# ECDSA adoption in DNSSEC

a view on 3 gTLDs, a special TLD and 7 ccTLDs

UNIVERSITY OF TWENTE.

SURF NET

# Introduction

- ECDSA was standardised for DNSSEC in 2012 —> RFC 6605
- No use at all until end of 2015 (less than 50 domains in our datasets)
- 2015: CloudFlare announces “Universal DNSSEC” On-the-fly DNSSEC signing using ECDSA
- 2016: PowerDNS makes ECDSA the default algorithm

# Recap: why use ECDSA?

- DNSSEC suffers from **reachability problems because of fragmentation** [1]
  (and yes, that is still a thing in 2017)

- DNSSEC is abused for **amplification attacks** [2]
  (see e.g. reports from DDoS protection services)

- Common cause: large messages because of large RSA signatures and keys

- Solution: use elliptic curve cryptography
  - **Smaller keys, smaller signatures, stronger cryptographic security!**

# Datasets

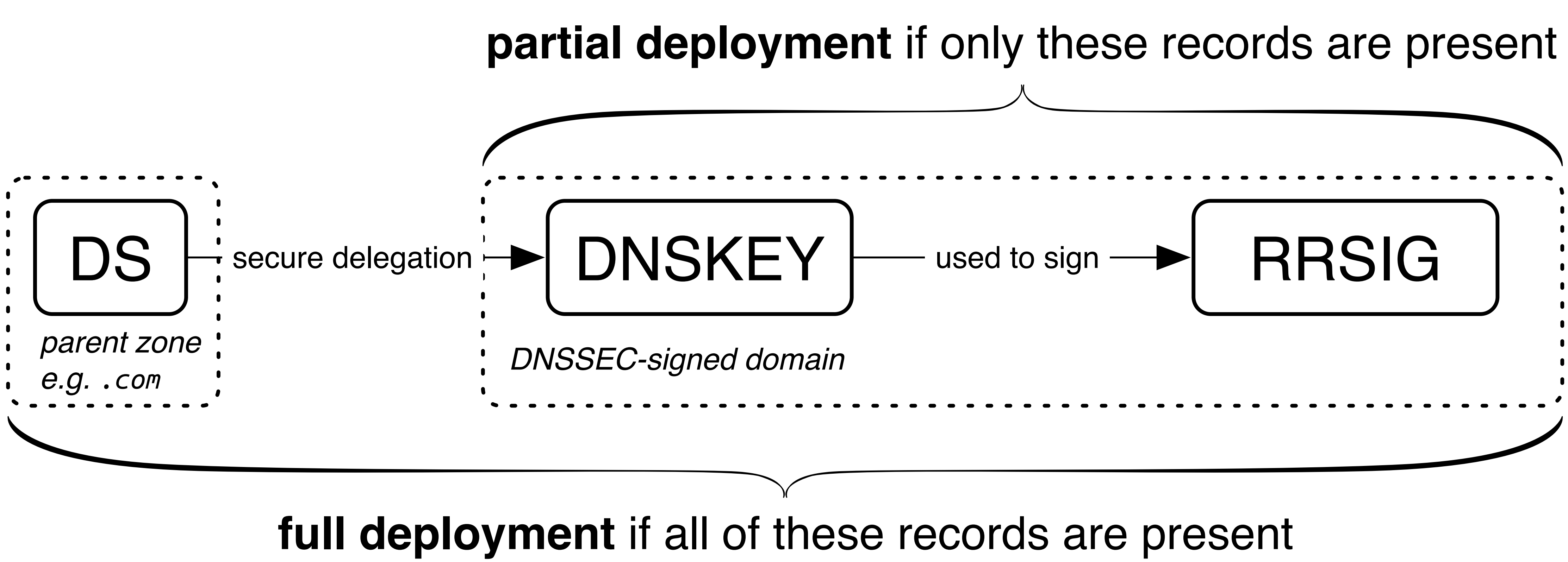
| Dataset# | TLD | Start date | End date | #Domains* | #Signed* | (%*) |
|---|---|---|---|---|---|---|
| I | .com | Mar. 1, 2015 | Feb. 14, 2017 | 126.6M | 0.63M | (0.5%) |
| | .net | | | 15.1M | 0.10M | (0.7%) |
| | .org | | | 10.5M | 0.08M | (0.7%) |
| II | .nl | Feb. 9, 2016 | Feb. 14, 2017 | 5.7M | 2.59M | (45.5%) |
| III | .gov | February 14, 2017 | | 1083 | 990 | (91.4%) |
| IV | .at | February 14, 2017 | | 1.3M | $< 0.01$M | (0.3%) |
| | .ca | | | 2.5M | $< 0.01$M | ($<$ 0.1%) |
| | .dk | | | 1.3M | 0.02M | (1.8%) |
| | .fi | | | 0.4M | $< 0.01$M | (0.4%) |
| | .nu | | | 0.3M | 0.08M | (26.0%) |
| | .se | | | 1.4M | 0.07M | (48.6%) |

*On February 14, 2017

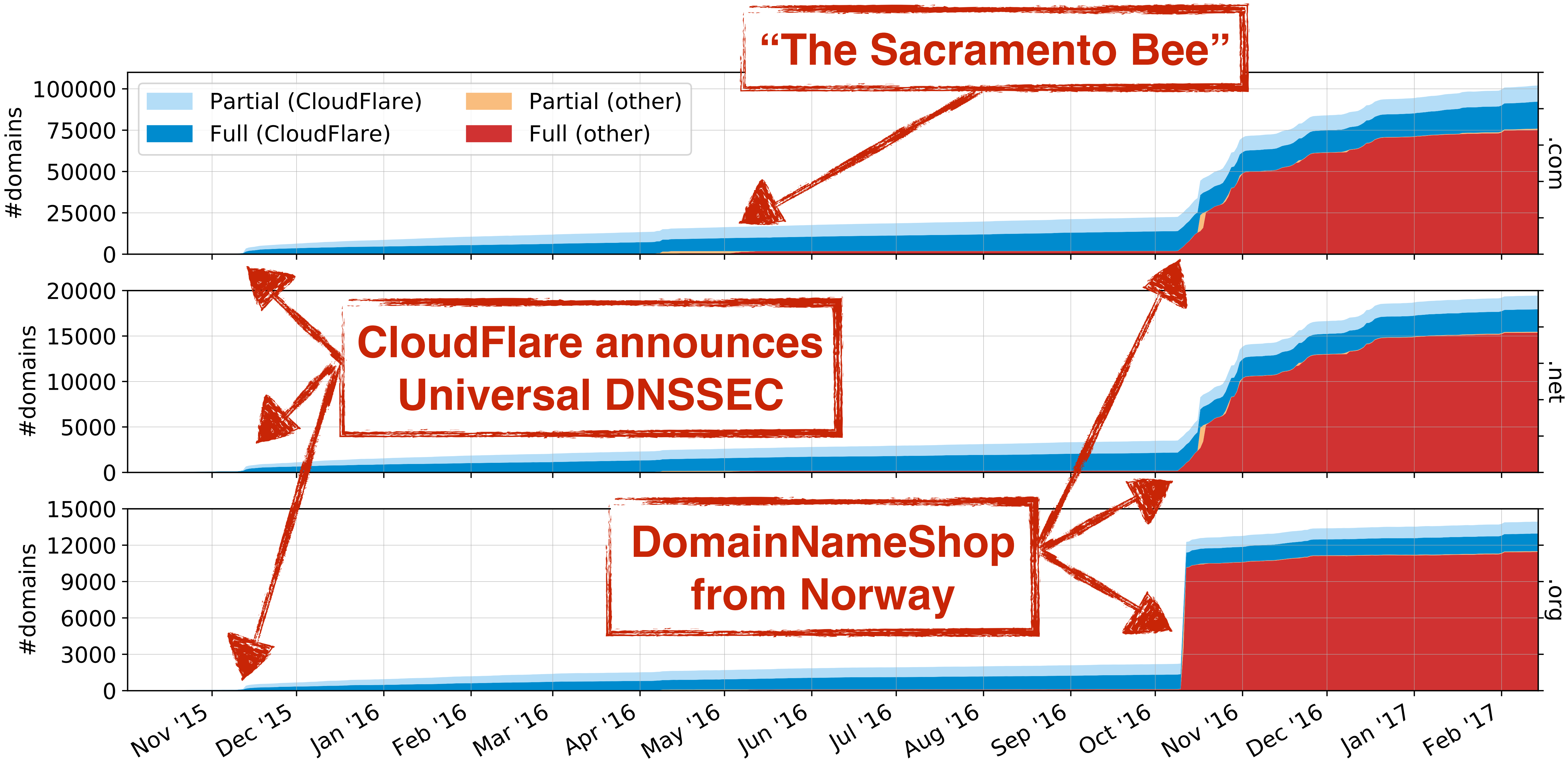
data sourced from OpenINTEL (see last slide)

# Methodology

- We looked at algorithm identifiers in DS, DNSKEY and RRSIG records
- We distinguish between **full** and **partial** deployments:

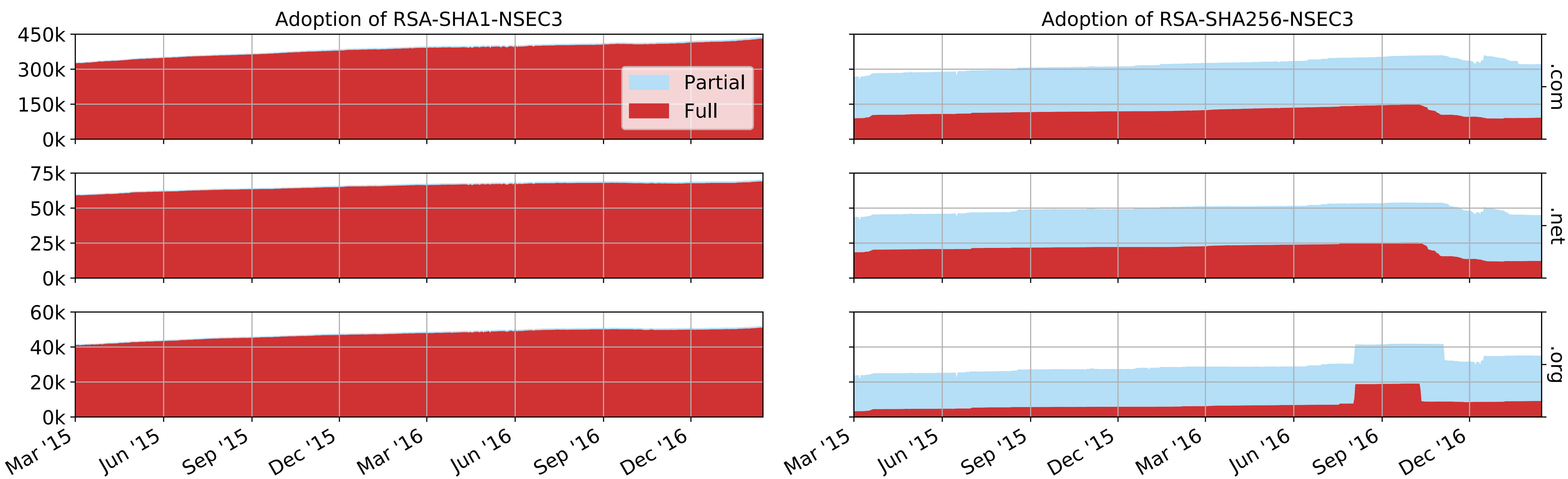


# The three largest gTLDs

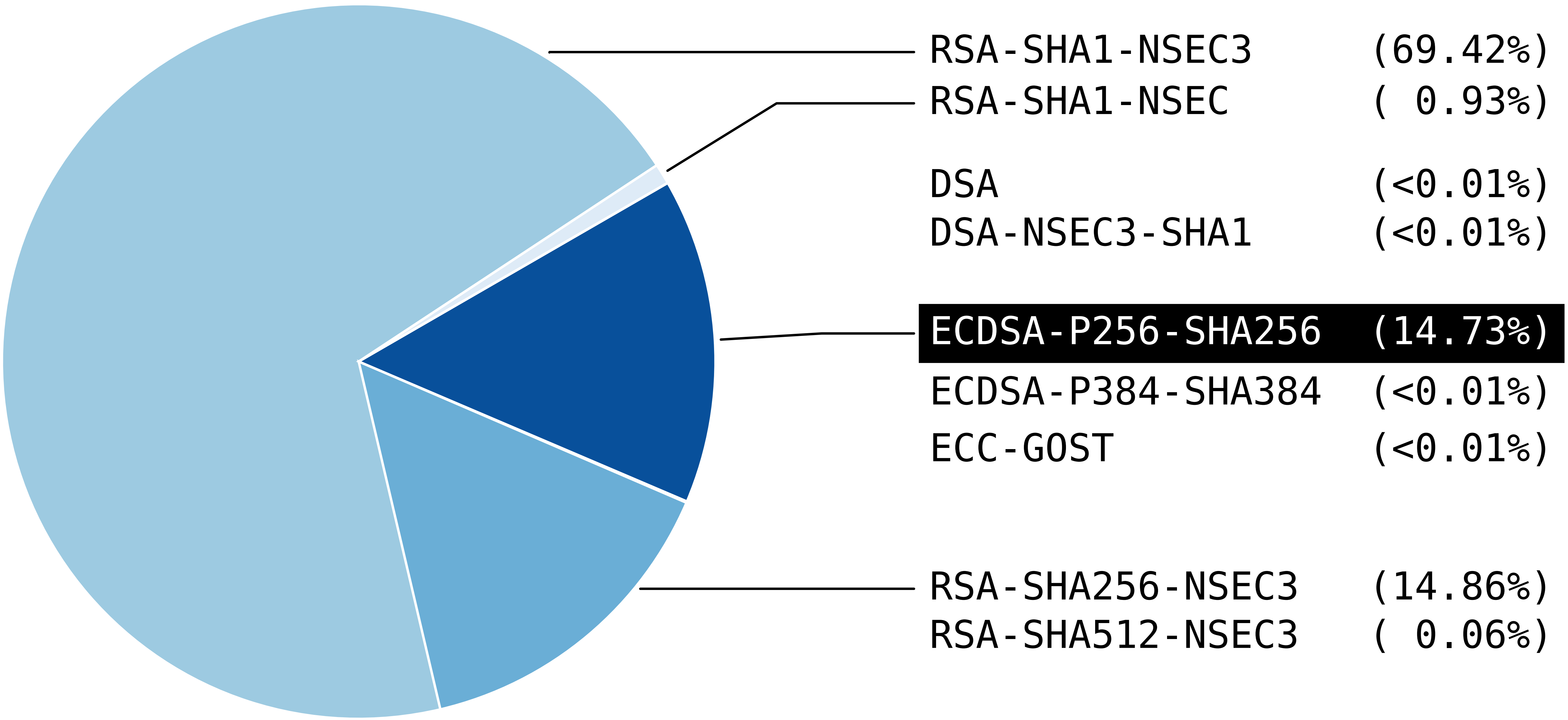


# Partial adoption

- Partial deployments also occur for other algorithms
- Causes: no support for secure delegations, operators or registrants not registering a DS



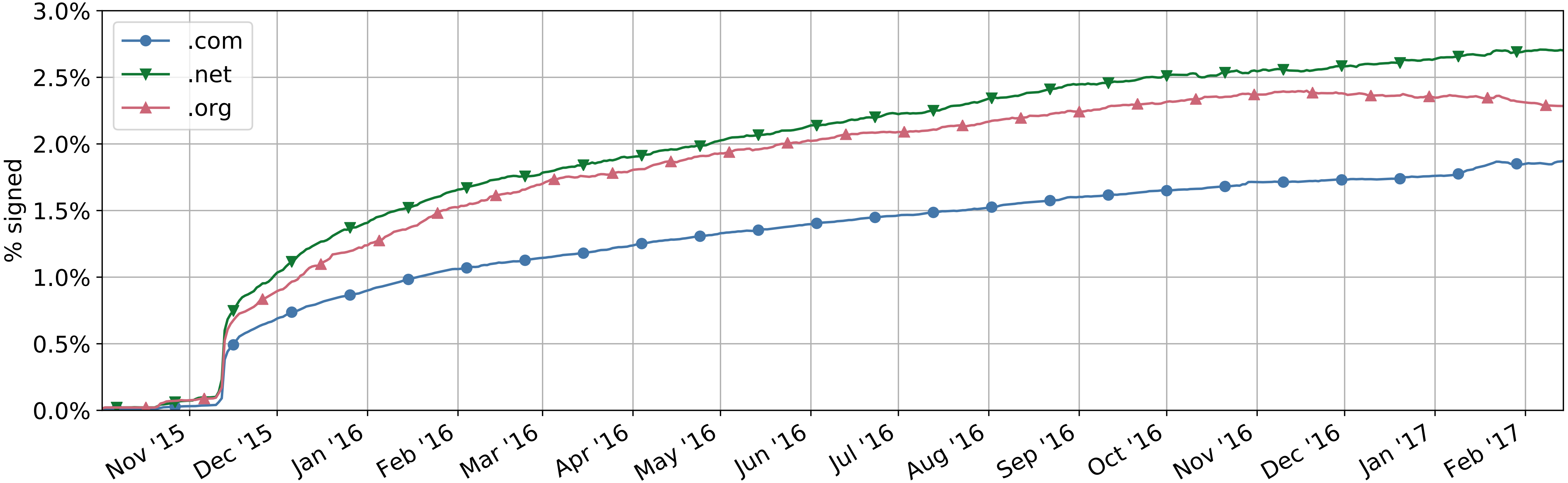
# Algorithm distribution in .com




- on February 14, 2017

# Making ECDSA great(er) (again)

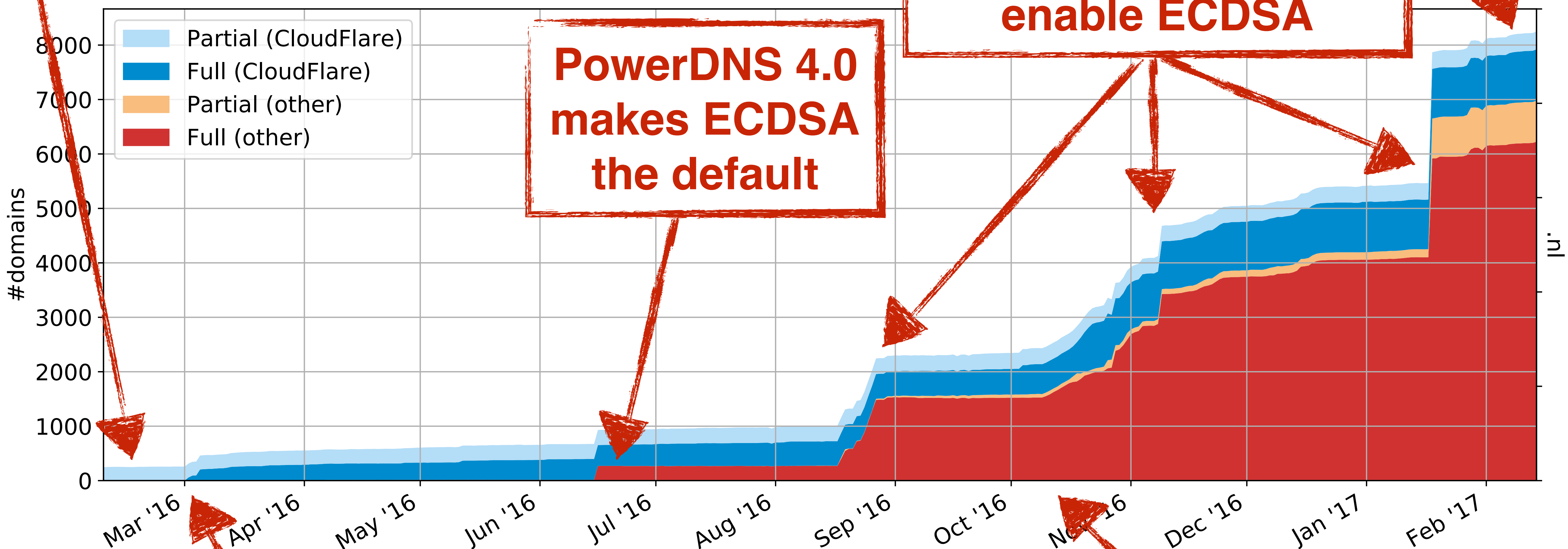
- If all domains managed by **CloudFlare** fully deploy DNSSEC, this **would make ECDSA "YUGE"!**




| TLD | #Domains | #Signed | (%) | %ECDSA | #CloudFlare | %Signed* | %ECDSA* |
|---|---|---|---|---|---|---|---|
| .com | 126.6M | 0.63M | (0.50%) | 14.73% | 1.40M | 1.59% | 72.5% |
| .net | 15.1M | 0.10M | (0.69%) | 17.49% | 0.15M | 1.65% | 63.7% |
| .org | 10.5M | 0.08M | (0.72%) | 17.23% | 0.11M | 1.73% | 63.3% |

# Adoption in .nl

More than 50% of these partial (CloudFlare) deployments still exist!




.nl starts supporting ECDSA for DS

DomainNameShop from Norway

# Adoption in other ccTLDs

- We also studied 6 other ccTLDs, specifically:

| | | | |
|---|---|---|---|
| **.at** | - Austria | **.fi** | - Finland |
| **.ca** | - Canada | **.nu** | - Niue |
| **.dk** | - Denmark | **.se** | - Sweden |

| | **ccTLD** | | | | | |
|---|---|---|---|---|---|---|
| | `.at` | `.ca` | `.dk` | `.fi` | `.nu` | `.se` |
| **%Signed** | 0.30% | 0.01% | 1.81% | 0.38% | 25.99% | 48.59% |
| **%ECDSA P-256** | 0.99% | 41.25% | 88.47% | 75.13% | 14.58% | 2.64% |

- Takeaway: adoption varies, local hosters adopting ECDSA makes a big difference

# Adoption in .gov

- Federal agencies **must sign** their **.gov** domains
- **NIST recommended** a switch to ECC and larger RSA keys years ago
- So do .gov domains use ECDSA?

**NO, NONE, ZERO, ZILCH, NADA.**

- Some “fun” facts:
  - **8%** of .gov domains **exclusively use 1024-bit RSA**
  - **Six** .gov domains still **use 512-bit RSA**
  - Almost **50%** of .gov domains **use SHA1** hashing in DNSSEC (against NIST recommendations from 2015!)

# Signing with a CSK

- In earlier work, we showed that signing with a **Combined Signing Key (CSK)** has additional advantages to **further reduce fragmentation** and **amplification**

- So we asked ourselves: do people use CSKs with ECDSA?

| | TLD or ccTLD | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Scheme** | .com | .net | .org | .at | .ca | .dk | .fi | .nl | .nu | .se |
| KSK/ZSK | 97.7% | 98.4% | 98.4% | 74.0% | 97.4% | 47.8% | 99.5% | 53.4% | 85.4% | 99.1% |
| CSK | 2.3% | 1.6% | 1.6% | 26.0% | 2.6% | 52.2% | 0.5% | 46.6% | 14.6% | 0.9% |

- Takeaway: some operators choose to use a CSK, but there is no clear trend. From other data we know that CSK uptake for ECDSA appears to be higher than for RSA

# RSA developments

- But what is happening in the RSA space? **1024-bit** is considered **too weak**, but are people switching?

| TLD | KSK: 2048 ZSK: 1024 | KSK: 1024 ZSK: 1024 | KSK: 2048 ZSK: 2048 | KSK: 1280 ZSK: 1280 | KSK: 4096 ZSK: 2048 | KSK: 4096 ZSK: 4096 | Other | !Power of 2 KSK | !Power of 2 ZSK |
|---|---|---|---|---|---|---|---|---|---|
| .com | 59.9% | 37.9% | 0.9% | 0.3% | 0.3% | 0.2% | 0.5% | 0.3% | 0.4% |
| .net | 54.3% | 42.3% | 1.3% | 0.4% | 0.5% | 0.3% | 0.9% | 0.5% | 0.5% |
| .org | 55.4% | 41.3% | 1.1% | 0.3% | 0.6% | 0.3% | 1.0% | 0.4% | 0.5% |

| TLD | KSK: 2048 ZSK: 1024 | KSK: 1536 ZSK: 1280 | CSK: 2048 | KSK: 2048 ZSK: 2048 | CSK: 1024 | KSK: 4096 ZSK: 2048 | Other | !Power of 2 KSK | !Power of 2 ZSK |
|---|---|---|---|---|---|---|---|---|---|
| .nl | 96.2% | 2.3% | 0.9% | 0.2% | 0.2% | 0.1% | 0.1% | 2.3% | 2.3% |

(data is for 2017-02-14)

- Takeaway: window of **opportunity to go** from insecure RSA variants **to ECC algorithms** during upgrades or **a risk of increases in RSA keysizes for many domains** (with the associated problems)

# EdDSA

- **EdDSA** has very **recently** been **standardised** for use in DNSSEC
  (thanks to Ondřej Surý and Robert Edmonds!)

- **RFC 8080** standardises two curves:
  - **Ed25519 (algo 15)**
    256-bit curve, 128-bit security, **highly attractive**, keys only require 32 bytes in a DNSKEY record
  - **Ed448 (algo 16)**
    448-bit curve, 224-bit security, **high security**

# EdDSA (cont'd)

- EdDSA support is (virtually) non-existent in software
- There are good reasons to push for support:
  - EdDSA is **much faster**
  - EdDSA keys require only **half the space of** an equivalent **ECDSA key** in a DNSKEY record
  - EdDSA has better security properties (see https://safecurves.cr.yp.to)
- So support your favourite OSS project to implement EdDSA!
- **SURFnet** is **pushing** for our new **HSM vendor** to support EdDSA; they claim to have put it on the roadmap

# Conclusions

- ECDSA adoption has taken off, there are now significant numbers of domains signed with this algorithm
- Deployments still traceable to a hand full of operators
- Secure delegations through the RRR channel are blocking deployment of DNSSEC in general, and ECDSA in particular

# Recommendations

- **For DNSSEC signer operators:**
  - *Planning a new deployment?*
    **Choose ECDSA P-256** as signing algorithm
  - *Existing deployment:*
    Consider **switch**ing **to ECDSA** (or even EdDSA) as part of your upgrade/replacement cycle (not trivial)
    ***(this is what we will be doing in 2017)***
- **For DNS resolver operators:**
  - *Doing DNSSEC validation?*
    **Check support for ECDSA**, consider upgrading if not supported

# SURFnet plans for 2017

- SURFnet will be switching all signed domains to **ECDSA P-256 in 2017**
- Migrating to **new HSMs**
- **Simpler key management** scheme: **single key** ("CSK")
- **Live algorithm rollover** of about 1200 domains
- We will **blog** about our progress and **share** our automation **scripts and code**

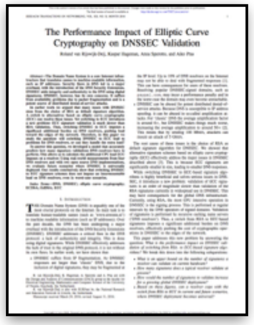
# Further reading

- [1] DNSSEC Meets Real World: Dealing with Unreachability Caused by Fragmentation.
  IEEE Communications Magazine, 52 (April), 2014
  **http://bit.ly/commag14-dnssec-frag**

- [2] DNSSEC and its potential for DDoS attacks
  Proceedings of ACM IMC 2014, Vancouver, BC, Canada
  **http://bit.ly/imc14-dnssec**

- [3] Making the Case for Elliptic Curves in DNSSEC
  ACM Computer Communication Review (CCR), 45(5).
  **http://bit.ly/ccr15-ecdsa**

- [4] The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation
  To appear in IEEE Transactions on Networking
  **http://bit.ly/ton16-ecc-impact**



- Internet Society Deploy 360 Programme, DNSSEC
  **http://www.internetsociety.org/deploy360/dnssec/**

# Thank you for your attention! Questions?

**acknowledgements:**

**Thanks to Mattijs Jonker for helping crunch numbers**

**The results in this presentation were made possible by OpenINTEL, a joint project of SURFnet, SIDN and the University of Twente https://www.openintel.nl/**

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl

UNIVERSITY OF TWENTE.

SURF NET