DNSSEC
в корпоративных сетях
и ISP

Сергей Мясоедов

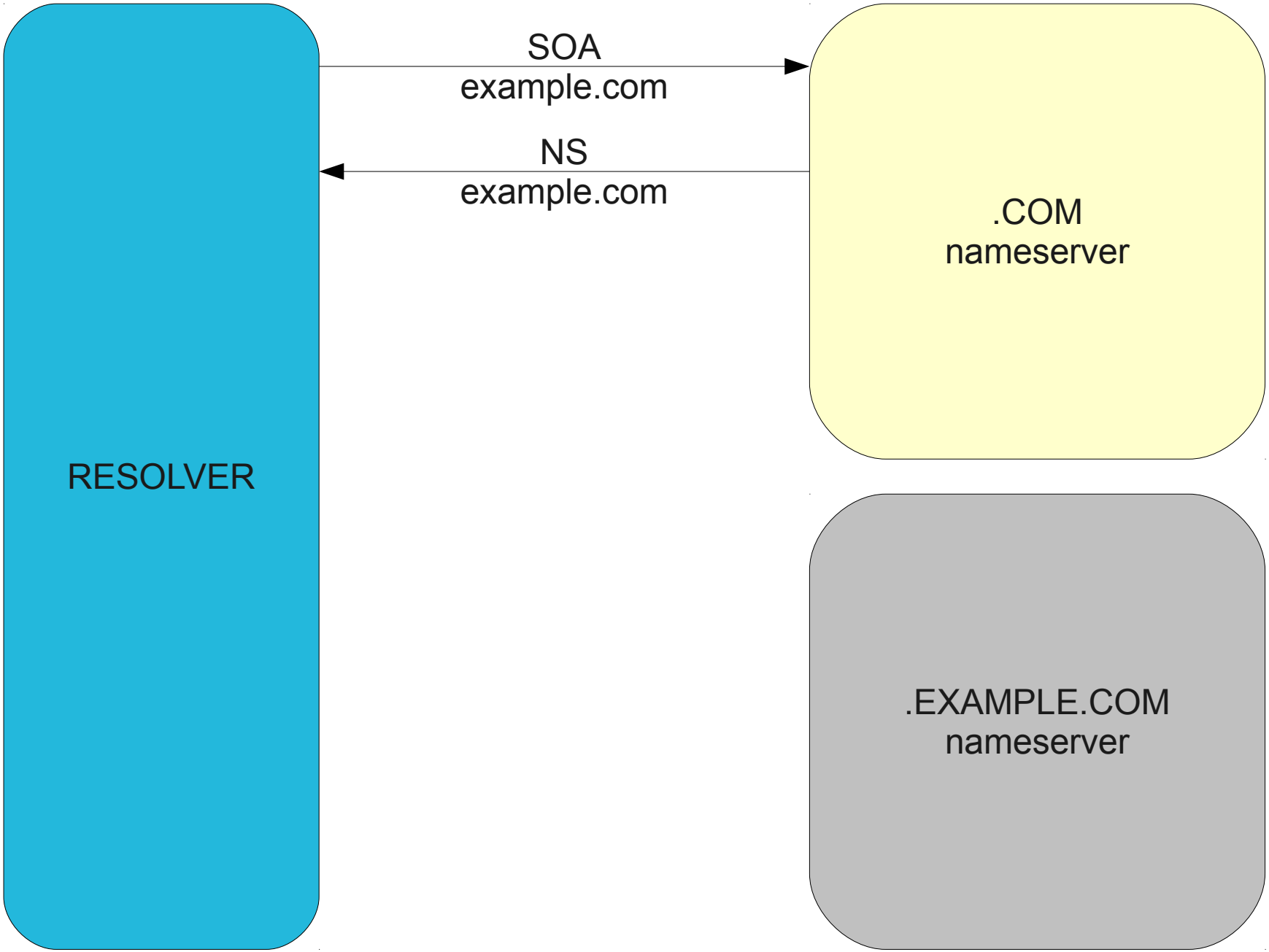
Москва, 7.6.2011

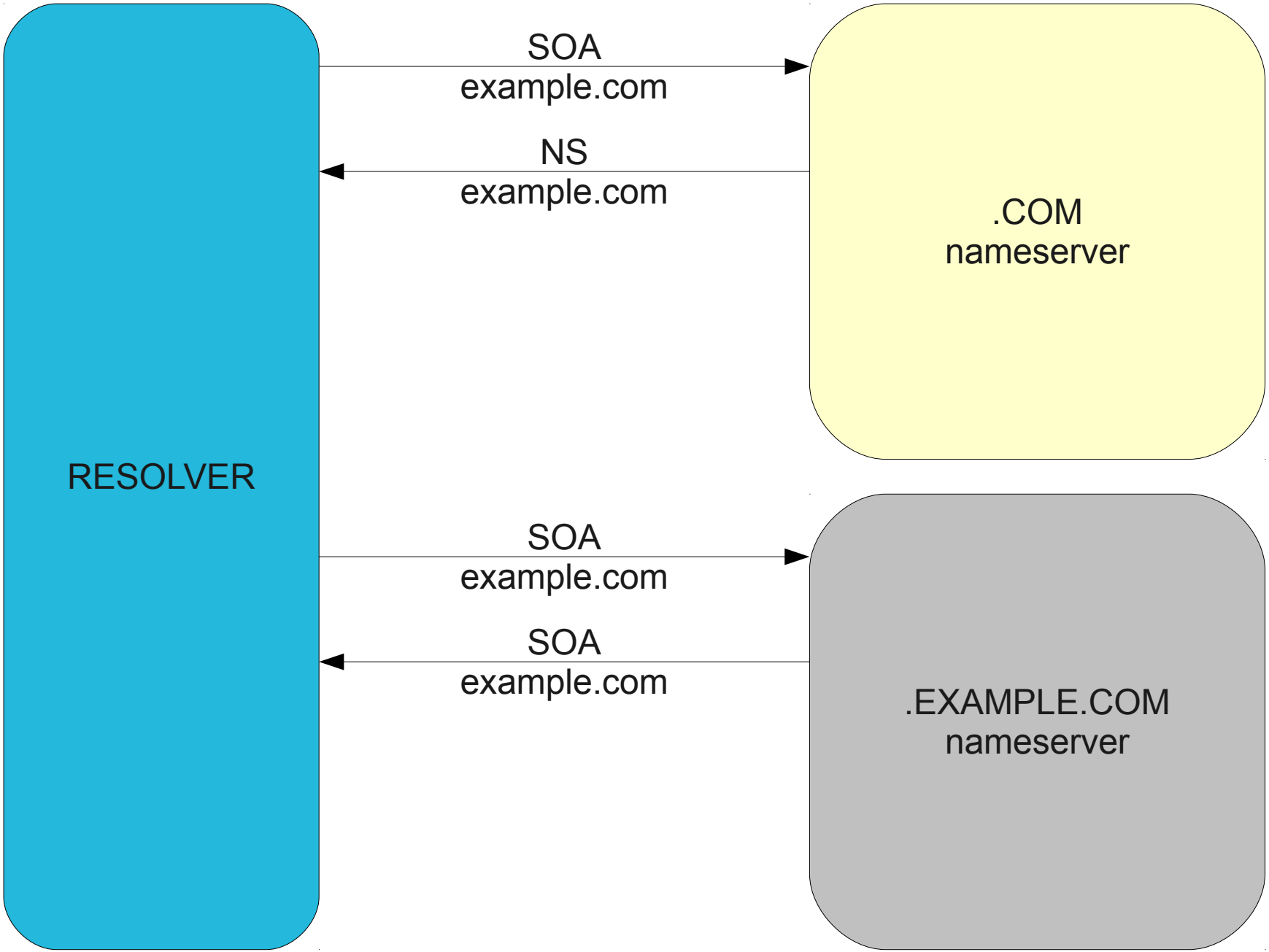
Цель:

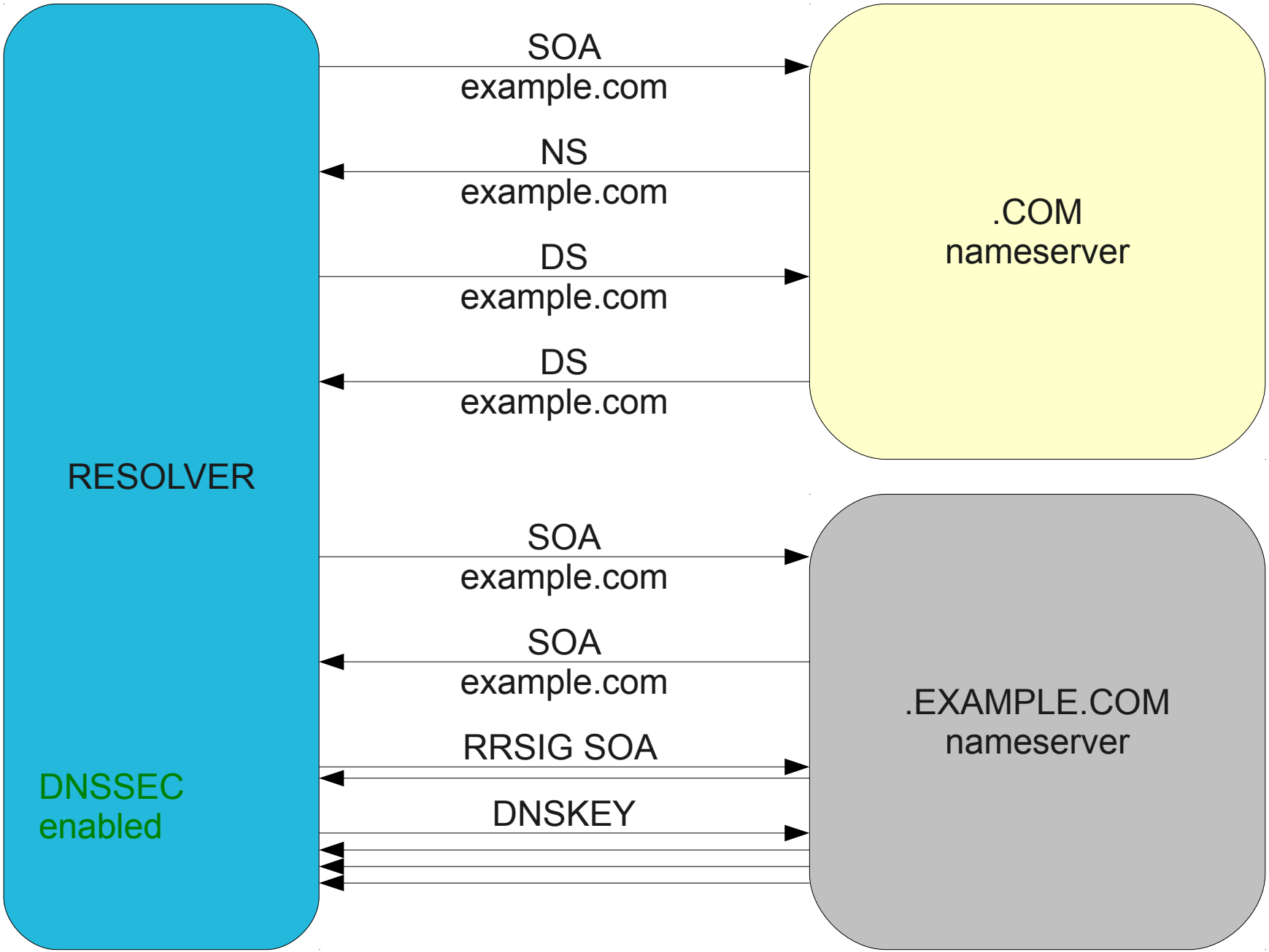
валидация данных, передаваемых в DNS-записях (RR)

Методы:

- Сервер верхнего уровня знает о ключе, которым подписываются данные уровнем ниже
- Данные о ключах (DS-records) на верхний уровень передаются **не средствами DNS:** это работа регистраторов доменов
- NS-серверы не занимаются валидацией, это задача клиентских резолверов


SOA
example.com
NS
example.com
RESOLVER
.COM
nameserver
.EXAMPLE.COM
nameserver


SOA
example.com
NS
example.com
.COM
nameserver
RESOLVER
SOA
example.com
SOA
example.com
.EXAMPLE.COM
nameserver


SOA
example.com
NS
example.com
DS
example.com
DS
example.com
.COM
nameserver
RESOLVER
SOA
example.com
SOA
example.com
RRSIG SOA
DNSKEY
.EXAMPLE.COM
nameserver
DNSSEC
enabled

Криптография реализована только в текстовых записях в зонах и в клиентских резолверах

Проверка валидности подписи лежит на резолвере:

- подпись невалидна – клиенту выдается NXDOMAIN
- невозможно проверить подпись (отсутствие DS-RR в TLD, неизвестный алгоритм) – выдается запись без флага AD

```
; <<>> DiG 9.7.3 <<>> +adflag A gosuslugi.ru
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
gosuslugi.ru.           10800   IN      A       109.207.1.97

; <<>> DiG 9.7.3 <<>> DNSKEY gosuslugi.ru
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; ANSWER SECTION:
gosuslugi.ru.               IN      DNSKEY  256 3 5 AwEAAbVUdleYuWEdyEh9n...
gosuslugi.ru.               IN      DNSKEY  257 3 5 AwEAAdEo8A7hM7OXfSLxc...
```

```
; <<>> DiG 9.7.3 <<>> +adflag www.root-dnssec.org
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 0
;; ANSWER SECTION:
www.root-dnssec.org.  86400   IN  A   208.77.188.126

; <<>> DiG 9.7.3 <<>> DNSKEY root-dnssec.org
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; ANSWER SECTION:
root-dnssec.org.      IN  DNSKEY  256 3 5 BQEAAAABnO2bzsGvfFcWahycSR7igGpqCuY...
root-dnssec.org.      IN  DNSKEY  257 3 5 BEAAAAPWujWRLYUW4Yp9fIluNZuCrZlo7cA...
```

Включение валидации DNSSEC в BIND9:

```
trusted-keys {
  "." 257 3 8
    "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
     FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
     bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
     X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
     W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
     Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
     QxA+Uk1ihz0=";
};
options {
        dnssec-validation yes;
        };
```

Trusted-key берётся из корневой зоны (ftp.internic.net)

BIND4, BIND8, DLV – устарели!

Возможные проблемы

Не касаются резолверов:

- срок жизни ключа (ZSK) истёк и зону не переподписали
- рассинхронизация данных в TLD и на NS-сервере зоны (KSK rollover, ...)

Во всех случаях резолвер выдаст NXDOMAIN (host/record not found)

Решение: зоны, подписанные DNSSEC следует держать у надёжного хостера с мониторингом и поддержкой

Касаются резолверов:

- задержки разрешения имён :-(

Решение: тесты, сравнения, обновление ПО (Bind10?, Unbound)

Выводы

Включать DNSSEC на резолверах – следует!
(устойчивость перед атаками на кэш)

Выводы

Включать DNSSEC на резолверах – следует!
(устойчивость перед атаками на кэш)

Подписывать собственную зону при возможности у TLD – желательно, особенно тем, у кого IT-инфраструктура в зоне риска (платёжные системы, банки и т.п.)

Выводы

Включать DNSSEC на резолверах – следует!
(устойчивость перед атаками на кэш)

Подписывать собственную зону при возможности у TLD – желательно, особенно тем, у кого IT-инфраструктура в зоне риска (платёжные системы, банки и т.п.)

Контролировать работу DNSSEC при помощи браузера – легко!

Прикладной контроль DNSSEC

DNSSEC Validator
(www.dnssec-validator.cz)

Firefox plugin:

Вопросы?

kaa@net-art.cz