DNSSEC usage statistics

and some observations

SEE 5, Tirana

Sergey Myasoedov
20.4.2016

DNSSEC history

- Defined by RFCs 4033-4035 – March 2005
- Root zone signed – July 2010
- March 2011 – the biggest zone .com signed
- New GTLD programme (2013) require to run DNSSEC
- Current state: more than 110 ccTLDs are signed

netart group

DNSSEC principles

Put DNSKEYS in zone

Records signing

Zone publishing

```
zone.   IN SOA ns1.zone. admin@zone.
zone.   IN NS ns1.zone.
zone.   IN NS ns2.zone.

zone.    IN DNSKEY 257 3 10 AwEAbPGd04qzYZmBbhU…
zone.    IN DNSKEY 256 3 10 AwEAAbywQfdma4SxQMn…
zone.    IN RRSIG SOA 10 2 86400 20130619092425 (…
zone.    IN RRSIG NS 10 2 86400 20130619092425 (…
```

netart group

DNSSEC principles

Put DNSKEYS in zone

Records signing

Zone publishing

```
zone.   IN SOA ns1.zone. admin@zone.
zone.   IN NS ns1.zone.
zone.   IN NS ns2.zone.

zone.    IN DNSKEY 257 3 10 AwEAbPGd04qzYZmBbhU…
zone.    IN DNSKEY 256 3 10 AwEAAbywQfdma4SxQMn…
zone.    IN RRSIG SOA 10 2 86400 20130619092425 (…
zone.    IN RRSIG NS 10 2 86400 20130619092425 (…
```

E-mail, web request,
fax, paper letter

Dear root/TLD admin,

Please put our DS record in your zone:
zone. IN DS 64656 10 2 DF8F614B79C
Thank you.

DNSSEC principles

Put DNSKEYS in zone

Records signing

Zone publishing

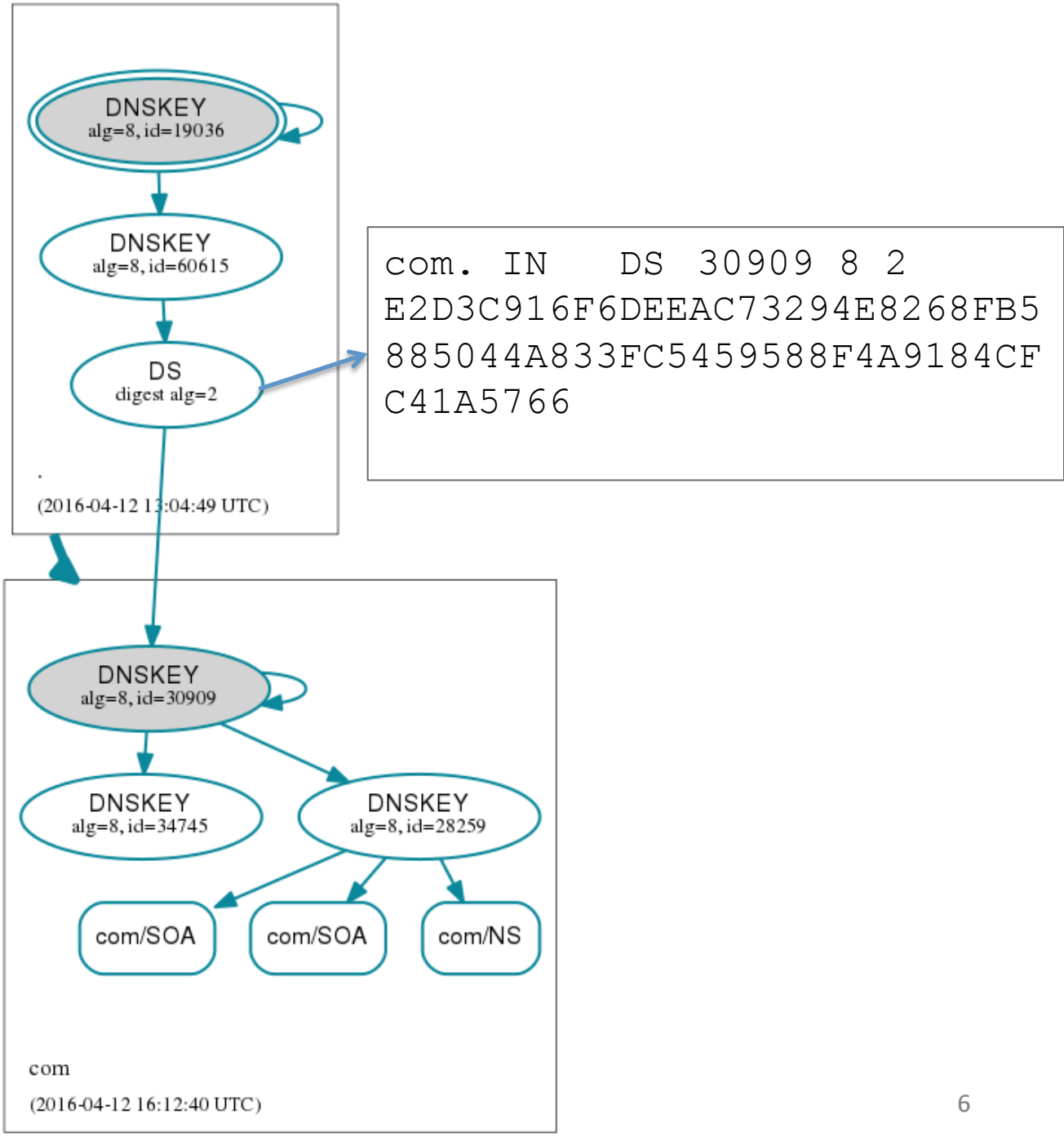
```
zone.   IN SOA ns1.zone. admin@zone.
zone.   IN NS ns1.zone.
zone.   IN NS ns2.zone.

zone.    IN DNSKEY 257 3 10 AwEAbPGd04qzYZmBbhU…
zone.    IN DNSKEY 256 3 10 AwEAAbywQfdma4SxQMn…
zone.    IN RRSIG SOA 10 2 86400 20130619092425 (…
zone.    IN RRSIG NS 10 2 86400 20130619092425 (…
```

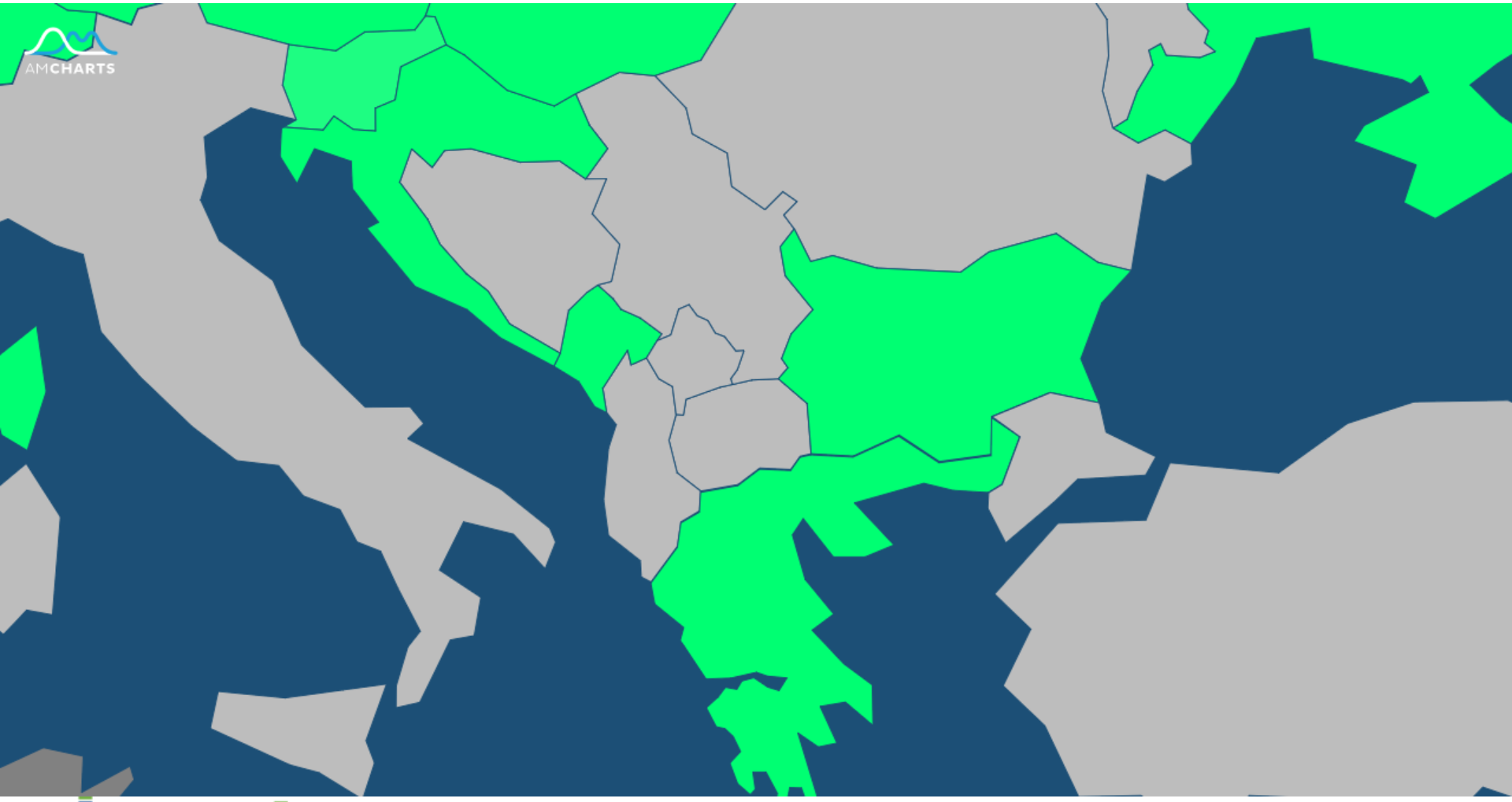
E-mail, web request,
fax, paper letter

Dear root/TLD admin,

Please put our DS record in your zone:
zone. IN DS 64656 10 2 DF8F614B79C
Thank you.


DNSKEY
alg=8, id=19036
DNSKEY
alg=8, id=60615
DS
digest alg=2
.
(2016-04-12 13:04:49 UTC)
com. IN DS 30909 8 2
E2D3C916F6DEEAC73294E8268FB5
885044A833FC5459588F4A9184CF
C41A5766
DNSKEY
alg=8, id=30909
DNSKEY
alg=8, id=34745
DNSKEY
alg=8, id=28259
com/SOA
com/SOA
com/NS
com
(2016-04-12 16:12:40 UTC)

Status of ccTLD implementation of DNSSEC

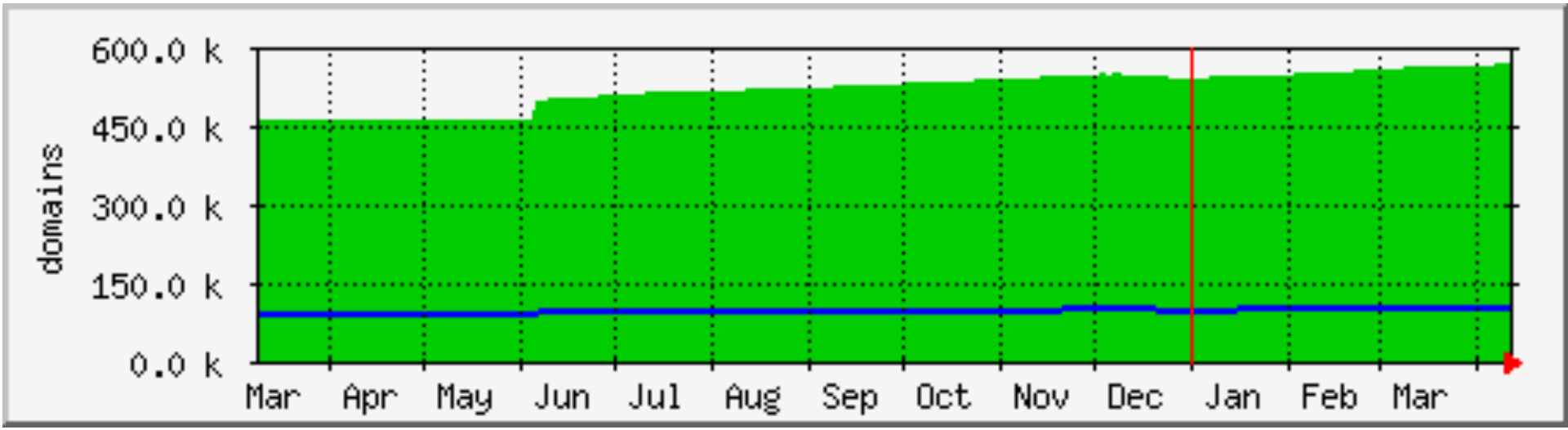


Why to analyze .com zone?

- The biggest zone ever (zone file about 10 Gbytes)
- It's difficult to receive the ccTLDs zones
- Small percentage of DNSSEC-enabled domains
- But the big amount of domains - ~600k
- Different crypto parameters

netart group

.COM / .NET statistics



2016 April's data

.com - 578.000 ds-records

.net - 102.000 ds-records

Digging into .COM

- 580.000 DS-records correspond to 550.000 domain names
- Many of them are signed by a single hoster using the same key
- Some domains have more than 1 digest published
- Some domains are clearly experimental

TOP nameservers (grouped by company)

- 100320 nsX.transip.eu/net/nl
- 64968 nsX.hyp.net
- 47651 [d]ns200.anycast.me
- 17749 *.ovh.net
- 12620 vX.pcextreme.eu
- 9999 nsX.binero.se
- 7015 nsX.webhostingserver.nl
- 5907 nsX.openprovider.eu/be/nl

Selected key parameters

Algorithms:

404091	RSASHA1-NSEC3-SHA1
153004	RSA/SHA-256
13349	RSA/SHA-1
7438	ECDSA Curve P-256 with SHA-256
602	RSA/SHA-512
67	RSA/MD5 (?)
41	DH
37	DSA
33	ECDSA Curve P-384 with SHA-384
24	GOST R 34.10-2001
15	PRIVATEDNS
10	PRIVATEOID
9	DSA-NSEC3-SHA1

Hashes:

403752	SHA-1
174675	SHA-256
175	GOST R 34.11-94
118	SHA-384

netart group

Key re-usage

More than 10.000 domains are signed by a single key of binero.se

That's the perfect example of multiply key usage.

In the ccTLD zones I currently have, that is an extremely RARE situation.

(except .CZ where many registrars are using one key for all its (customers) domains)

.net key parameters

Algorithms:

69033	RSASHA1-NSEC3-SHA1
27128	RSA/SHA-256
6539	RSA/SHA-1
1460	ECDSA Curve P-256 with SHA-256
287	RSA/SHA-512
50	ECDSA Curve P-384 with SHA-384
22	DSA
18	RSA/MD5 (?)
6	GOST R 34.10-2001

Hashes:

77097	SHA-1
27332	SHA-256
69	GOST R 34.11-94
55	SHA-384

netart group

Similar statistics in .net zone

Similar rate of DNSSEC penetration – 97k DNSSEC-enabled domains per 15.6 mil. domains

Same distribution of algorithms and hashes

Similar observation of key re-usage:

2400+ entries of key ID 41182 – it's a key ID of Swedish hoster Binero AB

And the same situation in .org

58k DNSSEC-enabled domains per 10.9 mil. domains

Same distribution of algorithms and hashes; but only SHA-1 and SHA-256 are present

Similar observation of key re-usage:

Binero AB is a leading DNSSEC DNS-service for .net and .org

New GTLDs

- 948 new top-level domains, including IDN
- Admins are obliged to provide access to the zone
- DNSSEC is a necessary condition
- Easy access to zone files

Crypto statistics

From 716 newGTLD:

564 – RSA/SHA-512

127 – RSASHA1-NSEC3-SHA1

18 – RSA/SHA-1

7 – RSA/SHA-512

No GOST. Surprise?

Top new GTLDs

Domains registered:

.xyz – 2665k	.top – 1854k	.wang – 1065k
.win – 886k	.club – 738k	.link – 358k

TOP DNSSEC penetration (GTLDs with 100+ domains):

.ovh – 47%	.amsterdam – 25%
.webcam – 11%	.golf – 9%
.immo – 9%	.brussels – 8%
.sarl – 8%	.taxi – 7%

Top new GTLDs

DNSSEC penetration rate for

the top new GTLDs

is in 0.00% – 0.28% range

Top new GTLDs

The higher penetration rate
(10% - 47%)
is being observed in the TLDs
with 24k - 82k domains

Specific requirements

Some TLD administrators define its own policy on DNSSEC. This policy could affect:

- The WHOIS output
- Allowed algorithms/keylength/hashes etc
- Allowance of key re-usage within the registry

One should take such policies into account

Software for DNSSEC operations

- There are about 10 open source software packages to manage your DNSSEC-enabled zone
- There are also some proprietary solutions
- With the widely deployment of DNSSEC, the number of different tools is growing
- Most of DNS servers have its own utilities
- For the relatively small number of zones, OpenDNSSEC may be the best solution

netart group

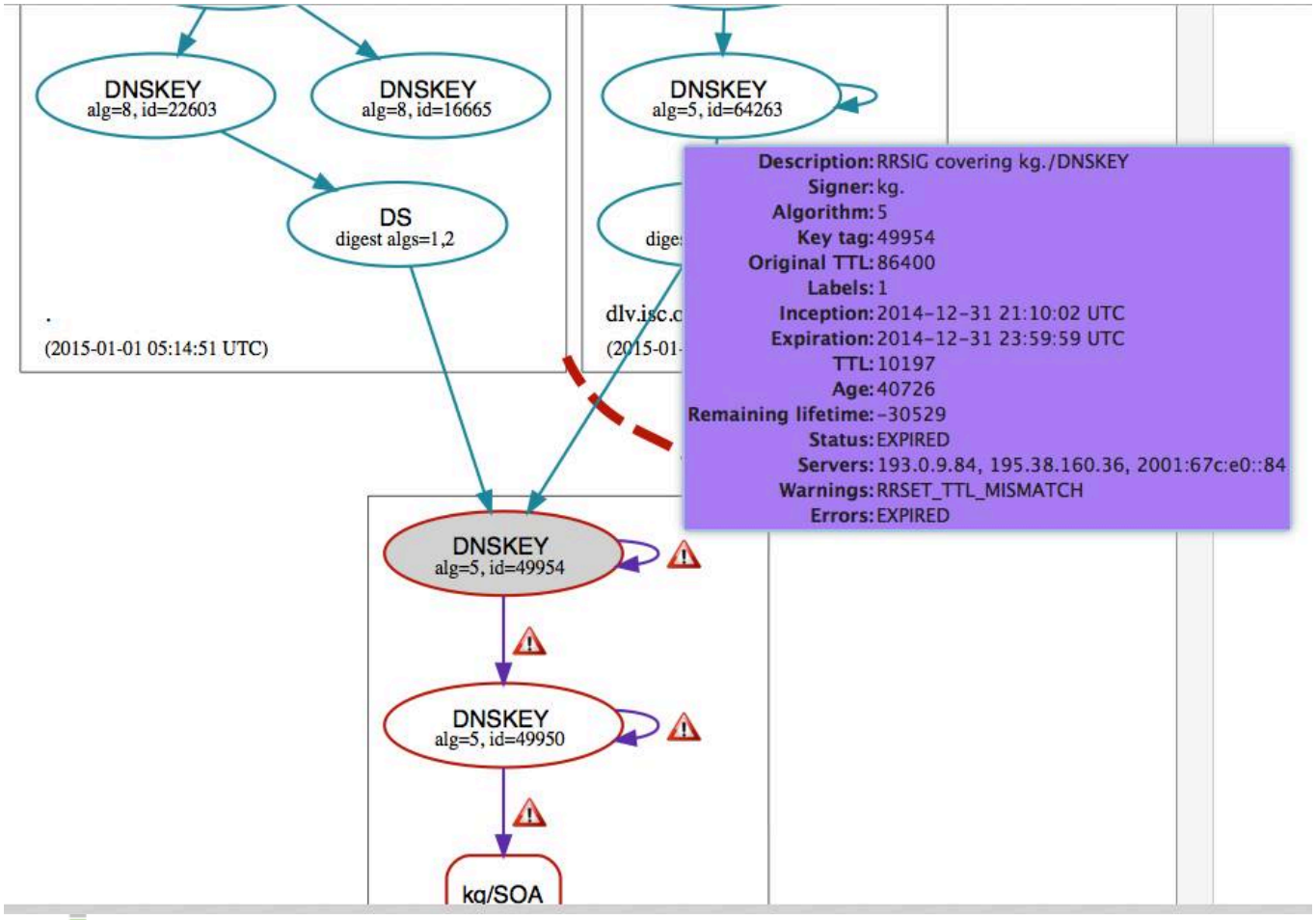
The most common configuration error

The most common configuration error

Expiration of the signature validity

All the trust chains will be broken

The most common configuration error



The most common configuration error

DANE overview

- As we have trusted DNS date with the DNSSEC, we could wish to secure other sensitive data
- So we can put the trust anchor of our website/ mailserver/whatever certificate to our secured DNS zone
- This could be either certificate fingerprint, the whole certificate or pointer to a CA root cert

netart group

Is DANE dead?

The deployment of DANE resource record is tiny.

What could be a reason?

- Low demands from the WEB
- Implementation difficulties?

DANE usage statistics

Not measured because…

Almost nobody is using DANE

MXs is only the DANE field can be useful today

Research by Go6.si is at http://goo.gl/8QcWE1

What could be a killer app?

- Let's encrypt initiative can provide you a valid recognized certificate for your domain name
- This certificate can be published in DNS using DANE
- Then this certificate can be used to encrypt all information exchange of your server
- There will be two possibilities to check the trust chain: classic with the certificate storage and DANE

netart group

Questions?

LinkedIn.com/in/myasoedov

netart group