



# Federated Access 2.0

Glenn Wearen  
Middleware Specialist  
HEAnet

## Agenda

### 1. Federated Access 1.0

Past to current status

### 2. Federated Access 2.0

LoA, Inter-federation , confederation, vendor adoption, cloud adoption, groups, discovery UI, Non-Web-SSO, multiple protocols.

### 3. Edugate

1.0 or 2.0?

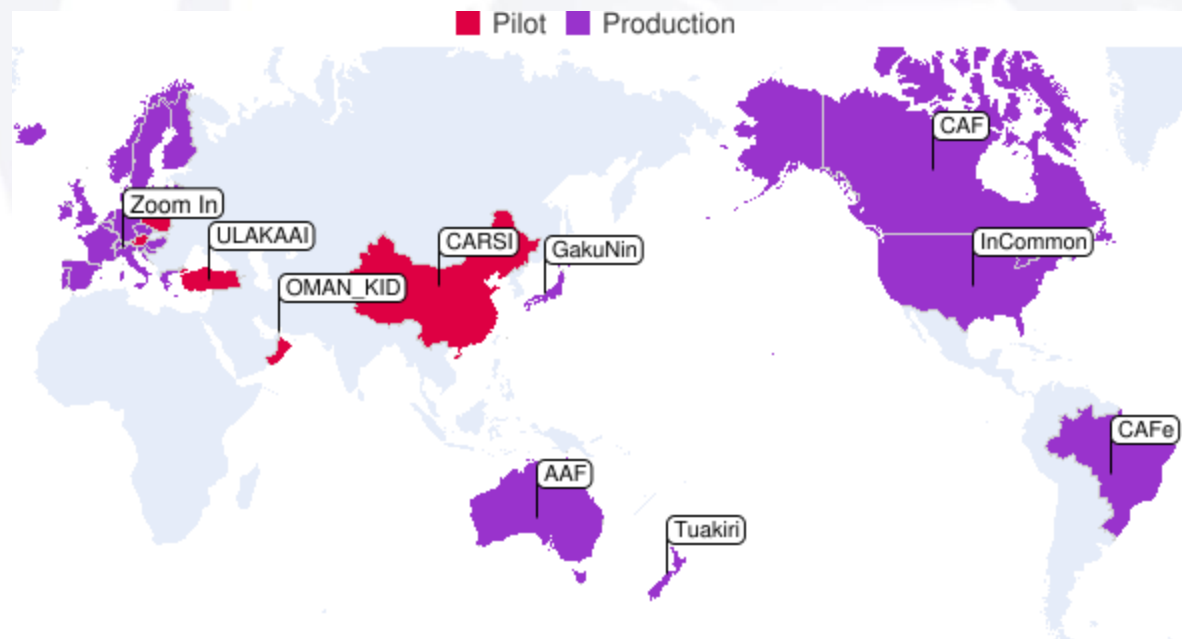
## History of Federated Access (*academic sector*)

- ✓ **2001:** Shibboleth, SAML 1.x, OASIS ID-FF V1.2 standards
- ✓ **2003:**
  1. SAML 2.0 protocol combines elements of all of the above.
  2. Feide.no federation launched (not SAML, but similar)
- ✓ **2004:** Switzerland launches AAI (Shibboleth 1.3)
- ✓ **2005:** UK Federation and InCommon launched (Shibboleth 1.3),
- ✓ **2006:** JISC announces migration from Athens to UK Federation
- ✓ **2007:** SURFFederatie.nl launched, Google Apps supports SAML
- ✓ **2008:**
  1. Shibboleth 2.0 implements SAML 2.0 as default protocol
  2. SimpleSAMLphp 1.0 released.
  3. WAYF.dk launched.

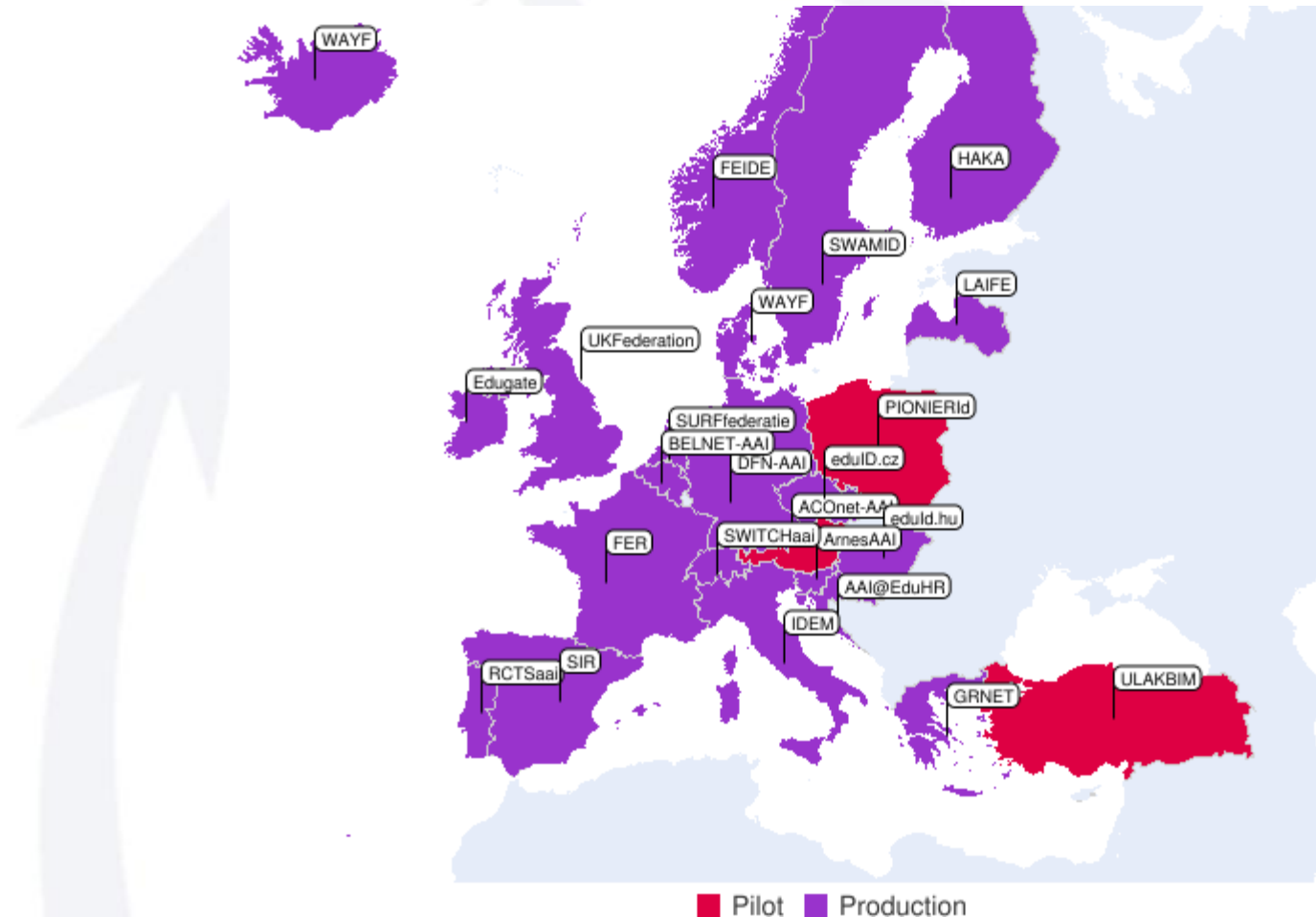
- **History of Federated Access (*academic sector*)**
  - ✓ **2009:** Edugate pilot commences.
  - ✓ **2010:** Edugate production federation launched

- **Academic Federations**

- **US:** 4 Million ID's covered
- **SWISS:** 95% of ID's
- **UK:** 850 Members



- **Academic Federations**



1. Confederation
2. Inter-federation
3. Use outside web-browser
4. Wide application support, incl. *Cloud*
5. Levels of Assurance (LoA)
6. Cross institutional group management
7. SAML Metadata extensions.
8. Reporting
9. Attribute Aggregation
10. Protocol pluralism

 **eduGAIN** Production confederation commenced April 2011

## Standard Attribute Schema

- displayName, cn, mail
- eduPersonAffiliation and eduPersonScopedAffiliation
- schacHomeOrganization and schacHomeOrganizationType

## Standard SAML Protocol (SAML2 Interoperable Profile)

- *Persistent* NameID format mandatory, support for *Transient* format optional
- Either format should be accepted by relying services.
- AuthRequests >HTTP-Redirect binding, AuthResponses using HTTP-POST
- SAML 2 Metadata standard and Discovery recommendations.

## Standard Policy

- Data Protection profile for personal and non-personal data
- Federation joins eduGAIN, federation members opt-in.



## Union

**Standards Attribute Schema**

**Standard SAML Protocol (SAML2 Int.)**
















**Opt-in model**

- 20+ IdP's
- 30+ SP's

### Kalmar Identity Providers

-  Feide - Norwegian Educational and Research
-  CSC - IT Center for Science Ltd. [ [more](#) ]
-  MDH [ [more](#) ]
-  HB [ [more](#) ]
-  UmU [ [more](#) ]
-  NORDUnet [ [more](#) ]
-  Arcada [ [more](#) ]
-  KIOLD [ [more](#) ]
-  Tampere University of Technology [ [more](#) ]
-  KAU [ [more](#) ]
-  GU [ [more](#) ]
-  UU [ [more](#) ]
-  University of Helsinki [ [more](#) ]
-  WAYF - Where are you from [ [more](#) ]

### Kalmar Service Providers

-  NIAS AsiaPortal [ [more](#) ]
-  Feide RnD Translation Portal [ [more](#) ]
-  OpenWiki [ [more](#) ]
-  SUNET E-Meeting Service [ [more](#) ]
-  University of Turku [ [more](#) ]
-  Tampere University of Technology [ [more](#) ]
-  CLARIN Service Provider Federation/MPI [ [more](#) ]
-  SWAMID Test SP [ [more](#) ]
-  NORDUnet TV [ [more](#) ]
-  Feide RnD Blog [ [more](#) ]
-  SUNET Lobber (BETA) [ [more](#) ]
-  University of Helsinki [ [more](#) ]
-  NORDUnet Tools [ [more](#) ]
-  Tampere University of Technology [ [more](#) ]
-  CSC - IT Center for Science Ltd. [ [more](#) ]

## 2. Inter-federation

- **Technically similar to confederation**
- **Bilateral agreement between two federations.**
  - ✓ Members Opt-in (or opt-out)
  - ✓ UK-Ireland under investigation

### 3. Wide application support

- Google Apps, Salesforce.com since 2009
- Microsoft Live@edu via WIF since 2010
- More recently...
  - ✓ WebEx, Workday & Zendesk
- SAML recommended
- Account provisioning still proprietary
  - ✓ SCIM proposed by Ping ID and others to standardise account provisioning using choice of REST & SAML



### 3. Wide application support

- **MS ADFS can be configured with SAML IdP's**
  - ✓ Opens up SAML access to Sharepoint and Dynamics CRM
- **Microsoft WIF SAML 2 support in Beta**
  - ✓ No need for ADFS gateway to federated Sharepoint
- **Blackboard join InCommon**

## 4. Use outside browser

### – Networks

- ✓ NAC, SSL VPN, Web-redirect based wifi

### – Desktop clients

- ✓ OpenSSH, Jabber

### – 1.0

- ✓ browser plugin ( Mindterm SSH applet)

### – 2.0

- ✓ GSS-API or GSS-SASL
- ✓ SAML Attributes conveyed within protocol messages.



## 5. Levels of Assurance

- **InCommon Bronze and Silver**

- ✓ Align with ICAM\* Bronze/Silver.

- **WAYF.dk approximates to NIST levels 1-4**



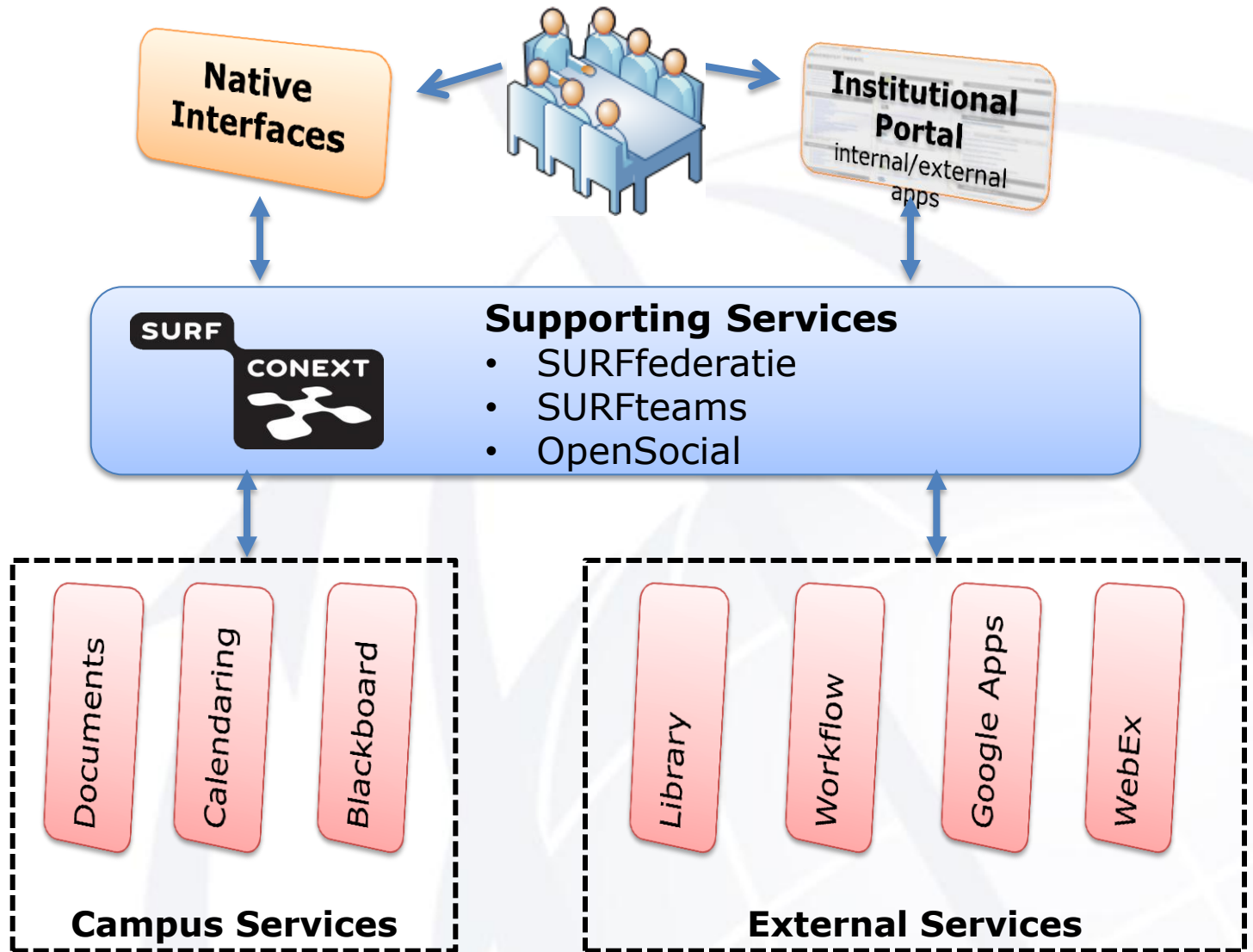


## 6. Cross institutional group management

- How can an identity provider assert that a user is a member of a cross institutional group that the identity provider doesn't control?
- How can a service provider create a group from identities that reside at different institutions?

What about cross-federation groups?

# Federated Access 2.0



## 7. User experience

### – Metadata

- ✓ Logo
- ✓ Requester

### – Standard

- ✓ 'Login'
- ✓ Discover
- ✓ List
- ✓ Institution



s

privacy URL

page.

incremental search  
of requester

# 8. Repo

– Ide

– Ser

- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓
- ✓

http://localhost:8112/raptor-web/spring/reports?execution=e3s3
java virtual file system

RaptorWeb Statistics Viewer
HIBERNATE - java.lang.NoClassDe...

Cardiff Universitys MUA	
Statistic	Modify
<a href="#">Number of authentications over defined interval</a>	
<a href="#">Number of authentications grouped by particular field</a>	
<a href="#">Number of authentications over defined segments</a>	
<a href="#">Number of authentications per school</a>	
<a href="#">Comparison of authentications for particular Service Providers</a>	
<a href="#">Number of authentications per affiliation type</a>	

**Options**

**Statistic Name:** Number of authentications grouped by particular field

**Event Type:** Shibboleth

**Resource Category:** All

**Start Time:** 01/10/2010 14:00

**End Time:** 20/01/2011 17:00

**Parameters:** Group By Field:

**Graph Title:** Number of authentications grouped by

**Postprocessors:** SortGroupsAlphabeticallyPostProcessor

No.	Series Label	Filter	Remove
0	Number of authentications	+	×

Processing Status: Done

Graph
Table
Download

### Number of authentications grouped by

Time

■ Number of authentications

## 9. Attribute aggregation

- The institutional account is but one part of the a users digital identity.
- ✓ Shouldn't a user be able to self-assert attributes from non-institutional account?

 [Glenn.wearen](#)

 [Glennamddy](#)

 [glennwearen@gmail.com](mailto:glennwearen@gmail.com)

 <http://ie.linkedin.com/in/glennwearen>

## 10. P

Kim Cameron's

### Laws of Identity

#### 1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

#### 2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

#### 3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

#### 4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

#### 5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

#### 6 Human Integration

The universal identity metasytem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

#### 7 Consistent Experience Across Contexts

The unifying identity metasytem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.



Flickr: Alatan

- ✓ Confederation
- ✓ Inter-federation
- ✓ Use outside web-browser
- Wide application support, incl. *Cloud*
- Levels of Assurance (LoA)
- Cross institutional group management
- ✓ SAML2 and SAML2 Metadata extensions.
- ✓ Reporting
- Attribute Aggregation
- Protocol pluralism



## **Local implementation of Federated Access**

## Edugate

1. Funding
2. Find early adopters
3. Switch to production

## 1. Funding

- ✓ Long lasting research infrastructure
- ✓ ...needs a long lasting identity access system
  - *Establishment of identity service at each institution must have local campus benefits to ensure longevity*



e·INIS

The Irish National e-Infrastructure

## 2. Find early adopters

### – Extol the benefits of Federated Access

- ✓ Diverse range of identity providers
- ✓ Campus IDM first concern, intra-campus secondary.
  - *Initial effort to deploy IdP services HEAnet's part.*

### – Find applications

- ✓ HEAnet's own web applications (TCS, Media)
- ✓ Web applications open to large range of institutions
- ✓ Web applications that participate in other federations
- ✓ Services suffering from **high user attrition**
  - *'Register here' / 'forgot password', infrequent use*

- **Extol Benefits for identity providers**
  - **Add value to existing user account**
    - ✓ Multiple accounts => low value placed in account
  - **Potential to use identity for;**
    - ✓ Cloud services, Shared services
    - ✓ Alliances
    - ✓ Campus Single-Sign-On
  - **Potential for strong password policy or two-factor authentication, less handling of passwords**
  - **Helpdesk costs reduced / productivity gains**

- **Extol Benefits for service providers**
  - ✓ Standard platform for your *service* to access market
  - ✓ Potential to re-use your implementation worldwide.
  - ✓ Improved service offering for users
  - ✓ Digital ID card Vs. Physical ID card
  - ✓ Distinguish staff from student and 6 *others*
  - ✓ Personalisation capability (personal or non-personal)
  - ✓ Use as one-time provisioning or validation system
  - ✓ Use as just-in-time access system.

### **3. Switch to production**

- 1. Establish Governance Committee**
- 2. Define Member agreement, attribute schema**
- 3. Establish production infrastructure**
- 4. Sign-up members**
- 5. Launch service**
- 6. Migrate pilot participants (October 2011)**
- 7. Deploy new IdP's, support new Service Providers**
- 8. Gain critical mass (+50% of identities).**

## **Service Provider production joining steps**

- Must provide service of benefit to staff/students
- ...or be contracted provide service to identity member
- Complete Edugate membership contract
  - ✓ Identities must be used for AuthZ/AuthN
- Pay the membership fee of €1
- Add support for Shibboleth2/SAML2
- Decide and declare attribute requirements

## **Identity providers production joining steps**

- **Must be part of HEAnet (except schools)**
- **Complete membership agreement**
  - ✓ Account cannot be a generic shared account, disabled or compromised account
  - ✓ Student must be treated as student for all campus services.
- **Deploy SAML2 Identity Provider service**
- **Decide what user attributes to release**
- **Offer service to departments**

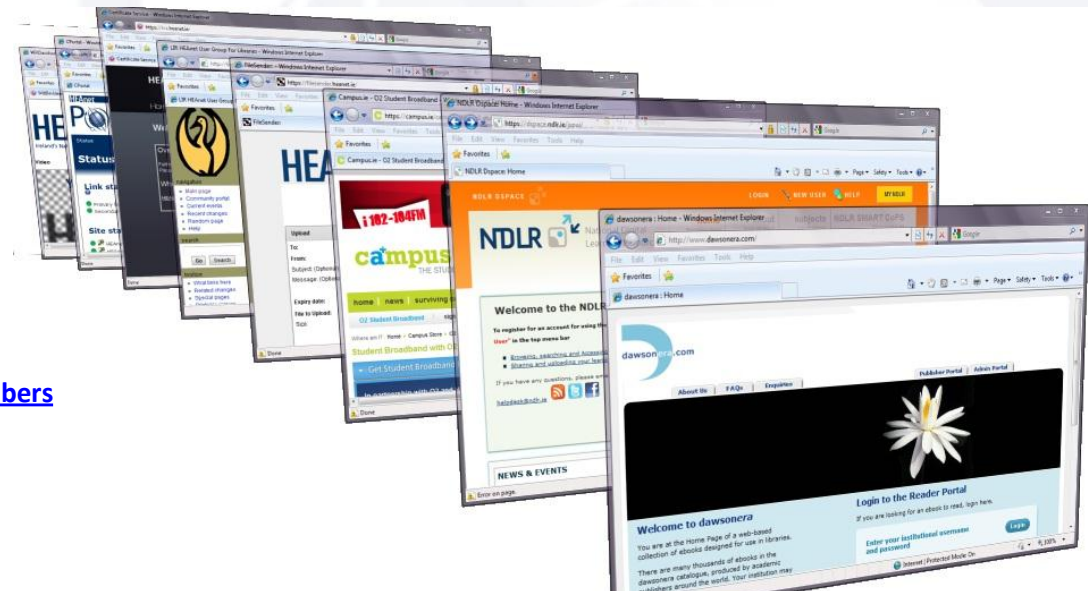
## Current status

### – Service Providers

- ✓ 20+ providers, 1 using Edugate for student discount

### – Identity providers

- ✓ 80% of HEI's, 100% target for September 2011



<http://www.edugate.ie/content/edugate-federation-members>

## Edugate

1. Funding
2. Find early adopters
3. Switch to production
4. Add 2.0 features where there is demand

- Confederation
- ✓ Inter-federation
- Use outside web-browser
- Wide application support, incl. *Cloud*
- Levels of Assurance (LoA)
- Cross institutional group management
- ✓ SAML Metadata extensions.
- ✓ Reporting.
- Attribute Aggregation
- Protocol pluralism

- **Conclusion**
  1. **Federated Access is maturing**
    - ✓ 2.0 is not far from here
  2. **Edugate**
    - ✓ 1.0 Federation but using SAML2.

