Změna algoritmu podepisování zóny .cz

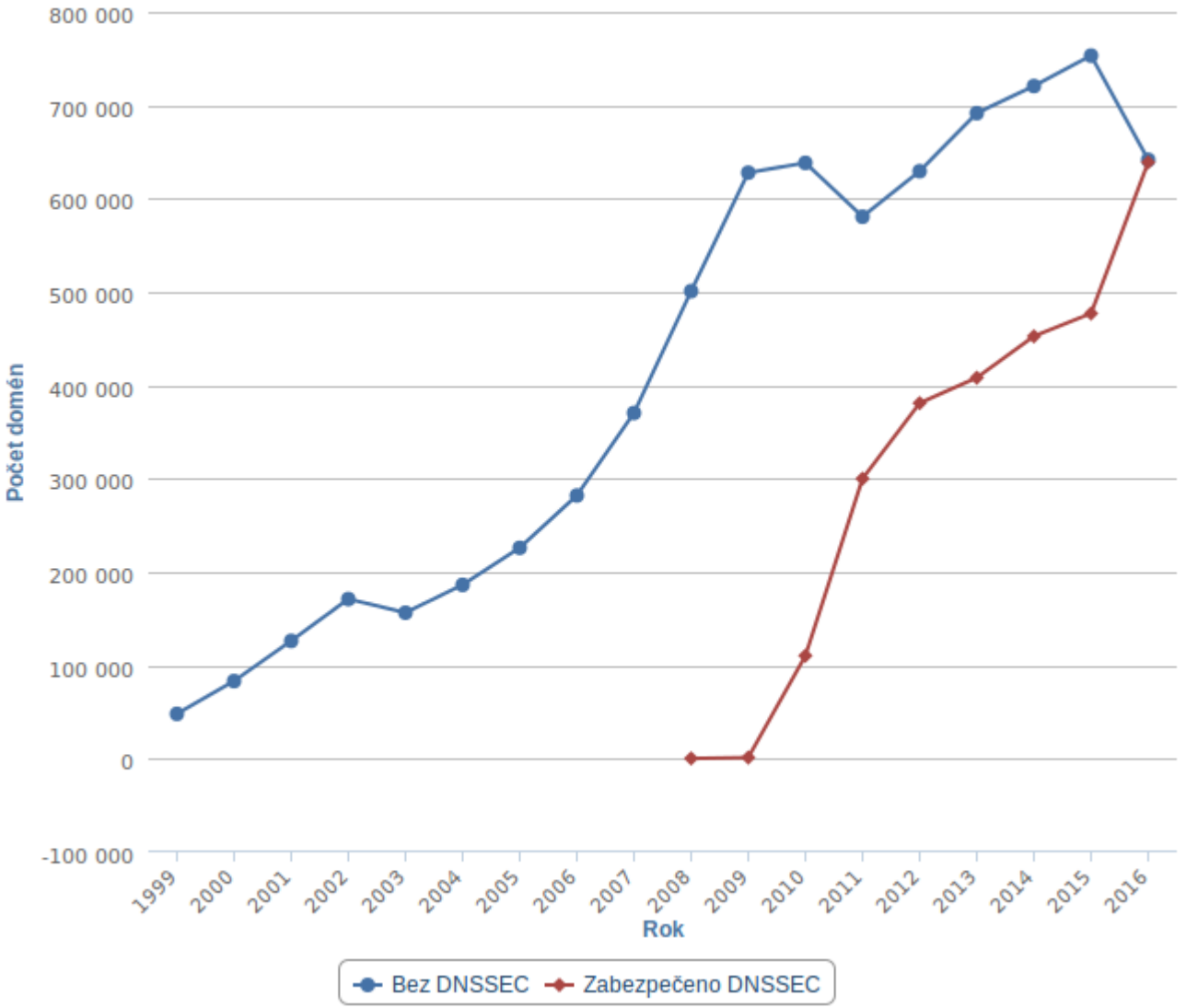
Zdeněk Brůna • zdenek.bruna@nic.cz • 3.12.2016

Obsah

- Stav DNSSEC
- Eliptické křivky
  - Co to vlastně je?
  - Co to znamená pro DNSSEC?
  - Proč je chceme?
  - Prerekvizity zavedení
  - Stav zavádění pro .cz zónu
- Výměna kořenového klíče

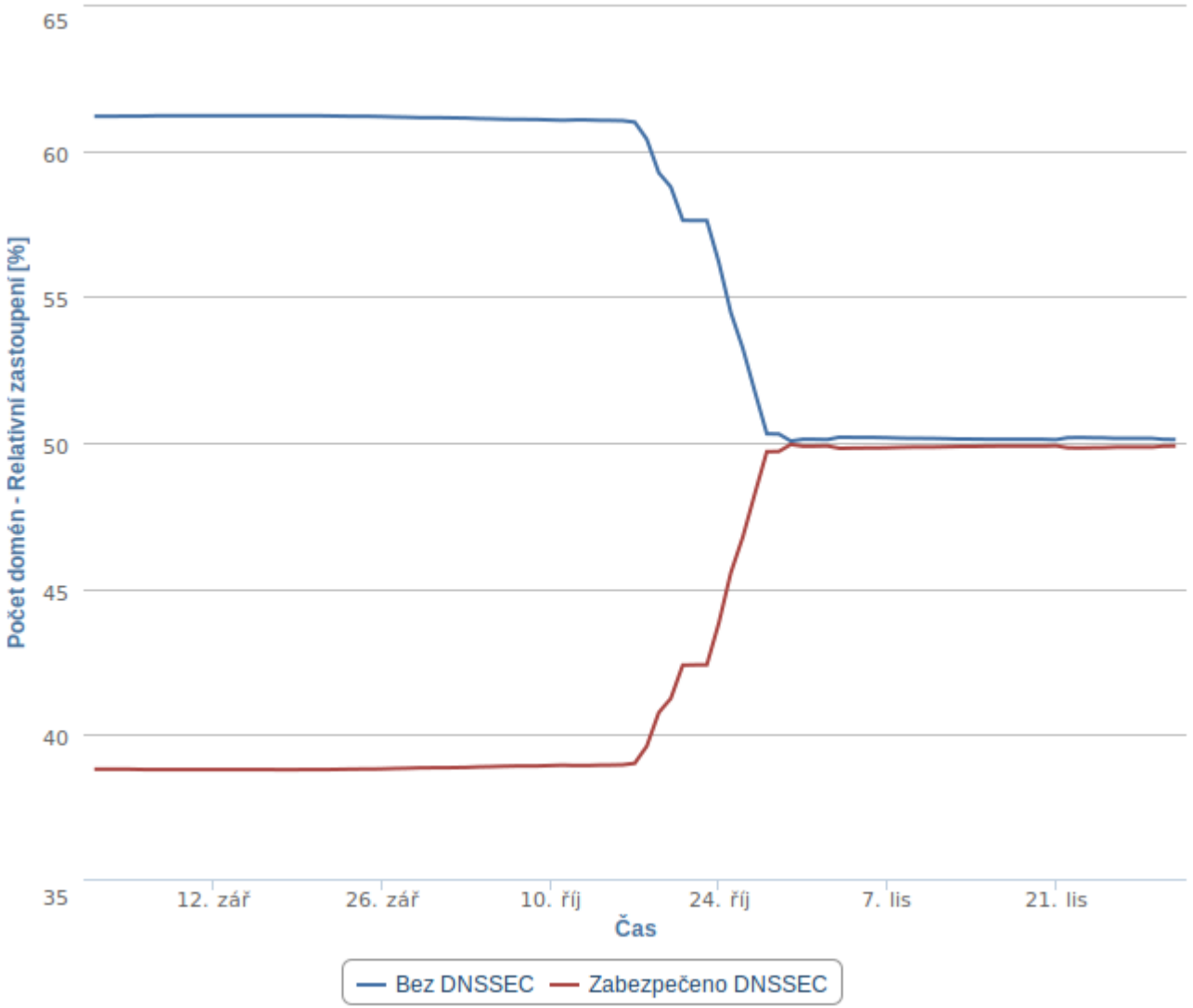
Stav DNSSEC

Počet zabezpečených domén



Stav DNSSEC

Podíl zabezpečených domén



chybí jen 2794 domén!

Stav DNSSEC

.cz vs. ccTLDs a tradiční gTLDs

Počet domén s DNSSEC		
Pořadí	**TLD**	**Počet**
1	.nl	2 551 923
2	.br	953 771
3	.se	659 664
4	**.cz**	**638 849**
5	.com	605 839
6	.no	413 943
7	.eu	356 138
8	.fr	294 100
9	.be	124 193
10	.net	101 321

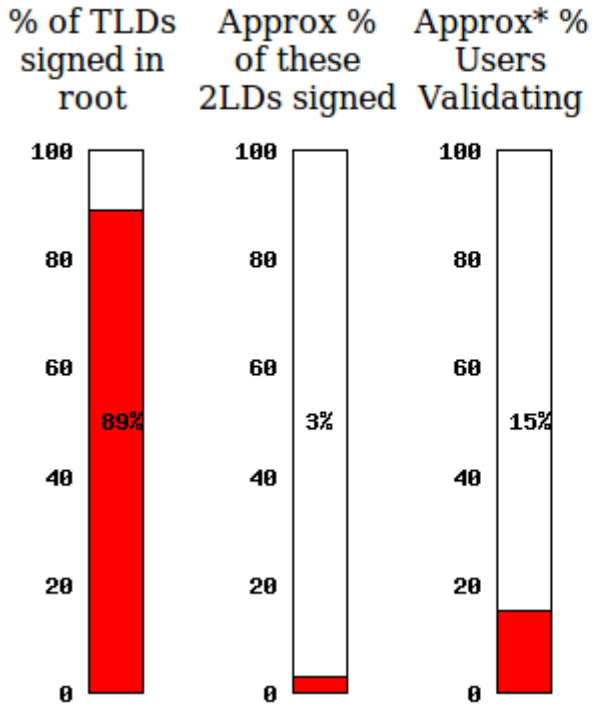
% domén s DNSSEC		
Pořadí	**TLD**	**%**
1	.no	58,21%
2	**.cz**	**49,89%**
3	.se	46,59%
4	.nl	45,02%
5	.br	10,58%
6	.fr	9,85%
7	.eu	9,29%
8	.be	8,01%
9	.lv	2,77%
10	.pt	1,53%

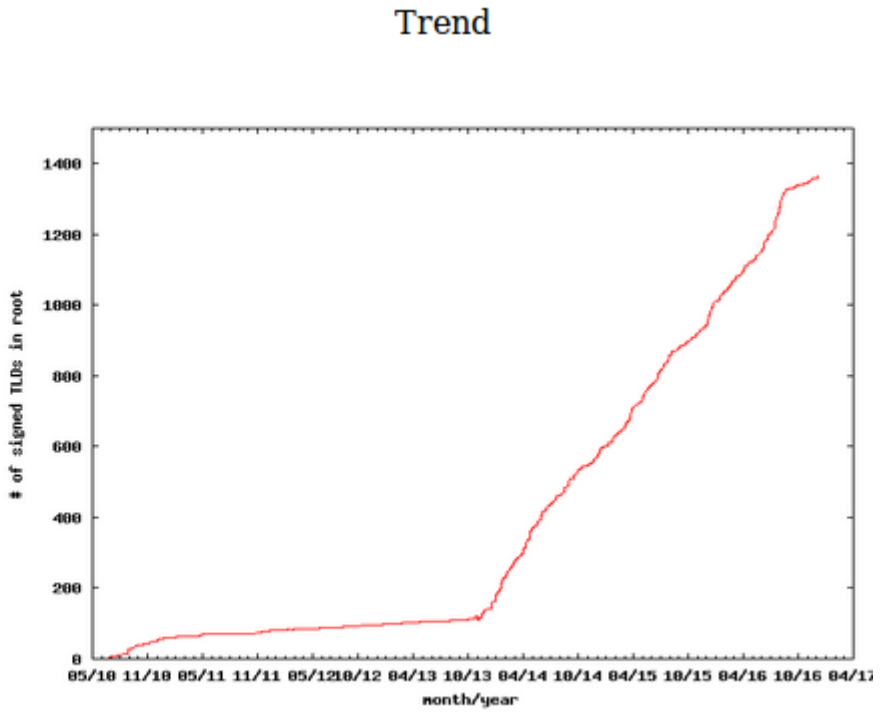
k 1.12.2016

zdroje: statistiky CENTR, registro.br, statdns.com

Stav DNSSEC

Podpora ve světě





zdroj: https://rick.eng.br/dnssecstat/

Eliptické křivky

Co to vlastně je?

- využívá ECC namísto RSA
  - co je stejné
    - asymetrické šifrování (privátní a veřejný klíč)
    - princip trapdoor ~ „padací dveře“

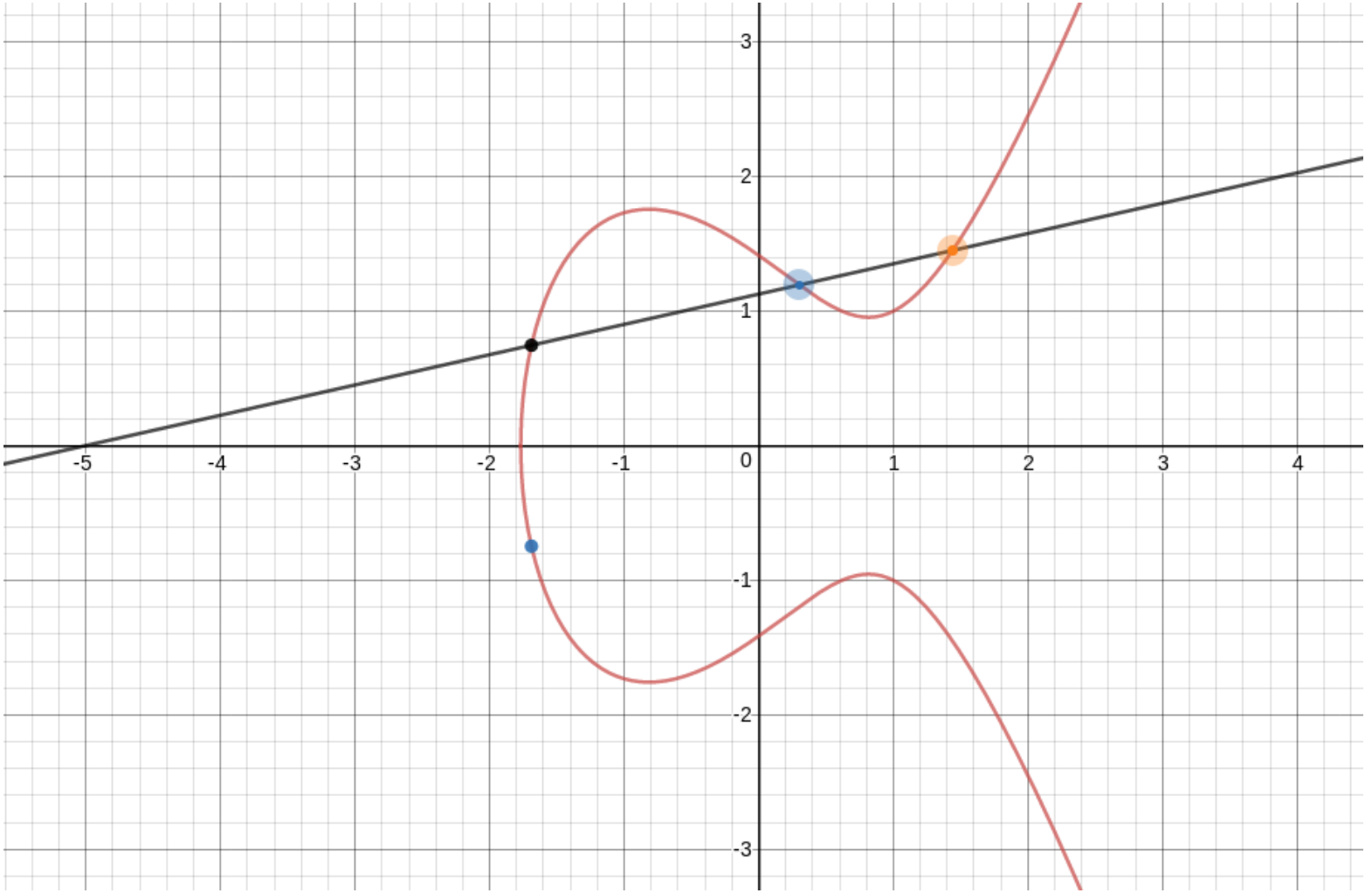
$$A \rightarrow B \neq B \rightarrow A$$

  - rozdíly
    - RSA (rozkládání velkého čísla na součin prvočísel)
    - ECC (hledání diskrétního logaritmu náhodného elementu eliptické křivky s ohledem na známý základní bod)

Eliptické křivky

Co to vlastně je?

$$y^2=x^3+ax+b$$



Eliptické křivky

Co to znamená pro DNSSEC?

- ECDSA ~ Elliptic Curve Digital Signature Algorithm
- RFC6605 (duben 2016)
- dva nové DNSSEC algoritmy
  http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
  - ECDSAPSHA256 (alg13)
  - ECDSAPSHA384 (alg14)
- nejsou založeny na RSA, ale na ECC (Elliptic Curve Cryptography)
- https://blog.apnic.net/2016/10/06/dnssec-and-ecdsa/

Eliptické křivky

Proč je chceme?

- **bezpečnost** (velikost klíče vs. odolnost klíče)
  - ECDSA P-256 ~ RSA 3072 (stejná síla)
  - Nyní máme:
    - ZSK:1024b
    - KSK: 2048b

      => budeme odolnější
  - menší velikost DNS odezev (menší výkon pro reflection útoky)

Eliptické křivky

Proč je chceme?

- provozní aspekty pro zónu
  - velikost zóny:
    - RSASHA512 – 796M
    - ECDSAP256SHA256 – 634M (**-20%**)
  - rychlost podepisování:
    - dle dostupných studií se zvýší
    - prověřujeme

Eliptické křivky

Proč je chceme?

- další impuls pro upgrade DNS resolverů
  - některé starší verze DNS ECDSA nepodporují
  - provozovatelé neupgradují
  - příležitost upoutat na nutnost upgradu pozornost (zvýšit podporu DNSSEC na resolverech)

každá druhá vs. **každý třetí**

Eliptické křivky

Prerekvizity zavedení

- prověření nových postupů
  - v roce 2010 jsme přecházeli z RSASHA1 na RSASHA512
  - opět nejde pouze o rotaci klíčů, ale o změnu algoritmu!

=> **dvojí podepsání zónového soubory obojími algoritmy**

- BIND, KNOT resolver a poslední Unbound jsou OK
- starší verze Unbound (do října 2015) jsou příliš striktní a bez dvojího podepsání zónového souboru tuto označí jako „BOGUS“
- není velký problém, jen je zóna 2 x větší na nějaký čas (testujeme)

Eliptické křivky

Prerekvizity zavedení

- podpora ECDSA v DNS resolverech
  - resolvery nepodporující ECDSA vrací odpověď jako „INSECURE“, ne jako „BOGUS“
  - stará verze Dnsmasq ale „BOGUS“ vrací
    - od verze 2.72 (září 2014)
    - opraveno ve verzi 2.75 (červenec 2015)
  - testujeme, jak moc s tím mohou být problémy

Eliptické křivky

Prerekvizity zavedení

- podpora ECDSA v DNS resolverech
  - RIPE atlas sondy
  - Turris (zatím jen úvahy)
  - APNIC měření (Geoff Huston)
    http://stats.labs.apnic.net/ecdsa

Eliptické křivky

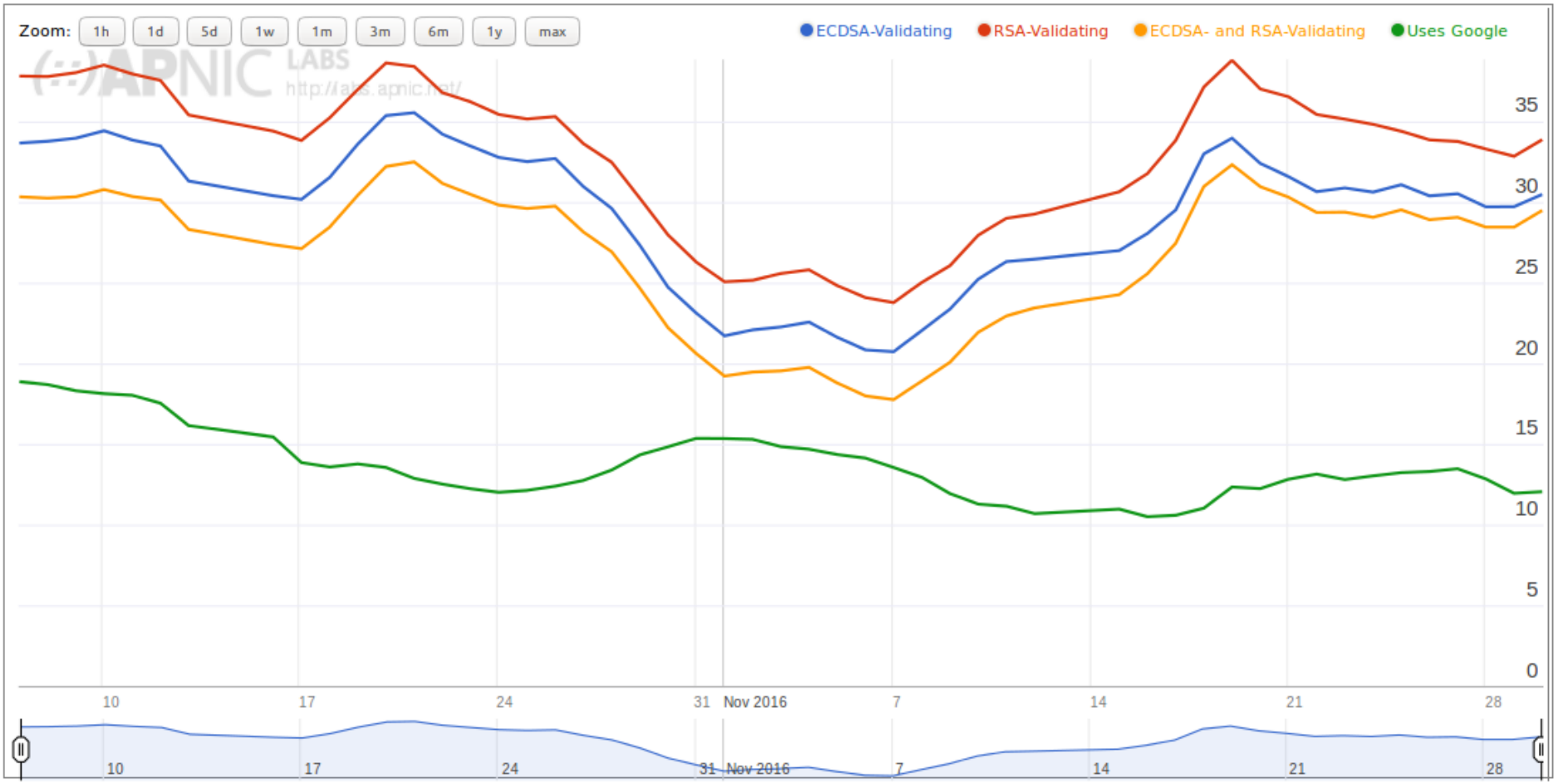
Prerekvizity zavedení

- podpora ECDSA v DNS resolverech

Eliptické křivky

Prerekvizity zavedení

Use of DNSSEC-ECDSA Validation for Czech Republic (CZ)



Eliptické křivky

Prerekvizity zavedení

- podpora ECDSA v DNS resolverech (pro CZ)

Společnost	Validuje ECDSA	Validuje RSA	Validuje RSA, ECDSA	Podíl ECDSA:RSA	Vzorků
INTERNET CZ	0,03%	0,03%	0,03%	100,00%	95 230
O2	33,54%	34,22%	31,77%	97,99%	66 685
UPC	9,29%	10,76%	7,80%	86,34%	37 016
STARNET	94,59%	92,75%	88,94%	100,00%	36 534
T-MOBILE	89,79%	90,55%	83,18%	99,16%	11 535
VODAFONE	1,59%	69,18%	1,24%	2,29%	8 195
CDT	20,14%	68,13%	16,20%	29,56%	7 810
GTS	52,61%	54,20%	43,83%	97,07%	6 493
DIAL TELECOM	26,14%	26,43%	22,13%	98,94%	6 051

Eliptické křivky

Prerekvizity zavedení

- IANA a její (ne)podpora
  - Root Zone Management v aktuální verzi nepodporuje DS záznamy s ECDSAP256SHA256!
  - zavedení podpory zamrzlo v průběhu přechodu dohledu od min. obchodu USA na ICANN komunitu
  - mělo by změnit Root Zone Evolution Review Committee
  - zatím se trošku tápe (odpovědnosti, kompetence)

Eliptické křivky

Stav zavádění pro .cz zónu

- začali jsme u sebe
  - ECDSA využito pro cca 90 interních SLD
  - zatím žádné problémy
- probíhá informování veřejnosti
  - konference
  - blogposty
  - komunikace s ISP
- další se přidávají
  - více jak 30 000 .cz domén již ECDSA využívá
  - ZONER od 1.12. pro všechny své domény

Eliptické křivky

Stav zavádění pro .cz zónu

- přehled používaných algoritmů pro .cz domény (2.12.2016)

Algoritmus	Popis	Počet domén	% domén
5	RSA/SHA-1	370 288	57,96%
7	RSASHA1-NSEC3-SHA1	186 596	29,21%
10	RSASHA512	40 798	6,39%
13	ECDSAP256SHA256	30 711	4,81%
8	RSASHA256	10 473	1,64%
14	ECDSAP384SHA384	15	0,00%
2	DH	10	0,00%
6	DSA-NSEC3-SHA1	1	0,00%
1	RSAMD5	1	0,00%

Eliptické křivky

Stav zavádění pro .cz zónu

- Historie šifrovacích algoritmů pro .cz zónu
  - 2008 – 2010 RSA SHA-1 (alg. 5)
  - 2010 – 2017 RSA SHA-512 (alg. 10)
  - 2017 - ? ECDSA P256 SHA-256 (alg. 13)

Eliptické křivky

Stav zavádění pro .cz zónu

- widget
  - na www.nic.cz
  - ukazuje nově i podporu ECDSA
  - javascript pro začlenění do vašich stránek na: https://labs.nic.cz/cs/ipv6-widget.html

- revidujeme postup rotace KSK pro .cz (se změnou algoritmu)
- zavedeme potom, co bude ECDSA podporováno IANA

Výměna kořenového klíče

O co jde?

- výměna KSK kořenové zóny
- KSK je součástí řetězu důvěry (validace DNSSEC)
- současný KSK se používá od prvního podpisu kořenové zóny (2010)
- výměna z důvodu „kryptografické hygieny“
- plán https://www.icann.org/resources/pages/ksk-rollover
- důležitá data:
  - nový KSK vygenerován 27.10.2016
  - únor 2017 – nový KSK k dispozici pro vývojáře DNS SW
  - nový KSK bude publikován v DNS 11.07.2017
  - nový KSK začne podepisovat kořenovou zónu **11.10.2017**
  - revokace starého KSK 11.1.2018

Výměna kořenového klíče

Co byste si měli pohlídat?

- pevný bod důvěry (trust anchor) v DNSSEC validátoru
  - pokud máte automatickou změnu trust anchor povolenu, proběhne změna automaticky (RFC 5011)
  - pokud ne, musíte změnit ručně
- **prověřte včas svoje DNSSEC validující resolvery**
- sledujte průběh výměny kořenového klíče (ICANN)

  (nebo alespoň sledujte nás)

Výměna kořenového klíče

Připravenost DNS serverů

- konfigurace se v čase mění
  - dříve statická
  - dnes dynamická (s podporou RFC 5011)
- právo zápisu do souboru, kde je uložen klíč (pro uživatele pod kterým běží resolver)

=> upgrade (ECDSA, RFC 5011) a důkladná kontrola konfigurace!

- **Prezentace z posledního ICANN**

KNOT RESOLVER
http://schd.ws/hosted_files/icann572016/16/Jaromir-Talir-CZNIC-KNOT-RESOLVER.pdf
BIND
http://schd.ws/hosted_files/icann572016/16/Mukund-Sivaramanbind-managed-keys-icann57.pdf
UNBOUND
http://schd.ws/hosted_files/icann572016/49/Jaap-Akkerhuis-Unbound-KSK-rollover.pdf

Shrnutí

- **zaveďte do svých DNS resolverů podporu ECDSA!**
- **implementujte automatickou změnu trust anchor!**

- **zaveďte podporu DNSSEC!**

Děkuji za pozornost

Zdeněk Brůna • zdenek.bruna@nic.cz