ICANN Update and KSK Rollover
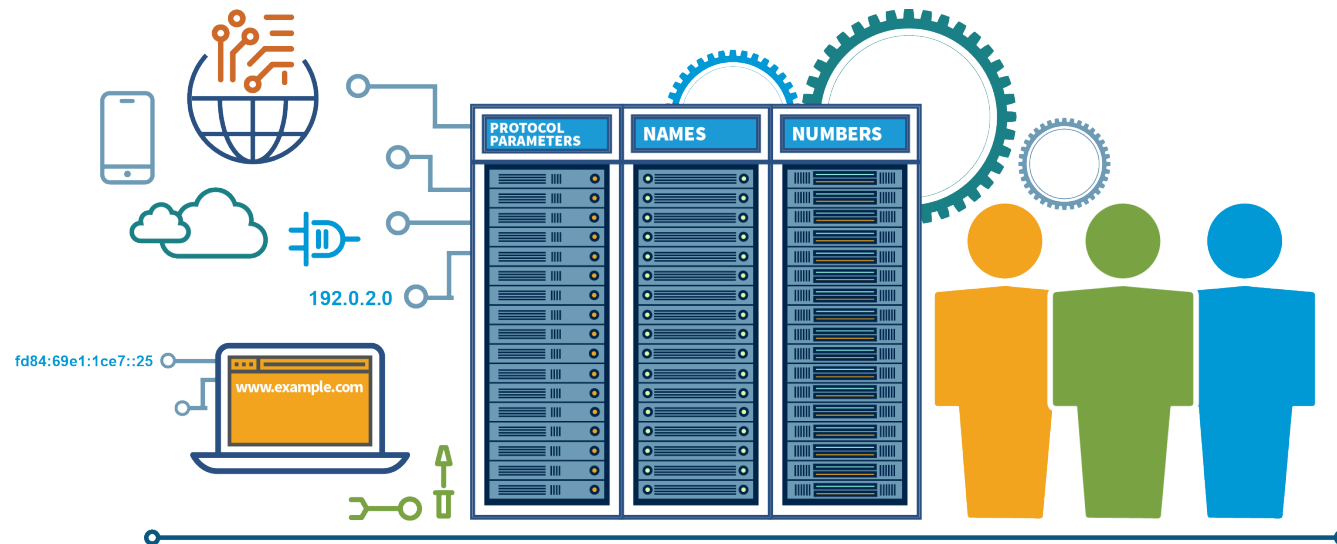
Savenaca Vocea – VP, Stakeholder Engagement - Oceania

PacNOG 20, Suva, FJ
3 July 2017

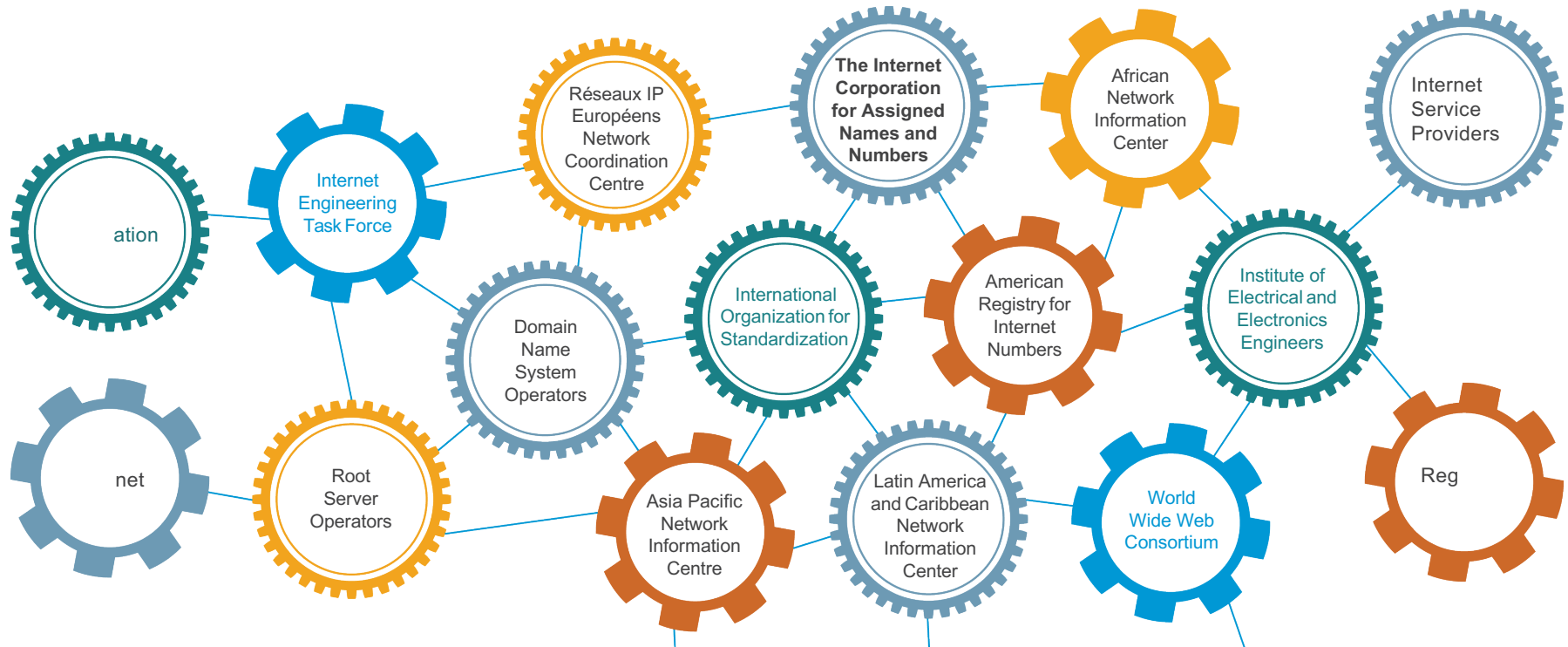**Coordinating with our partners,
we help make the Internet work.**

Our Technical Partners

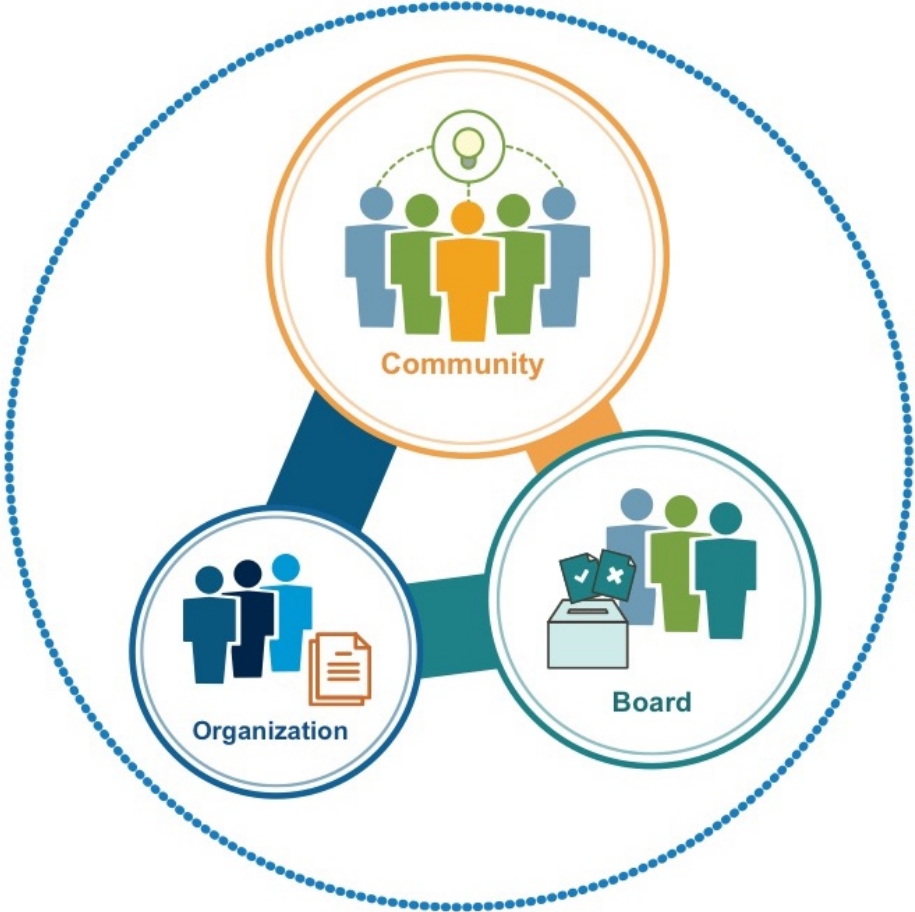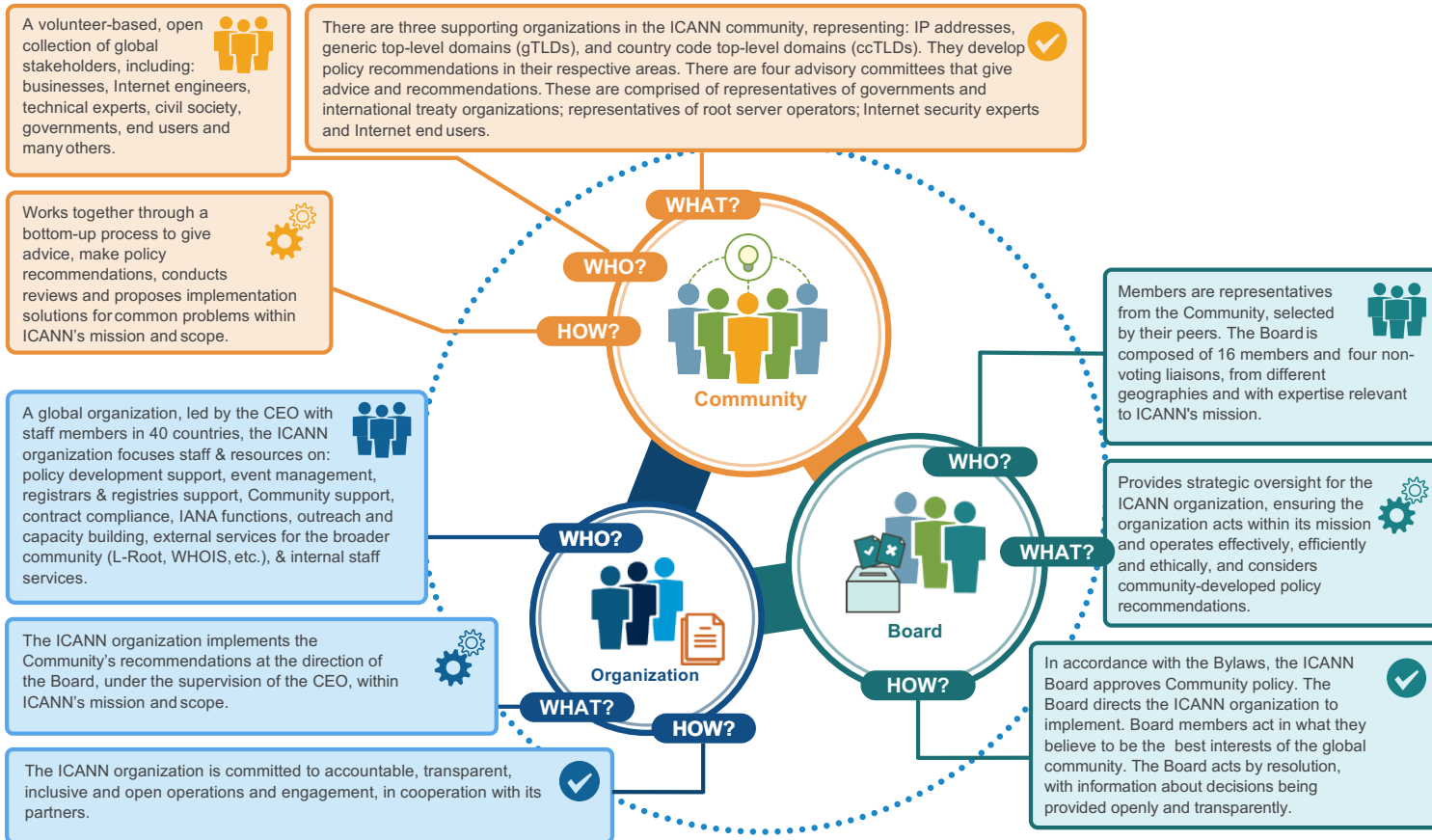## Coordinating with our technical partners, we help make the Internet work.

Our Other Partners

We all work together in different ways to help make the Internet work.
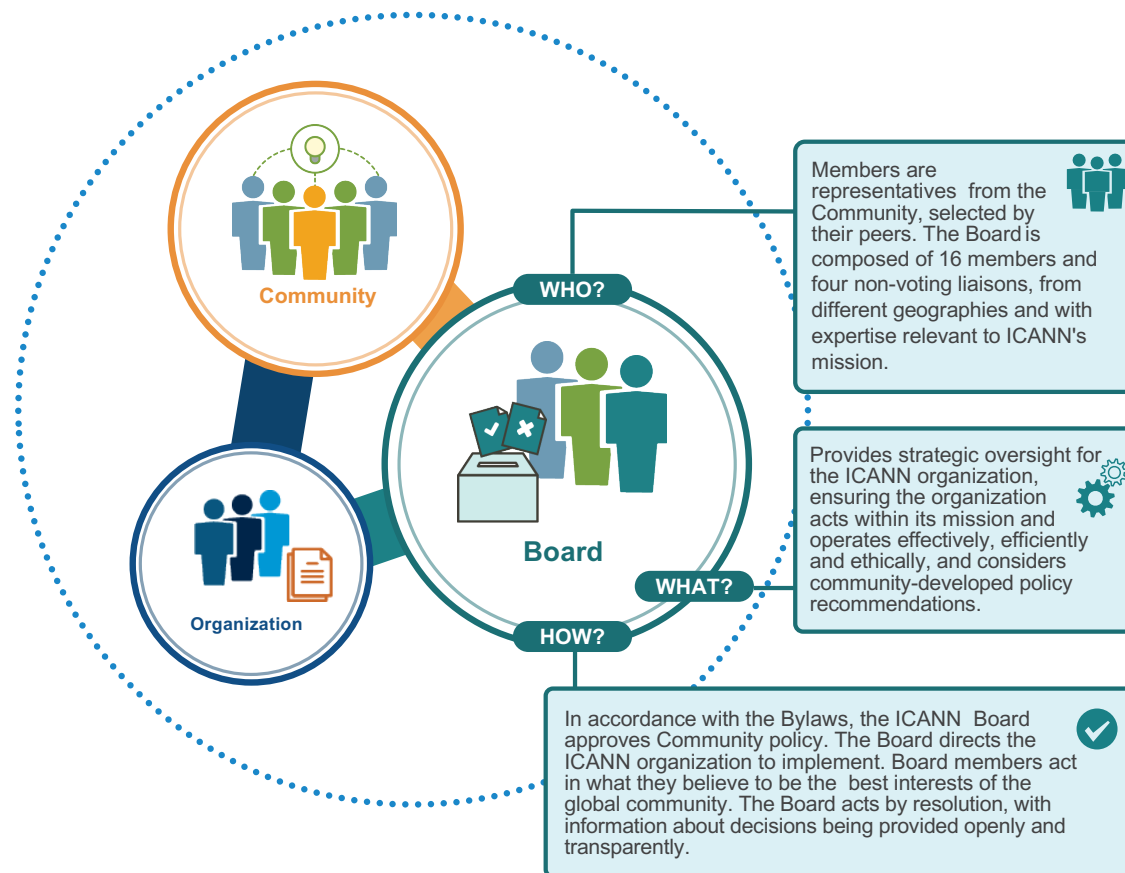
ICANN Ecosystem

Who We Are

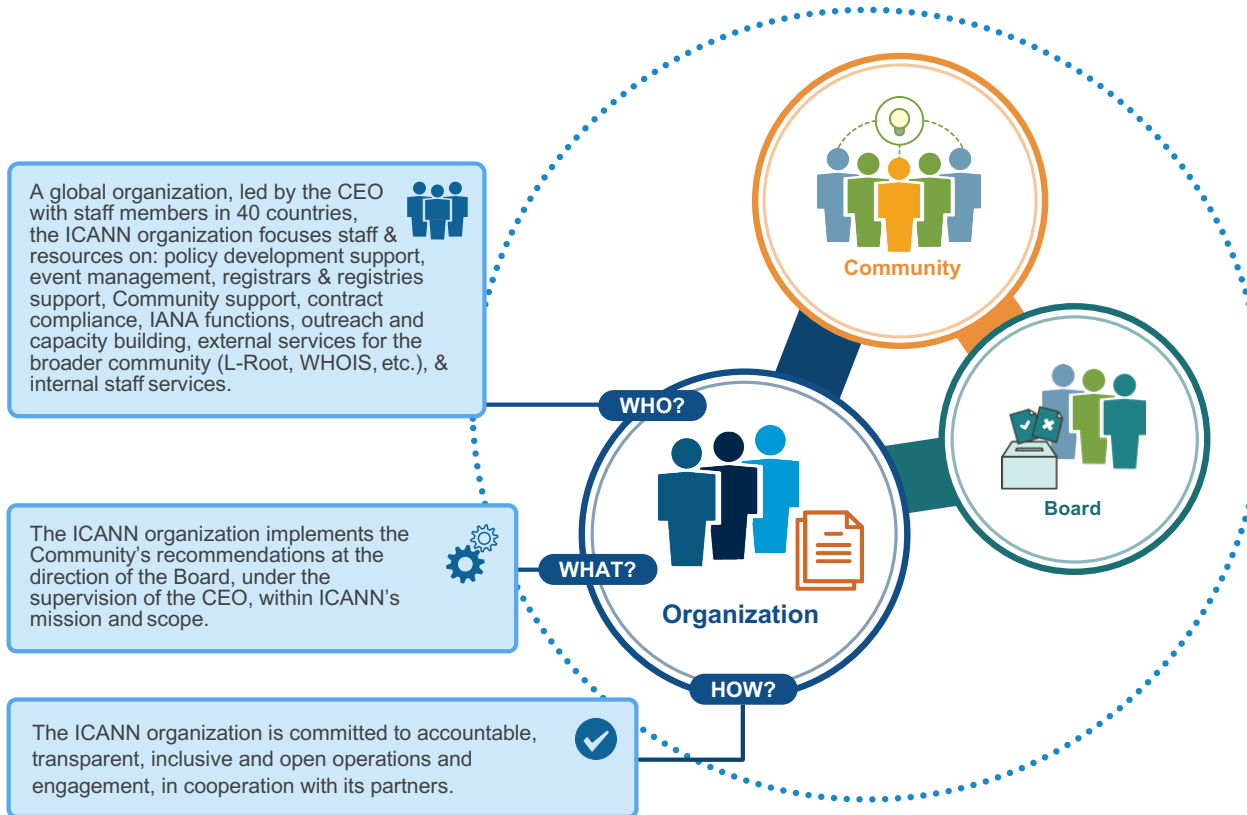A volunteer-based, open collection of global stakeholders, including: businesses, Internet engineers, technical experts, civil society, governments, end users and many others.

There are three supporting organizations in the ICANN community, representing: IP addresses, generic top-level domains (gTLDs), and country code top-level domains (ccTLDs). They develop policy recommendations in their respective areas. There are four advisory committees that give advice and recommendations. These are comprised of representatives of governments and international treaty organizations; representatives of root server operators; Internet security experts and Internet end users.

Works together through a bottom-up process to give advice, make policy recommendations, conducts reviews and proposes implementation solutions for common problems within ICANN's mission and scope.

Members are representatives from the Community, selected by their peers. The Board is composed of 16 members and four non-voting liaisons, from different geographies and with expertise relevant to ICANN's mission.

A global organization, led by the CEO with staff members in 40 countries, the ICANN organization focuses staff & resources on: policy development support, event management, registrars & registries support, Community support, contract compliance, IANA functions, outreach and capacity building, external services for the broader community (L-Root, WHOIS, etc.), & internal staff services.

Provides strategic oversight for the ICANN organization, ensuring the organization acts within its mission and operates effectively, efficiently and ethically, and considers community-developed policy recommendations.

The ICANN organization implements the Community's recommendations at the direction of the Board, under the supervision of the CEO, within ICANN's mission and scope.

In accordance with the Bylaws, the ICANN Board approves Community policy. The Board directs the ICANN organization to implement. Board members act in what they believe to be the best interests of the global community. The Board acts by resolution, with information about decisions being provided openly and transparently.

The ICANN organization is committed to accountable, transparent, inclusive and open operations and engagement, in cooperation with its partners.

WHAT? **WHO?** **HOW?**

Community

WHO? **WHAT?** **HOW?**

Organization

WHO? **WHAT?** **HOW?**

Board

The ICANN Community

A volunteer-based, open collection of global stakeholders, including: businesses, Internet engineers, technical experts, civil society, governments, end users and many others.

There are three supporting organizations in the ICANN community, representing: IP addresses, generic top-level domains (gTLDs), and country code top-level domains (ccTLDs). They develop policy recommendations in their respective areas. There are four advisory committees that give advice and recommendations. These are comprised of representatives of governments and international treaty organizations; representatives of root server operators; Internet security experts and Internet end users.

Works together through a bottom-up process to give advice, make policy recommendations, conducts reviews and proposes implementation solutions for common problems within ICANN's mission and scope.

WHO?

WHAT?

HOW?

Community

Organization

Board

The ICANN Board

Community

Organization

Board

WHO?

WHAT?

HOW?

Members are representatives from the Community, selected by their peers. The Board is composed of 16 members and four non-voting liaisons, from different geographies and with expertise relevant to ICANN's mission.

Provides strategic oversight for the ICANN organization, ensuring the organization acts within its mission and operates effectively, efficiently and ethically, and considers community-developed policy recommendations.

In accordance with the Bylaws, the ICANN Board approves Community policy. The Board directs the ICANN organization to implement. Board members act in what they believe to be the best interests of the global community. The Board acts by resolution, with information about decisions being provided openly and transparently.

The ICANN Organization

A global organization, led by the CEO with staff members in 40 countries, the ICANN organization focuses staff & resources on: policy development support, event management, registrars & registries support, Community support, contract compliance, IANA functions, outreach and capacity building, external services for the broader community (L-Root, WHOIS, etc.), & internal staff services.

WHO?

The ICANN organization implements the Community's recommendations at the direction of the Board, under the supervision of the CEO, within ICANN's mission and scope.

WHAT?

The ICANN organization is committed to accountable, transparent, inclusive and open operations and engagement, in cooperation with its partners.

HOW?

Community

Board

Organization

How Does the Community Develop Policy?

IDENTIFY AND SCOPE THE ISSUE

BOARD VOTES

Address Supporting Organization

Country Code Names Supporting Organization

Generic Names Supporting Organization

Supporting organizations identify, initiate and create policy

1 Identify issue

Issue report

Initiate policy development process

2 DEVELOP POLICY

DRAFT POLICY RECS

Consult with Community and produce policy

Call for volunteers to develop policy

3 Submit final report to Board

Public comments by Community

POLICY RECS

4 VOTING OR REVIEW

Board votes on final policy

5 Implementation

FINAL POLICY

Advisory Committees can participate during the process

At-Large Advisory Committee

Security and System Advisory Committee

Root Server System Advisory Committee

Government Advisory Committee

ICANN

Some of What ICANN Organization Does

Domain Name System
The domain name system provides addressing for the Internet so people can find websites, send email, and other tasks. The ICANN organization also supports the stability of the DNS through its work, and also its contracts and accreditations.

Policy Development
The ICANN organization supports inclusive, open and transparent multi-stakeholder bottom-up consensus based policy development mechanisms.

L-Root
The ICANN organization hosts and supports one of the 13 L-Root infrastructures. At over 150 locations worldwide, L-Root is critical to infrastructure that helps reduce latency and improves performance of the DNS.

Support and Grow the Community
The ICANN organization engages, nurtures and supports interested stakeholders for active and meaningful participation in ICANN. ICANN connects with stakeholders through outreach and engagement, and meeting & event support.

Generic Top-Level Domains
The ICANN organization manages the domain name system's top-level domains. ICANN helps promotes competition and choice in the gTLD marketplace.
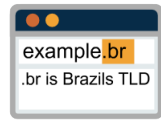
Country Code Top-Level Domains
The ICANN organization delegates top-level domains identified with a country code. Management is done by national ccTLD operators.

Protocol Parameters
The ICANN organization, in coordination with the Internet Engineering Task Force, manages protocol parameters by maintaining many of the codes and numbers used in Internet protocols.

Internet Protocol Addresses
By serving as the central repository for IP addresses, the ICANN organization helps coordinate how IP addresses are supplied – preventing repetition and conflicts.

Root Zone Management
The ICANN organization helps manage the root zone through the IANA functions, which involves assigning the operators of top-level domains, such as .bank and .com, and maintaining the technical and administrative details.

IANA Functions

Important topics discussed during ICANN59

Registration Directory Services (RDS) and Data Protection Rules

Public Safety (DNS Abuse) and Capacity Development to Underserved regions

New gTLD Auction Proceeds

Geographic Names as Top-Level Domains

Use of country code registration at 2nd Level Domain

Enhancing ICANN Accountability and

Subsequent round for new gTLDs

Universal Acceptance

Root zone Key Signing Key (KSK) Rollover

KSK Rollover: An Overview

ICANN is in the process of performing a Root Zone DNS Security Extensions (DNSSEC) Key Signing Key (KSK) rollover

⊙ The Root Zone DNSSEC Key Signing Key "**KSK**" is the top most cryptographic key in the DNSSEC hierarchy

⊙ The KSK is a cryptographic public-private key pair:

   o   Public part: trusted starting point for DNSSEC validation

   o   Private part: signs the Zone Signing Key (ZSK)

⊙ Builds a "chain of trust" of successive keys and signatures to validate the authenticity of any DNSSEC signed data

Why is ICANN Rolling the KSK?

- ⦿ As with passwords, the cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
  - ○ Ensures infrastructure can support key change in case of emergency

- ⦿ This type of change has never before occurred at the root level
  - ○ There has been one functional, operational Root Zone DNSSEC KSK since 2010

- ⦿ The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations

When Does the Rollover Take Place?

The KSK rollover is a process, not a single event

The following dates are key milestones in the process when end users
may experience interruption in Internet services:

19 September 2017	11 October 2017	11 January 2018	22 March 2018	August 2018
Size increase for DNSKEY response from root name servers.	New KSK is used for signing for the first time.	The old KSK is revoked.	Last day the old KSK appears in the root zone.	Old key is deleted from equipment in both ICANN Key Manage.
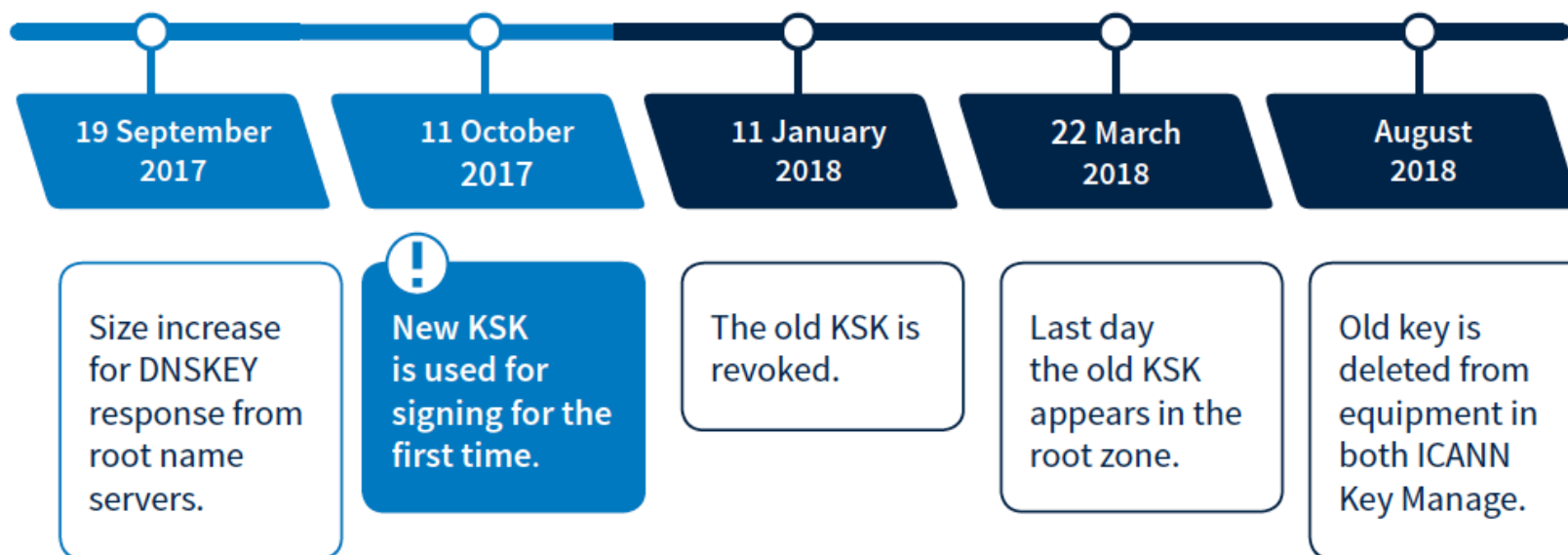
Who Will Be Impacted?

DNS Software Developers & Distributors	System Integrators	Network Operators
Root Server Operators	Internet Service Providers	End Users *(if no action taken by resolver operators)*

Why You Need to Prepare

> **If you have enabled DNSSEC validation, you must update your systems with the new KSK to help ensure trouble-free Internet access for users**

- Currently, 25 percent of global Internet users, or **750 million people**, use DNSSEC-validating resolvers that could be affected by the KSK rollover

- If these validating resolvers do not have the new key when the KSK is rolled, end users relying on those resolvers will encounter errors and be **unable to access the Internet**

What Do Resolver Operators Need to Do?

Be aware whether DNSSEC is enabled in your servers

Be aware of how trust is evaluated in your operations

Test/verify your set ups
- o Make sure trust anchor can be changed

Inspect configuration files, are they (also) up to date?

If DNSSEC validation is enabled or planned in your system
- o Have a plan for participating in the KSK rollover
- o Know the dates, know the symptoms, solutions

How To Update Your System

If your software supports automated updates of DNSSEC trust anchors (RFC 5011):

- ⊙ The KSK will be updated automatically at the appropriate time
- ⊙ You do not need to take additional action
  - ○ Devices that are offline during the rollover will have to be updated manually if they are brought online after the rollover is finished

If your software does <u>not</u> support automated updates of DNSSEC trust anchors (RFC 5011) or is not configured to use it:

- ⊙ The software's trust anchor file must be manually updated
- ⊙ The new root zone KSK is now available here after March 2017:

Root Anchors ▶

data.iana.org/ root-anchors/

Check to See If Your Systems Are Ready

ICANN is offering a **test bed** for operators or any interested parties to confirm that their systems handle the automated update process correctly.

Check to make sure your systems are ready by visiting:
go.icann.org/KSKtest

Automated Trust Anchor Update Testbed

The root zone Key Signing Key (KSK) is changing, or rolling, on 11 October 2017. Operators of recursive resolvers with DNSSEC validation enabled will need to ensure that their systems are updated with the new root zone KSK configured as a trust anchor before that date. If a recursive resolver supports RFC 5011, "Automated Updates of DNS Security (DNSSEC) Trust Anchors", and this feature is properly configured, the new KSK should automatically be installed as a trust anchor and DNSSEC validation should continue without problems.

If a validating resolver's implementation or configuration of the RFC 5011 automated trust anchor update protocol is incorrect for any reason, then its configuration might not be properly updated during the root zone KSK roll and resolution would fail after 11 October 2017.

This testbed allows operators of validating resolvers to test their implementation and confirm its ability to properly follow a KSK roll and update its trust anchor configuration.

This test protocol assumes that you understand **the upcoming KSK change**, and at least some about **RFC 5011**.

Purpose of This Testbed

- Allow resolver operator to test RFC 5011 support
  - Operates in real time.
  - Should not affect the resolver's normal operation.

The testbed starts a KSK roll in a new zone each week. For example, the current zone name is 2017-06-25.automated-ksk-test.research.icann.org.

Three Steps to Recovery

If your DNSSEC validation fails after the key role:

Stop the tickets
It's OK to turn off DNSSEC validation while you fix (but remember to turn it back on!)

Debug
If the problem is the trust anchor, find out why it isn't correct
   o Did RFC 5011 fail? Did configuration tools fail to update the key?
   o If the problem is fragmentation related, make sure TCP is enabled and/or make other transport adjustments

Test the recovery
Make sure your fixes take hold

Our "Ask" of you

⊙ Use ICANN's testing platform to confirm that your validating infrastructure supports the ability to handle the rollover without manual intervention.

  ⊙ Platform at go.icann.org/KSKtest

⊙ Help us increase awareness of the key change throughout your communities.

  ⊙ Awareness will assure the roll goes smoothly

For More Information

Join the conversation online
- Use the hashtag #KeyRoll
- Sign up to the mailing list https://mm.icann.org/listinfo/ksk-rollover

Ask a question to globalsupport@icann.org
- Subject line: "KSK Rollover"

Attend an event
- Visit https://features.icann.org/calendar to find upcoming KSK rollover presentations in your region

Learn more ▶

https://icann.org/kskroll

Upcoming Meetings

ICANN **60**
ANNUAL GENERAL
ABU DHABI
28 October–3 November 2017
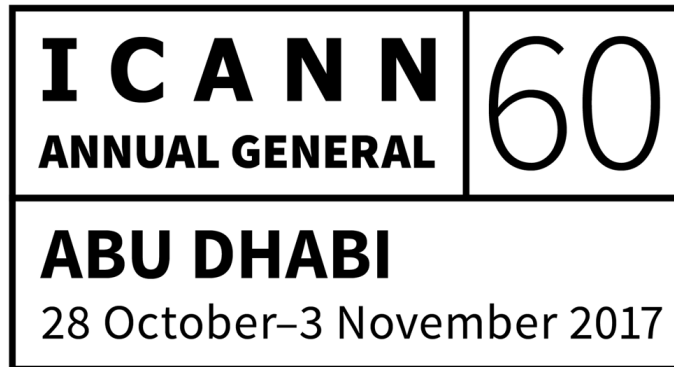
To find out how to participate, go to: https://meetings.icann.org/en/about

For a schedule of past and upcoming meetings, go to: http://meetings.icann.org/calendar

If you belong to an organization that is interested in having an exhibit at a meeting or in sponsoring a meeting, please contact: meeting-sponsorship@icann.org

Get Involved and Informed

Attend an ICANN Public Meeting. Three times a year, ICANN holds free and open public meetings in different regions around the world. Visit **meetings.icann.org** to learn more.

Visit **go.icann.org/journey** to learn how you can attend an ICANN Public Meeting as part of the NextGen@ICANN or ICANN Fellowship programs.

Take a free online course at **learn.icann.org**.

Attend events in your region.

Find and participate in an ICANN community group by visiting **icann.org/community**.

Sign up for ICANN news alerts and regional newsletters.

Programs Available

Fellowship	Global Capacity Building Program to support ICANN's Multistakeholder community; online application process 3x year around an ICANN Meeting (1 Mtg for Alumni only)
NextGen	Regionally based Program to create awareness and promote future discussions within universities and other regional forums; online application process 3x a year around an ICANN Meeting
Newcomer	Those just entering the ICANN community can self-educate using the Newcomer webpage or participate in person or remotely at the ICANN Meeting Newcomer Sunday

Video on Fellowship/NextGen: https://www.youtube.com/watch?v=nrV_ZkDEfIQ
Video on Newcomers: https://www.youtube.com/watch?v=da1RQt9-e-g

Engage with ICANN

ICANN

Thank You and Questions

Visit us at **icann.org**
Email: save.vocea@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann