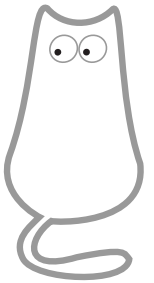
DNSSEC



РУКОВОДСТВО ОПЕРАТОРА DNS

Что надо знать. Что требуется. Как сделать.

ВЕРСИЯ 1

Филипп Кулин, III квартал 2017, UNLICENSE

Сложный DNSSEC

Технология DNSSEC сложная

Дорогая цена ошибки

Требуется непрерывное обслуживание

Зависимость от взаимодействия с регистратором

Практик очень мало

Реализация DNS с поддержкой DNSSEC сложная и требует аккуратности и внимания

DNSSEC в двух словах

Подпись записей зоны

Записи зоны подписаны с помощью системы электронной подписи.

Цепочка доверия

Родительская зона подтверждает достоверность ключа, которым подписана зона потомка.

От оператора DNS требуется подписывать зону и передавать информацию о ключах домена в родительскую зону через регистратора домена.

Оператор домена

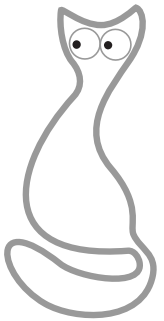
При выполнении действий, связанных с делегированием домена, исторически сложилась модель Администратор — Регистратор — Реестр. То, что обслуживание домена Администратор часто поручает сторонним исполнителям, не было большой проблемой, поскольку действия ограничивались редкими изменениями записей NS при делегировании.

Поддержка DNSSEC требует регулярных изменений в делегировании домена. В текущей модели это приводит к проблемам, поскольку требуется регулярное вовлечение в процесс технического обслуживания Администратора домена.

«Оператор домена» занимается техническим обслуживанием домена по поручению Администратора. В руководстве я буду использовать этот термин, поскольку он лучше отражает модель взаимодействия при поддержке DNSSEC.

Рассмотрим подробнее подпись зоны

Рассмотрение подписи записей зоны в рамках этого документа носит ознакомительный характер



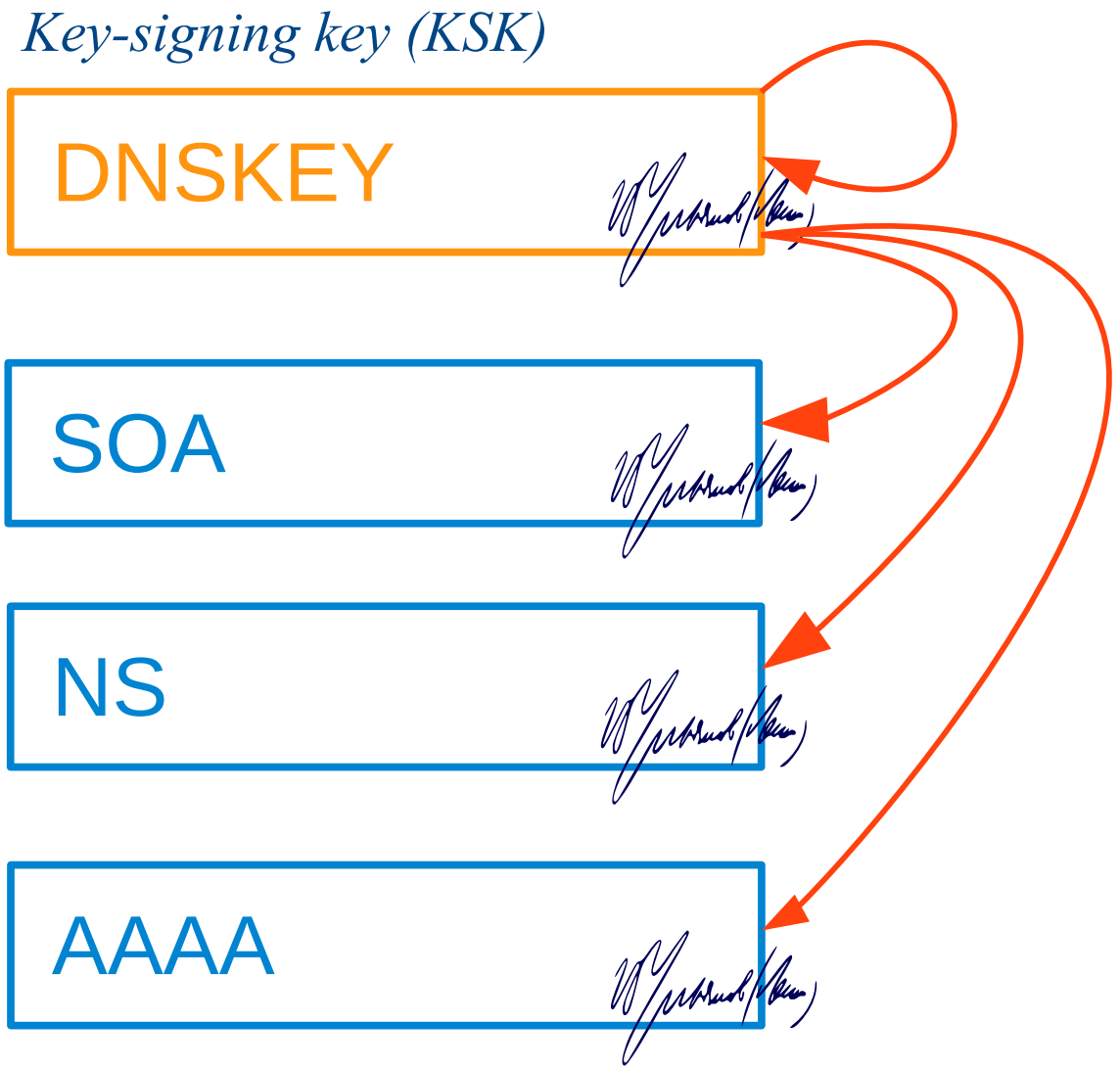
Подпись зоны одним ключом

Публикуется ключ. Записи зоны и сам ключ подписываются опубликованным ключом.

Записи зоны могут быть подписаны любым типом ключа. Но другой ключ (запись DNSKEY) может быть подписан только ключом типа KSK (Key-signing key).

Ключ KSK является «точкой входа» цепочки доверия в зону. Именно ключ KSK будет подтверждаться в родительской зоне.

Подпись зоны одним ключом



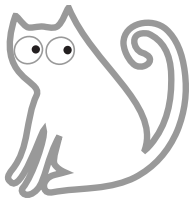
Ключом *KSK* подписан сам ключ *KSK* и все записи зоны

Подпись зоны двумя ключами

Публикуется ключ *KSK* и ключ *ZSK* (*Zone-signing key*)

Ключи *ZSK* и *KSK* подписываются опубликованным ключом *KSK*

Записи зоны подписываются ключом *ZSK*



Обновление ключа ZSK не требует подтверждения в родительской зоне. Следовательно, ключ ZSK можно обновлять, не беспокоясь о взаимодействии с регистратором домена

Подпись зоны двумя ключами

Ключом *KSK* подписан сам ключ *KSK* и ключ *ZSK*

Ключом ZSK подписаны все записи зоны

Обобщим виды подписи зоны

Подпись с использованием одного ключа

Публикуется ключ KSK. Записи зоны и сам ключ KSK подписываются опубликованным ключом KSK.

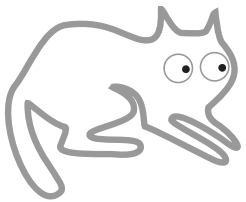
Подпись с использованием двух ключей

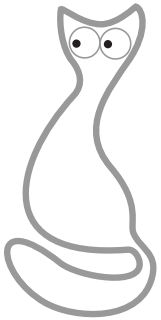
Публикуются ключи KSK и ZSK. Ключи ZSK и KSK подписываются опубликованным ключом KSK. Записи зоны подписаны ключом ZSK.

Цепочка доверия

Ключи KSK *являются «точками входа» цепочки доверия в зону*.

Рассмотрим подробнее организацию цепочки доверия





Общий принцип цепочки доверия

Общий принцип подписи зоны

Записи зоны подписываются закрытым ключом. Подписи и открытый ключ, соответствующий закрытому, публикуются в зоне.

Если мы доверяем данному ключу, то мы имеем возможность проверить любую подписанную запись.

Принцип доверия к подписи

Родительский домен подтверждает открытый ключ KSK зоны потомка. Подтверждения выстраиваются в цепочку доверия.

Делегирование подписи

В родительской зоне публикуется отпечаток открытого ключа *KSK* домена потомка, которому надо оказать доверие – запись DS (*Delegation Signer).*

Запись DS для домена потомка публикуется только в родительской зоне.

Наличие хотя бы одной записи DS для домена рассматривается как обязательство подписи зоны этого домена.

Делегирование подписи

.tld

example DS

Запись DS — это отпечаток ключа *KSK* потомка

Запись DS для example.tld размещена у «родителя»

example.tld

DNSKEY *(KSK)*

Родительский домен подтверждает ключ KSK потомка

Цепочка доверия

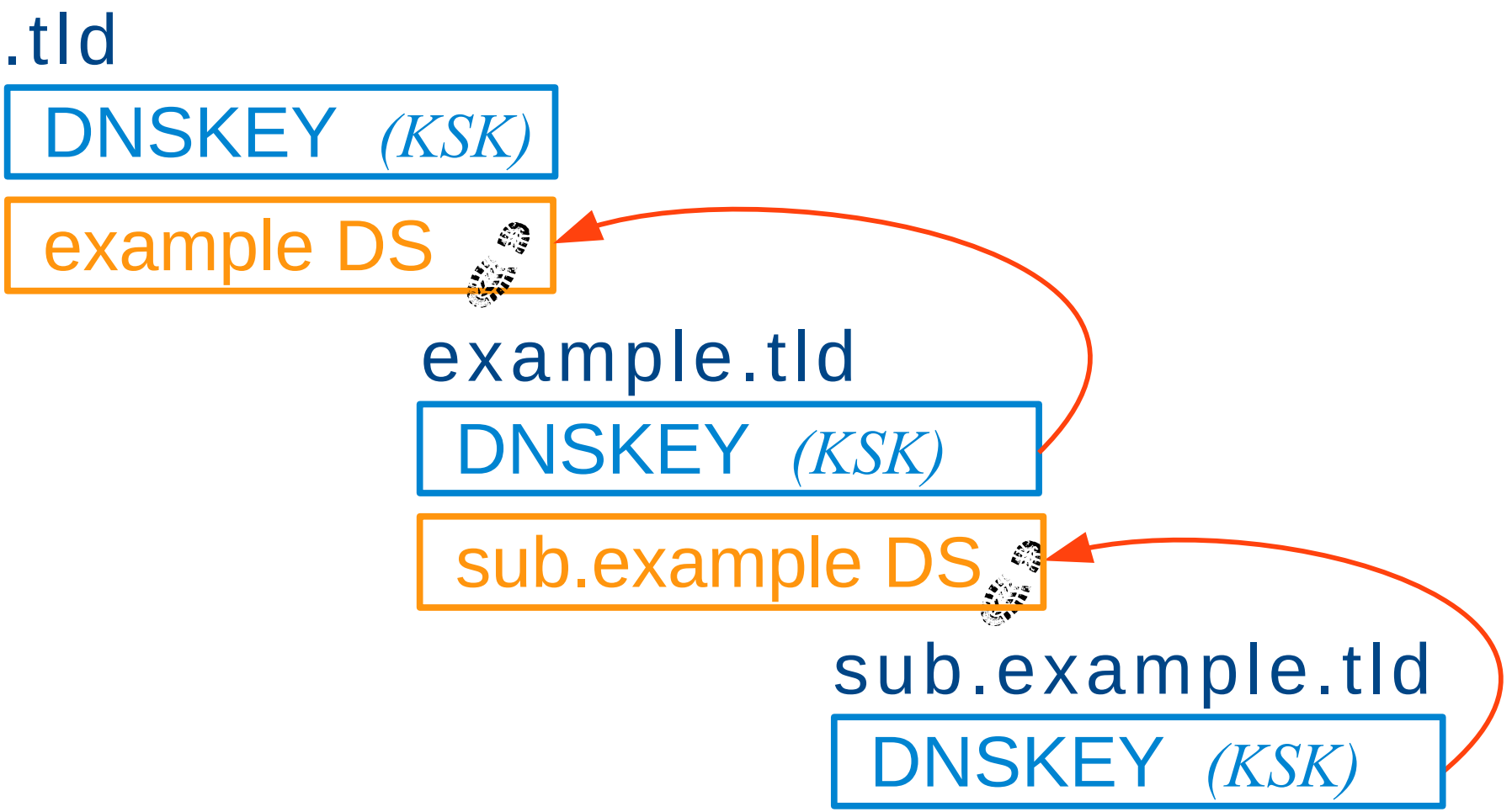
В резолверах «прошиты» корневые ключи

Цепочка доверия идёт от корневой зоны по записям DS

> *Иерархия доверия всегда соответствует иерархии делегирования зон*

Нет разницы, откуда получена информация о записях, если она сопровождается корректными подписями, ведущими по цепочке доверия к корневому ключу, которому доверяет резолвер

Цепочка доверия



Что требуется от оператора DNS

- Подписывать записи зоны и непрерывно обслуживать подписи
- Создавать, публиковать и регулярно обновлять (ротировать) ключи ZSK зоны
- Создавать, публиковать и регулярно обновлять (ротировать) ключи KSK зоны
- Передавать информацию об актуальных ключах KSK данного домена в реестр через регистратора домена

Важное отличие от обычного DNS

В отличие от обслуживания обычного DNS, при использовании DNSSEC от оператора DNS требуются определенные действия по регулярному обслуживанию зоны. Даже в том случае, если записи зоны не меняются.

Что не будет затронуто

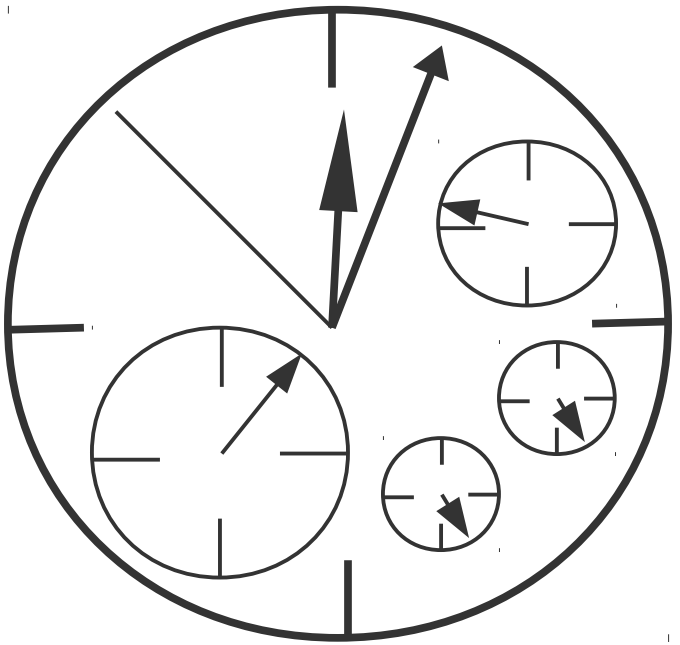
За рамками этого документа останется вопрос обслуживания так называемого *Trust Anchor* - исходного ключа цепочки доверия.

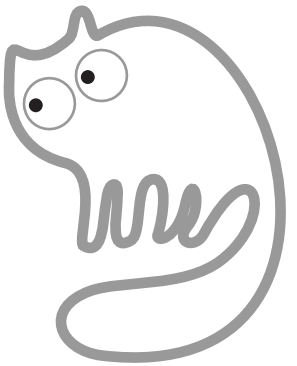
Здесь не будет описана «ротация» алгоритмов ключей и подписей.

Далее мы рассмотрим только рекомендованные автором практики, не делая обзор всех возможных вариантов.

Обслуживание подписей зоны

По мотивам **RFC 6781**





Подписывание зоны. Запись RRSIG

RRsets

Подписываются наборы записей с совпадающими полями *label*, *class* и *type* — *RRset*

DNSKEY RRset

Набор ключей может быть подписан только ключом *KSK*

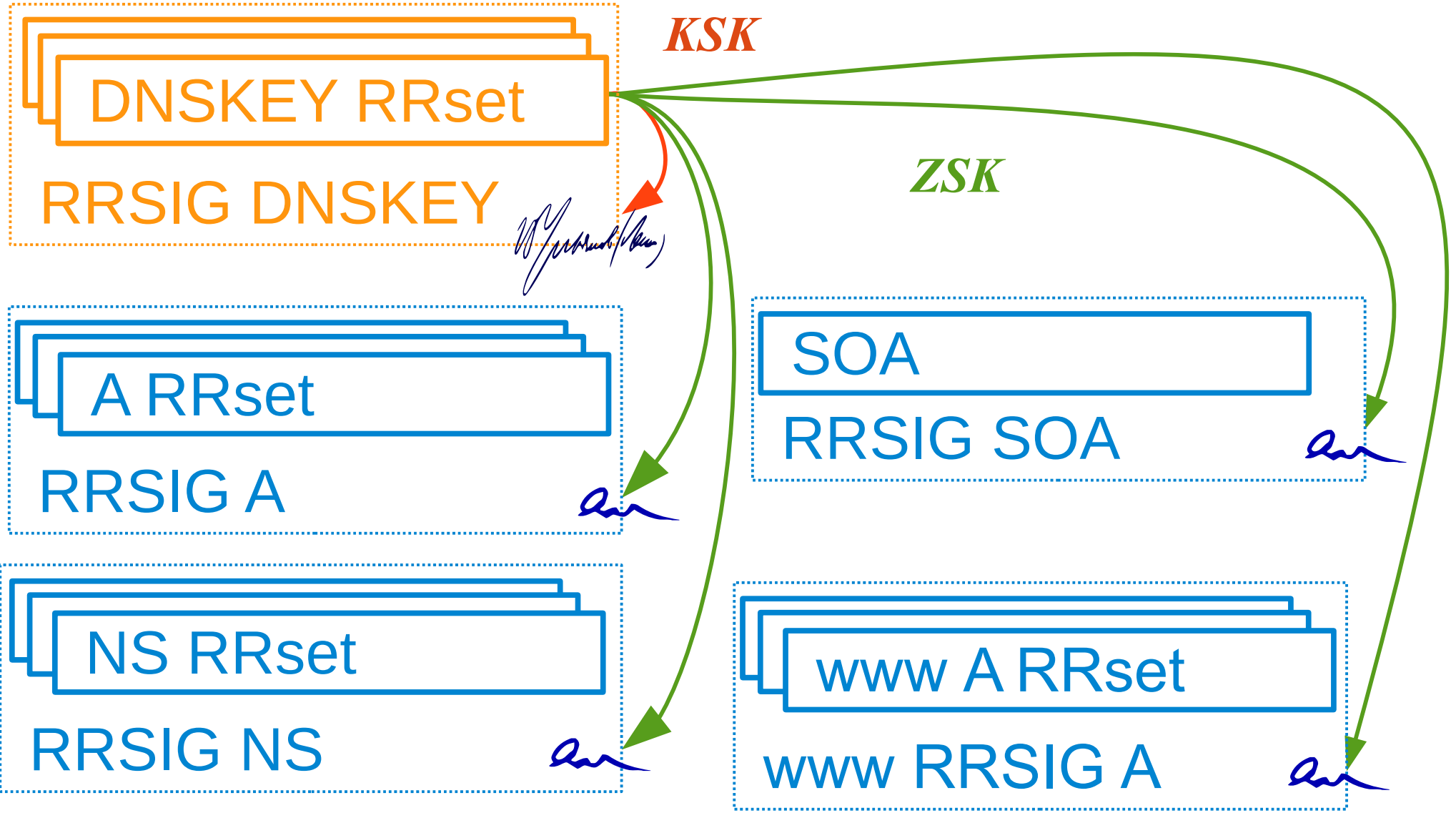
RRSIG

Подпись публикуется в записи RRSIG с такими же полями *label* и *class*. В данные записи RRSIG включается *type* и общий TTL набора

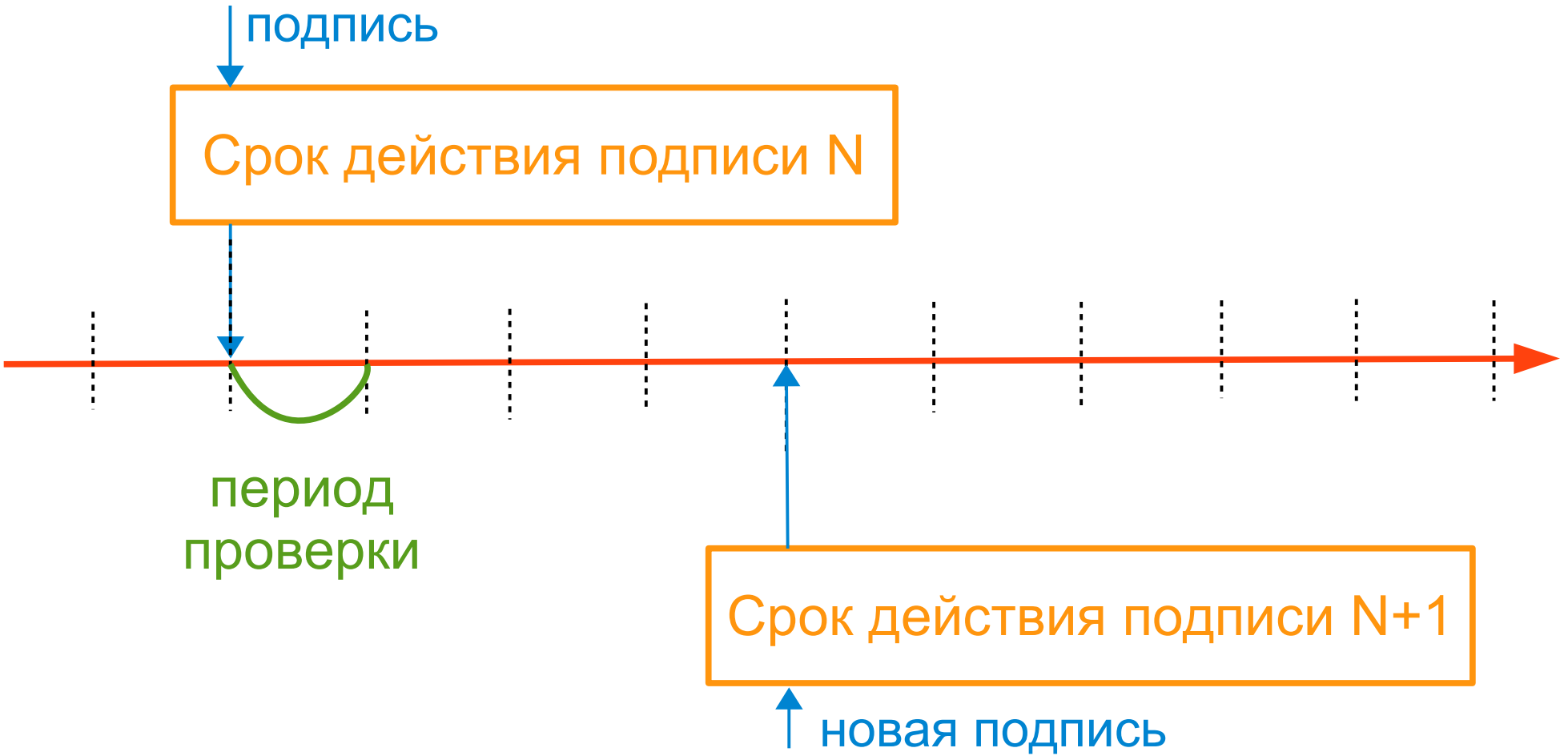
Периодическое переподписывание

Подписи периодически проверяются на истечение срока действия и обновляются при необходимости

Подпись наборов записей



Жизненный цикл подписи зоны



Время жизни записей и подпись

Максимальный TTL зоны

Должен быть кратным сроку подписи зоны

Минимальный TTL зоны

Должен быть таким, чтобы рекурсивный процесс проверки записей успевал пройти. Не рекомендуется меньше нескольких минут

Срок действия подписи

Максимальное значение

Должно учитывать возможность подмены устаревших ответов в рамках срока действия

Минимальное значение

Выбирается с учетом всех составляющих жизненного цикла зоны так, чтобы при неудачном обновлении подписи иметь запас времени для исправления

Отношение с TTL

Срок действия подписи должен быть в несколько раз больше максимального TTL зоны

Особенности срока действия подписи

Абсолютное время

Срок действия подписи задается в абсолютных значениях времени UTC. Различные ошибки настроек времени на хостах будут вызывать проблемы

Начальное значение

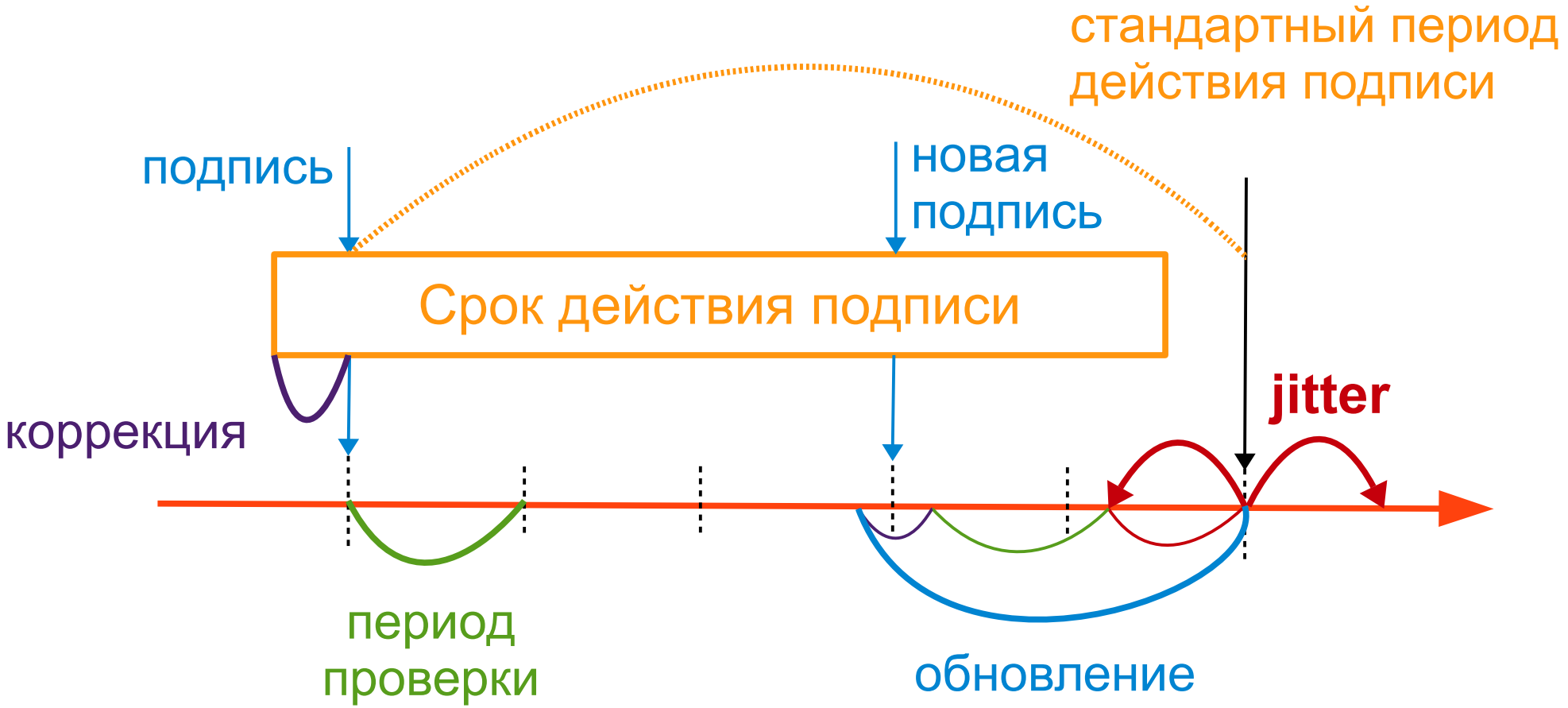
Устанавливается с небольшим корректирующим смещением в прошлое, чтобы избежать часть проблем с неточно установленным на резолверах временем

Случайное смещение времени конца действия

Конец срока действия устанавливается со случайным смещением, чтобы не загружать сервера DNS

Обновление подписи

Время обновления выбирается как сумма других времен, но не меньше, чем несколько максимальных TTL зоны



Времена подписей

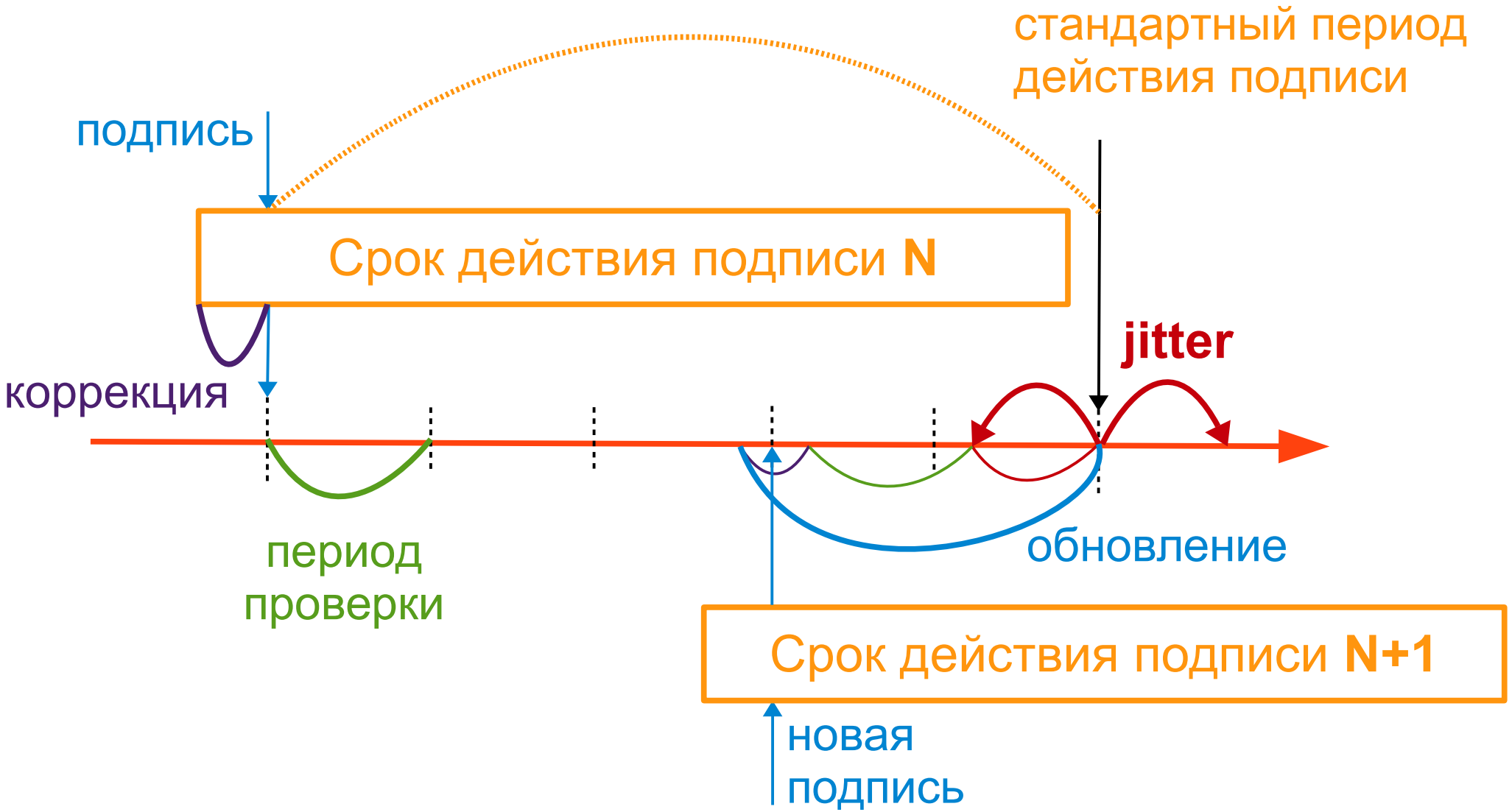
Коррекция начального значения срока действия
Устанавливается с небольшим корректирующим смещением в прошлое. Обычно 30 минут

Случайное смещение конца срока действия
Устанавливается со случайным смещением. Обычно от -60 до +60 минут

Срок действия подписи
Выбирается небольшим, кратным максимальному TTL. Обычно несколько дней

Граничные значения TTL
TTL зоны должны быть не меньше нескольких минут, но обычно не более чем четверть срока подписи

Жизненный цикл подписи



Лук подписей зоны

Подпись отрицательного ответа

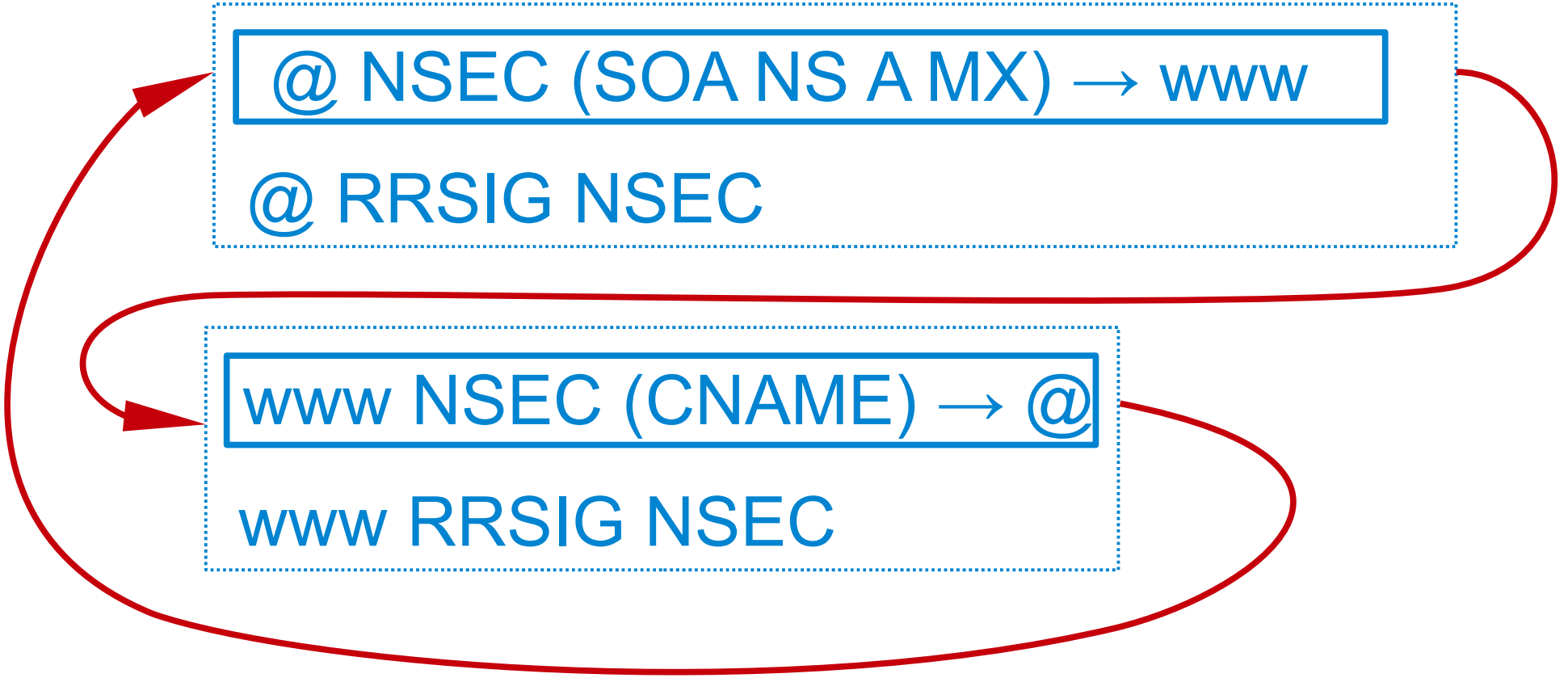
Запрос, на который нет подписанных записей

- Домен есть, но нет запрашиваемых типов записей
- Домена нет
- Домен совпадает с шаблонной записью «*»

Запись NSEC

Набор зацикленных записей NSEC, показывающих, что между двумя доменными именами нет других доменов

Запись NSEC



Ответ с NSEC

Запрос bbb (A)

AUTHORITY SECTION ответа

ccc NSEC (A AAA) → ccc

aaa RRSIG NSEC

Запрос ccc (A)

AUTHORITY SECTION ответа

ccc NSEC (TXT) → ddd

ccc RRSIG NSEC

NSEC3

Запись NSEC3

То же, что и NSEC, но в качестве доменов используется хэши существующих доменов

Параметры NSEC3

- Соль
- Количество проходов хэширования
- Флаг opt-out для ускорения подписи зоны с огромным количеством отсылок на неподписанные домены

NSEC или NSEC3?

NSEC

- Простой понятный небольшой DNS-ответ
- Быстро создается
- Позволяет просто и быстро получить все записи зоны

NSEC3

- Получить все записи зоны возможно только с помощью специальных программных средств
- Большой размер DNS-ответа
- Ответы не поддаются диагностике «взглядом»
- Не выполняет цели. Получить все записи зоны всё равно возможно

Подпись отрицательного ответа «на лету»

RFC 4470 и **RFC 4471**

Существуют домены aaa и ccc

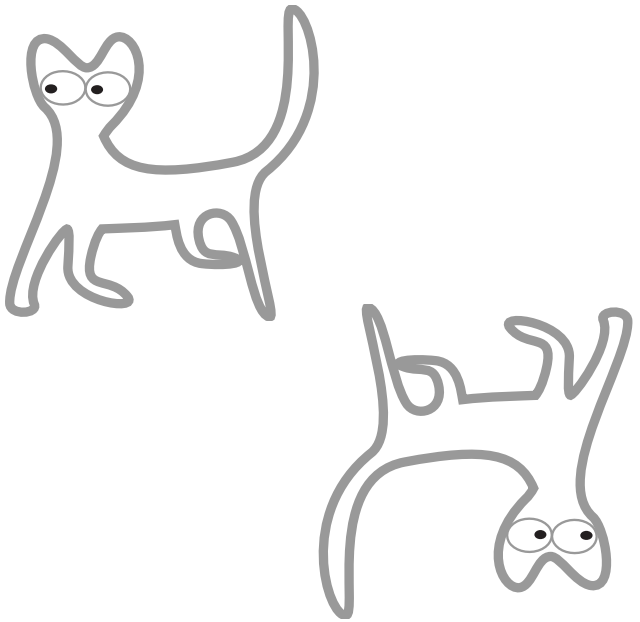
Запрос bbb (A)

AUTHORITY SECTION ответа

bba NSEC (A AAA) → bbc

bba RRSIG NSEC

Ротация ключей ZSK



По мотивам **RFC 7583**

Метод предварительной публикации ключа

Времена в ключах и отпечатках

Время жизни

У ключей нет «времени жизни» в отличии от подписей RRSIG

Но, например, BIND в метаинформации к ключам подразумевает «время жизни»

TTL ключей

TTL может быть отличным от обычных записей

DS TTL

TTL у записей DS обычно очень большой, и каждая родительская зона может устанавливать свой

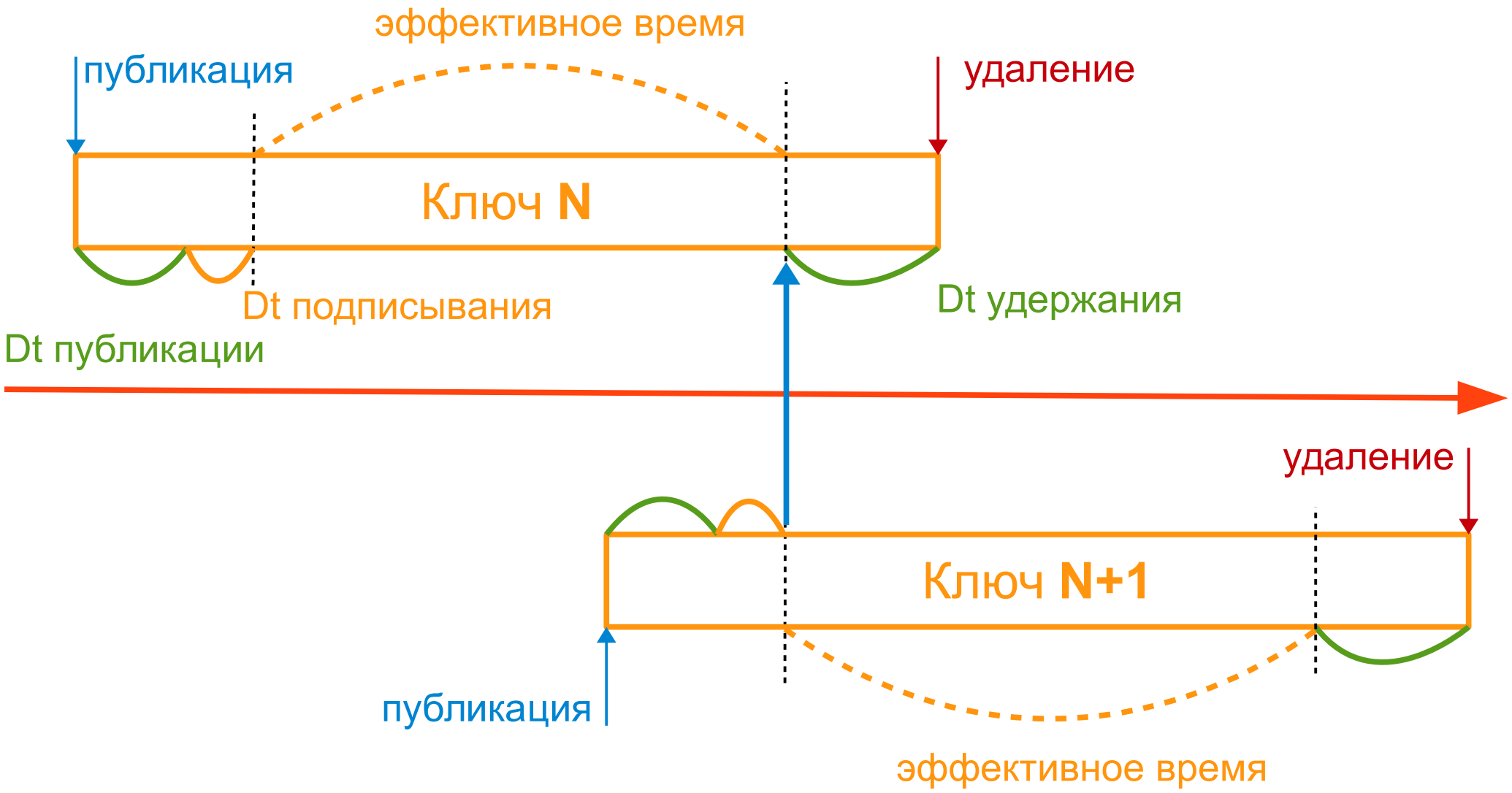
Ротация ZSK. Метод предварительной публикации ключа

- Ключ N публикуется в зоне
- Зона подписывается только ключом N

  Ключ N используется какое-то время

- Ключ N+1 публикуется в зоне
- Зона подписывается только ключом N+1
- Ключ N удаляется из зоны

Ротация ZSK. Метод предварительной публикации ключа



Ротация ZSK. Соображения по интервалам

Время публикации ключа

Больше или равно времени распространения зоны по всем авторитативным серверам + TTL ключа

Время удержания ключа

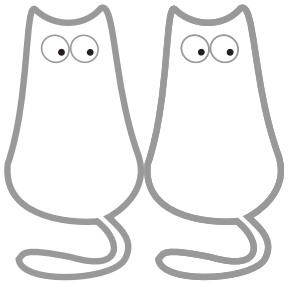
Отсчет инициируется после подписания зоны новым ключом. Больше или равно времени распространения зоны по всем авторитативным серверам + TTL ключа

Эффективное время ключа

Например около месяца

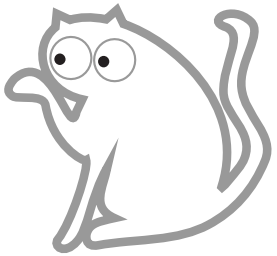
Ротация ключей KSK

По мотивам **RFC 7583**



Метод двойной подписи

Требует взаимодействия с регистратором домена



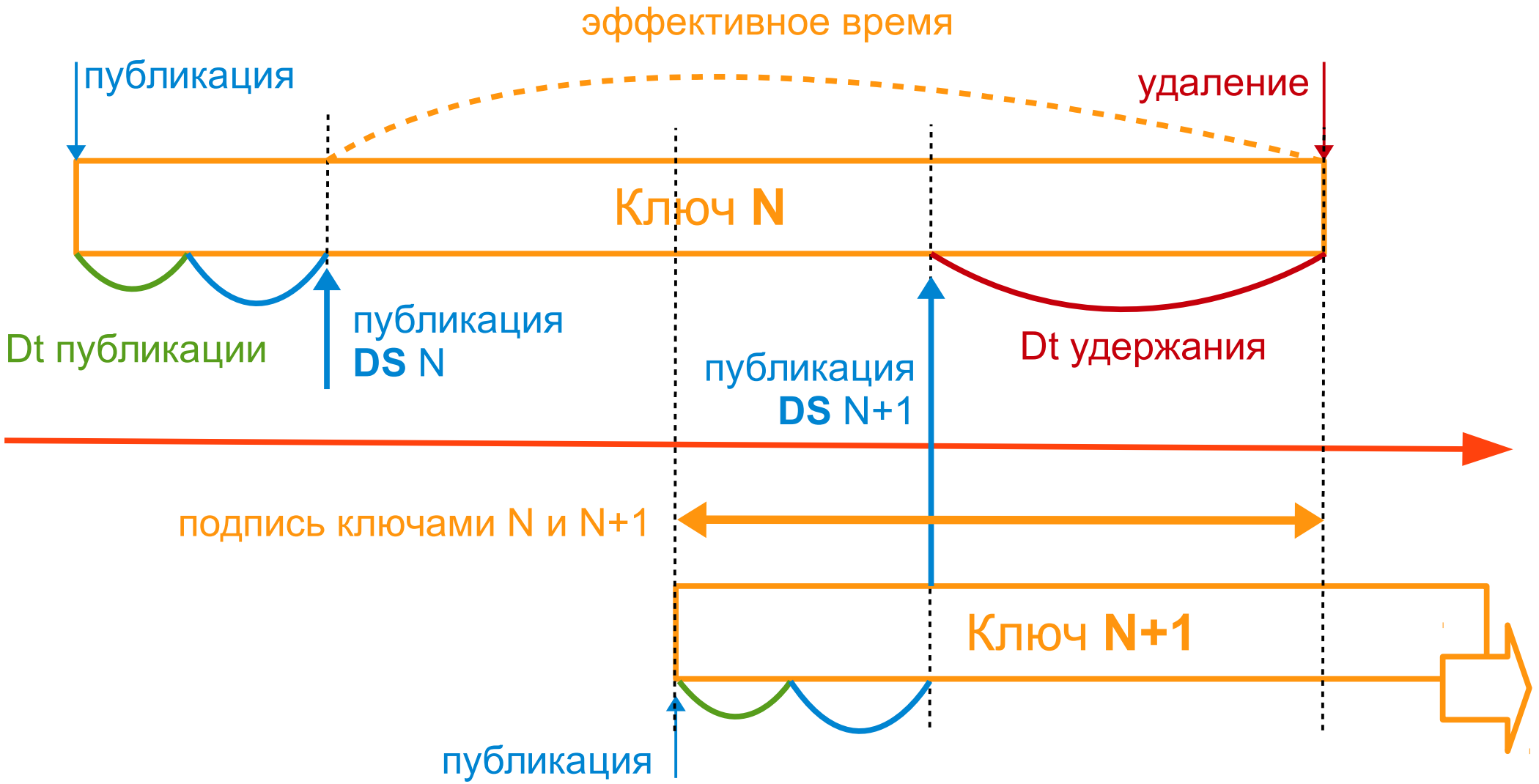
Ротация KSK. Метод двойного ключа

- Ключ N публикуется в зоне, и все ключи подписываются ключом N
- DS ключа N публикуется в родительской зоне

  Ключ N используется какое-то время

- Ключ N+1 публикуется в зоне, и все ключи подписываются ключами N и N+1
- DS ключа N+1 заменяет DS ключа N у родителя
- Ключ N удаляется из зоны

Ротация KSK. Метод двойного ключа



Ротация KSK. Метод двойного ключа. Соображения по интервалам

Время публикации ключа

Больше или равно времени распространения зоны по всем авторитативным серверам + TTL ключа, но не меньше часа

Время удержания ключа

Отсчет инициируется после реальной публикации нового DS ключа в родительской зоне. Больше или равно времени распространения родительской зоны по всем авторитативным серверам + TTL DS

Эффективное время ключа

Например около года

Запаска (standby keys)

Идея состоит в том, что существует запасной пассивный ключ, который можно незамедлительно использовать

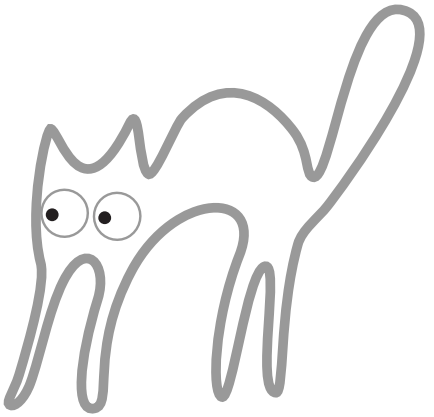
- Запасной ключ ZSK, не участвует в подписи
- Запасной ключ KSK должен участвовать в подписи. Смысл почти потерян

Безопасность ключей

- Рекомендуется хранить приватные ключи отдельно
- Раздельное хранение ключей усложняет процедуры поддержки DNSSEC

Смена оператора DNS

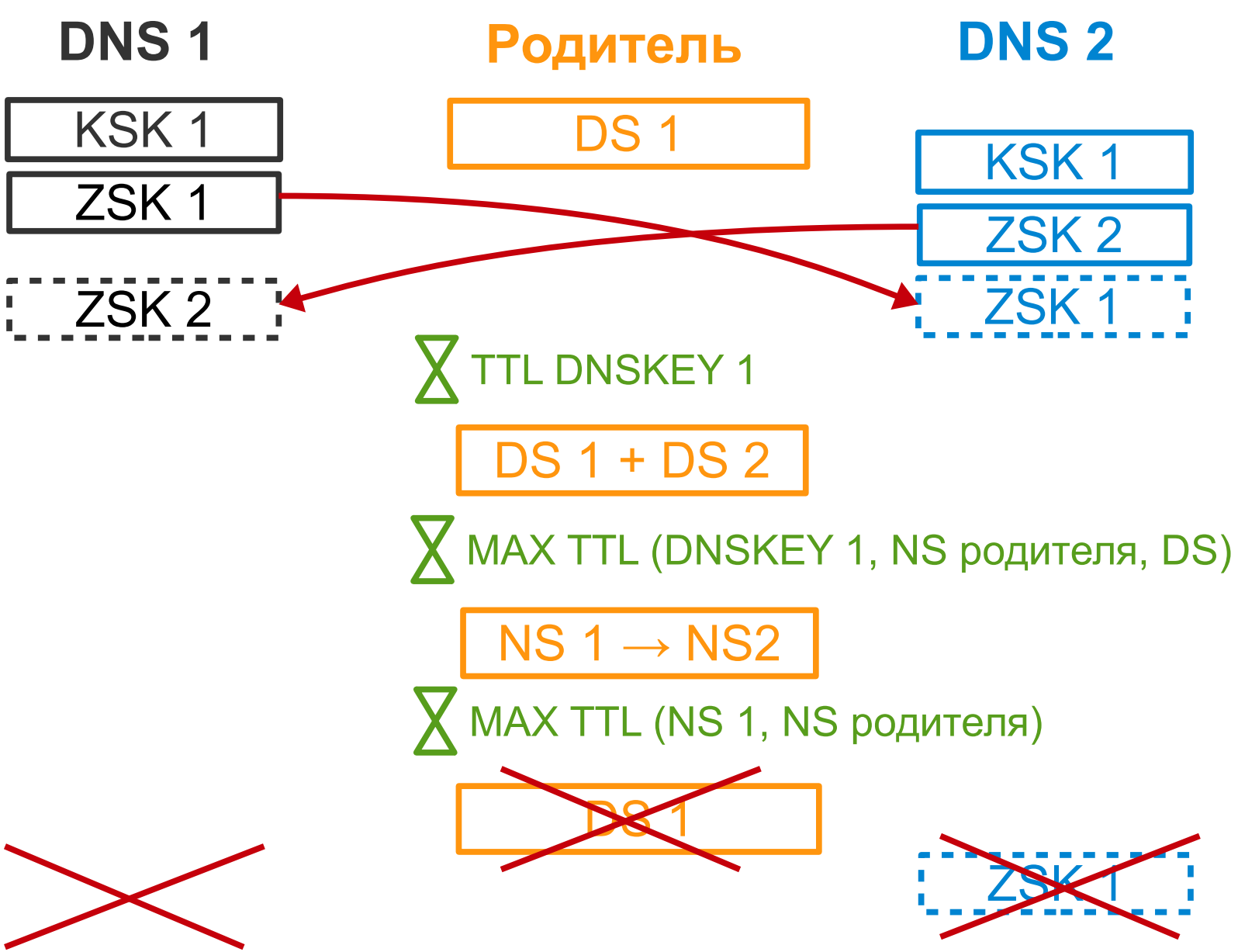
По мотивам **RFC 6781**



Смена оператора DNS. Метод обмена публичными ключами

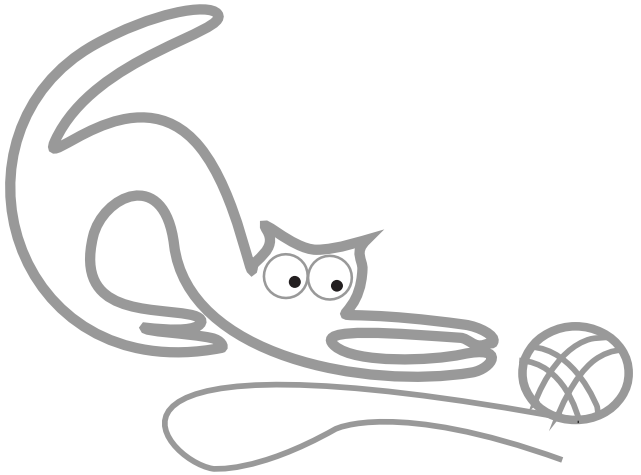
- Зона отдельно подписана на обоих DNS
- Оба DNS обмениваются ключами ZSK
- DS запись для нового DNS добавляется родителю
- Ожидание — максимальный TTL из DNSKEY, NS (у родителя), DS
- Смена NS серверов у регистратора
- Ожидание — TTL NS (у родителя)
- Удаление DS записи старого DNS
- Удаление публичного ZSK старого DNS у нового DNS

Смена оператора DNS



Автоматическое делегирование DNSSEC

По мотивам **RFC 7344** *и* **RFC 8078**

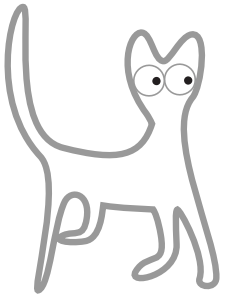


Записи CDS/CDNSKEY

- Записи CDS и CDNSKEY соответствуют желаемым записям DS
- CDNSKEY — для проверки CDS или генерации DS
- Являются сигналом для замены текущего DS RRset
- Для удаления DS — алгоритм «0» в CDS/CDNSKEY
- Регистратор сам устанавливает политики:
  - периодически просматривает дочернюю зону
  - требует явной инициации просмотра
- Регистратор может требовать дополнительной авторизации
- Требуется самостоятельный мониторинг DS

Мне не известны регистраторы, поддерживающие такую автоматизацию

Подходы к реализации



Что поддерживать. Что не поддерживать. Как поддерживать.

Мониторинг

Реакция на сбои

Любая процедура работы с DNSSEC должна иметь регламент по реакции на сбой. Вплоть до экстренного снятия делегирования подписи

Прогнозирование

Требуется прогнозирование возможных сбоев, связанных с интервалами времени

Программное обеспечение не хочет ходить строем

Требуется непрерывный мониторинг состояния подписанной зоны и целостности цепочки доверия

Подписывание зоны «на лету»

Предварительное подписывание

Зона предварительно подписывается и распространяется на авторитативные сервера

Автоматическое подписывание

DNS сервер имеет доступ к ключам и подписывает зону автоматически. Обычно возможен трансфер подписанной зоны на вторичные сервера

Подписывание «на лету»

DNS сервер имеет доступ к ключам и подписывает ответ на каждый запрос

Поддержка нескольких алгоритмов

Совместимость

Несколько записей DS с разными алгоритмами отпечатка и несколько ключей с разными алгоритмами создаются для поддержки совместимости с резолверами

Бессмысленность

Дублирование ключей и подписей заметно увеличивает размер DNS-ответа, а уровень распространения DNSSEC сегодня так низок, что тянуть бремя совместимости бессмысленно

Рекомендуемые алгоритмы

Оператор DNS может и должен использовать только один выбранный набор алгоритмов

Эффективным алгоритмом подписи является ECDSA:

- защищенность не хуже RSA
- ECDSA в разы быстрее RSA
- данные ECDSA по размеру меньше RSA
- ECDSA позволяет умещать большинство ответов DNS в один UDP пакет

Для отпечатка наиболее практично использовать алгоритм SHA-256

Мы все ждем DNSSEC API от регистратора

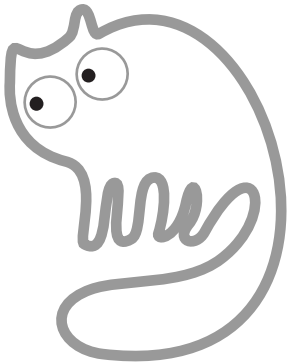
Поддержка CDS/CDNSKEY

Просить у регистраторов поддержку автоматизации делегирования подписи

API для операторов доменов?

Реестр доменов .CA (CIRA) предлагает специальный протокол для операторов доменов:
https://github.com/CIRALabs/DSAP/

Нельзя не сделать DNSSEC API, когда на слайде есть котик



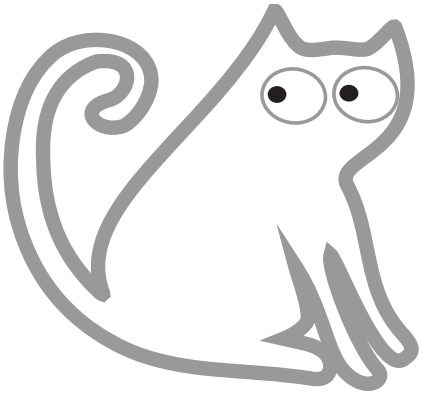
Что ещё может оператор DNS

Оператор DNS может предоставить инструмент для проверки делегирования домена. Например: http://dnsviz.net/

Оператор DNS может предложить клиентам прописывать используемые сертификаты x509 в записях TLSA домена

Оператор DNS может создать собственные практики внедрения DNSSEC. На текущий момент их очень мало

Автоматизация обслуживания зоны



DNSSEC tools

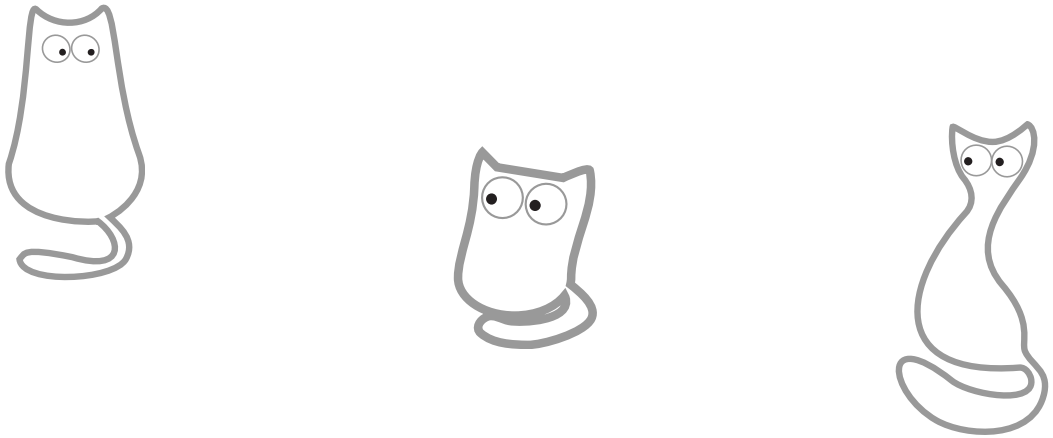
https://www.dnssec-tools.org/

- Набор утилит на Perl, использующих bind tools
- Автоматическое управление ключами
- Не умеет CDS/CDNSKEY (или я не нашел)
- Переподписывание требует внешней инициативы
- Есть собственный мониторинг
- Сайт «съедает» всю память моего компьютера

OpenDNSSEC

- Быстрый
- Умеет переподписывать
- Автоматическое управление ключами
- «Hook» для передачи записи DS
- Не умеет CDS/CDNSKEY
- Конфигурация в XML
- Много компонентов, включая программный HSM

DNSSEC в различных реализациях серверов DNS



BIND (9.7+)

https://www.isc.org/downloads/bind/dnssec/

Предварительное подписывание

- Хороший, проверенный набор утилит
- `bind9tools` в Linux дистрибутивах
- С версии 9.11 есть утилита управления ключами `dnssec-keymanager`

Динамическое подписывание

- `auto-dnssec` — с версии 9.7
- `inline-siging` — с версии 9.9
- Подписывает всю зону, а не ответы «на лету»
- Не умеет CDS/CDNSKEY

PowerDNS (4.0+)

Предварительное подписывание

- Своих утилит не имеет
- Делает что-то странное

Динамическое подписывание

- NSEC3 «на лету» (режим narrow, «белая ложь»)
- Умеет подписать трансфер

Управление ключами

- Требуется внешнее управление
- Умеет CDS/CDNSKEY

NSD

- Своих утилит не имеет
- Только предварительно подписанные зоны
- Зато быстрый

KNOT

Предварительное подписывание

- Имеет небольшой набор собственных утилит

Динамическое подписывание

- Автоматическое подписывание и «на лету»
- NSEC «на лету», ссылается на **RFC 7129**
- Имеет странные ограничения и недоработки
- «На лету» умеет только схему с одним ключом

Управление ключами

- Вручную
- Автоматическое
- CDS/CDNSKEY с проверкой DS у родителя

Инструменты командной строки

BIND utils

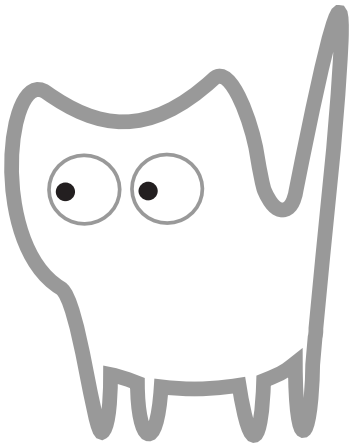
Один из самых популярных инструментов командной строки. Входит в полную поставку ISC BIND. В UNIX-дистрибутивах обычно называется *bind9utils*

LDNS utils

Набор инструментов командной строки на основе библиотеки Ldns. Разработан при поддержке RIPE. В большинстве UNIX-дистрибутивах называется *ldns-utils*

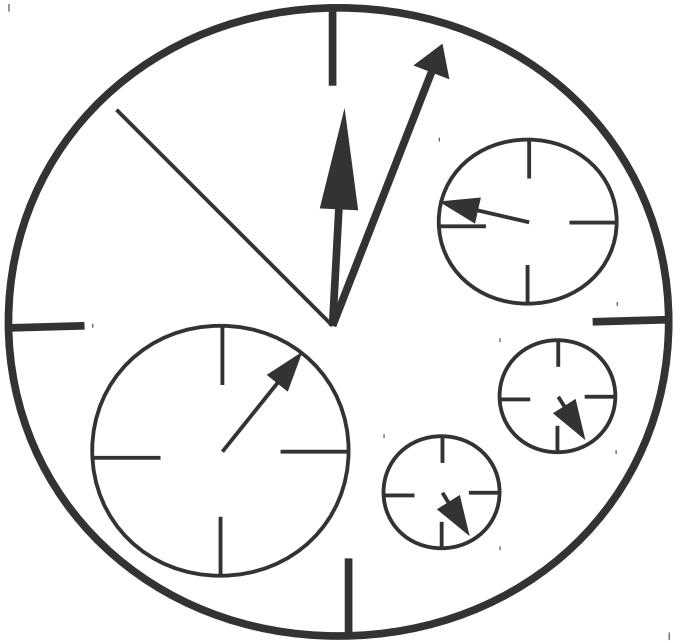
Итог в трех слайдах

Слайд «вопросы» близко



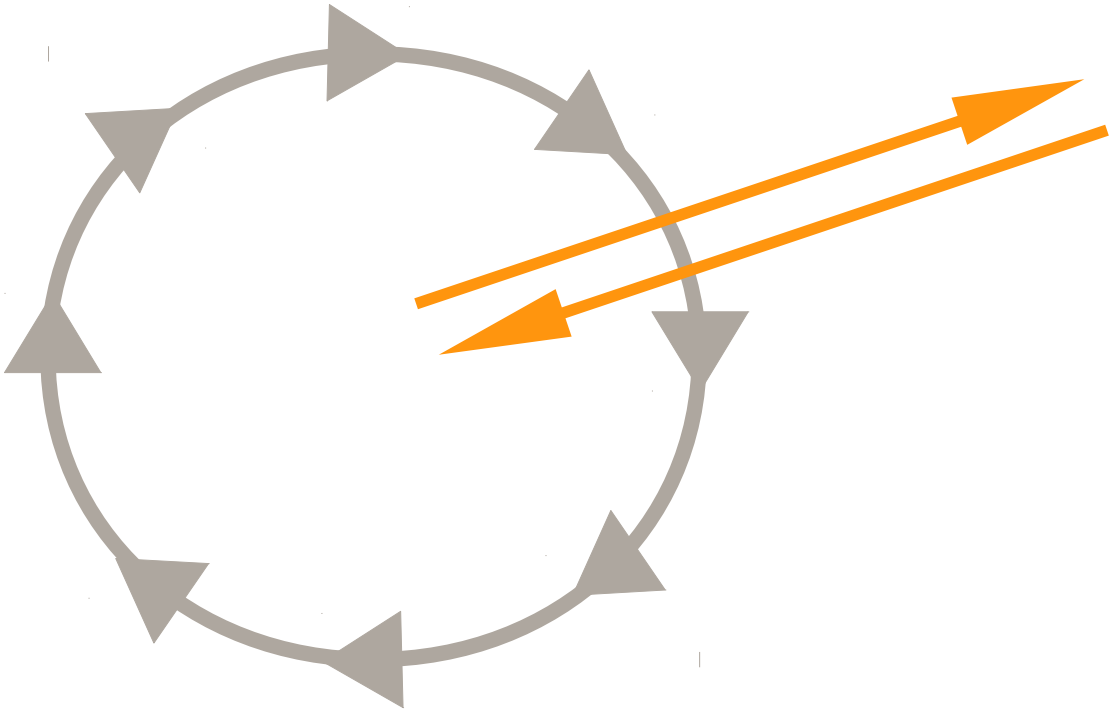
Итог. Слайд 1

Непрерывное обслуживание подписей



Итог. Слайд 2

Ротация ключей и общение с регистратором



Итог. Слайд 3

Практики

Пишите мне

Если возникли вопросы, предложения или требуется помощь, да и в любом случае — пишите мне:

phil@diphost.ru

Полезные ресурсы

Самое популярное программное обеспечение для работы с DNSSEC. Проект OpenDNSSEC
https://www.opendnssec.org/

Набор утилит dnssec-tools для обслуживания DNSSEC
https://www.dnssec-tools.org/

Библиотека Ldns
https://www.nlnetlabs.nl/projects/ldns/

Визуализация DNS и DNSSEC
http://dnsviz.net/

Предложение CIRA по протоколу обновления DS
https://github.com/CIRALabs/DSAP/

Подборка RFC по DNSSEC

RFC 4033 Введение в DNSSEC
RFC 4034 Ресурсные записи для DNSSEC
RFC 4035 Модификации протокола DNS для DNSSEC

RFC 4509 Использование SHA-256 для записей DS
RFC 5702 Использование SHA-2 в DNSKEY и RRSIG
RFC 6605 Использование ECDSA и SHA-384 в DNSSEC

RFC 6781 Эксплуатация DNSSEC
RFC 7583 Соображения по ротации ключей DNSSEC

RFC 4470 Подпись отрицательных ответов «на лету»
RFC 7129 Подпись отрицательных ответов
RFC 7344 Автоматизация делегирования доверия DNSSEC
RFC 8078 Управление записями DS через CDS/CDNSKEY

Общественное достояние

Это бесплатный документ, переданный в общественное достояние.

Любой человек может свободно копировать, изменять, публиковать, цитировать, использовать, продавать или распространять этот документ на любых носителях целиком или по частям для любых коммерческих или некоммерческих целей во всех смыслах.