

# **E-Infrastructure Security: Authentication Levels of Assurance (LoAs)**

## **– Summary of initial findings IdP/SP/Grid**

Ning Zhang, Aleksandra Nenadic, Li, Yao, Terry Morrow, Mike Jones  
the University of Manchester, UK

- Target: Service Providers, Identity Providers and Grid community

UKERNA/JANET UK

University of Cardiff

Centre for Health Informatics and Multi-Professional Education, UCL

Elsevier

National e-Science Centre, Glasgow

National e-Science Centre, Grid Security Group, Glasgow

Foundation for Research and Technology, Greece

IOP Publishing

Swets

UK Data Archive

University of Exeter

Feide (Norwegian HE federation)

CERN

Manchester Computing

CSC, Finnish IT Science Centre

SWITCH (Swiss HE federation)

University of Queensland, Australia

OCLC Inc

PsyGrid

JSTOR

Cambridge University Press

Oxford University Computing Services

MIMAS

Grid-Ireland/Trinity College Dublin

Xrefer Ltd

Taylor & Francis Group Ltd

Emerald Group Publishing Ltd

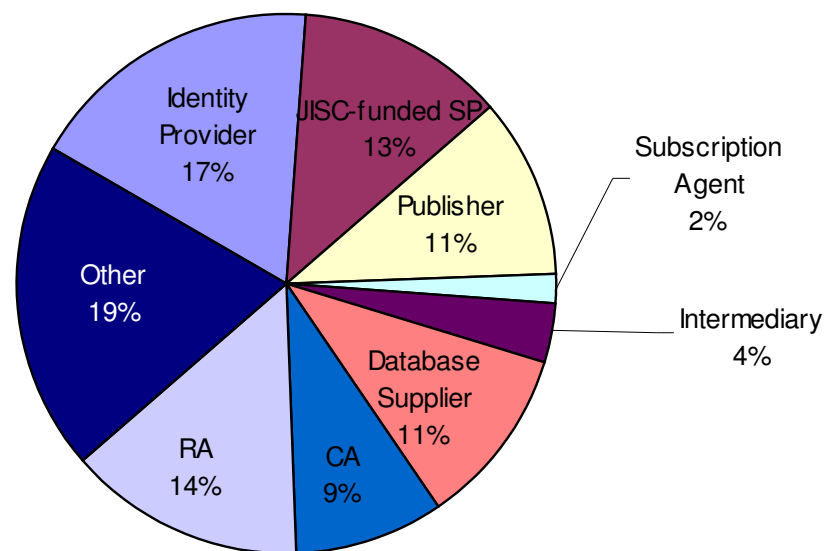
STFC

Victorian Partnership for Advanced Computing, Australia

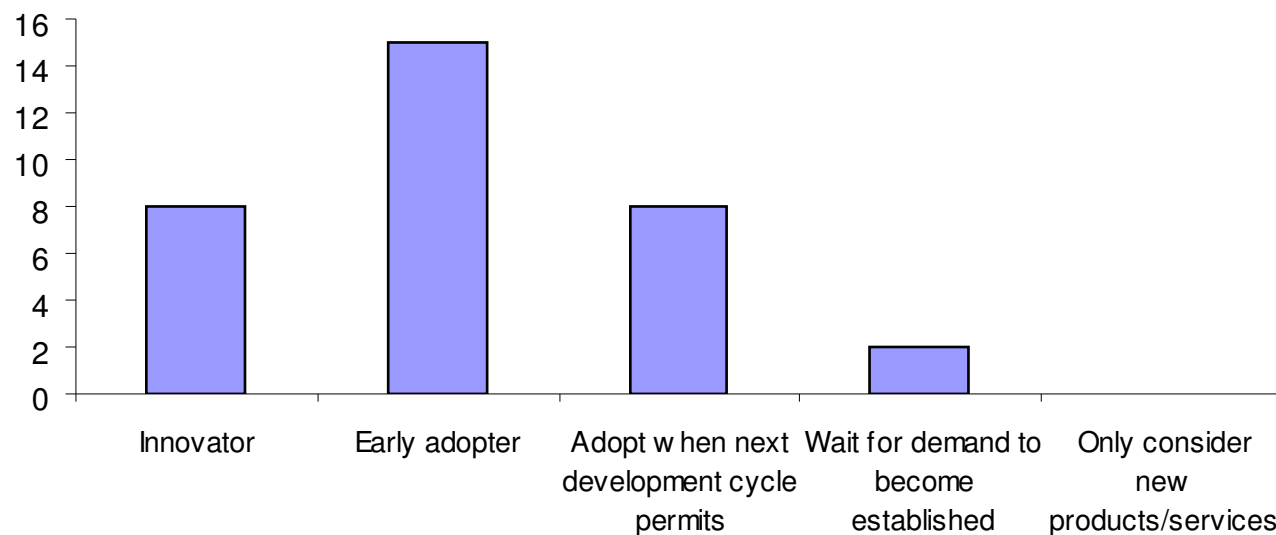
ESnet/LBNL

# About the respondents

Type of organisation



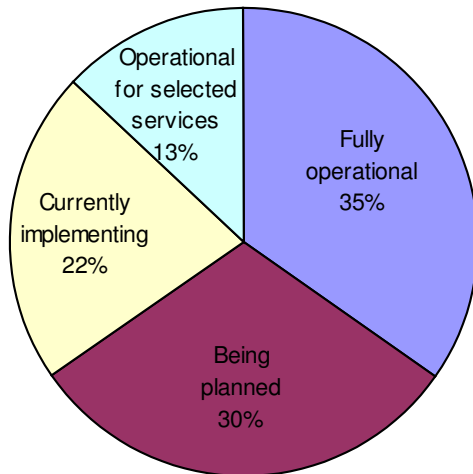
Attitude towards adopting new technologies



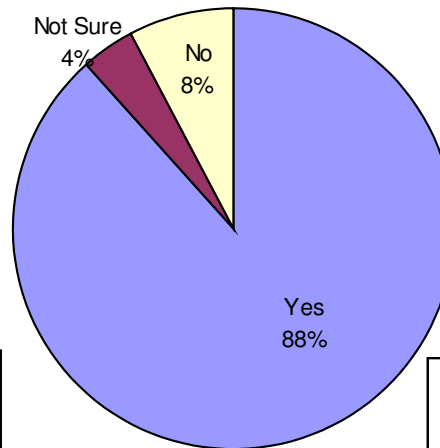
# The State of Federated Access Management

## Service Providers

**Current status of Federated Access Management Deployments**

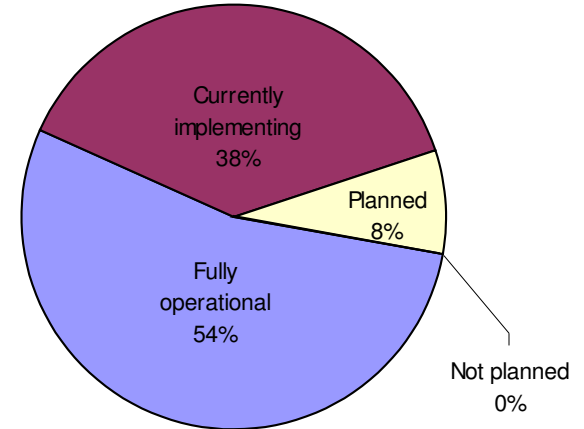


**Are you planning to employ Federated Access Management?**



## Identity Providers

**Status of Federated Access Management deployment**

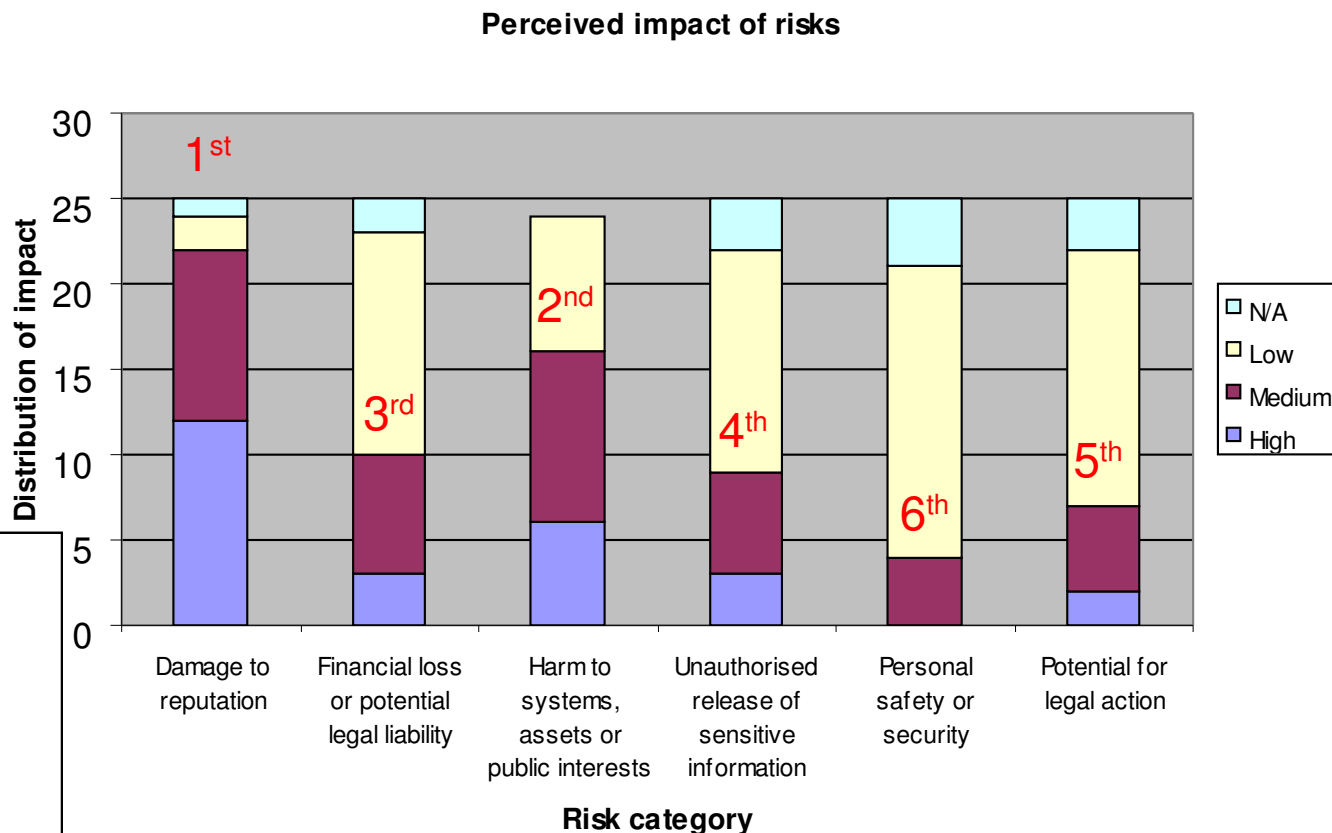
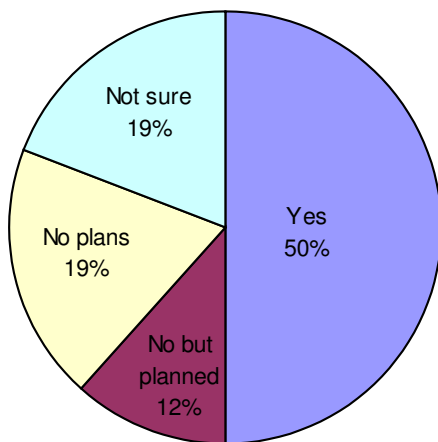


# Questioning Service Providers

# Risks and consequences

Mainly it is reputation that is at stake

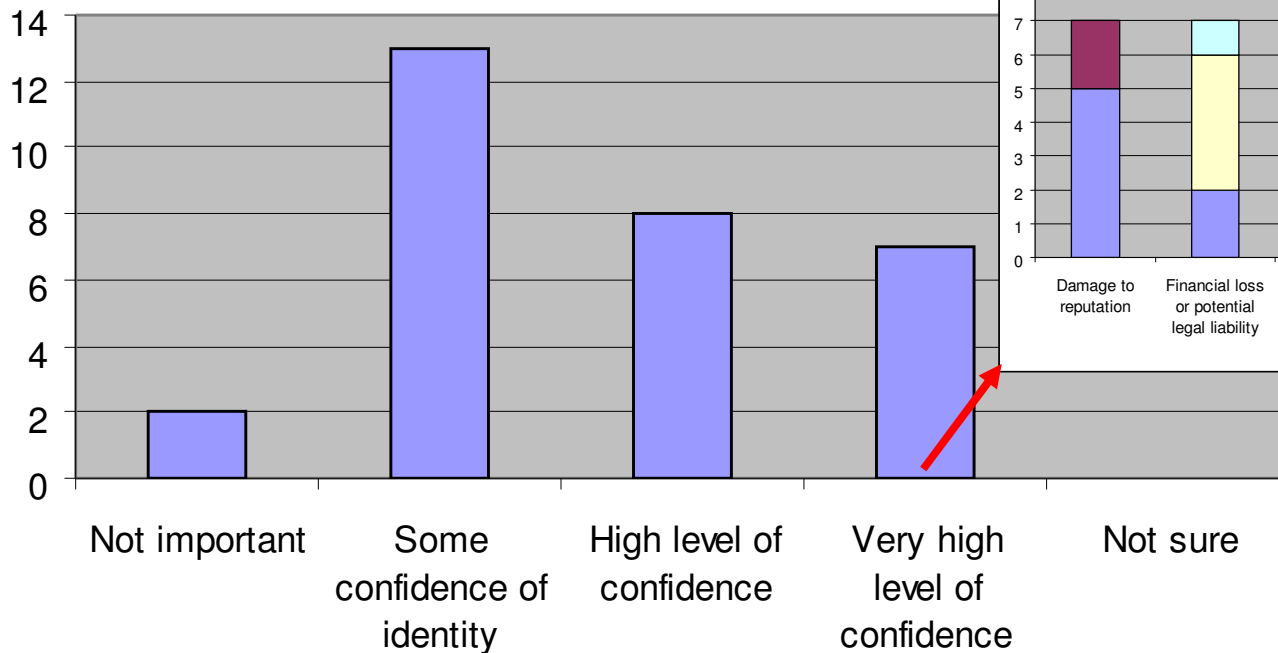
Percentage of organisations having carried out a Risk Assessment



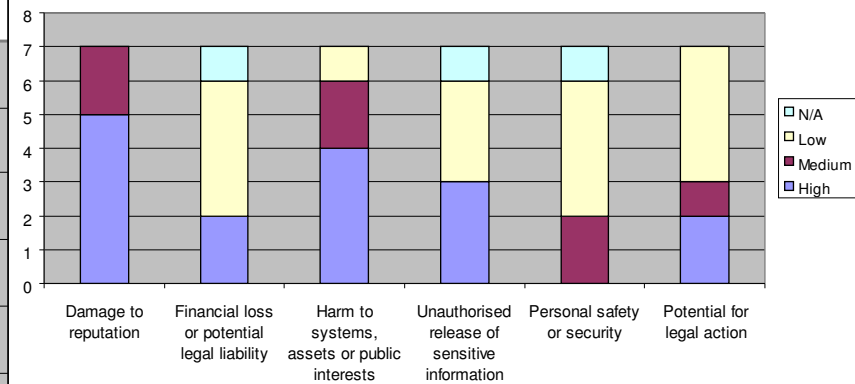
Those not sure or not planning to adopt FAM all indicated medium to high perceived risks

# The importance of identity

**Direct authentication: the required level of confidence in clients' identities**

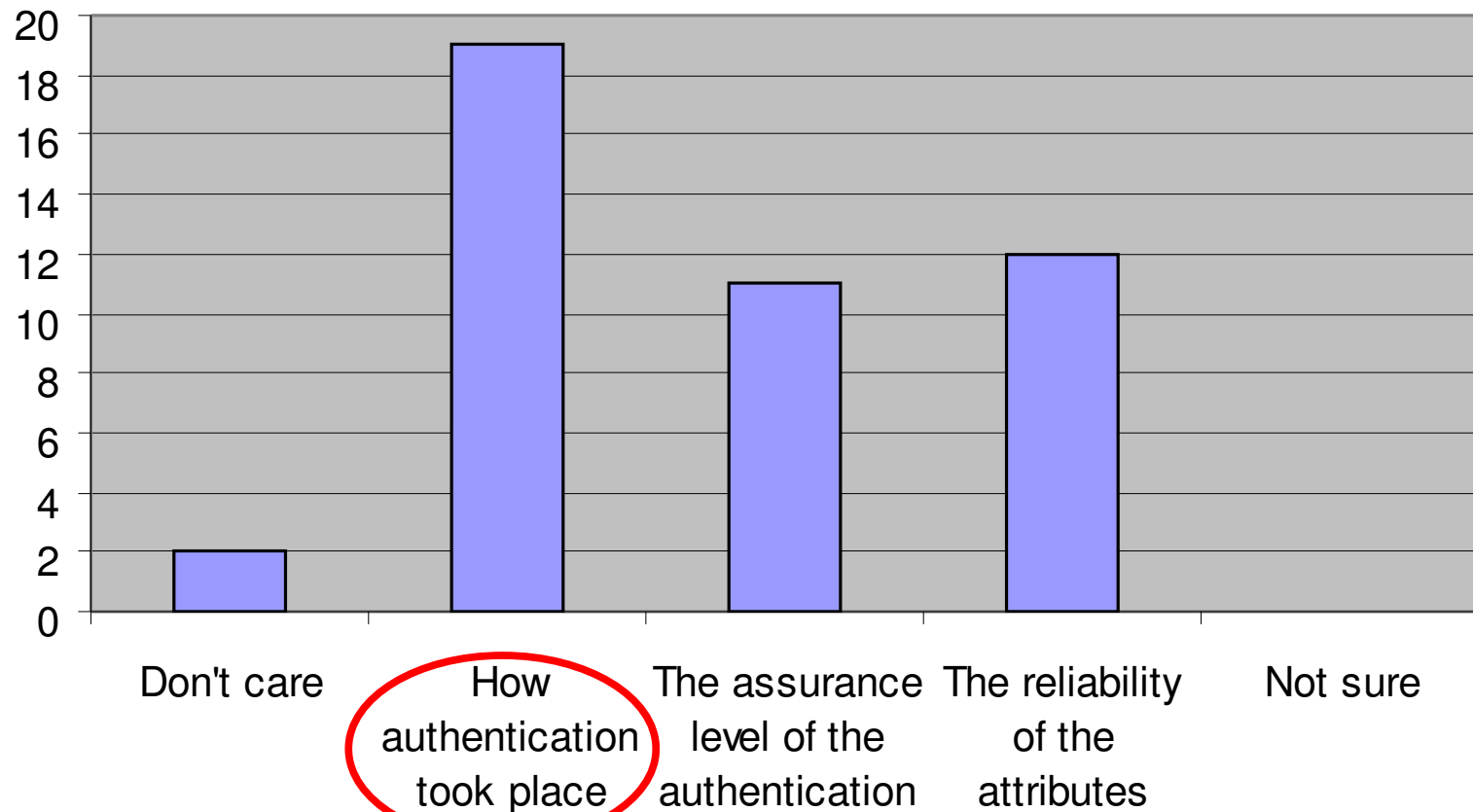


**Perceived impact of risks for those Service Providers requiring the highest LoA**



# 3<sup>rd</sup> party authentication info

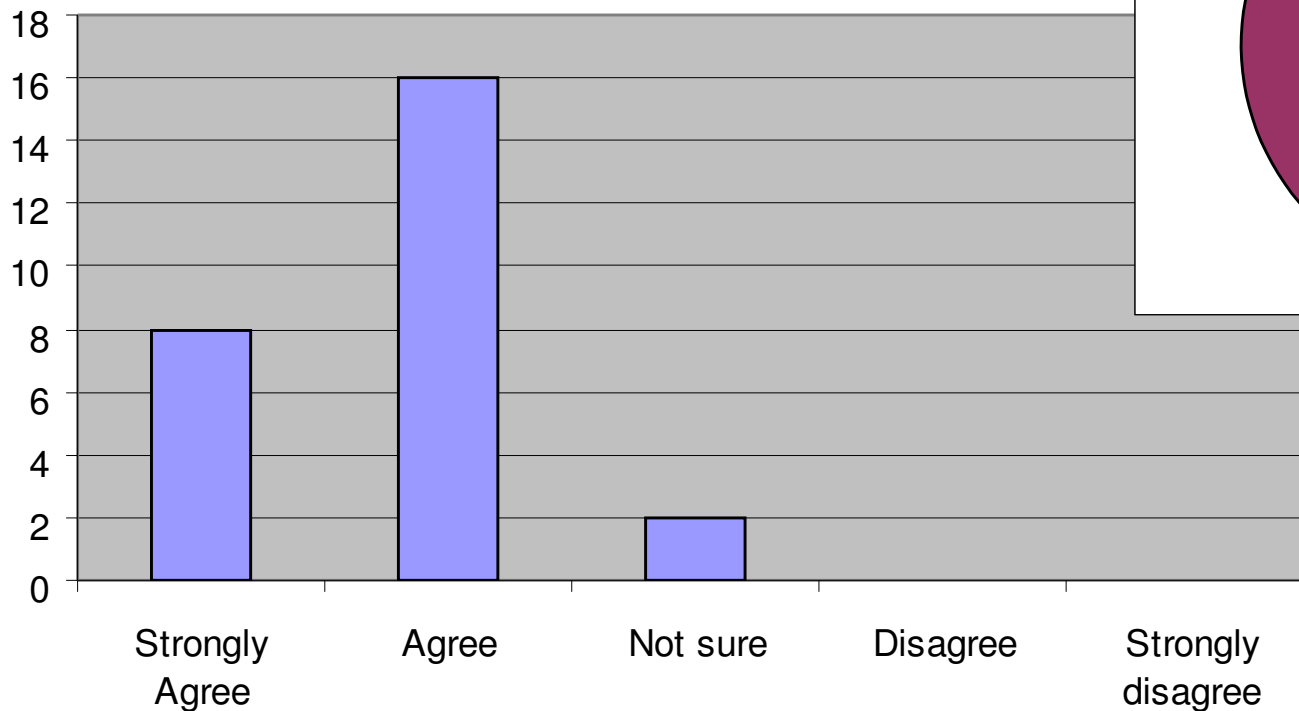
Third party authentication: the required information about the authentication process



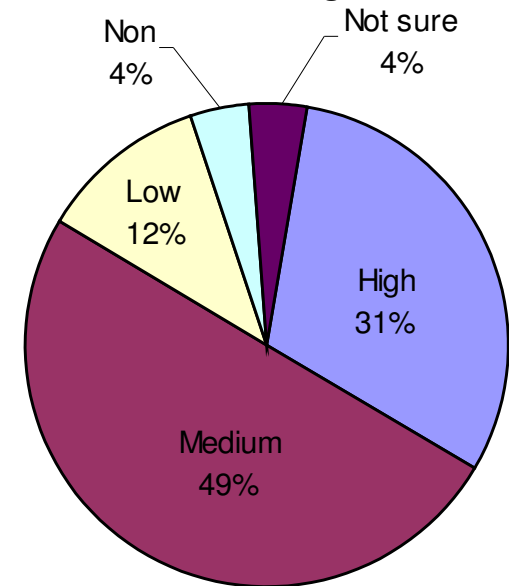


# Guidelines and governance

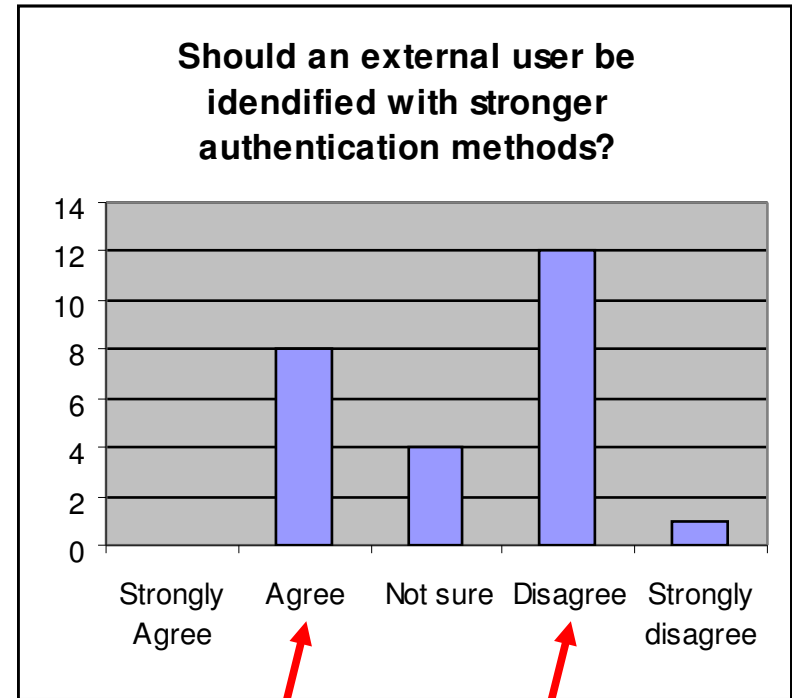
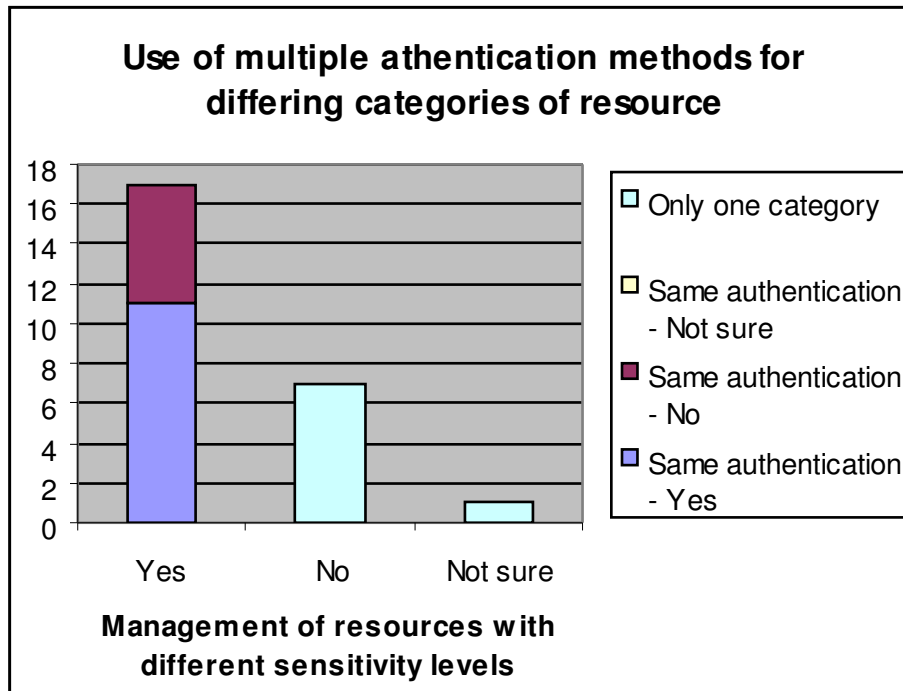
Willingness to adhere to guidelines



Preferred level of governance

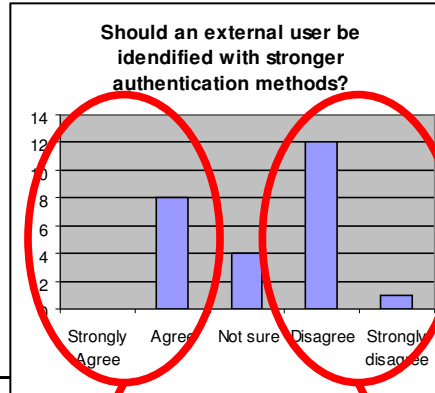


# Multiple authentication methods

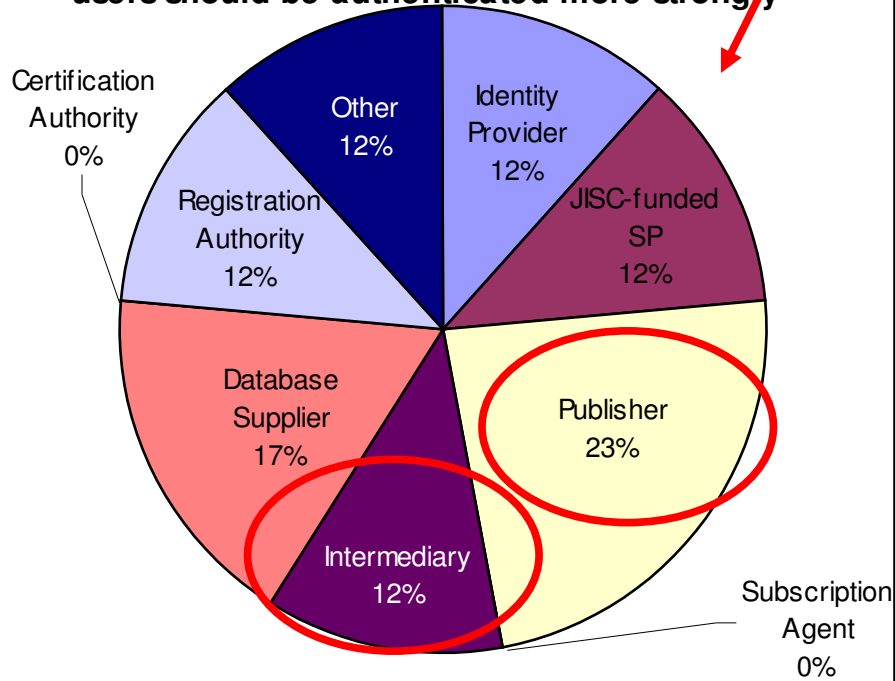


Split interests

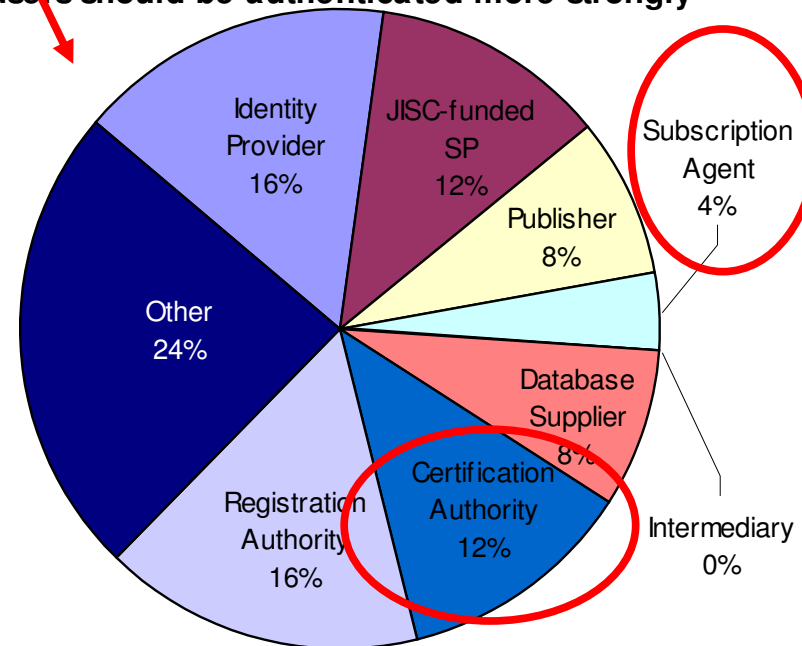
# Multiple authentication methods



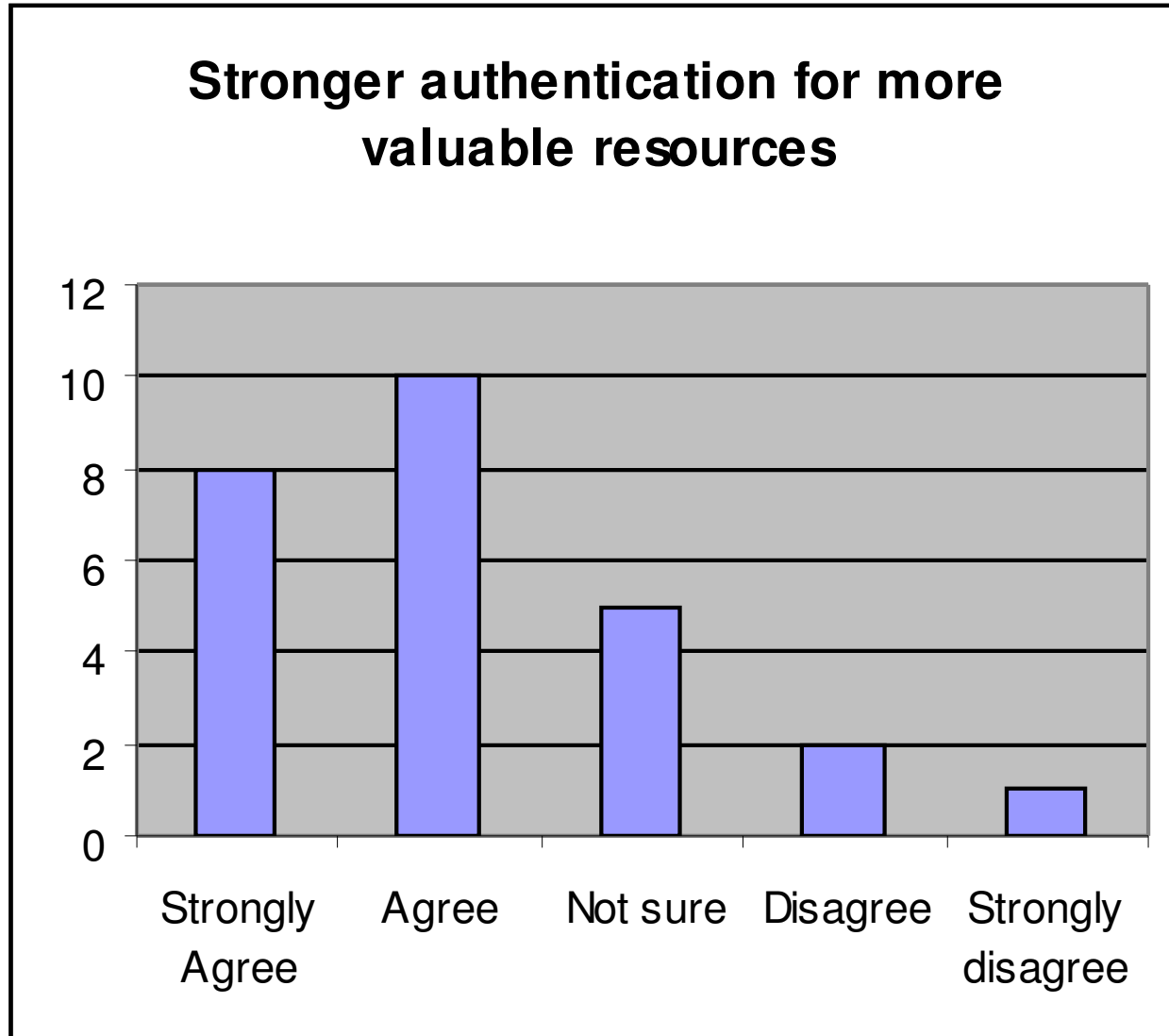
**Type of organisation agreeing that external users should be authenticated more strongly**



**Type of organisation disagreeing that external users should be authenticated more strongly**

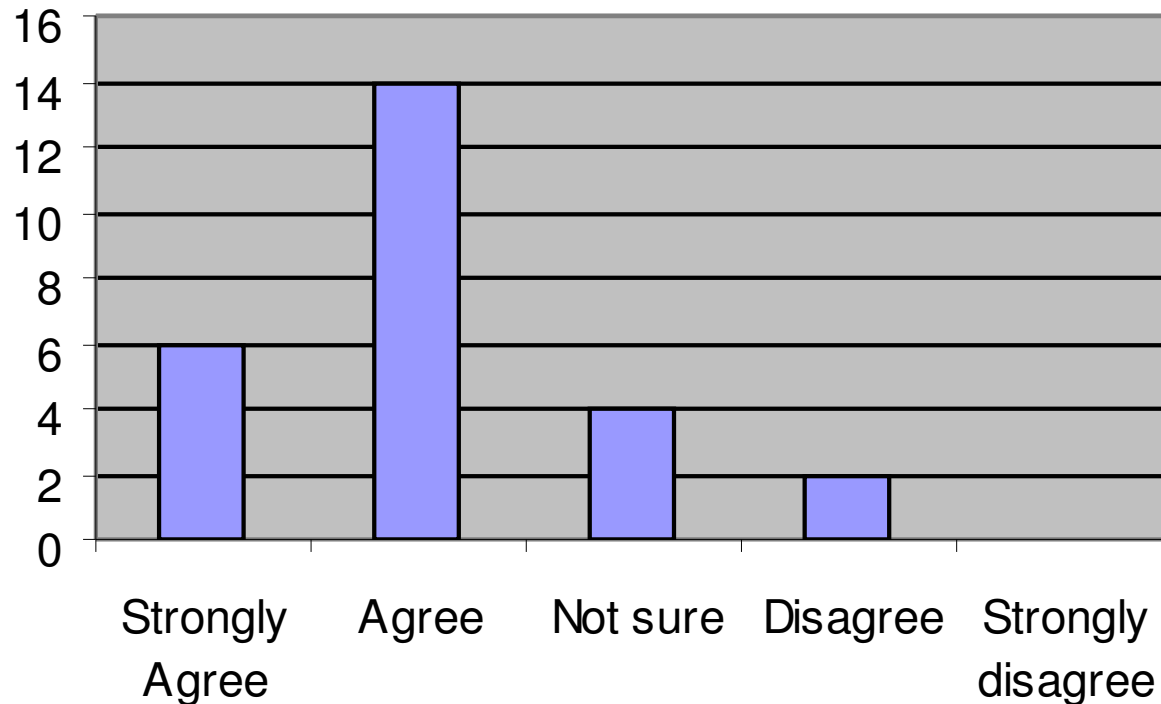


# Do valuable resources need stronger authentication



# LoA drives willingness to join a federation

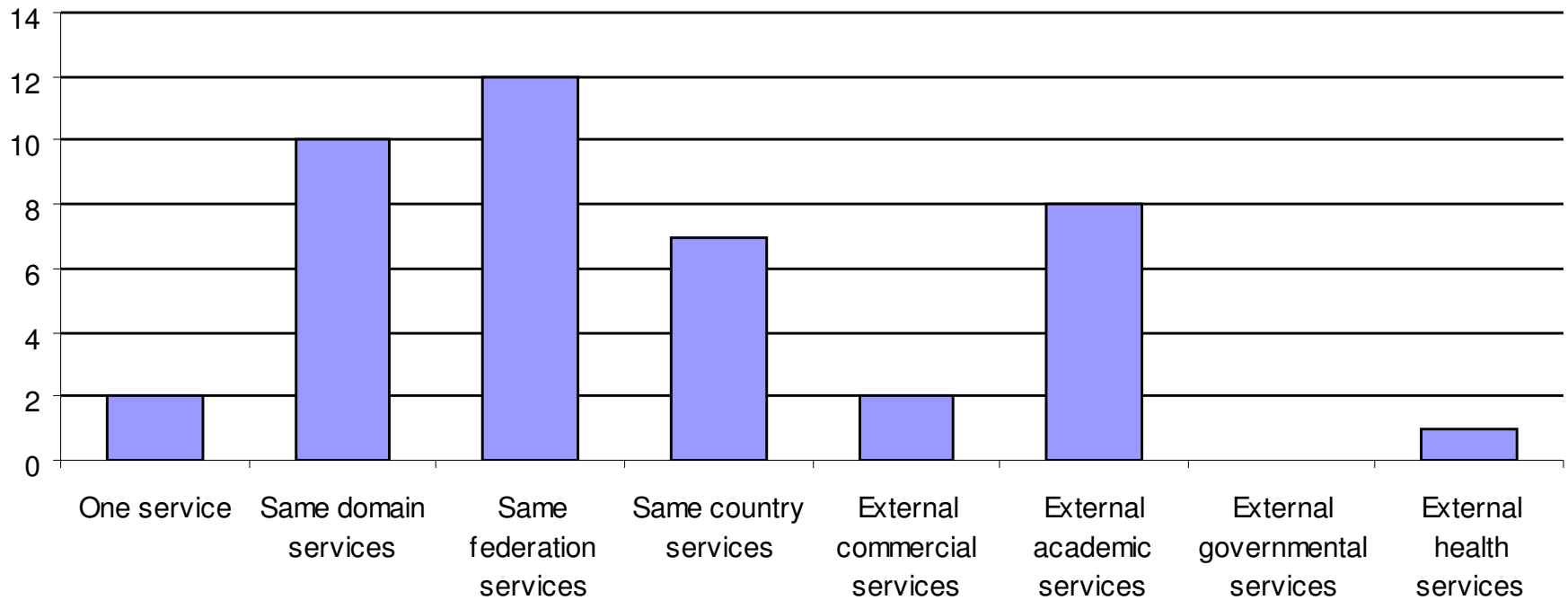
**Reluctance to place data or services into a federation until there are more formal LoA procedures**



# Questioning Identity Providers

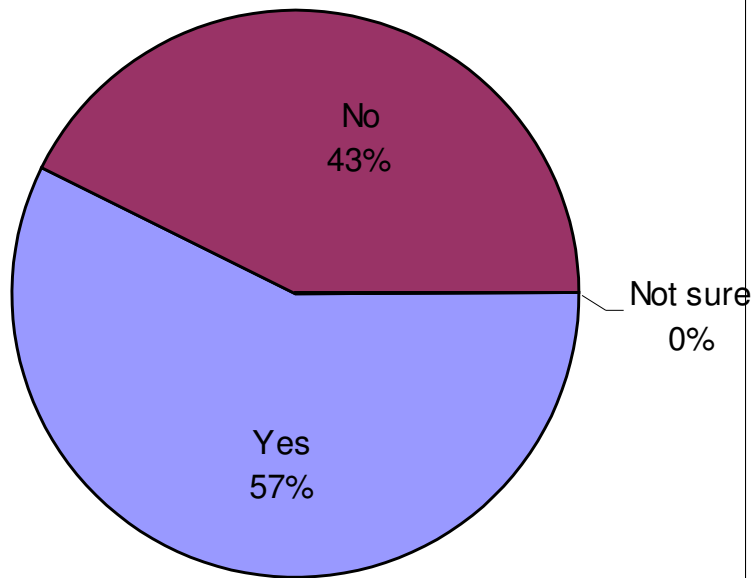
# Where assertions go

Who consumes your authentication assertions?

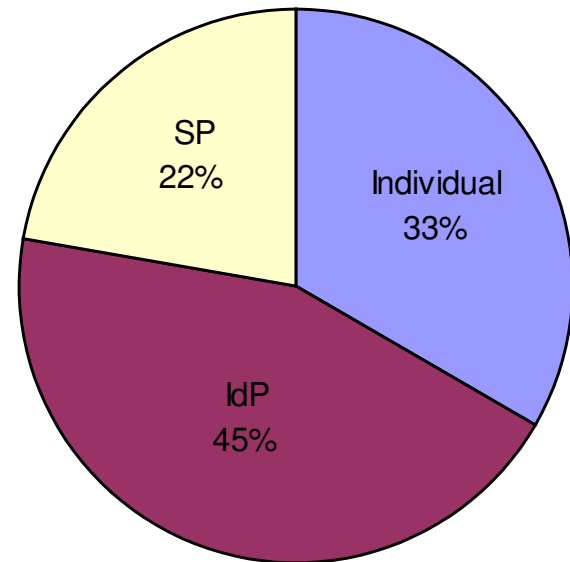


# Authenticating more than one way

**Do you allow individuals to authenticate using multiple mechanisms**



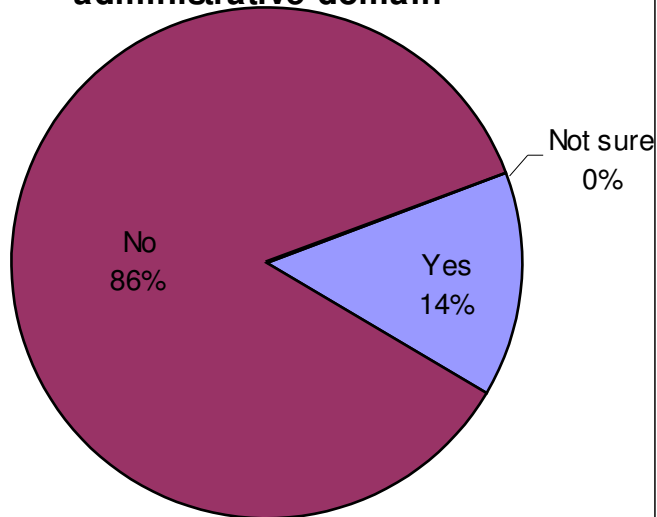
**Who decides about authentication method**



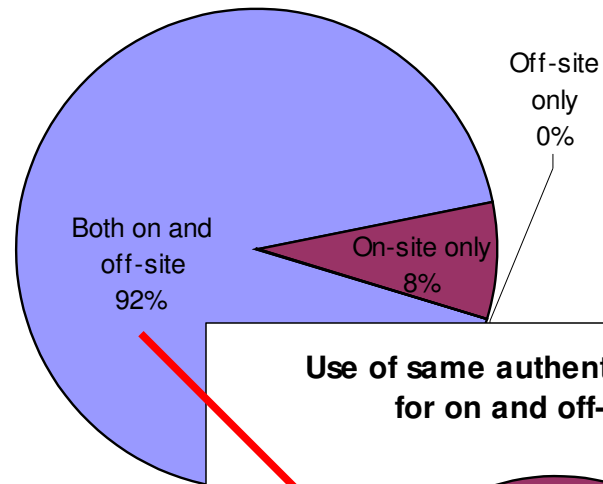


# Identifying your own

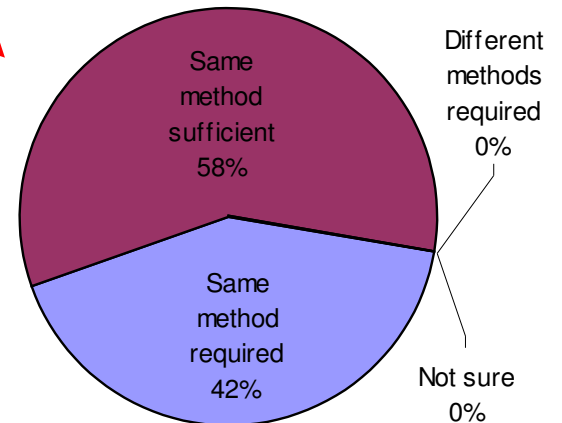
**Use of different authentication methods for users in and outside an administrative domain**



**Authentication assertions for on and off-site users**

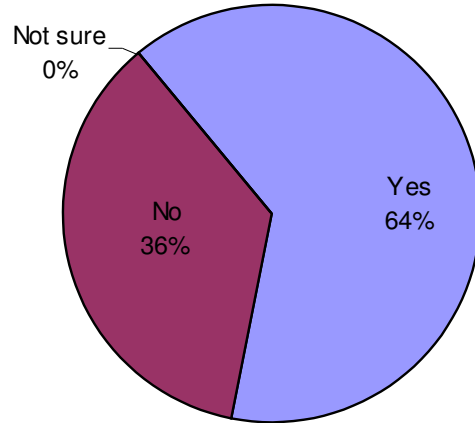


**Use of same authentication method for on and off-site users**

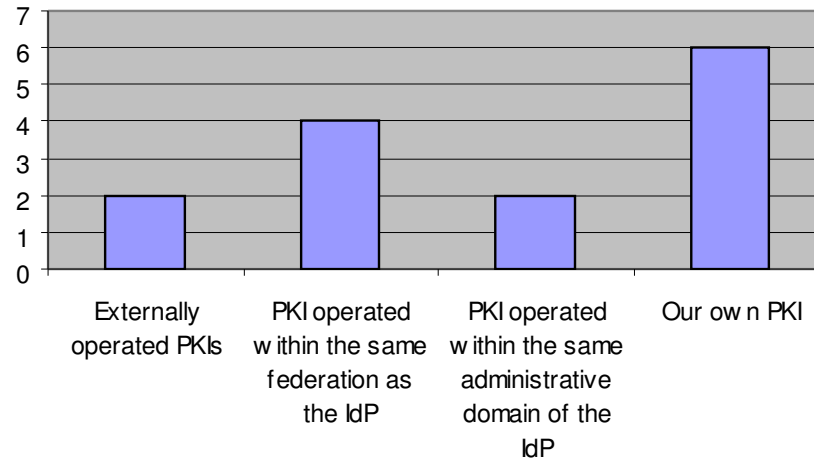


# The use of PKI

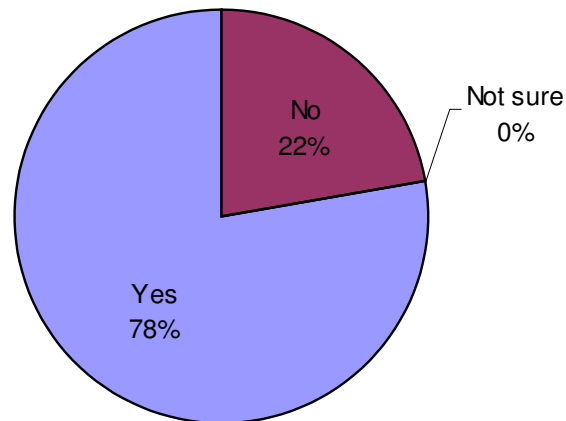
Do you make use of a PKI for identifying your users?



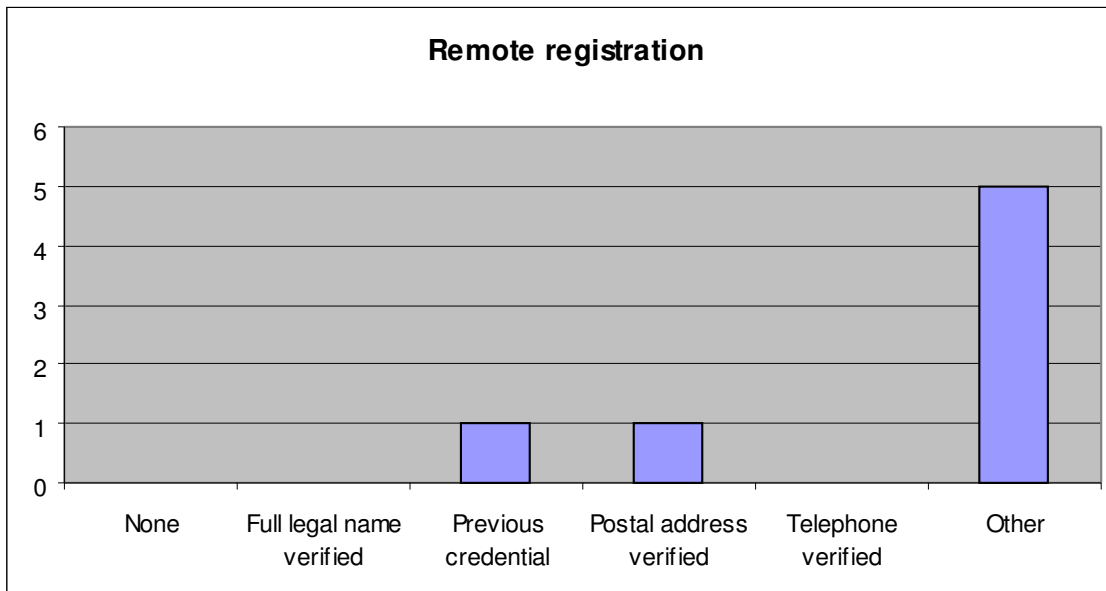
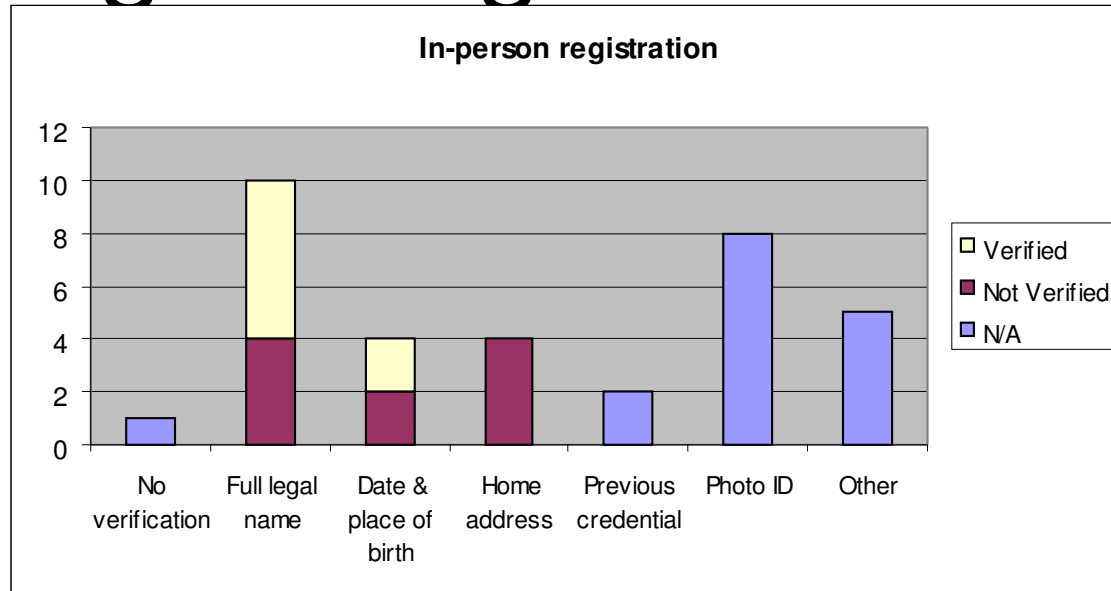
Who provides your PKI



Do you delegate the identity vetting to Registration Authorities?



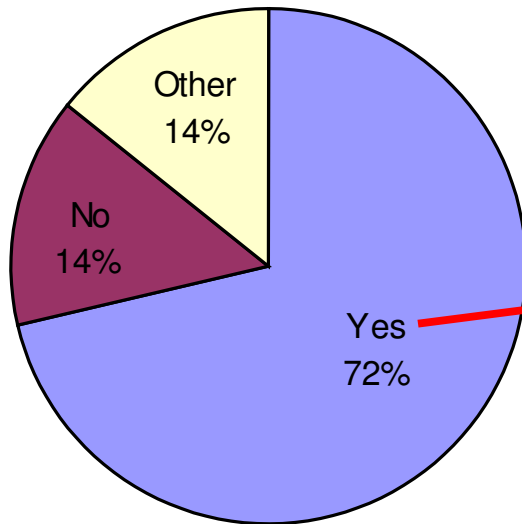
# Registering with the PKI



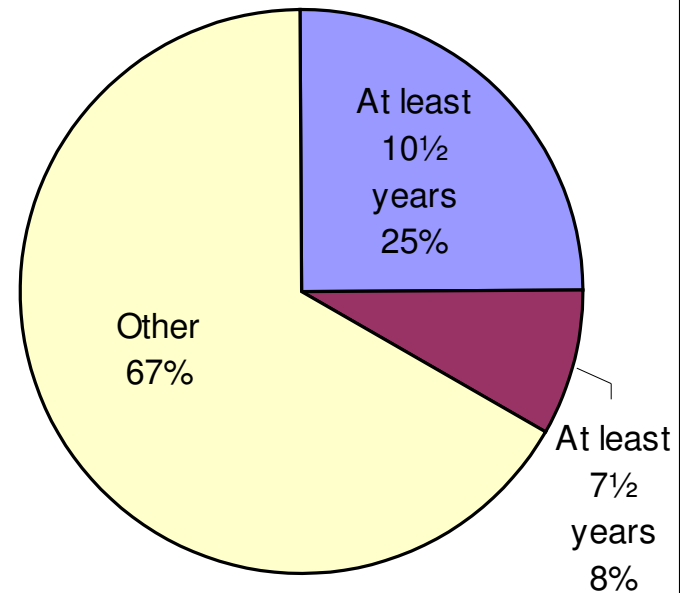
- valid matriculation card numbers,
- telephone communication with the individual
- trusted departments (e.g. payroll) to assert user attribute

# Registration records

**Do you preserve user registration records?**



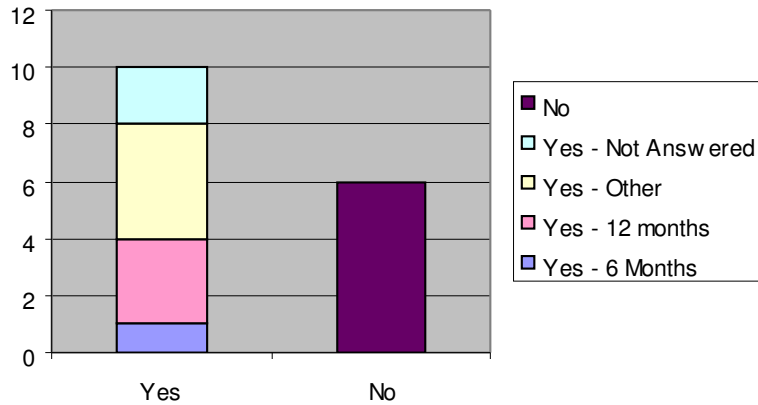
**How long do you retain registration records for?**



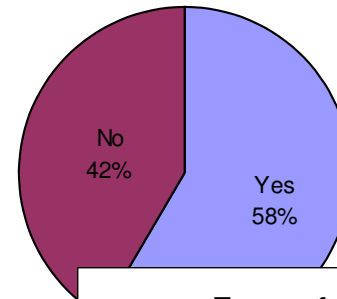
NIST SP 800-63 requires records to be kept for 7½ years for LoA 2

# About user passwords

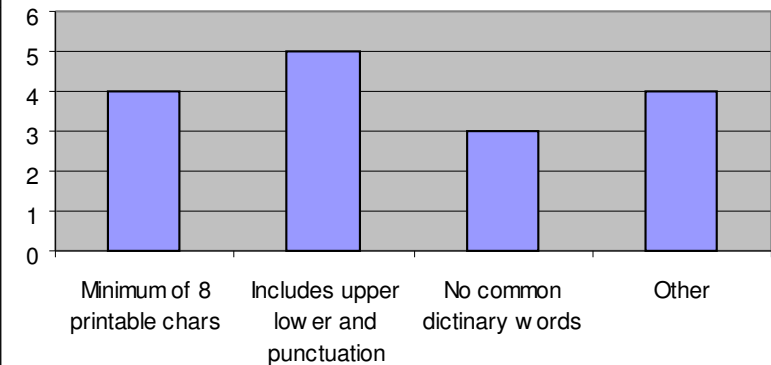
### Imposing password validity period



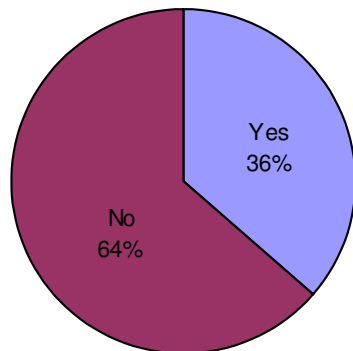
### Imposing rules by which passwords may be chosen



### Types of rules imposed when choosing passwords



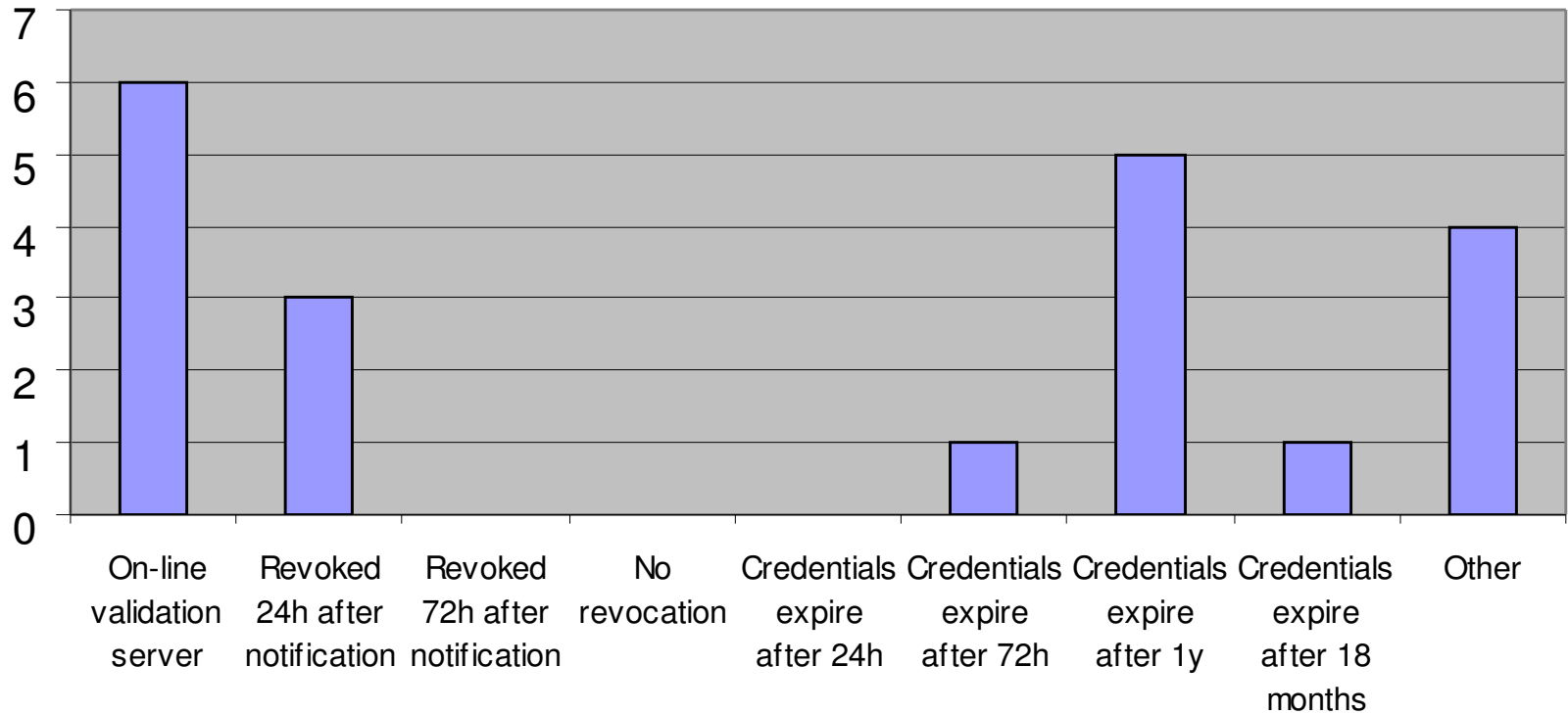
### Account lockouts after a number of failed attempts



No respondents meet the lowest NIST LoA level: 1

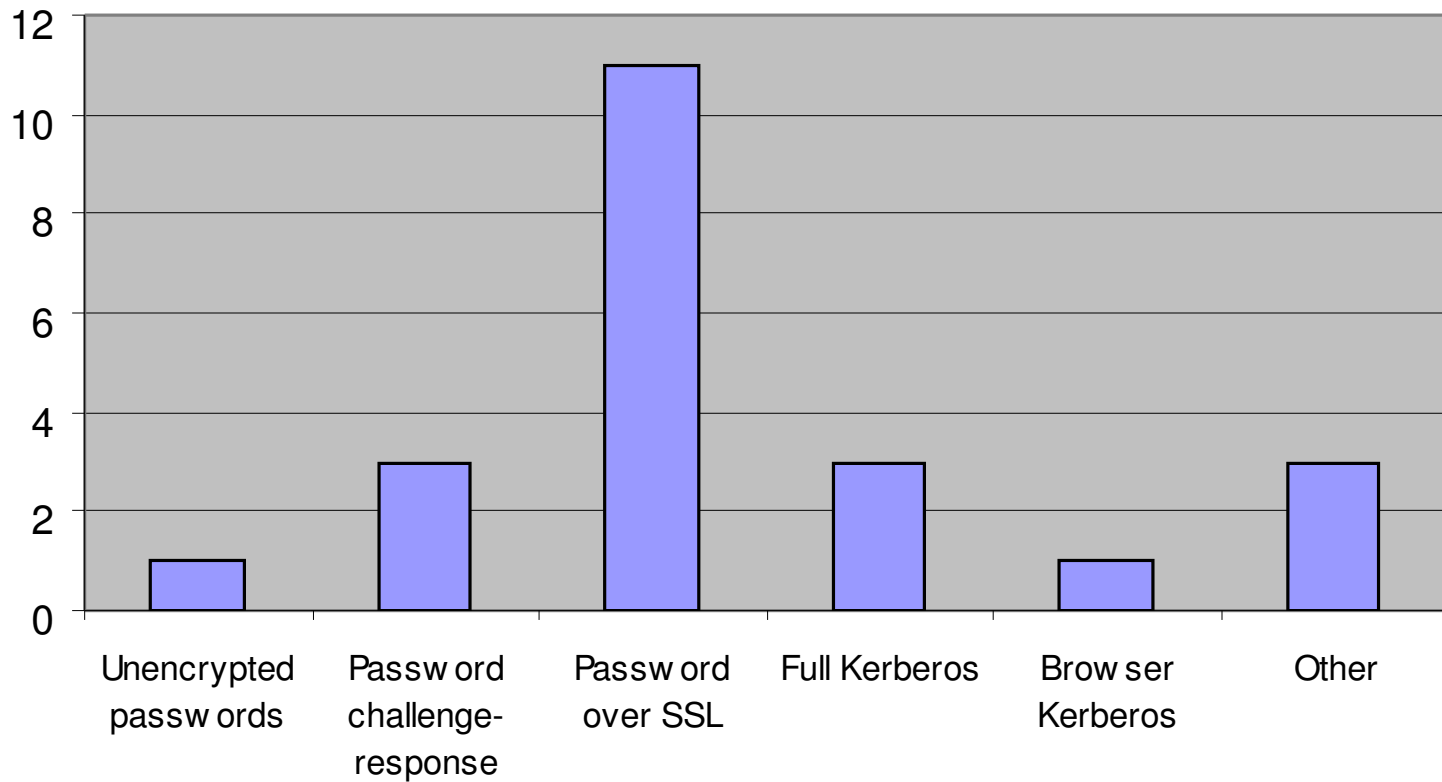
# Revocation

Types of revocation facilities for PKI



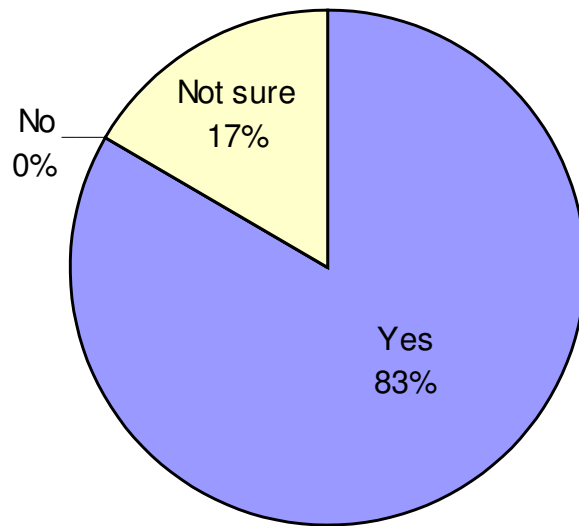
# Which security protocols

Types of authentication protocols in use by IdPs

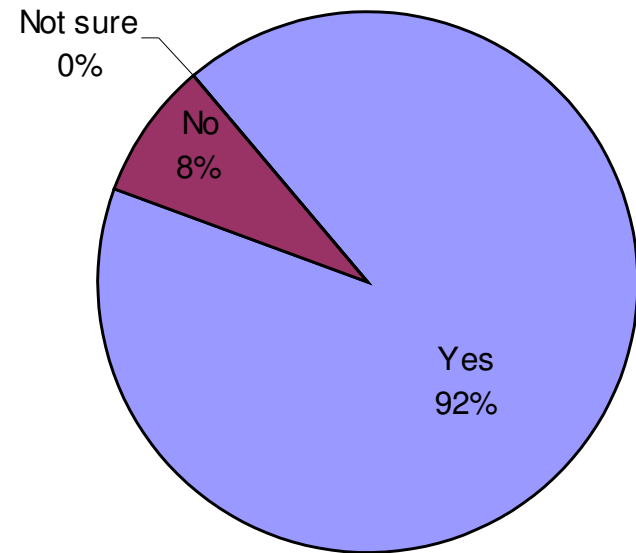


# Willingness to follow guidelines

**Willingness to follow technical guidance for e-authentication**



**Willingness to know about LoA and risk-based authentication**

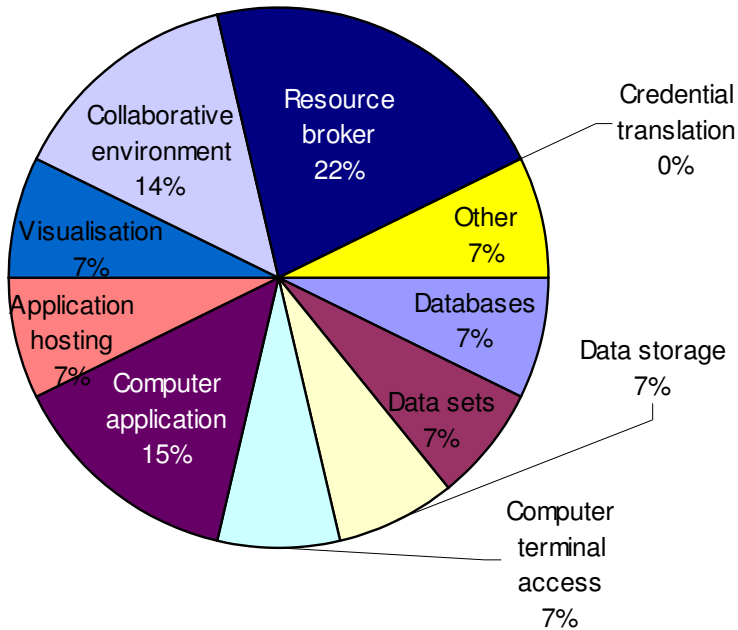




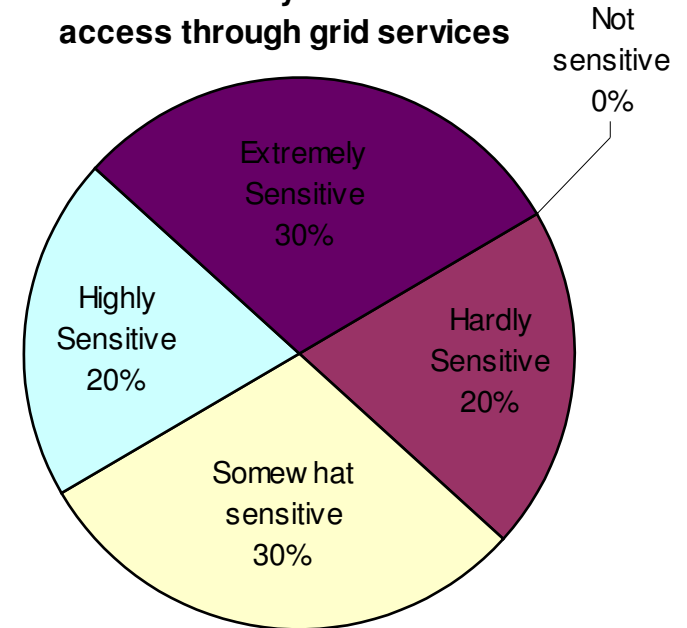
# Questioning the Grid Community

# Grid resources

**Services types exposed via grid mechanisms**

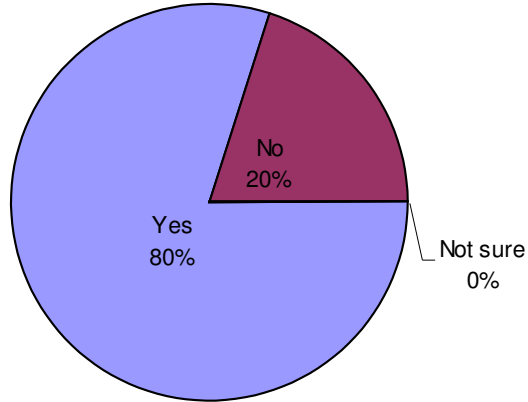


**Levels of sensitivity of data users can access through grid services**

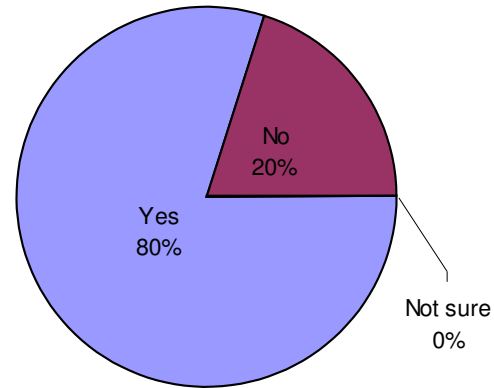


# Types of risk

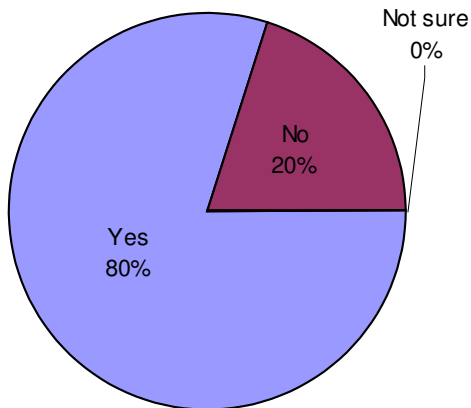
**Can users run their own code on your grid?**



**Do you provide access to large compute resources via your grid?**

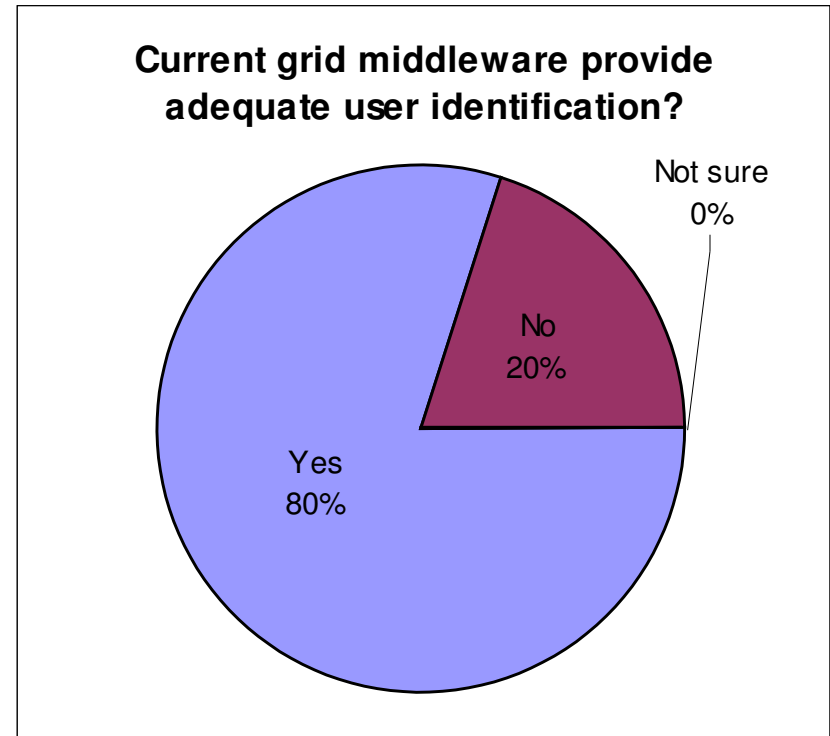


**Current grid middleware provide adequate user identification?**



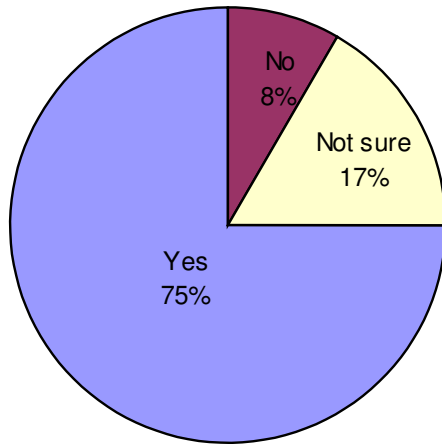
# Types of identification

- 90% are able to use PKIs (with CAs)
- 80% are able to use direct key exchange (without CAs)
- 10% can use community portals

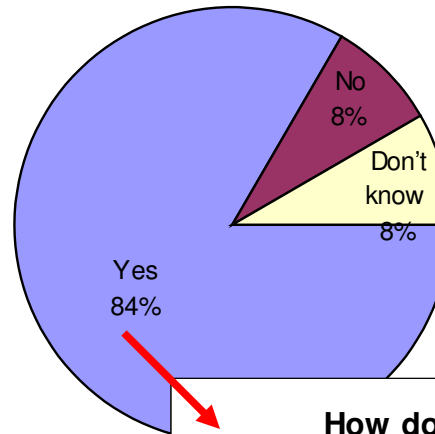


# CAs and policy documents

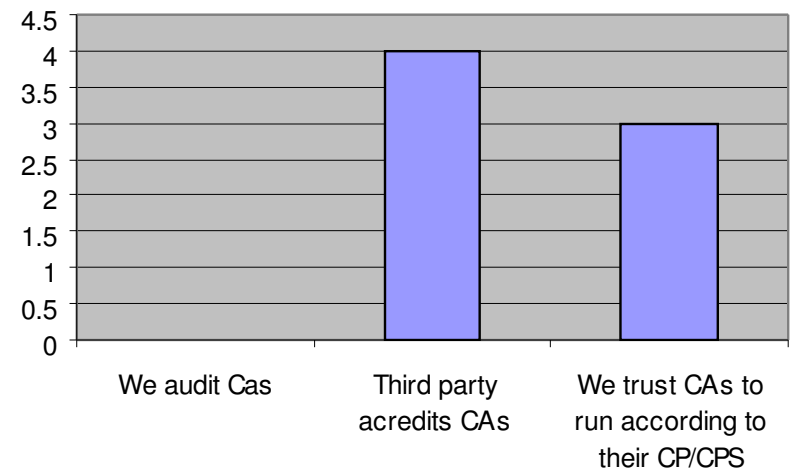
**CAs required to publish a CP/CPS?**



**CA required to adhere to their CP/CPS?**

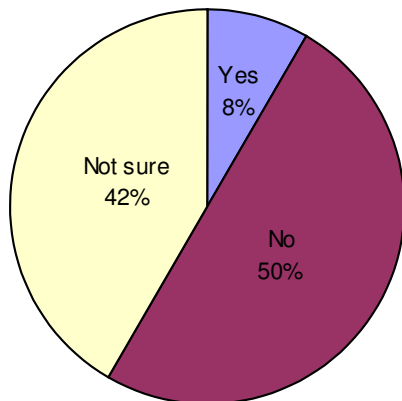


**How do you enforce adherence to CP/CPS?**

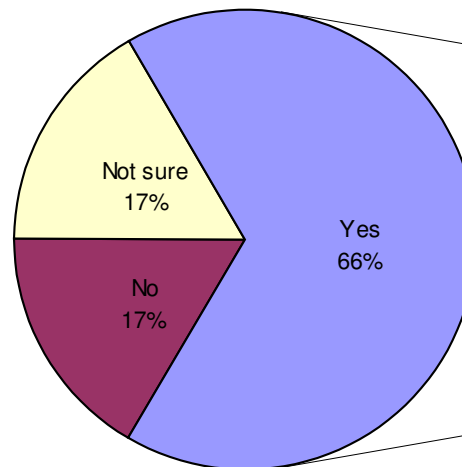


# PKI Certificates

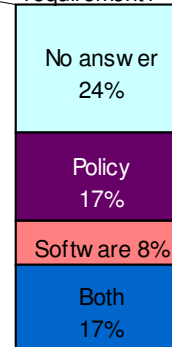
**Imposing a maximum length on a certificate chain?**



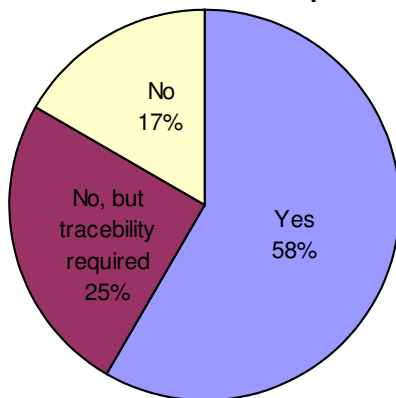
**Well-defined Namespace required?**



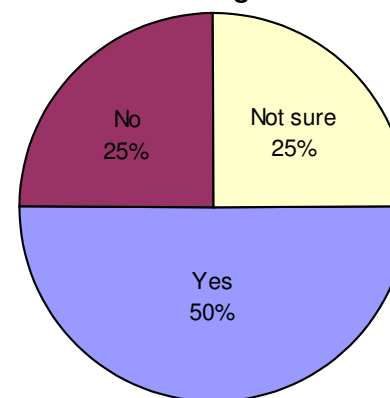
**What drives this requirement?**



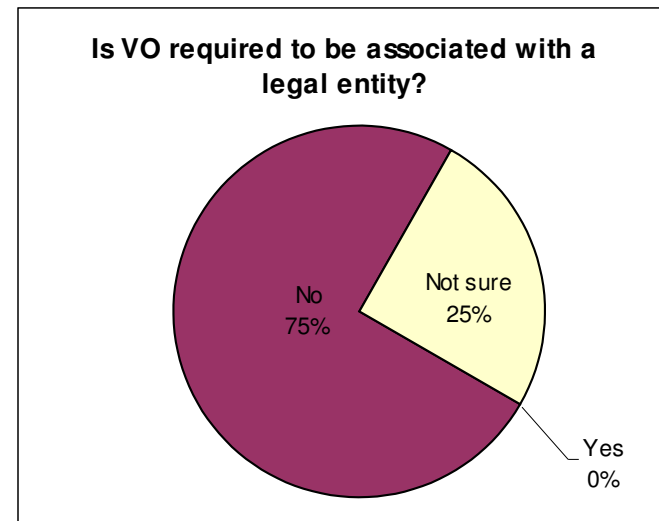
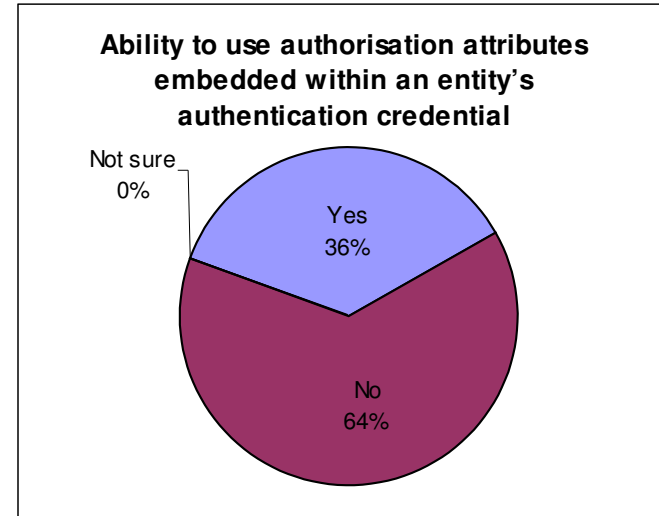
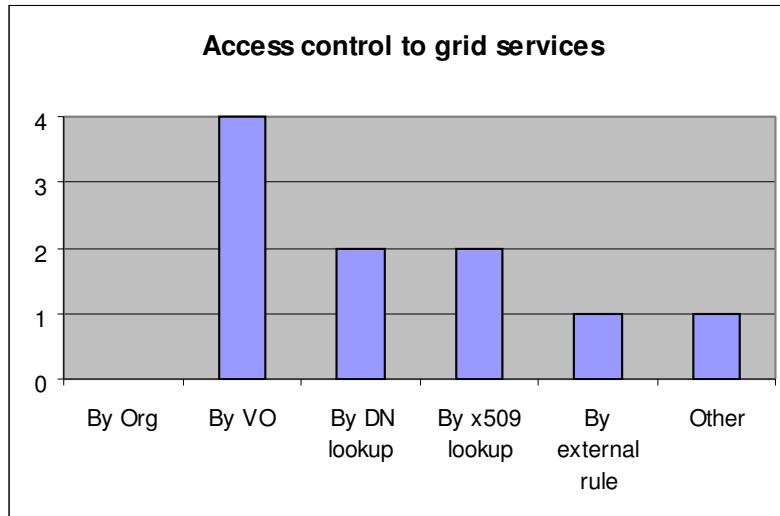
**"Meaningful names" in the commonName field required?**



**Imposing restrictions on elements allowed in Distinguished Name?**

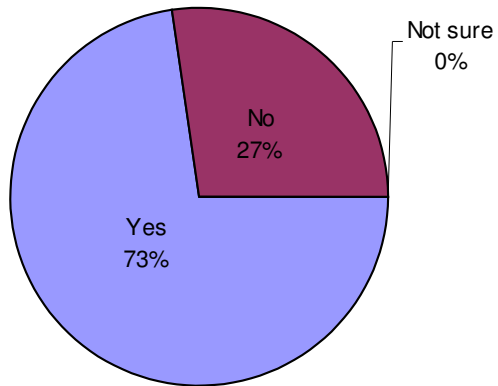


# Controlling access

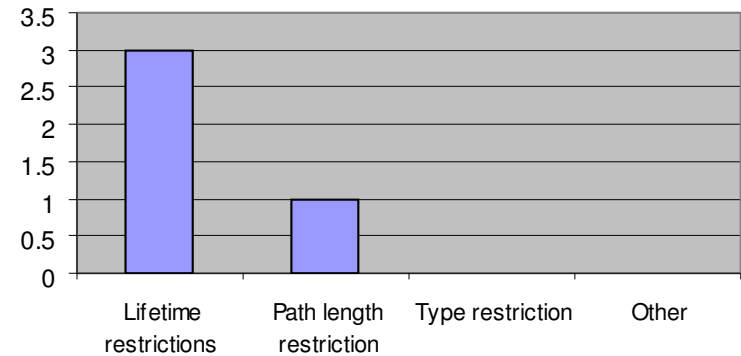


# GSI Proxies

Do your services accept GSI proxy credentials?



How do you distinguish between GSI proxy certificates?





# Topics for Group Discussions

- A) what are the limitations of existing access control systems?
- B) suggest some benefits/practical applications of an LoA model?
- C) what are the barriers to successful introduction of LoA compliant systems?
- D) what funded work would be most effective in aiding the adoption of LoA?