On the Adoption of the Elliptic Curve Digital Signature Algorithm (ECDSA) in DNSSEC

Roland van Rijswijk-Deij★,☆
r.m.vanrijswijk@utwente.nl

Mattijs Jonker★
m.jonker@utwente.nl

Anna Sperotto★
a.sperotto@utwente.nl

★ Design and Analysis of Communication Systems (DACS), Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands

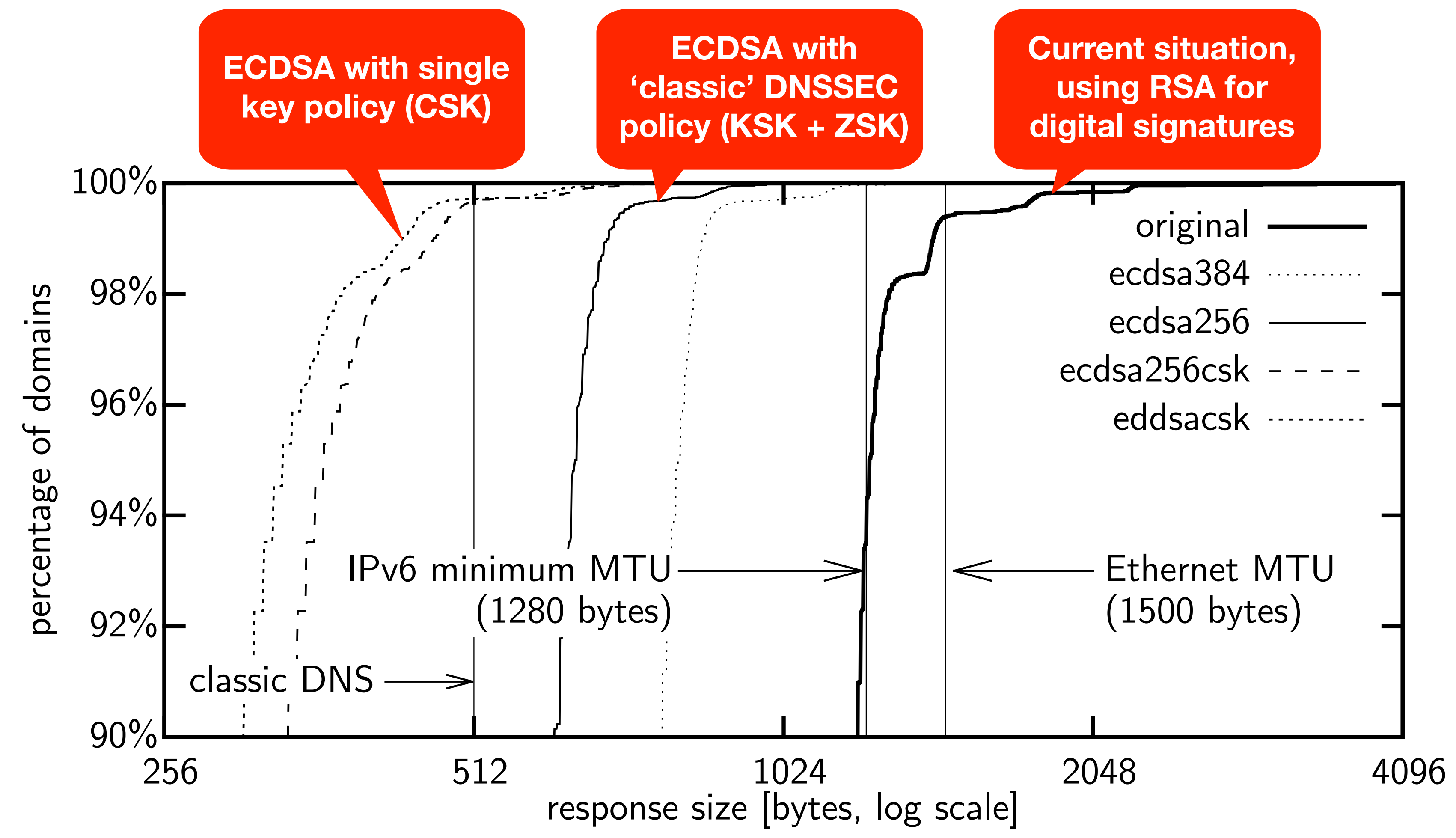
☆ SURFnet bv, Utrecht, The Netherlands

Why should DNSSEC use ECDSA?

The goal of the Domain Name System Security Extensions (DNSSEC) is to improve the security of the DNS protocol. It adds two vital properties: authenticity and integrity. The digital signatures used to achieve this goal, however, make DNS messages much larger. The cause of this is the use of RSA as default signature algorithm. Because of this, DNSSEC suffers from two problems:

1) Packet fragmentation - fragmented DNS messages lead to availability and performance issues.
2) Amplification attacks - DNS can be abused in so-called amplification attacks; DNSSEC with RSA makes this much worse. Amplification factors for RSA-signed domains average around 50x.

ECDSA signatures and keys are much smaller than RSA signatures and keys. Thus, switching DNSSEC to ECDSA results in much smaller DNS messages as the figure from [1] below illustrates:

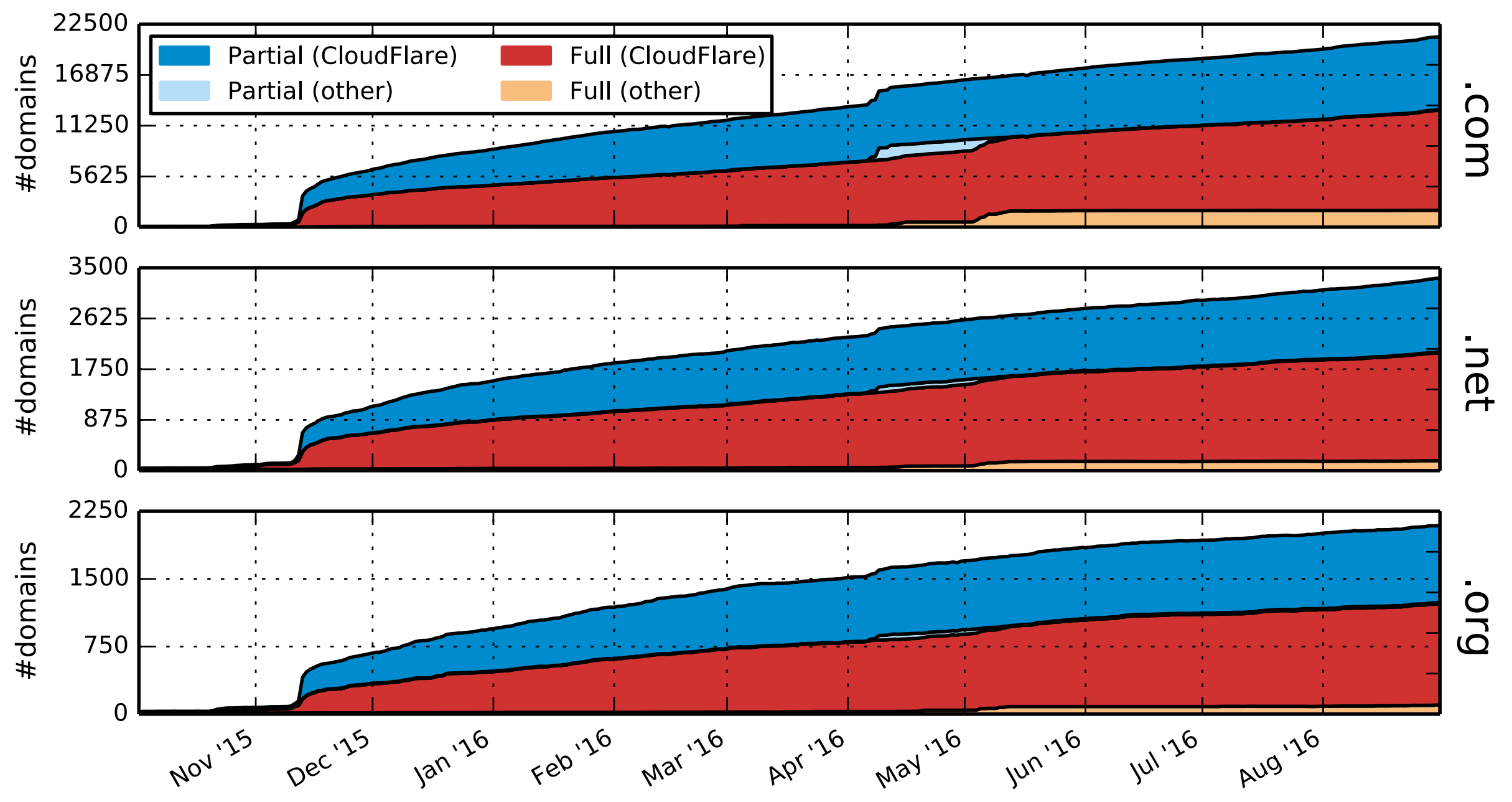

ECDSA with single key policy (CSK)

ECDSA with 'classic' DNSSEC policy (KSK + ZSK)

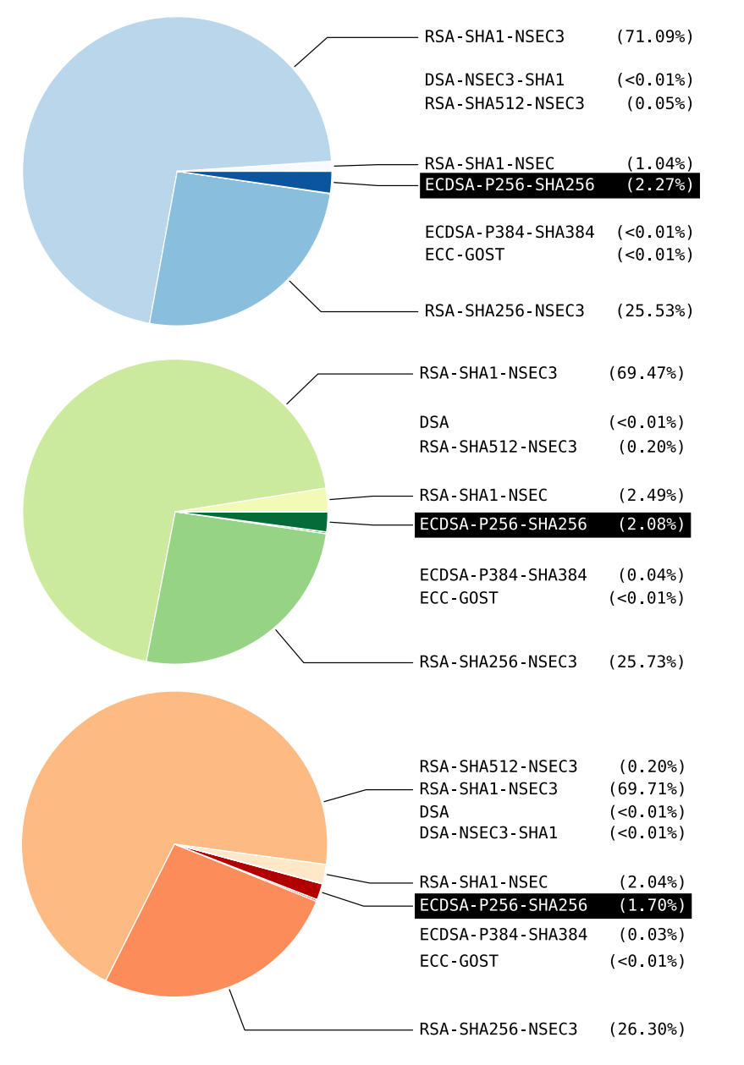
Current situation, using RSA for digital signatures

Adoption in .com, .net and .org

Adoption over time

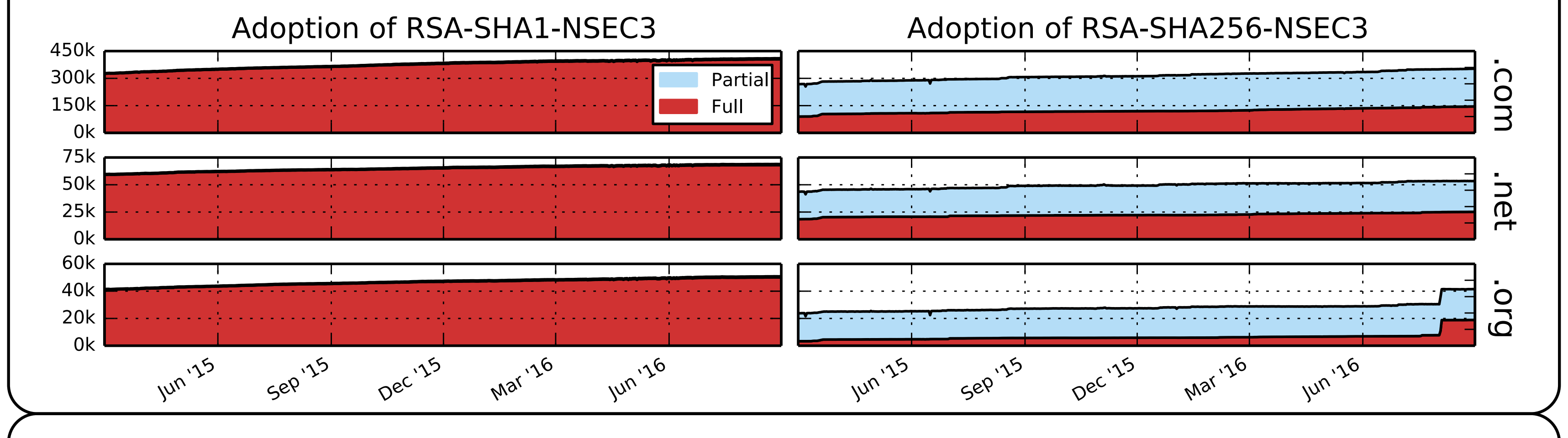


Current use



Hurdles

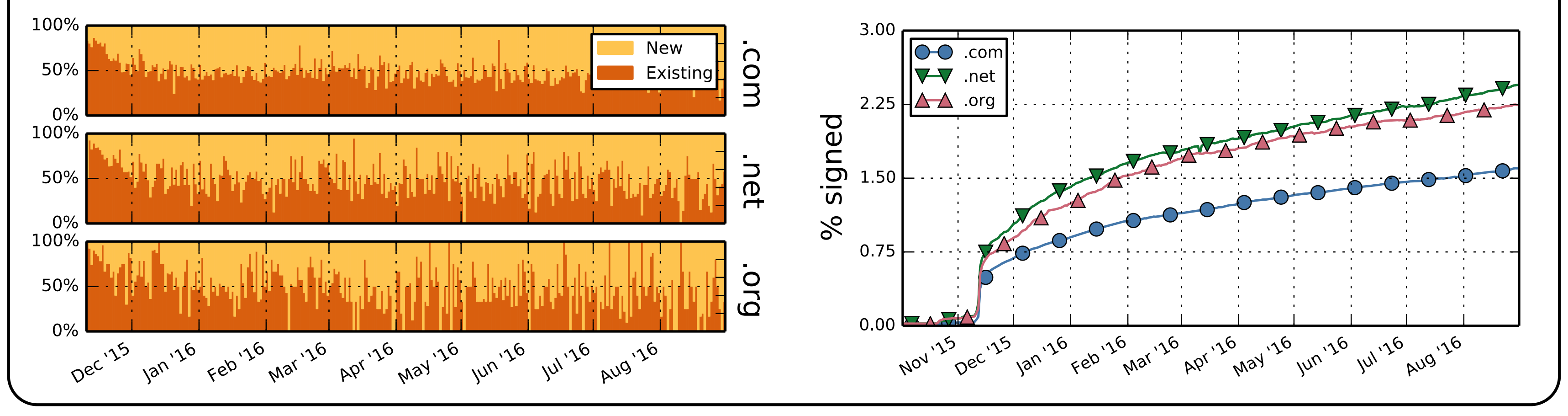
As the figure for adoption over time shows, there are **many partial deployments**. This is due to registrars **not supporting creation of secure delegations for domains signed using ECDSA**, but also because domain owners **forget to create a secure delegation**. These issues also occur for other algorithms, as the figure below shows.


Adoption of RSA-SHA1-NSEC3

Adoption of RSA-SHA256-NSEC3

CloudFlare

The majority of domains that are signed using ECDSA in .com, .net and .org are operated by **CloudFlare**, a company that offers DDoS Protection Services. They **offer DNSSEC signing as part of their service** since **November 2015**. We analysed whether it is mostly **existing customers or new customers** that enable DNSSEC (left), and **what percentage of domains for which CloudFlare is the DNS operator have been signed** (right).



Datasets

To study the adoption of ECDSA in DNSSEC, we used data from the **OpenINTEL project**[1]. Our datasets, listed in the table below, cover **around 50% of the global DNS namespace** over **1.5 years**.

Dataset#	TLD	start date	end date	#domains†	#signed†	(%†)
1	.com .net .org	Mar. 1, 2015	Aug. 31, 2016	127.0M 15.6M 10.8M	0.58M 0.10M 0.07M	(0.46%) (0.64%) (0.67%)
2	.nl	Feb. 9, 2016	Aug. 31, 2016	5.6M	2.54M	(44.95%)
3	.gov	August 31, 2016		1151	1023	(88.88%)

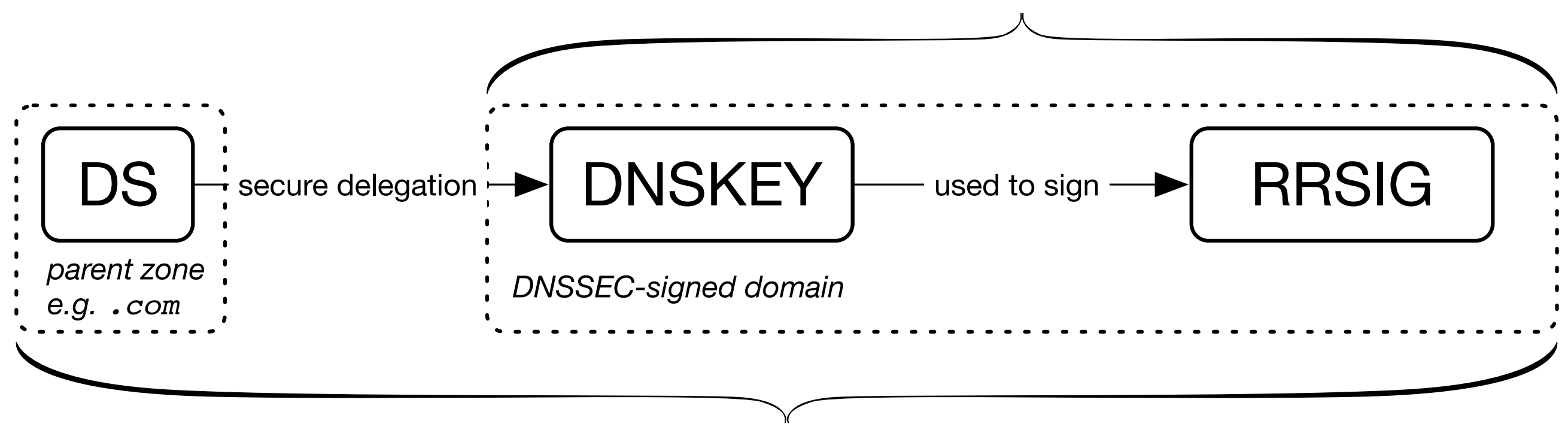
†on August 31, 2016

We detect the use of ECDSA by looking at **algorithm identifiers in DNSSEC-specific record types**. The example below illustrates the record types and algorithm identifier.

```
example.com   IN  DS     31589 8 1 3490A6806D47F17A...
example.com   IN  DNSKEY 257 3 8   AwEAAZ0aqu1rJ6orJynrRfNpPmayJZoAx9Ic2...
example.com   IN  RRSIG  A       8 2 86400 20160925160202 20160904150942...
```

We distinguish between *partial* and *full* deployments of DNSSEC with ECDSA, the figure below explains the difference between the two:

partial deployment if only these records are present



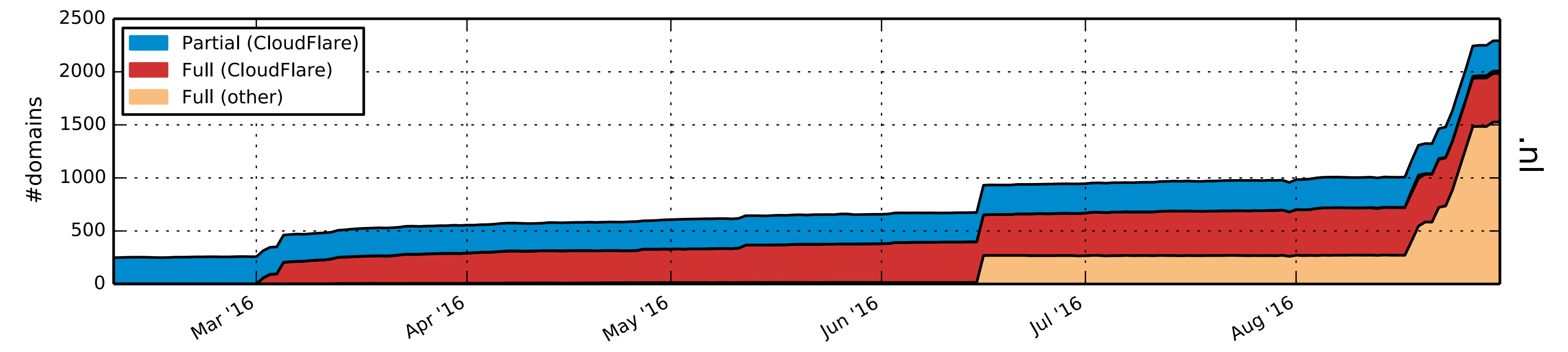
full deployment if all of these records are present

[1] https://www.openintel.nl/

Adoption in ccTLDs

.nl

The .nl ccTLD has the **highest number of DNSSEC-signed domains in the world**, with over 2.5M signed domains (**45% of the 5.7M names**). The vast majority of these use RSA, with **only 0.08%** of domains **using ECDSA**. Also, the .nl ccTLD did not support secure delegations with ECDSA before March 2016. Interestingly, **.nl is the only TLD** where the **majority of domains signed with ECDSA are not operated by CloudFlare**. This is probably **due to the popularity of PowerDNS**. This DNS implementation uses ECDSA by default since version 4.0 (July 2016).

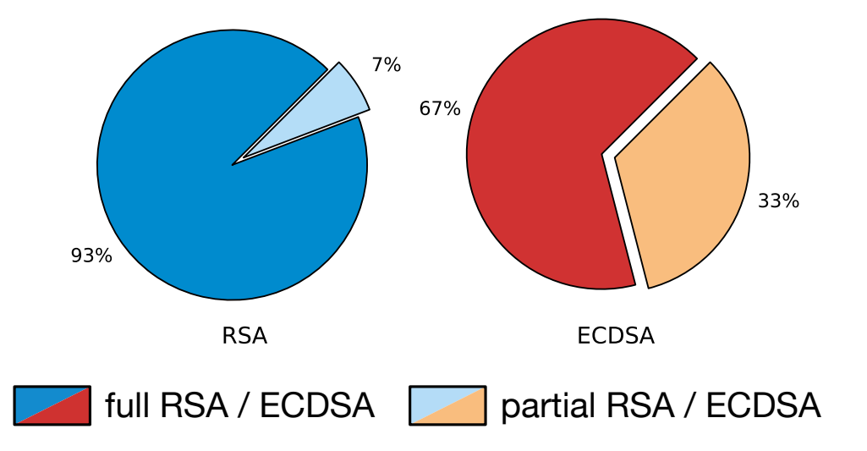


.se

1.38M domains

49.1% signed

≤0.04% use ECDSA

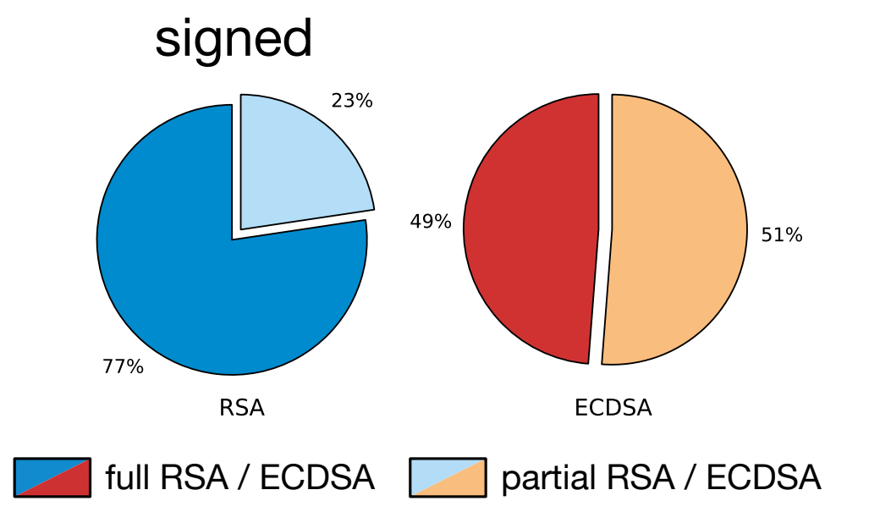


.nu

0.30M domains

23.8% signed

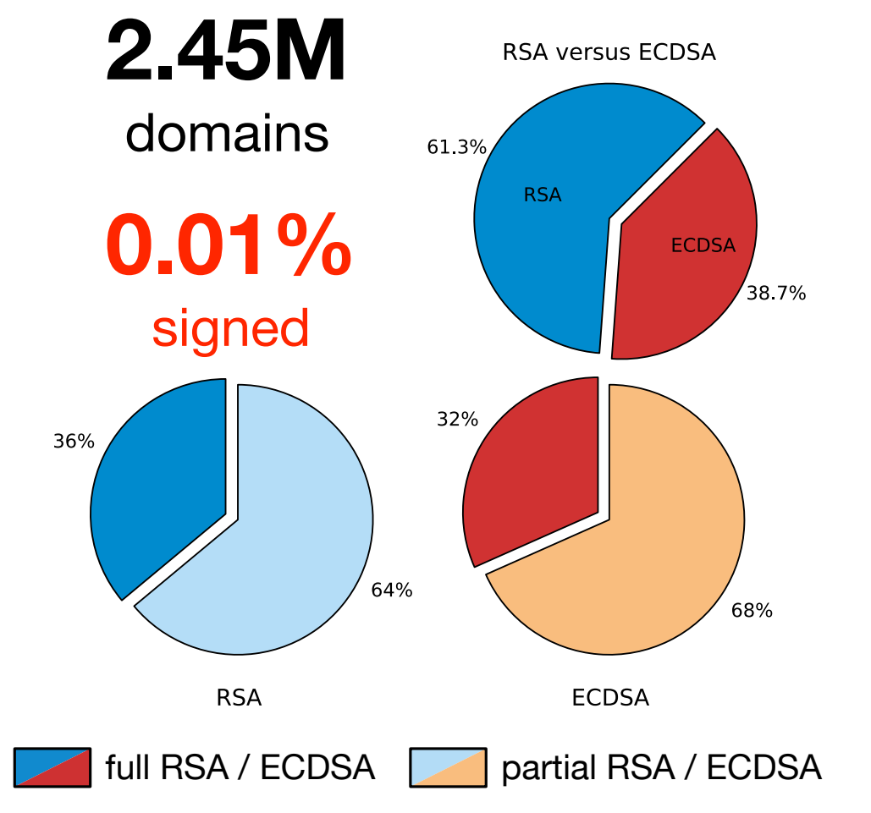
≤0.05% use ECDSA



.ca

2.45M domains

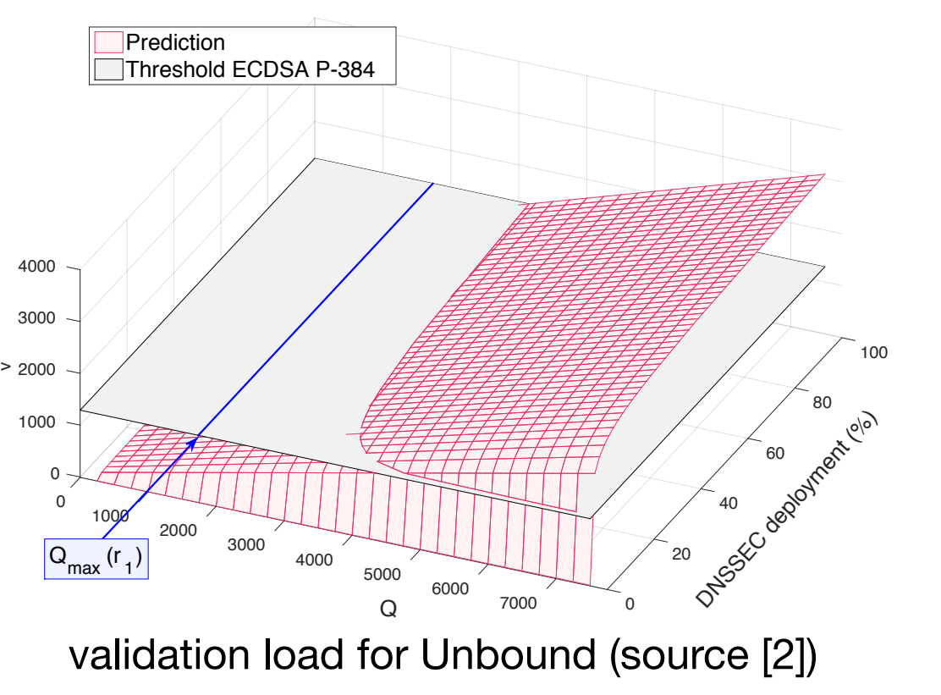
0.01% signed



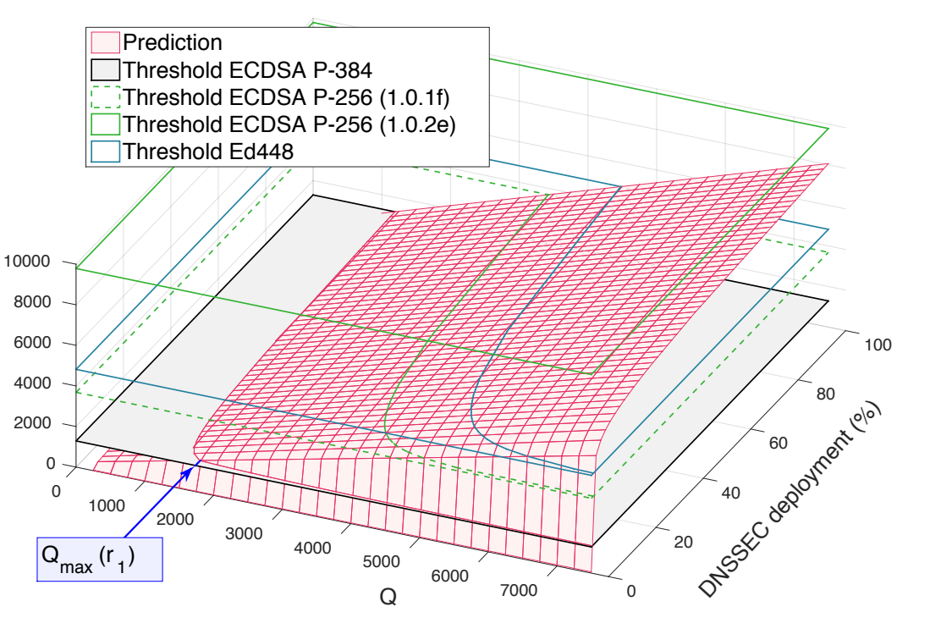
Other adoption considerations

In other work [1,2] we have argued for the adoption of elliptic curve cryptography for DNSSEC. Apart from the hurdles discussed in our paper, there are other issues that operators need to be aware of. First, **DNS resolvers need to support signature validation** of ECC algorithms. Recent work by APNIC (Huston & Michaelson) shows that **around 82% of validating DNS resolvers support ECDSA**.

Second, **validation of elliptic curve digital signatures** is significantly **slower than validation of RSA signatures**. Thus, adoption of ECC may **push load to validating DNS resolvers**. As these figures from [2] show, however, this load is manageable for validating resolvers.



validation load for Unbound (source [2])



validation load for BIND (source [2])

[1] van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2015). Making the Case for Elliptic Curves in DNSSEC. ACM Computer Communication Review (CCR), 45(5).

[2] van Rijswijk-Deij, R., Hageman, K., Sperotto, A., & Pras, A. (2016). The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation. To Appear in IEEE/ACM Transactions on Networking.

DACS Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

SURF NET

SIDN LABS

scan QR for paper