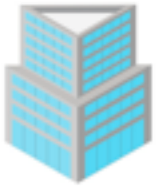
Analysis of Business Cases for Trust and Identity Federation

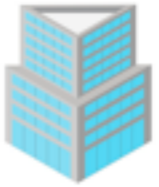
Rainer Hörbe, 13-June-2012

Kantara Initiative / OASIS

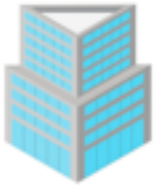
Why Identity Management?

Context
Enterprise 
B2C
B2B
G2C
G2G

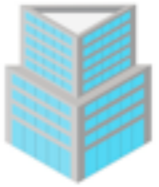
Why Identity Management?

Context	*Key Issue*
Enterprise 	Increasing number of systems -> provisioning and authentication too expensive and slow
B2C	Account registration with email confirmation: 30% loss rate
B2B	Provisioning does not scale; Liability and compliance
G2C	Unique identification
G2G	Provisioning

Why Identity Management?

Context	*Key Issue*	*Solution*
Enterprise 	Increasing number of systems -> provisioning and authentication too expensive and slow	Kerberos Enterprise Directory
B2C	Account registration with email confirmation: 30% loss rate	3rd-party sign-on Facebook twitter Google OpenID Windows Live ID YAHOO!
B2B	Provisioning does not scale; Liability and compliance	Federation (Trust Frameworks; PKI, SAML)
G2C	Unique identification	National eID scheme European Citizen Card protected by EAC SAMPLE SANDRA Specimen
G2G	Provisioning	Federation (SAML)

Why Identity Management?

Context	*Key*	*Solution*	
Enterprise 	Increasing number of systems -> provisioning and authentication too expensive and slow	Kerberos Enterprise Directory	✓
B2C	Account registration with email confirmation: 30% loss rate	3rd-party sign-on Facebook twitter Google OpenID Windows Live ID YAHOO!	✗
B2B	Provisioning does not scale; Liability and compliance	Federation (Trust Frameworks; PKI, SAML)	✓✗
G2C	Unique identification	National eID scheme	✗
G2G	Provisioning	Federation (SAML)	✓✗

Adoption? Success? Business Value?

Value Proposition for Trust & Identity Federation

Need to argue:

- Reduce OpEx
- Reduce risk
- Improve compliance
- Improve customer satisfaction
- Increase existing business
- Develop new business
- Feasibility

Need to know:

- Operational in which industries?
- Metrics?
- CapEx, Opex, saving?
- Trust constellation?
- Technology?
- Trust framework?
- Benefits

Replace business plans with factual data!

Bad News: Critical Voices

- „eID does not really take off“ [1]
- „Claims of federated IDM are unrealistic; IDs cannot be easily abstracted from business context“ [2]
- „Arguments for failed FIM-projects: Technical interoperability, liability, privacy, economic model.“ [3]

[1] H. Kubicek, “Zeit für einen Paradigmenwechsel – Schlussfolgerungen aus einem Vergleich von eID-Systemen in acht Ländern,” eGov Präsenz, vol. 11, no. 1, pp. 50–52, 2011.

[2] S. Wilson, “Over-engineering a No-No except in digital identity!” Jan. 2011. [Online]. http://lockstep.com.au/blog/2011/01/11/id-over-engineered

[3] S. Landau and T. Moore, “Economic tussles in federated identity management,” in 10th Workshop on the Economics of Information Security, Jun. 2011.

Good News

- Educause reports benefit from implementing federation technology [1] (compliance, usability, OpEx saving)
- WAYF (Denmark) reports significant cost savings
- There **are** large federations, hence there must be a business value

[1] M. C. Sheehan, C. Bennett, P. Arroway, S. Grajek, J. Pirani, and R. Yanosky,"ECAR identity management in higher education, report 2011," Educause Center for Applied Research, Tech. Rep., 2011.

Approach

1. Find studies:

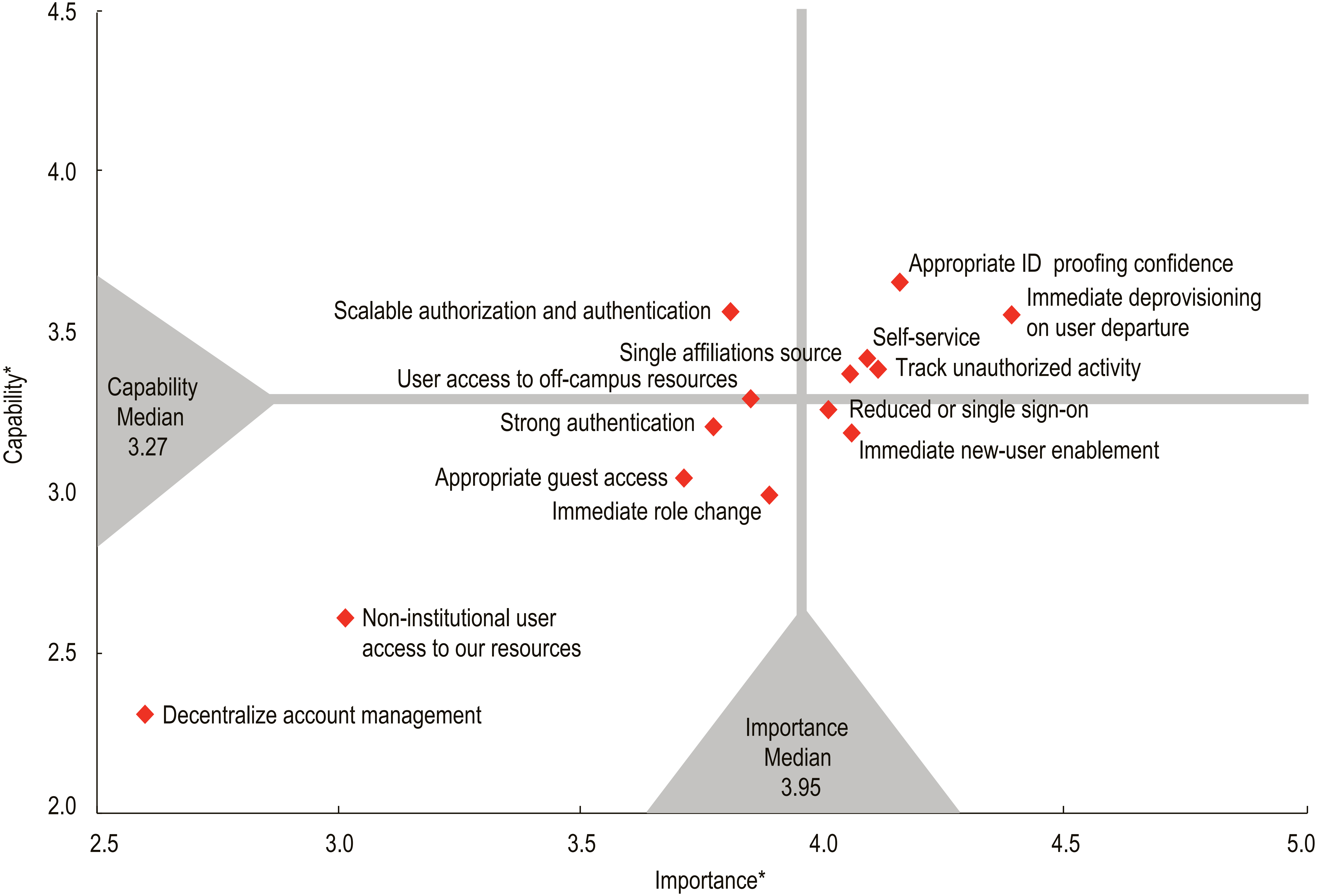
   [1] M. C. Sheehan, C. Bennett, P. Arroway, S. Grajek, J. Pirani, and R. Yanosky, "ECAR identity management in higher education, report 2011," Educause Center for Applied Research, Tech. Rep., 2011

2. Gather raw data and analyze

   Kantara BCTF Survey

Educause 2011 Report: Management View

Figure 1-1. Identity Management Benefit Mean Importance and Capability Ratings (N = 314)



Kantara Initiative BCFT DG

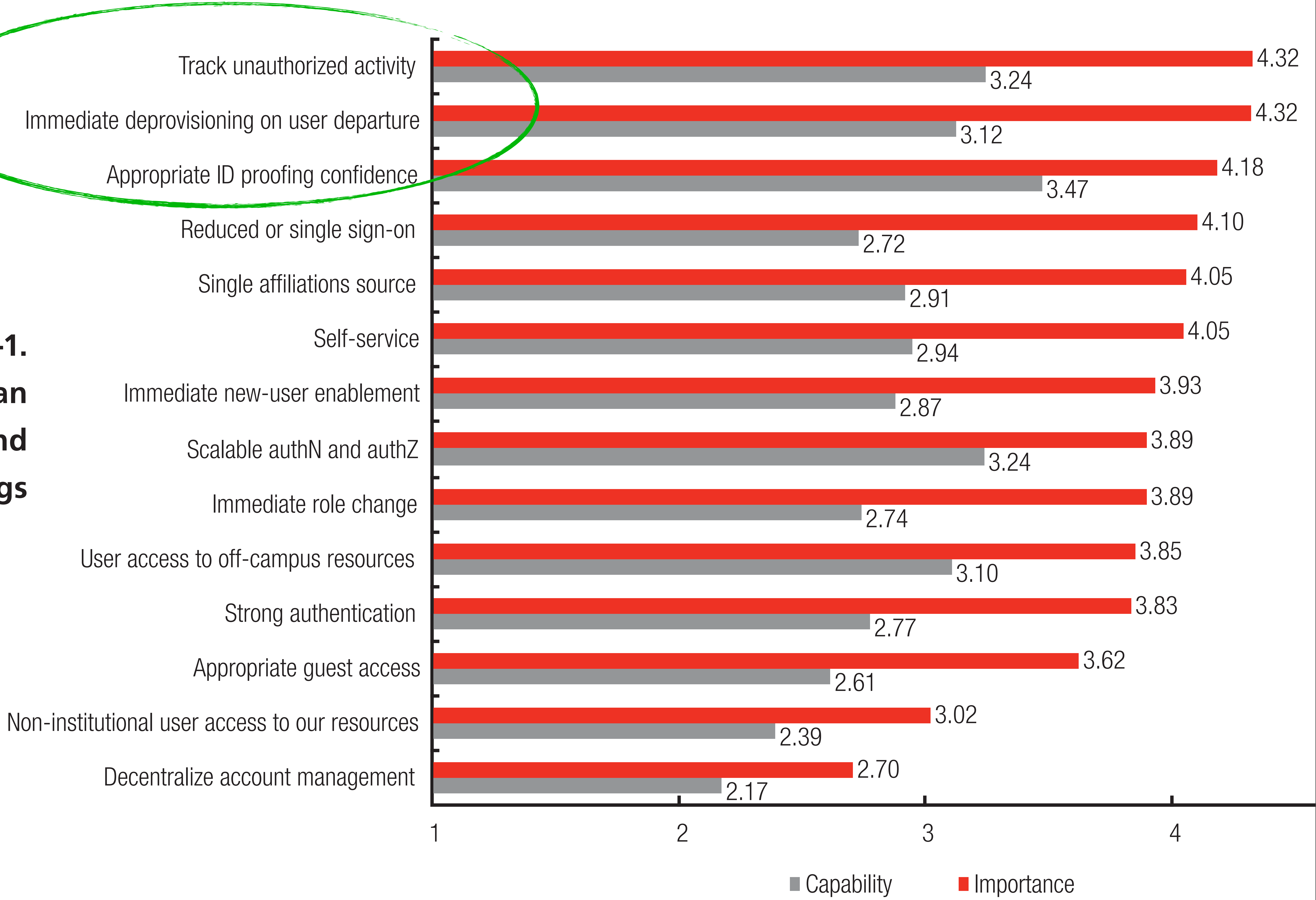


Figure 4-1. IdM Benefit Mean Importance and Capability Ratings

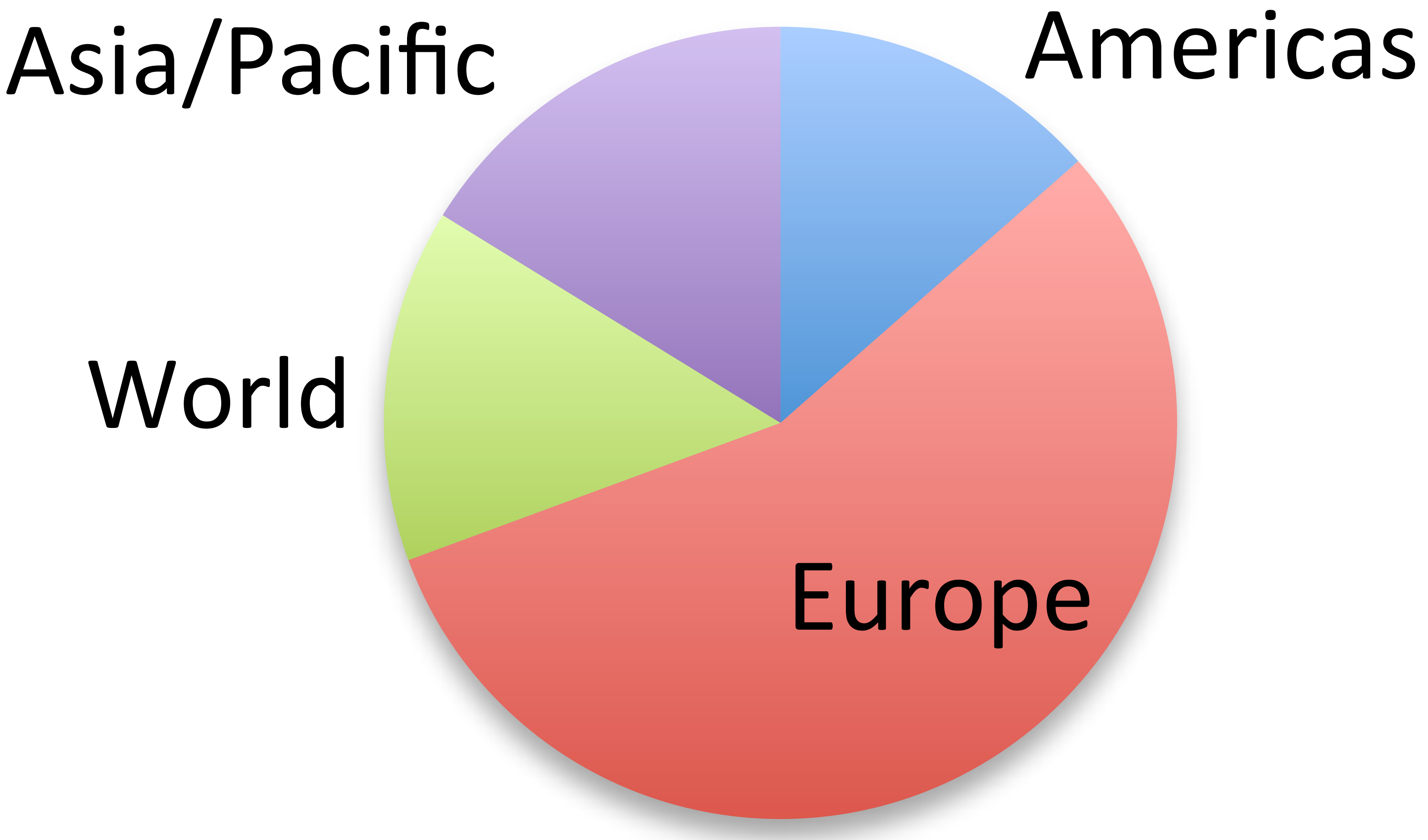
Kantara Initiative BCFT DG

Kantara BCTF Survey

- Data about identity federations is at best patchy
- To argue the value proposition a factual, quantitative basis is required
- The Kantara BCTF started data collection and analysis in 2011
- A **preliminary** report is available on the wiki: http://kantarainitiative.org/confluence/display/bctf/
- Sources from Kantara, REFEDS, EU-projects, web research and the professional network was conducted
- Data collection is probalby biased by availability of sources.

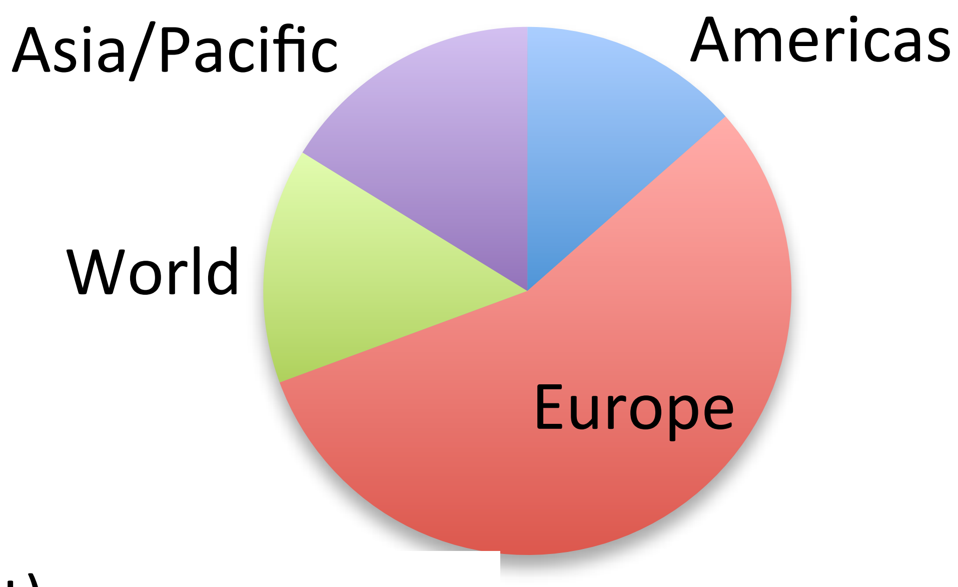
# of Federations: Geographical Breakdown

Europe	62
Asia/Pacific	18
World	16
Americas	15

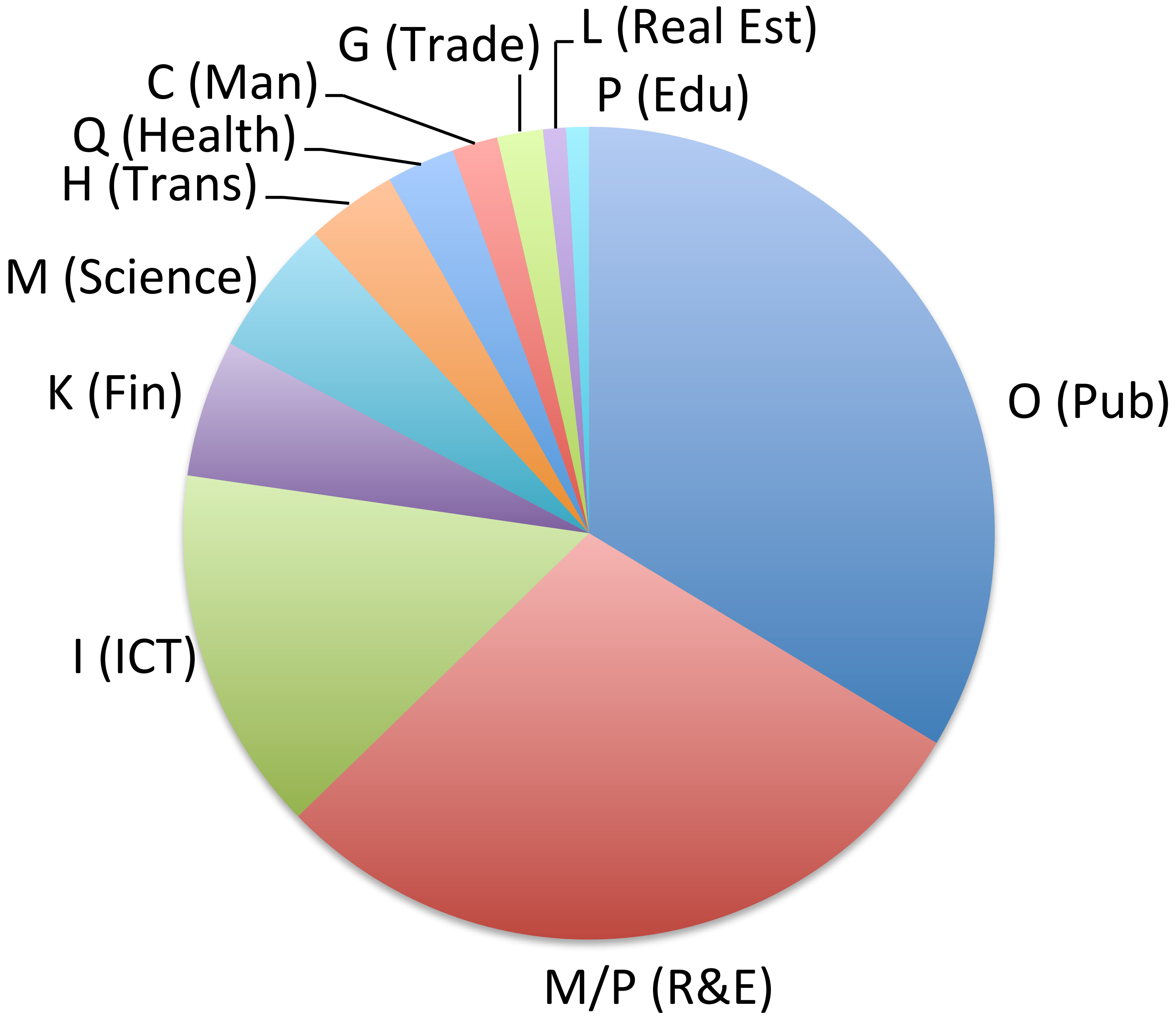


# of Federations: Breakdown by Industry

Europe	62
Asia/Pacific	18
World	16
Americas	15



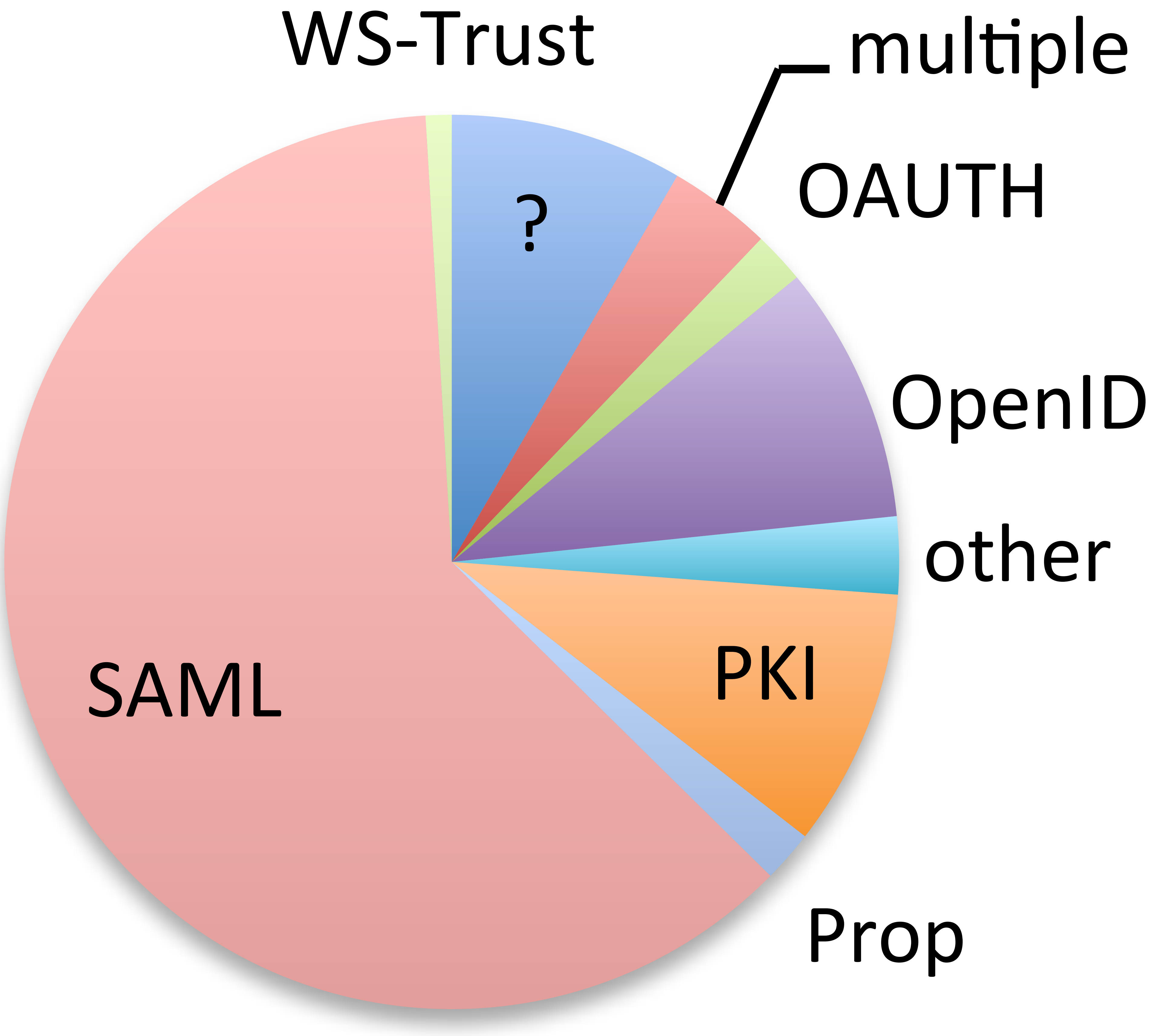
O (Pub)	37
M/P (R&E)	32
I (ICT)	16
K (Fin)	6
M (Science)	6
H (Trans)	4
Q (Health)	3
C (Man)	2
G (Trade)	2
L (Real Est)	1
P (Edu)	1



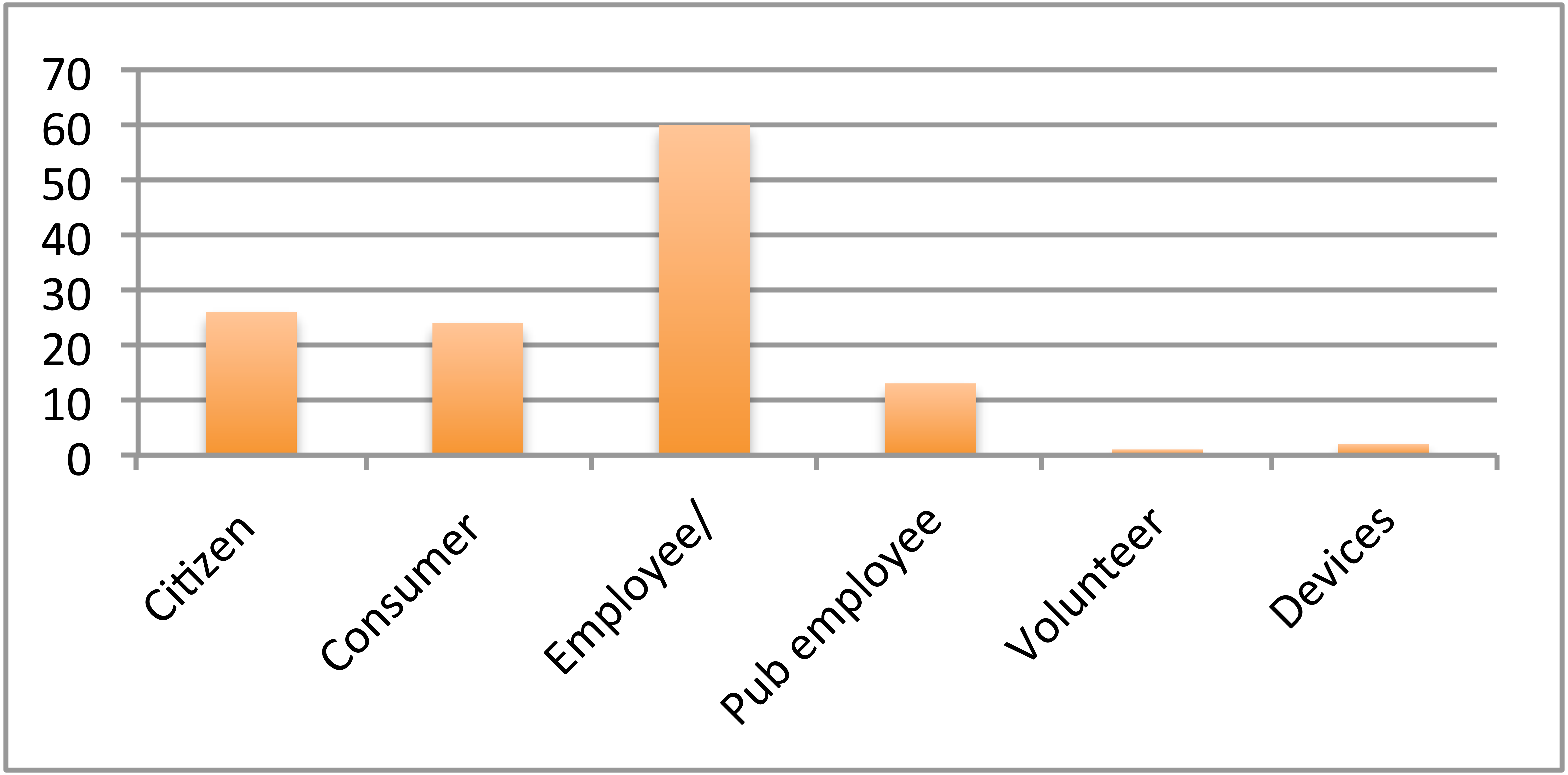
Kantara Initiative BCFT DG

# of Federations: Breakdown by Technical Protocol

SAML	66
OpenID	10
PKI	10
?	9
multiple	4
other	3
OAUTH	2
Prop	2
WS-Trust	1



Distribution by User Type



Top 5 in numbers: IDP, RP, Transctions and Users

Project Name	Description	Geog. scope	Industry	IDPs	RPs	Transactions [m/year]	Users [m]
UK Access Management Federation	NREN	UK	R&E	900	236		3
AAI@EduHr	NREN	HR	R&E	222	100	100	0,7
InCommon	NREN	US	R&E	214	140		5
FEIDE/Uninett	NREN	NO	R&E	202	150	6	0,7
WAYF/Forskningsnettet	NREN	DK	R&E	130	110	5,5	
IGTF	Grid computing	global	Science	86	2500		
SWITCHaai	NREN	CH	R&E	47	581		
UK Access Management Fed.	NREN	UK	R&E	900	236		
SIR	NREN	ES	R&E	102	200		
Portalverbund	G2G	AT	Public	50	165		
NETS	Payment	nordic	Fin			500	7
Certipath	Supply Chain	global	Man	20	100	400	2
BankID	B2C, G2C	SE	Pub			400	3,5
AAI@EduHr	NREN	HR	R&E	222	100	100	0,7
SWITCHaai	NREN	CH	R&E	47	581	15	0,3
Mobile Phone Network	Mobile phones	global	ICT				1600
Google-Yahoo-Facebk	Social logins	global	ICT	3			1500
Rakuten	eCommerce	JP	Trade	1			62
JAL	Travel	JP	Trans	1			15
PIV	G2G	US	Pub				8

Service Type	Authentication (physical acess)
	Authentication (logical acess)
	Attributes
	Digital signature
	Delegated Authorization
	Encryption
Trust Constallation	C20 (SP-centric)
	C23 (central SP=IDP)
	C30 (Intra-organizational IDM)
	C31 (Ruling Party IDM)
	C32 (Identity Federation)
	C33 (Cross-Boder Federation)
	C50 (Enterprise Federation)
	Cxx 4-Corner Model
Business Value	Improve Usability/Flexibility
	Reduce IT OpEx
	Regulatory Compliance
	Risk Reduction: Fraud/Error
	Consolidate Systems/Data
	Business Process Integration
	Part of Critical Infrastructure
Trust Framework	Bilateral Contract
	Multilateral Contract
	Law/Regulation

Left: There are categories with yet insuffient data.

Other questions are:

- Who is audited?
- Who is covered by Liability?
- How man LoA are allowed?
- Which LoA-Policies?
- Which AuthN schemes are used?

Kantara BCTF Survey

How can you profit? (planning, Sales, Evaluation)

How can you help? (share data you have available)

How can you find us? (google: Kantara BCTF)

Rainer Hörbe, CISSP
rainer@hoerbe.at

Constellations and Use Case Overview: http://kantarainitiative.org/confluence/display/fiwg/Trust+Federation+Constellations+and+Use+Case+Overview

Trust Framework Meta Model: http://kantarainitiative.org/confluence/display/fiwg/Trust+Framework+Meta+Model

identityblog.hoerbe.at