KSK Rollover 2015-2019: What We've Learned So Far

Edward Lewis

Grupo de Trabalho de Engenharia e Operação de Redes (GTER) 46
13 December 2018

ICANN

Agenda

- KSK Rollover Project
- Lessons learned along the way - *so far*
- Something surprising about Brazil

KSK Rollover Project

- Goal: Replace the key (KSK) used to sign the DNS root zone's DNSSEC key set since 2010 without disruption

- Passed many milestones, still more to go
  - Next up: Formal revocation of the old key, first sign of that on 11 January 2019

2015 - 2019

2015	2016	2017	2018	2019
Design Team	Plans Made; Key Created	Publicize; The "Pause"	Publicize; Change Key	Revoke; Clean Up

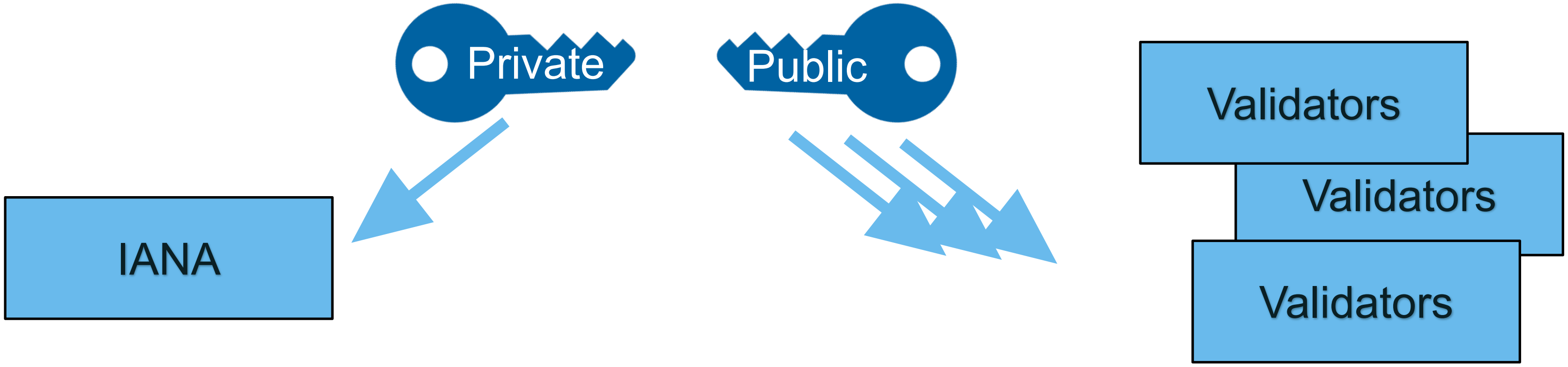
- A key rollover can be done more quickly, but "going fast" has never been the goal

Operator Actions

- Have you done nothing so far and have seen no problems?
  - Continue what you are doing!
- Have you been relying on Automated Updates (RFC 5011)?
  - Continue what you are doing!
- Are you manually managing the configuration of DNSSEC trust anchors?
  - Remove the old key (2010) from trust anchors after 11 January 2019.

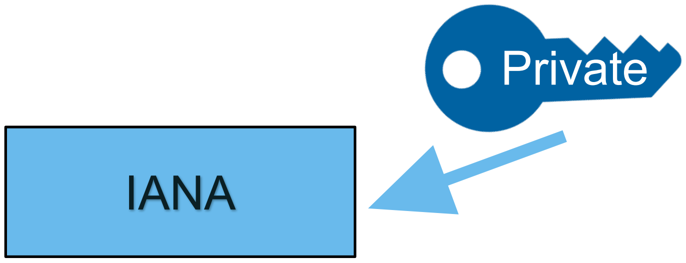
Project Considerations

- The KSK is a private-public key pair
- IANA uses the **private key** to sign the "top" of the DNSSEC hierarchy
- Validator operators configure their DNSSEC validating servers with the **public key**

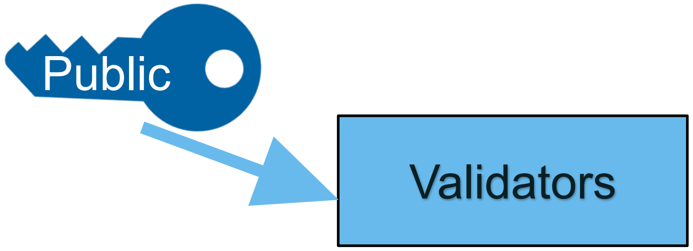


The Project's "Problem to Solve"

- Rolling the Private Key
  - Simple



- Rolling the Public Key
  - Simple



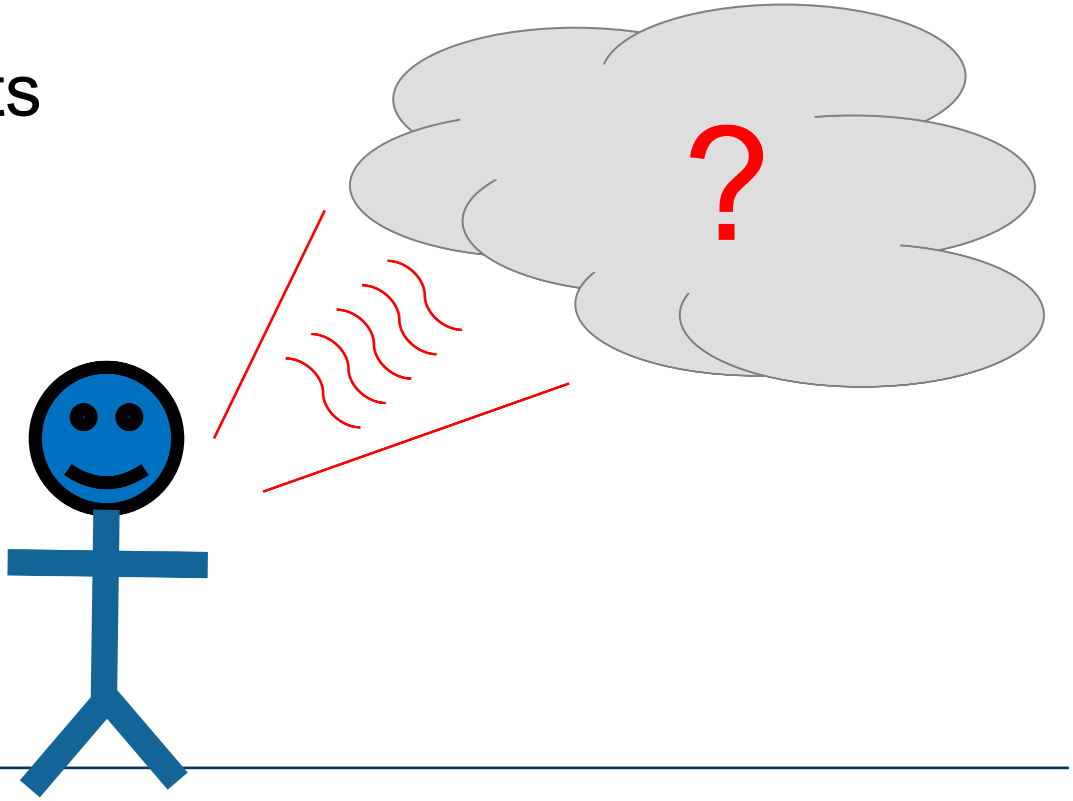
- Coordinating the actions
  - Difficult
  - An exercise in communications

The Permission-less Internet

- *Permission-less* means operators make their own choices and are responsible for their actions
- This has enabled DNS to scale very well
- But
  - No list of operators configuring the key
  - Not easy to "snoop", no pervasive monitoring

Communications to/with an Unknown Audience

- Permission-less: No list of audience members
- Timing of messages
- Different skill sets
- Different focus
- Different forums



Shift in Project Focus

- In 2015, discussions were theoretical, academic
  - Nature of "trust", what is the true "top key"
  - Preferred ways to get new key
  - Design measurements, testbeds
- By 2018, practical considerations
  - Include the new key in DNS software
  - Use email and surveys to reach operators
  - "Get it done"

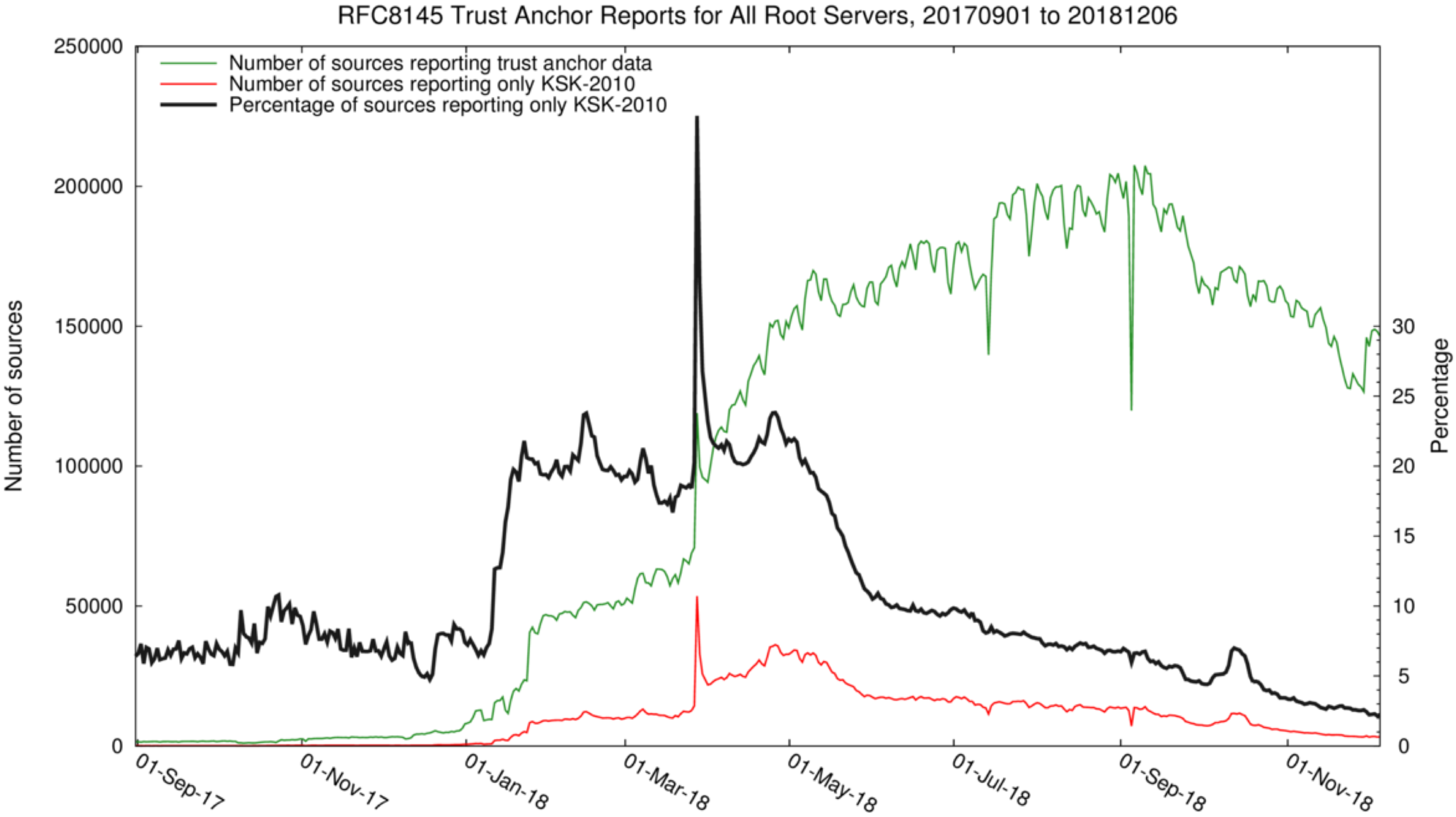
Technical Solution

- Automated Updates of DNSSEC Trust Anchors
  - Also known as "RFC 5011"
- Some don't like idea of self-configuring edge devices, others rely on the convenience
- A functional but difficult to manage protocol
  - Proven (albeit in few cases)
  - Lacks measurement hooks
  - Lacks testing hooks
  - Requires attentive operators

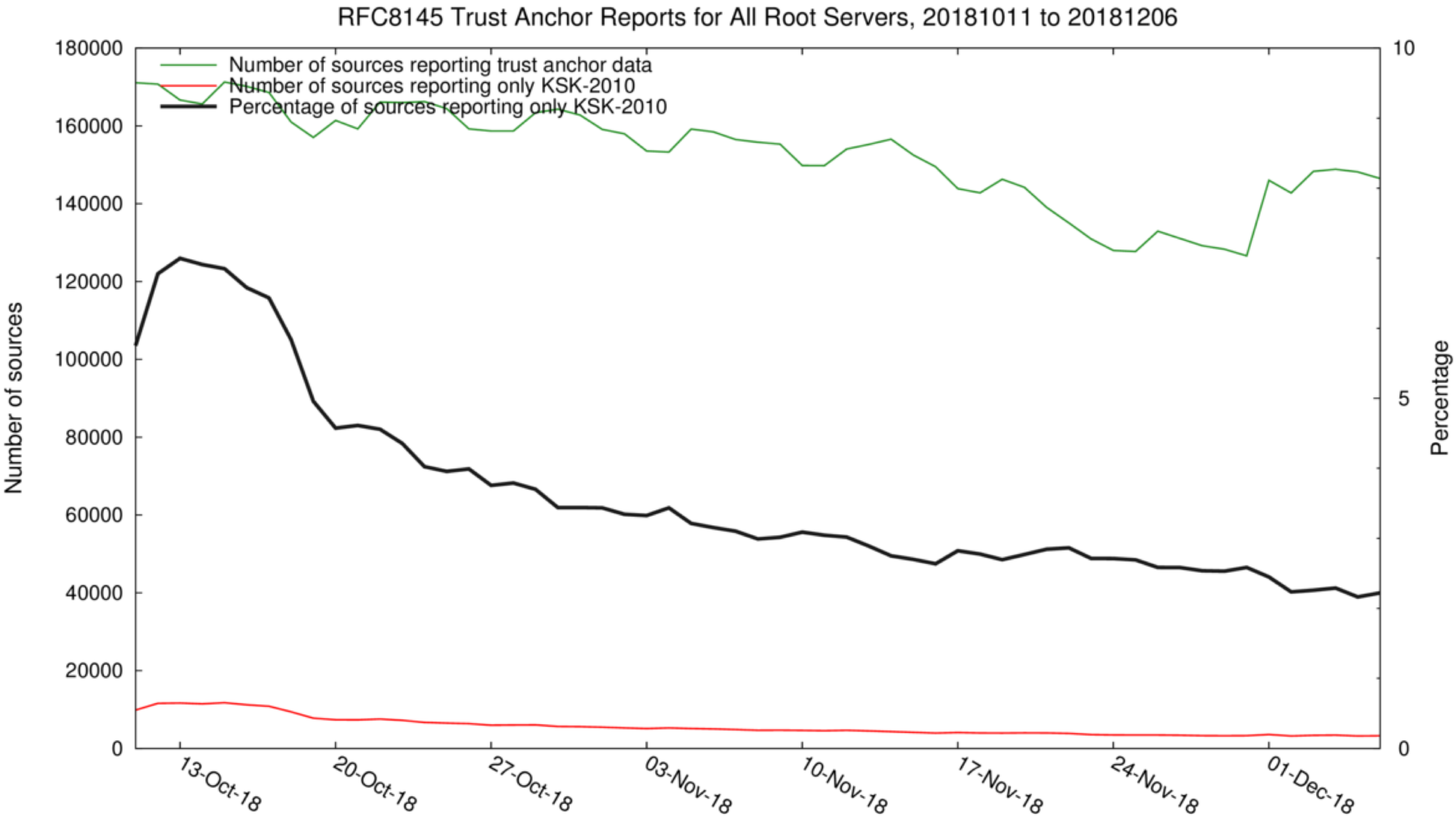
Adventures in Measurement

- Many tried to design a way to "third-party" test readiness
  - Not possible
- IETF rushed to define "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)" (RFC 8145)
  - "Key Tag" : Heartache!
- IETF is about to propose "A Root Key Trust Anchor Sentinel for DNSSEC" (draft)
  - Still in draft stage

Key Tag Reports, 01 Sept 2017- 06 Dec 2018



Key Tag Reports, 11 Oct 2018- 06 Dec 2018



Is Measurement/Monitoring Possible?

- Why aren't there effective tests or measures?
  - Knowledgeable people tried
  - The DNS is not built to make this easy
- What then?
  - Look for alternatives
  - Different expectations
  - Innovate/change coordination model

Monitoring a KSK Rollover

- How does one visualize a KSK rollover?

- Can't see into resolver configurations
- Can see what DNSKEY set a resolver holds
  - But only of the resolver permits

- Representative visualizations aren't feasible

Questions about General Readiness of the DNS

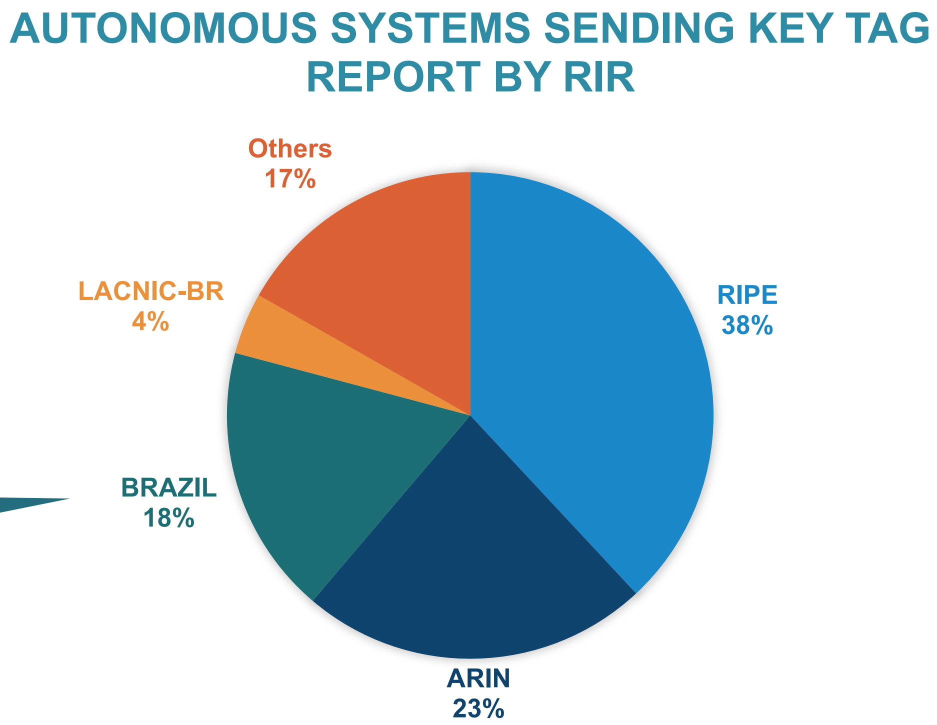
- Beyond the KSK, beyond DNSSEC
  - The DNS still needs out of band coordination

- Many variations, code and configurations, to consider
  - Noted in a paper from "way-back" in 1988!

- Fear of "abuse" has built walls against needed cooperation

Brazil

- Autonomous Systems sending a key tag report
  - Over 16,000 globally



Brazil
18% !

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: ksk-rollover@icann.org

@icann	linkedin/company/icann
facebook.com/icannorg	slideshare/icannpresentations
youtube.com/icannnews	soundcloud/icann
flickr.com/icann	instagram.com/icannorg