



# DNSSEC Workshop

Dan York, Internet Society | ICANN 54 | October 2015

# Remote Participation

Slides and audio streams at:

- **<https://meetings.icann.org/en/dublin54/schedule/wed-dnssec>**

Live video stream via YouTube at:

- **<http://bit.ly/dnssec54am>**
- **<http://bit.ly/dnssec54pm>**

# Program Committee

- Steve Crocker, Shinkuro, Inc.
- Mark Elkins, DNS/ZACR
- Cath Goulding, Nominet
- Jean Robert Hountomey, AfricaCERT
- Jacques Latour, CIRA
- Xiaodong Lee, CNNIC
- Luciano Minuchin, NIC.AR
- Russ Mundy, SPARTA, A Parsons Company
- Ondřej Surý, CZNIC
- Yoshiro Yoneya, JPRS
- Dan York, Internet Society
- Julie Hedlund and Kathy Schnitt, ICANN

# Luncheon Sponsors

- Afilias
- CIRA
- Dyn
- .SE
- SIDN



NOTE: One new sponsor will be needed for 2016!

# DNSSEC Implementer's Gathering Sponsors

The Program Committee held a DNSSEC Implementers Gathering on 19 October sponsored by:

- **Afilias**





# DNSSEC Implementer's Gathering



Thanks to:

- **Afilias**

**Who can sponsor the gathering at ICANN 55 in Marrakesh?**

The DNSSEC Workshop and associated activities at ICANN are an organized activity of the:

- **ICANN Security and Stability Advisory Committee (SSAC)**



with additional assistance from the:

- **Internet Society  
Deploy360 Programme**



# Program

**0900-0915 – Presentation: Dan York, Internet Society – *DNSSEC Workshop Introduction, Program, Deployment Around the World – Counts, Counts, Counts***

**0915-1045 – Panel Discussion: DNSSEC Activities in the European Region**

**1045-1100 – Coffee Break**

**1100-1215 – Panel Discussion – DNSSEC on the Edge**

**1215-1230 – Great DNS/DNSSEC Quiz**

**1230-1315 – Lunch Break**

**1315-1430 – Demonstrations and Presentations: DNSSEC and Applications**

**1430-1500– Presentation: *Services to Stimulate DNSSEC Validation***

**1500-1515 – Presentation: *DNSSEC - How Can I Help?***

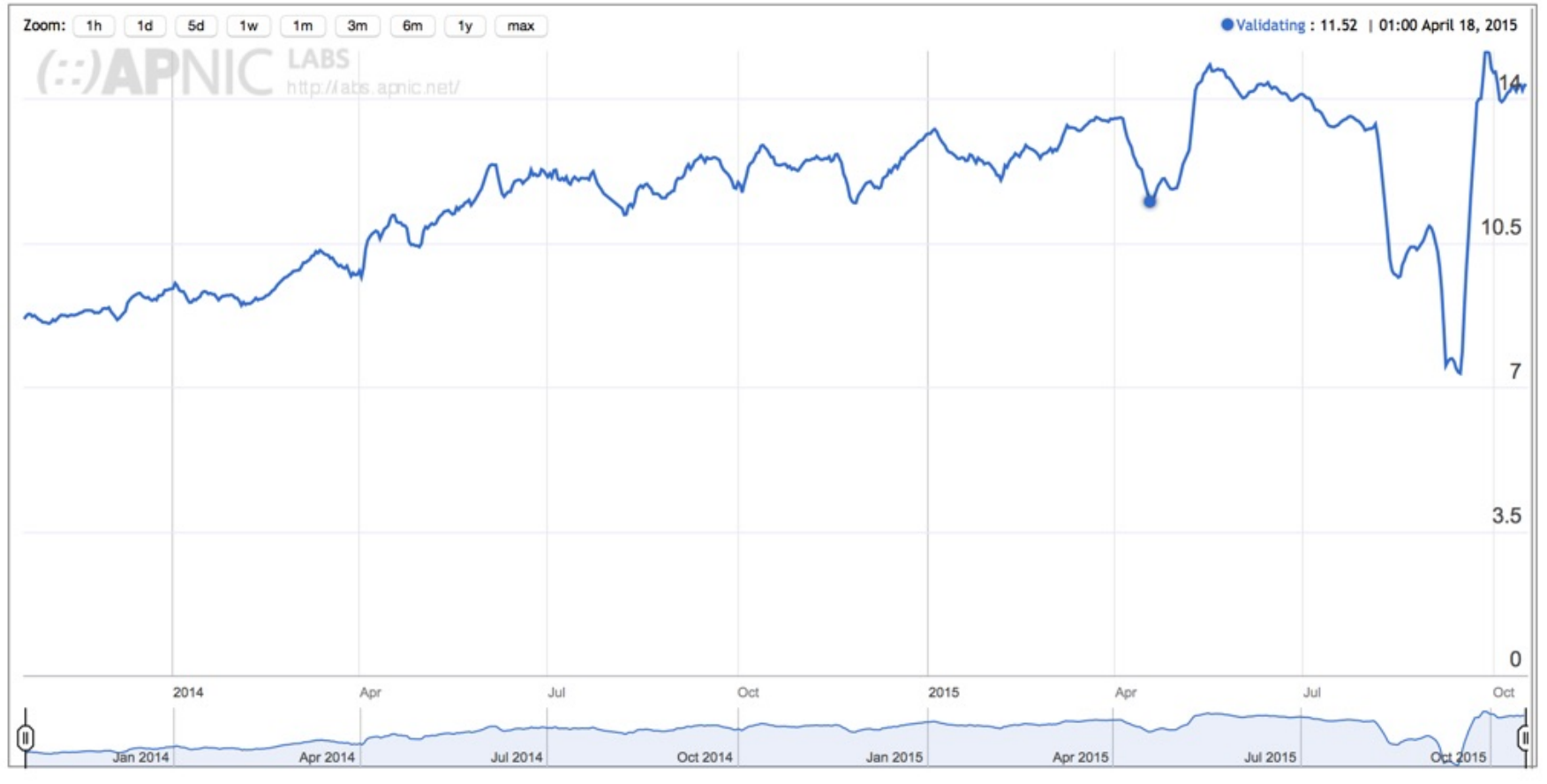




# DNSSEC Deployment Around the World: Counts, Counts, Counts

Dan York, Internet Society | ICANN 54 | October 2015

# Use of DNSSEC Validation for World (XA)



<http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=0&r=0&w=7&r=1>

Code	SubRegion	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
XH	Eastern Africa, Africa	30.45%	27.46%	3396719	3.23	10967673
XK	Southern Africa, Africa	23.81%	13.17%	707071	5.19	3668907
QQ	Melanesia, Oceania	23.43%	35.08%	255599	0.56	142310
XP	South America, Americas	21.77%	15.72%	49048713	0.64	31350807
XQ	Northern America, Americas	19.78%	11.76%	18344984	2.26	41389771
XW	Eastern Europe, Europe	19.51%	12.73%	35581051	0.64	22604741
QP	Australia and New Zealand, Oceania	18.47%	4.36%	1628665	2.01	3270567
QM	Northern Europe, Europe	18.13%	6.33%	10915805	1.11	12115432
QO	Western Europe, Europe	16.71%	7.24%	14404480	1.49	21480438
XU	South-Eastern Asia, Asia	15.52%	20.83%	62340122	0.46	28794140
XT	Southern Asia, Asia	14.14%	24.79%	39614279	1.67	66176071
XV	Western Asia, Asia	12.19%	11.96%	46678665	0.34	15782967
XL	Western Africa, Africa	11.72%	40.08%	2391900	4.82	11537650
QN	Southern Europe, Europe	11.06%	10.39%	53611739	0.24	12894012
XJ	Northern Africa, Africa	10.92%	15.47%	39226092	0.32	12382039
QR	Micronesia, Oceania	10.06%	30.96%	239907	0.1	24264
XI	Middle Africa, Africa	9.97%	27.62%	566551	2.68	1517584
XN	Caribbean, Americas	9.45%	18.87%	3006303	0.74	2226989
XO	Central America, Americas	7.77%	16.16%	11581661	0.87	10062123
XR	Central Asia, Asia	4.85%	8.41%	1387638	2.59	3588158
QS	Polynesia, Oceania	3.72%	9.14%	207967	0.16	32708
XS	Eastern Asia, Asia	2.95%	4.87%	31364555	3.65	114492792

<http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=0&w=7&r=1>



CC	Country	DNSSEC Validates	Uses Google PDNS	Samples	Weight	Weighted Samples
SE	Sweden, Northern Europe, Europe	76.55%	7.53%	1030914	1.19	1222901
SI	Slovenia, Southern Europe, Europe	63.64%	7.29%	1653579	0.12	197884
FO	Faroe Islands, Northern Europe, Europe	61.96%	6.30%	50584	0.11	5710
EE	Estonia, Northern Europe, Europe	53.51%	4.35%	567113	0.24	138094
DK	Denmark, Northern Europe, Europe	53.16%	6.32%	613566	1.15	706658
CZ	Czech Republic, Eastern Europe, Europe	41.75%	21.22%	1363396	0.75	1028394
LU	Luxembourg, Western Europe, Europe	41.64%	7.50%	146436	0.48	70349
RO	Romania, Eastern Europe, Europe	41.55%	14.71%	5937596	0.21	1276158
EU	European Union, Western Europe, Europe	34.88%	40.42%	72509	0	0
IS	Iceland, Northern Europe, Europe	34.18%	6.24%	223543	0.19	41929
JE	Jersey, Northern Europe, Europe	33.15%	24.45%	12707	0.48	6117
PL	Poland, Eastern Europe, Europe	30.85%	12.26%	3419138	0.97	3302789
LI	Liechtenstein, Western Europe, Europe	29.13%	9.21%	9457	0.49	4642
MK	The former Yugoslav Republic of Macedonia, Southern Europe, Europe	28.06%	12.50%	2091935	0.07	155438
MT	Malta, Southern Europe, Europe	27.85%	6.83%	515340	0.07	37992
NO	Norway, Northern Europe, Europe	27.31%	5.42%	506050	1.29	653832
FR	France, Western Europe, Europe	25.93%	6.01%	7475918	0.95	7069016
RS	Serbia, Southern Europe, Europe	25.28%	10.71%	12543841	0.05	663155
BA	Bosnia and Herzegovina, Southern Europe, Europe	23.45%	9.35%	6777137	0.05	340306
BY	Belarus, Eastern Europe, Europe	21.88%	7.74%	901929	0.75	677089
IE	Ireland, Northern Europe, Europe	19.52%	6.16%	764625	0.63	483960
AD	Andorra, Southern Europe, Europe	19.38%	8.93%	87017	0.1	8661
GR	Greece, Southern Europe, Europe	18.57%	3.27%	3824140	0.23	862813
IM	Isle of Man, Northern Europe, Europe	16.17%	16.17%	371	14.17	5256
UA	Ukraine, Eastern Europe, Europe	16.05%	18.51%	4495731	0.55	2462734
VA	Holy See, Southern Europe, Europe	14.83%	19.78%	627	0.1	59
RU	Russian Federation, Eastern Europe, Europe	14.79%	11.56%	7678230	1.51	11592711
DE	Germany, Western Europe, Europe	14.68%	8.12%	1768237	5.18	9154185

<http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=0&w=7&r=1>

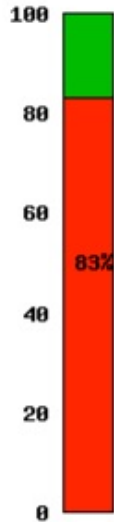
# DNSSEC Deployment Report

Tue Oct 20 00:28:05 UTC 2015

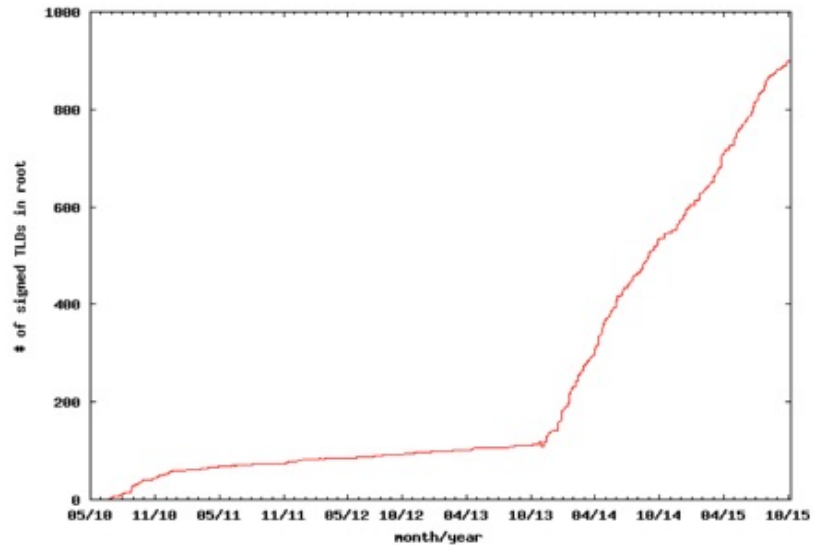
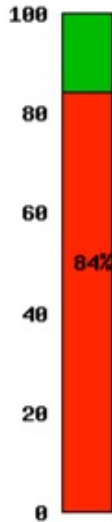
Total TLDs: 1080 / Signed TLDs in root: 909 / Recently added: aramco.  
xn--mgb3a3ejt. (10/15/2015)

Trend

% of TLDs  
signed in root










% of TLDs  
signed



<https://rick.eng.br/dnssecstat/>



TLD		Description	DS Date	% Signed	Signed/Total
<a href="#">nl.</a>		SIDN (Stichting Internet Domeinregistratie Nederland)	11-NOV-2010	43.95	2464494/5607305
<a href="#">br.</a>		Comite Gestor da Internet no Brasil	23-JUN-2010	22.25	830546/3733607
<a href="#">se.</a>		The Internet Infrastructure Foundation	27-AUG-2010	46.46	586298/1262057
<a href="#">com.</a>		VeriSign Global Registry Services	31-MAR-2011	0.45	533712/119659915
<a href="#">cz.</a>		CZ.NIC, z.s.p.o	24-JUN-2010	61.61	464766/754333
<a href="#">net.</a>		VeriSign Global Registry Services	9-DEC-2010	0.64	95045/14942386
<a href="#">org.</a>		Public Interest Registry (PIR)	22-JUL-2010	0.51	54417/10569221
<a href="#">biz.</a>		Neustar, Inc.	7-AUG-2010	0.77	16319/2133121
<a href="#">info.</a>		Afilias Limited	4-SEP-2010	0.31	15550/5092713
<a href="#">ovh.</a>		OVH SAS	19-JUN-2014	47.08	13868/29456
<a href="#">amsterdam.</a>		Gemeente Amsterdam	25-DEC-2014	28.48	6066/21300
<a href="#">frl.</a>		FRLregistry B.V.	31-AUG-2014	36.69	4013/10938
<a href="#">paris.</a>		City of Paris	19-APR-2014	15.50	3243/20923
<a href="#">bank.</a>		fTLD Registry Services, LLC	9-JAN-2015	100.00	2527/2527
<a href="#">xyz.</a>		XYZ.COM LLC	19-FEB-2014	0.19	1881/983102
<a href="#">webcam.</a>		dot Webcam Limited	20-MAR-2014	2.62	1714/65406
<a href="#">name.</a>		VeriSign Information Services, Inc.	24-JAN-2014	0.82	1381/169283

Note: Only includes the TLDs for which Rick Lamb can get statistics. (Example, .GOV is not listed.)

<https://rick.eng.br/dnssecstat/>

# TLD DNSSEC Implementation Status

**Experimental – internal experiments**

**Announced – Public commitment to deploy**

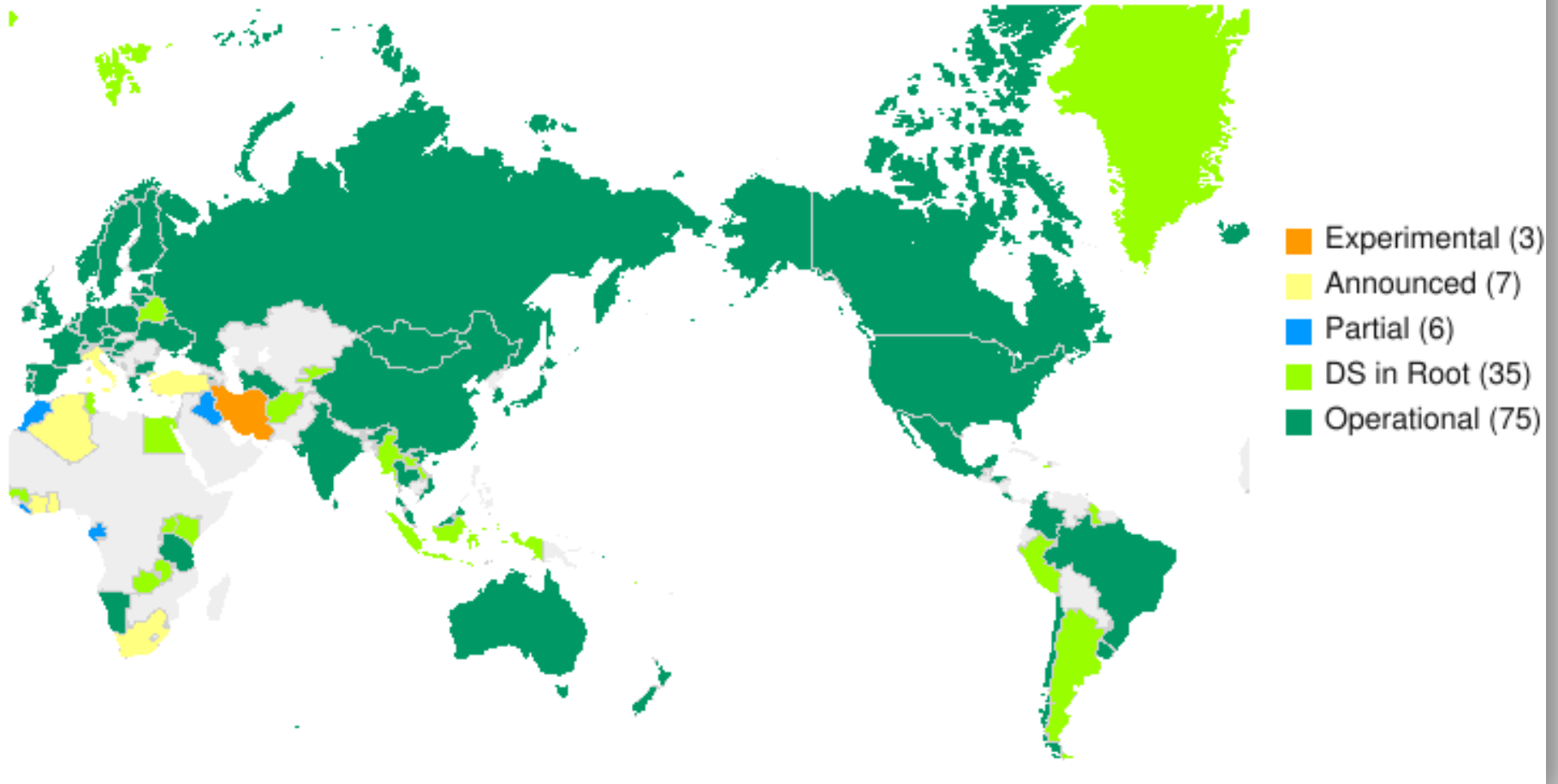
**Partial – Zone is signed but not in operation**

**DS in Root**

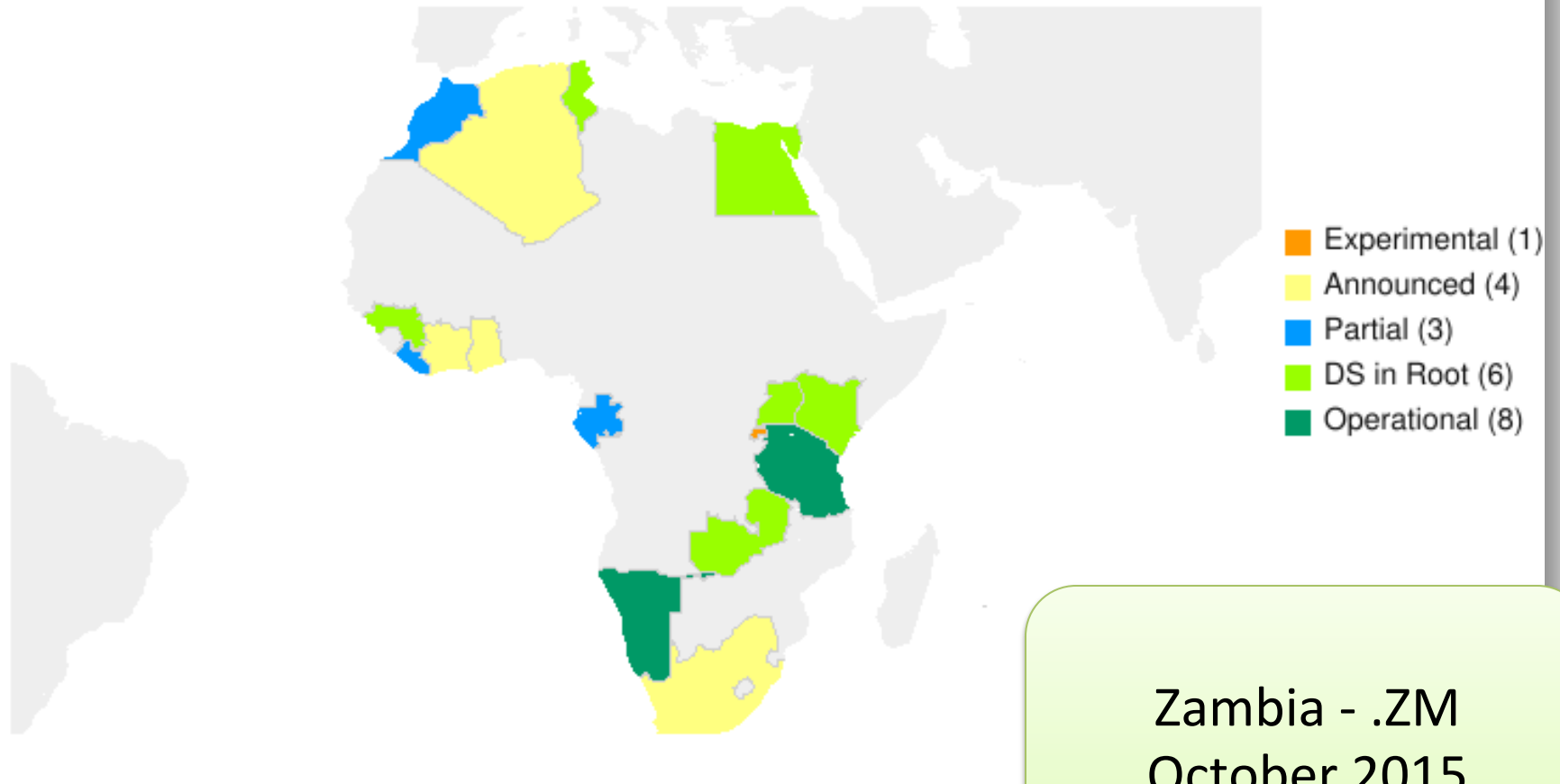
**Operational – Accepting signed delegations**



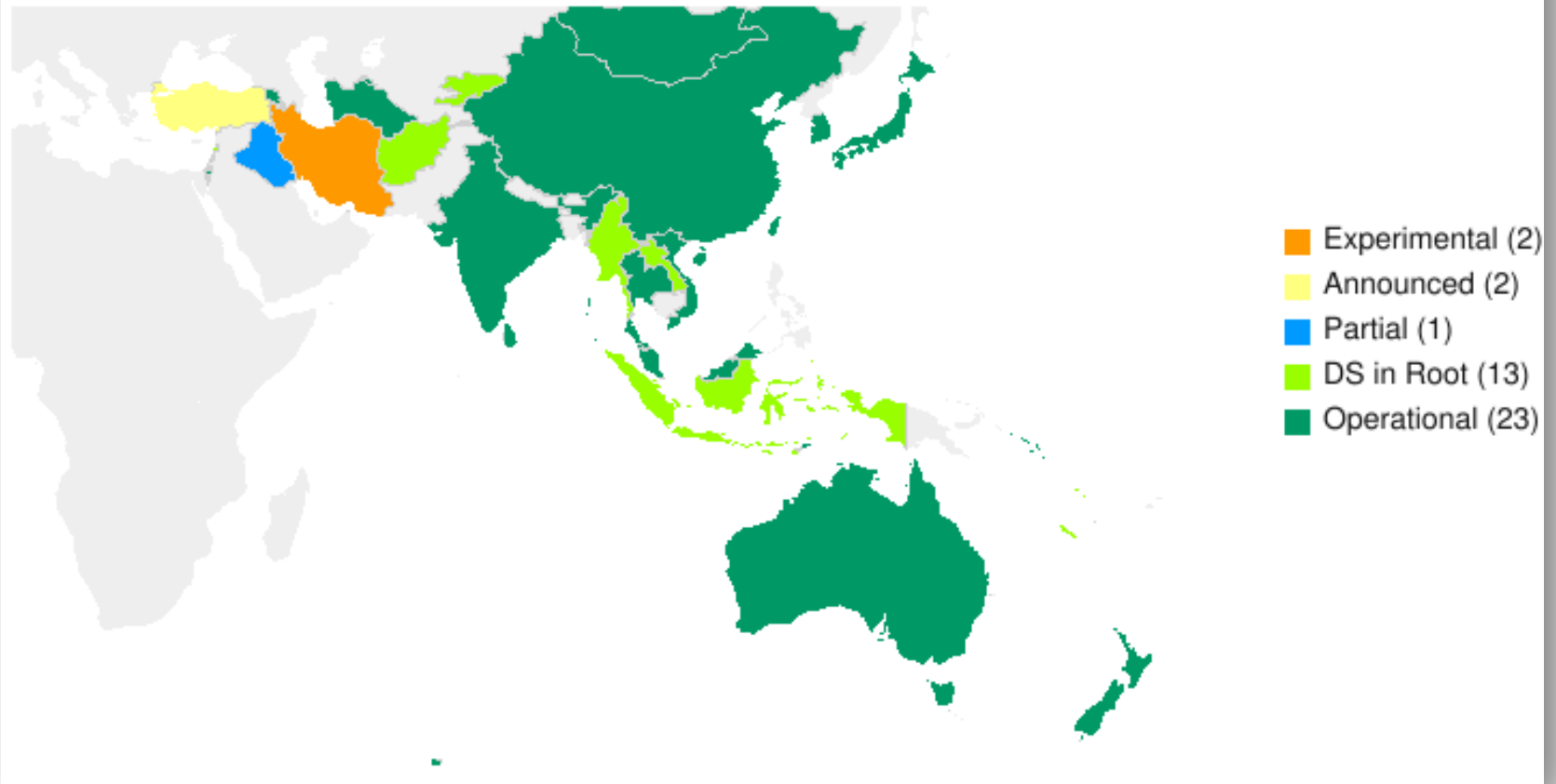
# ccTLD DNSSEC Status on 2015-10-19



## AF ccTLD DNSSEC Status on 2015-10-19

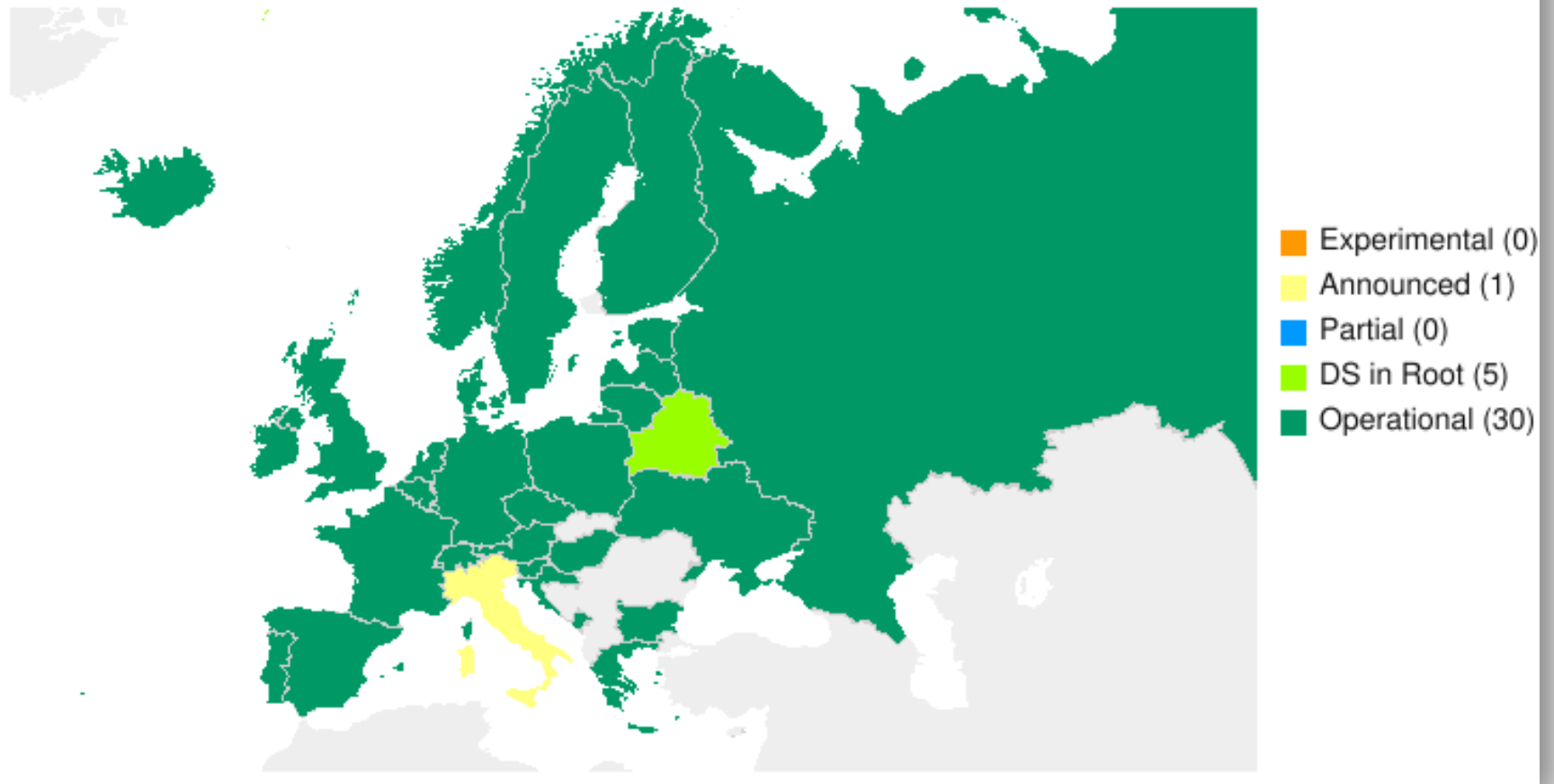


## AP ccTLD DNSSEC Status on 2015-10-19

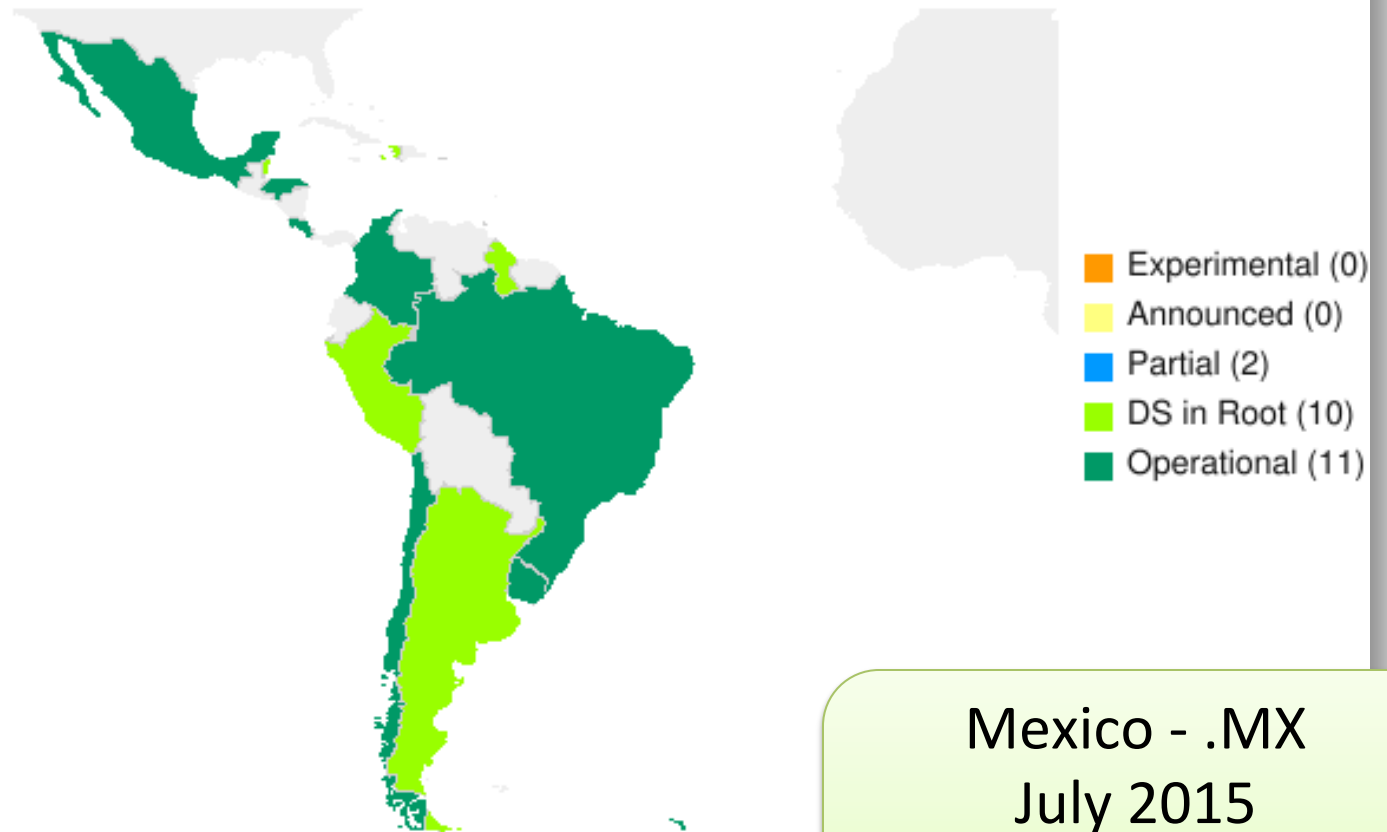




## EUR ccTLD DNSSEC Status on 2015-10-19

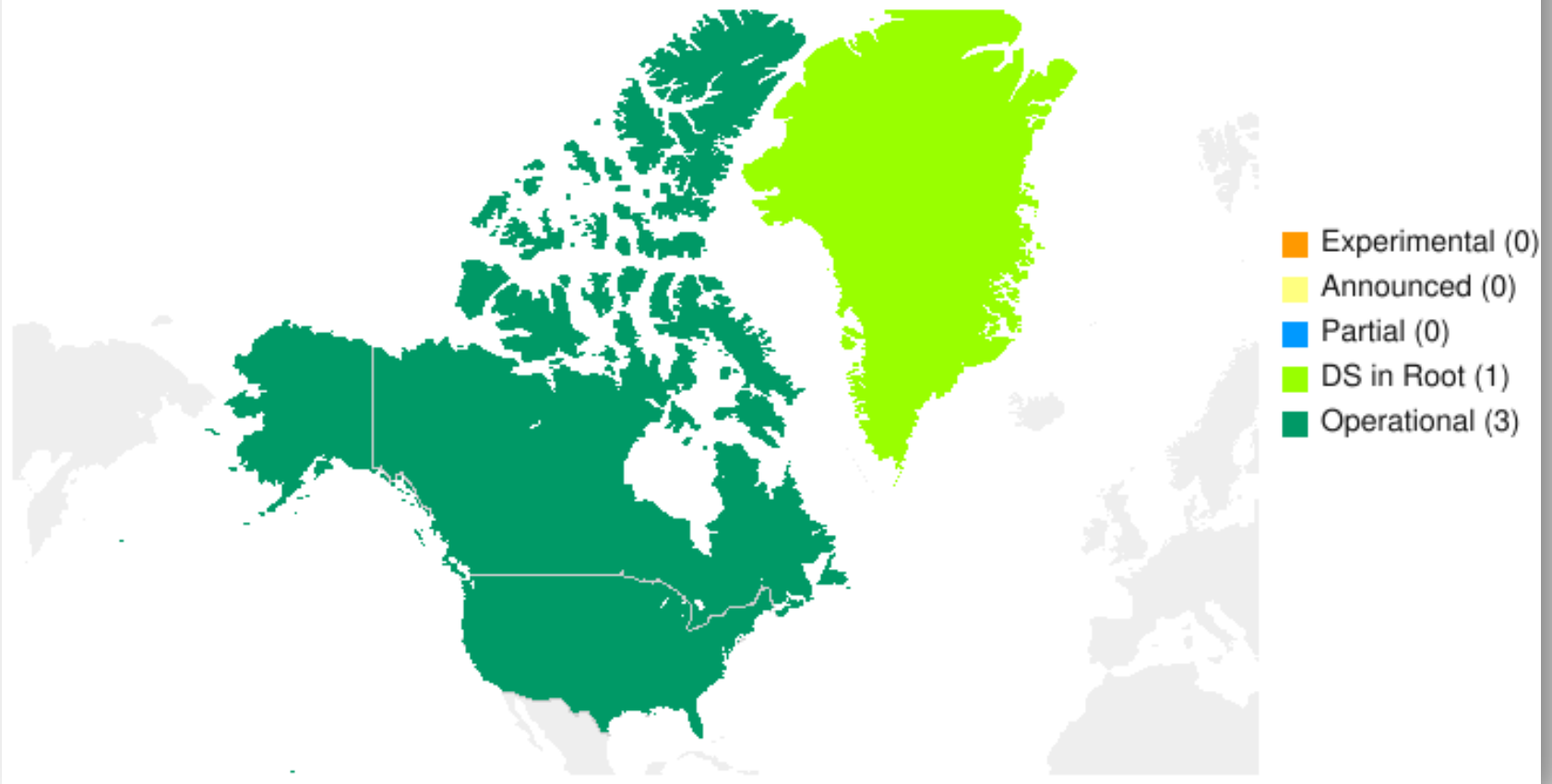


## LAC ccTLD DNSSEC Status on 2015-10-19



Mexico - .MX  
July 2015  
Uruguay - .UY  
August 2015

# NA ccTLD DNSSEC Status on 2015-10-19



# Receiving the DNSSEC Deployment Maps

The DNSSEC Deployment Maps are now published via email every Monday morning through the Internet Society Deploy360 Programme. To subscribe, visit:

[www.internetsociety.org/deploy360/dnssec/maps/](http://www.internetsociety.org/deploy360/dnssec/maps/)

# DNSSEC Event Calendar

New calendar to track DNSSEC/DANE-related events. Two views – event listing:

**<https://www.dnssec-deployment.org/events/>**

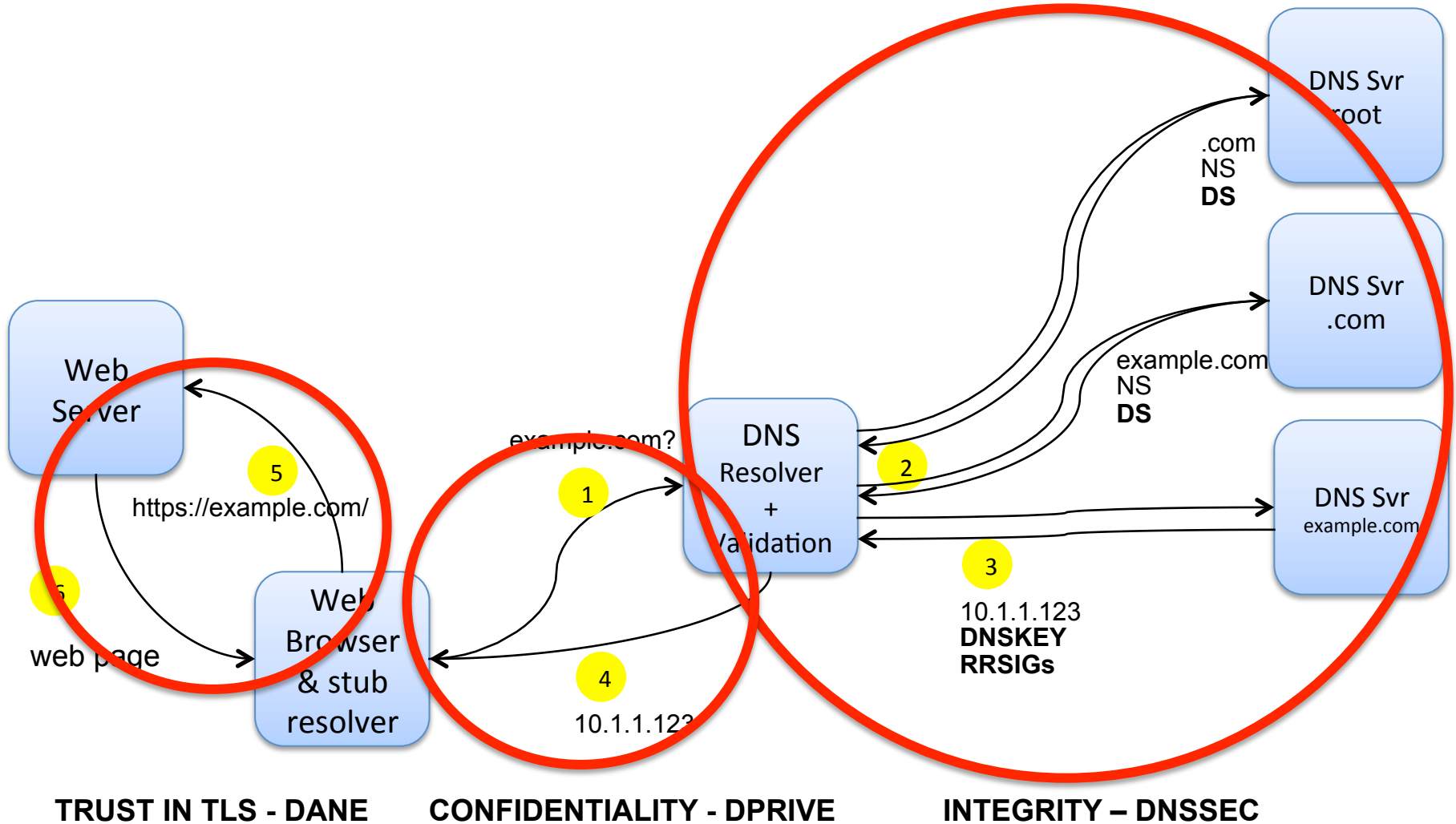
Calendar view:

**<http://www.dnssec-deployment.org/calendar/>**

Send event submissions to [york@isoc.org](mailto:york@isoc.org)



# IETF 93 Hackathon – Project Summary



- **Visual interface to show what DNSSEC algorithms are supported by a DNS resolver**
- **Tool to test for DNSSEC roadblocks**
  - draft-ietf-dnsop-dnssec-roadblock-avoidance
- **Prototype web server implementation – TLS extension to deliver DNSSEC authentication chain to client**
  - draft-shore-tls-dnssec-chain-extension
- **DNS confidentiality/privacy (DPRIVE)**
  - Fixed opportunistic TLS in both getdns and Unbound to be strict authenticated TLS
    1. Added functionality to getdns API to authenticate TLS server.
    2. Patched Unbound server: forward-secret key exchange; enabled sending full TLS certificate chain in handshake
- **JSON interface to IANA registry of DNSSEC algorithms**

# IETF 93 Hackathon - Public releases

- Visual interface to check DNSSEC algorithms
  - [https://github.com/ogud/DNSSEC\\_ALG\\_Check](https://github.com/ogud/DNSSEC_ALG_Check)
  - <https://github.com/getdnsapi/IETF93HackathonNode>
- Tool to test for DNSSEC roadblock avoidance
  - <https://www.ietf.org/registration/MeetingWiki/wiki/dnsresolvercapabilities>
  - <https://getdnsapi.net/roadblock.php>
  - <https://github.com/getdnsapi/IETF93HackathonPHP>
- DNS confidentiality/privacy - TLS
  - Patches going into next release of getdns API
  - Patch available for Unbound
- JSON interface to IANA registry of DNSSEC algorithms
  - <https://github.com/danyork/dnssec-algs-json>

# IETF 94 Hackathon

Sat/Sun, Oct 31 / Nov 1, 2015 – Yokohama –  
IETF 94

- <https://www.ietf.org/hackathon/94-hackathon.html>
- <https://www.ietf.org/registration/MeetingWiki/wiki/94hackathon>
- Opportunity to work on new tools or services for DNSSEC / DANE / DNS Privacy
- Join us!

# IETF 94 Hackathon

Sat/Sun, Oct 31 / Nov 1, 2015 – Yokohama –  
IETF 94

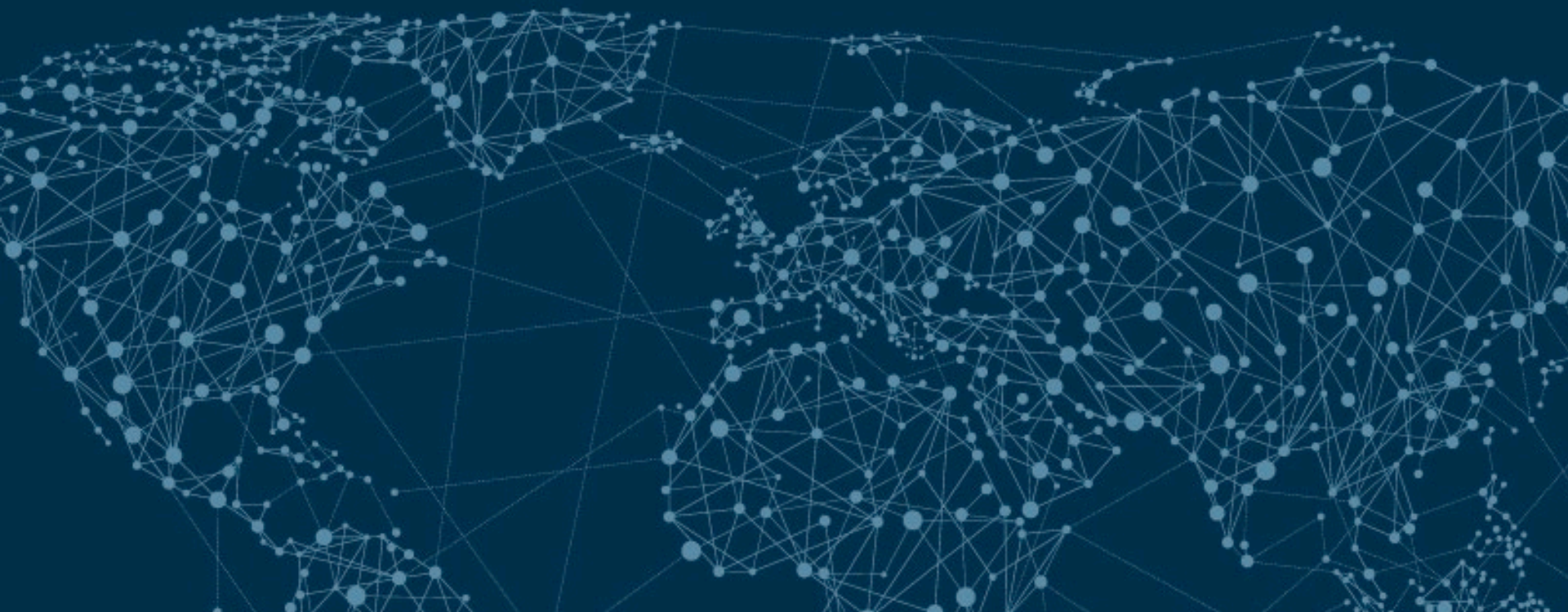
- <https://www.ietf.org/hackathon/94-hackathon.html>
- <https://www.ietf.org/registration/MeetingWiki/wiki/94hackathon>
- Opportunity to work on new tools or services for DNSSEC / DANE / DNS Privacy
- Join us!

# DNSSEC History Project

The DNSSEC History Project is an ongoing project to collect and record the history of the work that went into bringing about the deployment of DNSSEC. To view – or to contribute – please see:

[https://wiki.tools.isoc.org/DNSSEC\\_History\\_Project](https://wiki.tools.isoc.org/DNSSEC_History_Project)





# Thank you and Questions

Dan York, Internet Society | ICANN 54 | October 2015