



DNSSEC and Security Workshop
ICANN75 | 21 September 2022



DNSSEC and Security Hybrid Workshop

ICANN75

Jacques Latour, CIRA

21 September 2022



Program Committee

- Steve Crocker, Shinkuro
- Mark Elkins, DNS/ZACR
- Jacques Latour, CIRA
- Russ Mundy, Parsons
- Ondřej Filip, CZNIC
- Yoshiro Yoneya, JPRS
- Fred Baker, ISC
- Dan York, Internet Society
- Andrew McConachie and Kathy Schnitt, ICANN Org

Support

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**



Agenda

DNSSEC and Security Workshop – Part 1 13:15 – 14:30 MYT (05:15– 06:30 UTC)

1. 13:15 – 13:30 (05:15 – 05:30 UTC) – Jacques Latour, CIRA: Deployment Around the World – Counts, Counts, Counts

Moderator:

2.0 13:15 – 13:35 (05:55 – 05:35 UTC) – Jacques Latour, CIRA: Digital Identity

2.1 13:35 – 13:55 (05:35 – 05:55 UTC) – Viktor Dukhovni, NEED TITLE

2.2 13:55 – 14:15 (05:55 – 06:15) – Peter Thomassen, deSec/SSE: CDS Consistency

2.3 14:15 – 14:30 (06:15 – 06:30) – Q&A

DNSSEC and Security Workshop – Part 2 15:00 – 16:00 MYT (07:00 – 08:00 UTC)

3. Steve Crocker and Shumon Huque: DNSSEC Provisioning Automation

3.1 Steve Crocker, Shinkuro, Inc.: Overview: DNSSEC Provisioning Automation

3.2 Brian Dickson, GoDaddy: GoDaddy DNSSEC DS

3.3 Peter Thomassen, deSEC/SSE: DS Automation specs

3.4 Johan Stenstam & Roger Murray, Swedish Internet Foundation: MUSIC : Multi-Signer Controller - Status Update

3.5 Jan Včelák, NS1: Multi-signer DNSSEC with NS1 Managed DNS

3.6 Steve Crocker, Shinkuro, Inc.: Multi-Signer Testing: Testbeds and Scenarios

DNSSEC and Security Workshop – Part 3 16:30 – 17:30 MYT (08:30 – 09:30 UTC)

Moderator:

4.0 16:30 – 16:45 (08:30– 08:45 UTC) – Kim Davies, ICANN: KSK Update

4.1 16:45 – 17:15 (08:45– 09:15 UTC) – Adiel Akplogan, ICANN KINDNS

4.2 17:15 – 17:30 (09:15 – 09:30 UTC) – Q&A

DNSSEC, DANE & RPKI Deployments Around the World

ICANN75

Jacques Latour, CIRA

21 September 2022



DNSSEC Validation

Roughly 30 - 32%

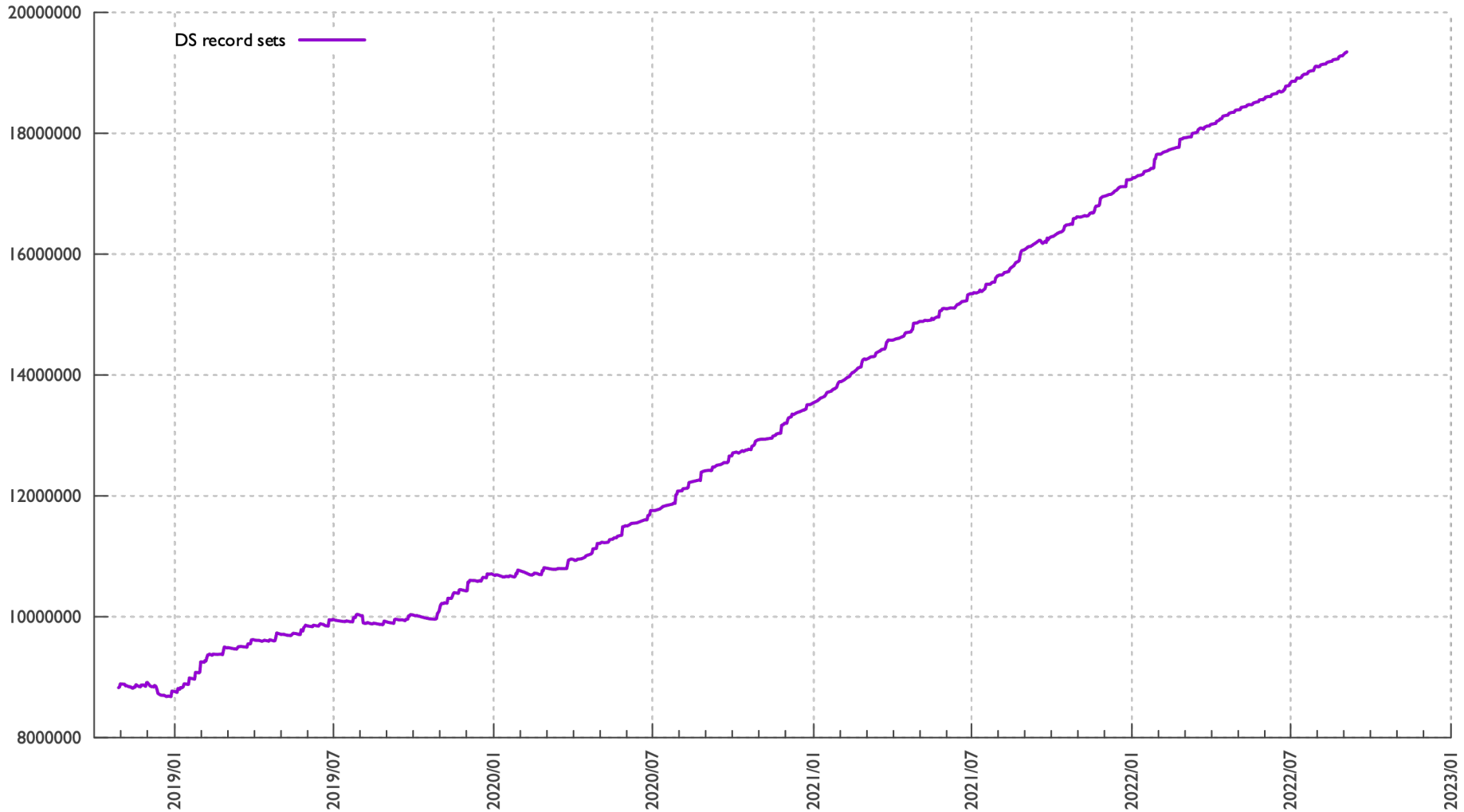


<https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=0&hr=1&w=7>

Code	SubRegion	DNSSEC Validates	Samples	Weight	Weighted Samples
QR	Micronesia, Oceania	74.88%	1,660	0.94	1,560
QS	Polynesia, Oceania	72.88%	1,829	0.76	1,382
QQ	Melanesia, Oceania	62.46%	4,150	1.82	7,540
XT	Southern Asia, Asia	55.42%	4,053,108	0.62	2,521,883
QO	Western Europe, Europe	54.86%	289,345	1.98	573,952
XV	Western Asia, Asia	48.60%	1,056,594	0.67	709,732
XW	Eastern Europe, Europe	45.24%	386,050	2.01	775,516
XI	Middle Africa, Africa	41.63%	56,306	1.66	93,511
XR	Central Asia, Asia	40.02%	113,000	1.28	144,929
XP	South America, Americas	39.27%	1,443,874	0.74	1,075,355
XK	Southern Africa, Africa	38.96%	68,406	1.94	132,516
QM	Northern Europe, Europe	38.61%	693,663	0.5	343,578
QP	Australia and New Zealand, Oceania	38.16%	65,747	1.39	91,118
XQ	Northern America, Americas	34.36%	912,876	1.06	971,346
XJ	Northern Africa, Africa	28.15%	529,119	0.82	436,304
XN	Caribbean, Americas	24.94%	115,238	0.68	78,925
XU	South-Eastern Asia, Asia	23.83%	2,022,780	0.59	1,200,757
XH	Eastern Africa, Africa	23.16%	235,883	1.4	329,111
XL	Western Africa, Africa	22.93%	395,604	1.01	398,455
QN	Southern Europe, Europe	21.27%	485,646	0.8	389,649
XO	Central America, Americas	15.17%	516,053	0.76	392,167
XS	Eastern Asia, Asia	3.81%	698,770	4.97	3,476,110

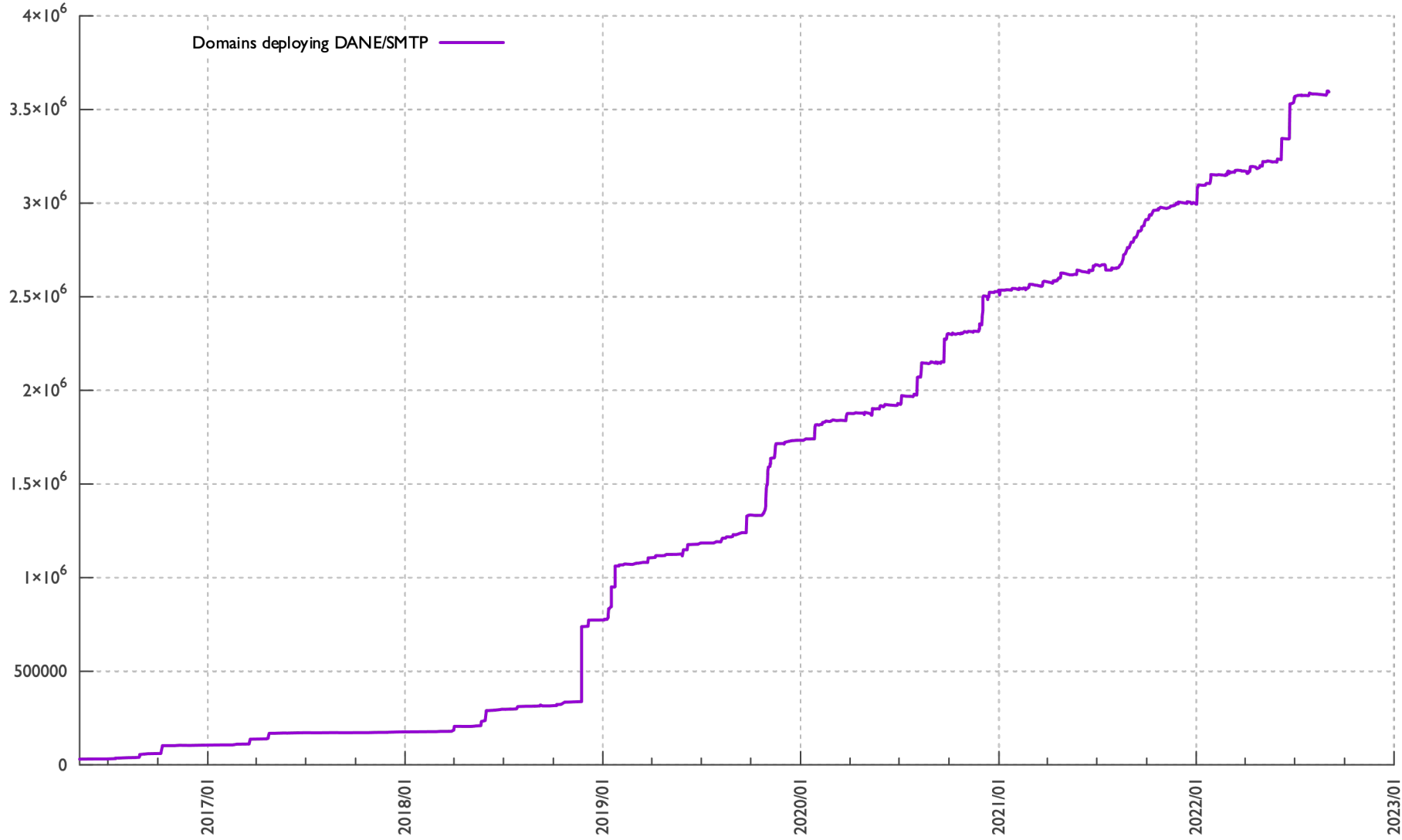
<https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=1&hr=1&w=7&p=0>

Observed DS Record Count Growth



<https://stats.dnssec-tools.org/>

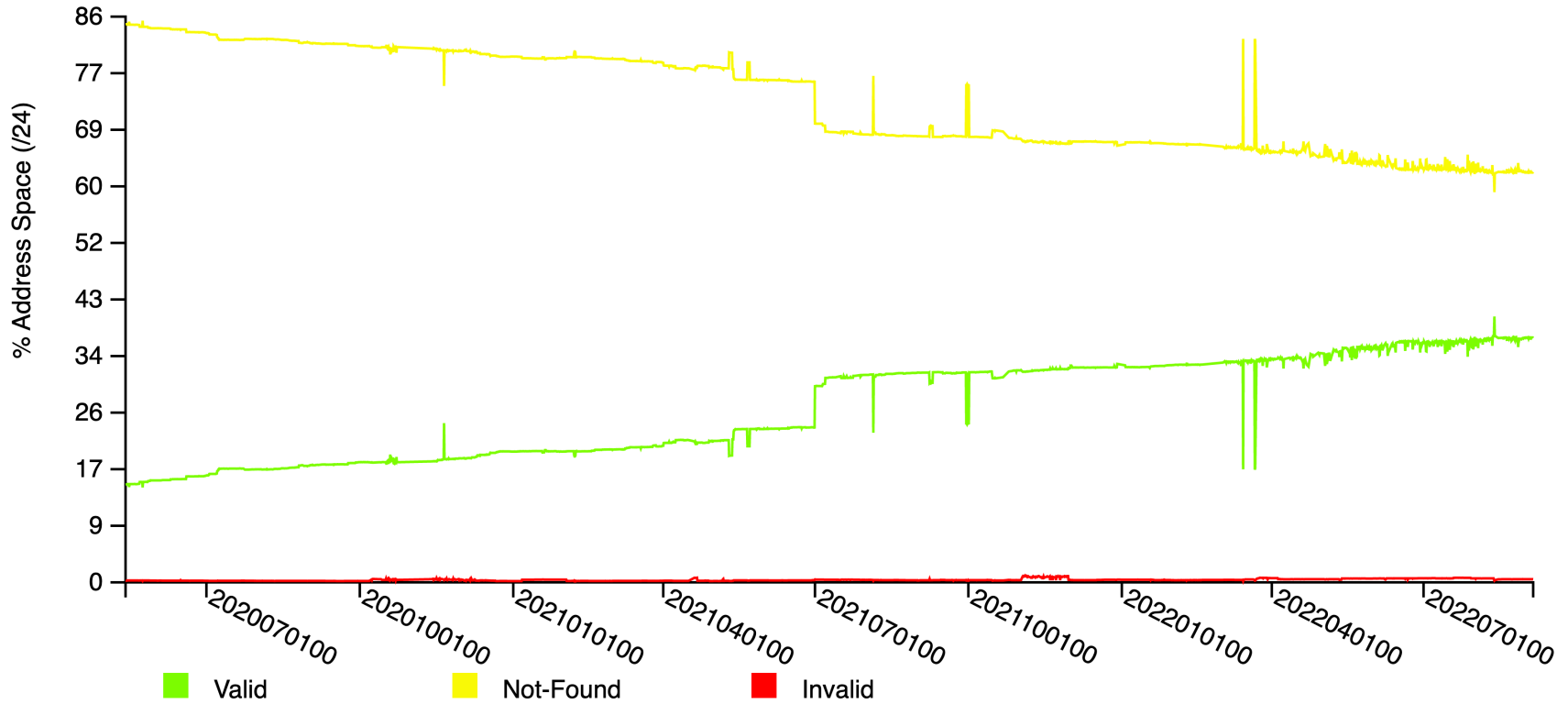
Domains with signed MX and DANE records



<https://stats.dnssec-tools.org/>

RPKI Global IPv4 Prefixes

RPKI-ROV History of Address Space (/24s) in Unique Prefix-Origin Pairs (IPv4)



NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: All

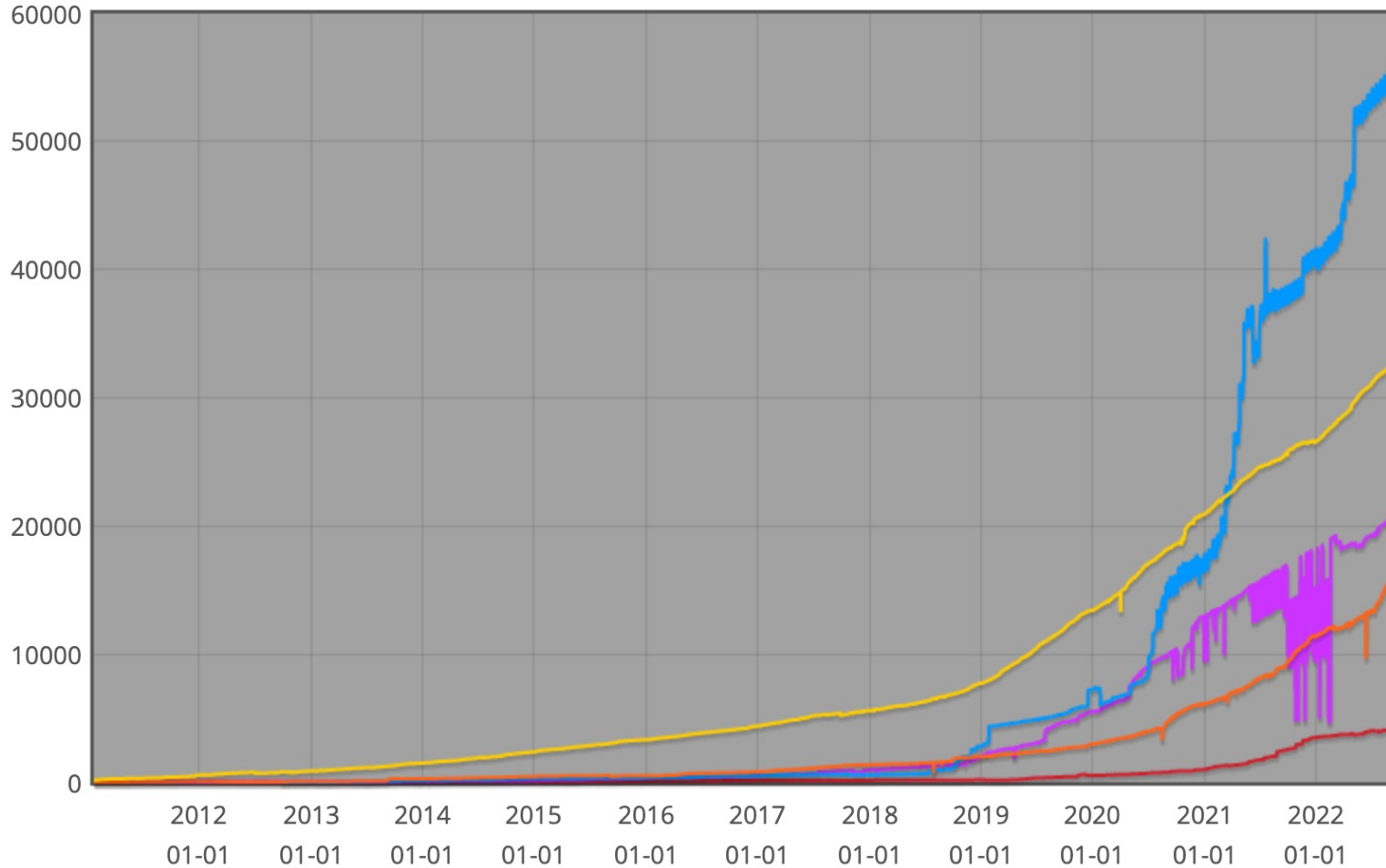
<https://rpki-monitor.antd.nist.gov/>

RPKI Covered IPv4 Prefixes by RIR

Number of ROAs

AfriNIC APNIC ARIN LACNIC RIPE NCC

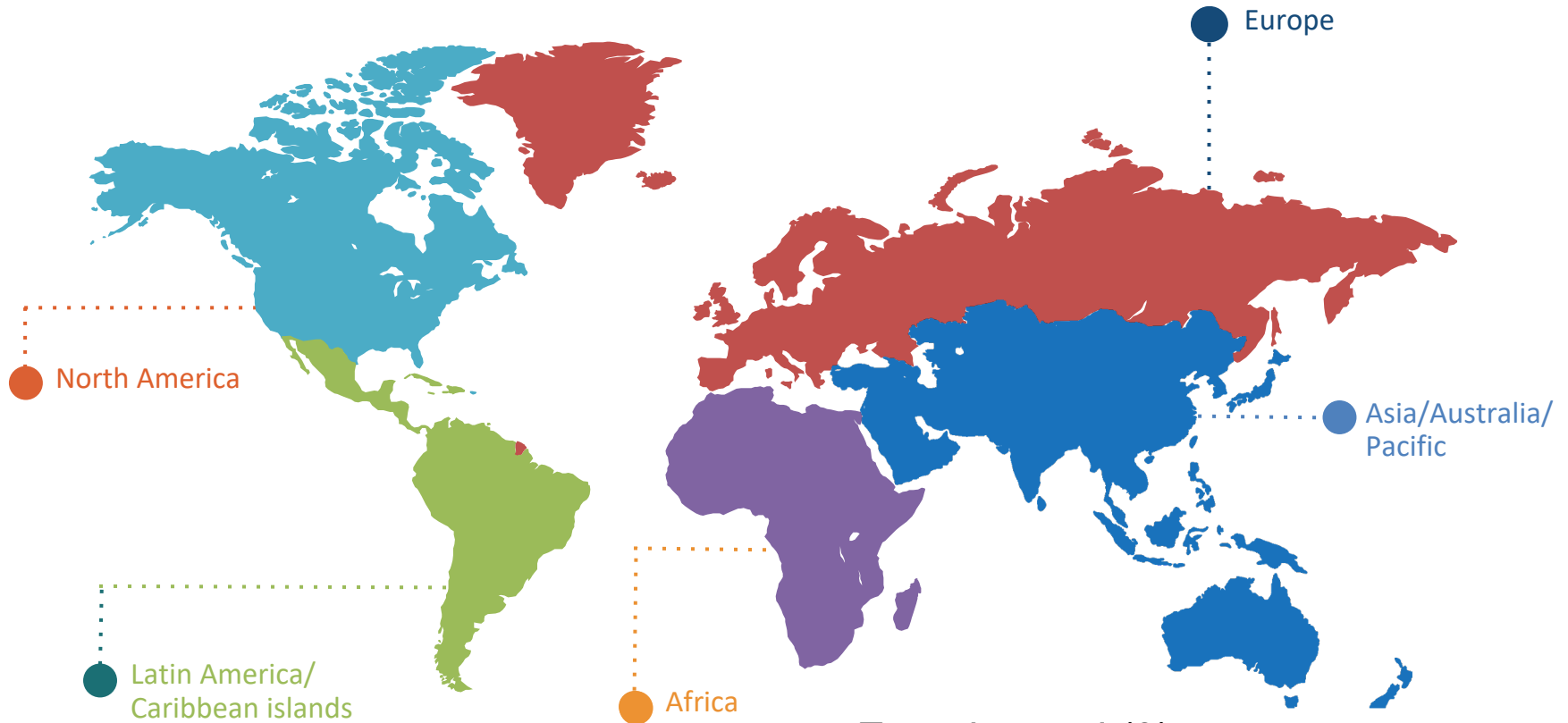
This graph shows the total number of valid Route Origin Authorisation (ROA) objects created by the holders of a certificate



<https://certification-stats.ripe.net/>

ccTLD DNSSEC Deployment Status

ccTLD DNSSEC Status 2022-03-07



Experimental (9)
Announced (4)
Partial (1)
DS in Root (59)
Operational (78)
DS Automation (7)

ccTLDs DNSSEC Operational Status

TLD	Map Region	Status
CH	EUR	DS Automation
CZ	EUR	DS Automation
LI	EUR	DS Automation
SE	EUR	DS Automation
NU	AP	DS Automation
CR	LAC	DS Automation
SK	EUR	DS Automation

DS Automation is a new status for ccTLD that support and implement CDS/CDNSKEY automation

—

more to come on that today 😊

ccTLDs DNSSEC Operational Status

TLD	Map Region	Status
IR	AP	Experimental
UM	AP	Experimental
GB	EUR	Experimental
AI	LAC	Experimental
CI	AF	Experimental
HT	LAC	Experimental
IQ	AP	Experimental
MS	LAC	Experimental
MU	AF	Experimental
TO	AP	Experimental
XN--J1AMH	EUR	Experimental

Excluding the “Operational and DS in Root”

TLD	Map Region	Status
GH	AF	Announced
GA	AF	Partial
PY	LAC	Announced
SD	AF	Announced
TR	AP	Announced
XN--FZC2C9E2C	AP	Partial
XN--LGBBAT1AD8J	AF	Announced
XN--XKC2AL3HYE2A	AP	Partial

If you are listed here and are fully DNSSEC operational, please contact us.

ccTLDs DNSSEC <DS in Root> Status

AD	DZ	LA	SJ	XN--H2BRJ9C
AG	FJ	LB	SN	XN--L1ACC
AR	FM	LC	SY	XN--MGBBH1A71E
AW	FO	LR	TN	XN--MGBX4CD0AB
AX	GD	LY	TV	XN--PGBS0DH
AZ	GG	MA	UG	XN--S9BRJ9C
BH	GI	MC	UZ	XN--WGBH1C
BN	GN	MD	VC	XN--XKC2DL3A5EE0H
BT	GW	MM	VE	
BV	GY	MR	VU	
BW	ID	NC	WS	
BZ	JE	PW	XN--45BRJ9C	
CC	KG	RS	XN--FIQS8S	
CY	KW	RW	XN--FIQZ9S	
DM	KY	SG	XN--FPCRJ9C3D	
			XN--GECRJ9C	

If you are listed here and are fully DNSSEC operational, please contact us.

Questions & Answers

DNSSEC Resources

www.dnssec-tools.org

stats.dnssec-tools.org

stats.labs.apnic.net/dnssec

RPKI Resources

rpki-monitor.antd.nist.gov

certification-stats.ripe.net

www.securerouting.net

Thank You