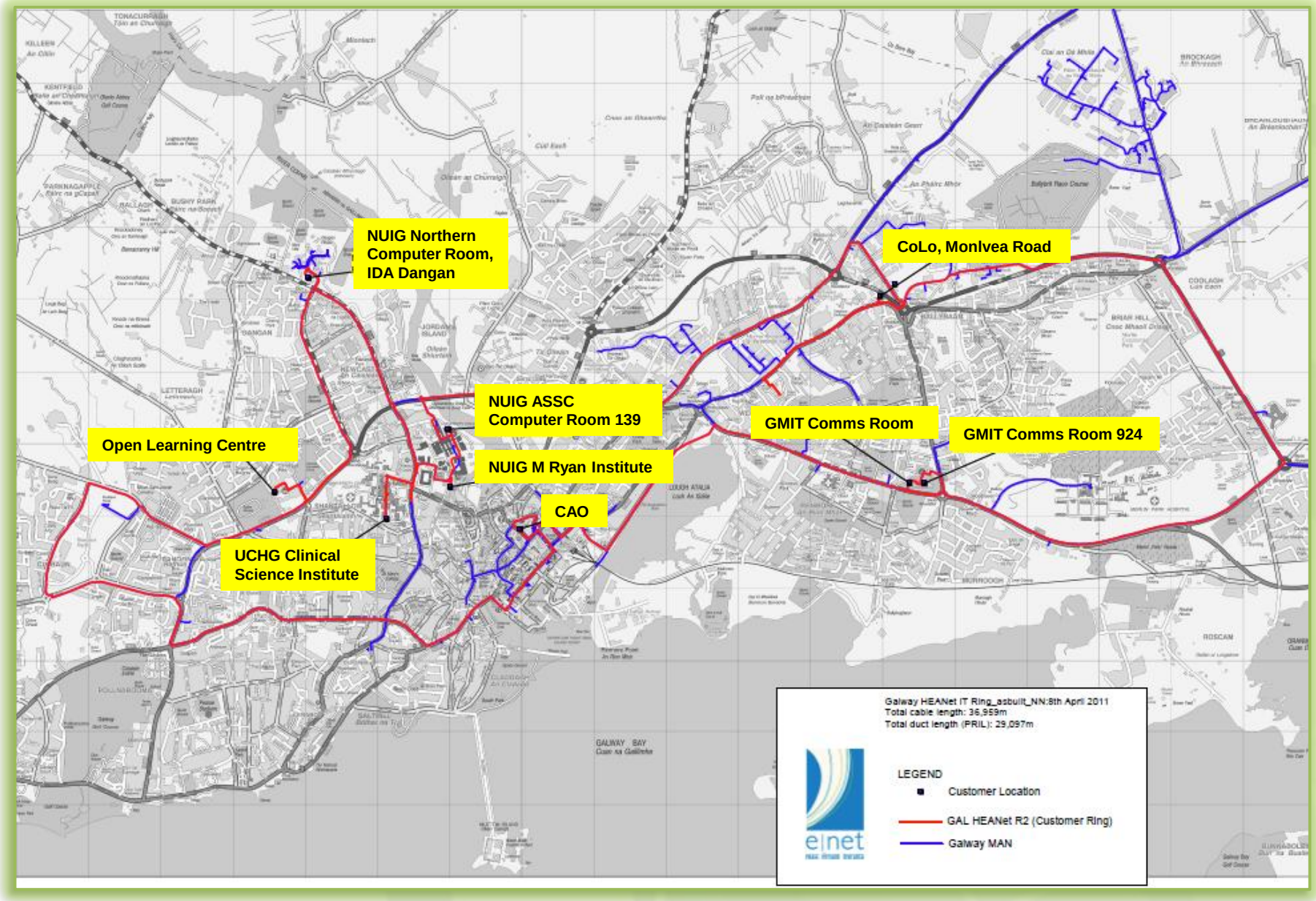
What We Do

- Provide high quality Internet Services to Irish Universities, Institutes of Technology and the research and educational community, including all primary and post-primary schools
- Enable research and learning through leading edge shared services to our clients
- Act as a representative body for the ICT education & research community, at home and abroad
- Facilitate innovation and collaboration worldwide
- Provide value for money

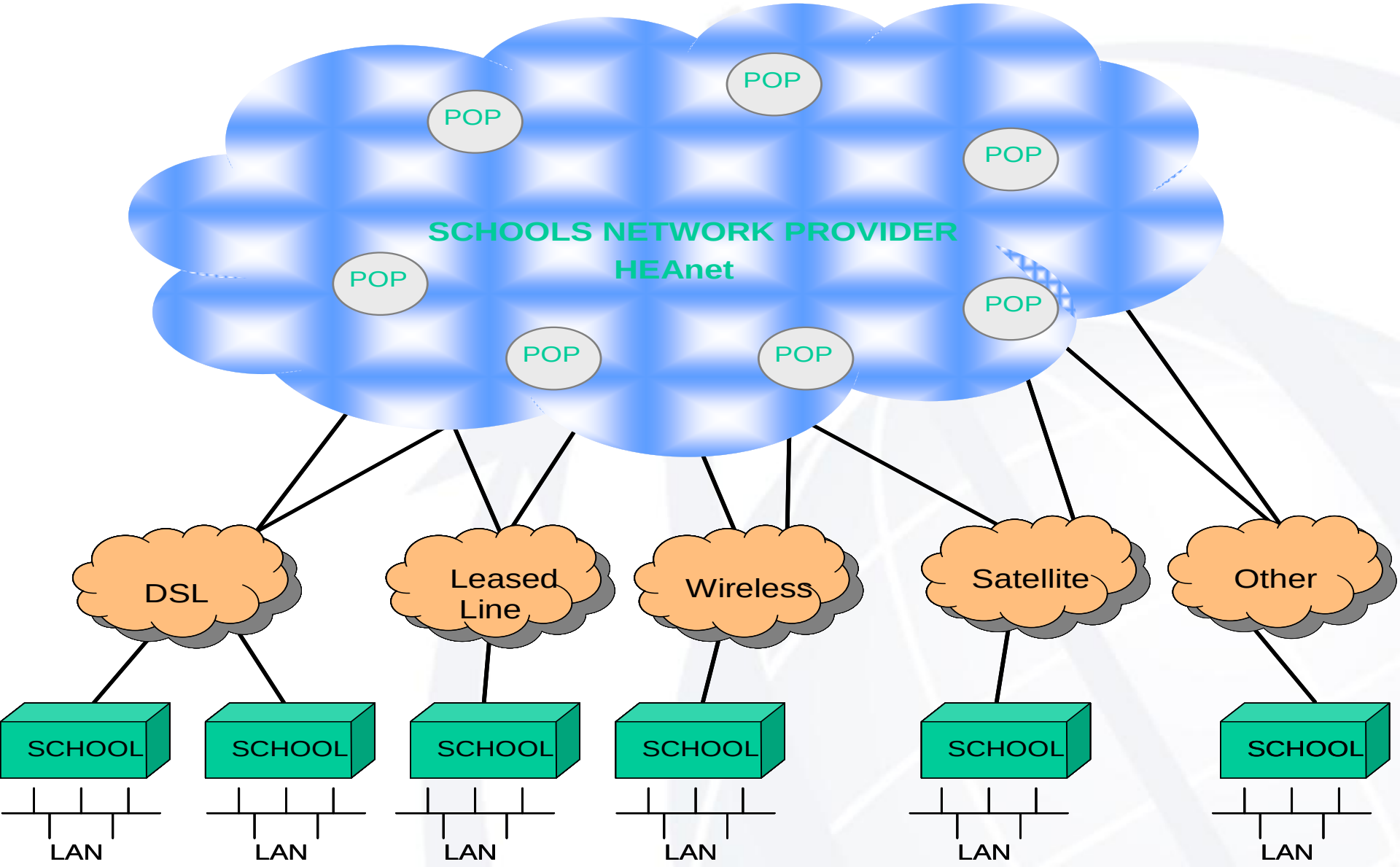
What We Do: Backbone



What We Do: Access Rings



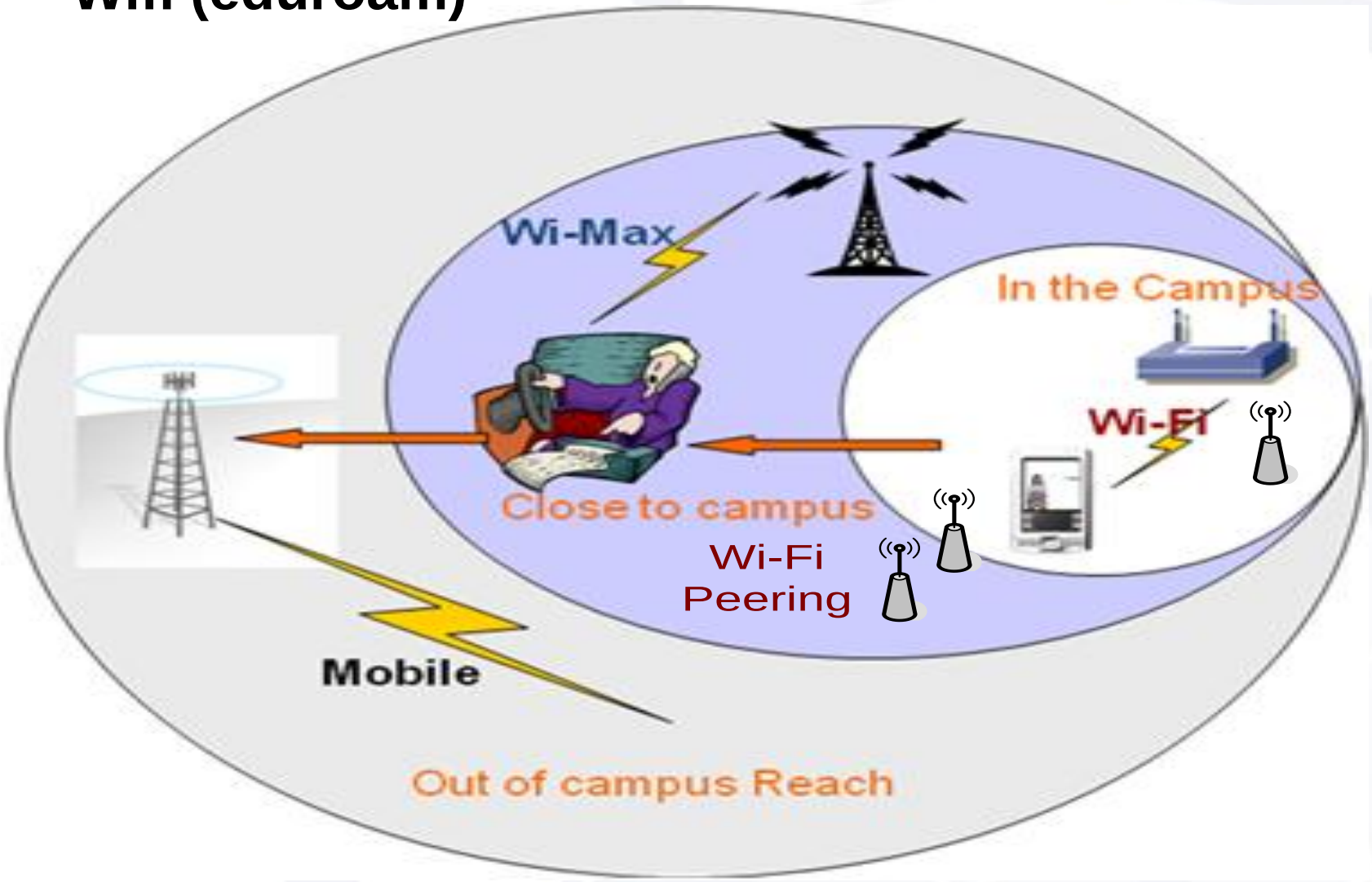
What We Do: Schools



Schools Network Map

What We Do: Wireless

- **3G**
- **Wifi (eduroam)**



What We Do: Middleware

For WWWifi

Both have;

- ***Identity Providers***
- ***Service Providers***
- ***Policy***
- ***Central component/operator***

For the WWW

What We Do: Data Storage

What We Do: Multimedia

- Seminar recording
- Large file transfers
- Video conferencing
- Video hosting

What We Do: Software Licence Consortium

- **Microsoft, Apple, Adobe, Cisco**
- **o2**
- **Chest Ireland (Eduserv)**

What We Do: Hosting

- MediaWiki, Drupal, Wordpress
- Custom hosting (e.g NDLR DSpace)
- ListServ
- Co-location, hot-standby DNS, SSL Certificates

HEAnet's National Networking Conference

10th and 11th November 2011

Lyrath Estate Hotel, Kilkenny

Shibboleth Access

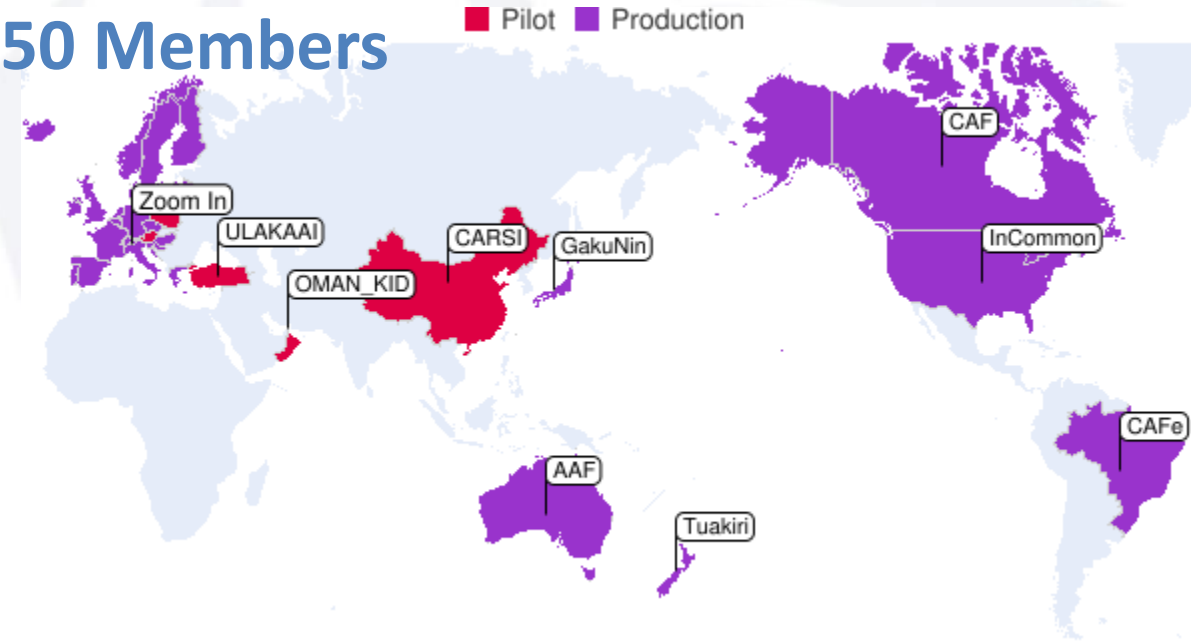
- History
- Current Status
- Future Outlook

Shibboleth Access

- **History**
  - Shibboleth Internet2 activity since 2001
  - SAML1.1 protocol since 2001 in enterprise
  - SAML2 combined Shibboleth and SAML1
  - Migration from Eduserv Athens to UK Federation 2006-2008
  - Swiss SWITCH federation established 2005

Shibboleth Access

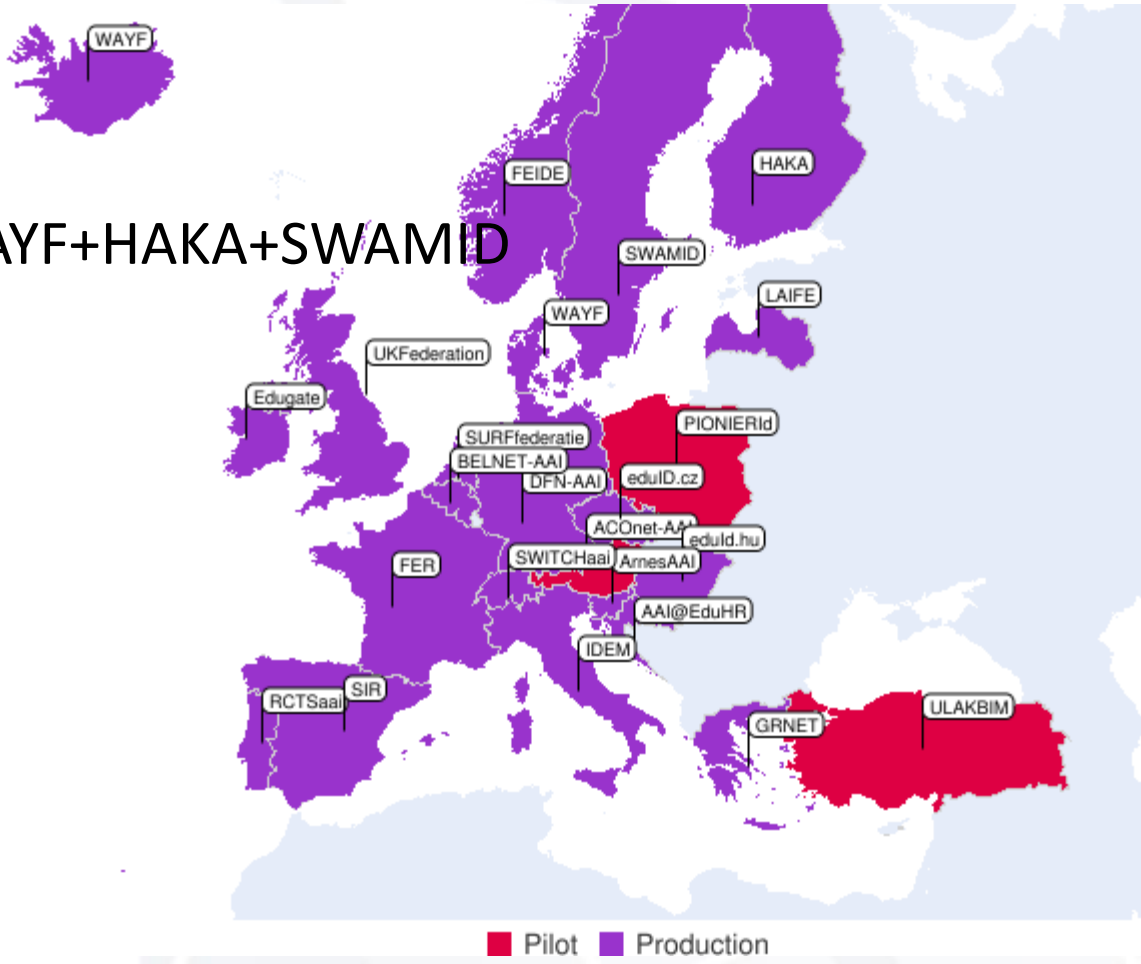
- **Current Status**
  - US: 6.5 Million ID's covered
  - SWISS: 95% of ID's
  - UK: 850 Members



Shibboleth Access

- **Current Status**

Kalmar=FEIDE+WAYF+HAKA+SWAMID



Shibboleth Access

- **Current status (publishers)**
  - Some are members of multiple federations
  - Some support SAML 1+2
  - Some are limited to UK federation only
  - Some are limited to SAML1
  - Some are limited to IP access control
  - Some, until recently, only supported SAML
  - Some are more strict than others on licencing
  - Some will support Shibboleth when requested by the subscriber only

Shibboleth Access

- **Future Outlook**
  - eduGAIN
  - UK-Irl inter-federation
  - SAML2 becoming widespread across sectors
  - IPv4 Address depletion
  - More and more off-campus users
  - Google ingrained as “the internet”
  - Single-Sign-On* expected

Shibboleth Access

- **Future Outlook**
  - **eduGAIN**
    - ✓ Production service
    - ✓ Open to new federations
    - ✓ Opt-in model

Shibboleth Access

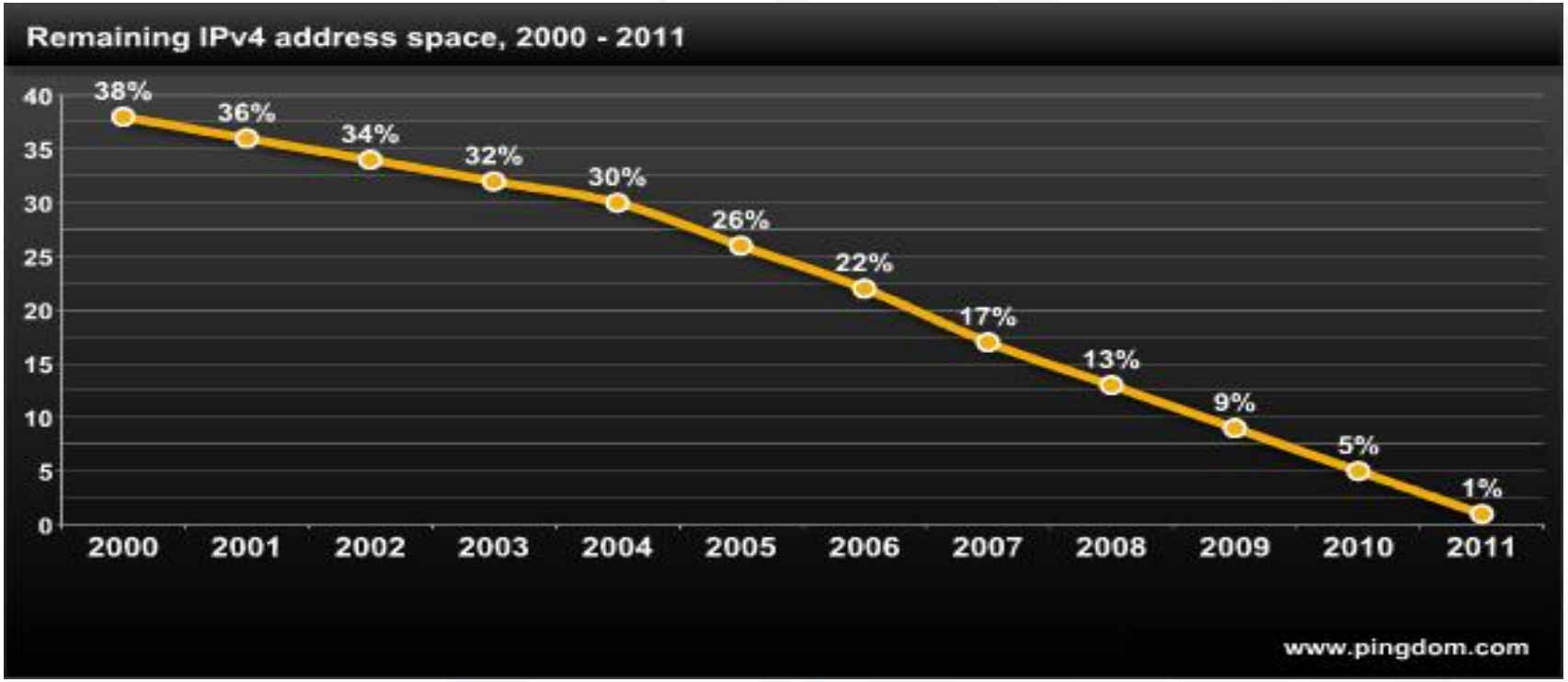
- **Future Outlook**
  - **UK-Irl inter-federation**
    - ✓ Focusing on SAML 2 compliant entities that are members of a single federation
    - ✓ Metapress
    - ✓ Second preference to becoming direct Edugate members
    - ✓ July2011 earliest estimate.

Shibboleth Access

- **Future Outlook**
  - **SAML2 becoming widespread across sectors**
    - ✓ Now part of Microsoft's services
    - ✓ In use by Google (Google Apps)
    - ✓ Cloud providers adopting
    - ✓ Leading IT security companies advocating it for cloud

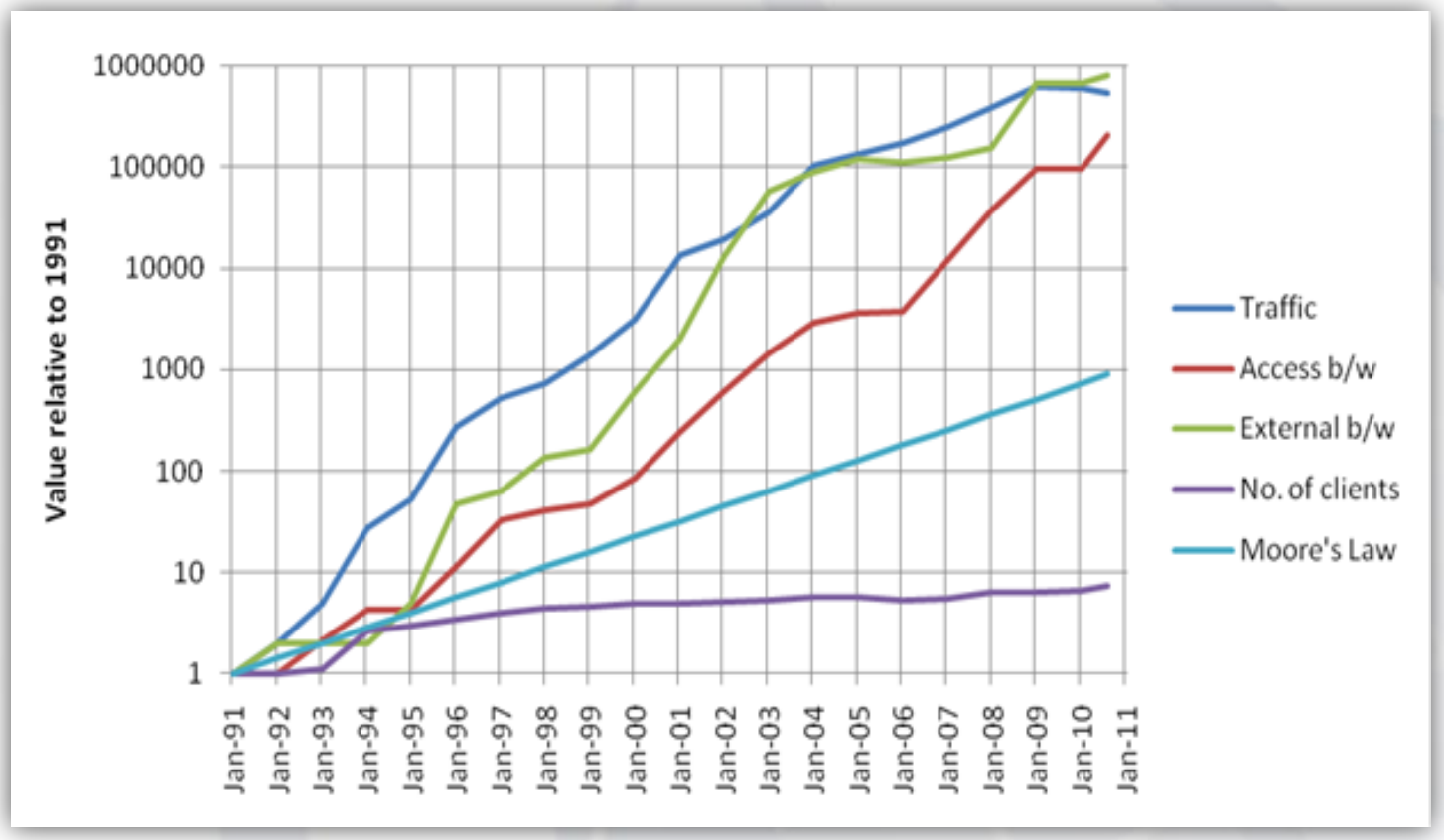
Shibboleth Access

- **Future Outlook**
  - IPv4 Address depletion



Shibboleth Access

- **Future Outlook**
  - More and more off-campus users



Shibboleth Access

- **Future Outlook**
  - **Google continues to be ingrained as...**

    "the internet"

    - ✓ Google (not scholar) search results that return results from publisher abstracts can bring user to institutions login page.
    - ✓ Even students who have heard of Google scholar are not aware that they can configure their institution
    - ✓ Anecdotal evidence that some students and staff are paying for content that has already been subscribed to.

Shibboleth Access

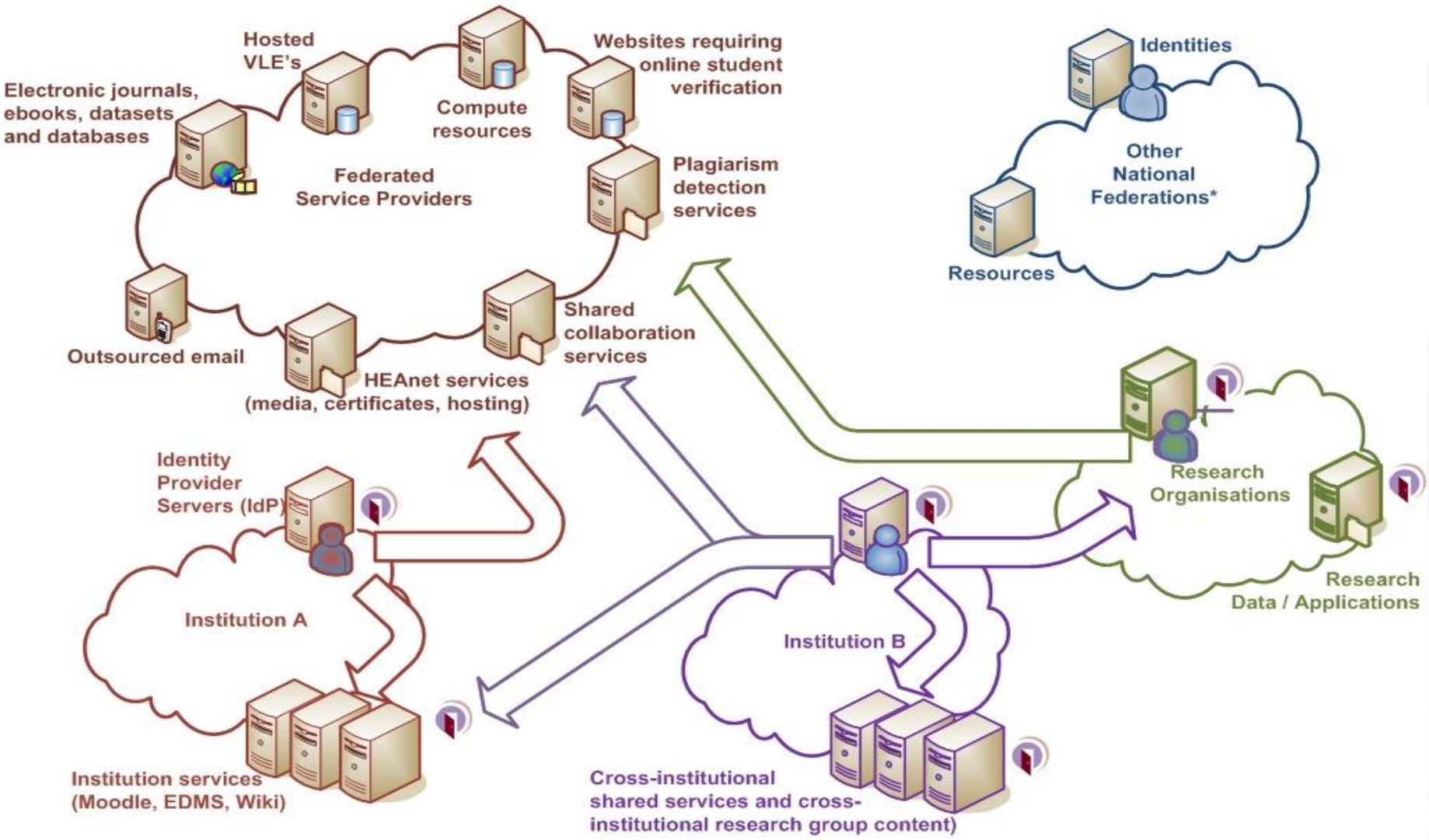
- **Future Outlook**
  - **Single Sign On expected**
    - ✓ Users who use the ‘facebook’ or ‘Twitter’ login, expect to be asked only once a day (or session) for their student/staff username and password
    - ✓ What is the rate of attrition for the web-opac, LMS etc?

Edugate

Edugate

- Why HEAnet
- How it works
- Benefits
- Who's a member
- What it takes to join
- Technical information
- Implementation options

Edugate


Hosted VLE's
Websites requiring online student verification
Electronic journals, ebooks, datasets and databases
Compute resources
Federated Service Providers
Plagiarism detection services
Identities
Other National Federations*
Resources
Outsourced email
HEAnet services (media, certificates, hosting)
Shared collaboration services
Identity Provider Servers (IdP)
Research Organisations
Research Data / Applications
Institution A
Institution B
Institution services (Moodle, EDMS, Wiki)
Cross-institutional shared services and cross-institutional research group content)

Edugate

Why HEAnet?

- NREN counterparts are federation operators
- Intra-institution collaboration
- Synergy with eduroam
- Shared services platform
- IPv4 / IPv6

Edugate

How it works

1. IdP authenticates its users, and asserts identity

- ✓ Single password -> potential for strong authentication
- ✓ Password exposed to minimum services
- ✓ Users can be offered consent prompt
- ✓ Re-useable session (SSO)
- ✓ Reduces import/export sharing of data on campus

2. Service Provider authorises access to its services

- ✓ Authorisation based on asserted identity attribute (user, role, org)
- ✓ Service provider does not issue passwords, and does not need to provision accounts in advance
- ✓ Service provider can build long-lived account around federated account

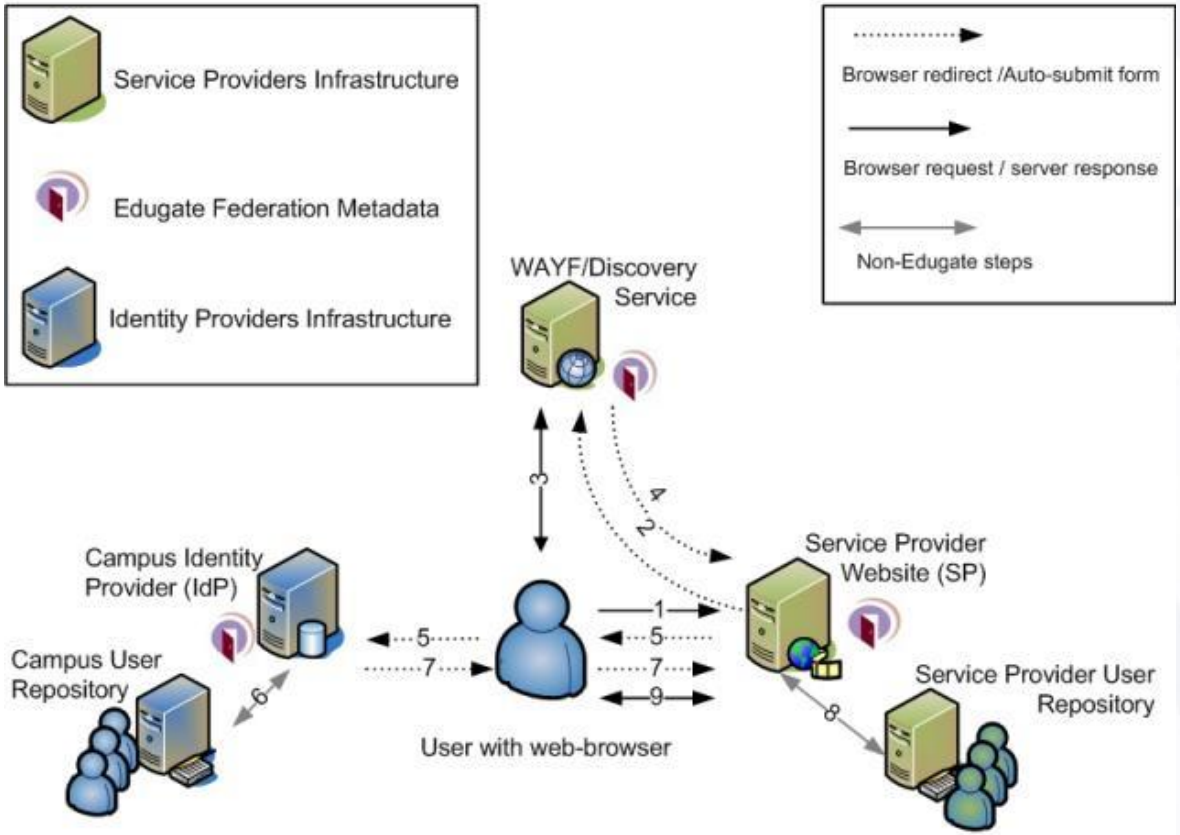
Edugate

How it works

1. Institution joins Edugate, sets up IdP service
2. Publisher invited (or contracted) to join (by whom?)
3. Federation operator refreshes metadata
4. User can access service

Edugate

How it works



Edugate

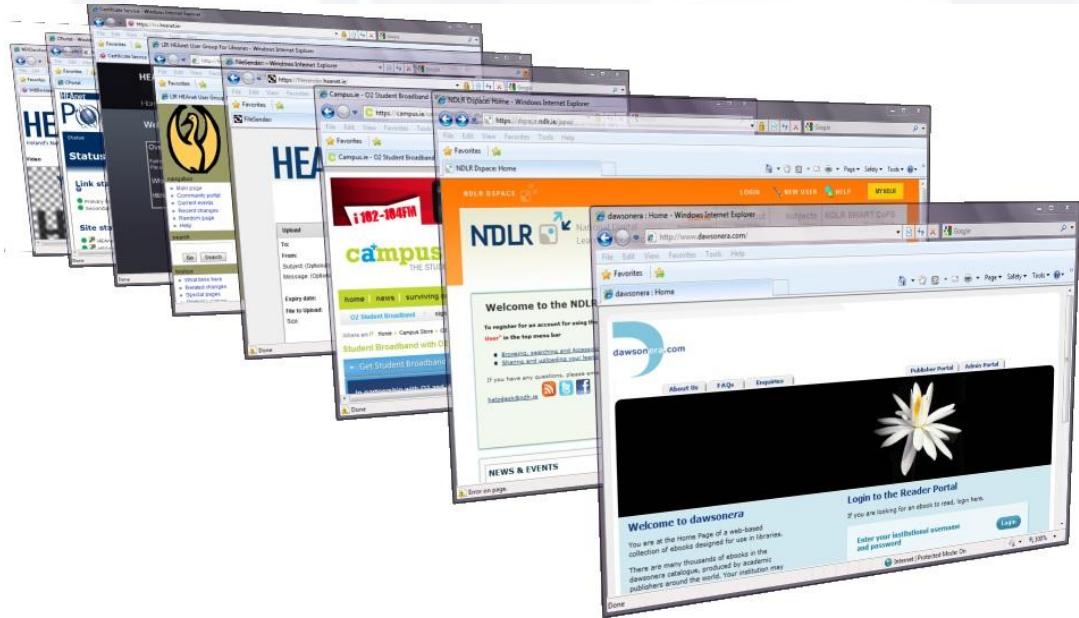
- **Benefits for libraries**
  - Single-Sign-On *not* Single-Log-On
  - Solution for the "*Googlers*" and "*bookmarkers*"
  - Helps with licence compliance
  - Potential to limit access by groups/role
  - Content delivered direct from publisher to browser
  - An institution-wide shared service (inst. repositories too)
  - Prepared for future IP migration
  - Personalisation capability (saved search, abstracts, favs)
  - Less abuse of accounts, less need for guest accounts
  - Less passwords, less prompts

Edugate

- **Benefits for libraries**
  - **Access options**
    - ✓ On campus using IP address as before
    - ✓ On campus using Shibboleth and URL change*
    - ✓ Off campus using Shibboleth protected proxy
    - ✓ Off campus by direct access to publisher
    - ✓ Off campus via Google search result
      - **http://search.proquest.com.remote.dcu.ie/login...*
      - *http://search.proquest.com/WAYF?target=idp.dcu.ie...*

Edugate

- **Who's a member**
  - **Service Providers**
    - ✓ Dawson, Thomson-Reuters, eBrary
    - ✓ 20+ others non-publishers
  - **Identity providers**
    - ✓ 80% of HEI's



www.edugate.ie

Edugate

- **Potential and current members**
  - Institutional services
    - » *Any website requiring a login [for non-campus users]*
  - Shared services
    - » *HEAnet services, An Cheim services, IReL, NDLR*
  - Academic content
    - » *Publishers (EBSCO, Elsevier, JSTOR) and databases*
  - Research portals
    - » *Or any cross-institutional research group resource*
  - Organisations offering academic discount
    - » *Microsoft Dreamspark, o2, Travelcard*

Edugate

- **What it takes to join**
  - **Service Providers**
    - ✓ Must provide service of benefit to staff/students
    - ✓ Or be contracted provide service to institution
      - *(e.g. IReL model license, or at the request of a dept)*
    - ✓ Complete Edugate agreement
    - ✓ Add support for Shibboleth2/SAML2 if not supported
    - ✓ Exchange metadata
    - ✓ Declare attribute requirements

Edugate

- **What it takes to join**
  - **Identity providers**
    - ✓ Must be part of HEAnet (mostly publicly funded HEI's)
    - ✓ Complete membership agreement
    - ✓ Deploy Identity Provider (IdP) service, connect to user repository such as LDAP, Active Directory, or a DB
    - ✓ Exchange IdP metadata with Edugate
    - ✓ Release any required user attributes
    - ✓ Offer service to departments (e.g. Library).

Edugate

- **What it takes to join**
  - **Once service is offered by IT department, library can avail of Edugate.**
    - ✓ Protect proxy or LMS with Shibboleth IdP
    - ✓ Amend A-Z URL's or LMS embedded links
    - ✓ Request publisher to join Edugate or support SAML2

      (or)
    - ✓ Advise publisher of intent to use Shibboleth
    - ✓ Release any required user attributes *where reqd*

Edugate

- **Technical information**
  - **Edugate protocol is SAML2, specifically SAML2int**
  - **Edugate attribute schema is subset of eduPerson**
    - ✓ Attribute schema describes a user
    - ✓ Includes firstname , surname, email and organisation
    - ✓ Includes federated version of local users ID
      - *Joebloogs-245@cit.ie*
      - *22ddkde949rrejde03e0dldrkre90448ew3jd*
    - ✓ Includes role (more on this)
    - ✓ Includes entitlement

Edugate

- **Technical information**
  - **Edugate attribute schema is subset of eduPerson**
    - ✓ eduPersonScopedAffiliation
      - *Staff**
      - *Student**
      - *Alum**
      - *Affiliate*
      - *Library-walk-in*
      - *Employee*
      - *Faculty*
      - *Member**

Edugate

- **Technical information**

  eduPersonScopedAffiliation

  - *Account cannot be a generic account, disabled account, or compromised account*
  - *Student must be treated as student for all campus services*
  - *Staff must be treated as staff for all campus services.*
  - *No distinction made between part-time, distance, postgrad or student enrolled in single module*

Edugate

- **Technical information**

Attribute release procedures

- *IT Department defines a default release policy for all services*
- *When new service joins Edugate, HEAnet proposes a specific policy for that service*
- *Each IT department has two weeks to approve*
- *Policy comes into affect*
- *90% of publishers require eduPersonScopedAffiliation and eduPersonTargetedID*

19/20 or HEI's release these attributes by default

Edugate

- **Implementation options**
  - Shibboleth protected proxy (days)
  - Shibboleth protected Repository (weeks)
  - Shibboleth protected LMS (cost)
  - Migrate from IP access to Shibboleth access, resource by resource*, phasing out IP. (months)
  - Access to shared services between libraries
  - COUNTER stats.

**Resources that presented a challenge, or behave poorly behind a proxy, or on mobile devices, or resources that offer enhanced features via personalisation. A-Z lists migrated first*