DNSSEC Operational Practices: The Good, The Bad and The Ugly

Roland van Rijswijk-Deij
Nordic Domain Days

joint work with: Tho Le, Luca Allodi and Nicola Zannone
of TU Eindhoven

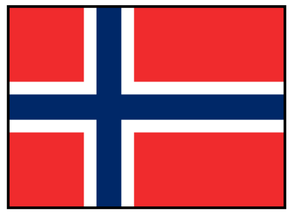
NLNETLABS

DNSSEC in the second decade

- **Mass deployment** of DNSSEC **took off in 2008, after "Kaminsky"**
- We have **just entered the second decade** of DNSSEC
- **Things** seem to be **going well**:
  - Vast **majority of top-level domains** support DNSSEC
  - Number of **validating resolvers still growing**
- **But also: many "important" domains still not signed**
  (Google, Facebook, Amazon, ...)

NLNETLABS

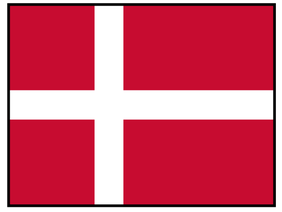
DNSSEC in the Nordic region



.no 58%

.se 54%

.is 3%



.dk 2%

.fi 1%

What do these have in common?

For comparison:

.com 0.7%

.net 1%

.org 1%

But also:

.nl 53%

NLNETLABS


Incentives, incentives, incentives!

Studying incentives

- **Both** .nl and .se **have financial incentives for registrars** to encourage DNSSEC deployment
- These **incentives are modest** (a few percent discount on registration)
- This means that the incentives **only pay off** financially **if you deploy** DNSSEC **for 100,000s of domains**
- While this **clearly** has **led to mass deployment** of DNSSEC, we wondered if it has **also led to secure deployments?**

Study goals

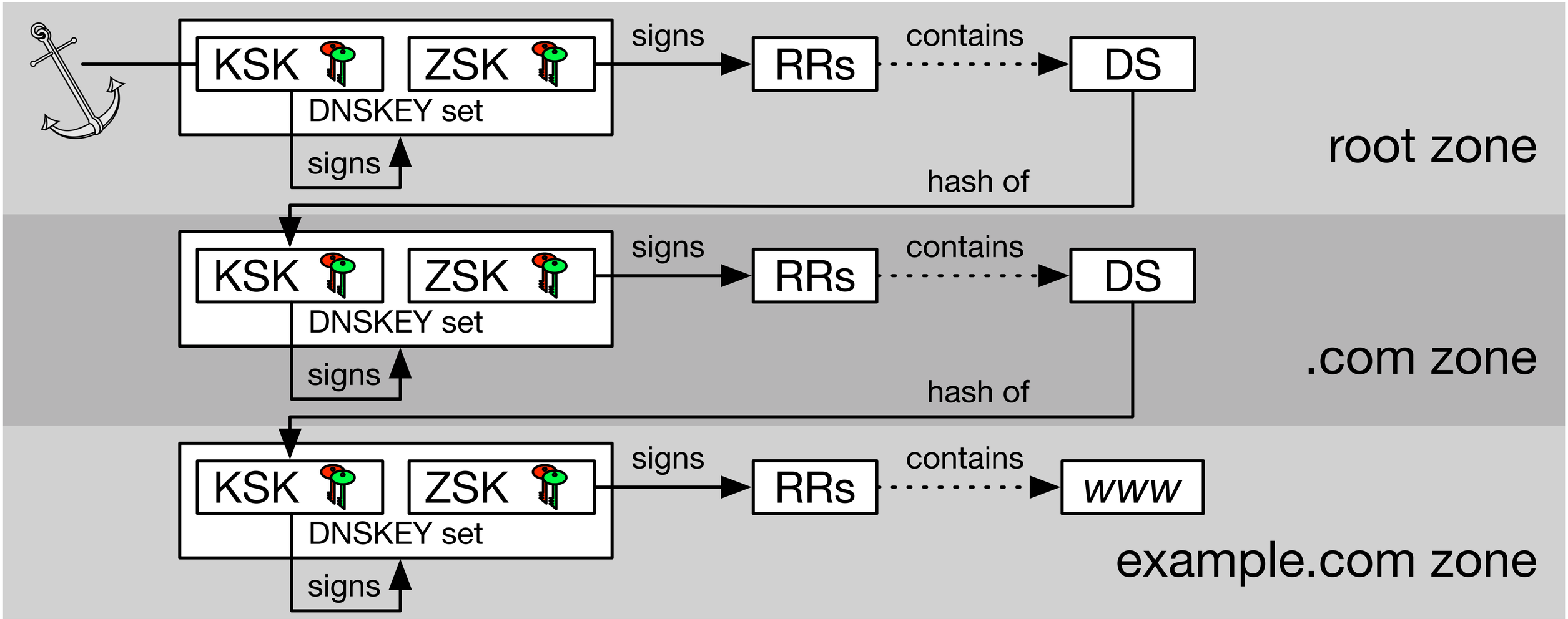
- We wanted to **study** the **quality** of DNSSEC deployments **in terms of security** as **defined in** DNSSEC **best practices**

- Our **assumption: only large operators benefit economically from incentives**, therefore **we expect small operators to deploy** DNSSEC **with a different motivation**

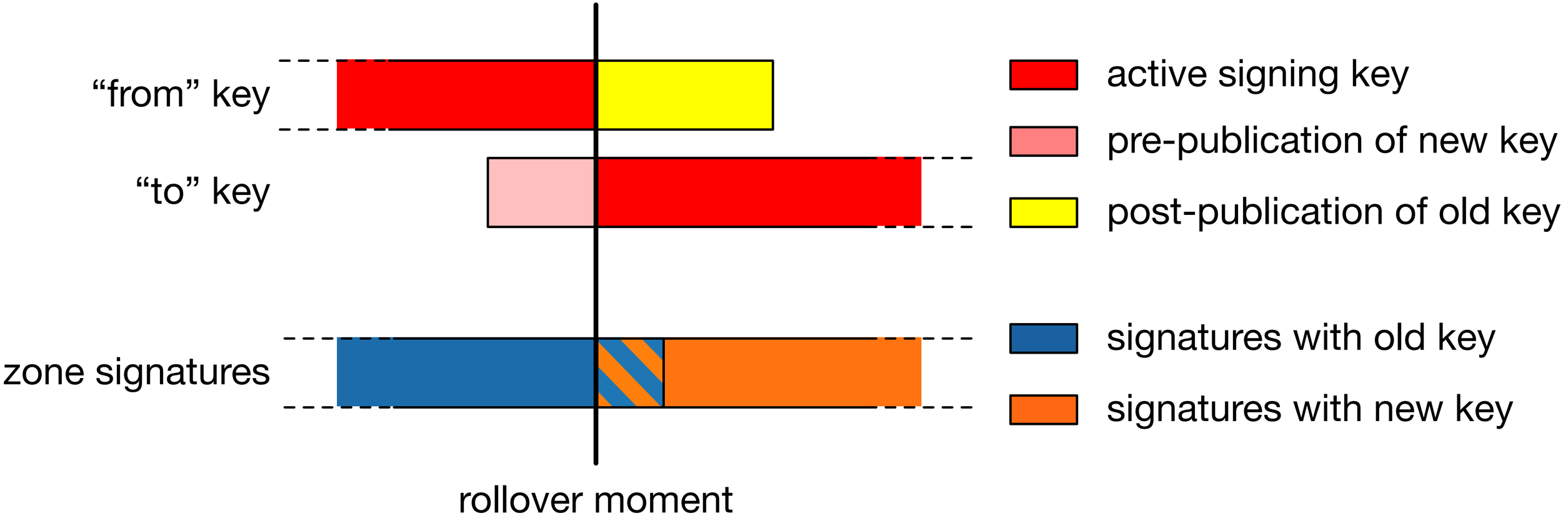
- **Hypothesis:**
  "Despite the presence of 'per-domain' economic incentives in .nl and .se, large DNS operators deploy DNSSEC with lower compliance to security guidelines than small DNS operators."

NLNETLABS

DNSSEC in two slides



DNSSEC in two slides



NLNETLABS

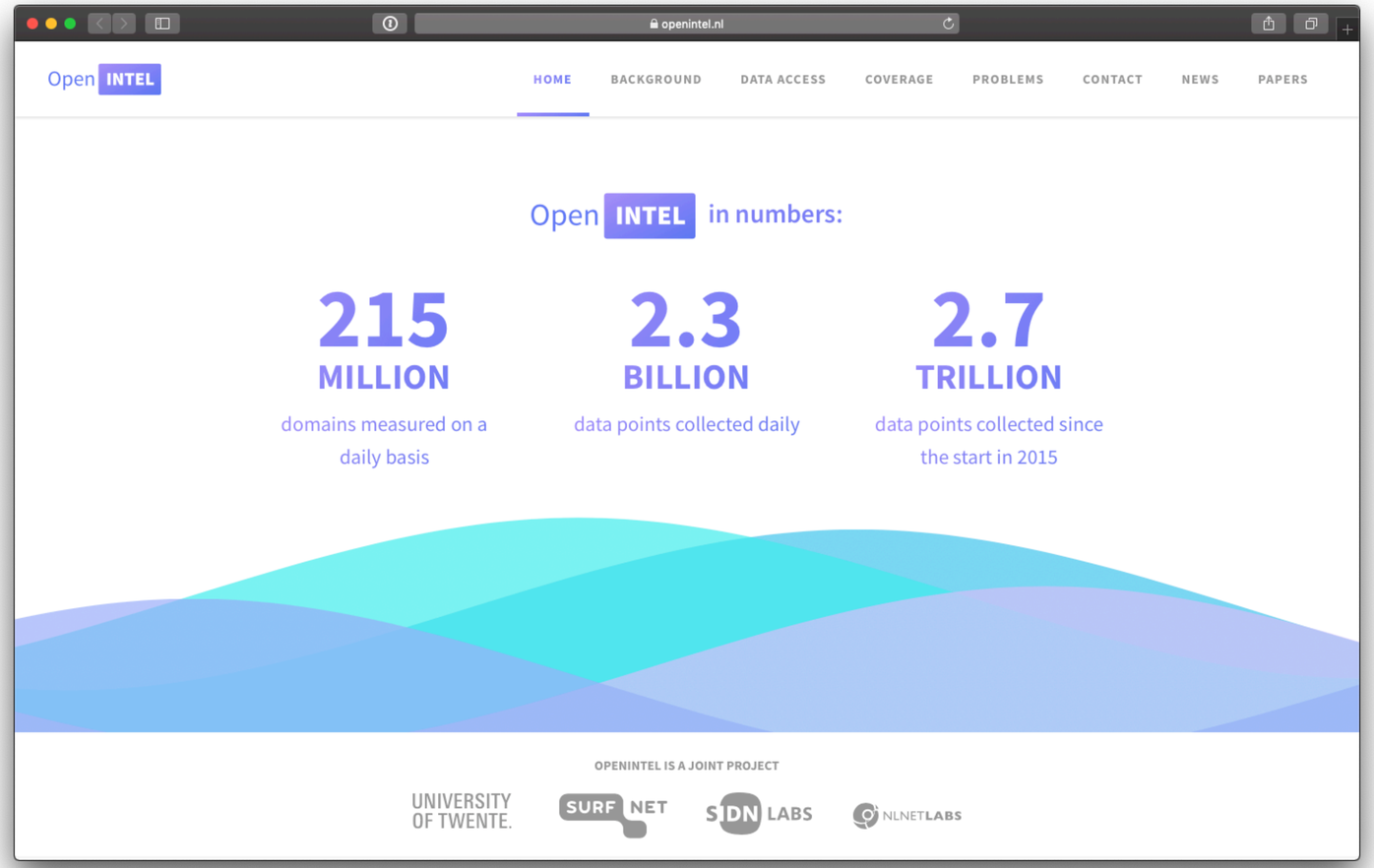
Best Current Practice

Aspects	NIST recommendation
Key size	- ECDSA keys. - RSA: KSKs >= 2048 bits and ZSKs >= 1024 bits.
Key algorithm	- Recommended: Algorithms 8 and 10. - Highly recommended: Algorithms 13 and 14.
Key rollover	**KSKs/CSKs:** - ECDSA keys and and RSA keys (with key size >=2048 bits): rollover within 24 months. **ZSKs:** - 1024-bit RSA keys: rollover within 90 days. - RSA keys' size between 1024 - 2048 bits: rollover within 12 months. - ECDSA keys and RSA keys (with key size >= 2048 bits): rollovers within 24 months.

NLNETLABS

OpenINTEL

For this study we used data from the OpenINTEL project



https://openintel.nl/

NLNETLABS

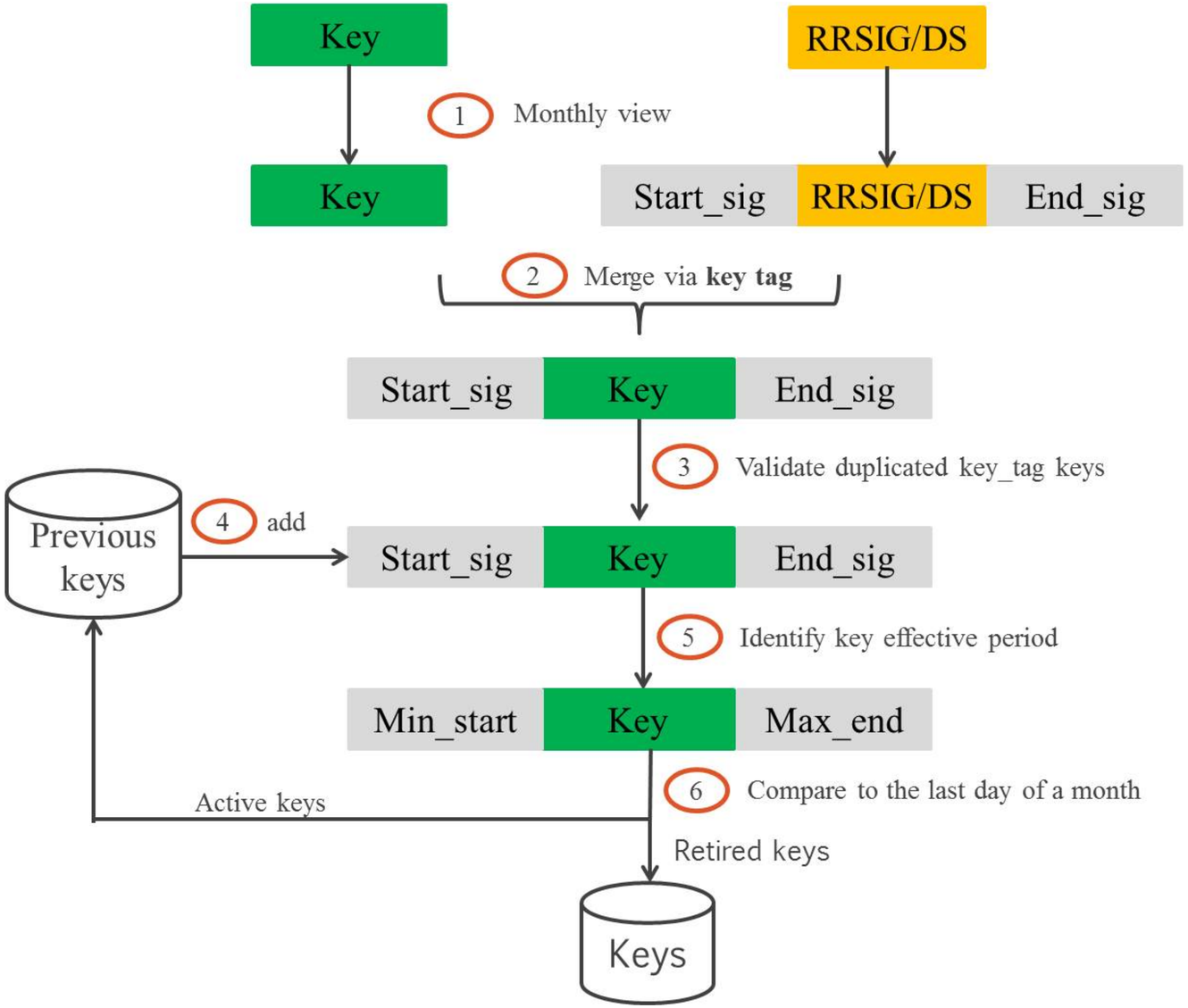
Approach

TLDs	Measurement Period	#Domains	
.com	2015-02-28 - 2017-07-31	116,814,548	
.net	2015-02-28 - 2017-07-31	13,011,428	→ For comparison
.org	2015-02-28 - 2017-07-31	9,373,214	
.nl	2016-02-09 - 2017-07-31	5,440,975	
.se	2016-06-07 - 2017-07-31	1,440,244	→ Focus of study

- Analyse **RRSIG** and **DNSKEY** records for **all signed domains every day** to check key sizes, algorithms and key rollovers

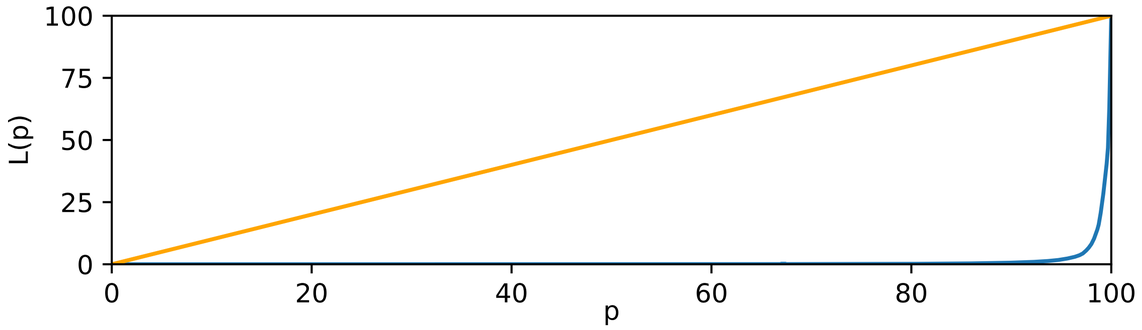
NLNETLABS

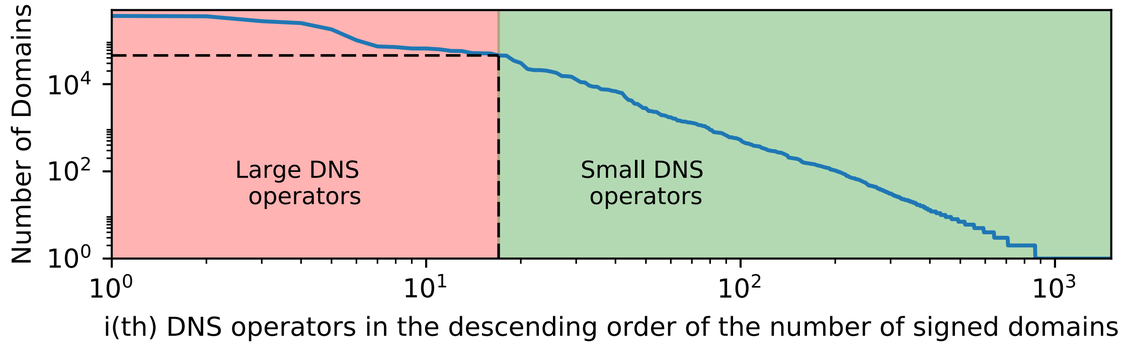
Rollover complexity

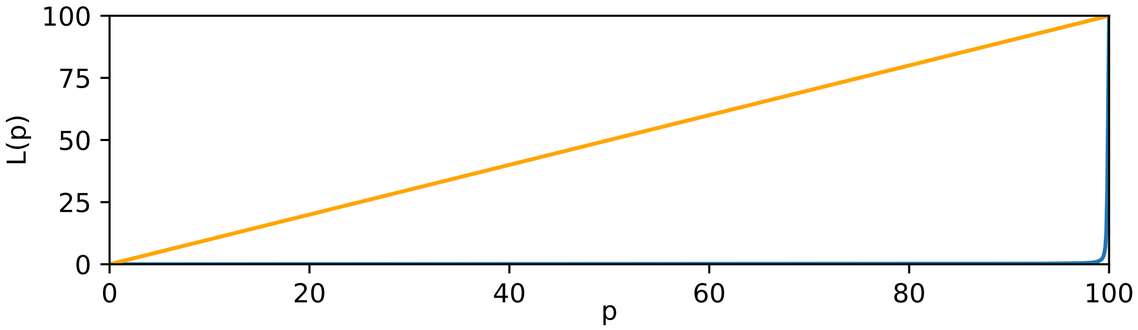


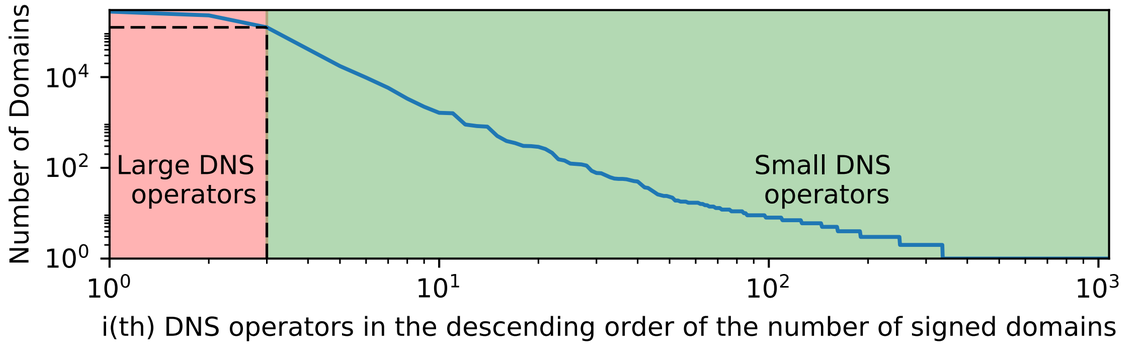
NLNETLABS

Large versus Small









.nl

Just **14 operators** responsible for **over 80% of signed domains**

.se

Just **3 operators** responsible for **over 80% of signed domains**

NLNETLABS

All the DNSSEC large and small

- To check if **large operators** are **more likely to deploy** DNSSEC **under an incentive**, we **compared .com/.net/.org to .nl and .se**

	Large operators			Small operators		
TLD	**#Domains**	**#Signed**	**%**	**#Domains**	**#Signed**	**%**
.com	93,464,626	712,162	0.76%	23,349,922	224,251	0.96%
.net	10,412,605	114,687	1.10%	2,598,823	26,400	1.02%
.org	7,501,310	85,166	1.14%	1,871,904	20,342	1.09%
.nl	4,353,518	2,736,393	62.85%	1,087,457	92,791	8.53%
.se	1,153,129	723,532	62.75%	287,115	13,794	4.80%

- **Takeaway: uptake** among large operators is an **order of magnitude higher under** an **incentive!**

NLNETLABS

Results for large operators in .nl

DNS operator	Master NS†	#Signed	Algorithm	KSK size	ZSK size	ZSK Rollover
TransIP	*.transip.net.	265,341	✗	✓	⚠+	✗
	*.transip.nl.	206,254	✗	✓	⚠+	✗
	*.sonexo.eu.	75,256	✓	✓	⚠+	✗
	ns0.nl.	50,273	✗	✓	⚠+	✗
Metaregistrar BV	*.metaregistrar.nl.	386,913	✓	✓	⚠+	✗
Hostnet BV Network	*.hostnet.nl.	359,793	✓	✓	⚠+	✗
Cyso Hosting	*.firstfind.nl.	246,385	✓	✓	⚠+	✗
Argeweb BV	*.argewebhosting.eu.	101,993	✓	✓	⚠+	✗
Openprovider	*.openprovider.nl.	79,367	✓	✓	⚠+	✗
Village Media BV	*.webhostingserver.nl.	67,150	✓	✓	⚠+	✗
Hosting2GO	*.hosting2go.nl.	64,568	✓	✓	⚠+	✗
Flexwebhosting BV	*.flexwebhosting.nl.	60,753	✓	✓	⚠+	✗
Internedservices	*.is.nl.	57,033	✓	✓	⚠+	✗
Neostrada	*.neostrada.nl.	56,295	✓	✓	⚠+	✗
One.com	*.one.com.	55,397	✓	✗	✓	?
PCextreme	*.pcextreme.nl.	50,102	✓	✓	⚠+	✗
AXC B.V.	*.axc.nl.	47,861	✓	✓	⚠+	✗

- **Measured over 18 months** (so no KSK rollover)

Takeaways:

- **Algorithm** and **key sizes** mostly **OK**
- **ZSKs** are mostly 1024-bits (borderline secure) but **are never rolled!**

NLNETLABS

Results for large operators in .se

DNS operator	Master NS†	#Signed	Algorithm	KSK size	ZSK size	ZSK Rollover
Loopia AB	*.loopia.se.	282,604	✔	✔	⚠+	✗
One.com	*.one.com.	221,372	✔	⚠⋆	⚠+	✗
Binero AB	*.binero.se.	123,131	✔	✔	⚠+	✗

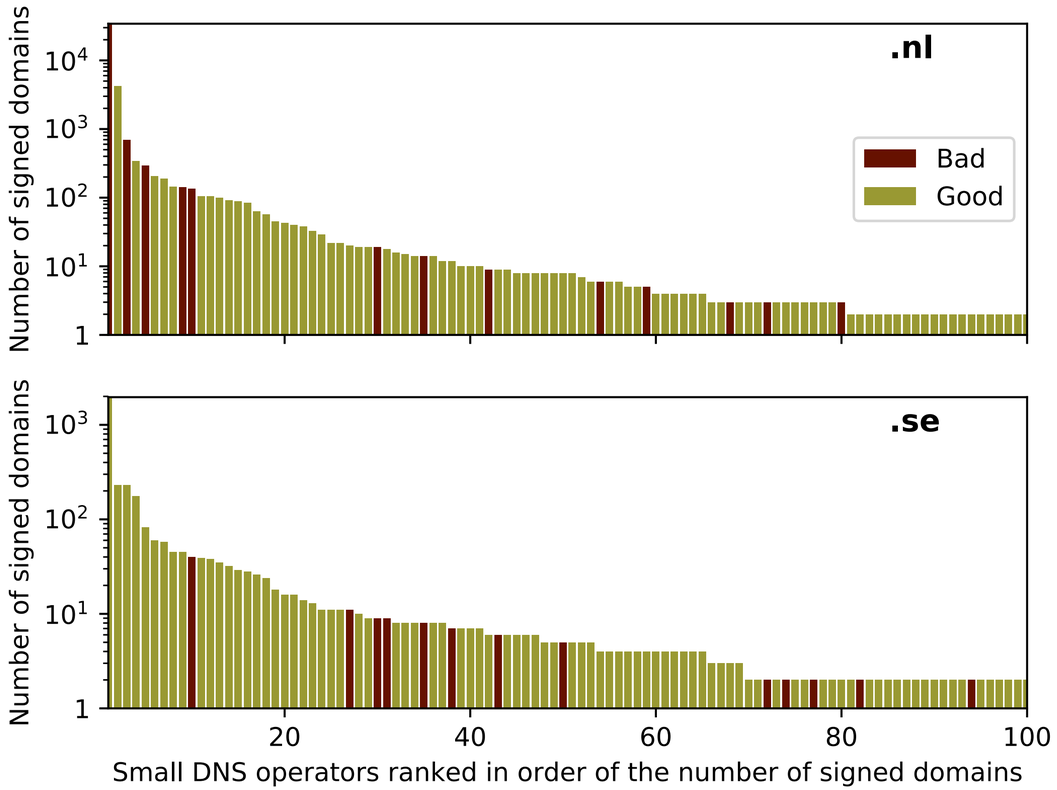
- **Measured over 14 months** (so no KSK rollover)

Takeaways:

- Story **similar to .nl**
- **Algorithm** and **key sizes** mostly **OK**
- **ZSKs** borderline secure but **never rolled!**

NLNETLABS

What about the smaller operators?



.nl

.se

Takeaways: Domains from **small operators much more likely to roll** their **ZSKs properly**

Compliance is **independent of size**

NLNETLABS

Why are large operators not rolling?

- **Are you in the room? I'd love to hear from you!**
- DNSSEC is complex; **rollovers are** arguably **hard and** potentially **risky**
- We know (from private communication) **some** large **operators implement** their **own DNSSEC** signer **systems**
- **Rolling** keys **not a requirement to qualify for the** DNSSEC **incentive**
- **Smart operators** know: **reduce complexity -> reduce** operational **risk**
- No one wants to be called out of bed at 3AM because of a DNSSEC problem

NLNETLABS

I have a theory about .se

- I had a quick look in OpenINTEL last week, for RSA keys in .se:

key size	key type	#dns records	#unique keys
2048	257	651255	202802
2048	256	1841	1839
1024	257	1179	1179
1024	256	1171742	274868

Lots of key sharing

key size	start of key	#keys	
2048	c948a41599cc2d90	321550	**Loopia**
1024	d11791959e2af6ff	321550	
1024	eaf2a4dfbb808f12	321550	
2048	ea37aa563c6e0514	115821	**Binero**
1024	e63c67ebfc23d58a	115821	
1024	d07ba941f50034f5	115821	
2048	c38eb9a20c640dac	9450	**Telia**
1024	ceb092a78cbf7606	9450	
1024	c4cc5c2090f7d69a	9450	
2048	c9efecb5b5815640	917	**Binero**
1024	a1e9a5155ac9be2d	917	
1024	c2a2653d087aeef8	917	
2048	cacfa6615874581c	228	**Swebby**
1024	aac2b639be2a9967	228	
1024	bc231b0f27076953	228	

- Note: **rollovers are** even **trickier when** you're **sharing keys**

NLNETLABS

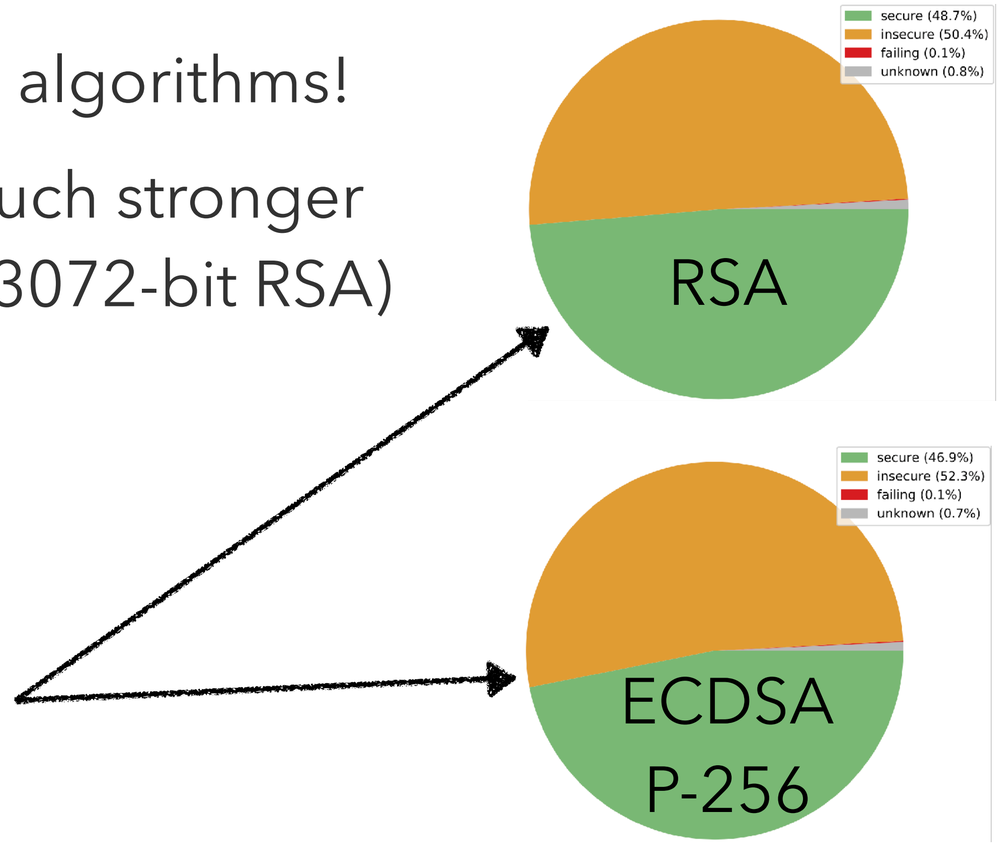
Conclusions

- Incentives got us massive DNSSEC deployment
- But not necessarily secure deployments!
- So perhaps it is time to tighten incentive requirements
- How to do this while keeping operators on board?

NLNETLABS

Recommendations

- Need to account for operational reality; operators want to minimise risk
- One way forward: use Elliptic Curve signing algorithms!
  - Smaller keys that are cryptographically much stronger (e.g. ECDSA P-256 roughly equivalent to 3072-bit RSA)
  - Not rolling a key is not a problem; according to current insights, these keys are good for 30+ years*
  - Widely supported by validating resolvers (source: rootcanary.org)



NLNETLABS

Thank you! Questions?

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland@nlnetlabs.nl

NLNETLABS