DNSSEC: проблемы и перспективы развития

Антон Басков,
RIPE NCC

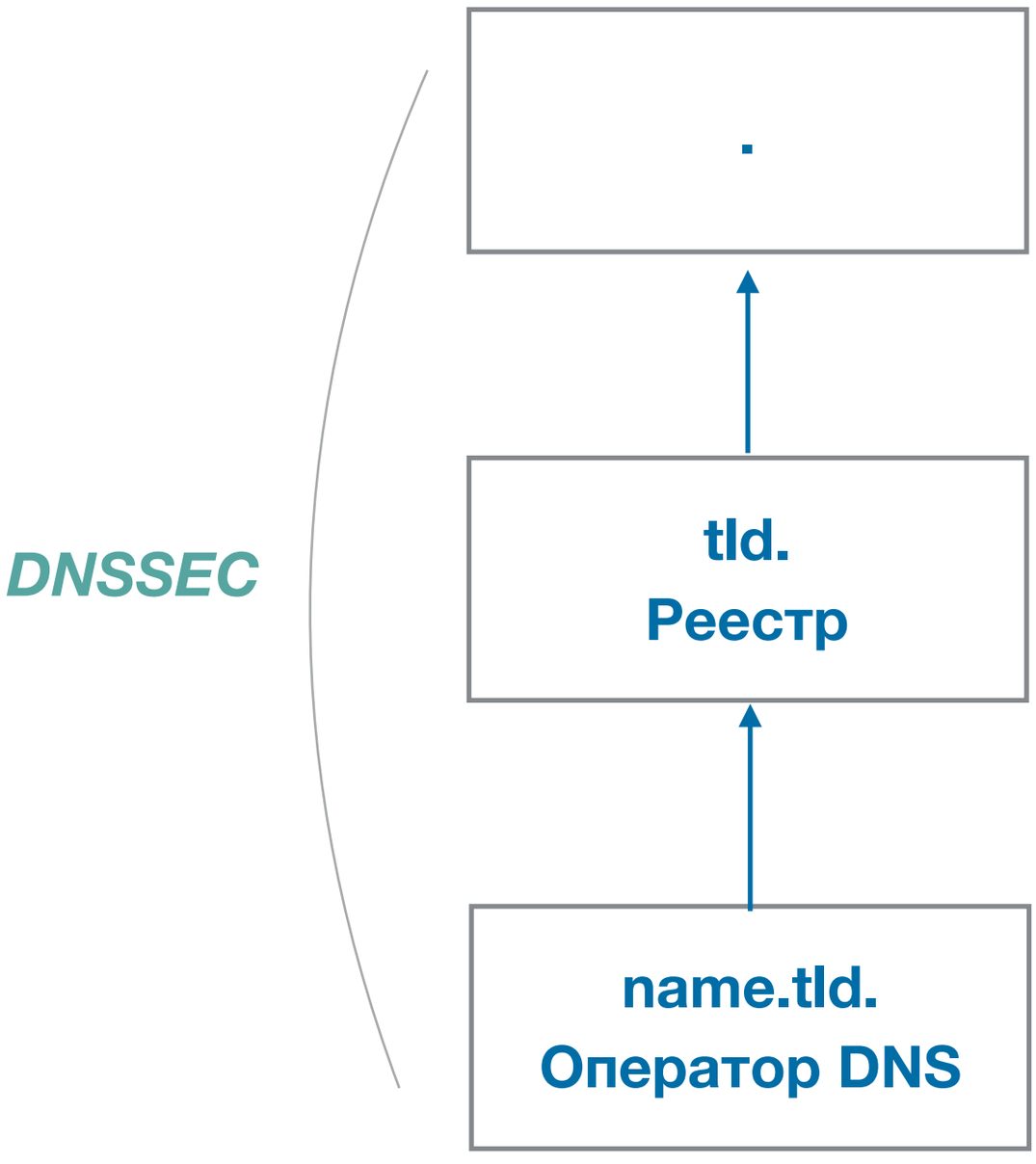
Ереван, 10 сентября 2015

Обновление зоны верхнего уровня

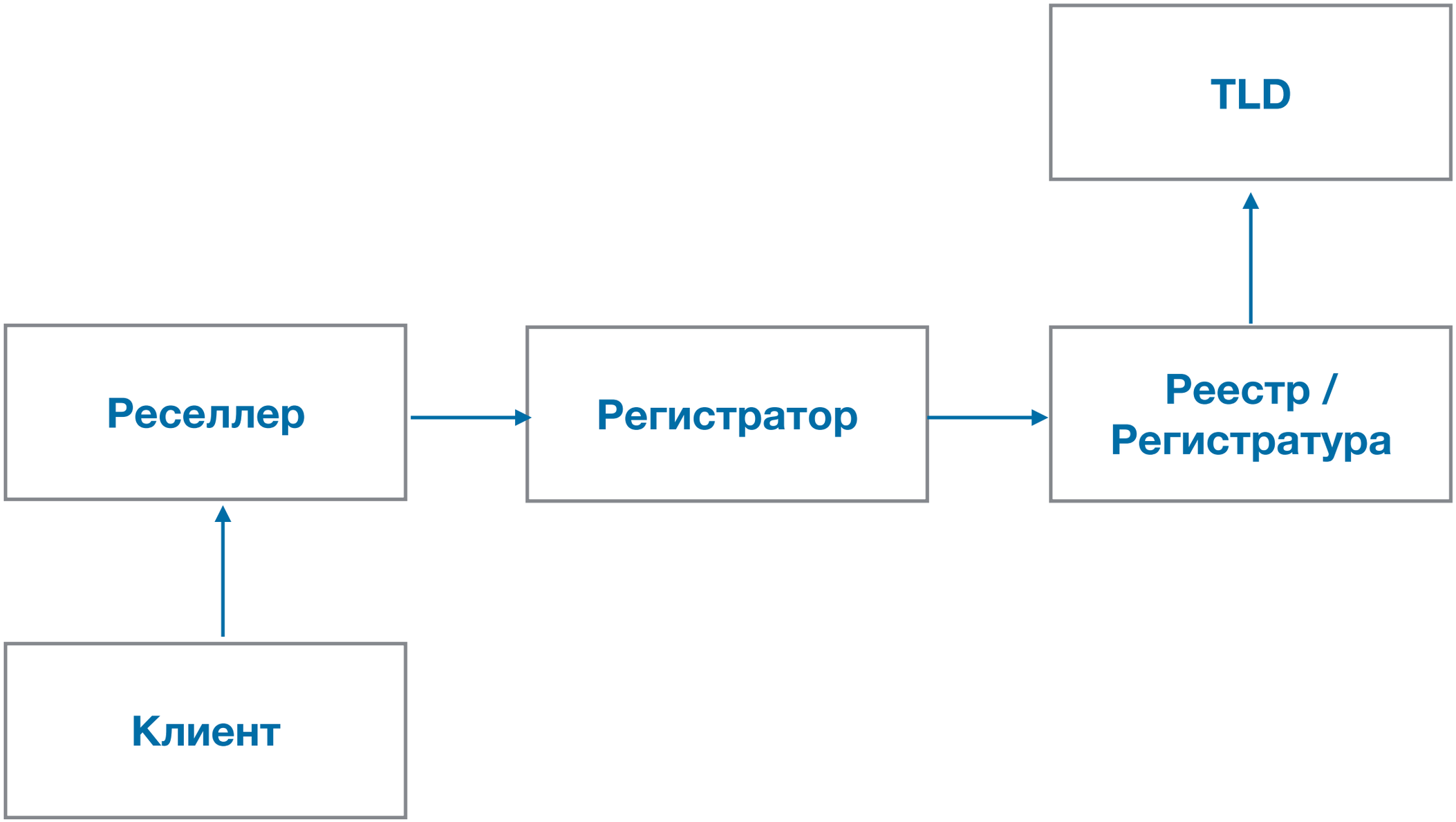
… без участия регистратора и регселера

Ереван, 10 сентября 2015

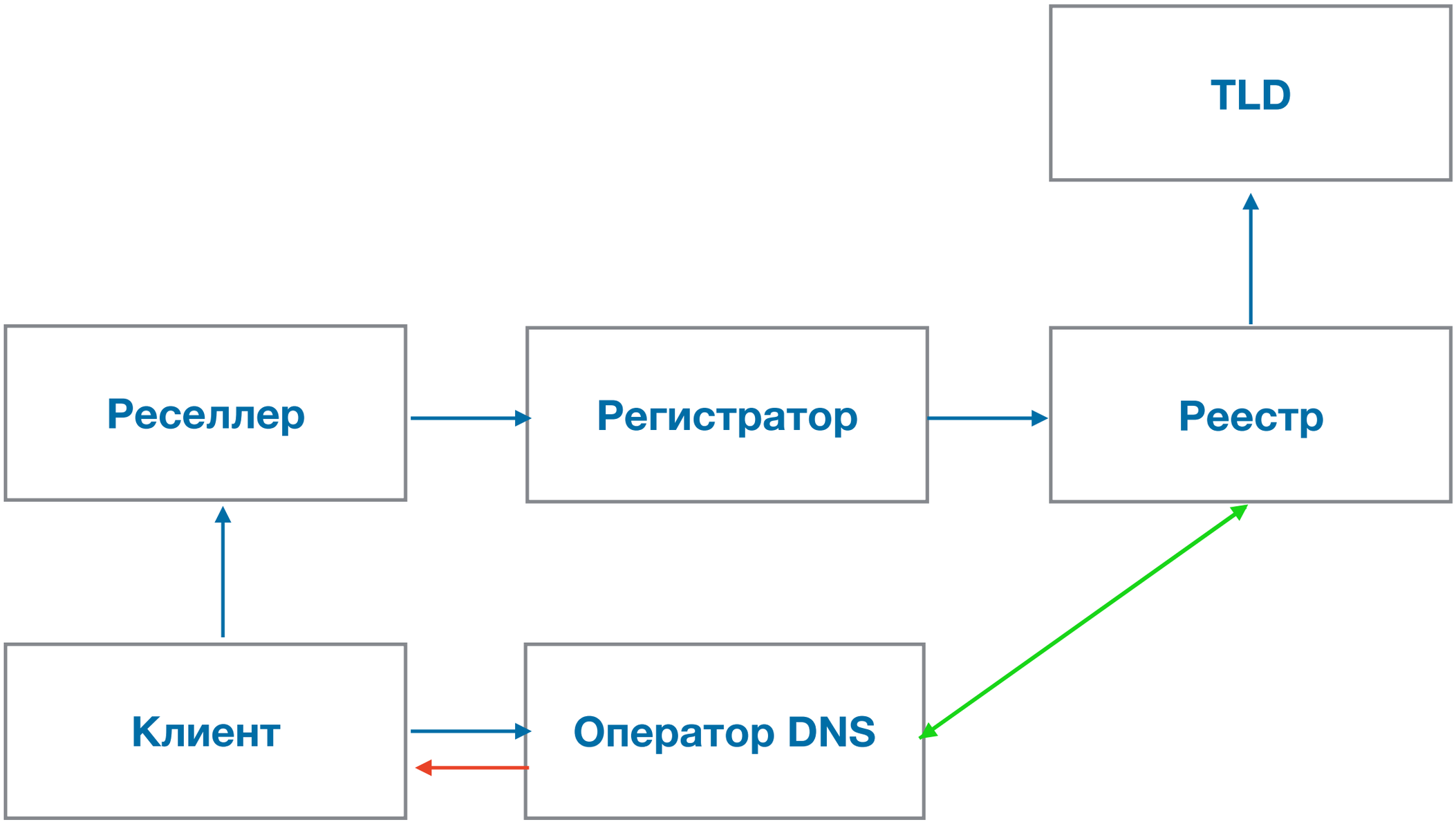
Структура отношений



Структура отношений



Структура отношений



Оператор DNS — Регистратура

- Регистратура
  - NS records
  - DS records
  - A/AAAA (glue) records
- Оператор DNS
  - NS записи
  - DNSKEY записи
- Операции
  - Изменение KSK
  - Изменение списка NS серверов

Обновление KSK

- Обновление DS без участия регистратора
  - DS запись можно вычислить из DNSKEY, но
    - нет влияния на алгоритм DS digest,
    - можно создать DS записи только по существующим ключам DNSKEY, что не совместимо с Double-DS rollover, см. стр. 24 RFC 6781

Обновление KSK

- Записи CDS и CDNSKEY
  - Automating DNSSEC Delegation Trust Maintenance, RFC 7344, Сентябрь 2014 г.
  - Указывают на необходимость обновления DS на домене верхнего уровня
  - Механизмы обновления: по запросу через API (например, без авторизации) или путём периодического опроса зоны
  - Проверка корректности полученных CDS / CDNSKEY записей НЕ РЕКОМЕНДУЕТСЯ (да, в оригинале это также указано большими буквами)

Поддержка новых алгоритмов DNSSEC

ГОСТ Р 34.10-2001 & ECDSA Curves

Ереван, 10 сентября 2015

Существующие алгоритмы

	Description	**Mnemonic**
1	*RSA/MD5*	*RSAMD5*
2	*Diffie-Hellman*	*DH*
3	*DSA/SHA1*	*DSA*
5	*RSA/SHA-1*	*RSASHA1*
6	*DSA-NSEC3-SHA1*	*DSA-NSEC3-SHA1*
7	*RSASHA1-NSEC3-SHA1*	*RSASHA1-NSEC3-SHA1*
8	*RSA/SHA-256*	*RSA/SHA-256*
10	*RSA/SHA-512*	*RSA/SHA-512*
12	*GOST R 34.10-2001*	*ECC-GOST*
13	*ECDSA Curve P-256 with SHA-256*	*ECDSAP256SHA256*
14	*ECDSA Curve P-384 with SHA-384*	*ECDSAP384SHA384*

Новое

- ГОСТ – RFC 5933, Июль 2010
- ECDSA – RFC 6605, Апрель 2012
  - … Ed25519, Ed448 …?
- Лучше, чем 1024-bit RSA
- Меньший размер ключа и подписи
  - меньший размер ответа DNS сервера;
  - меньше фрагментация;
  - меньше эффект от DDOS с использованием данной зоны

Поддержка новых алгоритмов

- Операторы связи
  - Validating DNS resolvers
- Операторы DNS
  - Zone signing tools
- Регистратуры и регистраторы
  - ...

Обновление ПО

Со стороны реестра

- Не все реестры поддерживают все типы алгоритмов, указанных в DS записи
  - Как узнать какие алгоритмы поддерживаются?
  - Зачем реестру ограничивать допустимые типы алгоритмов?
  - Зачем реестру проверять корректность подписания зоны? Защита пользователя от самого себя?

RIPE NCC

DANE: текущее состояние

DNS-based Authentication of Named Entities

Ереван, 10 сентября 2015

Известные проблемы

- Самоподписанные сертификаты
  - примерно 48% веб серверов
- Огромное количество местных центров сертификации
  - Государственные, отраслевые и корпоративные центры сертификации
- Большое число «общеизвестных» CA
  - Более 200 предустановленных CA в Apple OS X Yosemite
  - Есть ли к ним доверие?

Известные проблемы

- Несколько хранилищ сертификатов доверенных CA в каждой системе
- Огромное число предустановленных CA в каждом из них
  - Сложно удалить скомпрометированный CA из подобного списка
  - Местным CA достаточно сложно попасть в подобные списки

Известные проблемы

- Каждый центр сертификации может выдать сертификат на любое имя (домен, организацию)
  - Таким образом появляются подложные сертификаты для сервисов Google, Paypal и т.п.
- Сложность проверки сертификата на отзыв
  - Задержка при соединении
  - Вопросы доступности CRL

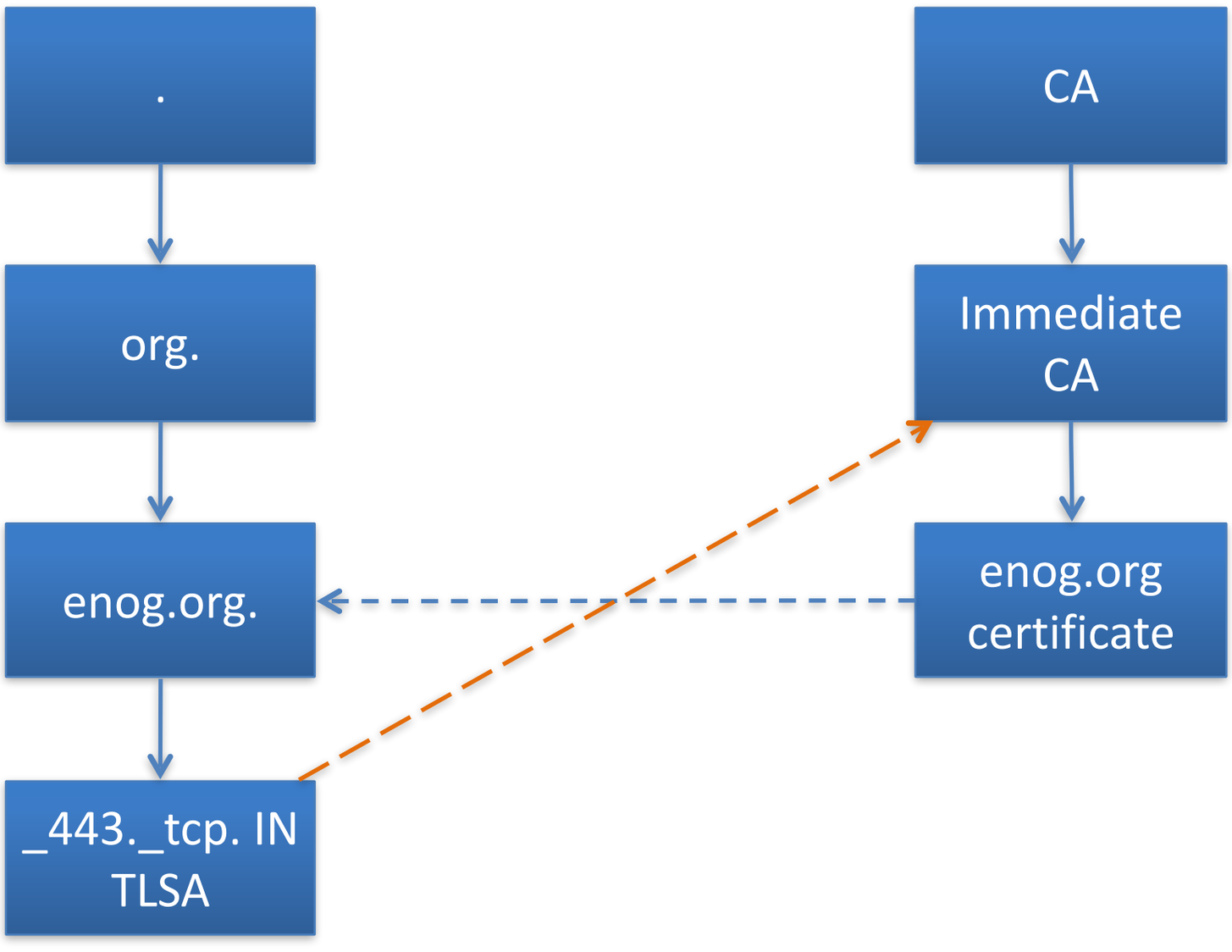
Certification Authority Authorisation

- CAA RR
  - Указывает центр сертификации, которому можно выдавать сертификаты для данного домена
  - Дополнительный уровень проверки со стороны центра сертификации перед выдачей сертификата
  - Служит для уменьшения вероятности выдачи сертификата мошеннику
- DANE
  - Используется для проверки сертификата на стороне клиента
- RFC 6844, Январь 2013 г.

PKIX & DANE

- PKIX:
  - Доверенный CA → Сертификат → Ресурс (домен)
- DANE:
  - Цепочка доверия DNSSEC → Домен → Ограничение на доверенный сертификат

DANE


.
org.
enog.org.
_443._tcp. IN TLSA
CA
Immediate CA
enog.org certificate

Варианты использования

- Варианты использования DANE
  - Ограничение по CA
    - Указанный сертификат должен находится в цепочке сертификации представленного сертификата
  - Ограничение на сертификат
    - Представленный сертификат должен не только совпадать с указанным сертификатом, но и пройти проверку согласно цепочке сертификации
  - Собственный доверенный сертификат
    - Представленный сертификат должен пройти проверку согласно цепочке сертификации, если указанный сертификат являлся бы единственным доверенным сертификатом
    - Если представленный сертификат совпадает с указанным, то проверка цепочки сертификации не производится

0. Ограничения на CA

- Выполняется обычная проверка по цепочке сертификации
  - Корневой или промежуточный сертификат должны находится в списке доверенных сертификатов
  - Указанный сертификат должен быть в цепочке сертификации

1. Ограничение на предъявляемый сертификат

- Выполняется обычная проверка по цепочке сертификации
  - Корневой или промежуточный сертификат должны находится в списке доверенных сертификатов
- Указанный сертификат должен совпадать с предъявленным

2. Указание доверенного сертификата

- Указанный сертификат является единственным доверенным сертификатом
- Выполняется проверка по цепочке сертификации при соблюдении вышеуказанного условия

3. Непосредственное указание сертификата

- Указанный сертификат должен совпадать с предъявленным
- Проверка по цепочке сертификации не производится

DANE vs PKIX

- DANE связывает сертификат с доменом
- Центр сертификации удостоверяет иные сведения, указанные в сертификате
  - Например, принадлежность сертификата организации или физическому лицу, место выдачи и т.п.

TLSA RR

- _port._protocol.domain + **TLSA** RR
  - *_443._tcp.www.example.com. IN TLSA (0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971)*

- RFC 6398: *DANE Transport Layer Security (TLS) Protocol – TLSA*
- RFC 6394: *Use Cases and Requirements for DANE*

DANE / SRV

- DANE for SRV
  - Defines client behavior
    - _xmpp-client._tcp.example.com. SRV 1 0 5222 im.example.net.
    - _5222._tcp.im.example.net. TLSA ...
  - См. draft-ietf-dane-srv

DANE / MX

- DANE for SMTP
  - Defines client behavior
    - example.com. IN MX 10 mail.example.net.
    - _25._tcp.mail.example.net. IN TLSA ...
  - См. draft-ietf-dane-smtp-with-dane

DANE / S/MIME

- S/MIME
  - <local-part-hash*>._smimecert.<domain> + **SMIMEA** RR
    - *db3cda86d4429a1d39c148989566b38f7bda0156296bd364ba2f878b._smimecert.antonbaskov.ru. IN SMIMEA*
    - *ab@antonbaskov.ru*
    - *UTF-8 lowercase SHA-2 224 HEX*
  - См. draft-ietf-dane-smime

DANE / OpenPGP

- OpenPGP
  - <local-part-hash*>._smimecert.<domain> + **OPENPGPKEY** RR
    - *fb977b8b4d5903b85055620603._openpgpkey.antonbaskov.ru. IN OPENPGPKEY <Base64 Public Key>*
      - *ab@antonbaskov.ru*
      - *UTF-8 lowercase SHA-2 256 HEX truncated from right side to 28 octets*
  - См. draft-ietf-dane-openpgpkey

DANE / Client certificate

- Клиентские сертификаты
  - _service.<domain> + **TLSA** RR
    - *_smtp_client.device1.example.org. IN TLSA*
  - См. draft-huque-dane-client-cert-01

Требования

- DANE требует внедрения DNSSEC
- DANE требует доверия к оператору DNS
- DANE требует **неразрывности цепочки доверия DNS**
  - что особенно важно в случае указания доверенного сертификата (2 и 3 сценарии использования)

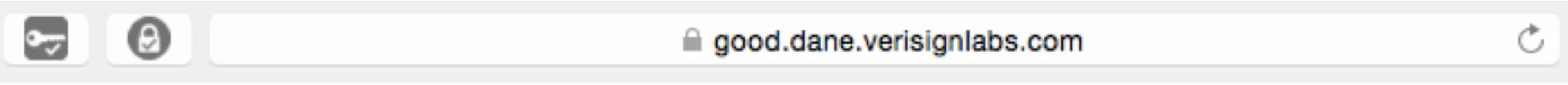
Конец эры центров сертификации?

- Не совсем…
  - Корпоративные, отраслевые и правительственные центры сертификации
  - Удостоверение владельца сертификата
    - Организации или физического лица
  - Extended validation, biometric data, etc.
- И кроме того
  - Обновление программного обеспечения затянется на долгий срок
  - DNSSEC до сих пор широко не распространён

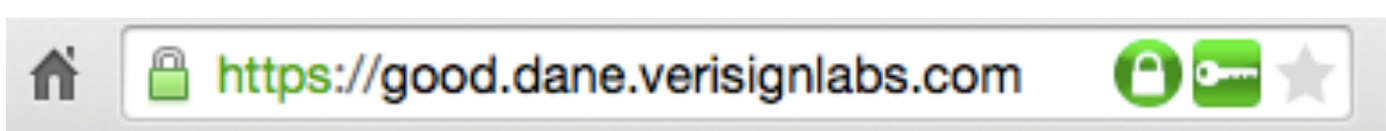
Реализации

- HTTPS
  - DNSSEC/TLSA validator from NIC.CZ
- XMPP
  - Prosody mod_s2s_auth_dane
- SMTP
  - POSTFIX
- OpenPGP
  - openpgpkey-milter (encrypt outgoing emails on MUA/MTA side)
- S/MIME
  - Smaug (Verisign) / Smaug Thunderbird Plugin

Установите расширение браузера



- Установите DNSSEC/TLSA validator от NIC.CZ
  - Отображает состояние DNSSEC и TLSA
  - Safari, Chromium, Firefox, Internet Explorer, Opera
  - https://www.dnssec-validator.cz/pages/download.html
- Проверьте правильность установки
  - http://dane.verisignlabs.com/



Anton Baskov
<ab@antonbaskov.ru>
<anton.baskov@ripe.net>

Вопросы?