

# Managing identities

TICAL 2012, Lima, Peru

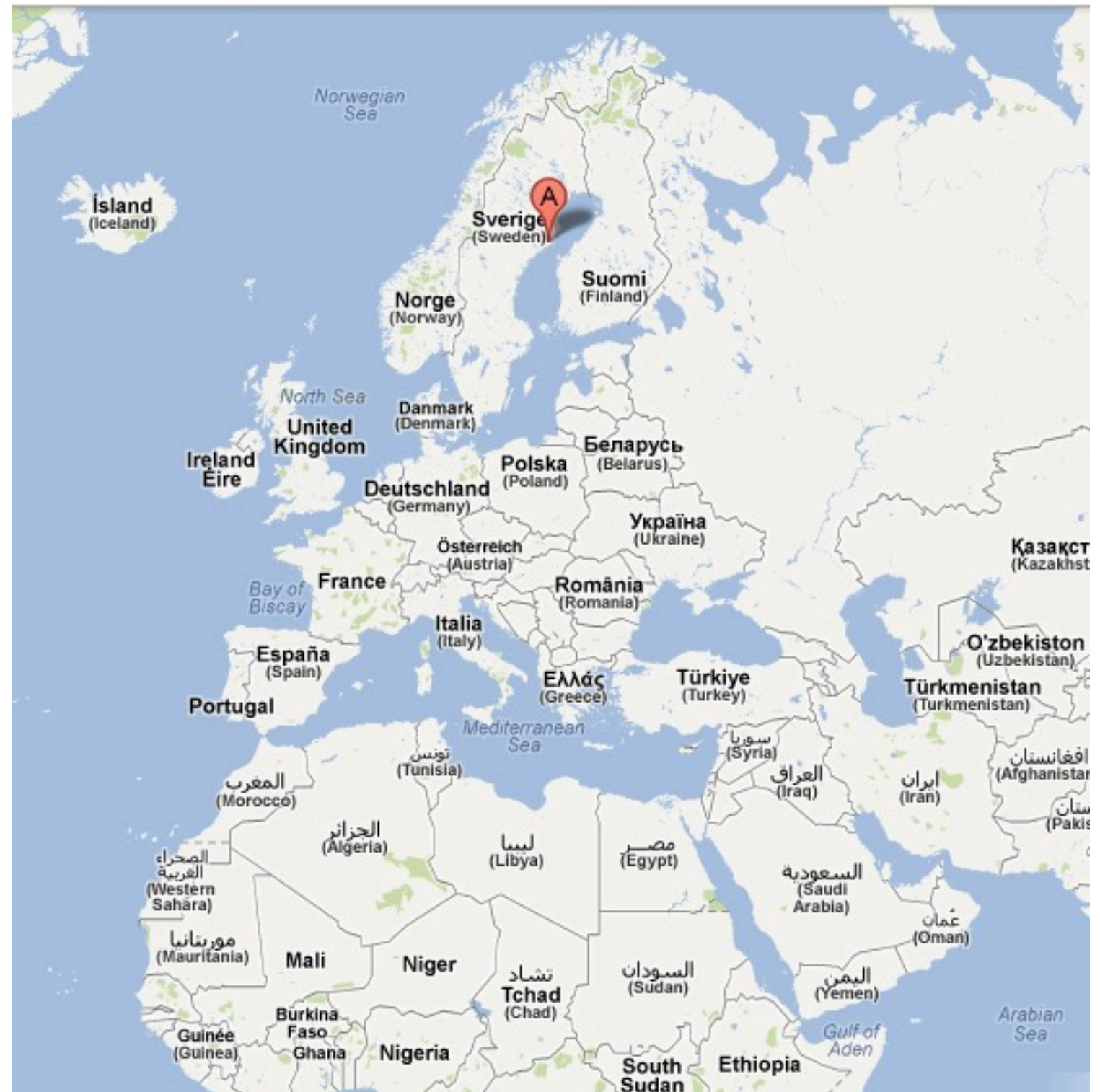
Roland Hedberg <[roland.hedberg@adm.umu.se](mailto:roland.hedberg@adm.umu.se)>

# Who am I ?

- Got into networking in 1987
- Managed computer networks and network applications
- Worked with standardisation of directory technologies
- Software developer/Senior researcher

# Umeå, Sweden

Latitude: 63° 50' North  
Longitude: 20° 15' East



# Topics

- Why
- How
- Future

# What's an identity ?

# What's an identity ?

”The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.”

# What's an identity ?

”The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.”

# What's an identity ?

”The collective aspect of the set of characteristics by which a thing is definitively recognizable or known.”

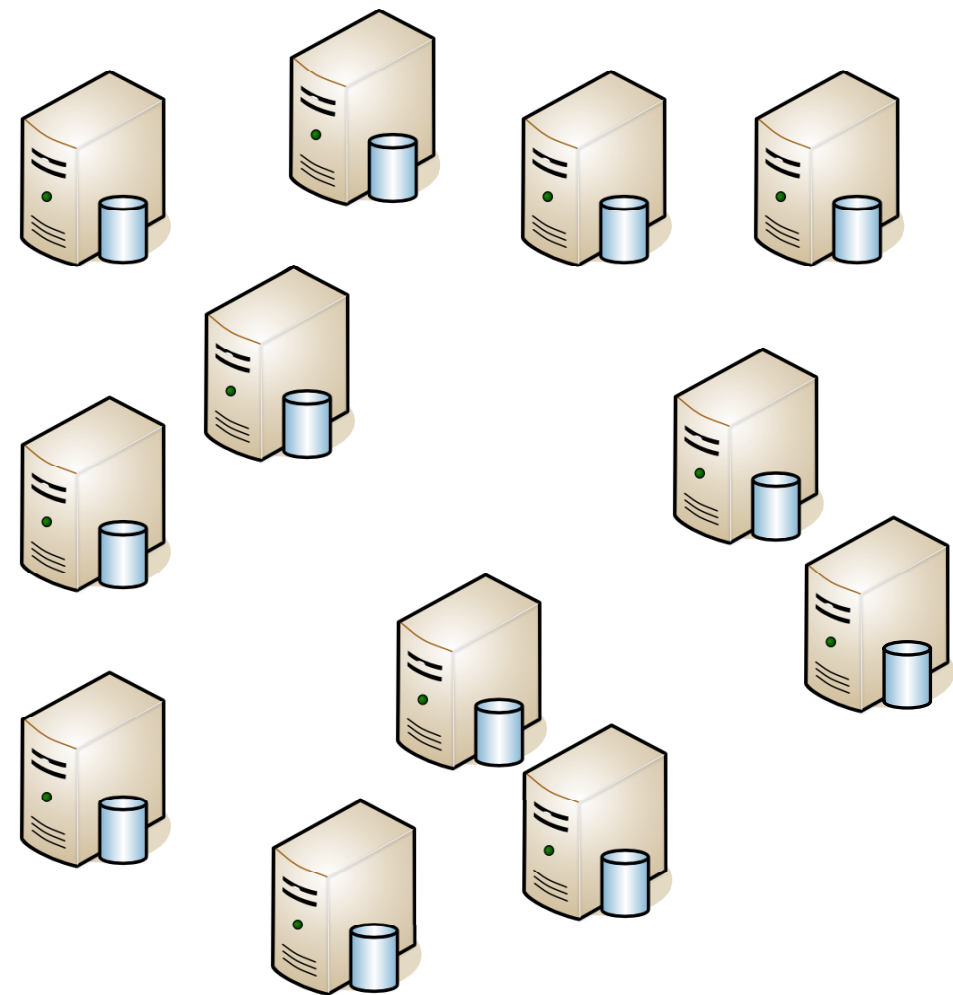
A set of attributes and values



# Why ?

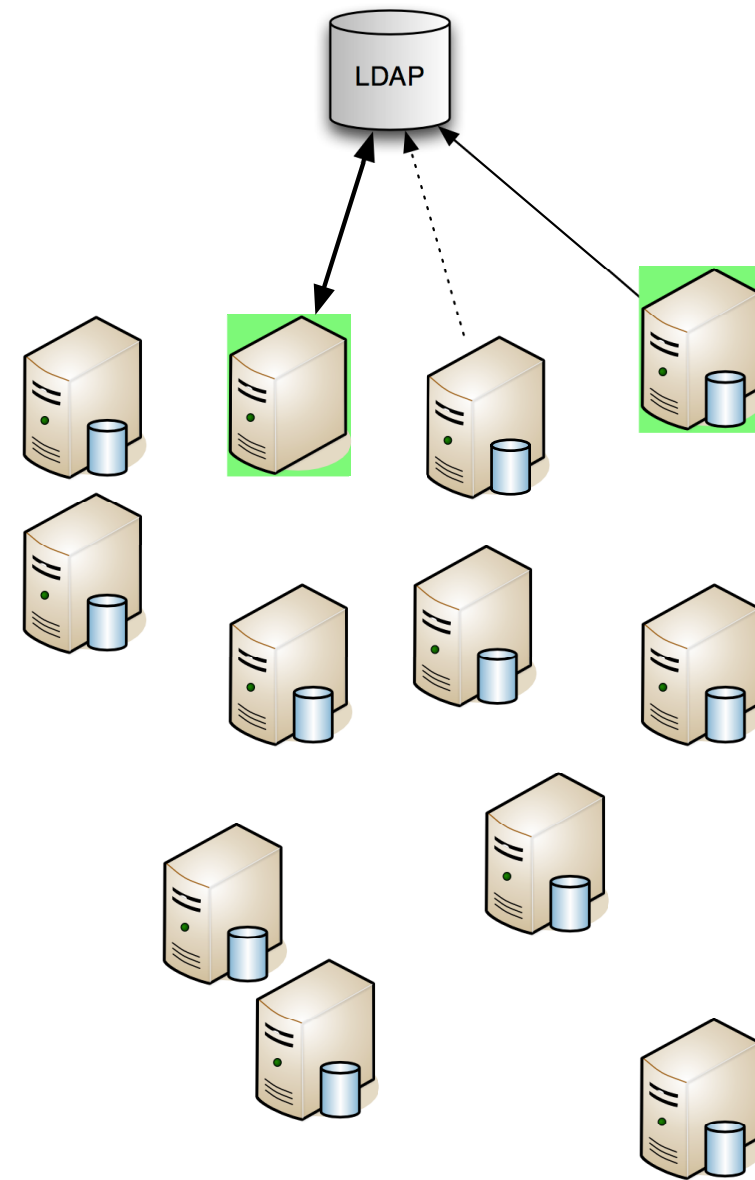
# Historic progression late '80

- A set of completely autonomous systems



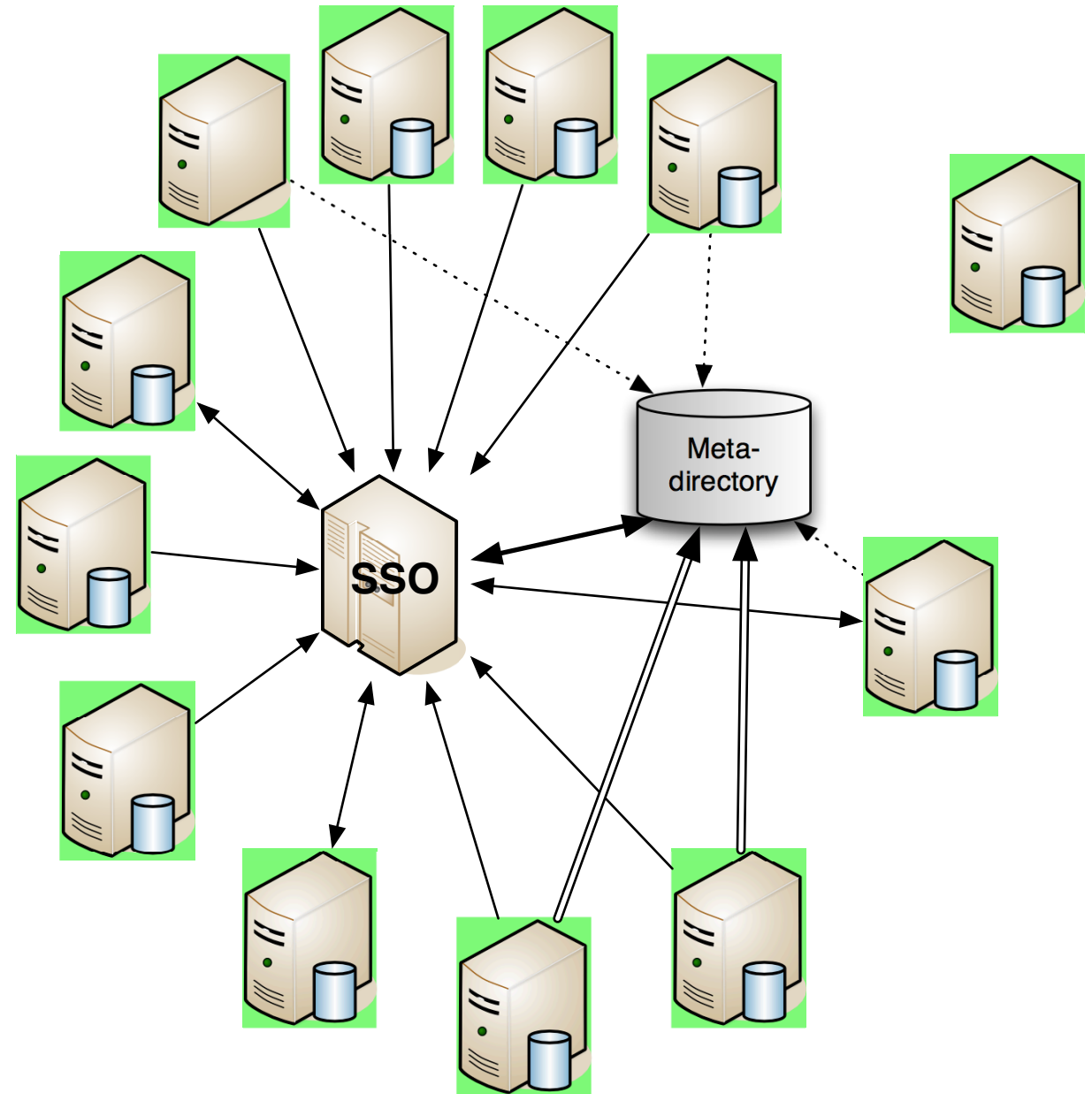
# 1st transition

- mid '90
- Some know how to use LDAP
- LDAP is populated manually



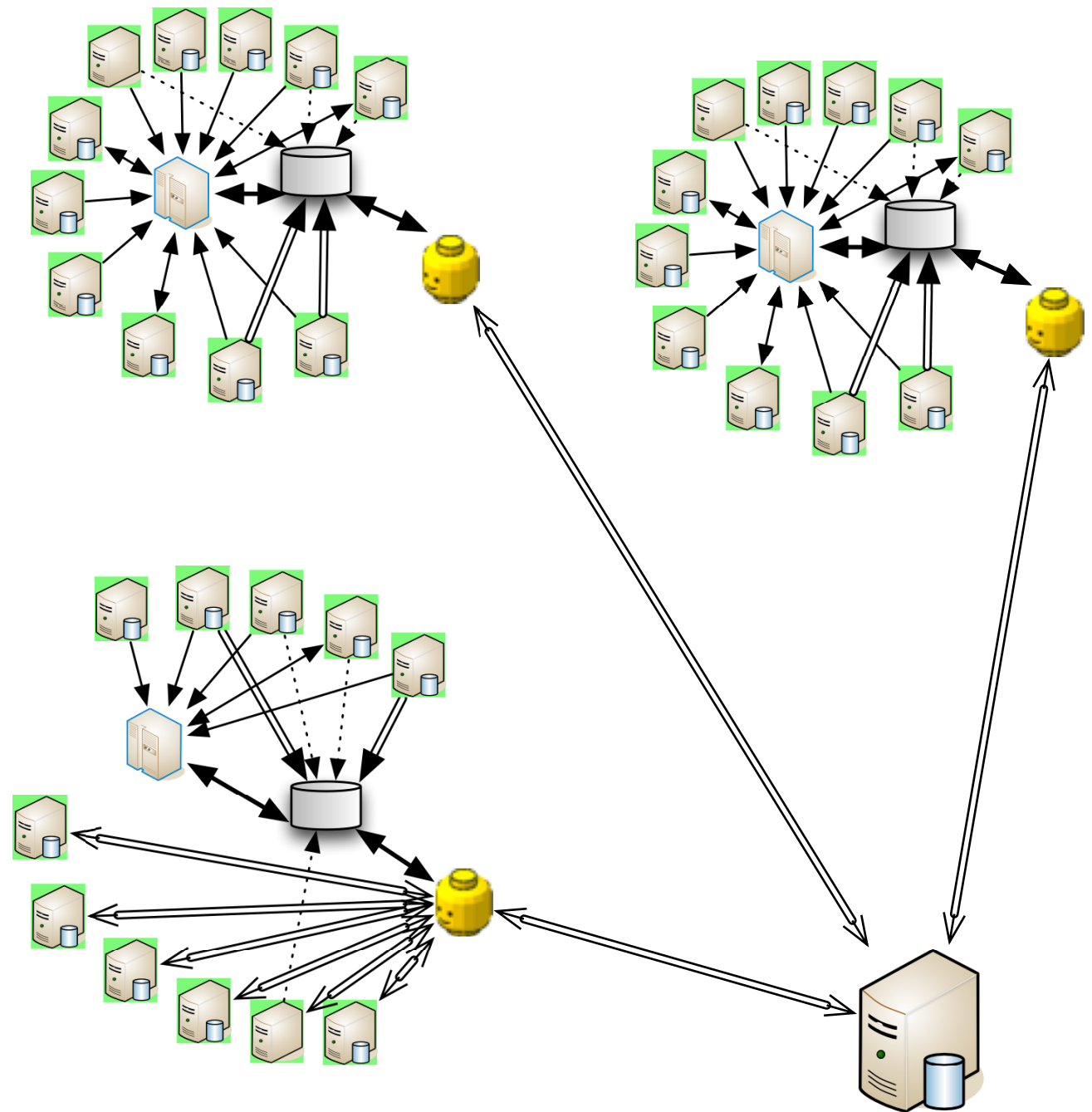
# 2nd transition

- 2007
- Single-Sign-On ubiquitous in-house
- Extra info from LDAP



# 3rd transition

- today
  - Identity federations
    - SAML
    - Eduroam



# IdPs over the world as seen from Norway

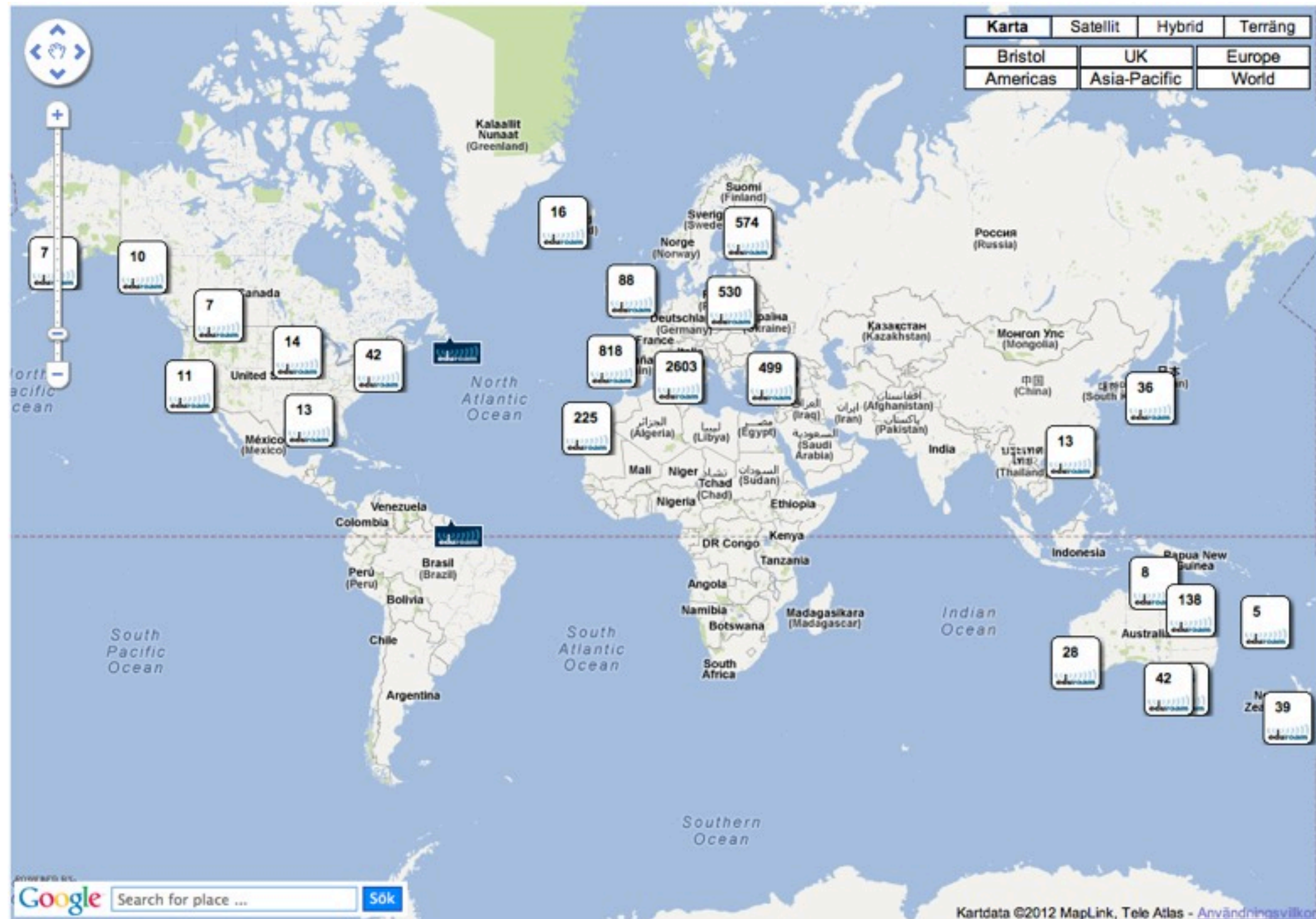


# Driving forces

- 1st & 2nd transition
  - Centralized cheaper than decentralized
- 3rd transition
  - User convenience and economy of scale



# Eduroam





# Eduroam status

- 43 member NROs
- > 5300 service locations + 400 (Au, Nz)
- 250 M successful authN (~6% international)  
may 2011 - april 2012
- eduroam is ranked as 27th most widely used SSID (5th most frequent operator SSID)

# Why !

- Enables trustworthy exchange of information between federations
- Reduces the costs of developing and operating services
- Improves the security and end-user experience of services
- Enables service providers to greatly expand their user base
- Enables identity providers to increase the number of services available to their users

# How

**SWAMID** offers quality assured and secure identification of employees, students, alumni and other associated in higher education in Sweden, in the Nordic countries, in the rest of Europe and also in North America and Asia.

The **eduGAIN** service is intended to enable the trustworthy exchange of information related to identity, authentication and authorisation between the GÉANT (GN3) Partners' federations.

**InCommon** provides a secure and privacy-preserving trust fabric for research and higher education institutions, and their partners, in the United States.

SWAMID offers quality assured and secure identification of formal and informal learning and other associated information in the Nordic countries, in the rest of Europe and also in North America and Asia.

**quality assured**

The eTrust project provides a trustworthy identity, authentication and authorisation between the GÉANT (GN3) Partners' federations.

**trustworthy exchange**

InCommon provides a privacy-preserving trust fabric for research and education institutions, and their partners, in the United States.

**trust fabric**

# TRUST

# Federation policies

- SWAMID Federation Policy v2.0
- SWAMID Basic Identity Assurance Profile v1.0
- SWAMID eduroam Technology Profile v1.0
- SWAMID SAML WebSSO Technology Profile v1.0

# Explicit trust

- Kantara Identity Assurance Framework (IAF)

<http://kantarainitiative.org/confluence/display/idassurance/Home>

- Common Organizational Service Assessment Criteria
- Operational Service Assessment Criteria



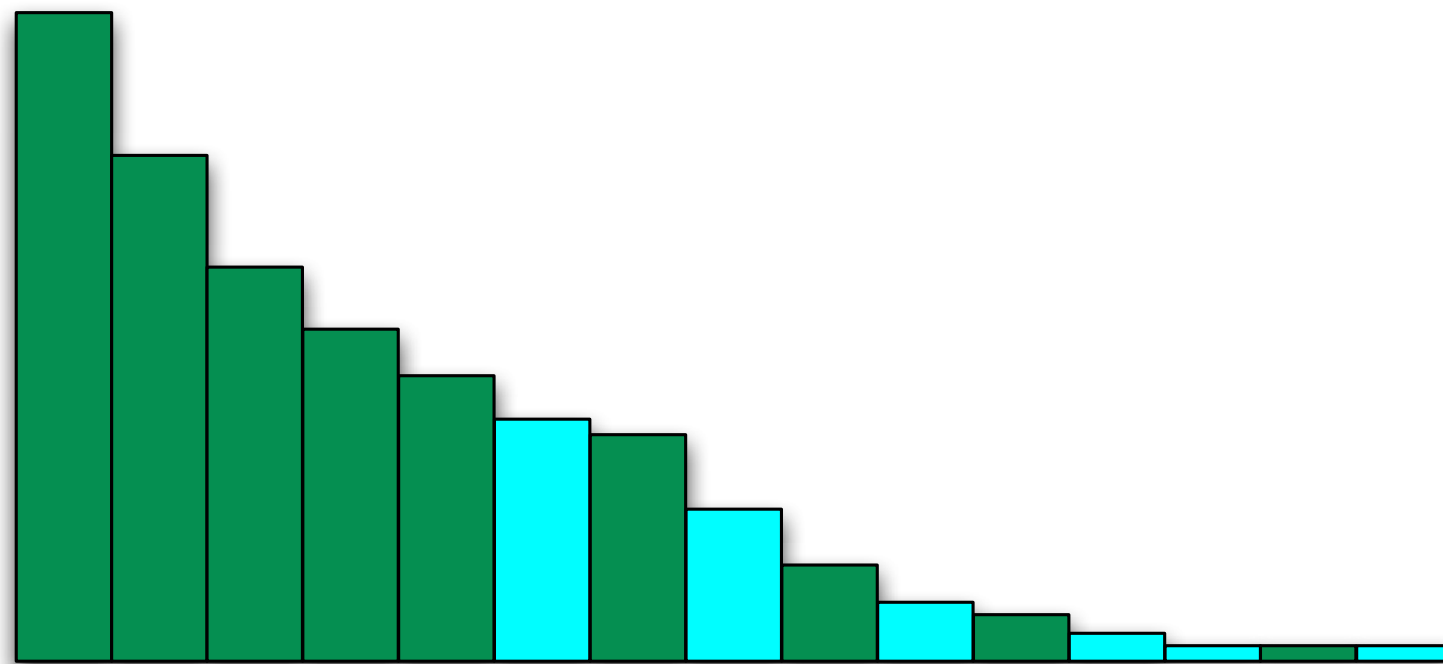
# Trust in Security environment

- IdM checklist

# Some outstanding issues

# Problem of scale

- A few services has many users
- Many services has few users



# Which identity provider to use ?

- OpenID NASCAR problem
- Where Are You From (WAYF)



# Attribute releases

- Specific for every Identity - Service provider pair
- Solution
  - Service categories

# Service examples

# SWAMID coverage

- All universities with more than 1000 FTE students are part of SWAMID
- ~ 97 % of all students and employees

# Studera.nu

**studera.nu**  **Sök**  **ANTAGNING.SE** >>

**STARTSIDA** **SÖK OCH JÄMFÖR UTBILDNING** **HÖGSKOLEPROVET** **STUDERA PÅ DISTANS** **STUDERA UTOMLANDS** **OM STUDIER**

## Sök och jämför utbildning

### Enkelt att jämföra utbildningar!

Med Sök och jämför utbildning kan du söka fram olika utbildningsalternativ efter intresseområde och jämföra bredvid varandra.

Du får information om utbildningen, högskolan och arbetsmarknaden.

Utsökningen kan du spara för att återkomma till.

När du bestämt dig finns en genväg till den utsökta utbildningen i VHS anmälan på Antagning.se.

[Välj med Sök och jämför »](#)

[Logga in och anmäl dig på Antagning.se »](#)







# NyA-webben

## Student administration

- Student admission system
- Base user
  - "urn:mace:swami.se:gmai:nya-dw:base:o=YY"
- Department user
  - "urn:mace:swami.se:gmai:nya-dw:department:o=YY:norEduOrgUnitUniqueNumber=ZZZZ"

# Adobe Connect


ADOBE® CONNECT™

swamid

☐ Enter as a Guest

☒ Enter with your login and password

Login SWAMID

 SUNET

[Help](#)

Copyright © 2001 - 2011 Adobe Systems Incorporated and its licensors. All rights reserved.

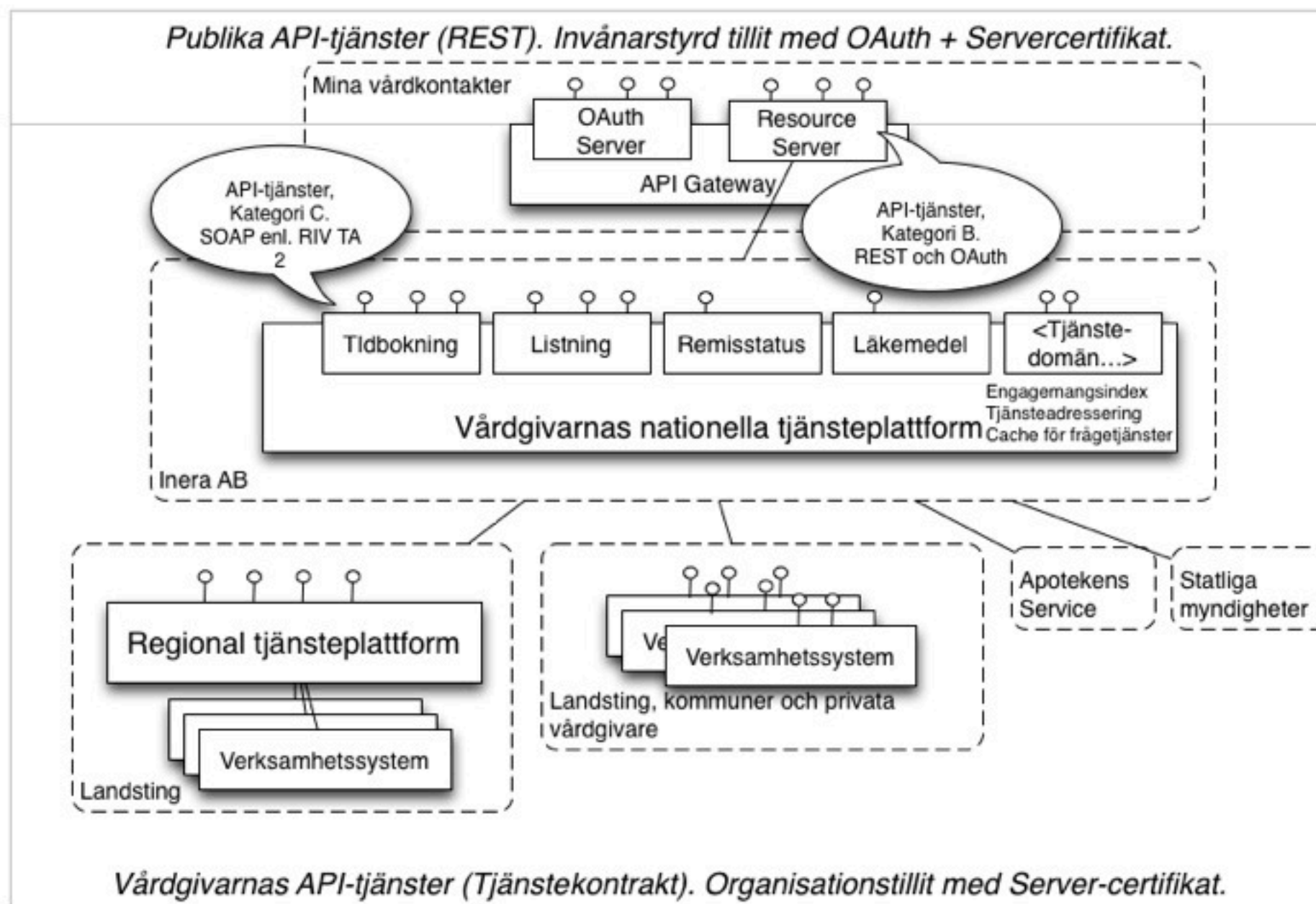


Feedback

# BOX.COM

















- Business agreement between SUNET and BOX.COM

# Hospital contact



# Foodl

<https://foodl.org/>

Mitt svar							Alla svar	Diskussion (0 inlägg)	Groups
	Namn	Fri 1. Jun 10:00-11:00	Mon 4. Jun 10:00-11:00	Tue 5. Jun 10:00-11:00	Wed 6. Jun 10:00-11:00	Thu 7. Jun 10:00-11:00	Senast uppdaterad		
	DemchenkoYuri	✖	✖	✖	✖	🕒	19 days		
	Jan Ruzicka	✖	✅	✅	✖	✅	26 days		
	Steluta (lcat) 	✅	✖	✅	✅	✅	26 days		
	Jordi Jofre	✖	✅	✅	✅	✅	26 days		
	Mary Grammatikou 	✅	✖	✅	🕒	✅	27 days		
	Marcin 	✅	🕒	🕒	🕒	🕒	27 days		
	Elena Torroglosa (UMU) 	✅	✅	✖	✅	✅	27 days		
	Roland Hedberg 	✖	✖	✅	✅	✅	27 days		
	Constantinos Marinos 	✅	✖	✅	✅	✅	27 days		
	Stella Kafetzoglou (@skafetzo)	✅	✖	✅	✅	✅	28 days		
	Antonio David Pérez Morales 	✅	✅	✖	✖	✅	29 days		
	Stella 	✅	✅	✅	✅	✅	30 days		
	Krzysztof	✅	✖	✖	✖	✖	30 days		
	pedromj 	✅	✅	✅	✅	✅	30 days		
	Sum	10	6	9	8	11			
E-postadresser 									

# Future

# Non-web

Project Moonshot is a JANET(UK)-led initiative, in partnership with the GEANT project and others, to develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging.

# The great divide

- Higher Education and public services
  - SAML2
- Social services
  - OpenId/OAuth2/OpenId Connect



# Conclusion

- Get your identity management in order
- Document and secure your IdM process
- Join the Identity federations