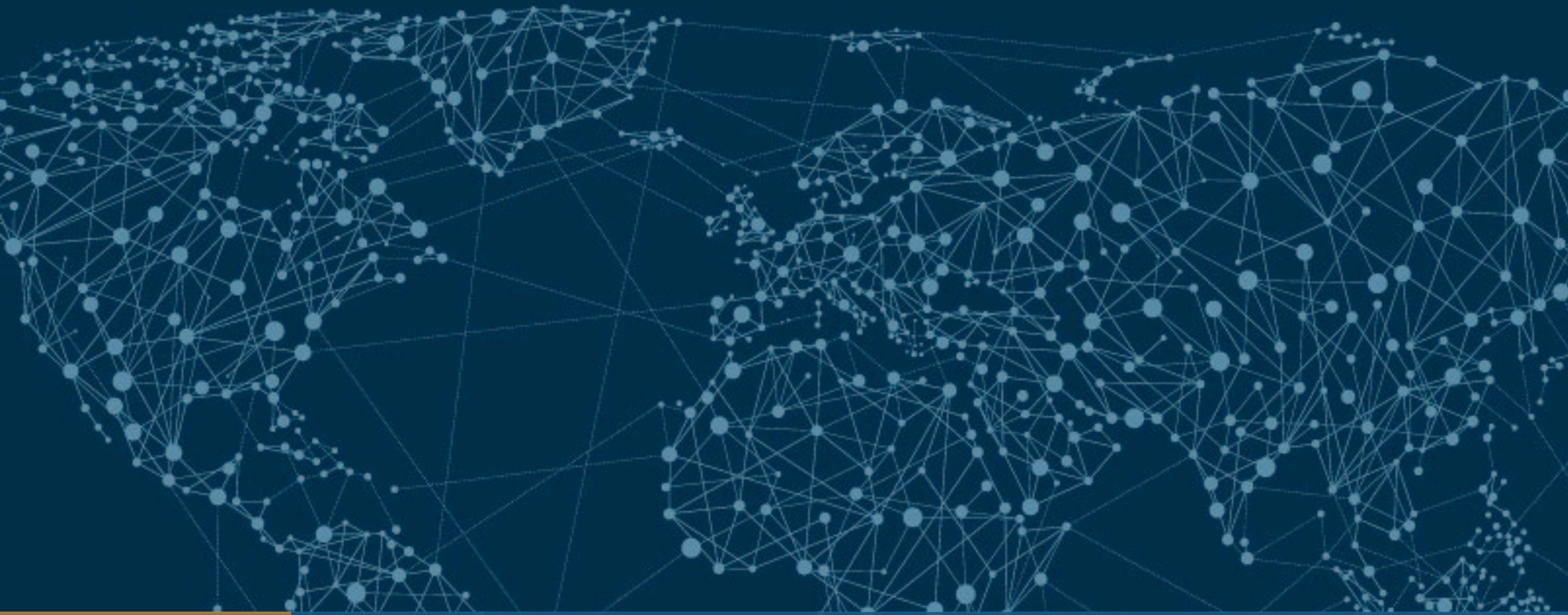


ICANN DNSSEC Roadshow

| Tunis, Tunisia | June 01, 2015

Yaovi Atohoun; Stakeholder Engagement & Ops Manager, Africa

Agenda

1

WHAT IS ICANN?

2

DNS and DNSSEC

3

DNS Cache Poisoning vulnerability

4

Africa DNSSEC Roadshow project

5

DNS-EC in Egypt

6

Conclusion

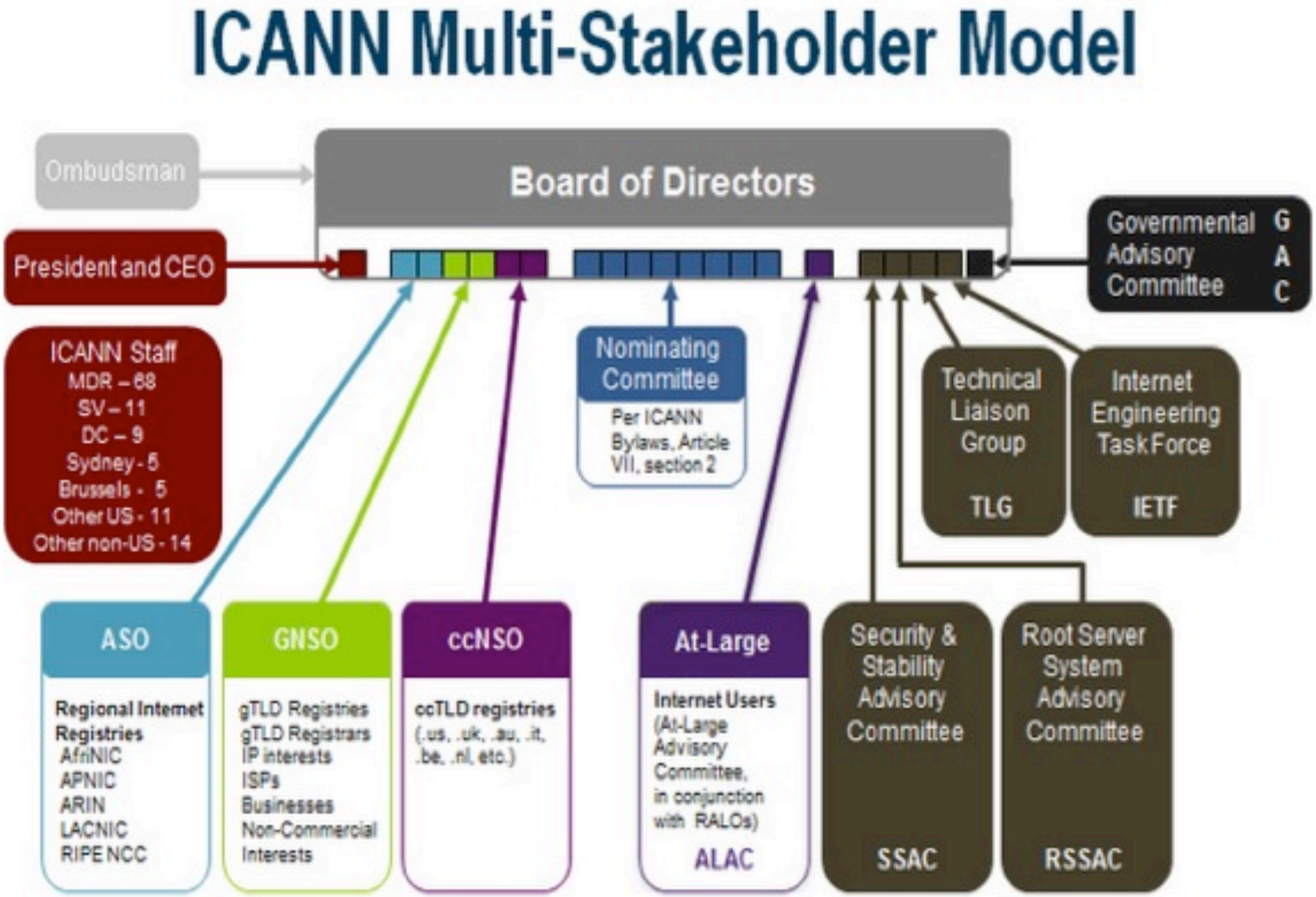
WHAT IS ICANN (I)

ICANN is a global multistakeholder organization created in 1998. ICANN manages Internet resources for the public benefit. It is a best known for its role as technical coordinator of the Internet's Domain Name System.

MISSIONS:

- Coordinates the allocation and assignment of Domain names, IP addresses, Protocol Ports
- Coordinates the operation and the evolution of the DNS root name server
- Coordinates Policy development reasonably and appropriately related to these technical functions

WHAT IS ICANN (II)


ICANN Multi-Stakeholder Model
Ombudsman
Board of Directors
President and CEO
Governmental Advisory Committee
G A C
ICANN Staff
MDR – 68
SV – 11
DC – 9
Sydney - 5
Brussels - 5
Other US - 11
Other non-US - 14
Nominating Committee
Per ICANN Bylaws, Article VII, section 2
Technical Liaison Group
TLG
Internet Engineering Task Force
IETF
ASO
Regional Internet Registries
AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC
GNSO
gTLD Registries
gTLD Registrars
IP interests
ISPs
Businesses
Non-Commercial Interests
ccNSO
ccTLD registries (.us, .uk, .au, .it, .be, .nl, etc.)
At-Large
Internet Users (At-Large Advisory Committee, in conjunction with RALOs)
ALAC
Security & Stability Advisory Committee
SSAC
Root Server System Advisory Committee
RSSAC

WHAT IS DNS ?

Every device on the Internet has a unique address (IP Address) – just like a telephone number – which is a rather complicated string of numbers. The DNS makes it easier by allowing a familiar string of letters (the "domain name") to be used instead of the IP address. Translating the name into the IP address is called "resolving the domain name.

WHAT IS DNSSEC?

DNSSEC abbreviates “DNS Security Extensions”. It adds security to the DNS (Domain Name System).

DNSSEC adds Security to the DNS by incorporating a public key cryptography into the DNS hierarchy

DNSSEC is a key solution to DNS Cache Poisoning

DNS Cache Poisoning vulnerability (I)

A method of inserting false data into a name server has been discovered by a security researcher. This method affects *recursive name servers*, which are usually provided by ISPs and network operators to provide DNS service to their end users.

As these types of name servers remember previous lookups in a cache, they are often called *caching name servers*, *caching resolvers* or similar.

DNS cache poisoning vulnerability (II)

The attack relies on the fact that an attacker can send fake DNS answers in response to a query and trick it into thinking the wrong data is correct for a given domain. The method is a specific type of *cache poisoning* attack.

It is called cache poisoning because the server remembers the wrong answer in its cache, and then provides that wrong answer in future lookups.

ILLUSTRATION: WITHOUT DNNSEC (I)

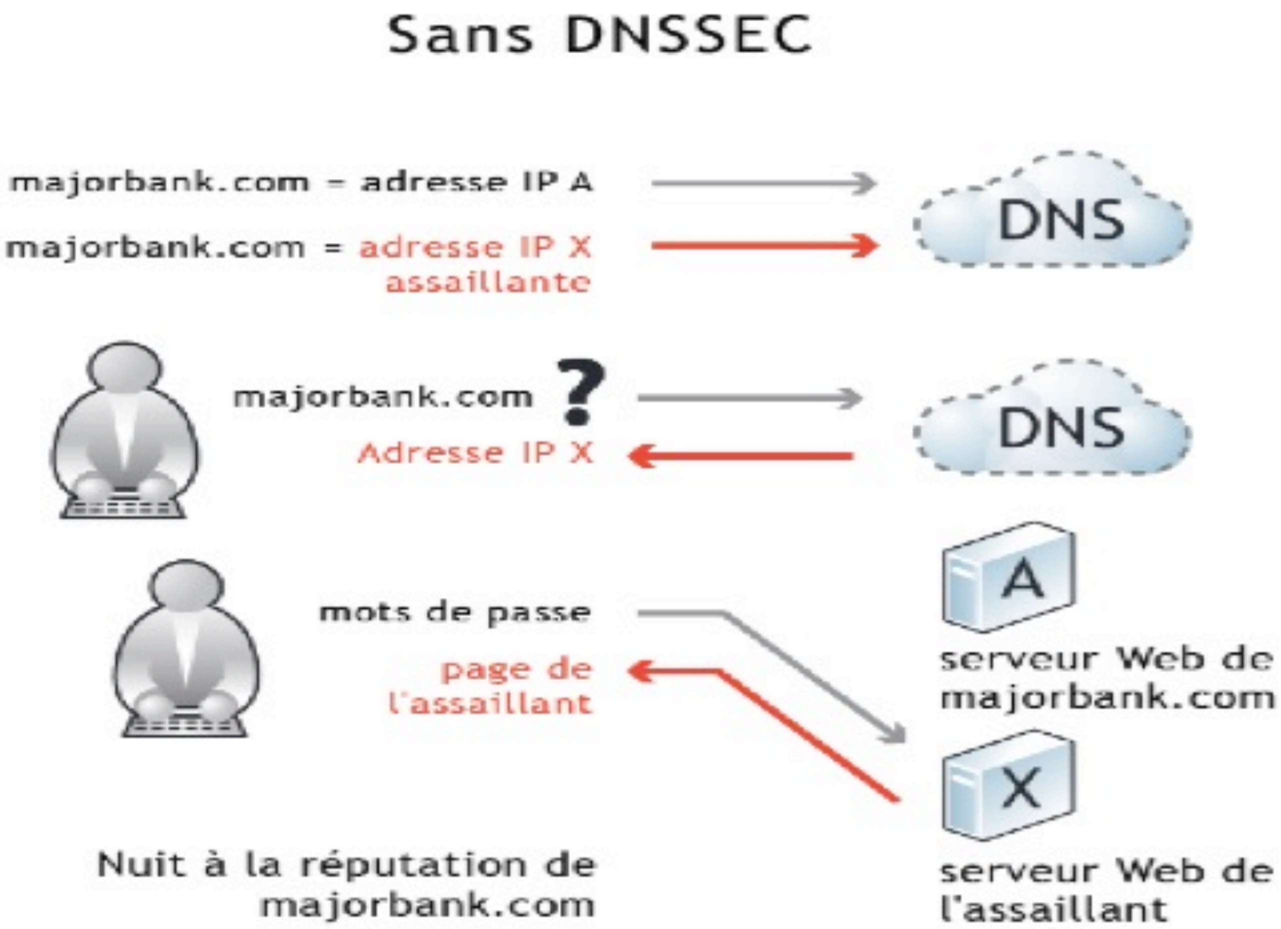
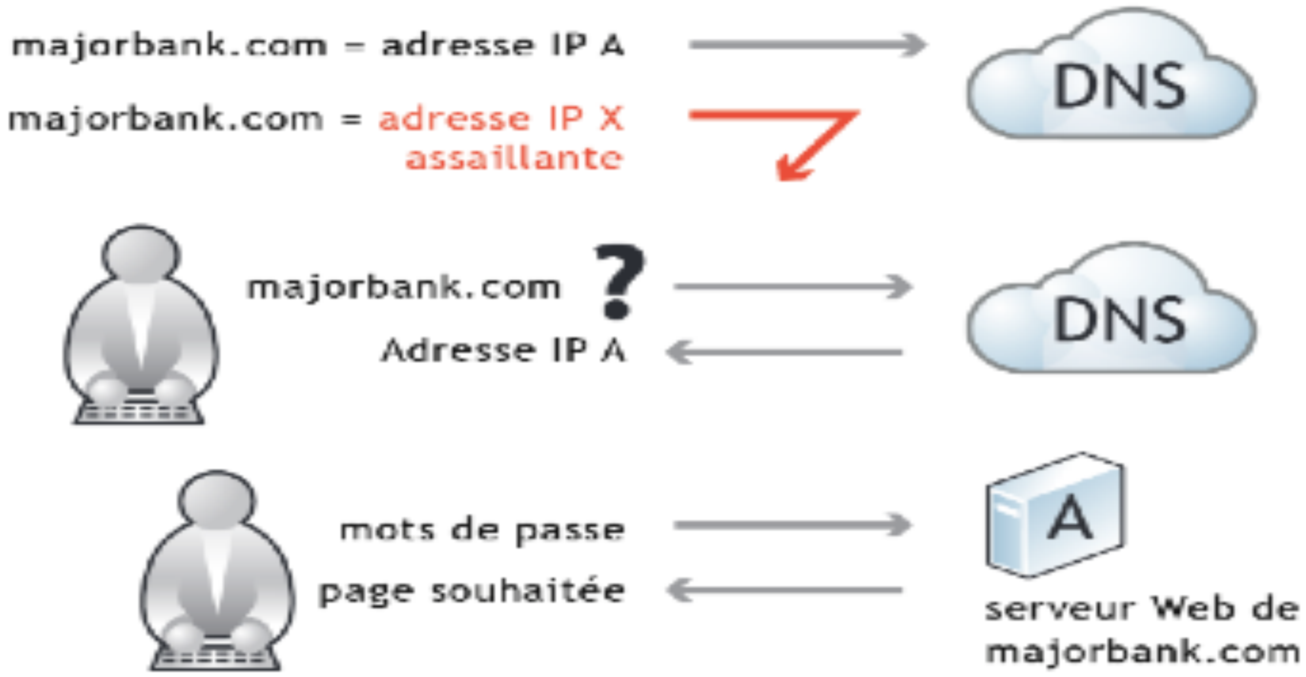
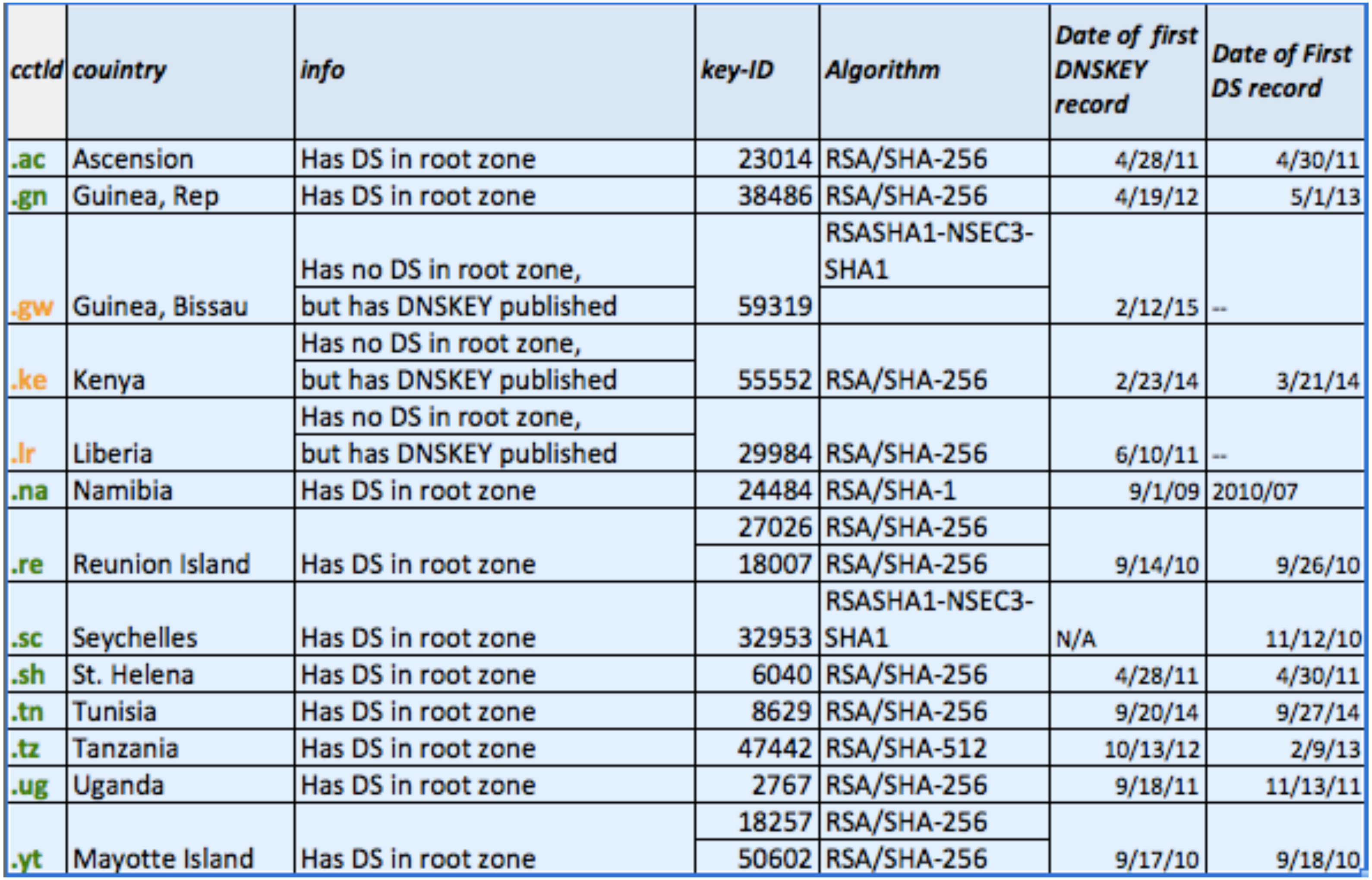

Sans DNSSEC
majorbank.com = adresse IP A
majorbank.com = adresse IP X assaillante
DNS
majorbank.com ?
Adresse IP X
DNS
mots de passe
page de l'assaillant
A
serveur Web de majorbank.com
X
serveur Web de l'assaillant
Nuit à la réputation de majorbank.com

ILLUSTRATION: WITH DNNSEC (II)

Avec DNSSEC


majorbank.com = adresse IP A
majorbank.com = adresse IP X assaillante
DNS
majorbank.com ?
Adresse IP A
DNS
mots de passe
page souhaitée
A
serveur Web de majorbank.com

AF DNSSEC IMPLEMENTATION STATUS Deployment in Africa SEEN on 2015/05/28



cctld	couintry	info	key-ID	Algorithm	Date of first DNSKEY record	Date of First DS record
.ac	Ascension	Has DS in root zone	23014	RSA/SHA-256	4/28/11	4/30/11
.gn	Guinea, Rep	Has DS in root zone	38486	RSA/SHA-256	4/19/12	5/1/13
.gw	Guinea, Bissau	Has no DS in root zone, but has DNSKEY published	59319	RSASHA1-NSEC3-SHA1	2/12/15	--
.ke	Kenya	Has no DS in root zone, but has DNSKEY published	55552	RSA/SHA-256	2/23/14	3/21/14
.lr	Liberia	Has no DS in root zone, but has DNSKEY published	29984	RSA/SHA-256	6/10/11	--
.na	Namibia	Has DS in root zone	24484	RSA/SHA-1	9/1/09	2010/07
.re	Reunion Island	Has DS in root zone	27026	RSA/SHA-256	9/14/10	9/26/10
			18007	RSA/SHA-256		
.sc	Seychelles	Has DS in root zone	32953	RSASHA1-NSEC3-SHA1	N/A	11/12/10
.sh	St. Helena	Has DS in root zone	6040	RSA/SHA-256	4/28/11	4/30/11
.tn	Tunisia	Has DS in root zone	8629	RSA/SHA-256	9/20/14	9/27/14
.tz	Tanzania	Has DS in root zone	47442	RSA/SHA-512	10/13/12	2/9/13
.ug	Uganda	Has DS in root zone	2767	RSA/SHA-256	9/18/11	11/13/11
.yt	Mayotte Island	Has DS in root zone	18257	RSA/SHA-256	9/17/10	9/18/10
			50602	RSA/SHA-256		

Source: dnssec-africa.org

AFRICA DNSSEC ROADSHOW **Project (I)**

1. Part of the implementation of the ICANN AFRICA Strategy
2. ICANN Africa Strategy adopted during ICANN meeting in Toronto. Version 2.0 discussed during ICANN 52 meeting in Singapore still considers the roadshow as a major project.

The Africa roadshows aim at sensitizing on DNSSEC deployment and contributing to showcase current deployments (where available) and organizing specific training for ccTLDs and ISPs managers.

AFRICA DNSSEC ROADSHOW Project (II)

The Roadshow is a 3 days event

Day1: is general awareness for the local community

Academia, Registries, Registrars, Registrants, ISPs, Decisions makers etc..

AFRICA DNSSEC ROADSHOW Project (II)

Day 2: is the tech day designated for the local DNS experts

- DNS
- Crypto
- Introduction to DNSSEC
- zones signature and validation
- Risk analysis
- Information on DNSSEC Key ceremony

Day3: is dedicated to the ccTLD registry

DNSSEC Roadshow Events

Madagascar: May 6-8, 201

Congo: March 11-13, 2015

Cote d'Ivoire: Feb 24-26, 2015

Botswana: 1-3 Dec 2014

Cameroon: 17-19 Sep 2014

Burkina Faso: 19-21-May 2014

Zambia: 28-30 April 2014

Senegal: 19-21 March 2014

Rwanda: 10-12 March 2014

Tanzania: 18-20 Sept 2013

Nigeria: 26-27 June 2013

Kenya: 11-13 June 2013

More countries to be covered in FY16

More information http://dnssec-africa.org

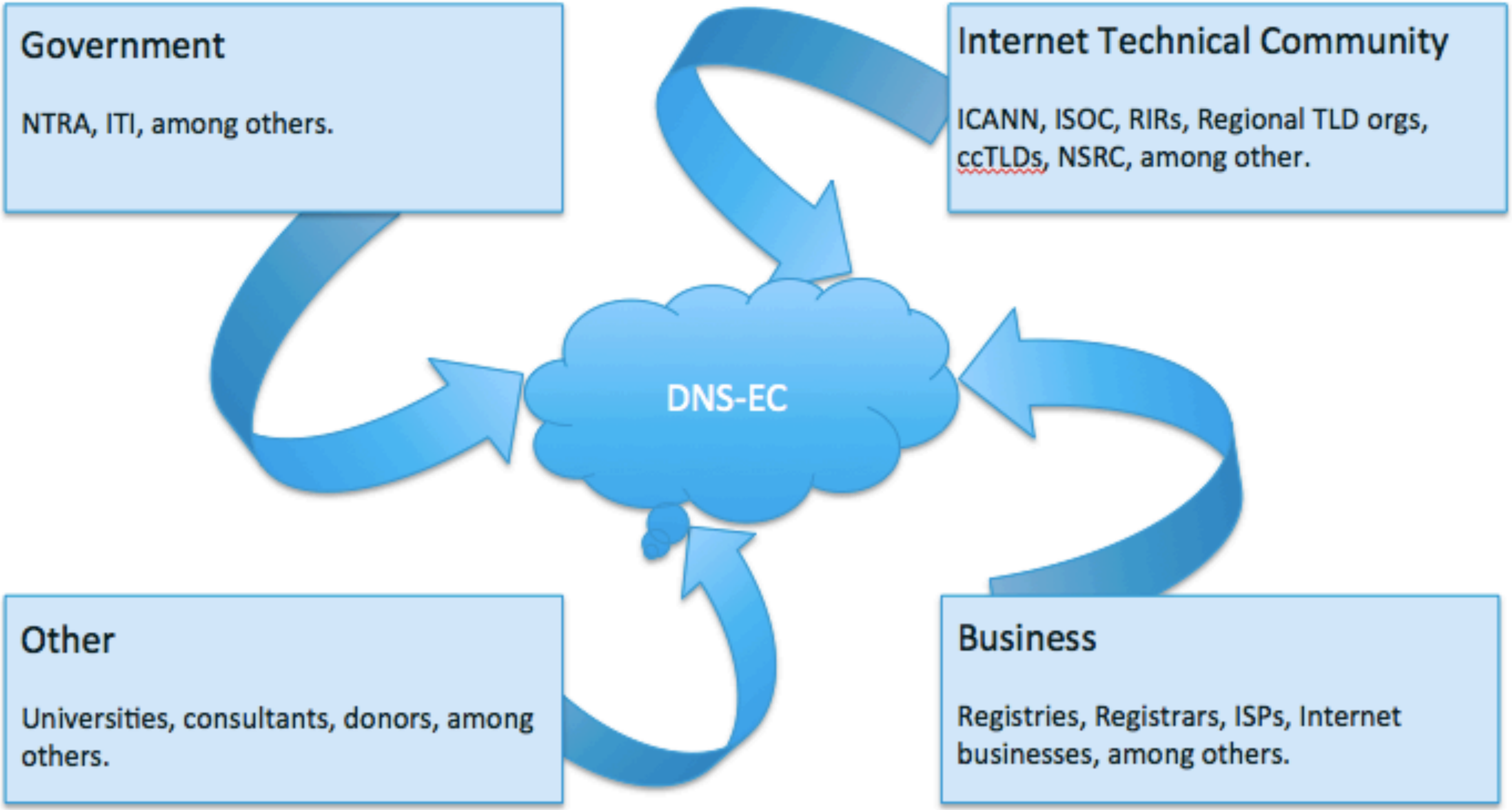
DNS-EC Egypt (I)

Background: Develop the domain name industry ecosystem in Africa and the Middle East (*ICANN Regional Strategies*).

Vision: The repository for DNS knowledge and expertise in Africa and the Middle East.

Mission: Develop a robust and healthy domain name ecosystem in Africa and the Middle East.

DNS-EC Egypt (II): Partners



Government

NTRA, ITI, among others.

Internet Technical Community

ICANN, ISOC, RIRs, Regional TLD orgs, ccTLDs, NSRC, among other.

Other

Universities, consultants, donors, among others.

Business

Registries, Registrars, ISPs, Internet businesses, among others.

Conclusion

- A secure ccTLD will contribute to secure many national entities as they have subdomains under the country ccTLD

- Only 13 out of 58 ccTLD have signed their zones means that there is a lot to be done

- Please are edu.yourcctld or ac.yourcctld signed?
  Are your resolvers validating signed zones?

- Please engage your REN community to enable validation and signed zones

- ICANN will continue to support any effort in DNSSEC deployment.

Engage with ICANN

Thank You and Questions

Reach us at:
Email: engagement@icann.org Website: icann.org

Other link: http://www.iana.org

- twitter.com/icann
- facebook.com/icannorg
- linkedin.com/company/icann
- youtube.com/user/icannnews
- gplus.to/icann
- weibo.com/ICANNorg
- flickr.com/photos/icann
- slideshare.net/icannpresentations