Measurement of DNSSEC Validation with Edwards Curve Cryptography

Geoff Huston, Joao Damas
APNIC Labs
September 2020

Edwards Curve Cryptography

- Relatively recent crypto offering, first published in 2011
- One of the Elliptic-Curve family of algorithms, using a “twisted Edwards Curve”
- Intended to distinguish itself from other crypto algorithms by being:
  - Faster
  - Unencumbered by lingering IPR disputes
  - High crypto “density”
  - Public domain source code

I’m really not a crypto geek

- So I’ll do a REALLY BRIEF summary of Edwards Curves
- The *normal form* of elliptic curves that Harold Edwards studied in 2007 was:

$$x^2 + y^2 = c^2 + c^2x^2y^2$$

- The *twisted transform* of such curves results from the relationship

$$ax^2 + y^2 = 1 + dx^2y^2$$

- These curves can be used to derive a digital signature algorithm for use in public key cryptography, described in RFC 8032.

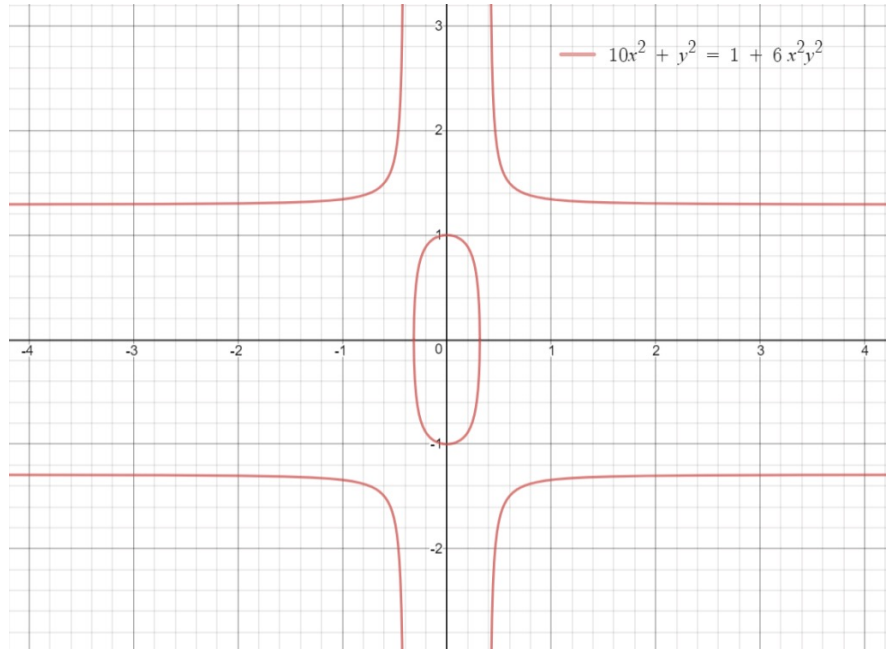
I’m still not a crypto geek

Ed25519 uses an instance of this Edwards Curve curve where:

a = -1 and d = -121665/121666

and is mapped into a prime field p where

$p = 2^{255} – 19$.



This produces the relationship:

$-x^2 + y^2 = 1 – (121665/121666)\, x^2y^2 \pmod{2^{255} – 19}$

Ed25519 crypto protocol

Domain Name System Security (DNSSEC) Algorithm Numbers

Created
2003-11-03
Last Updated
2020-04-14
Available Formats
XML HTML Plain text

Registries included below

- DNS Security Algorithm Numbers
- DNS KEY Record Diffie-Hellman Prime Lengths
- DNS KEY Record Diffie-Hellman Well-Known Prime/Generator Pairs

DNS Security Algorithm Numbers

Registration Procedure(s)
RFC Required
Reference
[RFC4034][RFC3755][RFC6014][RFC6944]
Note
The KEY, SIG, DNSKEY, RRSIG, DS, and CERT RRs use an 8-bit number used to identify the security algorithm being used.

All algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. Only algorithms usable for zone signing may appear in DNSKEY, RRSIG, and DS RRs. Only those usable for SIG(0) and TSIG may appear in SIG and KEY RRs.

* There has been no determination of standardization of the use of this algorithm with Transaction Security.

Available Formats
CSV

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
0	Delete DS	DELETE	N	N	[RFC4034][proposed standard][RFC4398][proposed standard][RFC8078][proposed standard]
1	RSA/MD5 (deprecated, see 5)	RSAMD5	N	Y	[RFC3110][proposed standard][RFC4034][proposed standard]
2	Diffie-Hellman	DH	N	Y	[RFC2539][proposed standard]
3	DSA/SHA1	DSA	Y	Y	[RFC3755][proposed standard][RFC2536][proposed standard][Federal Information Processing Standards Publication (FIPS PUB) 186, Digital Signature Standard, 18 May 1994.][Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard, 17 April 1995. (Supersedes FIPS PUB 180 dated 11 May 1993.)]
4	Reserved				[RFC6725][proposed standard]
5	RSA/SHA-1	RSASHA1	Y	Y	[RFC3110][proposed standard][RFC4034][proposed standard]
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	[RFC5155][proposed standard]
8	RSA/SHA-256	RSASHA256	Y	*	[RFC5702][proposed standard]
9	Reserved				[RFC6725][proposed standard]
10	RSA/SHA-512	RSASHA512	Y	*	[RFC5702][proposed standard]
11	Reserved				[RFC6725][proposed standard]
12	GOST R 34.10-2001	ECC-GOST	Y	*	[RFC5933][proposed standard]
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	Y	*	[RFC6605][proposed standard]
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384	Y	*	[RFC6605][proposed standard]
15	Ed25519	ED25519	Y	*	[RFC8080][proposed standard]
16	Ed448	ED448	Y	*	[RFC8080][proposed standard]
17-122	Unassigned				
123-251	Reserved				[RFC4034][proposed standard][RFC6014][proposed standard]
252	Reserved for Indirect Keys	INDIRECT	N	N	[RFC4034][proposed standard]
253	private algorithm	PRIVATEDNS	Y	Y	[RFC4034][proposed standard]
254	private algorithm OID	PRIVATEOID	Y	Y	[RFC4034][proposed standard]
255	Reserved				[RFC4034][proposed standard]

11	Reserved				[RFC6725][proposed standard]
12	GOST R 34.10-2001	ECC-GOST	Y	*	[RFC5933][proposed standard]
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	Y	*	[RFC6605][proposed standard]
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384	Y	*	[RFC6605][proposed standard]
15	Ed25519	ED25519	Y	*	[RFC8080][proposed standard]
16	Ed448	ED448	Y	*	[RFC8080][proposed standard]

https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

Ed25519 Evaluation

1. Key Size

Algorithm	Private Key	Public Key	Signature Record
Ed25519	**179 bytes**	**300 bytes**	**146 bytes**
ECDSA P-256	187 bytes	353 bytes	146 bytes
RSA-2048	1,776 bytes	620 bytes	403 bytes
RSA-4096	3,312 bytes	967 bytes	744 bytes

Ed25519 Evaluation

2. Key Processing Time

zone with 500K entries, OpenSSL 1.1.1k libraries on a FreeBSD 12.2 host with the DNSSEC toolset supplied with Bind 9.16.16. Validation time is elapsed time for 50K queries with DNSSEC validation

Algorithm	Signing Time	Relative	Validation Time
Unsigned			905 secs
Ed25519	**800 secs**	**1**	**1,008 secs**
ECDSA P-256	450 secs	0.56	1,036 secs
RSA-2048	3,000 secs	3.75	1,173 secs
RSA-4096	3,312 secs	4.14	1,176 secs

Validation Support for Ed25519

We used an ad-based measurement to measure the support for Ed25519

- Control URL – unsigned DNS name
- Positive URL – signed with Ed25519
- Negative URL – bad Ed25519 RRSIG record

What happens when a resolver does not support a signing protocol?

It treats the name as **unsigned** (RFC 4035)

A user is recorded as **supporting** Ed25519

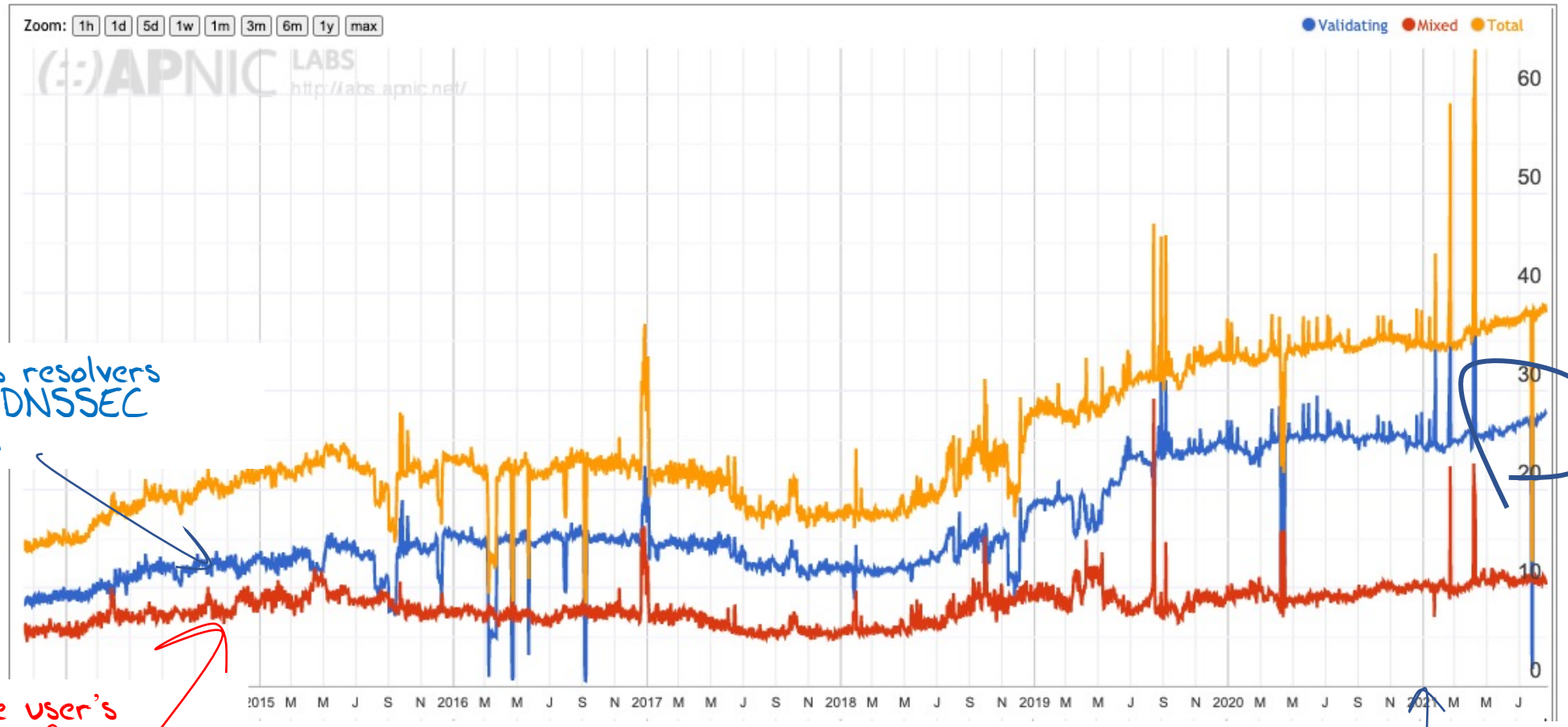
- We observe A/AAAA queries for both DNS names
- We observe DNSKEY and DS queries for both DNS names
- We observe a web fetch for the **valid** URI and no web fetch for the **invalid** URI

- The inference of the invalid condition is that all the recursive resolvers need to support ED25519 for the test to record a positive result

A user is recorded as NOT supporting Ed25519

- We observe A/AAAA queries for both DNS names
- If we observe DNSKEY and DS queries for both DNS names then we call this “**mixed**” support
- We observe a web fetch for the **valid** URI and a web fetch for the **invalid** URI

What is a DNSSEC validation “baseline”?



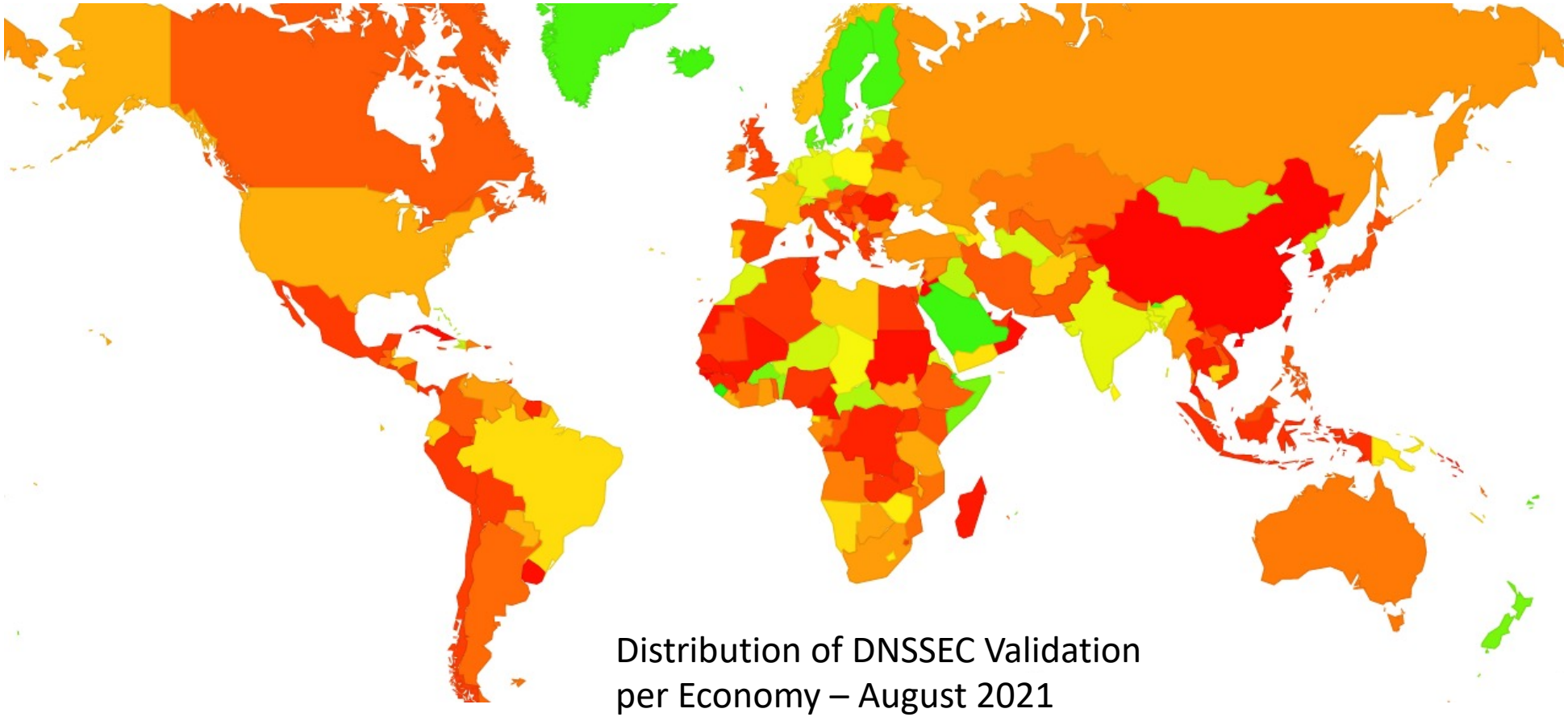
All user's resolvers perform DNSSEC validation

Only some user's resolvers perform DNSSEC validation

Test case uses RSA signatures

Test case uses ECDSA-P256 signatures

What is a DNSSEC validation “baseline”?



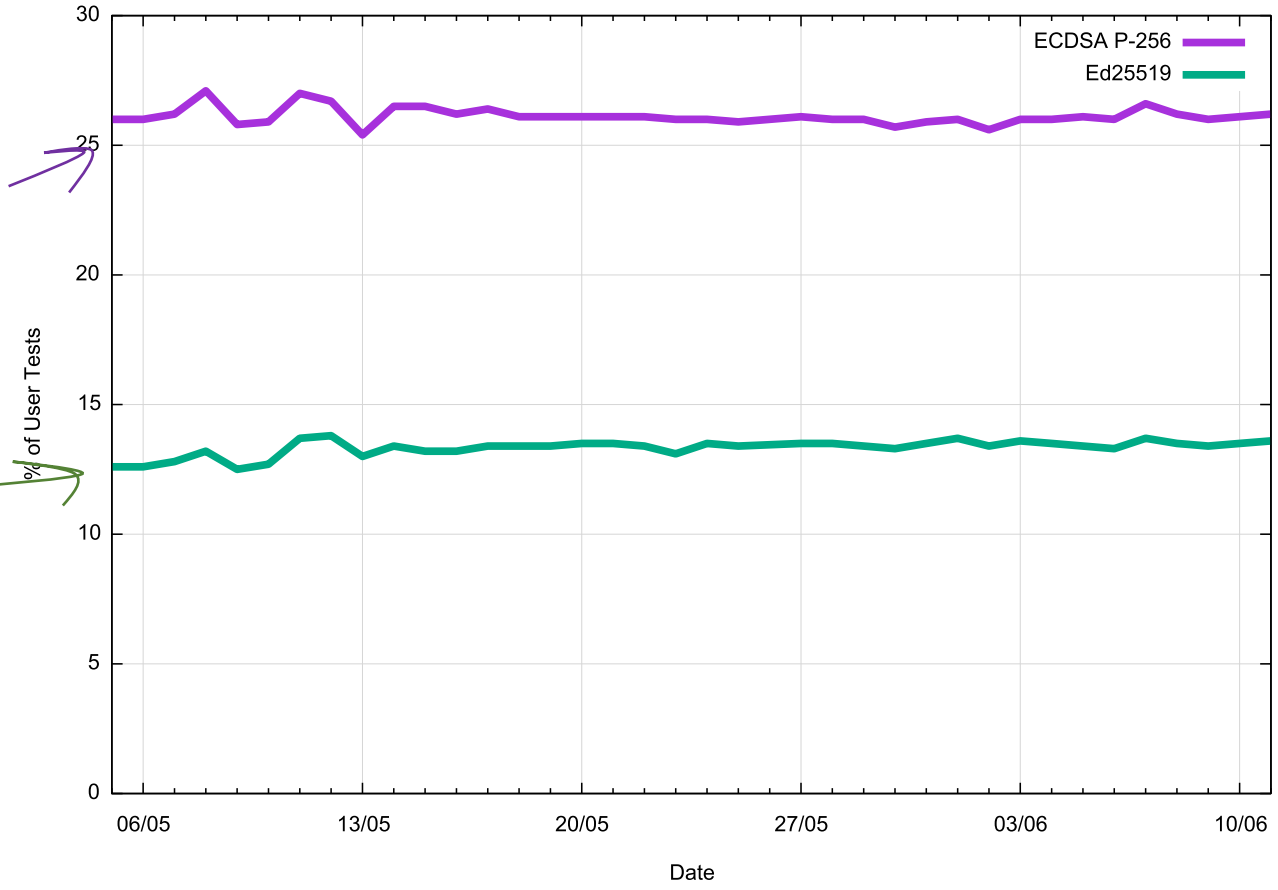
Distribution of DNSSEC Validation
per Economy – August 2021

ECDSA P-256 vs Ed25519

Measurement conducted in May 2021

% users who use ECDSA P-256-aware validating resolvers

% users who use Ed25519-aware validating resolvers

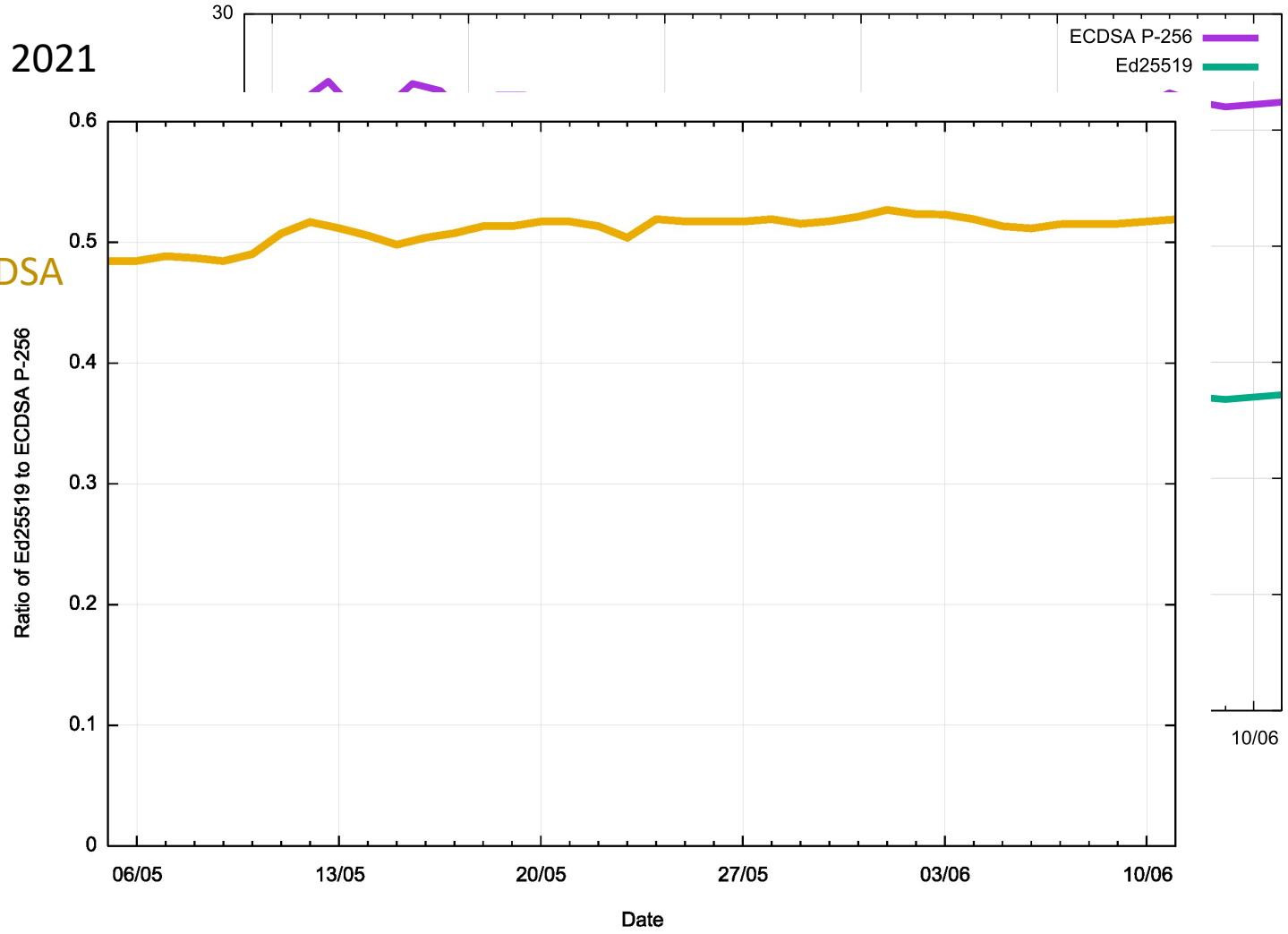


ECDSA P-256 vs Ed25519

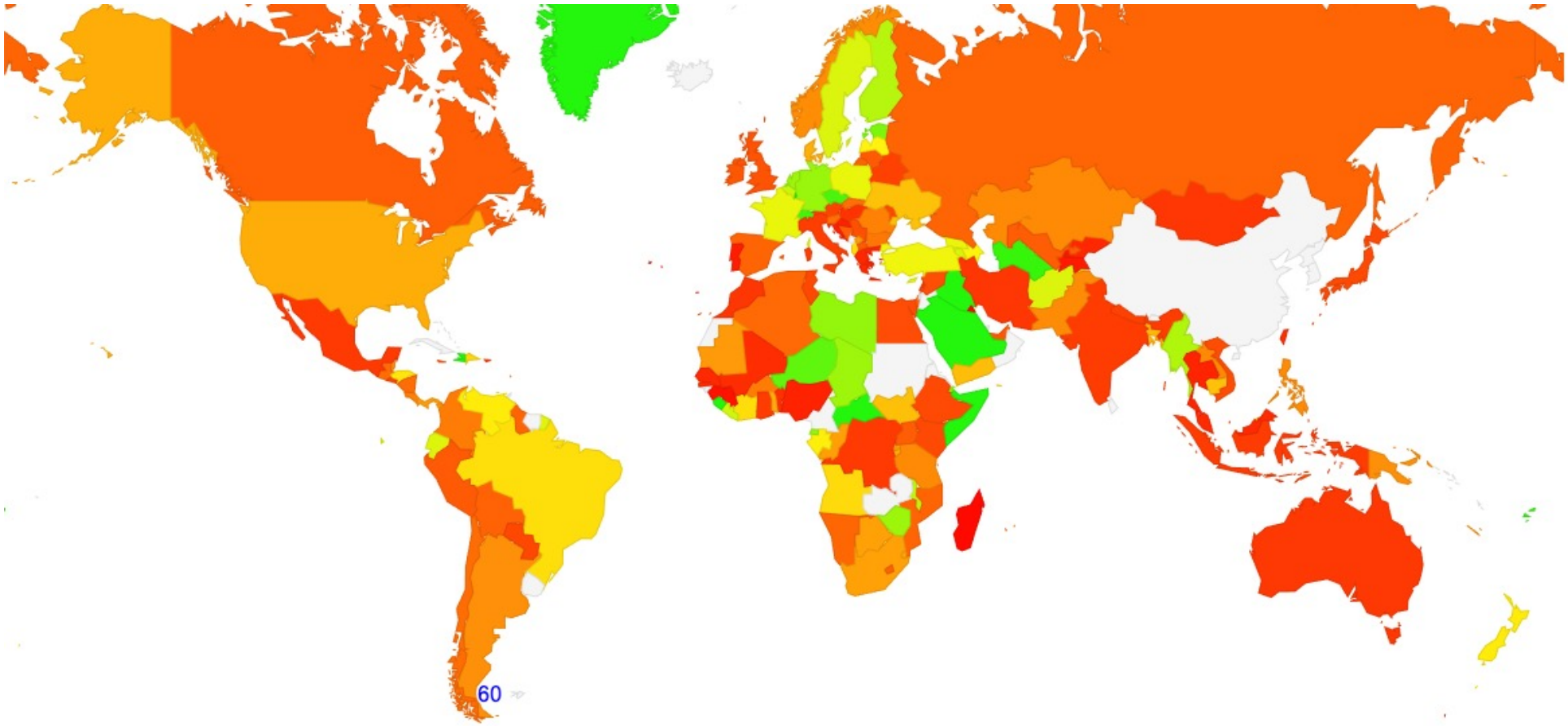
Measurement conducted in May 2021

Ratio of Ed25519 : ECDSA

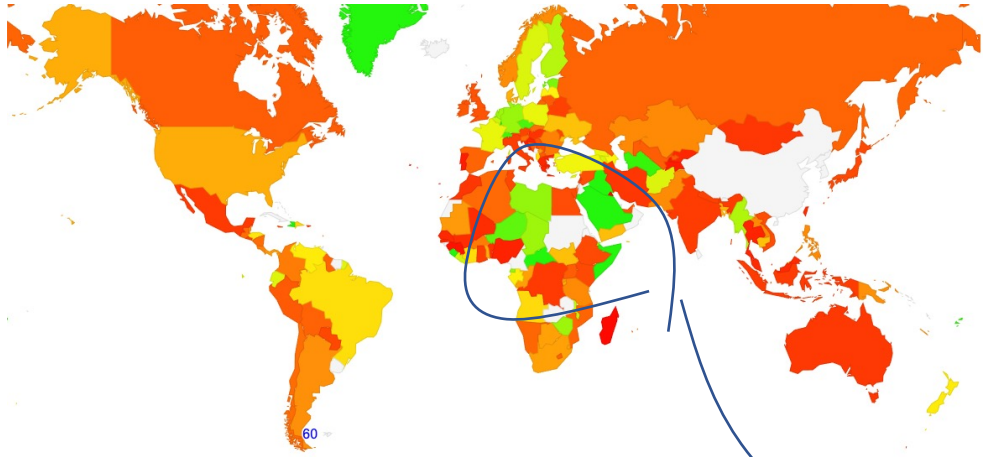
Only 50% of users who use ECDSA-aware validating resolvers are also capable of validating Ed25519 sigs



Where?

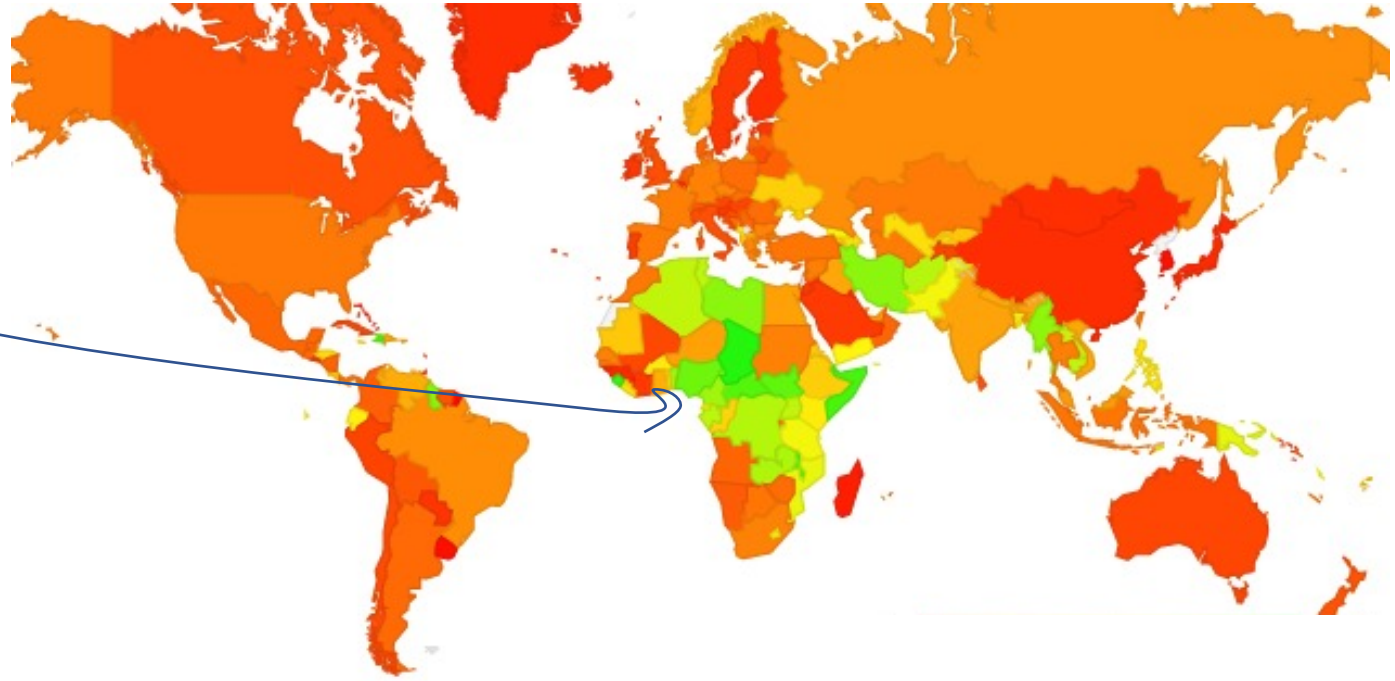


Is this due to Google's 8.8.8.8 Service?



Support for Ed25519

Uses 8.8.8.8



There is a reasonable correlation in Africa, but less so elsewhere

ISP View

List of the “largest” ISPs whose resolvers support ECDSA, but do not support Ed25519 for DNSSEC validation

AS	CC	Count	ECDSA	Ratio	Ed25519	Ratio	AS Name
55836	IN	22998060	21848577	0.95	899647	0.04	Reliance Jio, India
7922	US	4070748	3975062	0.98	251901	0.06	COMCAST, USA
36903	MA	2070044	1677701	0.81	148415	0.07	MT-MPLS, Morocco
36992	EG	885949	393591	0.44	64321	0.07	ETISALAT-MISR, Egypt
45245	BD	851055	670971	0.79	22466	0.03	BANGLALINK, Bangladesh
4818	MY	657060	610952	0.93	9234	0.01	DIGIIX, Malaysia
3243	PT	614634	605322	0.98	11220	0.02	MEO-RESIDENCIAL, Portugal
30689	JM	604787	370476	0.61	48738	0.08	FLOW-NET, Jamacia
45727	ID	599026	281679	0.47	27017	0.05	Hutchison, Indonesia
35819	SA	524105	471071	0.90	13819	0.03	Etihad Etisalat, Saudi Arabia
25144	BA	416270	174427	0.42	38926	0.09	TELEKOM-SRPSKE, Bosnia
43766	SA	330041	309512	0.94	10440	0.03	MTC-KSA, Saudi Arabia
8359	RU	281142	273762	0.97	4561	0.02	MTS, Russia
23889	MU	272176	267050	0.98	7127	0.03	Mauritius Telecom, Mauritius
17882	MN	255505	203365	0.80	24229	0.09	MCS, Mongolia
1241	GR	225024	221091	0.98	6626	0.03	Forthnet, Greece
26615	BR	194565	92371	0.47	18433	0.09	TIM, Brazil
37133	TZ	185453	182966	0.99	1529	0.01	AIRTEL, Tanzania
47589	KW	179303	152935	0.85	1207	0.01	KTC, Kuwait
4804	AU	154869	123355	0.80	2380	0.02	Microplex, Australia
6871	GB	133194	112411	0.84	3941	0.03	PLUSNET, UK
9231	HK	114751	89091	0.78	846	0.01	China Mobile Hong Kong, Hong
39603	PL	114310	112859	0.99	1380	0.01	P4NET, Poland
15146	BS	111989	108602	0.97	2871	0.03	CABLEBAHAMAS, Bahamas
37424	BJ	110672	107193	0.97	933	0.01	Spacetel, Benin
12083	US	110585	106278	0.96	10258	0.09	WOW-INTERNET, USA
34058	UA	109748	108367	0.99	1530	0.01	LIFECELL, Ukraine
44143	RS	102026	100691	0.99	1178	0.01	A1SERBIA, Serbia
16086	FI	99675	98390	0.99	1233	0.01	DNA, Finland
29244	BG	97964	96725	0.99	286	0.00	TELENORBG, Bulgaria

Is Ed25519 viable for DNSSEC?

No, not today

It has smaller keys and signatures than RSA-2048
It is the same size as ECDSA
It is a lot faster to sign a zone than RSA-2048 but a lot slower than ECDSA (2x)
It is (a little) faster to validate than ECDSA and RSA

But…

It is really not adequately supported by DNSSEC-validating resolvers deployed today

Questions?