MANCHESTER
1824

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

– Summary of initial findings IdP/SP/Grid

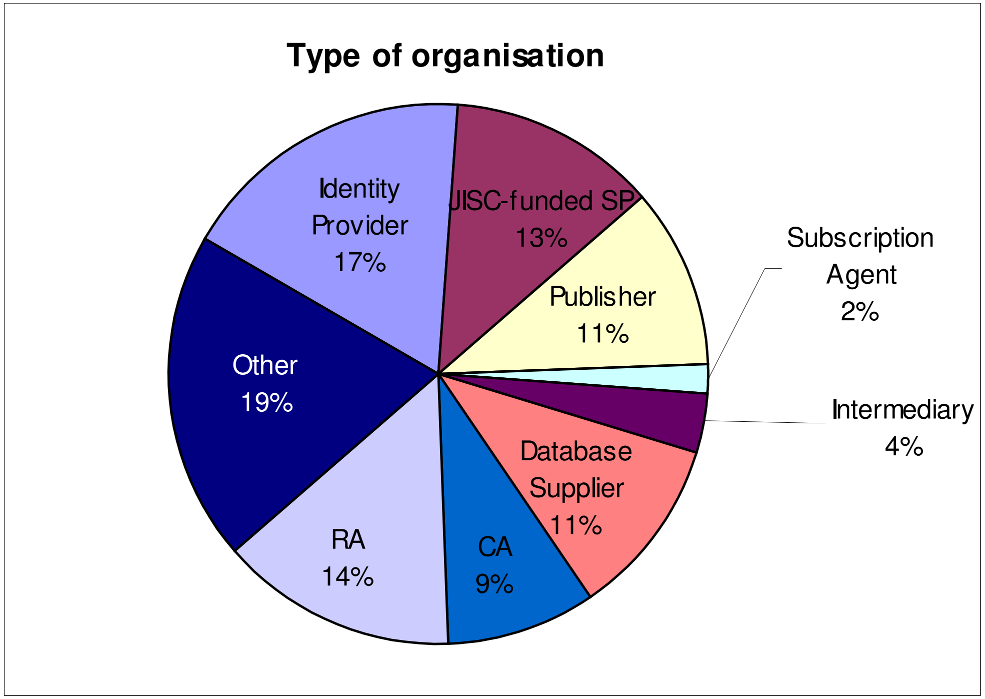
Ning Zhang, Aleksandra Nenadic, Li, Yao, Terry Morrow, Mike Jones
the University of Manchester, UK

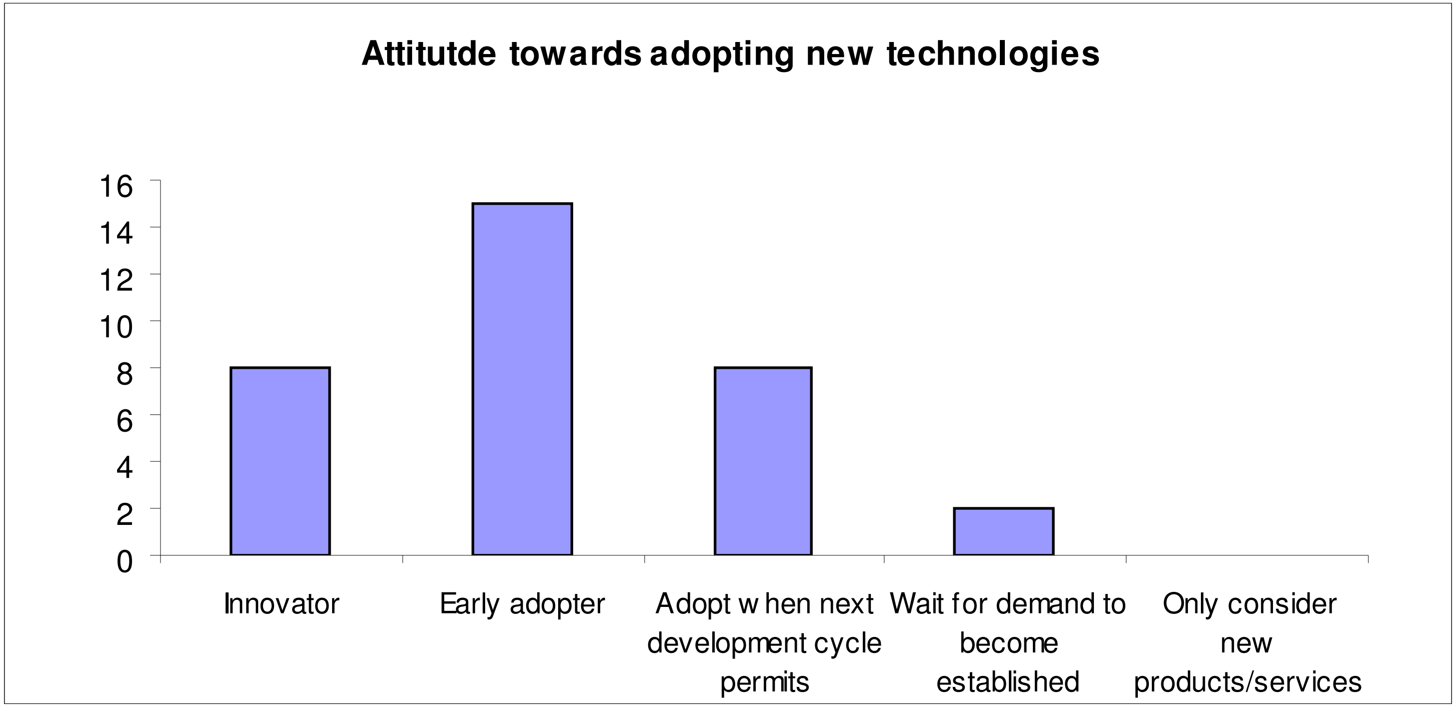
- Target: Service Providers, Identity Providers and Grid community

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

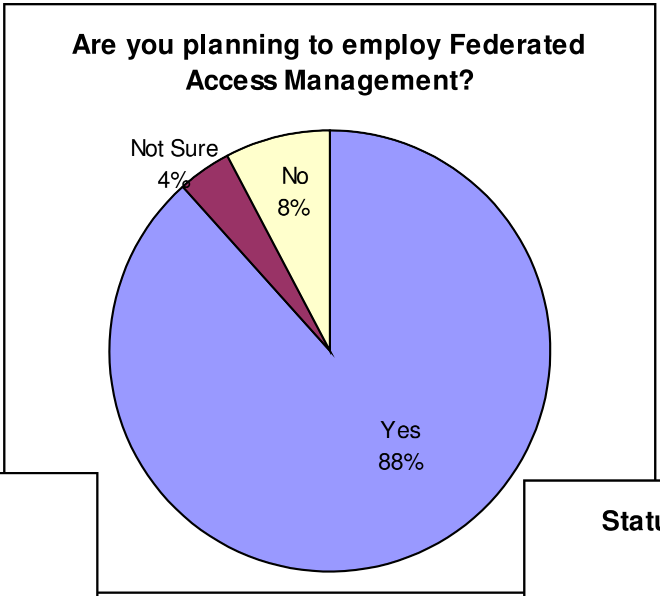
SWITCH (Swiss HE federation)
University of Queensland, Australia
OCLC Inc
PsyGrid
JSTOR
Cambridge University Press
Oxford University Computing Services
MIMAS
Grid-Ireland/Trinity College Dublin
Xrefer Ltd
Taylor & Francis Group Ltd
Emerald Group Publishing Ltd
STFC
Victorian Partnership for Advanced Computing, Australia
ESnet/LBNL

About the respondents

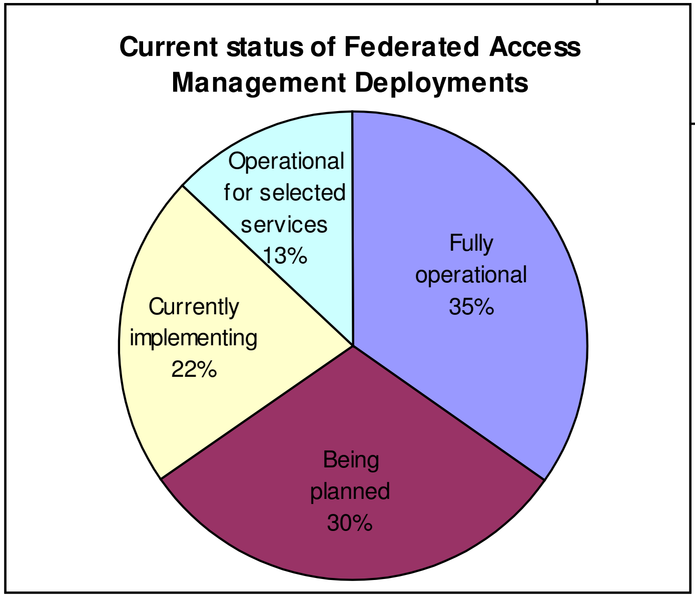




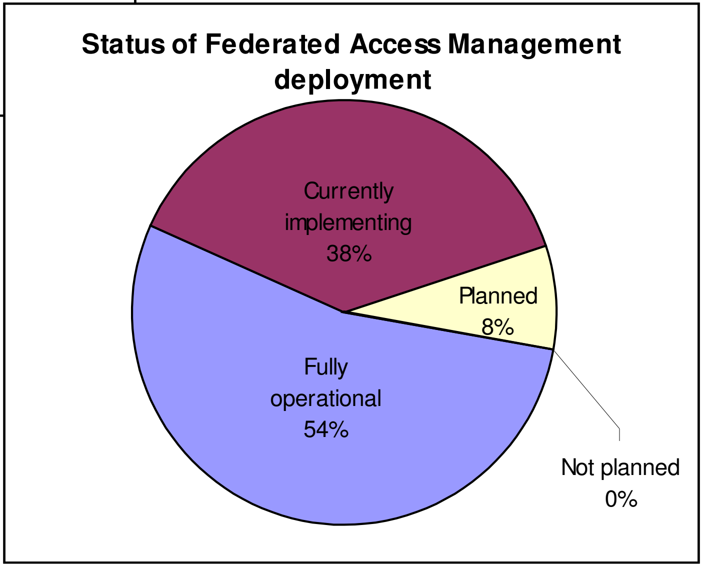
The State of Federated Access Management



Service Providers



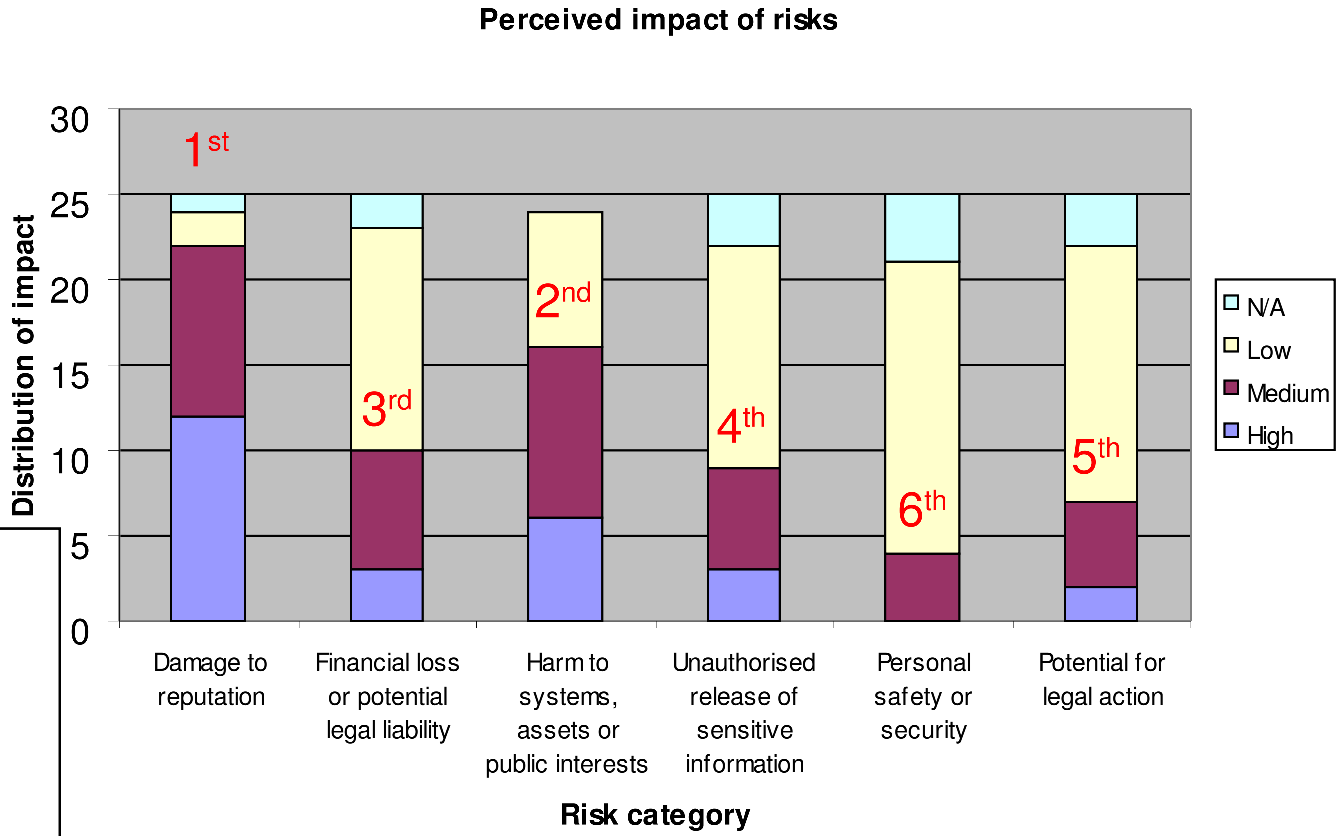
Identity Providers



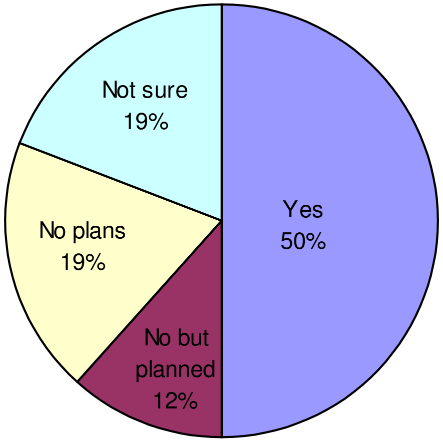
Questioning Service Providers

Risks and consequences

Mainly it is reputation that is at stake

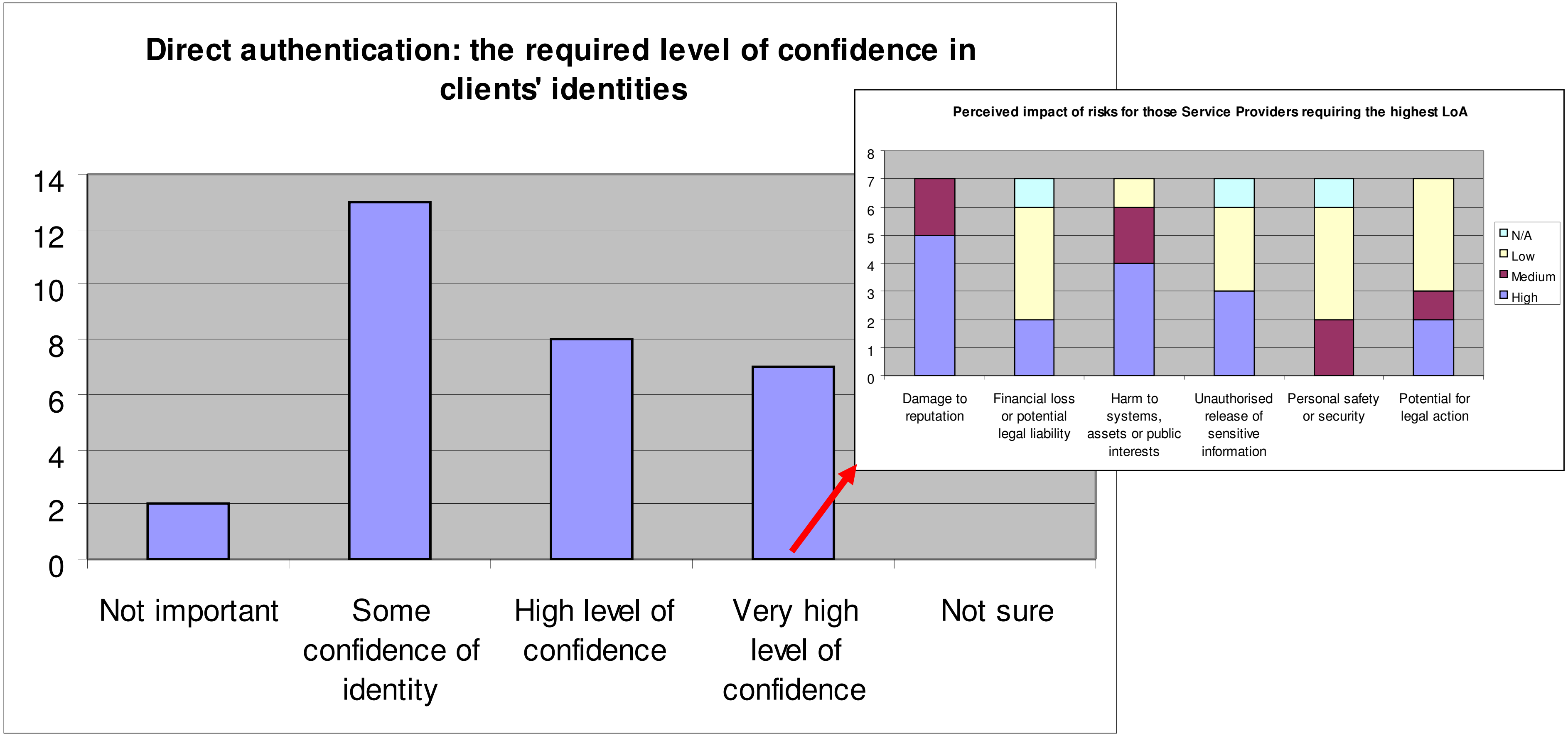


Percentage of organisations having carried out a Risk Assessment

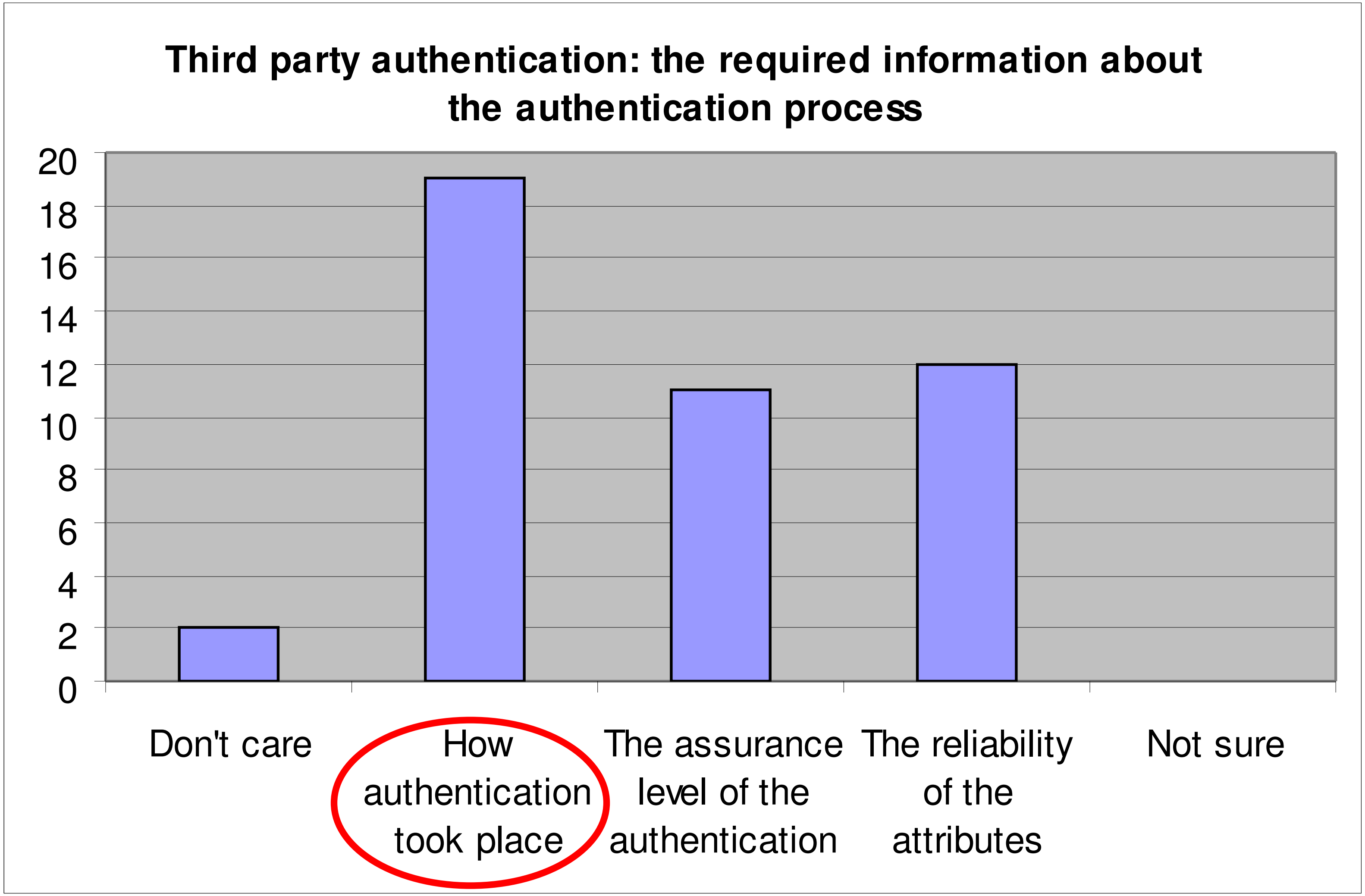


Those not sure or not planning to adopt FAM all indicated medium to high perceived risks

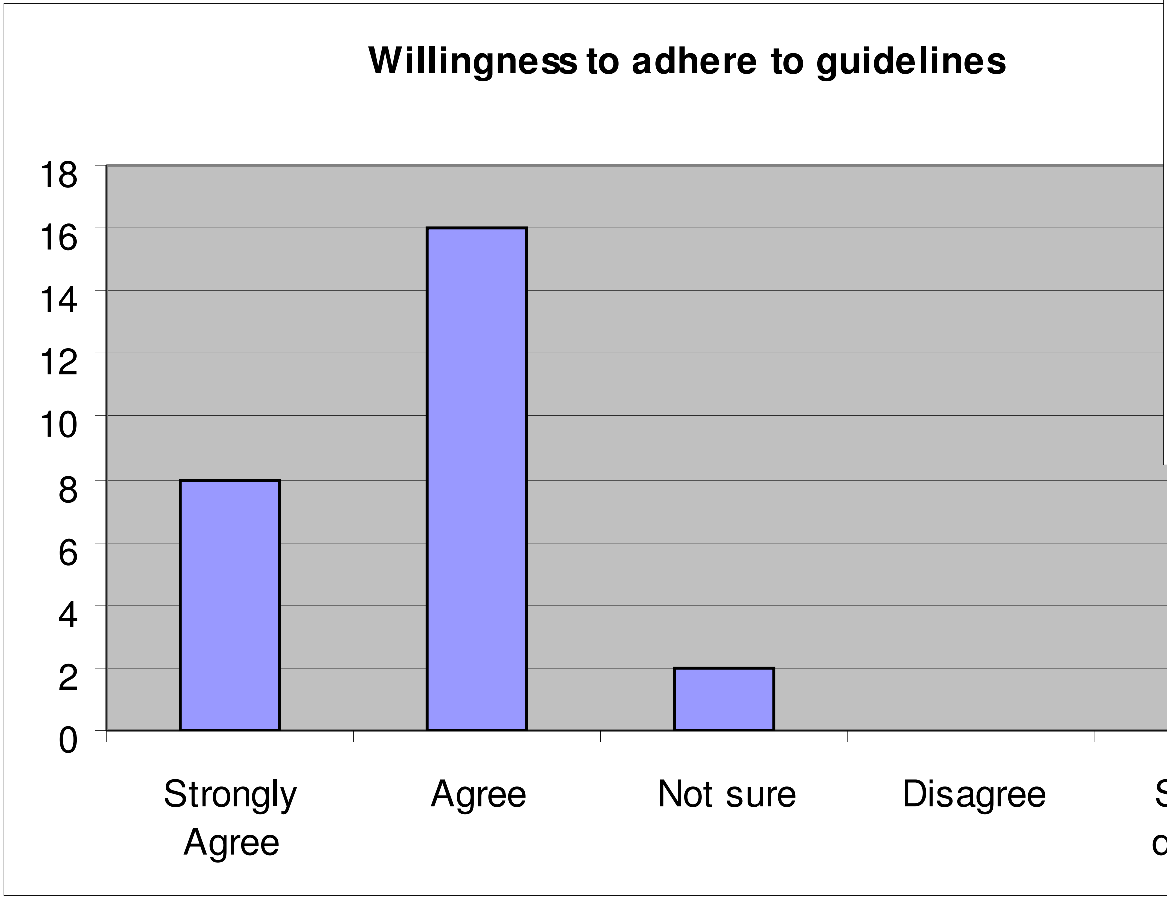
The importance of identity

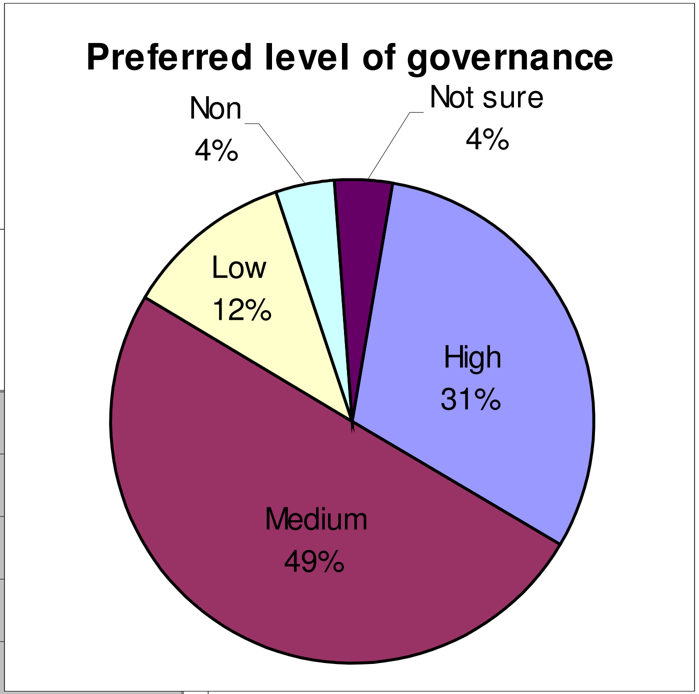


3rd party authentication info



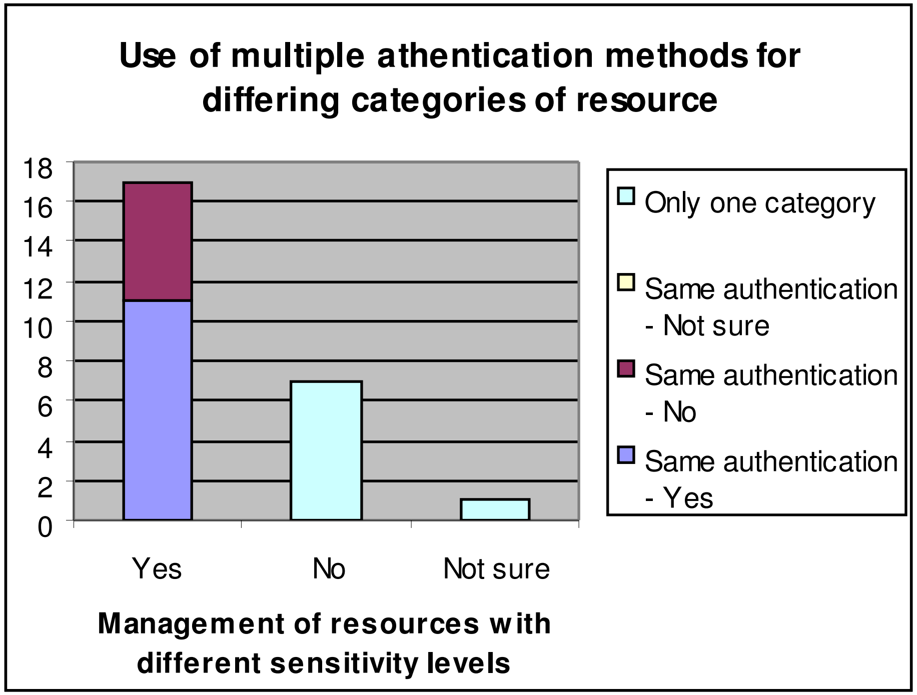
Guidelines and governance

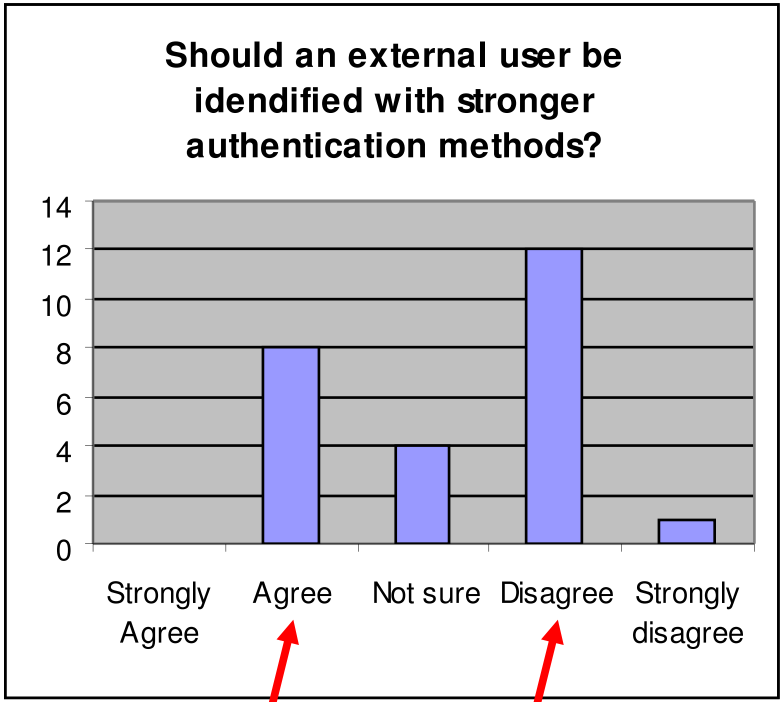




MANCHESTER
1824

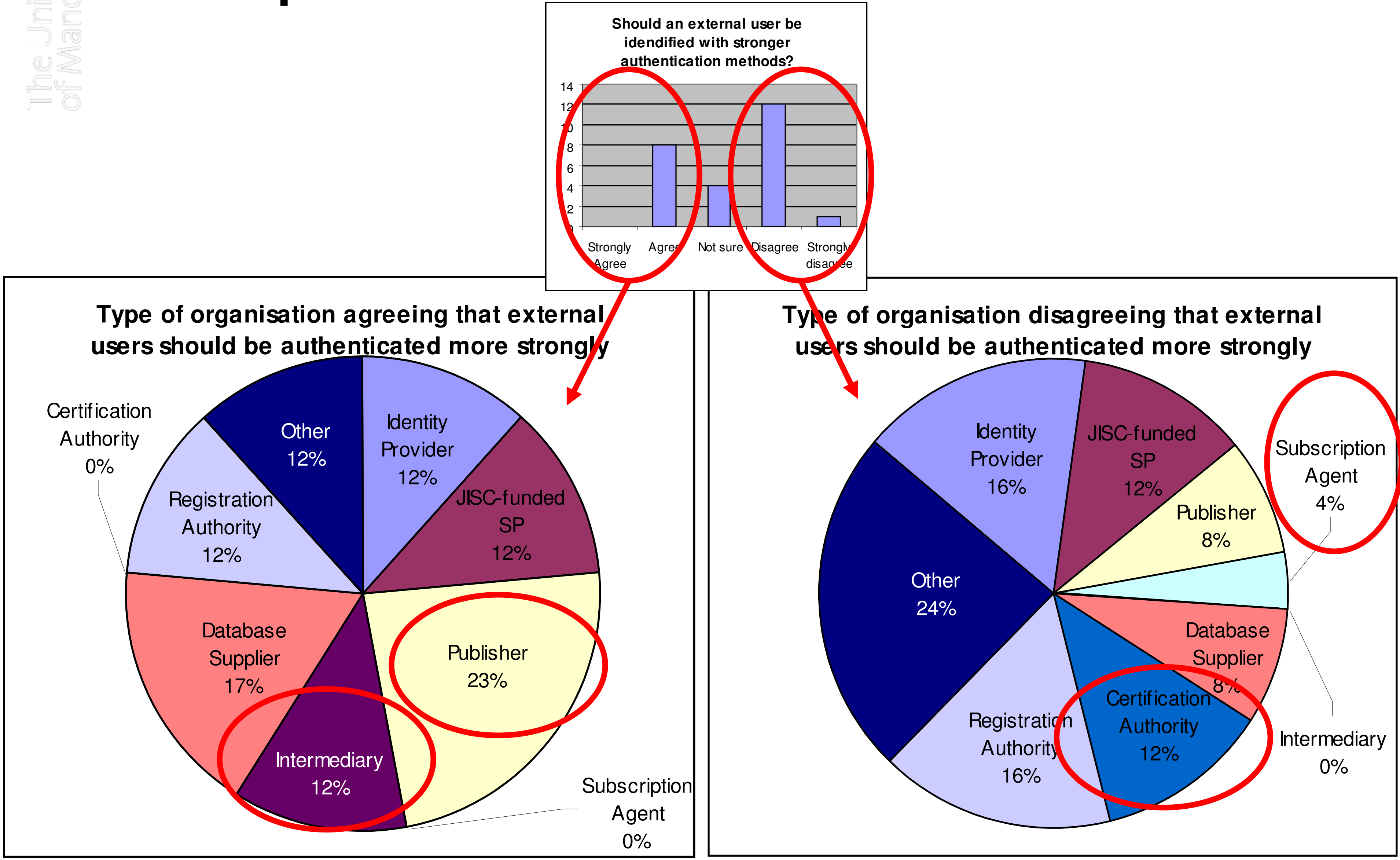
Multiple authentication methods



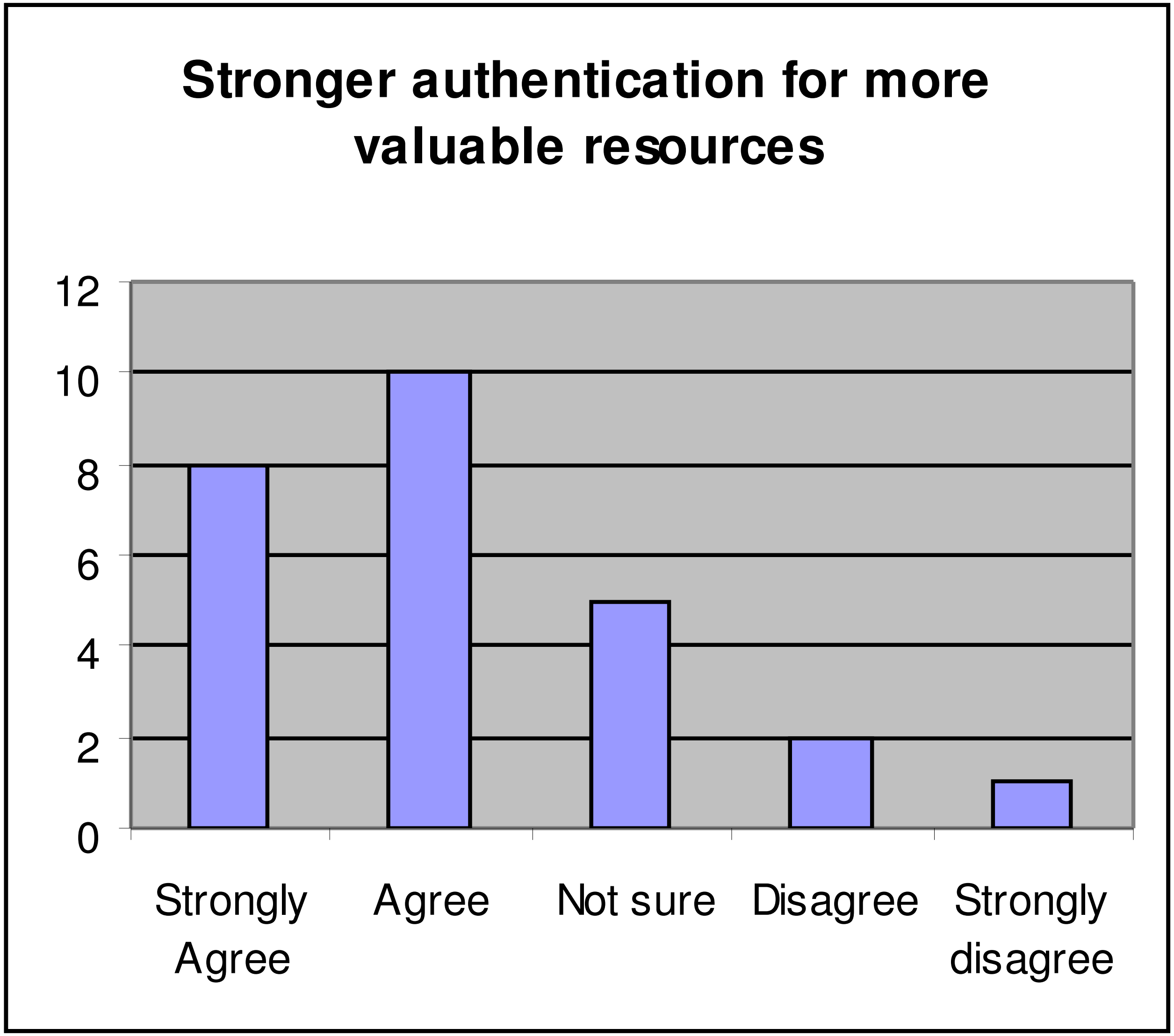


Split interests

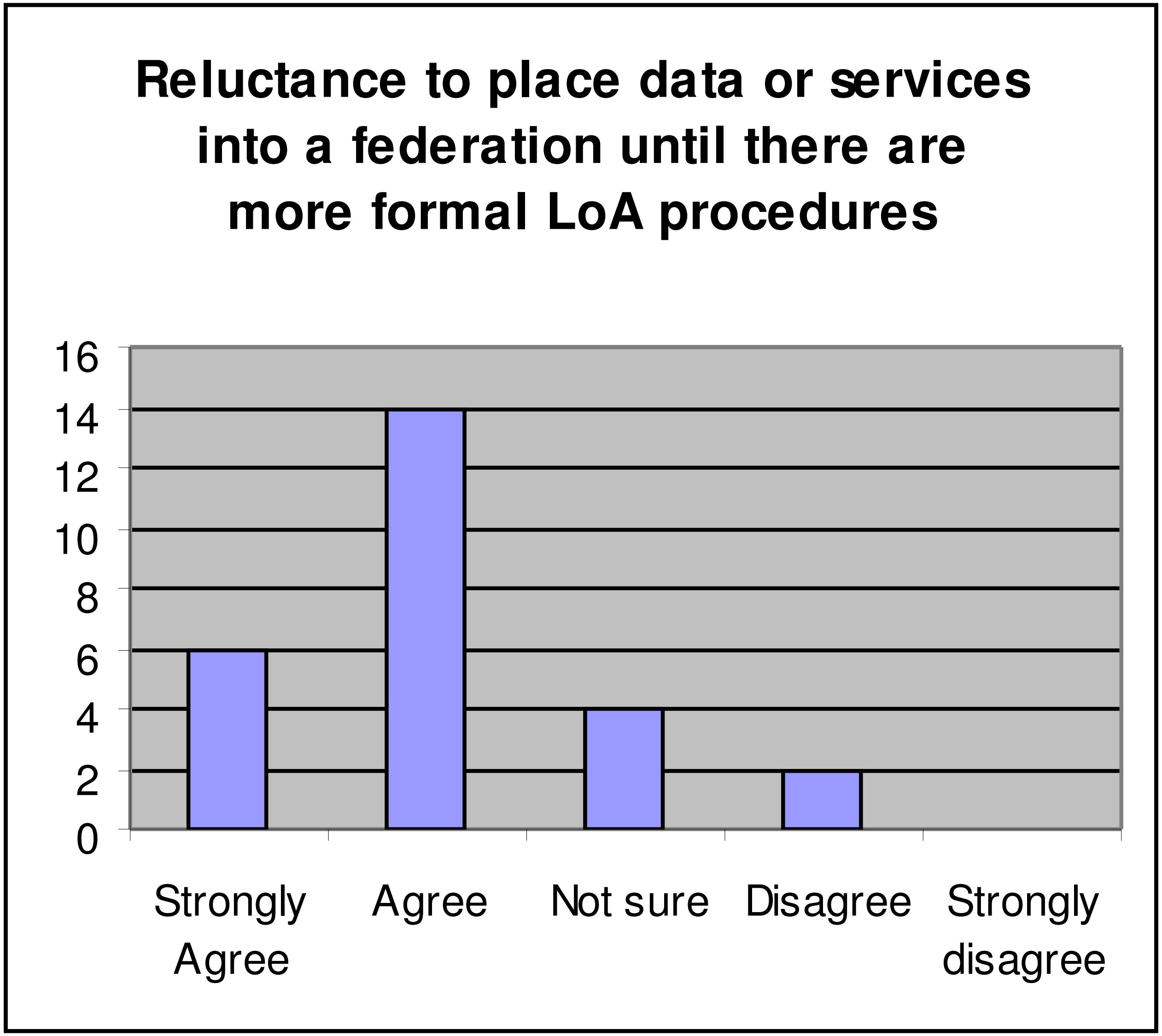
Multiple authentication methods



Do valuable resources need stronger authentication

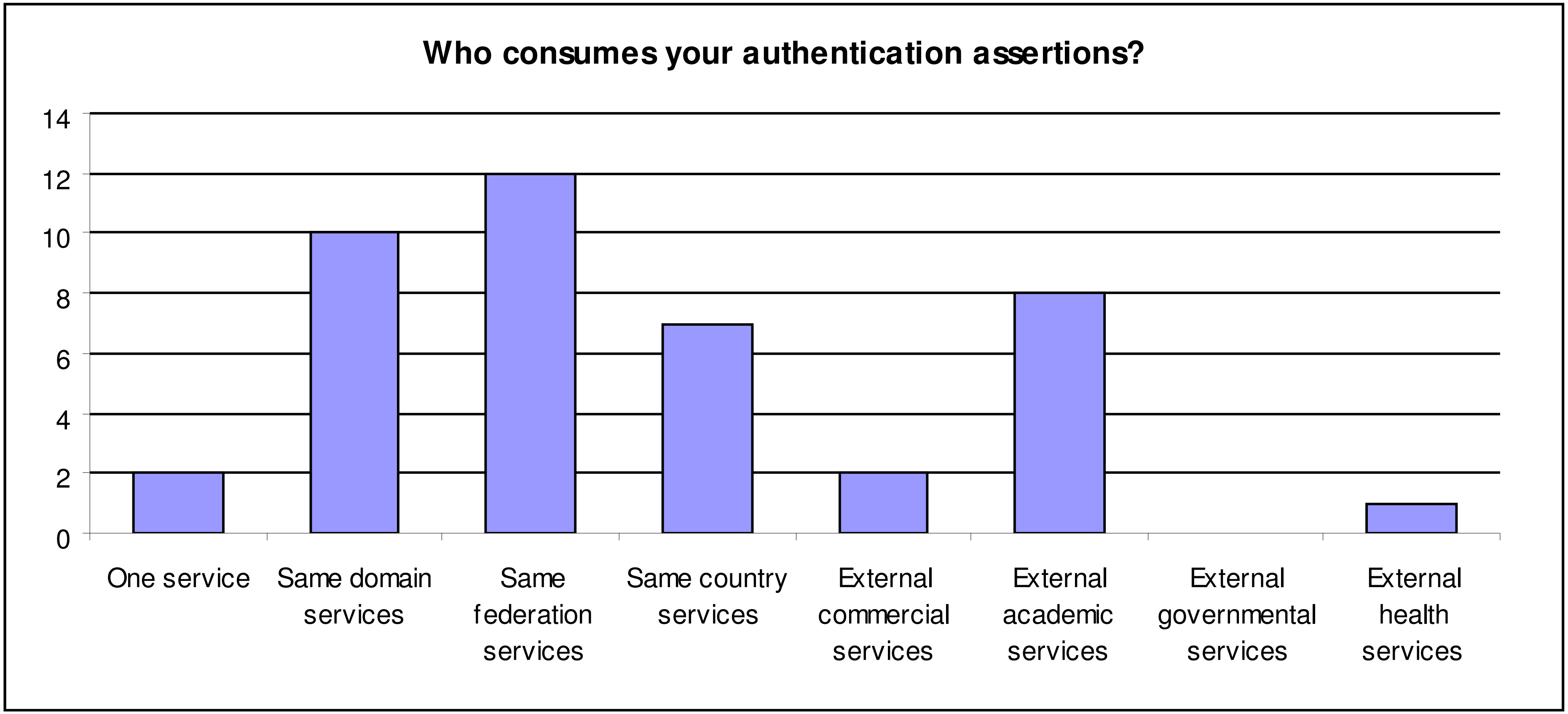


LoA drives willingness to join a federation

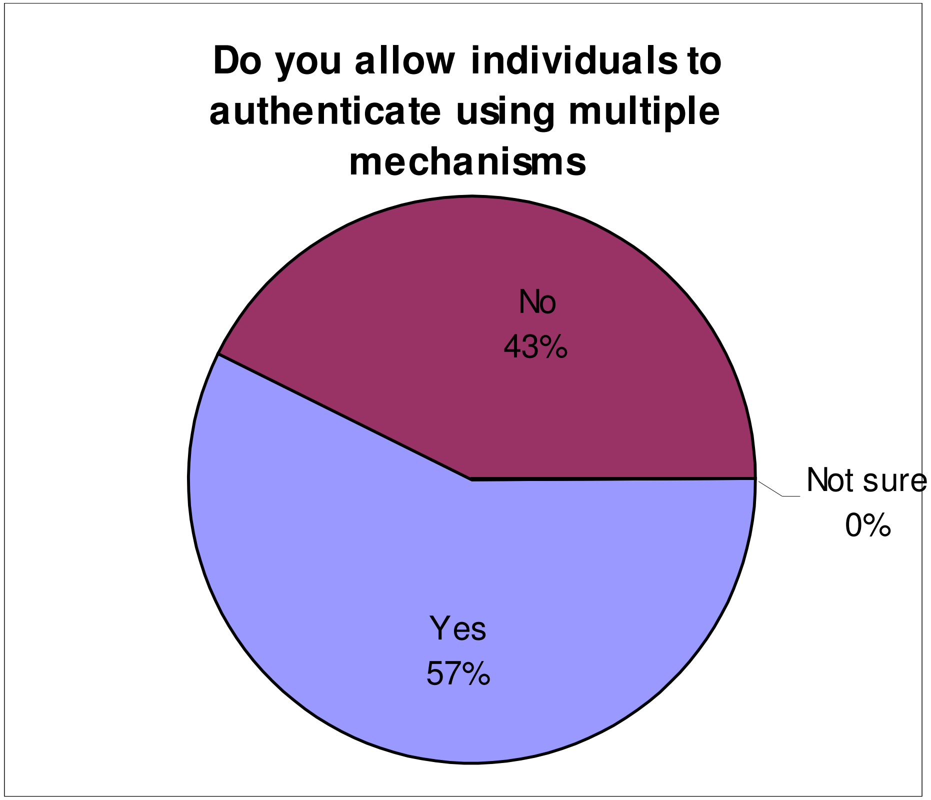


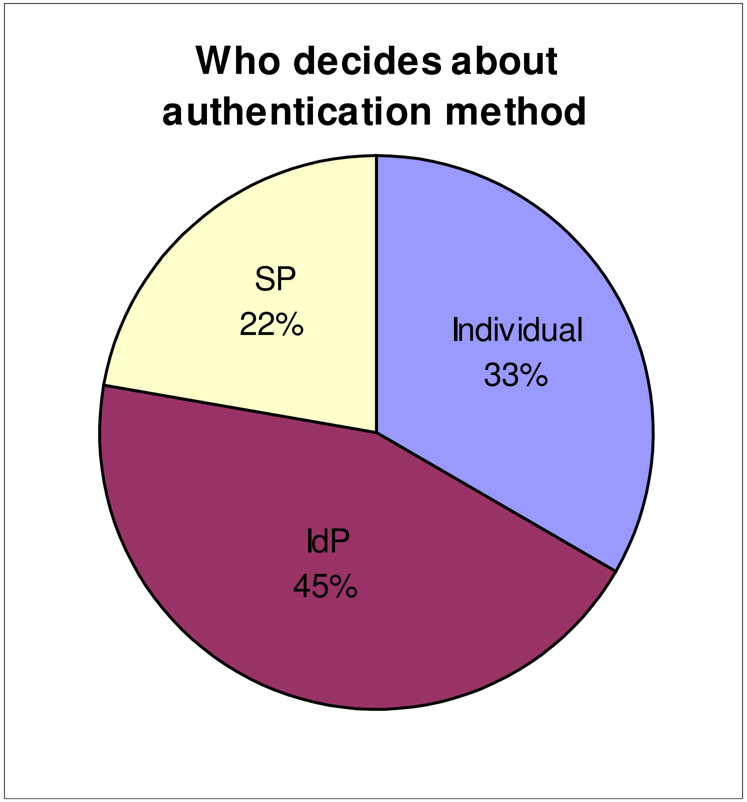
Questioning Identity Providers

Where assertions go

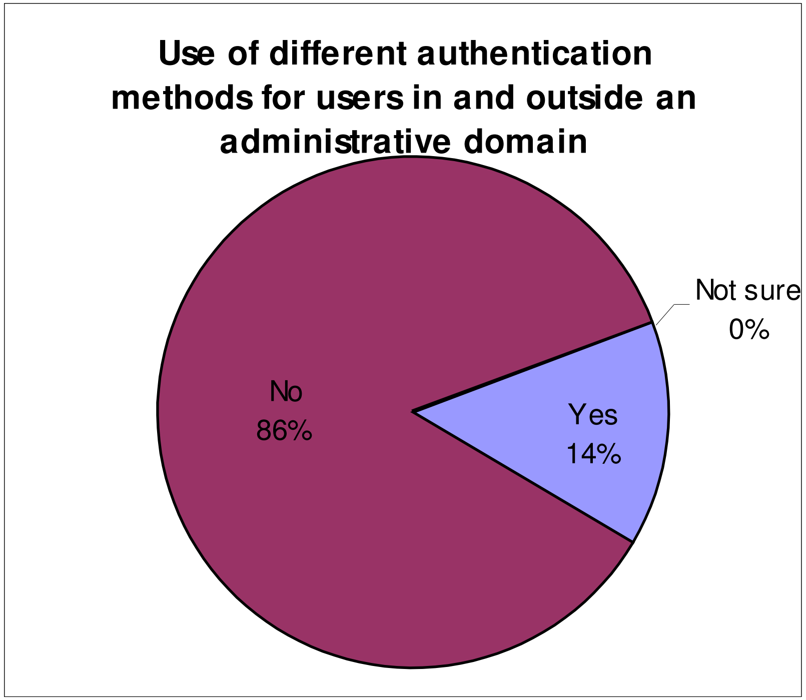


Authenticating more than one way

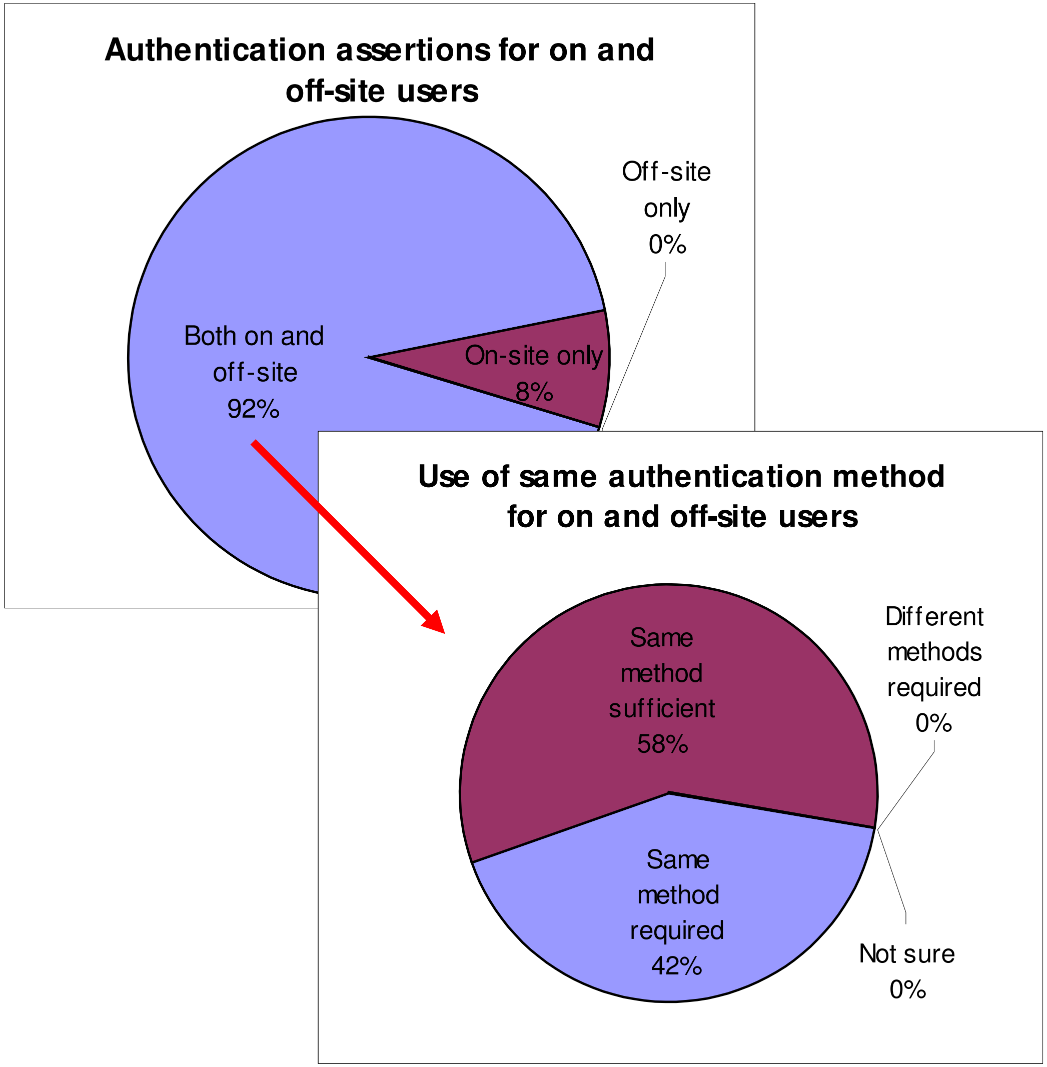




Identifying your own



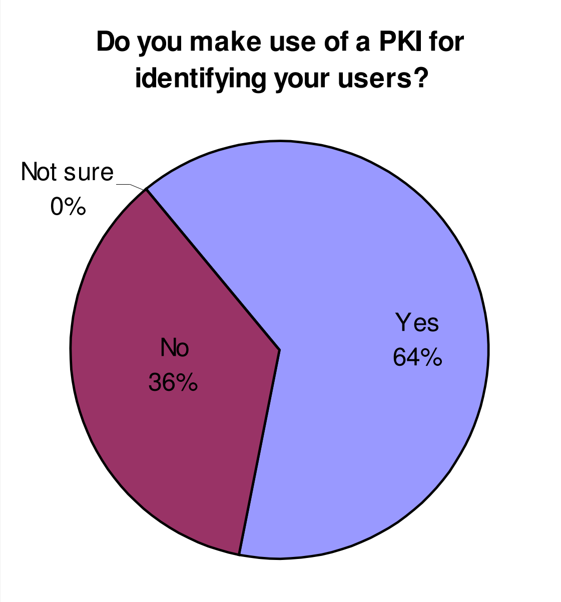
Use of different authentication methods for users in and outside an administrative domain

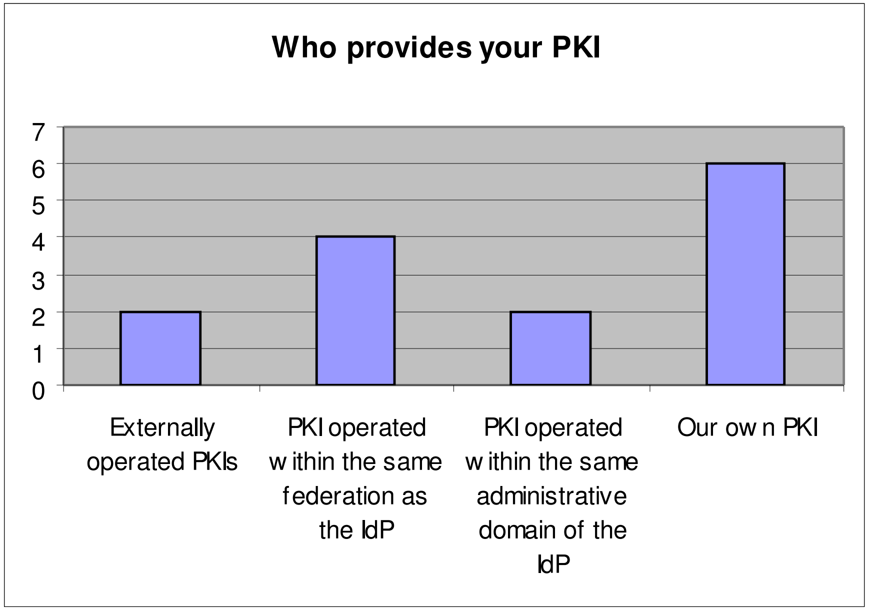


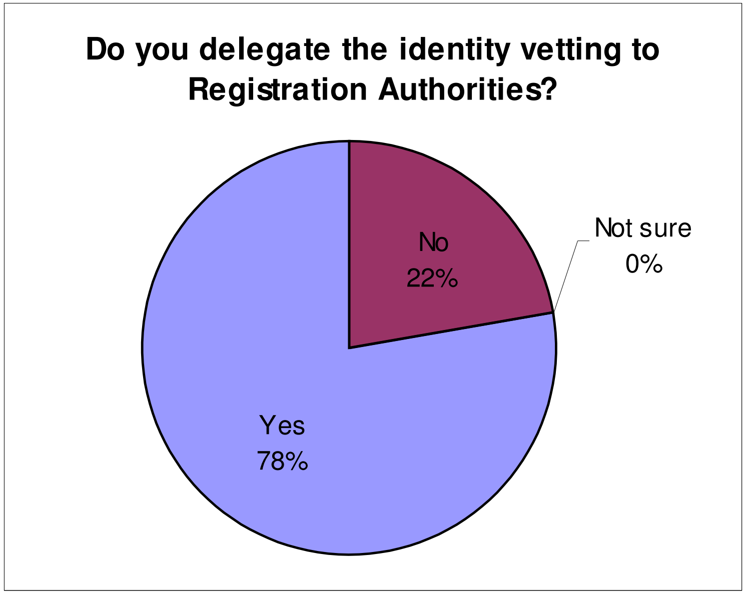
Authentication assertions for on and off-site users

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

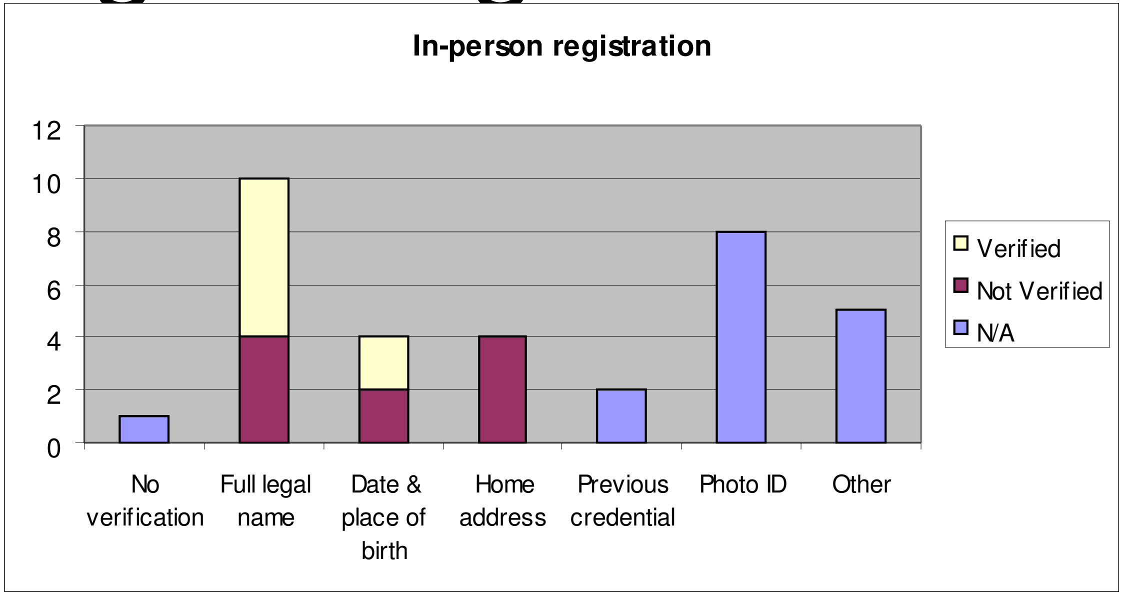
The use of PKI

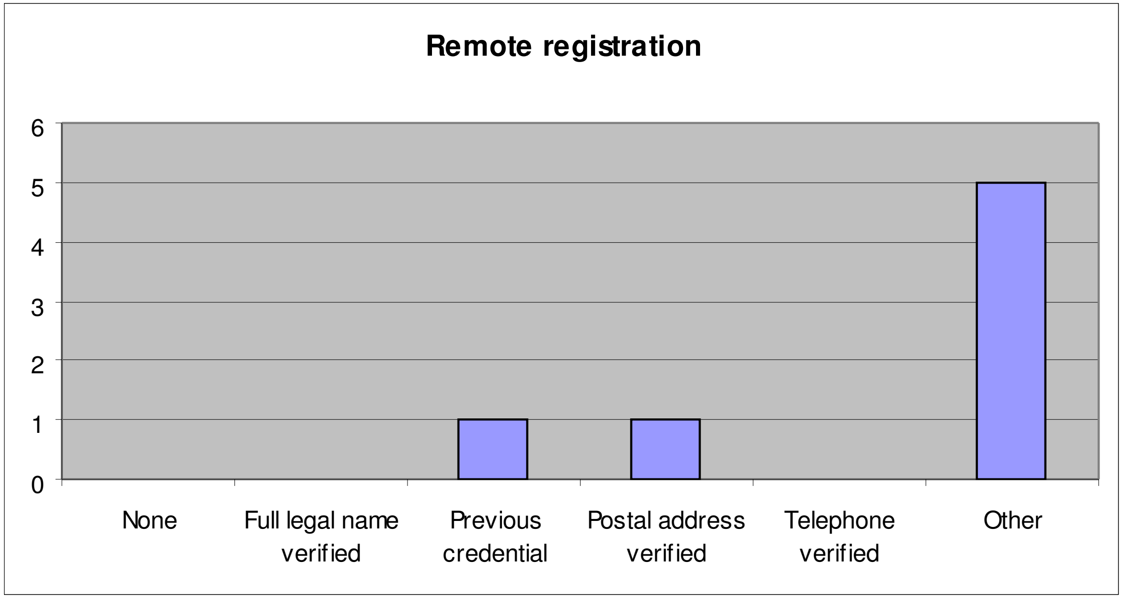






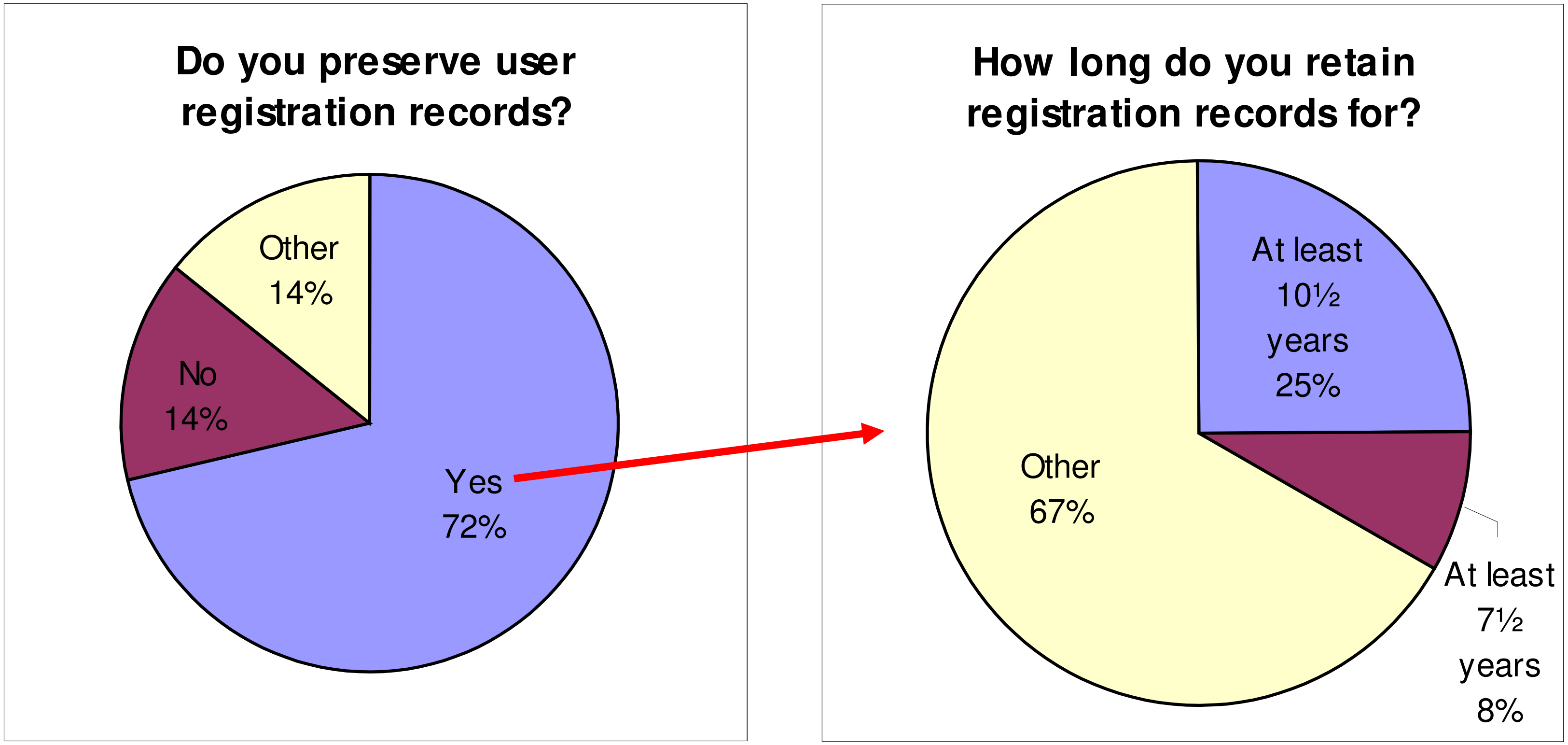
Registering with the PKI





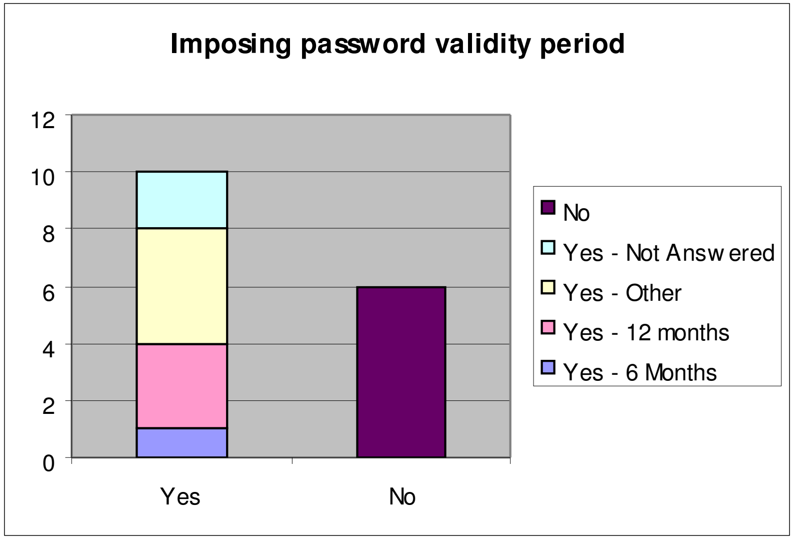
- valid matriculation card numbers,
- telephone communication with the individual
- trusted departments (e.g. payroll) to assert user attribute

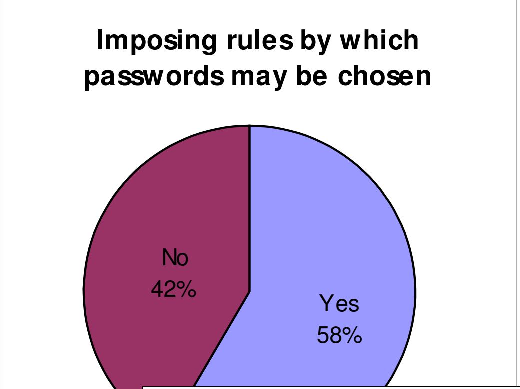
Registration records

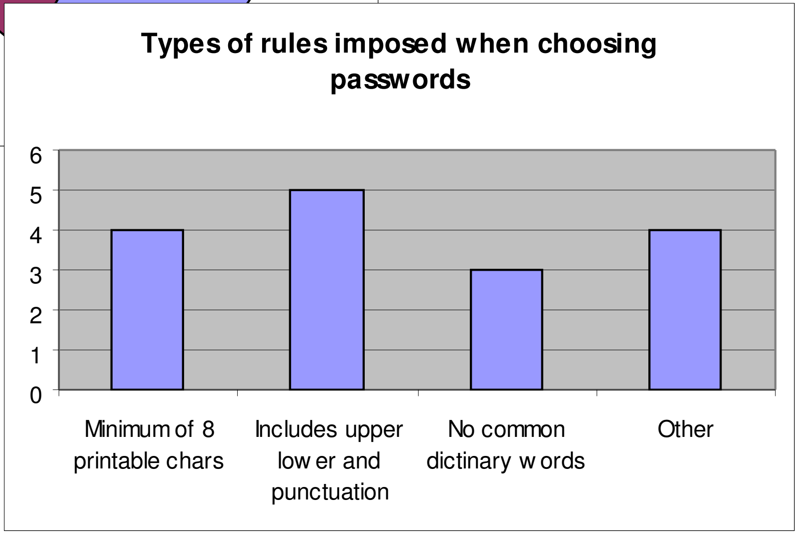


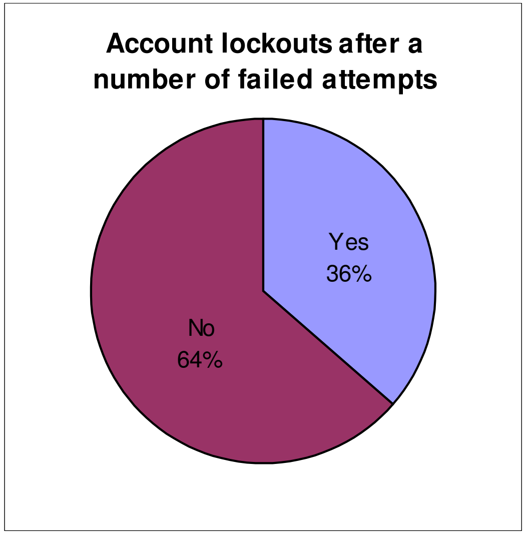
NIST SP 800-63 requires records to be kept for 7½ years for LoA 2

About user passwords


Imposing password validity period

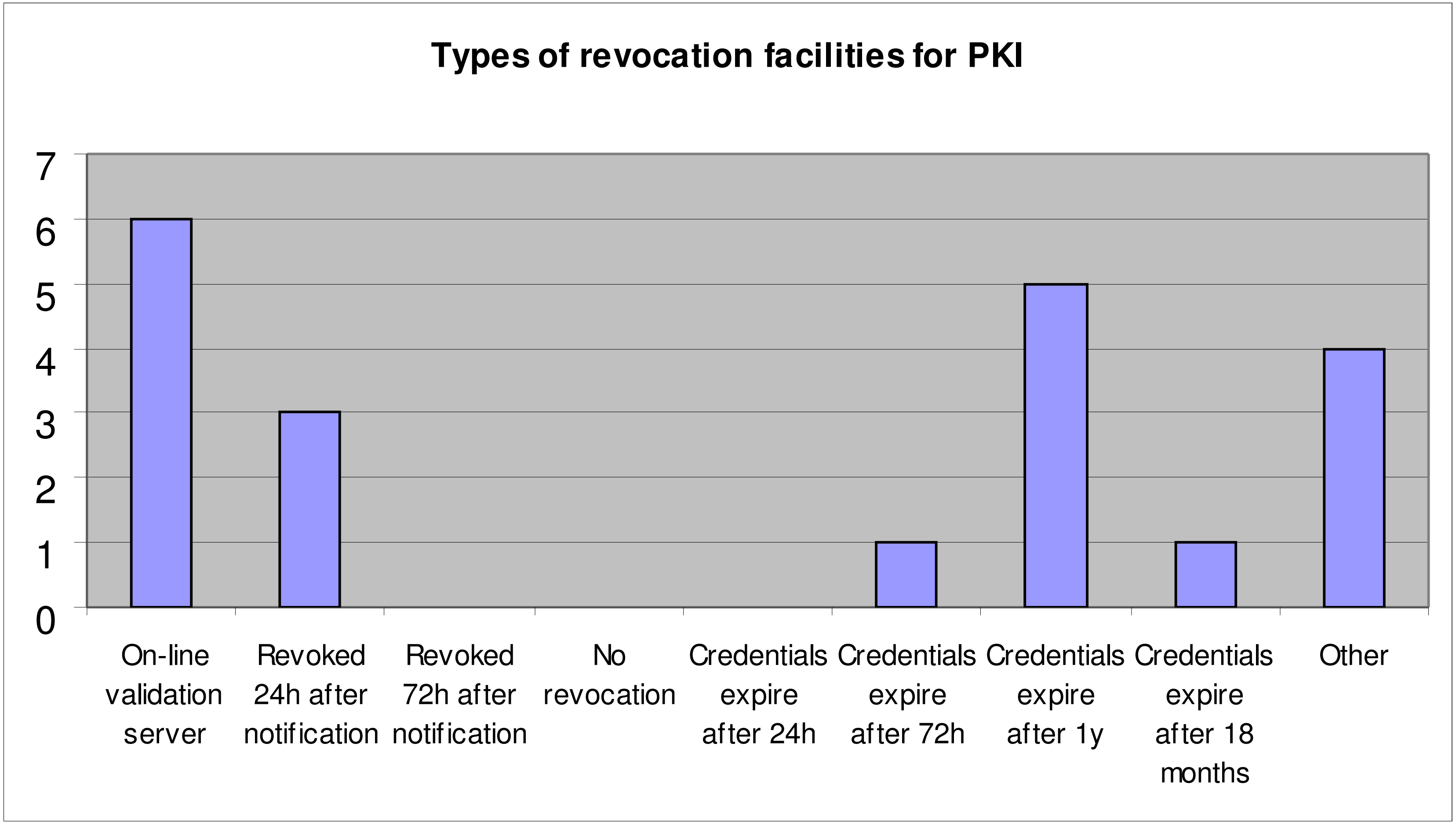

Imposing rules by which passwords may be chosen


Types of rules imposed when choosing passwords

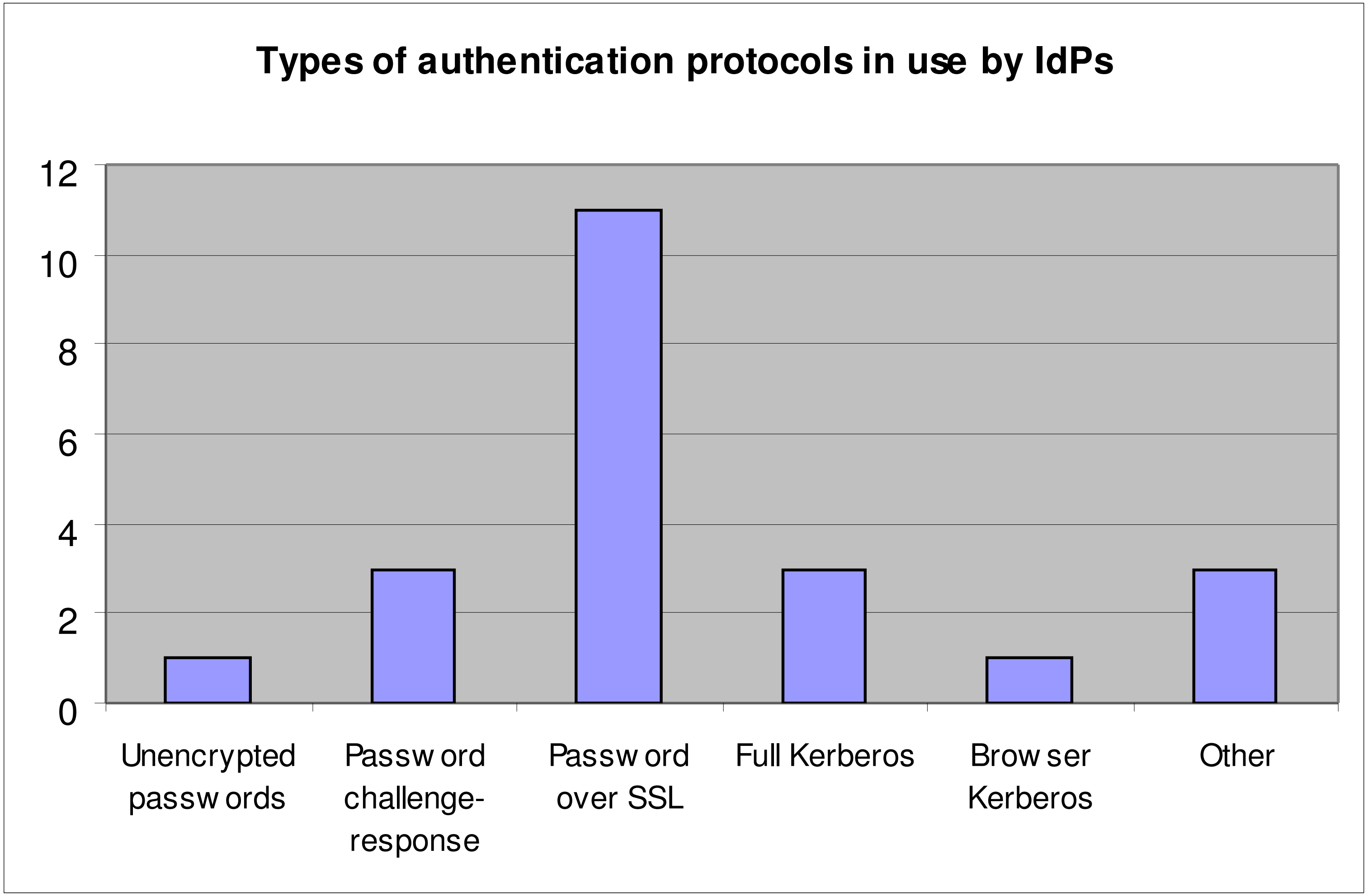

Account lockouts after a number of failed attempts

No respondents meet the lowest NIST LoA level: 1

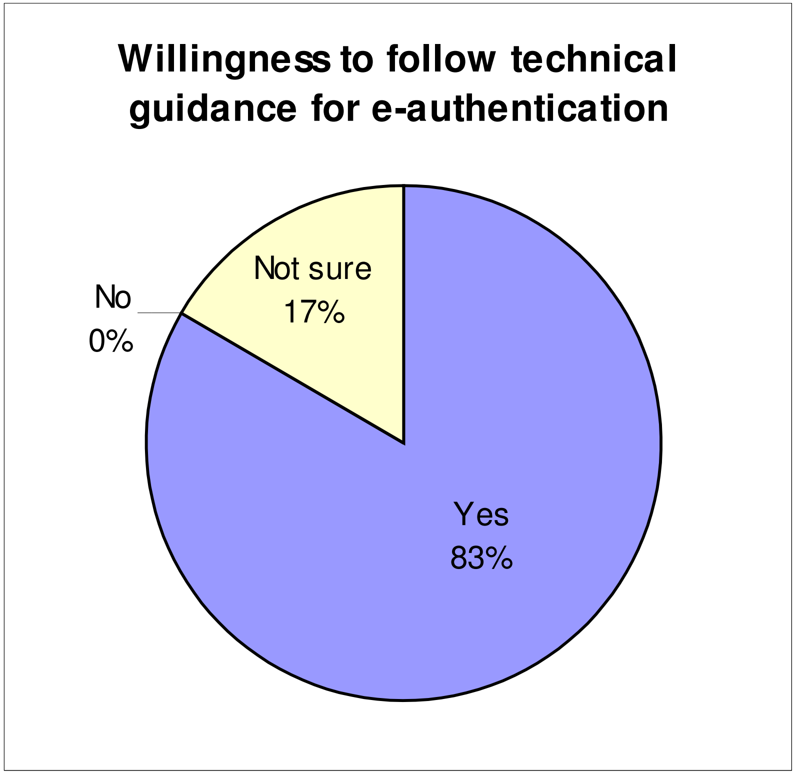
Revocation

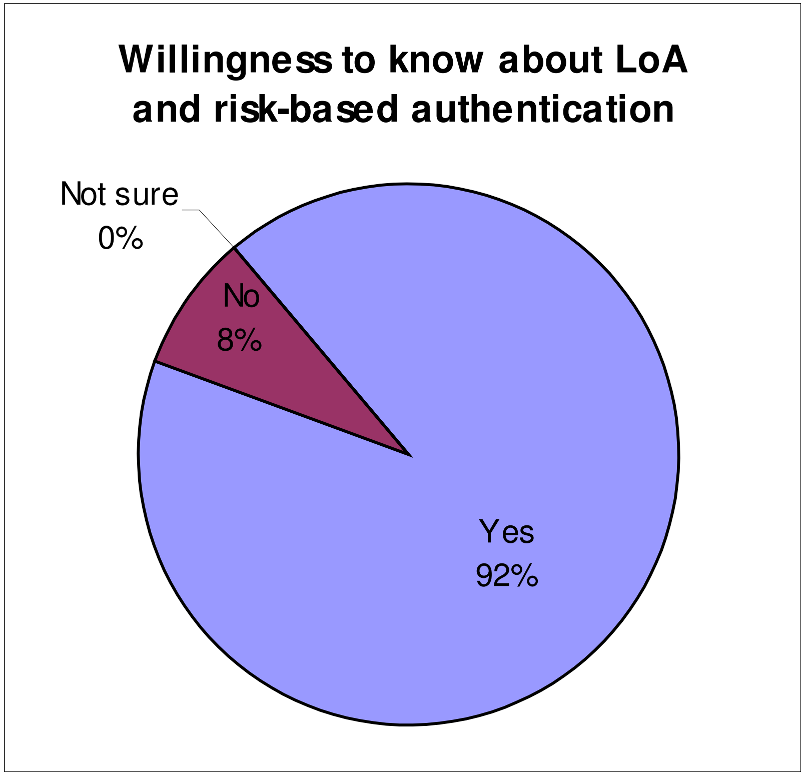

Types of revocation facilities for PKI
7
6
5
4
3
2
1
0
On-line validation server
Revoked 24h after notification
Revoked 72h after notification
No revocation
Credentials expire after 24h
Credentials expire after 72h
Credentials expire after 1y
Credentials expire after 18 months
Other

Which security protocols



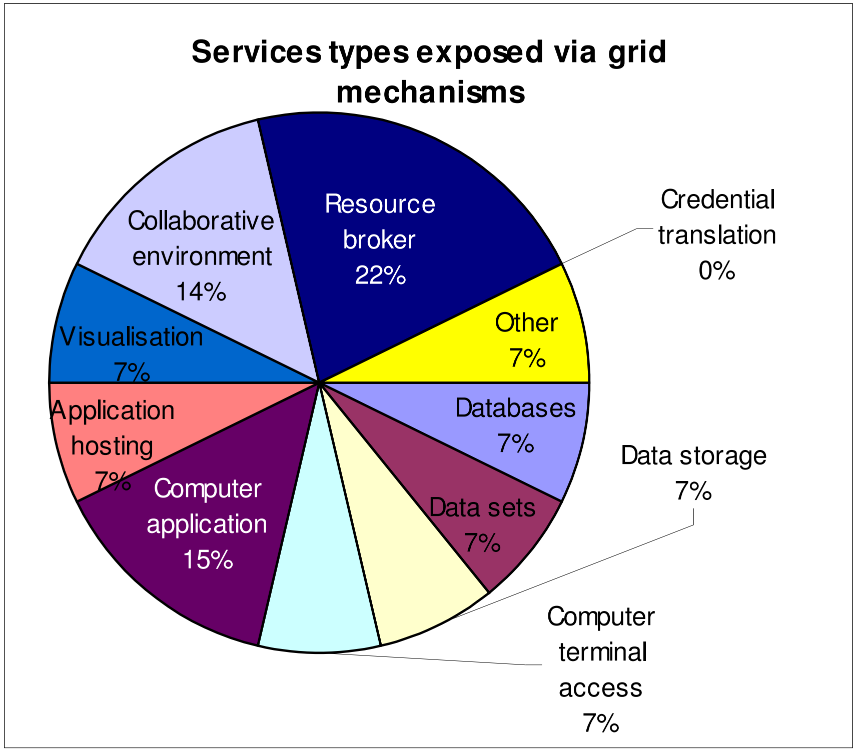
Willingness to follow guidelines

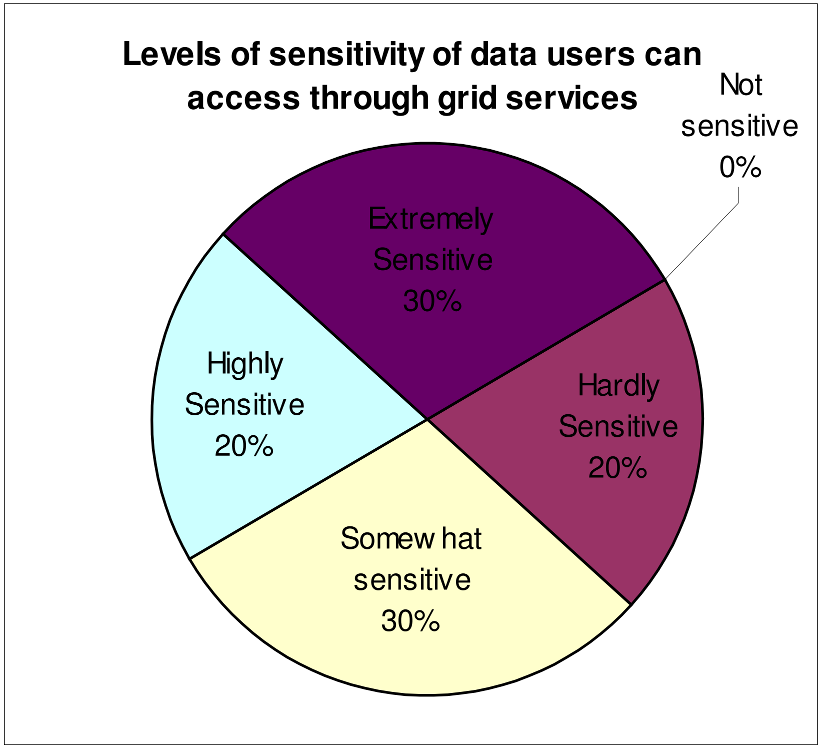




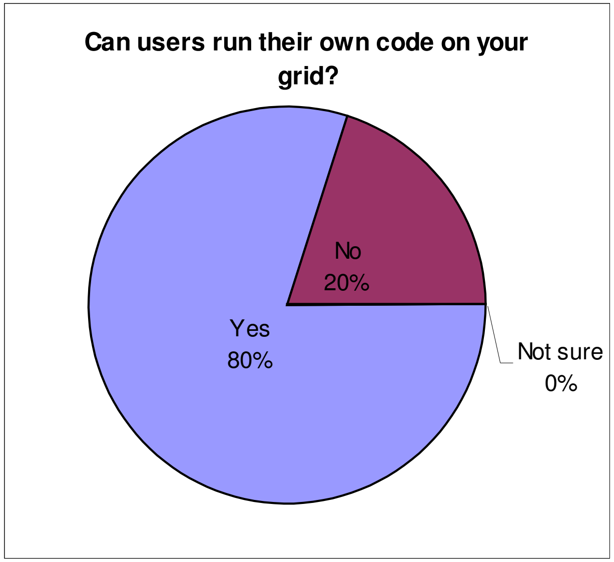
Questioning the Grid Community

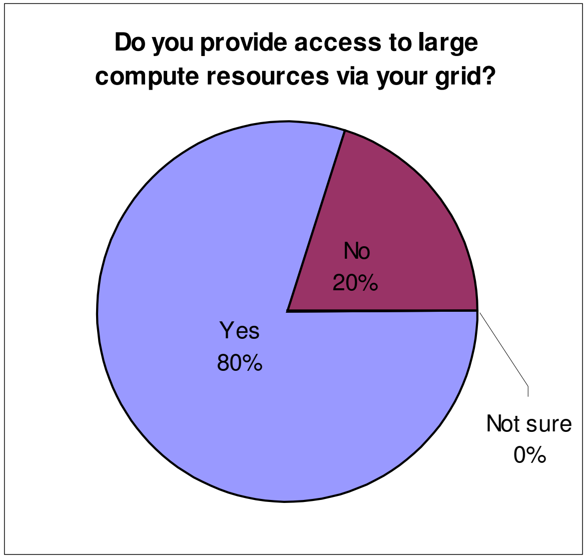
Grid resources

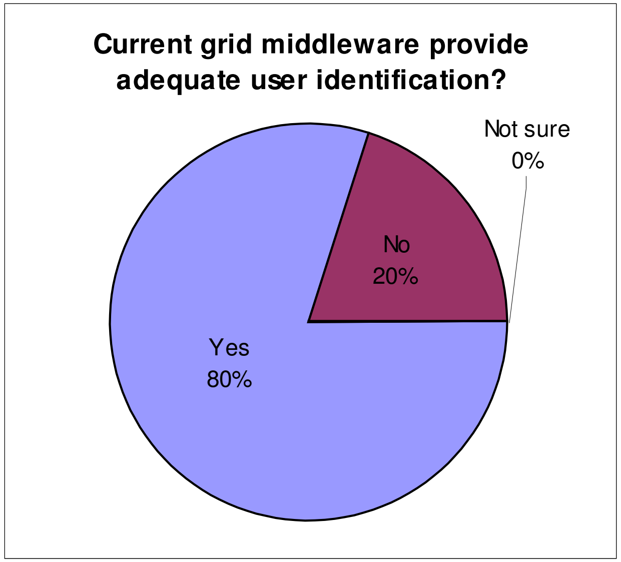




Types of risk

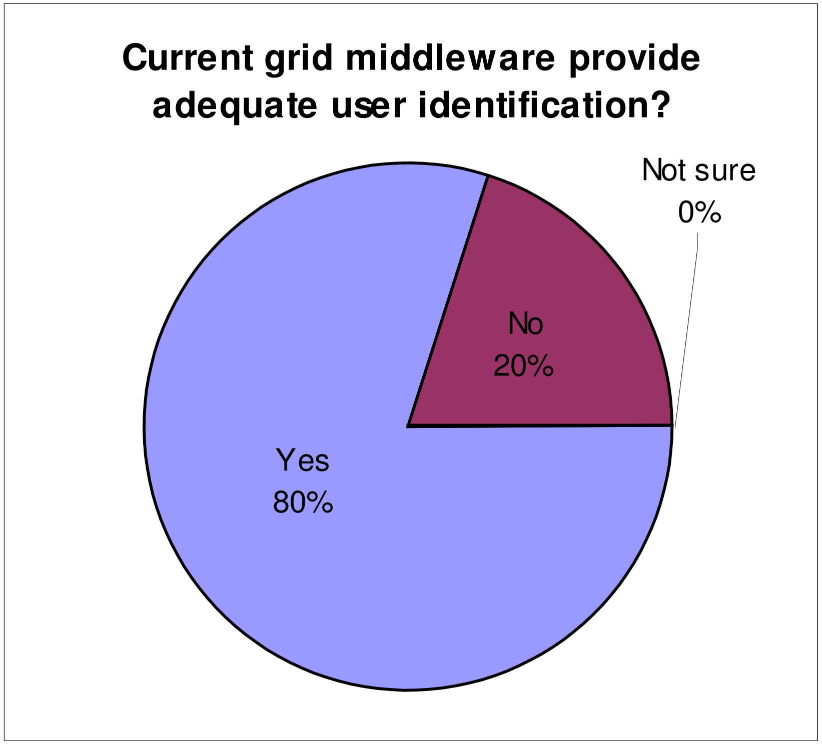




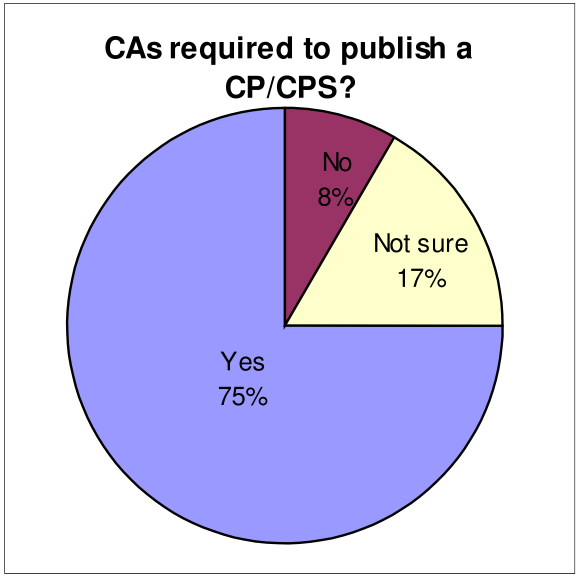


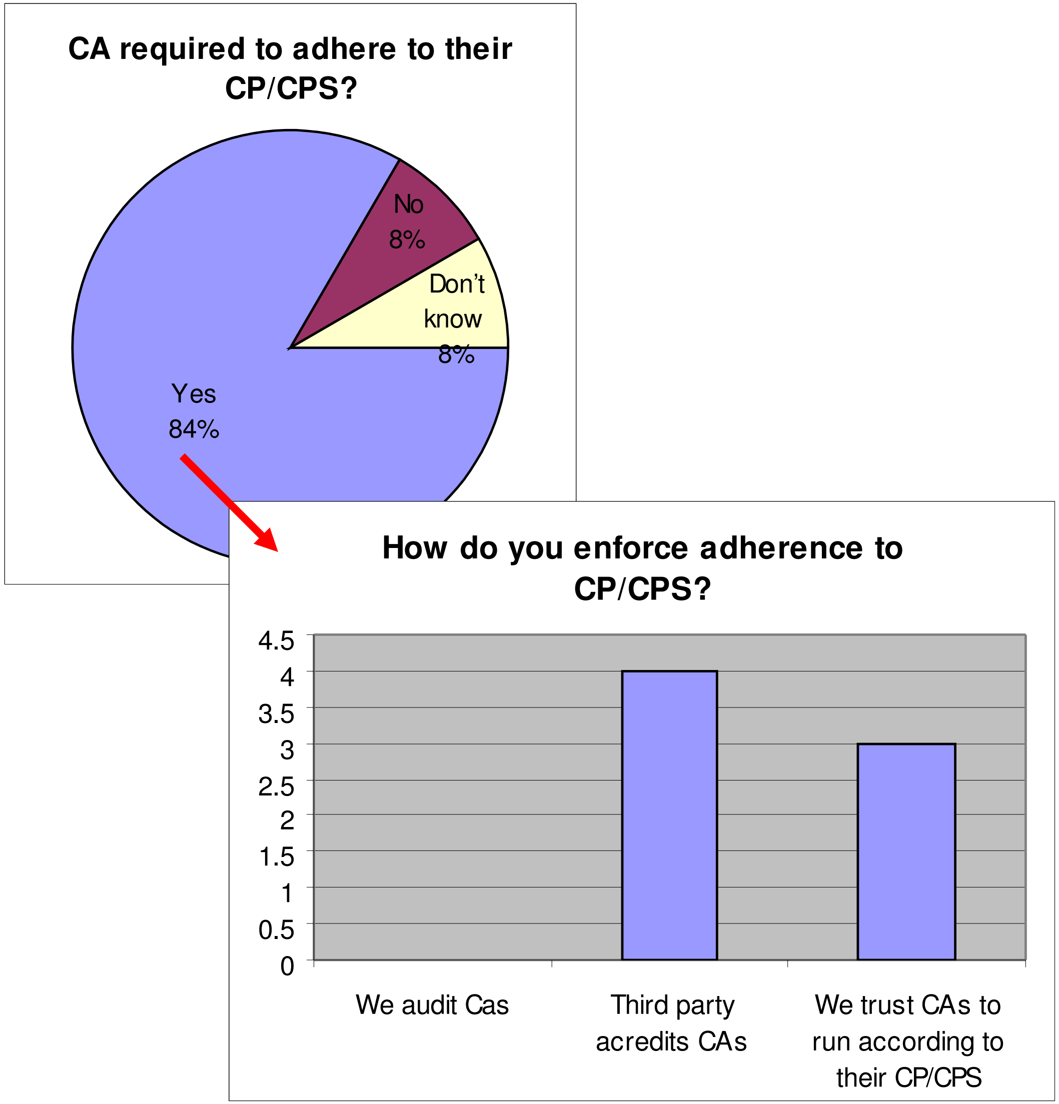
Types of identification

- 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?

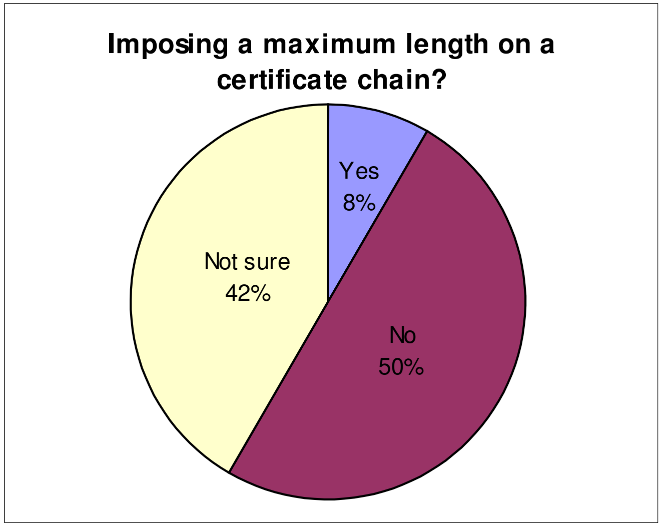

CA required to adhere to their CP/CPS?

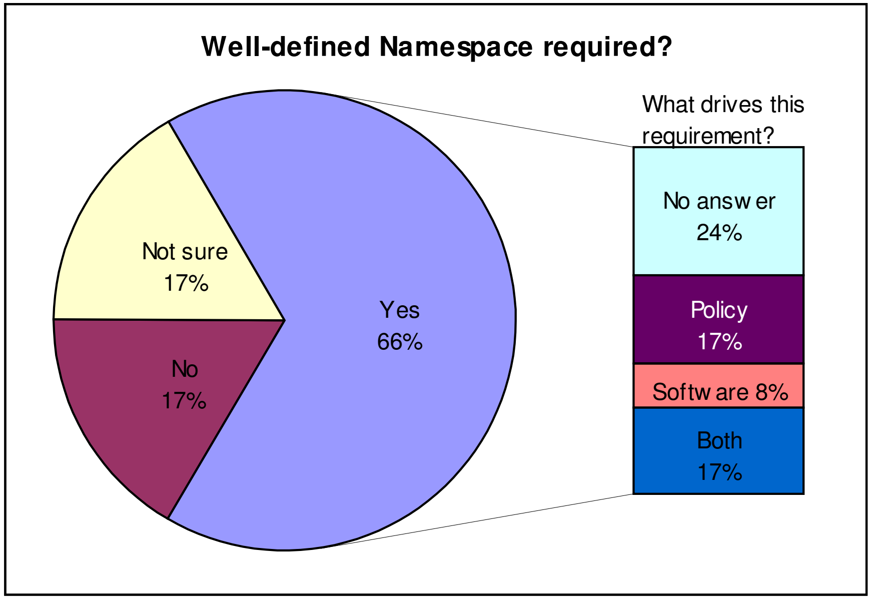
How do you enforce adherence to CP/CPS?

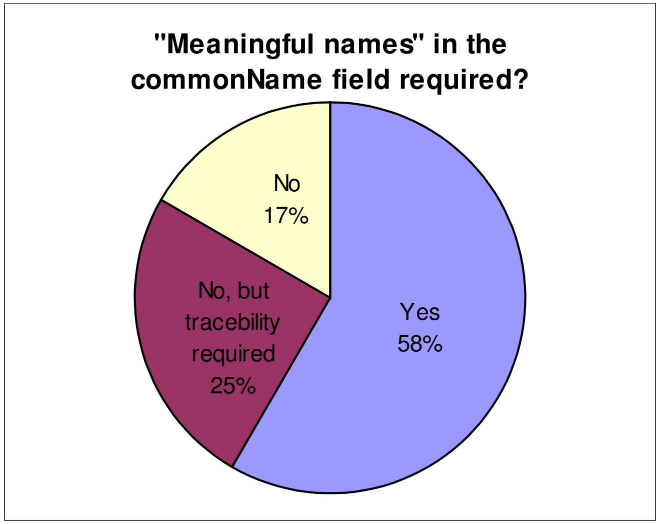
MANCHESTER
1824

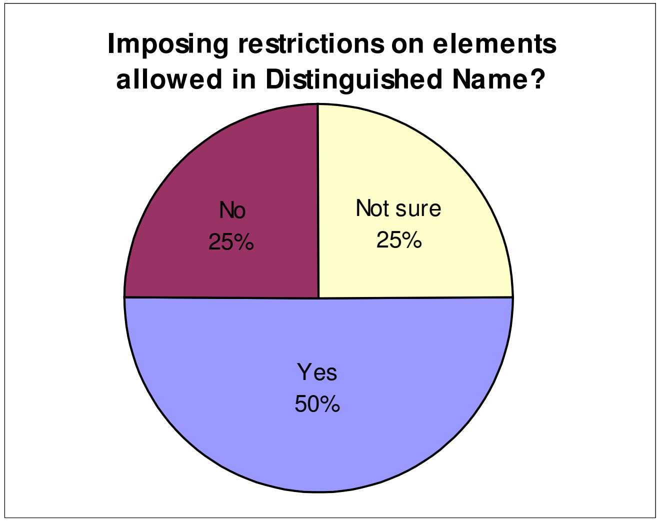
The University
of Manchester

PKI Certificates

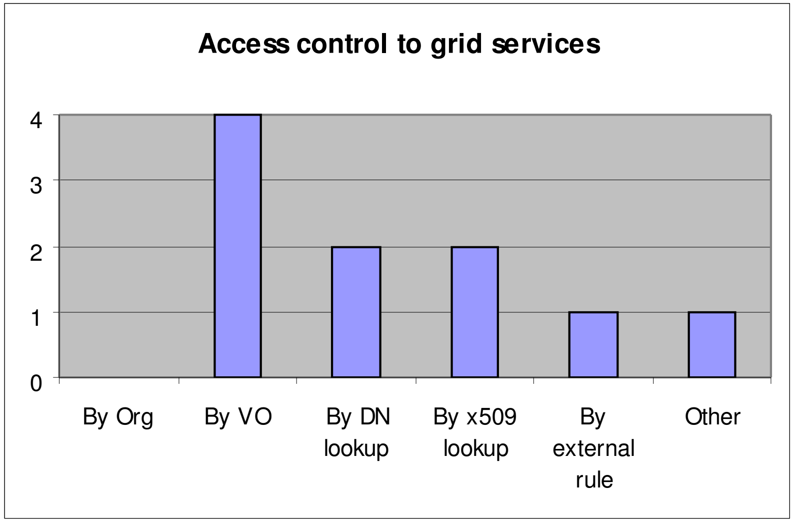


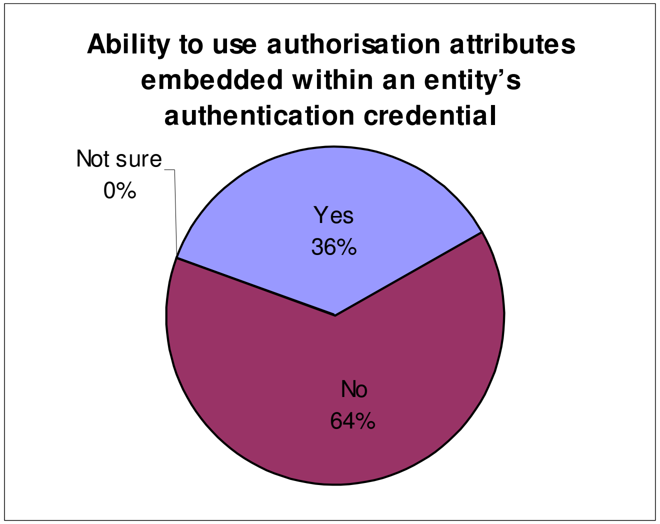


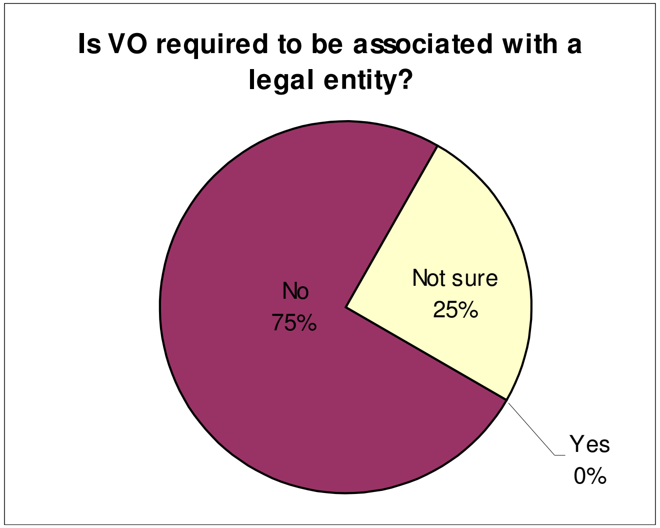




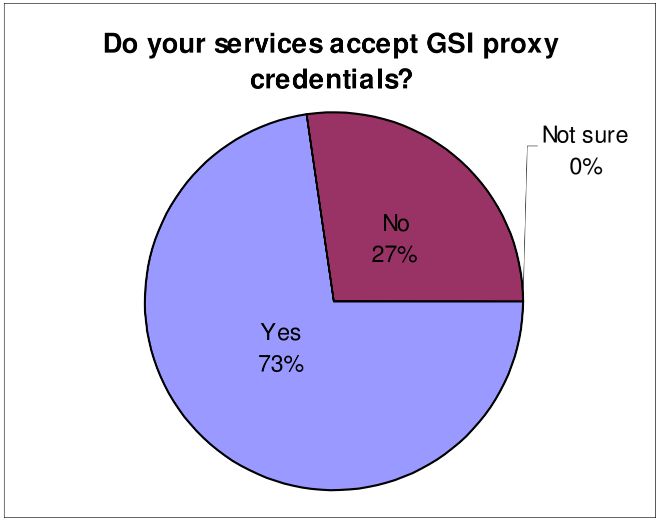
Controlling access

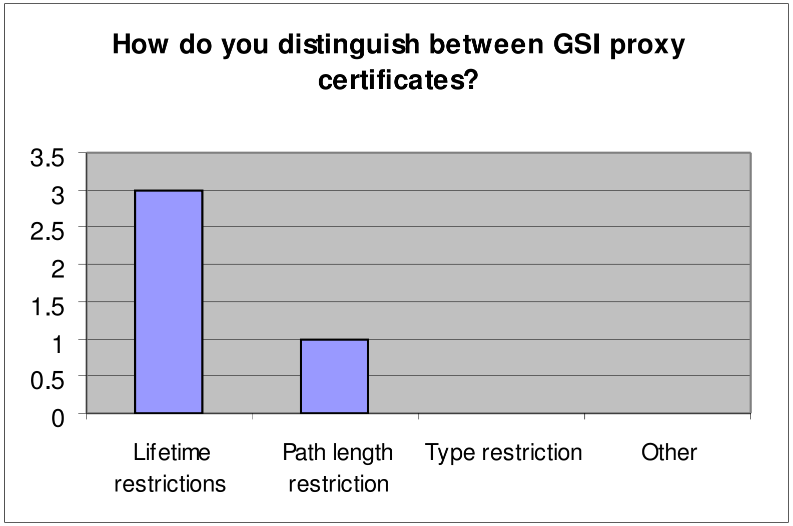






GSI Proxies


Do your services accept GSI proxy credentials?
Not sure 0%
No 27%
Yes 73%


How do you distinguish between GSI proxy certificates?
3.5
3
2.5
2
1.5
1
0.5
0
Lifetime restrictions
Path length restriction
Type restriction
Other

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?