DOM REG [.lt]

DNSSEC diegimas paslaugų teikėjams

KTU IPC

Kaunas, 2022-12-01

DNSSEC istorija

- 1997 m. – pirmas RFC, veikimo principai nepasiteisino
- 2005 m. – esminis atnaujinimas, naujas RFC
- 2010 m. – DNSSEC įjungimas . (*root*) zonoje
- 2013 m. – DNSSEC įjungimas .lt
- 2013 m. – DNSSEC validavimą aktyvuoja Google (8.8.8.8)
- …
- 2022 m. – DNSSEC naudojamas **0,7%** .lt domenų

DOM REG [.lt]

DNSSEC yra sudėtingas protokolas

DOM REG [.lt]

DNSSEC yra sudėtingas protokolas operatoriui

DOM REG [.lt]

DNSSEC iššūkiai: ZSK + KSK

- KSK – ilgas, keičiamas retai
- ZSK – trumpesnis, keičiamas dažnai

DOM REG [.lt]

DNSSEC iššūkiai: periodinis pasirašymas

- DNSSEC parašai turi galiojimo laiką
- DNSSEC pasirašyta zona, nors jos turinys nesikeičia, privalo būti periodiškai atnaujinama

DOM REG [.lt]

DNSSEC iššūkiai: TTL

- Aktyvuojant DNSSEC: pirmiausia zoną pasirašyti savo DNS serveryje, vėliau kelti DS įrašus
- Deaktyvuojant DNSSEC: pirmiausia pašalinti DS įrašus, vėliau išjungti pasirašymą savo DNS serveryje

DOM REG [.lt]

DNSSEC iššūkiai: TTL

- TTL – parašų įrašams (RRSIG)
- TTL – raktų įrašams (DNSKEY)
- TTL – delegavimo įrašams

DOM REG [.lt]

DNSSEC iššūkiai: paslaugų teikėjo keitimas

- Esamam paslaugų teikėjui nesiimant jokių veiksmų DNSSEC naudojančio domeno veikimas gali sutrikti (iki DS TTL laiko)

DOM REG [.lt]

DNSSEC iššūkiai: DNS paketo dydis

- RSA raktai ilgi:
  - RSA 2048 DNSKEY įrašas – apie 260 baitų

DOM REG [.lt]

DNSSEC nauda

- DNSSEC + HTTPS 😃
- HTTPS 😀
- DNSSEC + HTTP 😞
- HTTP 😔

DOM REG [.lt]

DNSSEC nauda: DANE

- 2012 m. – *DNS-Based Authentication of Named Entities (RFC)*

- **SSL sertifikatai DNS**

DOM REG [.lt]

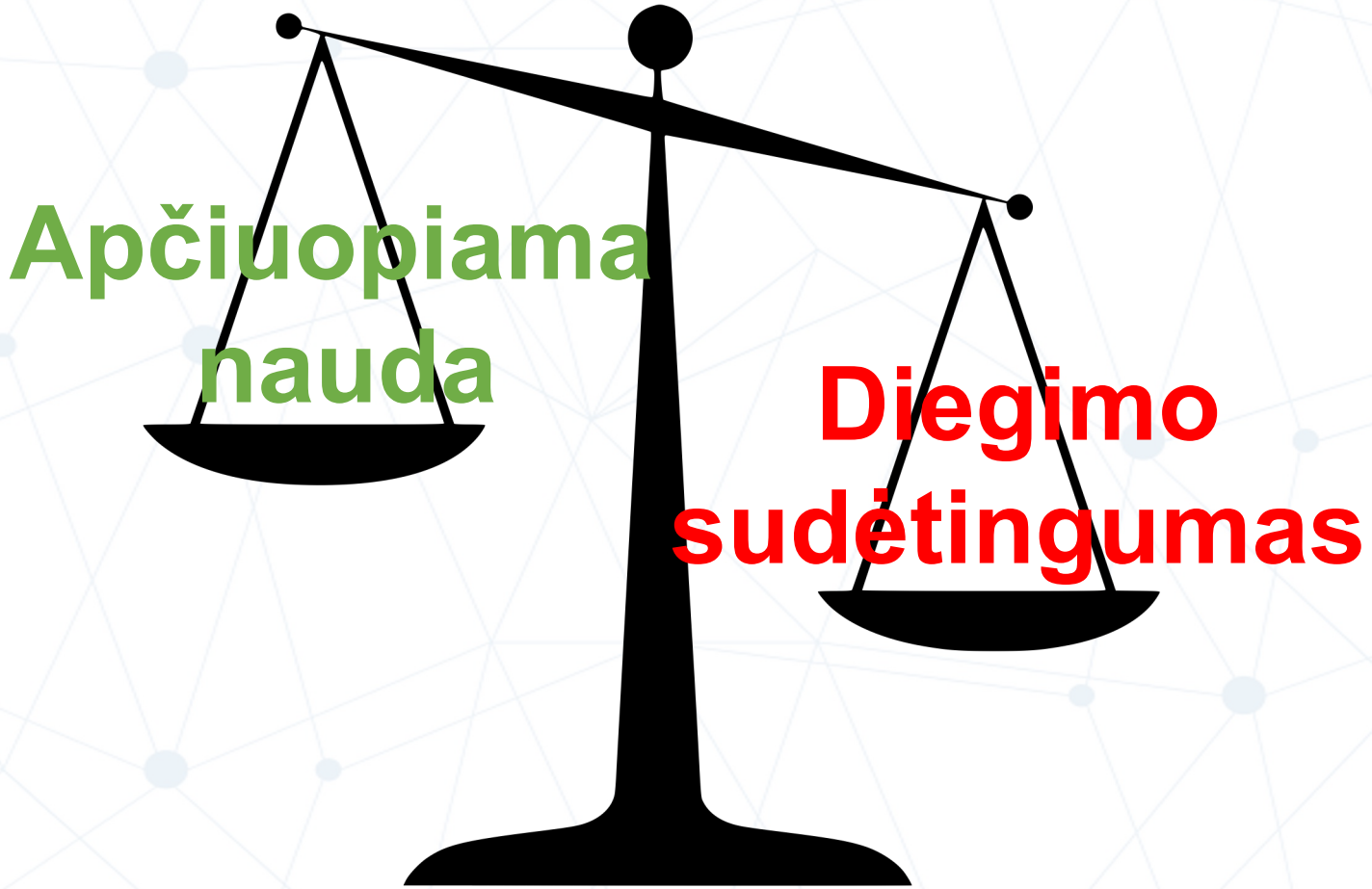
DNSSEC nauda: DANE

- 2015 m. - *Let‘s Encrypt* pradeda išdavinėti nemokamus SSL sertifikatus
- 2019 m. – vis dar nėra naršyklių palaikančių DANE

*„...DANE, as an authentication option, is effectively **dead** for the Web for the foreseeable future.“* 2019m., APNIC

DOM REG [.lt]

DNSSEC diegimas



DOM REG [.lt]

DNSSEC raktai

ZSK + KSK ≈ CSK

DOM REG [.lt]

DNSSEC raktų keitimas

„3. It should only be done when it is known or strongly suspected that the key can be or has been compromised, or in conjunction with operator change policies and procedures, like when a new algorithm or key storage is required.“

RFC6781

DOM REG [.lt]

DNSSEC periodinis pasirašymas

- Pasirinkti pakankamą parašų galiojimo laiką – bent savaitę.
- Periodiškai (ir atlikus pakeitimą) pasirašyti visą zoną – bent kelis kartus dažniau nei galioja parašai.

DOM REG [.lt]

DNSSEC trumpi raktai

ECDSA P-256 rakto parašai apie keturis kartus trumpesni nei RSA 2048, o jų kriptografinis stiprumas prilygsta RSA 3072.

DOM REG [.lt]

DNSSEC trumpi raktai

*„…is ECDSA a viable crypto algorithm for use in DNSSEC today? In our opinion these results indicate that, sadly, the answer is “**no**”.“*

2014 m., Geoff Huston

DOM REG [.lt]

DNSSEC trumpi raktai

*„Is ECDSA P-256 ready for use? In my view, this data is now telling us "**Yes**!"."*

2018 m., Geoff Huston

DOM REG [.lt]

DNSSEC raktai: bendras ar atskiras zonai

„Since the keys are all placed in the same storage a key compromise of one key will make all keys compromised. So having different keys for all zones don't make much sense in this sense.“

OpenDNSSEC blog

DOM REG [.lt]

DNSSEC: paslaugų teikėjo keitimas

- Papildomas naujo paslaugų teikėjo DS įrašas
- Keitimo metu išjungti DNSSEC (pašalinti delegavimo DS įrašus)

DOM REG [.lt]

DNSSEC: patarimai

- Pasirinkite paprastesnį diegimo sprendimą
- Validuokite sugeneruotas zoną
- Papildykite stebėsenos sistemas DNSSEC tikrinimu
- Pradėkite lėtai – *opt-in*

DOM REG [.lt]

AČIŪ

- dnssec-signzone, dnssec-keygen, dnssec-dsfromkey
- ldns-signzone, ldns-keygen, ldns-key2ds
- OpenDNSSEC
- validns
- unbound-host
- zonemaster (https://zonemaster.iis.se)
- https://dnsviz.net
- https://dnssec-analyzer.verisignlabs.com/

DOM REG [.lt]