

# Trust Anchor Distribution

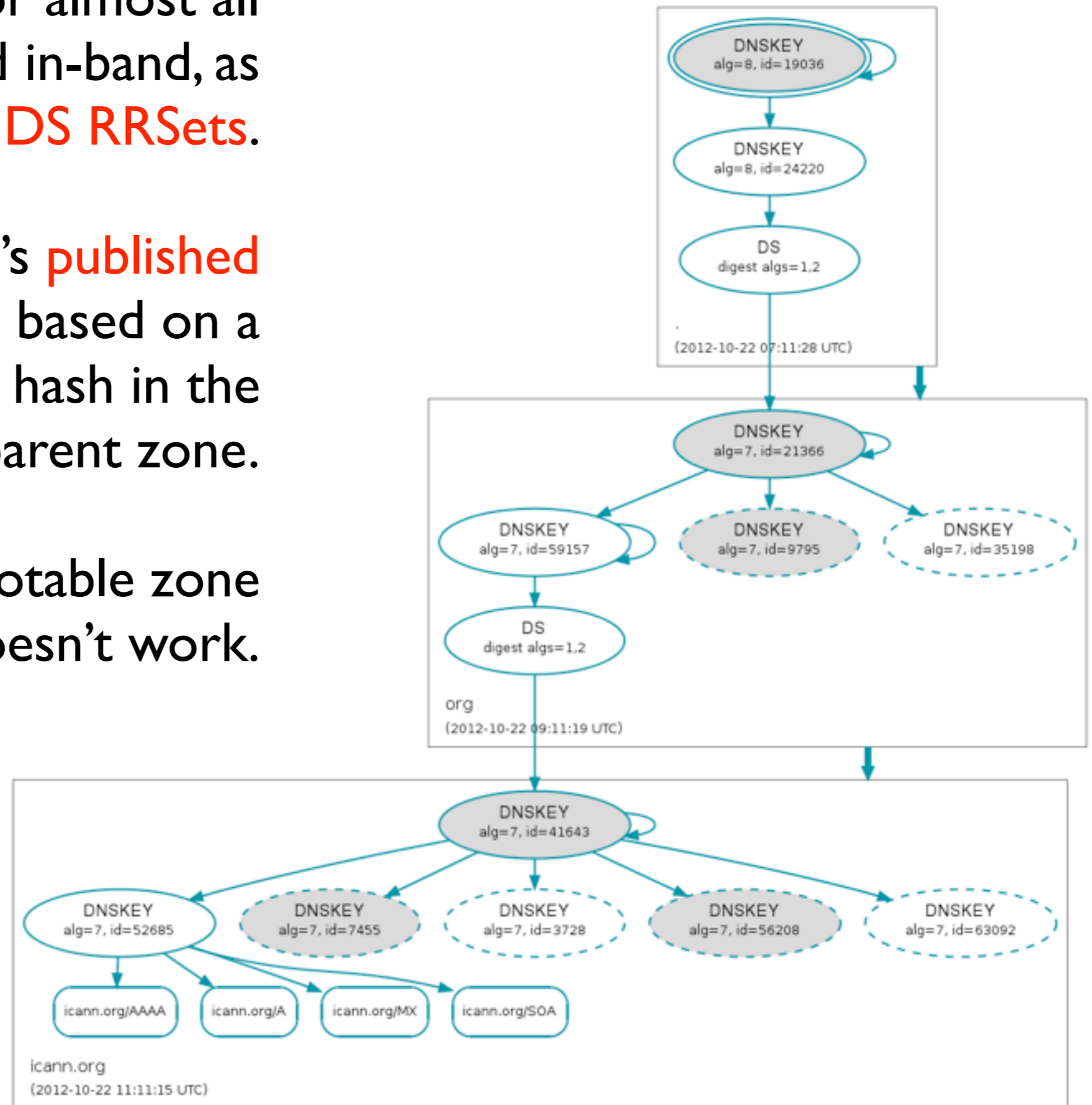
Joe Abley, ICANN  
22 October 2012



Trust anchors for almost all zones are published in-band, as **DS RRsets**.

Trust in a child zone's **published KSK** is based on a corresponding signed hash in the parent zone.

There is **one** notable zone where this doesn't work.



(graphic courtesy of [dnsviz.net](http://dnsviz.net))

# Validators

- DNS authority-only servers don't care about trust anchors; this is a validator thing.
- A trust anchor provides bootstrapping to a validator, akin to a hints file for a resolver



Internet Systems  
Consortium



# Root Zone Trust Anchor

- Publication of the root zone trust anchor is an IANA Function
- Direction provided in the Root Zone KSK Maintainer DPS
- <http://data.iana.org/root-anchors/>



# Root Zone KSK

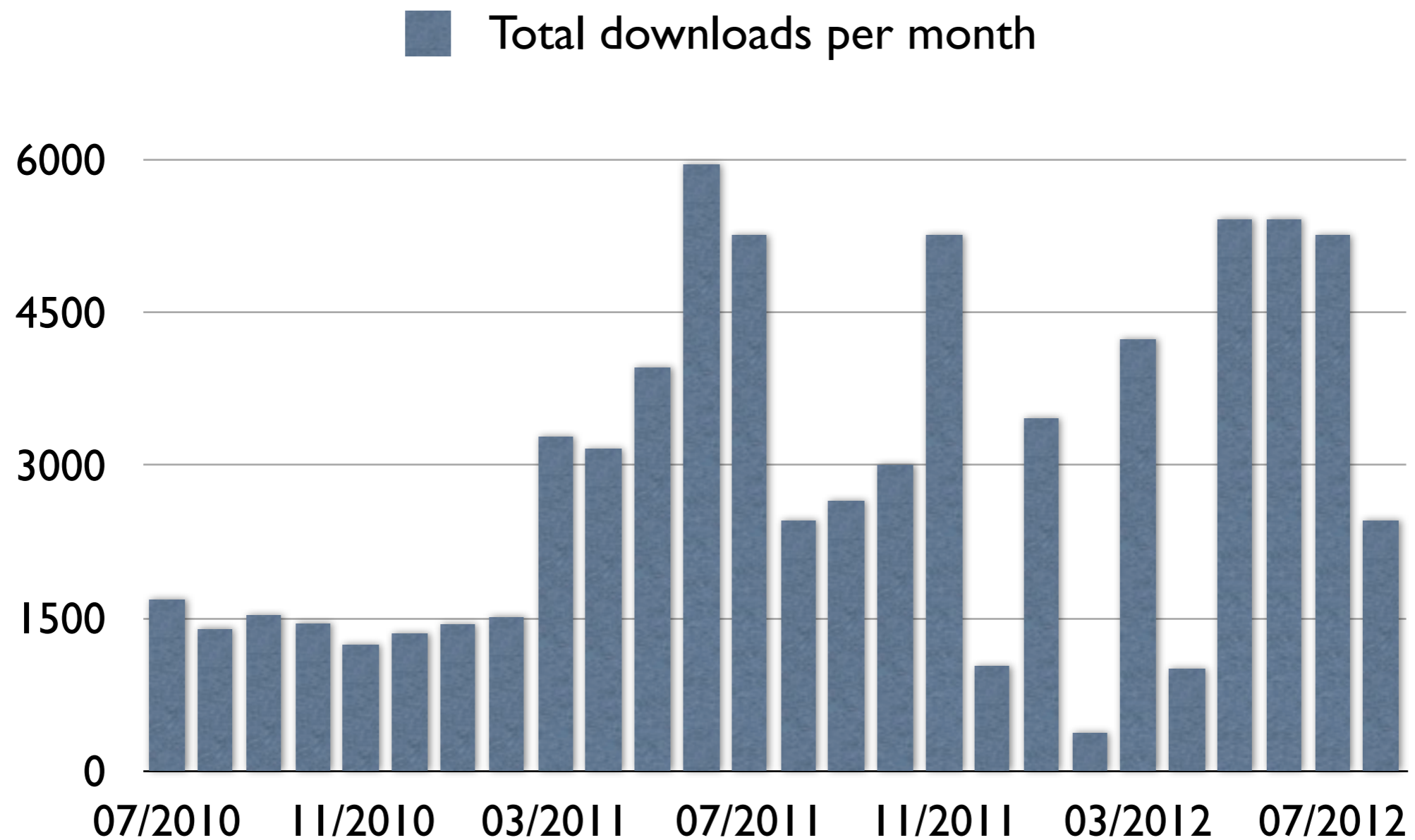
- The current Root Zone KSK was generated at KSK Ceremony 1 in Culpeper, VA in June 2010
- Went into production following KSK Ceremony 2 in Los Angeles, CA in July 2010
- The KSK has never been rolled (yet)



# Validator Bootstrap

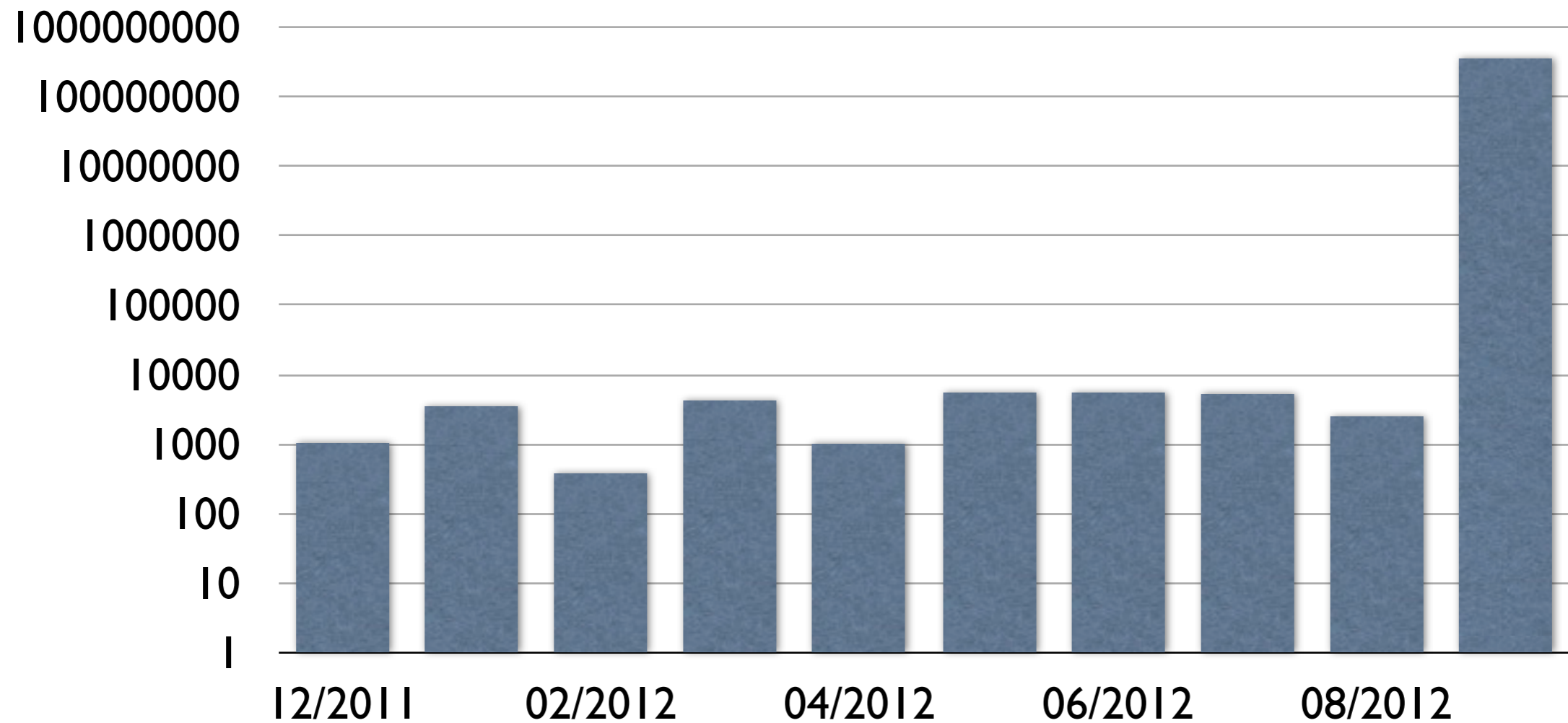
- Validators need a trusted copy of the root zone trust anchor when they start up
- System Administrators can use packaged tools like unbound-anchor, or just use eyeballs and brain
- (if you get it wrong, you know pretty quickly, and you can fix it)

# Trust Anchor Retrieval



# Trust Anchor Retrieval

■ Total downloads per month





**Yes, that's right.  
353 million.**

# Um.

- Something is going on!
- Does not appear to be an attack, although we were briefly entertaining that idea.
- All the extra retrievals have a consistent user agent string, “CFNetwork/609 Darwin/13.0.0”
- The heavy traffic started on September 19.
- Oh yeah.



# CFNetwork/609 Darwin/13.0.0

- Looks like the extra traffic all corresponds to iOS 6 devices.
- Our traffic was effectively tracking iOS activations and upgrades.
- Looks like everybody looking into this was inadvertently part of the cause.



# Brave New World

## before

- Validators with system administrators
- Sysadmins who are capable of determining whether they trust a particular trust anchor
- Ability to respond appropriately if anything ever breaks

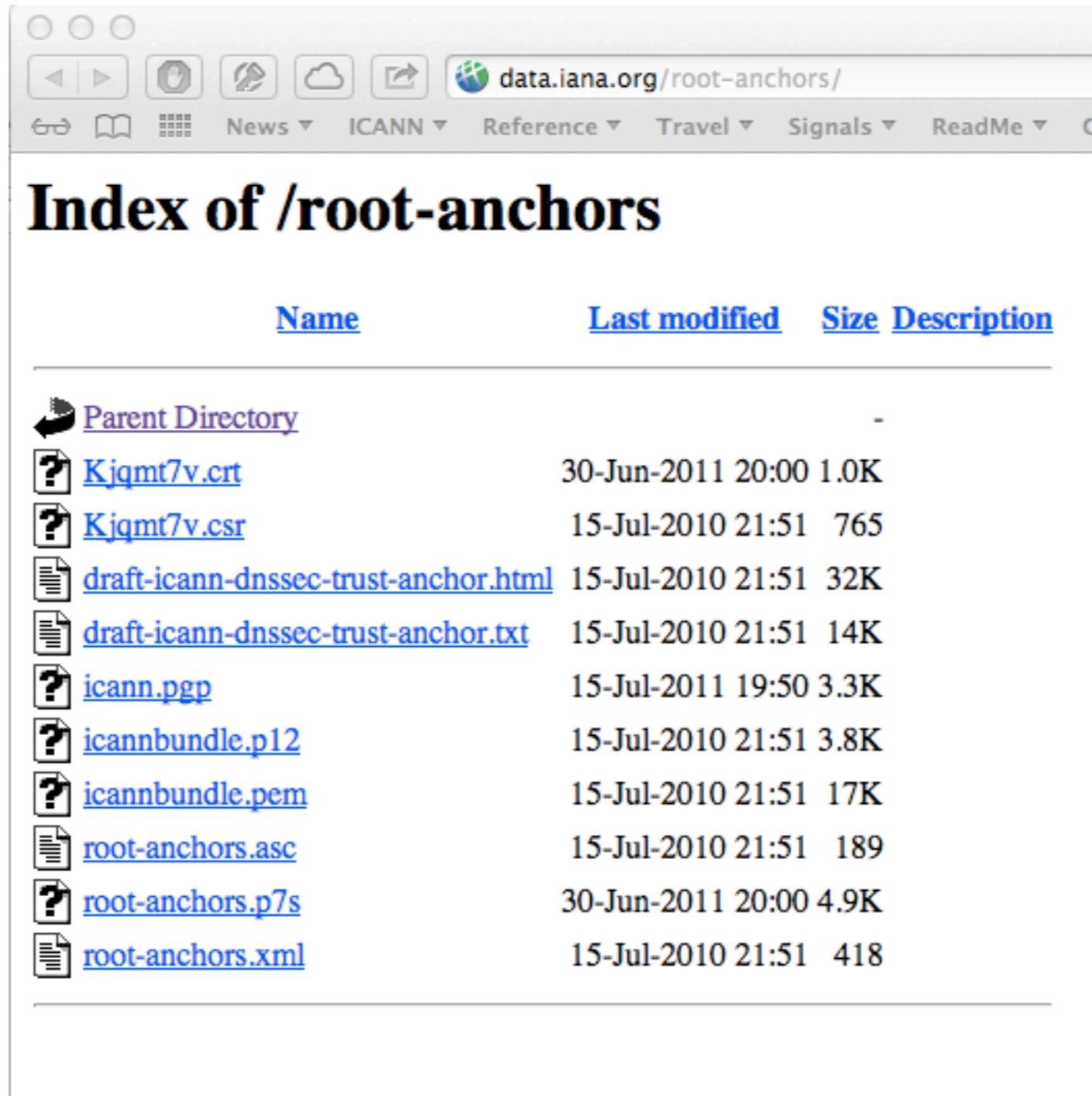
## after

- 12-year-olds
- Grandmothers
- Pointy-haired bosses
- Sales reps
- Lawyers











# Fortunately, we thought of this

- One of the products of KSK Ceremony was a PKCS#10 CSR with a non-standard (but documented) extension list containing an encoding of the current trust anchor
- People would make arrangements to sign that, and we/they would publish it
- Provides a strong chain of trust from KSK Ceremony 1 to the end user

# <http://data.iana.org/root-anchors/>



Index of /root-anchors

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">Kjqmt7v.crt</a>	30-Jun-2011 20:00	1.0K	
 <a href="#">Kjqmt7v.csr</a>	15-Jul-2010 21:51	765	
 <a href="#">draft-icann-dnssec-trust-anchor.html</a>	15-Jul-2010 21:51	32K	
 <a href="#">draft-icann-dnssec-trust-anchor.txt</a>	15-Jul-2010 21:51	14K	
 <a href="#">icann.pgp</a>	15-Jul-2011 19:50	3.3K	
 <a href="#">icannbundle.p12</a>	15-Jul-2010 21:51	3.8K	
 <a href="#">icannbundle.pem</a>	15-Jul-2010 21:51	17K	
 <a href="#">root-anchors.asc</a>	15-Jul-2010 21:51	189	
 <a href="#">root-anchors.p7s</a>	30-Jun-2011 20:00	4.9K	
 <a href="#">root-anchors.xml</a>	15-Jul-2010 21:51	418	

# How This Should Work

- Retrieve root-anchors.xml
- Obtain links to multiple candidate certificates (trust anchor + CA signature)
- Find one that works, and use it
- Accommodate roll-over
  - passive observation of ./IN/DNSKEY
  - RFC 5011
  - re-bootstrap

# Next Steps

- Continue trying to tell people that this is important
- Listen to early-adopters
  - do what we can to accommodate their constraints
- Keep serving those trust anchors



# Further Reading

- draft-jabley-validator-bootstrap
- draft-jabley-dnssec-trust-anchor
- both of these have triggered very little interest, but the world has now changed
- we live in hope

# Questions?

[joe.abley@icann.org](mailto:joe.abley@icann.org)

