



ICANN Updates

Rodrigo de La Parra | CANTO 33 – Punta Cana | 19 July 2017

Agenda- ICANN Updates

- ⦿ IANA Stewardship Transition -
COMPLETED
- ⦿ ICANN59 – Johannesburg - Policy
Forum
- ⦿ DNSSEC: Securing the Domain Name
System

IANA Stewardship Transition - COMPLETED

IANA Functions Contract Expires

- ⦿ **1 October 2016:** The contract between ICANN and the U.S. National Telecommunications and Information Administration (NTIA), to perform the IANA functions, officially expired.



Key Points

1

The U.S. Government's plan from the start

The USG always envisioned its role in the DNS as temporary because it recognized that the DNS would be better served by the private sector. It believes that ICANN has matured and taken steps in recent years to improve both its accountability and transparency, and its technical competence. The USG will continue to be active participants in the multistakeholder community through its membership in the GAC and participation in other Internet forums.

The status quo is not an option. The Internet is a global resource, over which the USG cannot expect to continue to hold unique authority without triggering international repercussions.

2

The success of the multistakeholder model

The private sector multistakeholder approach is a proven model in Internet Governance. This transition is the “canary in the coal mine” for ICANN and its multistakeholder community, and if the transition fails, issues dealing with the Internet will be given directly to governments for guidance in the future.

3

The enhancement of operational capability for the Internet

This transition will allow for the continued expansion, diversity and innovation of one, unified and interoperable Internet. ICANN is technically competent and capable of continuing to manage the IANA functions after the transition.

4

The evolution of ICANN

Accountability mechanisms were built into the ICANN structure and model itself, providing the organization with an inherent form of checks and balances through which all stakeholders can participate.

ICANN has convened a multistakeholder process to determine if ICANN's current accountability mechanisms can be enhanced to provide further assurance that it is safe from takeover in absence of the U.S. Government's stewardship role.

ICANN59

I C A N N
POLICY FORUM

59

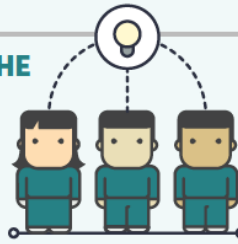
JOHANNESBURG

26-29 June 2017



GNSO PDP

IDENTIFY THE ISSUE



1

- GNSO Council, ICANN Board or an AC identifies issue.
- GNSO Council considers if issue will result in consensus policy.

2

- If yes, GNSO Council requests Preliminary Issue Report.
- Staff publishes Preliminary Issue Report for Public Comment Period.
- Following Public Comment review, Final Issue Report is submitted for GNSO Council consideration.

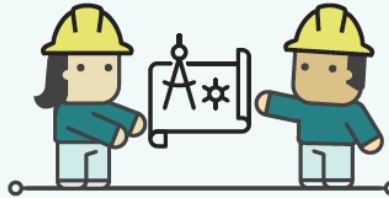
SCOPE THE ISSUE



3

- GNSO Council considers Final Issue Report and decides whether to initiate PDP.
- If yes, GNSO Council develops/adopts charter for PDP WG.
- GNSO Council calls for volunteers to form PDP WG.

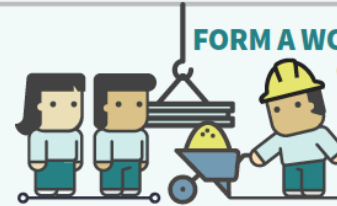
INITIATE THE PDP



4

- WG consults with Community and develops Initial Report for Public Comment Period.
- After reviews, WG submits Final Report to GNSO Council.

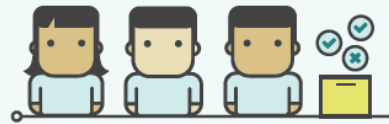
FORM A WORKING GROUP



5

- GNSO Council reviews Final Report and considers adoption.
- If adopted, GNSO Council submits Final Report to ICANN Board.

DELIBERATE THE FINAL REPORT



6

- ICANN Board consults Community and GAC.
- ICANN Board votes on Final Report recommendations.



VOTE BY ICANN BOARD

Post-ICANN59 Policy Report

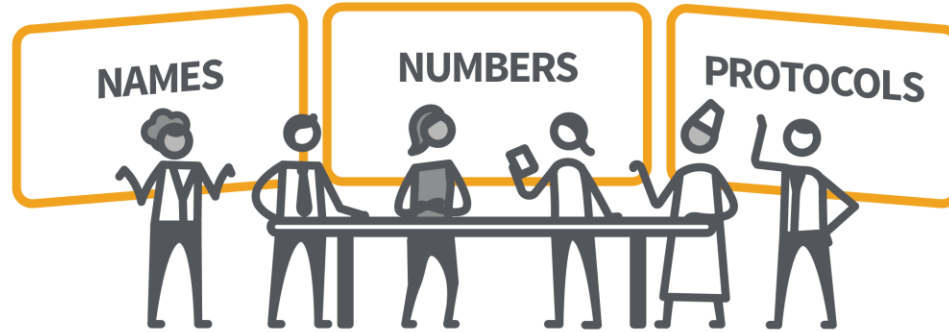


ICANN|59
JOHANNESBURG

DNSSEC: Making Domain Names Safer to use



IDENTIFIERS' PUBLIC REGISTRIES



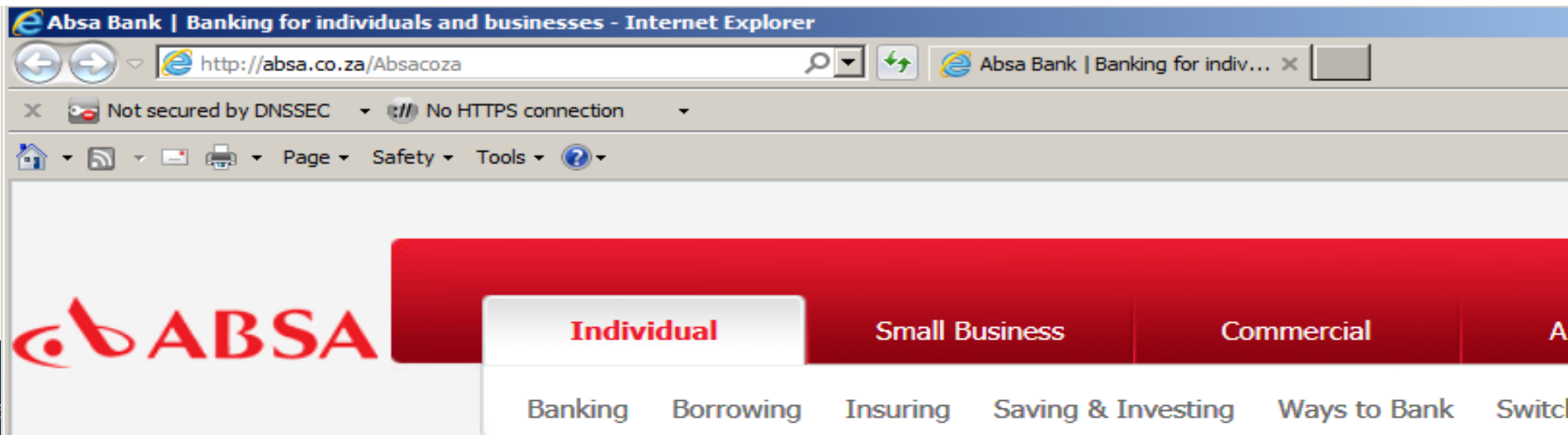


+



DNS Basics

- DNS converts names (absa.co.za) to numbers (196.36.75.6)
- ..to identify services such as www and e-mail
- ..that identify and link customers to business and visa versa



+1-202-70

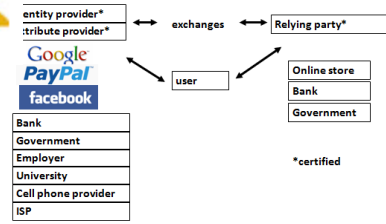
HealthCare.gov

US-NSTIC effort

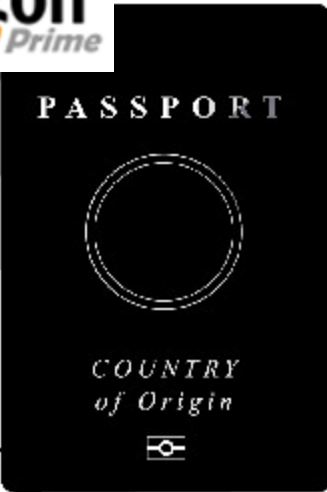
DNS is a part of all IT ecosystems



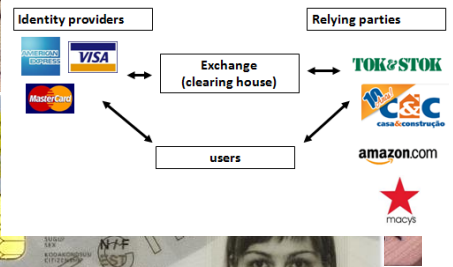
OECS ID effort



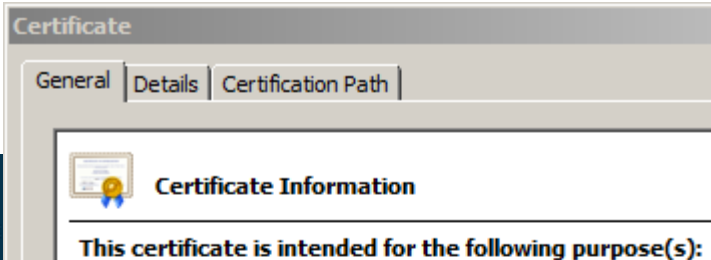
e-Passport symbol



Trust frameworks are not new



Smart Electrical Grid



mydomainname.com

amb@xtcn.com

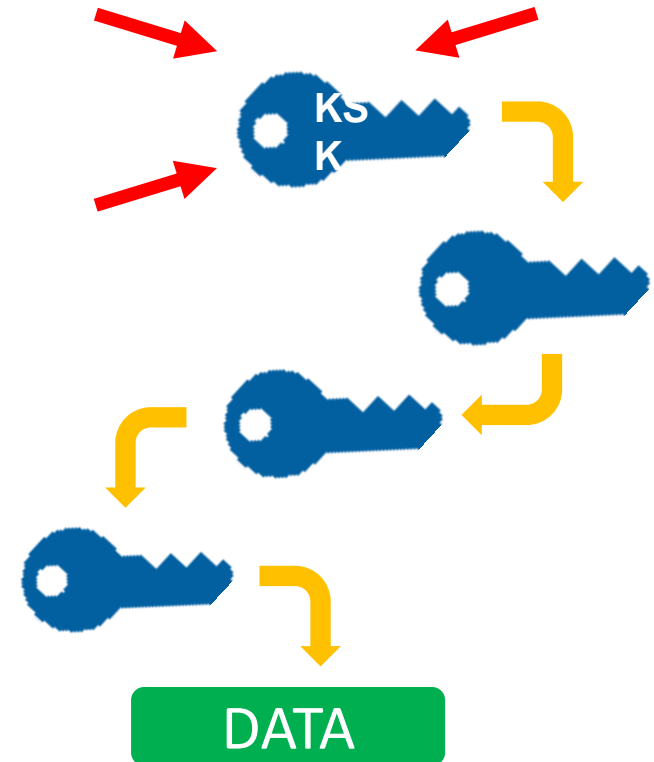


DNSSEC: Important Update

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:
 - Public part: trusted starting point for DNSSEC validation
 - 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?

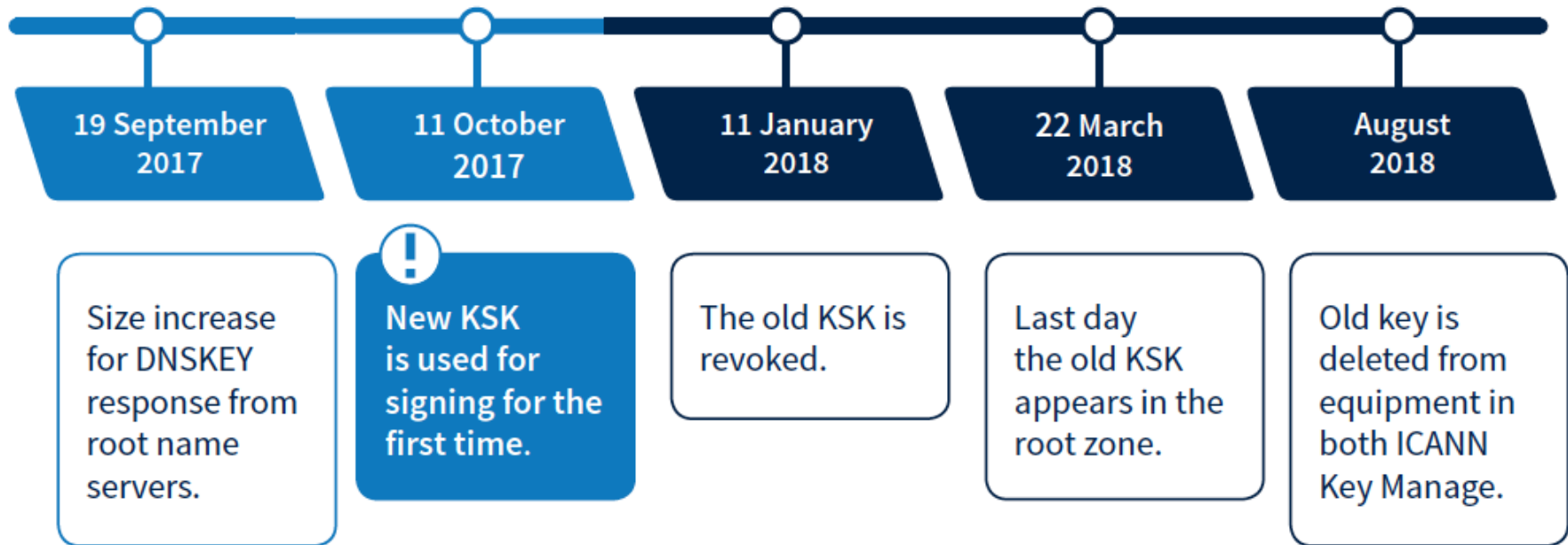
- ⦿ As with passwords, the cryptographic keys used in DNSSEC-signing DNS data should be changed periodically
 - Ensures infrastructure can support key change in case of emergency
- ⦿ This type of change has never before occurred at the root level
 - There has been one functional, operational Root Zone DNSSEC KSK since 2010
- ⦿ The KSK rollover must be widely and carefully coordinated to ensure that it does not interfere with normal operations

DNSSEC

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:



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 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



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



If DNSSEC validation is enabled or planned in your system

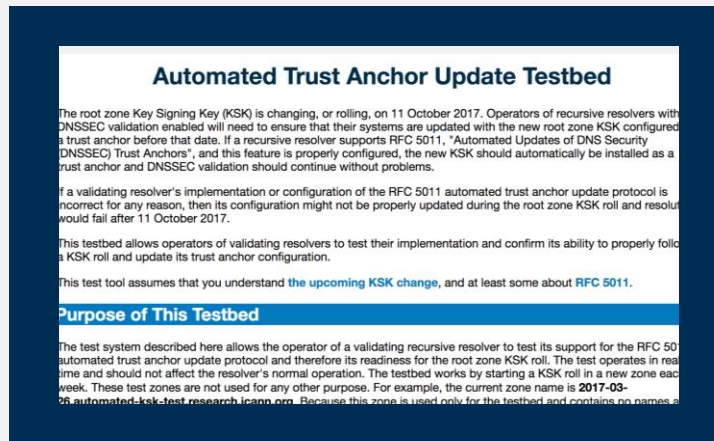
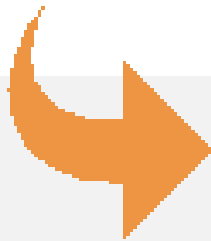
- Have a plan for participating in the KSK rollover
- Know the dates, know the symptoms, solutions



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

A screenshot of the 'Automated Trust Anchor Update Testbed' page. The page has a white background with a blue header and footer. The main content is in black text. The title is 'Automated Trust Anchor Update Testbed'. Below the title, there are several paragraphs of text. The first paragraph discusses the root zone Key Signing Key (KSK) change on October 11, 2017, and mentions RFC 5011. The second paragraph discusses the implementation of the RFC 5011 protocol. The third paragraph describes the testbed's purpose. The fourth paragraph mentions the current zone name '2017-03-28'. The page is framed by a dark blue border.

For More Information

1

Visit <https://icann.org/kskroll>

2

Join the conversation online

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

3

Ask a question to globalsupport@icann.org

- Subject line: “KSK Rollover”

4

Attend an event

- Visit <https://features.icann.org/calendar> to find upcoming KSK rollover presentations in your region





ICANN Updates

Rodrigo de La Parra | rodrigo.delaparra@icann.org
Albert Daniels | albert.daniels@icann.org