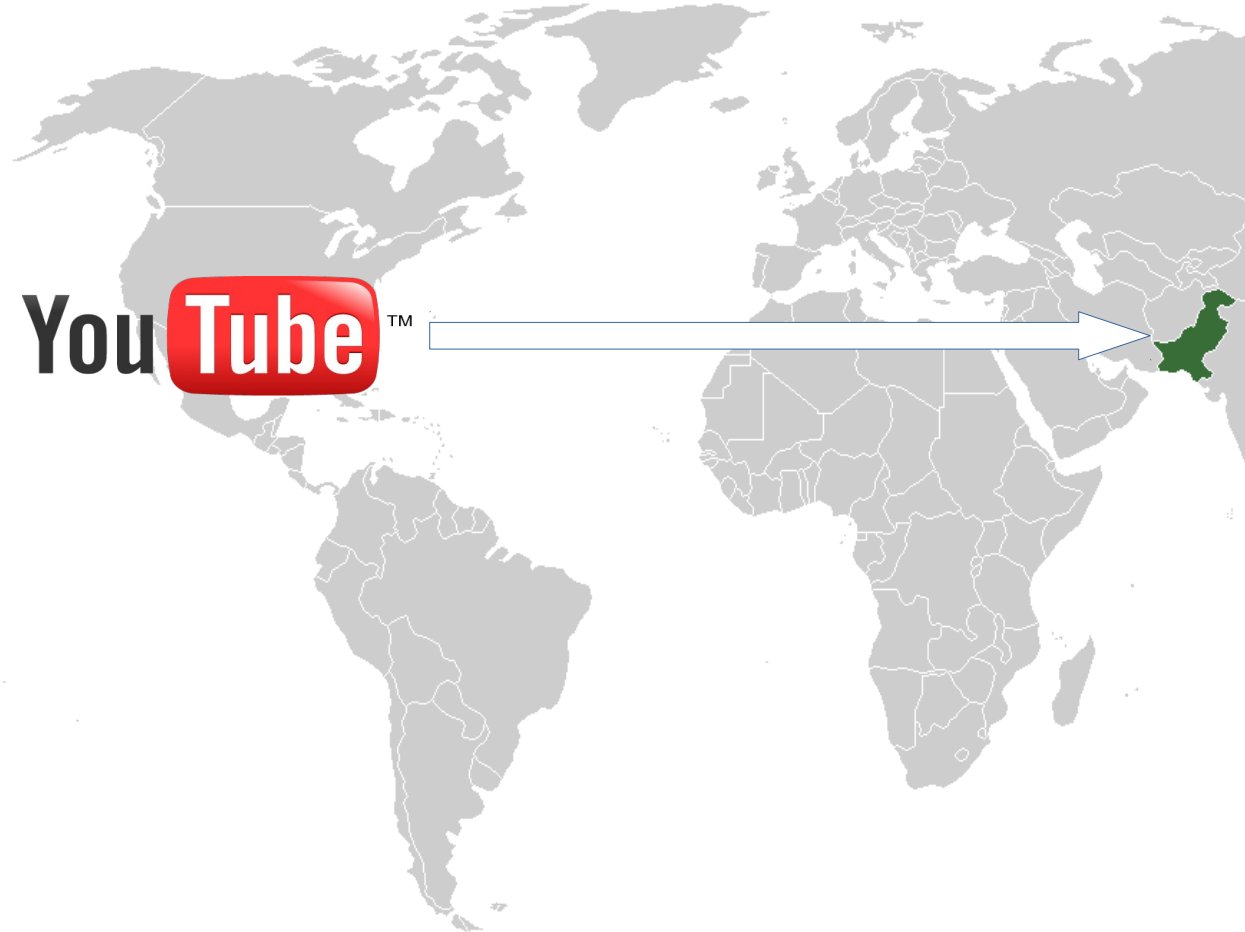
Trust in Protocol Design

Ashwin J. Mathew

Center for Long-Term Cybersecurity, UC Berkeley
Packet Clearing House

The Border Gateway Protocol (BGP)



PTA

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

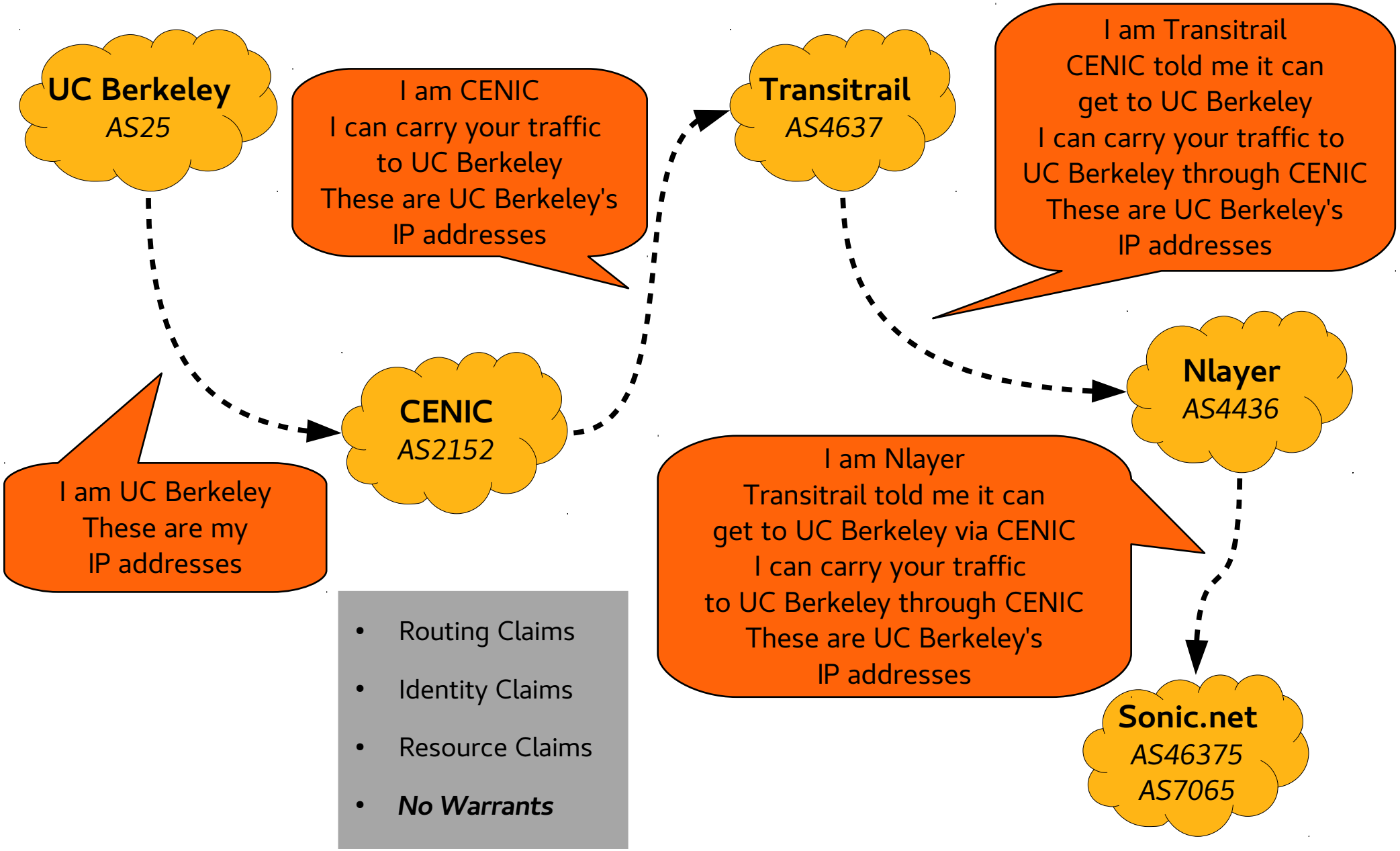
Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Deputy Director
(Enforcement)

To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.

Source: https://advox.globalvoices.org/2008/02/24/pakistan-partial-block-of-youtube/

BGP: Inter-Domain Routing

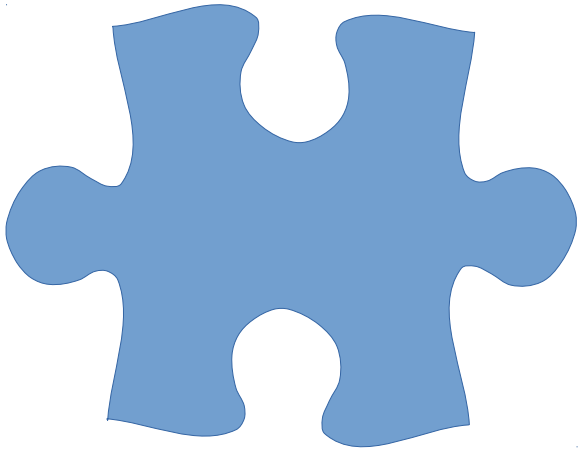


Autonomy

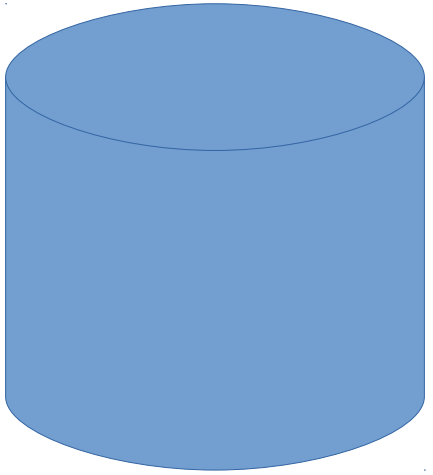
Accountability

Who can exert **control**?

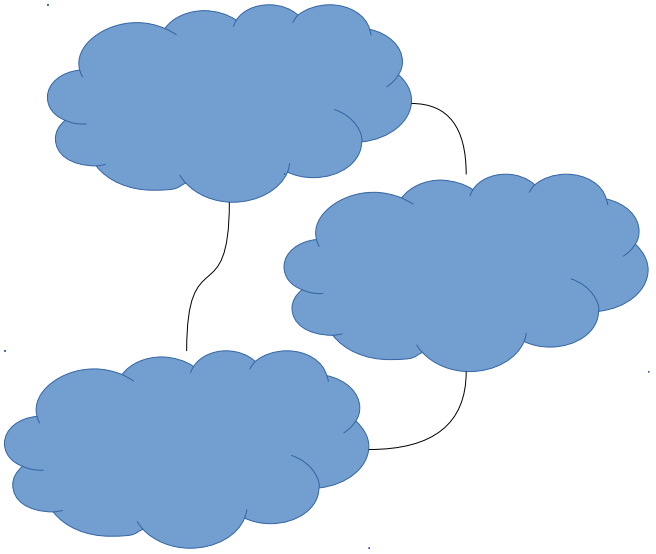
How can we **trust**?



Standards



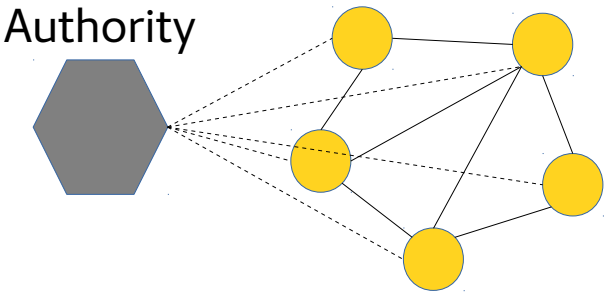
Resources



Topology

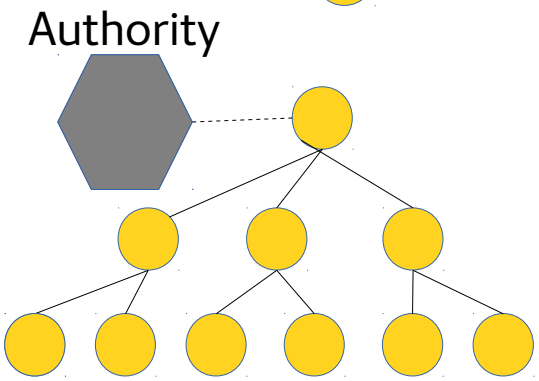
Shifting Authority

GGP



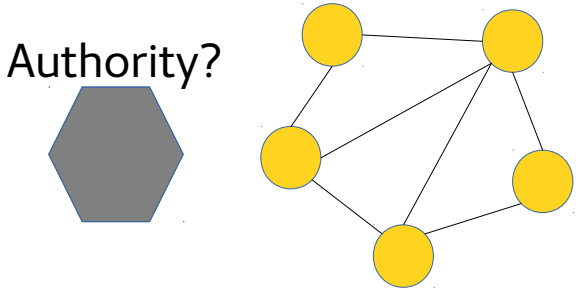
RFC 823:
"For reasons of maintainability and operability, it is easiest to build such a system in a homogeneous fashion where all gateways are under a **single authority and control**, as is the practice in other network implementations."

EGP

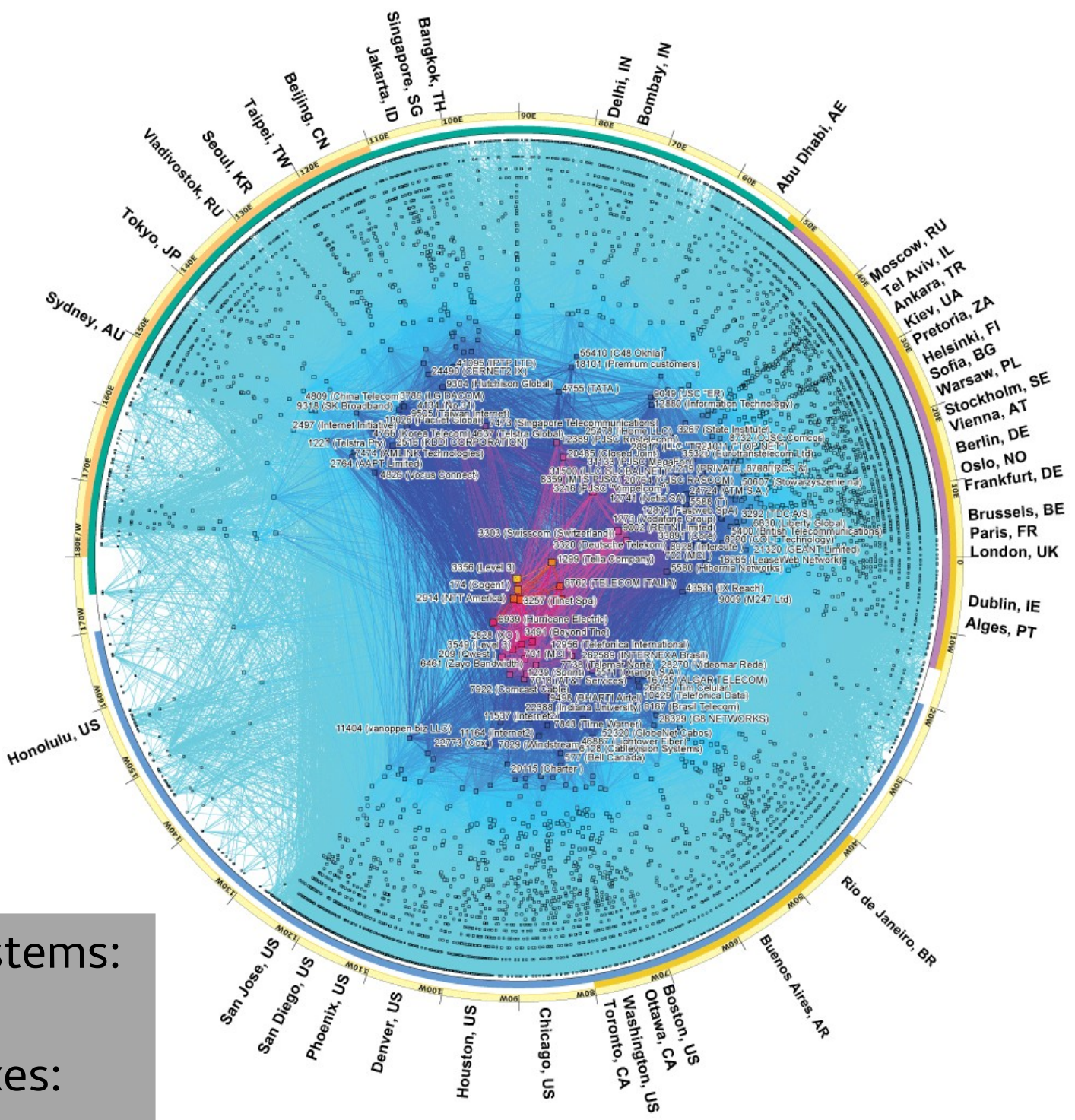


RFC 827:
"...intended for a set of autonomous systems which are **connected in a tree, with no cycles**...
...does not enable the passing of sufficient information to prevent routing loops if cycles in the topology do exist..."

BGP



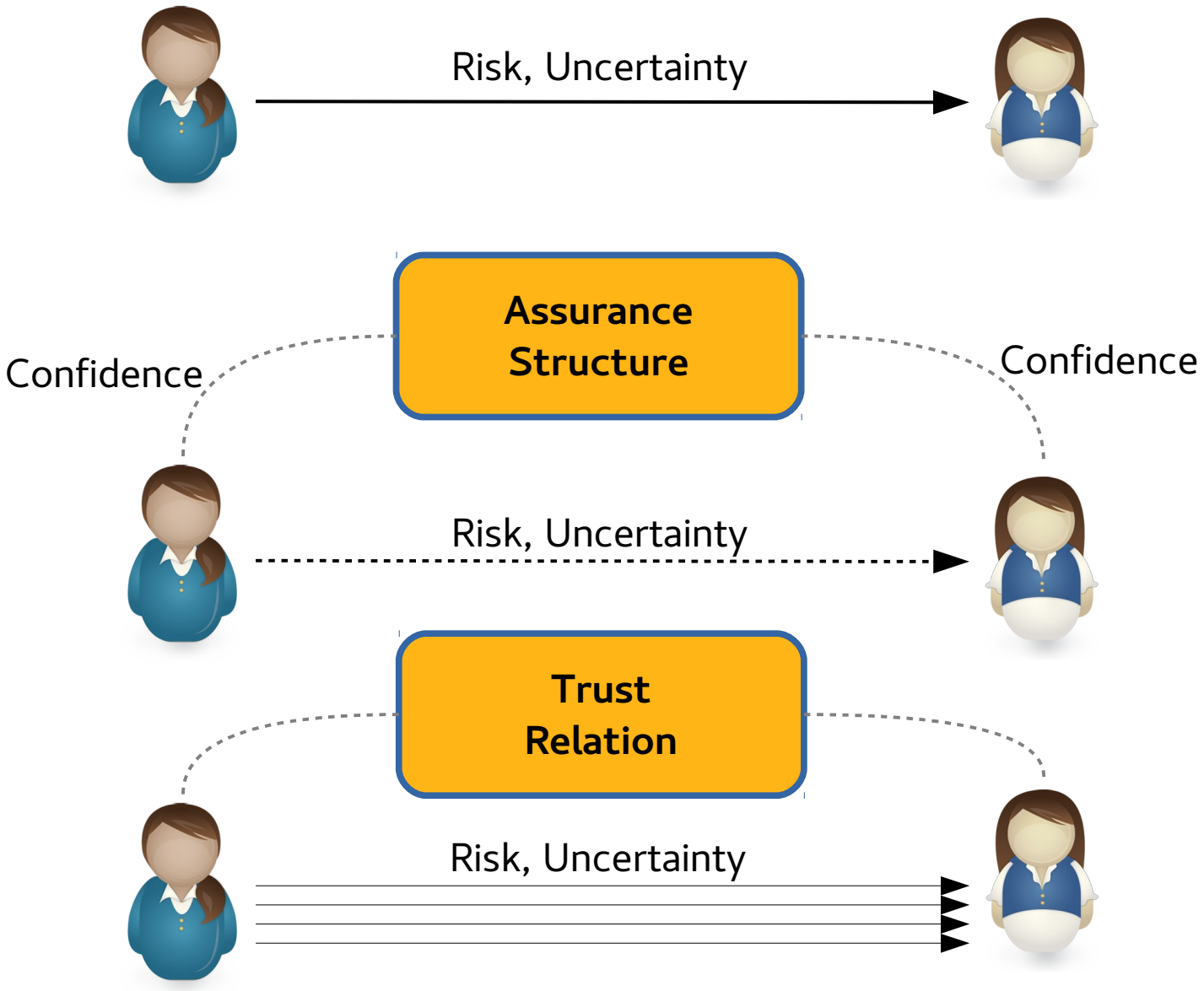
NSF 93-52:
"The solicitation also invites proposals for an RA organization to establish and maintain databases and routing services which **may** be used by attached networks to obtain routing information"



Autonomous systems:
>60,000
IP address prefixes:
>740,000

Sources: http://www.cidr-report.org/as2.0/
http://www.caida.org/research/topology/as_core_network/2017/

Models of Trust

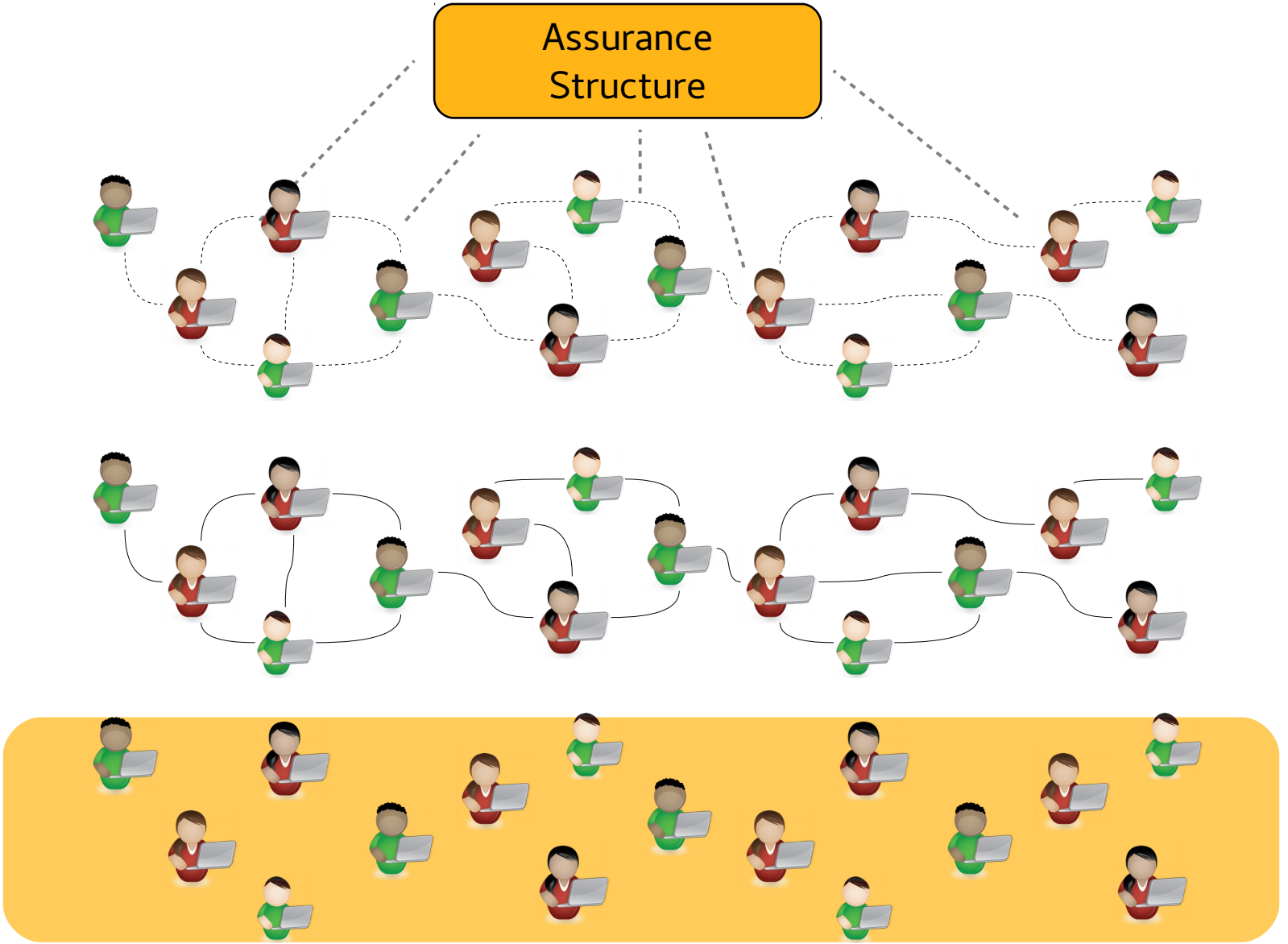


Problem

Solution: Assurance Structure

Solution: Trust Relation

Trust in Society



System Trust

Interpersonal Trust

Generalized Trust

Trust in
Communities of Practice

The Internet

In the idealized world of humans not being social animals … you'd have really, really high quality, low-friction, functioning contacts everywhere you needed to.

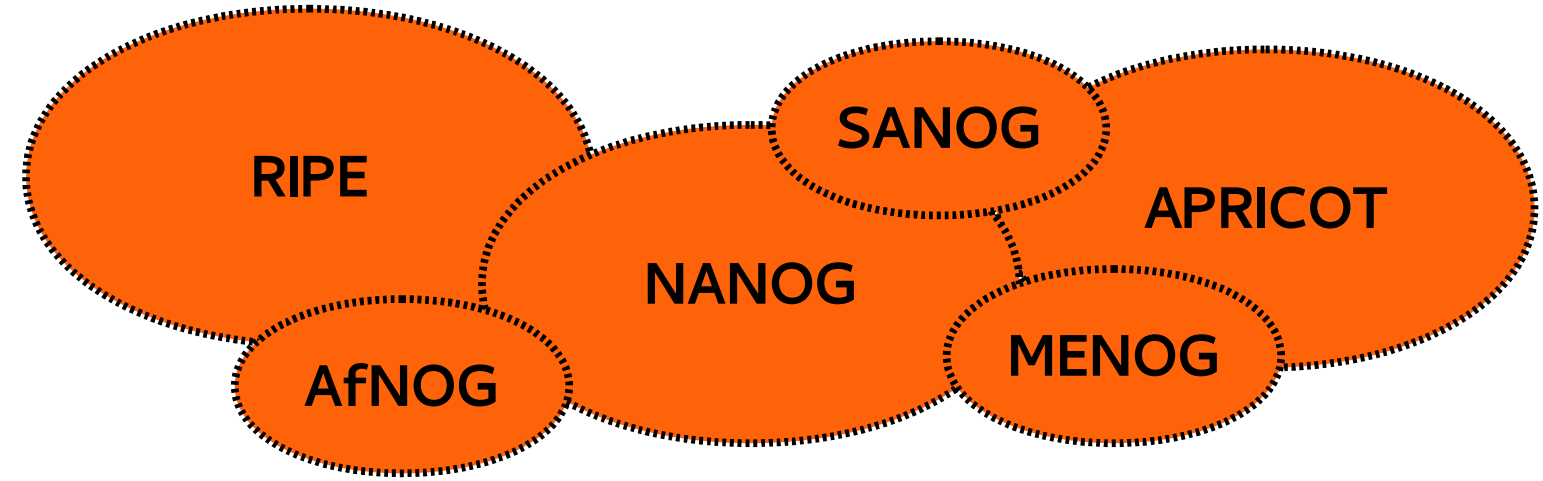
But the reality is that the problem with the Internet is that people with whom you have no direct adjacency or any direct contractual or financial relationship can ruin your network.

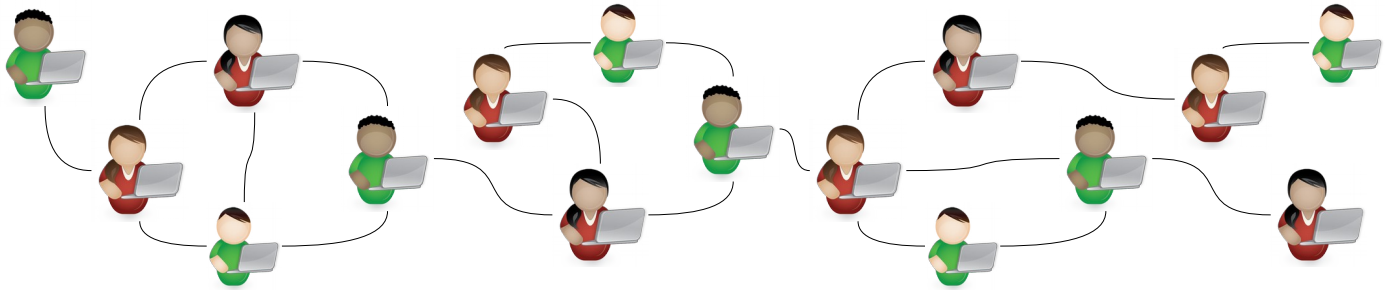
There’s lots of communication through backchannels, lots of unofficial communication. There’s lots of things that nobody can officially talk about, but if we can all share information about it, we can make the Internet a better place.

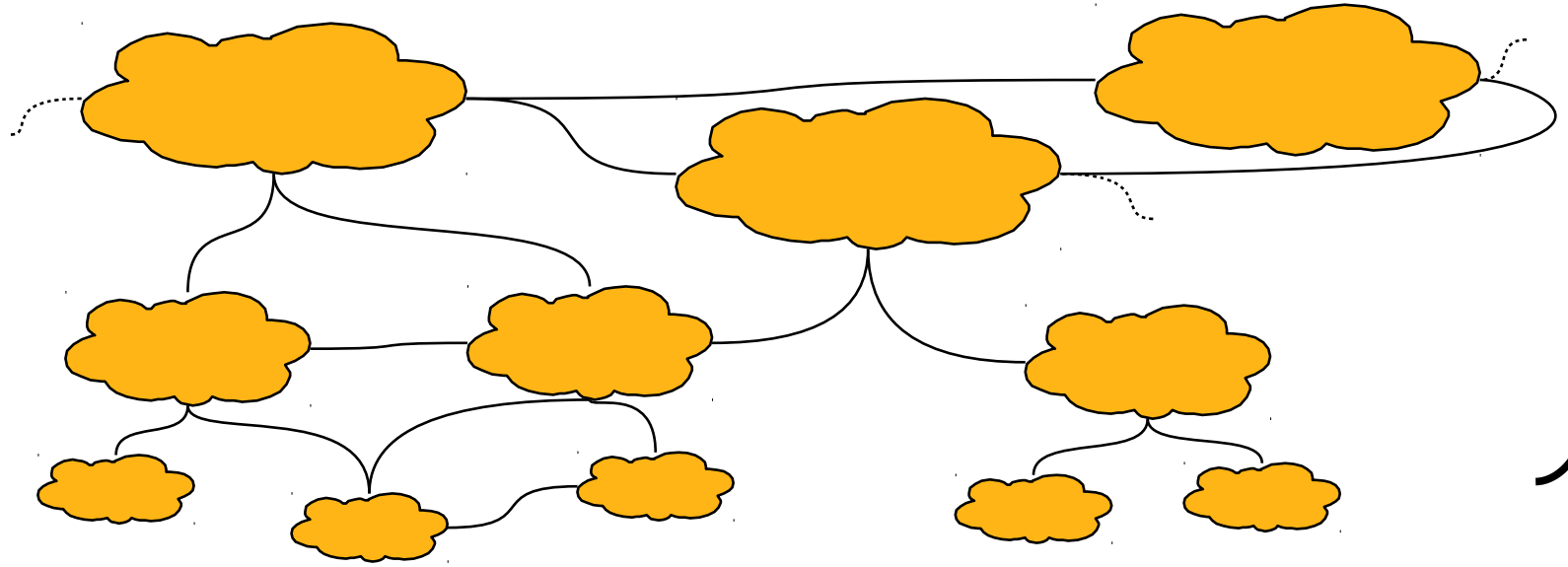
So there’s lots of communities, and the only way that you gain admission into a community is to be a trusted individual.

The North American Network Operators Group (NANOG)


The South Asia Network Operators Group (SANOG)



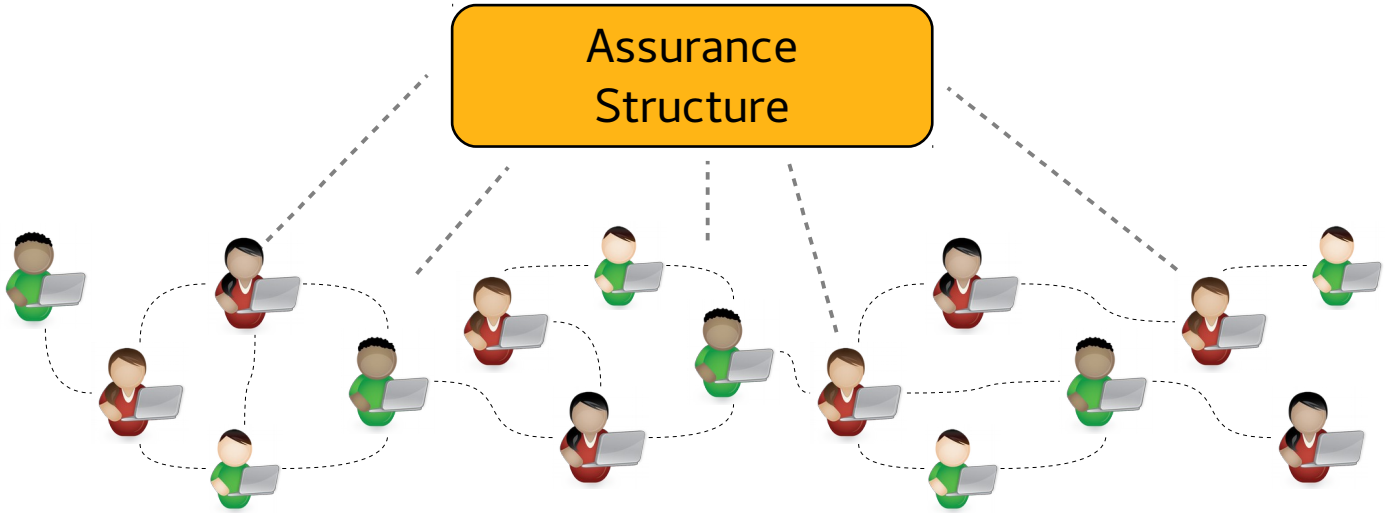




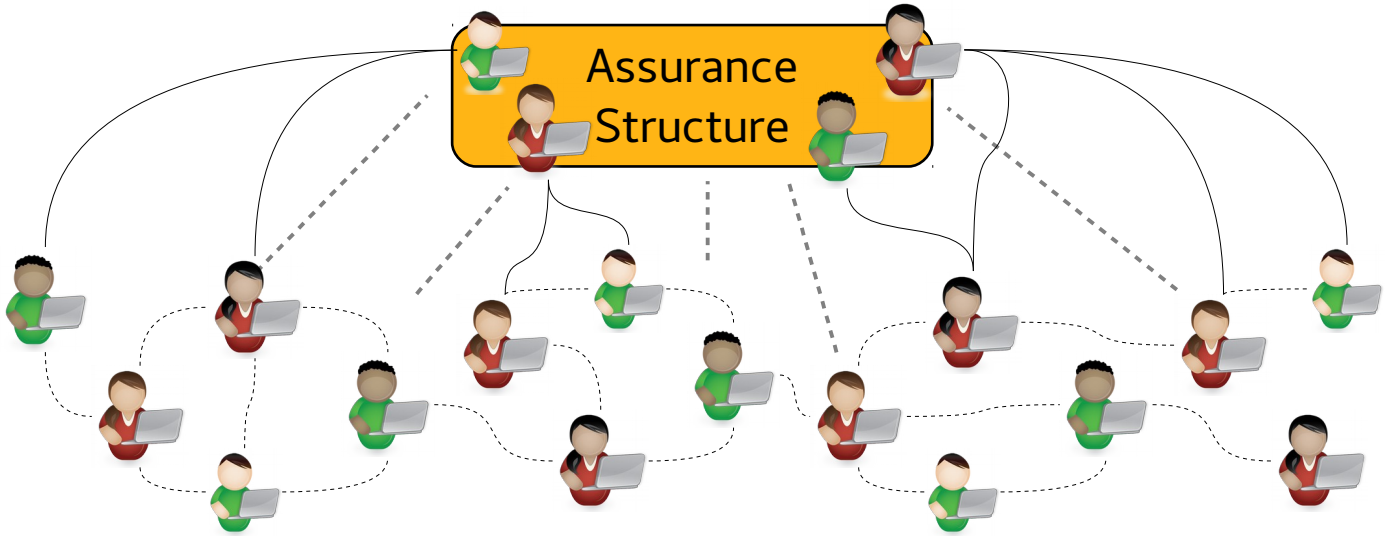
Social Organization

Technical/ Commercial Organization

Trust in Institutions



Autonomy



Embeddedness

Resources

ARIN NUMBER RESOURCE POLICY MANUAL

Version 2015.3 - 29 July 2015

This is ARIN's Number Resource Policy Manual (NRPM). It is available at: https://www.arin.net/policy/. This version supersedes all previous versions.

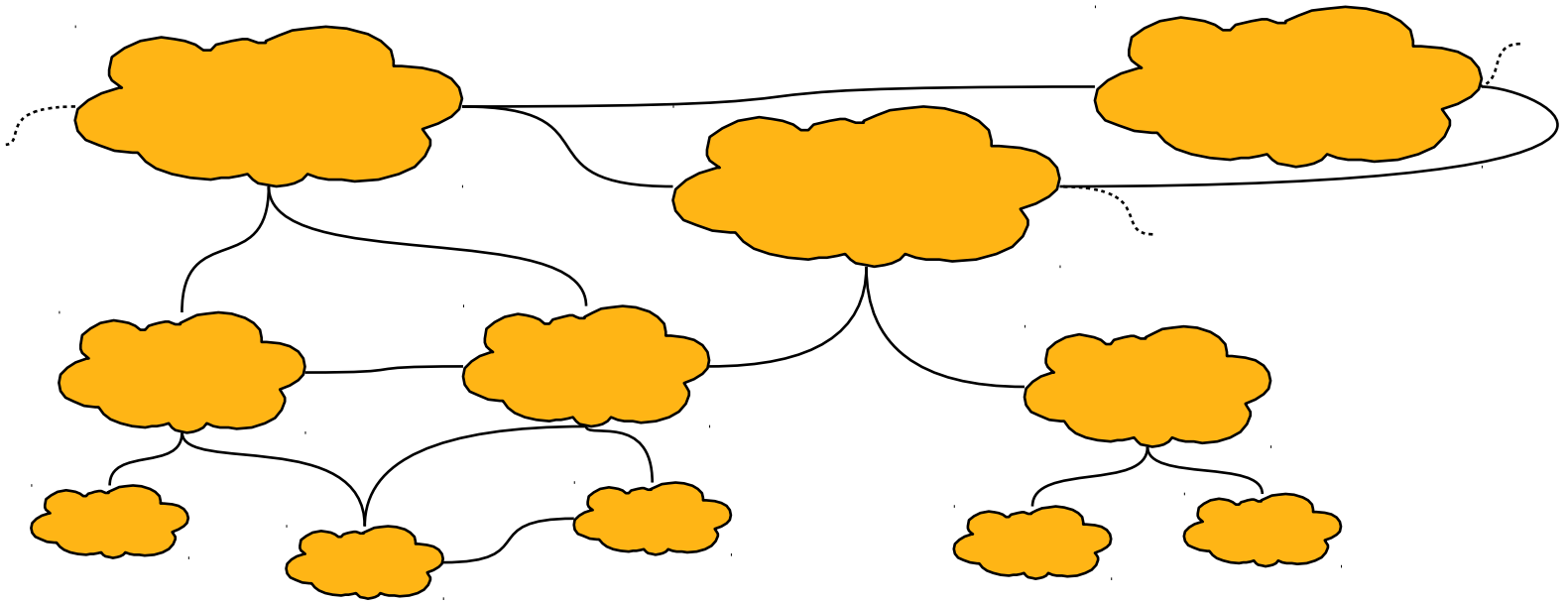
Number resource policies in the ARIN region are created in accordance with the "Policy Development Process" (https://www.arin.net/policy/pdp.html). The status of current and historical policy proposals can be found on the "Draft Policies and Proposals" page (https://www.arin.net/policy/proposals/).

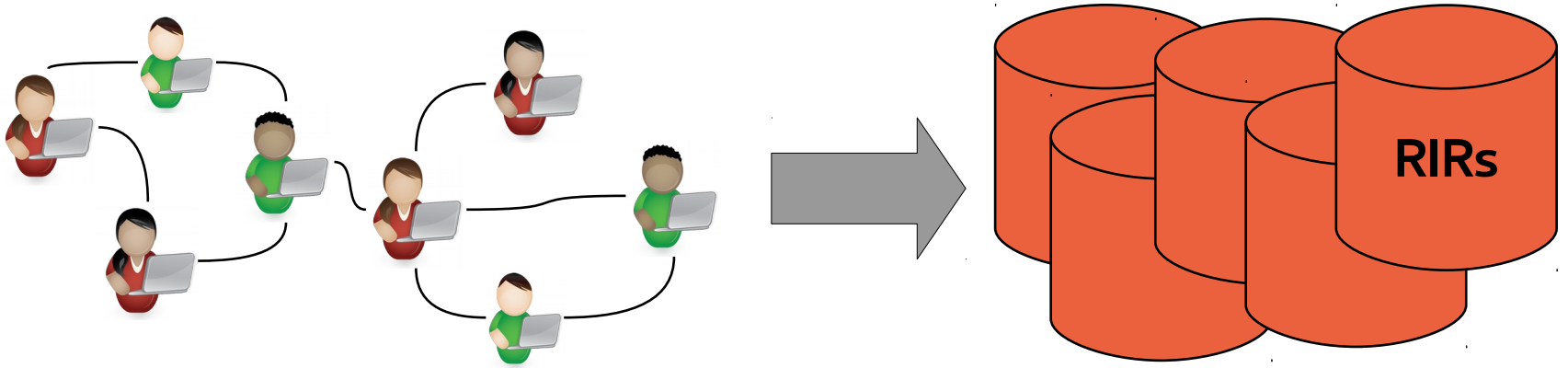
Each policy consists of a number of component parts separated by dots. The first figure to the far left and preceding the first dot (.), refers to the chapter number. The figure following the first dot indicates a policy section. Any subsequent figures are for the purpose of identifying specific parts of a given policy.

Contents

ARIN
American Registry for Internet Numbers

Shifting Authority with RPKI

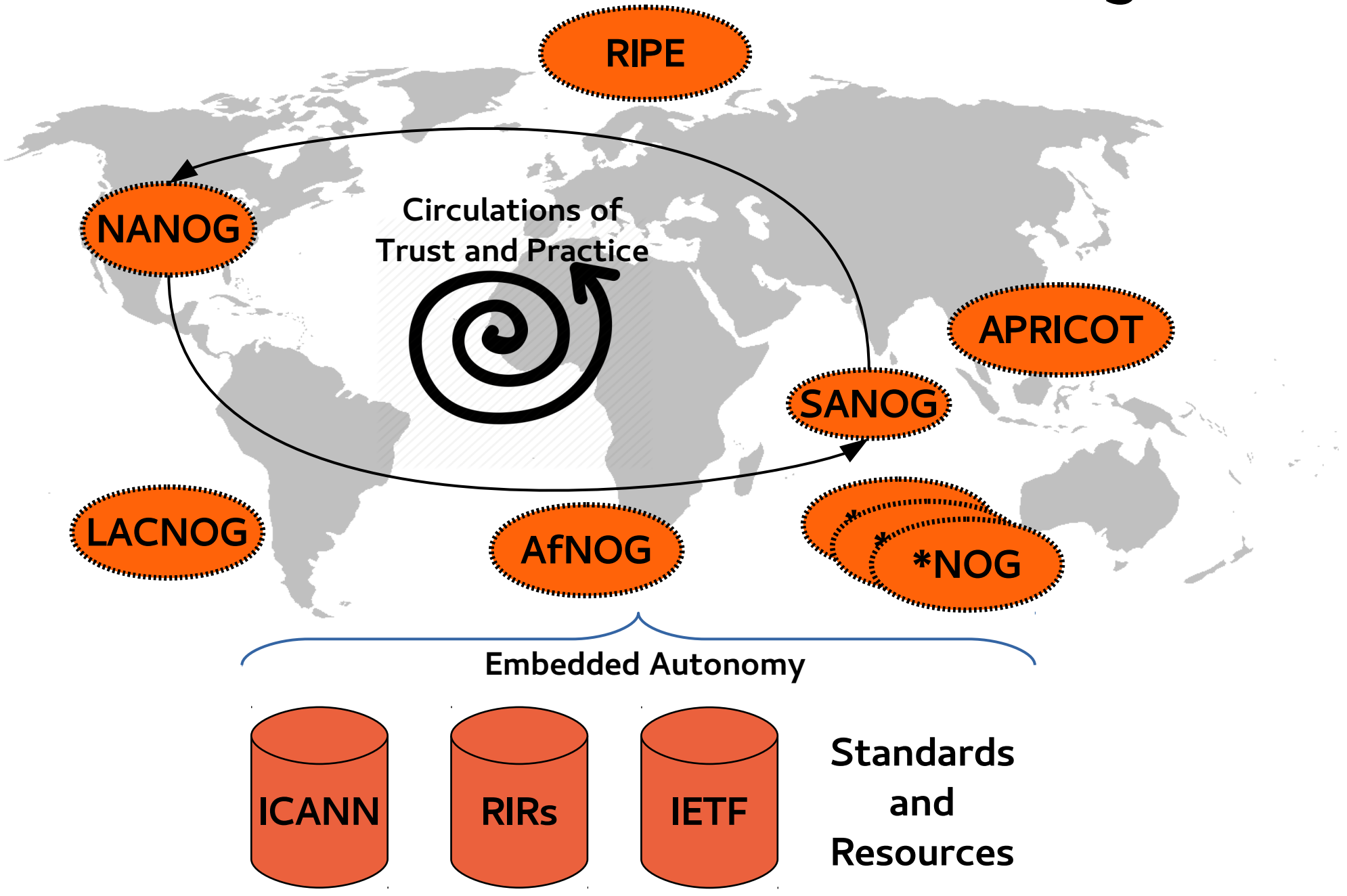




Interpersonal Trust

Institutional Assurance

BGP: Inter-Domain Routing



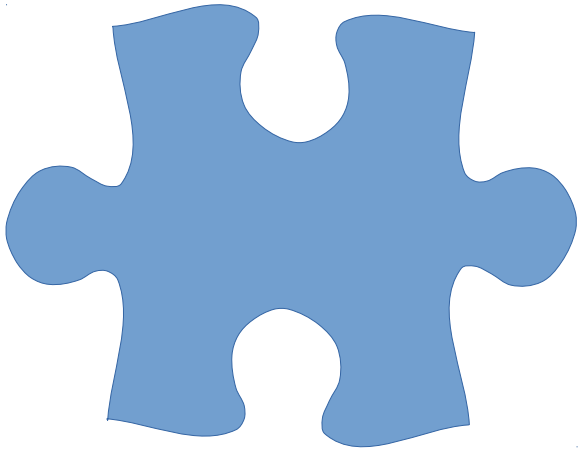
Autonomy

Rights

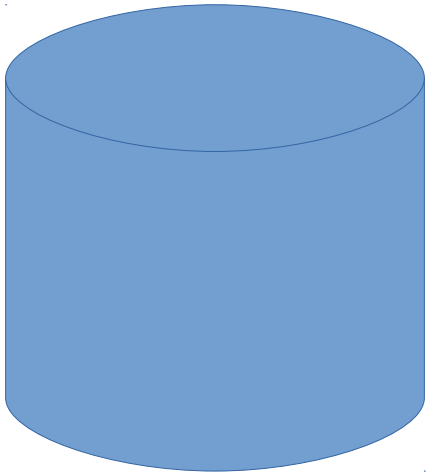
Accountability

Who can exert **control**?

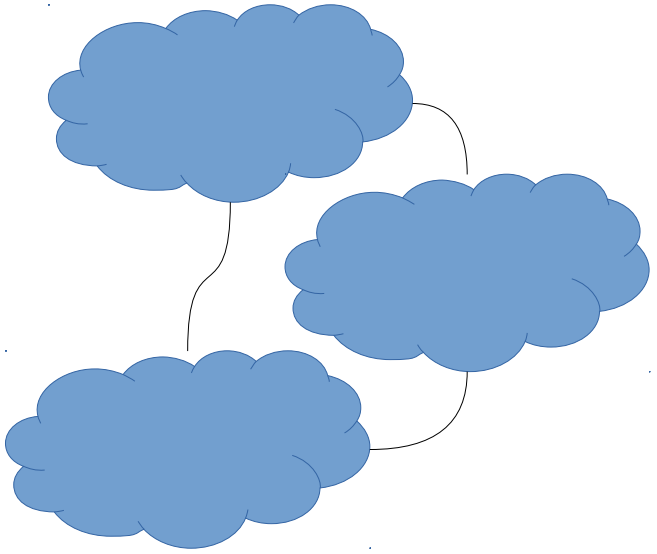
How can we **trust**?



Standards



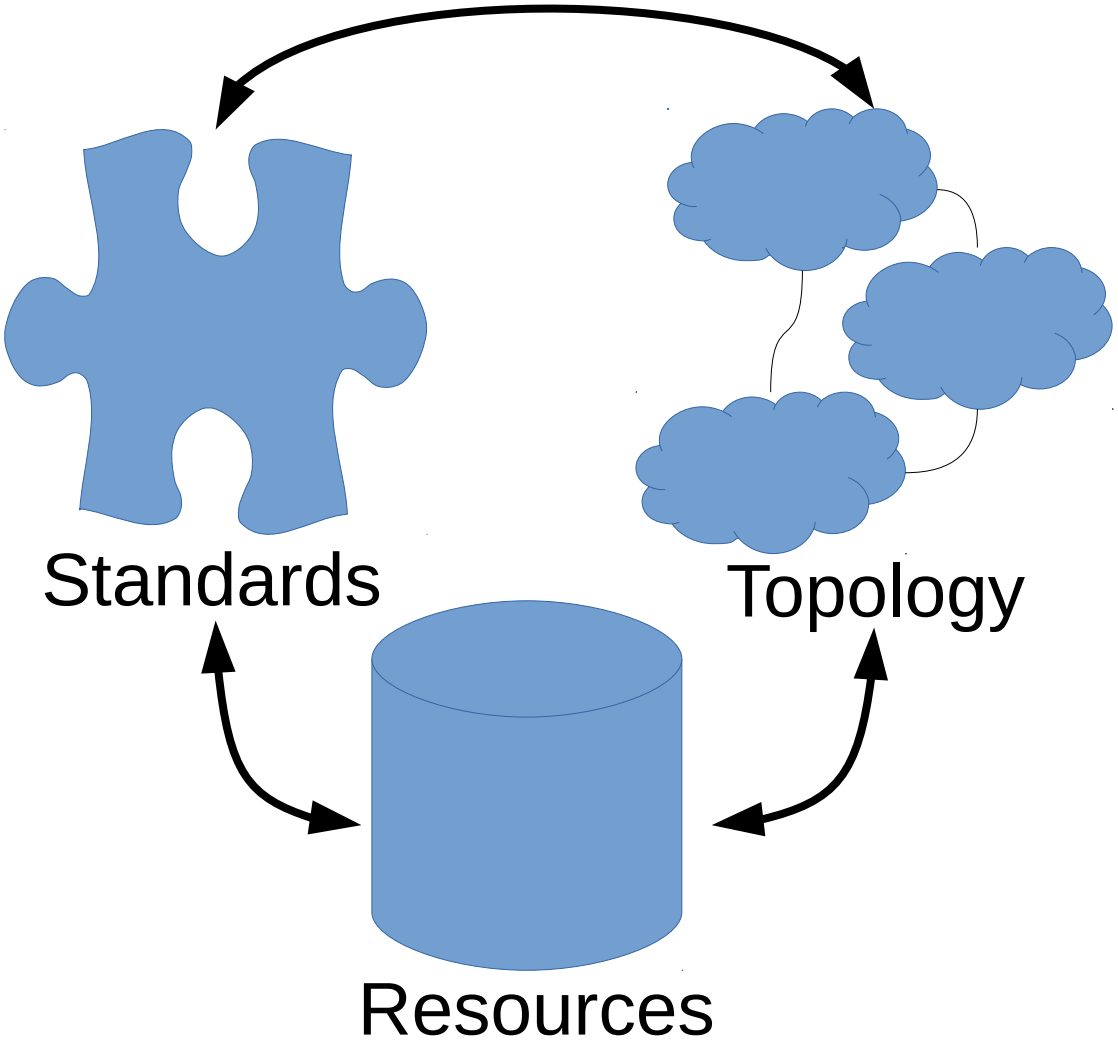
Resources

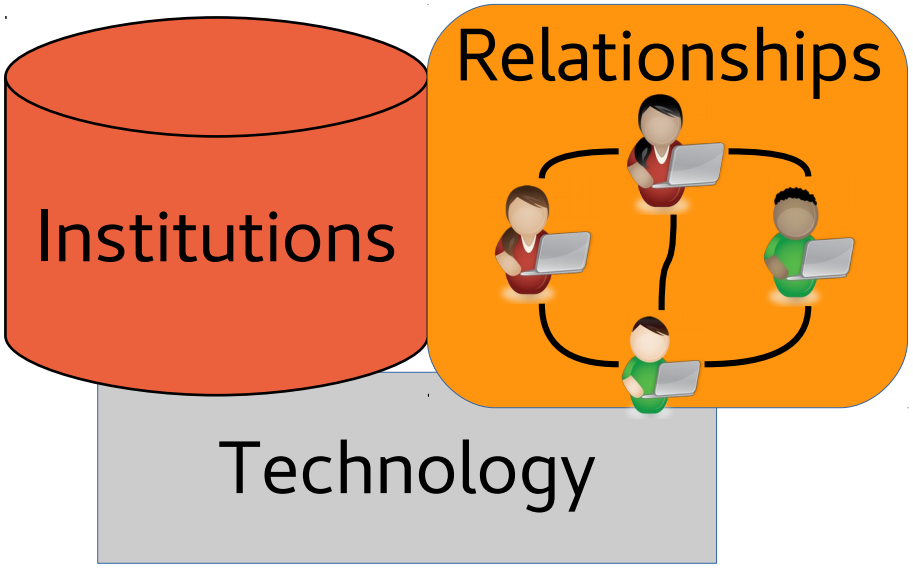


Topology

Who can exert **control**?

How can we **trust**?





Questions?

ashwinjmathew@berkeley.edu
ashwin@pch.net

https://sanmathi.org/ashwin/