SIDN

Your world. Our domain.

ONE Conference 2019

Current State and Development of DNS Security and Privacy (part 1: DNSSEC)

Marco Davids

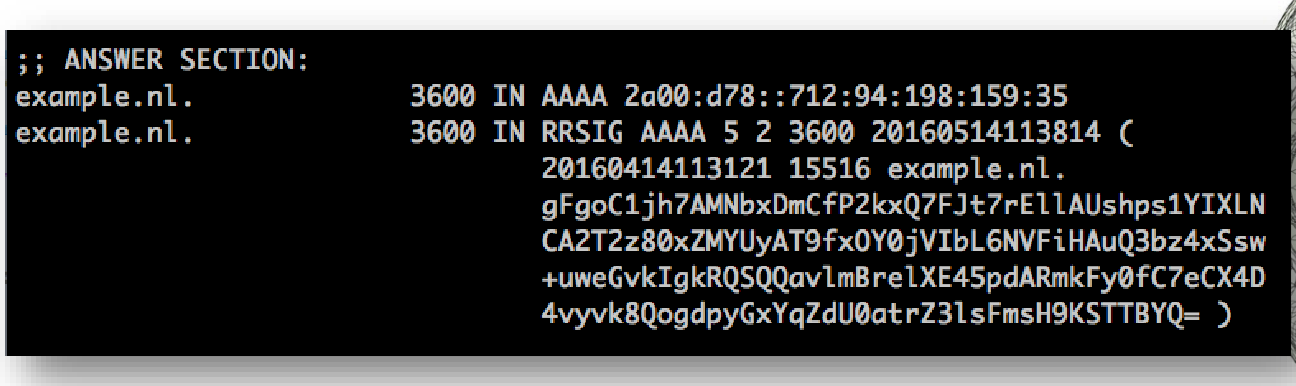
2 October 2019

DNSSEC – adding a security layer to DNS

- DNS was developed in 1983
- Still a key component in the core of the internet
- Critical shortcoming: vulnerable to manipulation and forgery
  - Kaminsky attack / cache pollution / cache poisoning / DNS spoofing

DNSSEC

- Answers from the DNS are digitally signed
  - Public-key cryptography
- Answers can be authenticated by (validating) resolver
- Provides data integrity (and origin authentication)
  - But not confidentiality / privacy (but wait for it, there's more in this session)



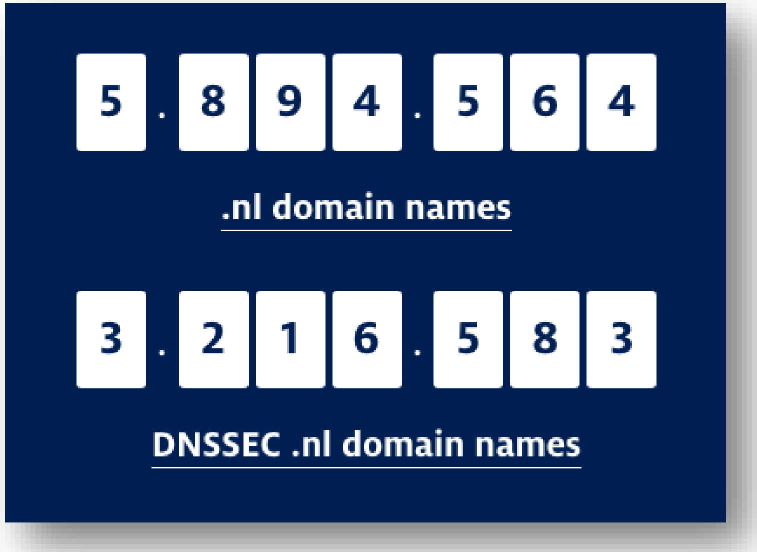
```
;; ANSWER SECTION:
example.nl.             3600 IN AAAA 2a00:d78::712:94:198:159:35
example.nl.             3600 IN RRSIG AAAA 5 2 3600 20160514113814 (
                                20160414113121 15516 example.nl.
                                gFgoC1jh7AMNbxDmCfP2kxQ7FJt7rEllAUshps1YIXLN
                                CA2T2z80xZMYUyAT9fxOY0jVIbL6NVFiHAuQ3bz4xSsw
                                +uweGvkIgkRQSQQavlmBrelXE45pdARmkFy0fC7eCX4D
                                4vyvk8QogdpyGxYqZdU0atrZ3lsFmsH9KSTTBYQ= )
```

CERTIFICATE • OF • AUTHENTICITY • CERTIFICATE • OF • AUTHENTICITY •

DNSSEC

- Enabler to make existing protocols better/more secure
  - DKIM, SPF, DMARC
  - CERT-records (RFC4398), SSHFP (RFC5255), IPSECKEY (RFC4025)
  - CAA (RFC6844)
  - DANE / TLSA (RFC6698 and RFC7672)
    - TLS trust anchors

DNSSEC



5.894.564

.nl domain names

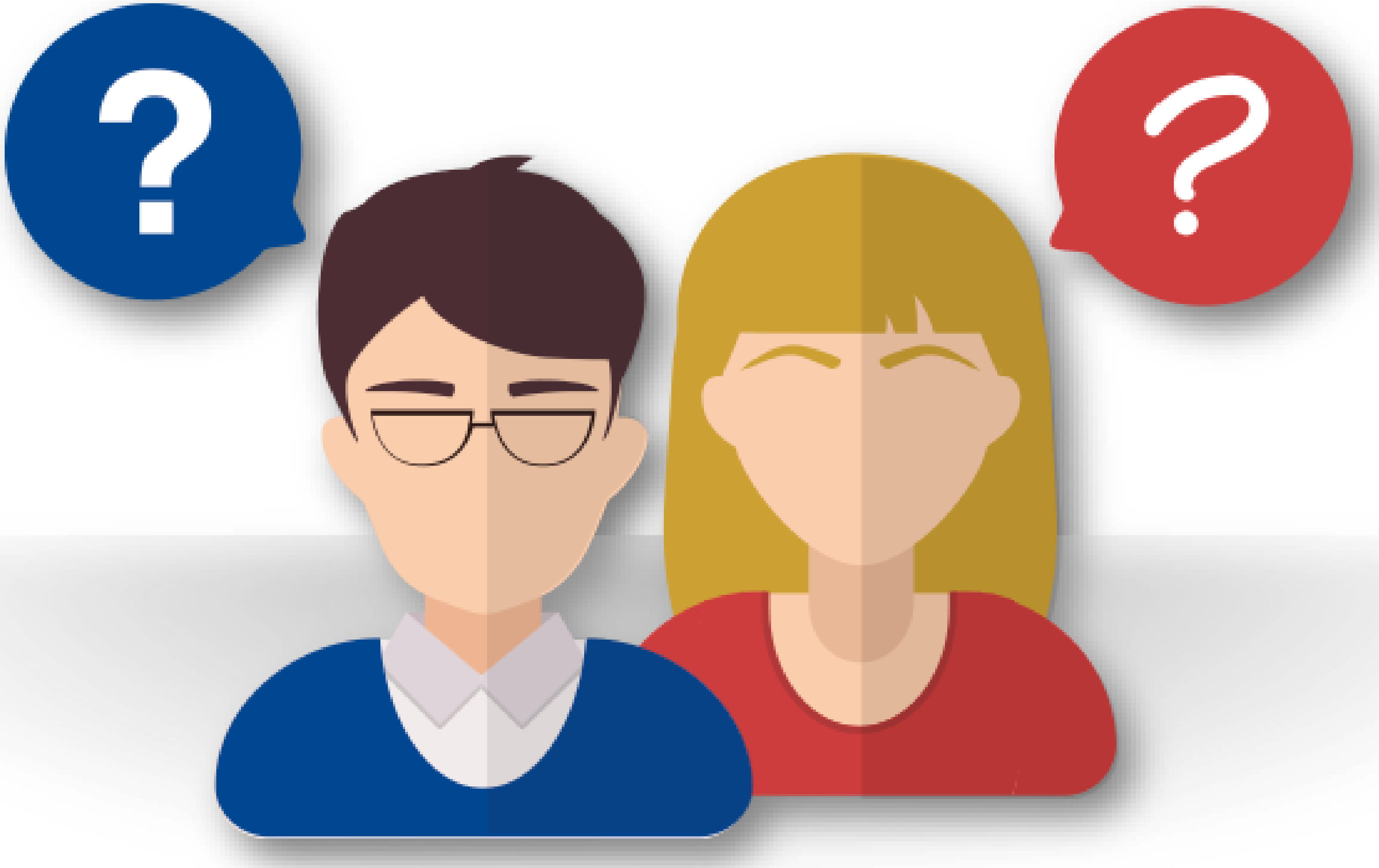
3.216.583

DNSSEC .nl domain names

- Enabled in the root zone since 2010
  - Also enabled in .nl zone since 2010
- Good support in software and services
  - BIND, Unbound, PowerDNS, Knot, Microsoft, Secure64, InfoBlox, etc.
  - Also, Public DNS resolvers offer support (1.1.1.1, 8.8.8.8, 9.9.9.9 etc.)
- Signing is popular in .nl zone[1]
  - Only 0.08% bogus
  - Not so much elsewhere…
  - Validation also still a bit of a challenge in many places[2]
  - Check it on https://en.internet.nl/

1) https://stats.sidnlabs.nl/en/dnssec.html 2) https://stats.labs.apnic.net/dnssec/XA

Questions ?



Thanks!

SIDN LABS