План обновления ключа для подписания ключей корневой зоны

Проект отчета группы разработчиков с обновлениями от 4 августа 2015 года

1 Обзор

ICANN готовит план обновления ключа для подписания ключей (KSK) корневой зоны DNSSEC. Планирование операции обновления ключа осуществляет ICANN в рамках ее роли оператора функций IANA в сотрудничестве с другими партнерами по управлению корневой зоной. Такими партнерами являются компания Verisign — специалист по обслуживанию корневой зоны — и Национальное управление по телекоммуникациям и информации (NTIA) Министерства торговли США — администратор корневой зоны.[1]

Обновление ключа подписания ключей корневой зоны заключается в изменении ключа, который используется с 2010 года, с момента первого подписания корневой зоны в соответствии с определением расширений безопасности DNS (DNSSEC)[2]. Изменение ключа означает, что будет сформулирован секретный компонент и распространен новый открытый компонент криптографической системы. Адекватное распространение нового открытого компонента является наиболее критически важным аспектом всей операции по обновлению ключа.

Настоящий документ выносится на общественное обсуждение и представляет собой проект отчета по итогам обсуждения в группе разработчиков, которая состоит из приглашенных на добровольной основе экспертов в области DNS и DNSSEC, а также представителей партнеров по управлению корневой зоной. Данный документ находится на стадии проекта и будет доработан с учетом отзывов и предложений интернет-сообщества, полученных в ходе открытого периода общественного обсуждения ICANN и дальнейшего рассмотрения. По итогам последующего диалога будет подготовлен и опубликован итоговый отчет.

---

[1] Настоящий проект плана разработан в соответствии и с учетом особенностей текущей структуры управления корневой зоной, которая в настоящее время определяется условиями договора об исполнении функций IANA и соглашениями о сотрудничестве между NTIA и Verisign. Группа разработчиков и партнеры по управлению корневой зоной признают тот факт, что предпринимаемые в настоящее время усилия по передаче координирующей роли в исполнении функций IANA могут оказывать влияние на участие NTIA в любых будущих процессах. Однако технические характеристики и соображения по большей части не зависят от усилий по передачи координирующей роли и конечного результата.

[2] См. документы RFC 4033, RFC 4034 и RFC 4035

2 Содержание

3 Сводное резюме

ICANN в качестве оператора функций IANA в сотрудничестве с компанией Verisign, выполняющей функции специалиста по обслуживанию корневой зоны, а также с Национальным управлением по телекоммуникациям и информации (NTIA) Министерства торговли США, выполняющим функции администратора корневой зоны, совместно именуемые «партнеры по управлению корневой зоной» (RZM), предприняли попытку разработать план обновления ключа для подписания ключей (KSK) корневой зоны.

В соответствии со спецификацией DNSSEC ключ KSK корневой зоны используется для подписания набора записей ресурсов DNSKEY корневой зоны. В такой набор входит ключ подписания зоны (ZSK), который используется для подписания всех других наборов записей ресурсов (RRset) в корневой зоне. Обновление ключа подписания ключей корневой зоны заключается в изменении ключа, который используется с 2010 года, с момента первого подписания корневой зоны в соответствии с определением расширений безопасности DNS (DNSSEC). Изменение ключа означает, что будет сформулирован секретный компонент и распространен новый открытый компонент криптографической системы. Адекватное распространение нового открытого компонента является наиболее критически важным аспектом всей операции по обновлению ключа.

В декабре 2014 года ICANN пригласила добровольцев из сообщества принять участие вместе с RZM-партнерами в работе группы разработчиков плана обновления ключа для подписей ключей корневой зоны, представленного в настоящем документе. Результатом такой работы стал всеобъемлющий набор технических и информационных рекомендаций, призванных помочь RZM-партнерам в подготовке подробного плана реализации для выполнения первого обновления KSK-ключа корневой зоны. Настоящий документ следует рассматривать в качестве проекта плана, призванного помочь в достижении таких результатов.

3.1 Терминология DNS

Настоящий документ касается технических особенностей DNS и DNSSEC. Для удобства обращения к разъяснениям терминологии и технического жаргона ниже представлены определения некоторых терминов, имеющих к этому отношение — Таблица 1.

Понятие	Сокращение	Пояснение
Набор записей ресурсов	RRSet	Набор данных, хранящихся в системе DNS, наименьшая единица данных, подписывае-мая ключом DNSSEC
Ключ для подписания ключей	KSK	Пара из открытого и секретного ключей[3], роль которых заключается в обеспечении подписи с возможностью проверки для набора ключей, использующихся в зоне DNS. Особенность этой роли заключается в том, что спецификация DNS требует распространять открытый ключ такого рода вне пределов использования протокола DNS.
Ключ подписания зоны	ZSK	Пара из открытого и секретного ключей, роль которых заключается в обеспечении подписи для всех других наборов данных в зоне DNS. Этот ключ не распространяется за пределами протокола DNS
DNSKEY RRset		Набор ключей, которые используются в зоне и выполняют роль в том числе ключей KSK и ZSK для подписания набора записей ресурсов DNSKEY
Обновление ключа		Операция упорядоченного перехода с использованием одного криптографического ключа на другой

[3] Ferguson, Niels; Schneier, Bruce (2003). *Practical Cryptography*. Wiley. ISBN 0-471-22357-3.

Понятие	Сокращение	Пояснение
Средство проверки DNSSEC		Программное обеспечение, которое выполняет проверку безопасности ответов DNSSEC, в том числе подписей данных в рамках одного этапа
Якоря доверия		Сохраненный открытый ключ для подписания ключей, пользующийся абсолютным доверием со стороны средства проверки
Автоматическое обновление якорей доверия DNSSEC	RFC 5011	Одна из методик автоматического обновления якорей доверия в средстве проверки
Двойная подпись		Использование для набора записей RRset двух подписей, обычно со старым и новым ключами, задействованными в операции обновления ключа. Обычно для набора записей RRset достаточно одной подписи
Консультативный комитет системы корневых серверов	RSSAC	Предусмотренный Уставом ICANN комитет, консультирующий сообщество ICANN по вопросам системы корневых серверов
Механизмы расширения DNS	EDNS или EDNS(0)	Предусмотренная в настоящее время стандартом RFC 6891 возможность расширения стандартного формата протокола DNS. EDNS(0) означает первый набор расширений
Запись ресурса отпечатка ключа подписи в DNSSEC	DS	Запись DNSSEC, указывающая на ключ KSK, используемый при субделегировании (или для корневой зоны ключ KSK домена верхнего уровня)
Отрицательный ответ	NSEC или NSEC3	Определенные в DNSSEC записи ресурсов, которые используются для указания на то, что данные для заданного вопроса не существуют

Понятие	Сокращение	Пояснение
Заявление о практических методиках DNSSEC	DPS	Документ, в котором описывается специфика обработки DNSSEC для зоны.
Церемонии создания ключей		События, в рамках которых секретный ключ используется в программно-аппаратном криптографическом модуле (HSM) для формирования подписей. Официальная процедура используется в случаях, когда желательно обеспечить наблюдения операций свидетелями.

Таблица 1. Терминология DNS и DNSSEC

3.2 Прочие термины из области безопасности

Понятие	Сокращение	Пояснение
OpenPGP	OpenPGP	Средство управления открытыми и секретными ключами. RFC 4880: *Формат сообщений OpenPGP*
Стандарт синтаксиса криптографических сообщений	PKCS#7	RFC 2315: *PKCS #7: синтаксис криптографических сообщений — версия 1.5*
Каталог — структура сертификатов атрибутов и открытых ключей	X.509	Стандарт ITU-T для управления открытыми и секретными ключами. Рекомендация ITU-T X.509 | ISO/IEC 9594-8
Запросный открытый ключ	KSR	Структура данных, содержащая запросы подписей, в частности по наборам DNSKEY, которые должны быть подписаны ключом KSK
Ответный подписанный ключ	SKR	Структура данных, содержащая подписи, сгенерированные с использованием секретного ключа, в частности подписи KSK для наборов DNSKEY.

Таблица 2. Прочие термины из области безопасности

3.3 Прочие термины из области сетевых технологий

Несколько дополнительно используемых терминов, определение которых может способствовать пониманию широкой публикой

Понятие	Сокра-щение	Пояснение
Протокол пользовательских дейтаграм DNS	UDP	Бесконтекстный транспортный протокол для передачи данных по Интернету на основе принципа наилучшего доступного качества
Протокол управления передачей	TCP	Ориентированный на подключение транспортный протокол, ориентированный на передачу данных по Интернету с гарантированным порядком октетов данных
Максимальный блок передаваемых данных	MTU	Максимальное количество октетов, которые могут содержать данные, отправляемые через Интернет за один раз. MTU маршрута означает наименьшее значение MTU для всех блоков данных, которые использовались при передаче по маршруту от отправителя до получателя в Интернете

Таблица 3. Прочие термины из области сетевых технологий

3.4 Сводка рекомендаций

Рекомендация 1. Обновление ключа на подписание ключей корневой зоны должно соответствовать процедурам, описанным в документе RFC 5011 для обновления якорей доверия во время обновления ключа для подписания ключей.

Рекомендация 2. ICANN следует определить ключевых поставщиков программного обеспечения DNS и работать в тесном контакте с ними для формализации процедур, которые позволили бы обеспечить надежность и безопасность распространения якорей доверия по каналам конкретных поставщиков.

Рекомендация 3. ICANN следует определить ключевых системных интеграторов DNS и работать в тесном контакте с ними для

формализации процедур, которые позволили бы обеспечить надежность и безопасность распространения якорей доверия по каналам конкретных интеграторов.

Рекомендация 4. ICANN следует играть активную роль в продвижении надлежащих методов проверки подлинности якорей доверия корневой зоны, в том числе за счет подчеркивания важности информации, публикуемой на веб-сайте ICANN, посвященном функциям IANA.

Рекомендация 5. Обновление ключа для подписания ключей для корневой зоны не должно требовать существенных изменений существующих процессов управления и использования ключей KSK для сохранения связанных с такими процессами высоких стандартов прозрачности.

Рекомендация 6. Все изменения наборов записей RRset DNSKEY корневой зоны должны быть согласованы с 10-дневными временными слотами, описанными в заявлении DPS оператора ключа KSK.

Рекомендация 7. Для первого изменения ключа для подписания ключей корневой зоны следует поддерживать существующий алгоритм и размер ключа для поступающего ключа для подписания ключей.

Рекомендация 8. Для поступающих обновлений ключа для подписания ключей корневой зоны в будущем следует пересмотреть выбор алгоритма и размера ключа.

Рекомендация 9. ICANN в сотрудничестве с RZM-партнерами должна подготовить и выполнить план информационной работы для повышения осведомленности об обновлении ключа для подписания ключей корневой зоны, включающий информирование глобального технического сообщества в рамках соответствующих технических конференций, а также по каналам партнеров, в частности определенных в настоящем документе.

Рекомендация 10. ICANN следует поручить комитету RSSAC координировать рассмотрение подробного графика на период обновления ключа KSK перед его публикацией и удовлетворить разумные запросы изменения такого графика в тех случаях, когда это понадобится по каким-либо операционным причинам того или иного оператора одного из корневых серверов.

Рекомендация 11. ICANN следует координировать свои усилия с комитетом RSSAC и RZM-партнерами и обеспечить использование каналов связи в режиме реального времени для обеспечения операционной осведомленности системы корневых серверов о каждом изменении корневой зоны, подразумевающем добавление или удаление ключа KSK.

Рекомендация 12. ICANN следует координировать с комитетом RSSAC, чтобы поручить операторам корневых серверов осуществлять сбор данных, призванных служить информационной основой для последующего анализа и определения характеристик операционных последствий обновления ключа для подписания ключей, а также обеспечить доступность планов и продуктов такого сбора данных для независимого анализа.

Рекомендация 13. RZM-партнеры должны сделать так, чтобы любое увеличение размера ключа подписания зоны в будущем тщательно координировалось с обновлением ключа для подписания ключей с тем, чтобы эти две операции не выполнялись параллельно.

Рекомендация 14. Чтобы свести к минимуму время, необходимое для восстановления после затруднений, возникающих в связи с поступающим ключом для подписания ключей, SKR, генерируемый с использованием только действующего ключа KSK, должен генерироваться параллельно SKR, генерируемого с использованием нового KSK.

Рекомендация 15. RZM-партнеры должны разработать процесс, подразумевающий использование SKR, сформированного новым KSK.

3.5 Целевая аудитория

Настоящий документ предназначен для технической аудитории, в первую очередь для специалистов, знакомых с протоколами DNS и DNSSEC, а также операционными аспектами DNSSEC и процессами, связанными с использованием DNSSEC в корневой зоне.

3.6 Круг вопросов, затрагиваемых в настоящем документе

Цель настоящего документа — очертить и определить набор рекомендаций, призванных помочь RZM-партнерам в выработке подробного плана реализации обновления ключа для подписания ключей в корневой зоне.

4 Краткая предыстория

4.1 Развертывание DNSSEC в корневой зоне

В 2009 году RZM-партнеры объединили свои усилия[4] для развертывания DNSSEC в корневой зоне. Кульминацией таких усилий стала первая публикация подписанной корневой зоны, поддерживающая возможности проверки в июле 2010 года. Ключ для подписания ключей, который используется в настоящее время, был сгенерирован в ходе первой церемонии создания KSK-ключа, которая прошла в защищенном дата-центре (KMF), работающем под управлением ICANN в Калпепере, штат Вирджиния, США. В последствии материалы ключа были перенесены во второй центр KMF в Эль Сегундо, Калифорния, США, и после проверки и подтверждения успешного переноса таких материалов открытая часть ключа KSK была опубликована в корневой зоне, а также в качестве якорей доверия.

Требования к генерированию и обслуживанию ключа KSK корневой зоны, а также соответствующие обязанности каждого из RZM-партнеров были определены NTIA[5]. Процедуры, используемые для выполнения таких требований специалистом по обслуживанию корневой зоны и оператором функций IANA, были опубликованы в отдельном заявлении о политиках и практике DNSSEC (DPS)[6].

В июле 2010 года договор об исполнении функций IANA между NTIA и ICANN был изменен — в него были включены обязанности, связанные с управлением ключом KSK корневой зоны, и затем эти требования переместились во все последующие редакции этого договора[7]. В соглашении о сотрудничестве между NTIA и Verisign в июле 2010 года также были внесены поправки, отражающие обязанности Verisign как оператора ключа подписания корневой зоны.[8]

Согласно договору об исполнении функций IANA ICANN должна выполнить обновление ключа KSK корневой зоны, однако подробный график или план реализации таких действий не указан. В заявлении DPS оператора KSK

[4] Подробные сведения о развертывании DNSSEC в корневой зоне были опубликованы на веб-сайте http://www.root-dnssec.org/
[5] «Требования к тестированию и реализации для первоначального размещения DNSSEC в полномочной корневой зоне», 29 октября 2009 года, http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf
[6] https://www.iana.org/dnssec, https://www.verisigninc.com/en_US/repository/index.xhtml
[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order
[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf

корневой зоны в разделе 6.5 содержится следующее утверждение, в котором определяются требования к обновлению ключа:

«Необходимо запланировать обновление каждого ключа KSK корневой зоны в рамках церемонии создания ключа при необходимости или по истечению пяти лет работы».

4.2 Общественное обсуждение обновления ключа KSK корневой зоны

8 марта 2013 года ICANN открыла период общественного обсуждения для сбора мнений и комментариев в отношении выполнения обновления ключа для подписания корневой зоны[9]. Свои ответы прислали 6 организаций и 15 частных лиц. В своей сводке по итогам полученных комментариев[10] ICANN определила 7 рекомендаций для рассмотрения RZM-партнерами.

1. Прежде чем приступать к обновлению ключа KSK в соответствии с документом RFC 5011, необходимо определить набор тестов и измеряемых показателей, а также платформу испытаний. На этапах тестирования необходимо обеспечить работу каналов обмена информацией и сформировать методики успешной оценки.
2. Обновление ключа KSK должно проводиться регулярно.
3. Измерение показателей и мониторинг определены как ключевые режимы оценки последствий для технических характеристик и конечных пользователей в результате обновления ключа KSK, если такое обновление будет реализовано.
4. Обновление ключа KSK должно проводиться регулярно.
5. Перед обновлением ключа KSK заблаговременно за достаточно большой период времени об этом должны быть открыто уведомлены различные и разнообразные группы заинтересованных сторон.
6. Необходимо дальнейшее изучение операционной стабильности, регулярных обновлений ключа KSK и [вероятности и последствий] несоблюдения требований RFC 5011.

[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf

4.3 Предварительное обсуждение обновления ключа KSK корневой зоны в 2013 года

В конце июля 2013 года RZM-партнеры провели встречу для обсуждения вариантов обновления ключа KSK корневой зоны. Группа определила, что процедура обновления ключа должна выполняться в рамках четко определенных этапов в течение достаточного периода времени, а также что будет полезно провести обширную работу по информированию сообщества и учесть возможные задержки с отзывом ключей в рамках измененного графика обновления ключей согласно RFC 5011. Эти высокоуровневые принципы были представлены на заседании рабочей группы IETF по вопросам эксплуатации DNS (DNSOP) на конференции IETF 87[11].

4.4 Рекомендация SSAC в отношении обновления ключа DNSSEC в корневой зоне

В ноябре 2013 года консультативный комитет по безопасности и стабильности (SSAC) опубликовал документ SAC063[12], касающийся обновления ключа KSK. В отчете рассматривались риски, связанные с выполнением такой операции, а также состояние базы исходного кода на тот момент (в частности, реализации программного обеспечения DNS с открытым исходным кодом). Данный отчет содержал рекомендации провести информационную работу для ознакомления широкой публики с операцией смены ключей KSK корневой зоны, а также призвал провести тестирование для сбора и анализа действий распознавателей DNS, а также создать показатели приемлемых уровней неудачных операций в ходе смены ключей KSK корневой зоны и определить меры по возврату в исходное состояние в случае чрезмерного уровня неудачных операций и собрать данные для использования в качестве информационной основы будущих действий по смене ключа такого рода.

В отчете SSAC подчеркивались три темы, которые будут рассмотрены далее в настоящем документе. Во-первых, по грубой оценке приблизительно 1,1% пользователей, зависящих от использования DNS с поддержкой DNSSEC, могут столкнуться с отрицательными последствиями даже в случае хорошо организованного обновления ключа KSK корневой зоны. Во-вторых, поддержка автоматизированного обновления якорей доверия DNSSEC, называемая также RFC 5011, присутствует, однако не поддается прогнозированию. И в-третьих, что озабоченность, согласно ряду мнений, вызывает размер ответов DNS в тех

[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf
[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

ситуациях, когда речь идет о существовании фрагментации транспортных пакетов UDP и переключении на запросы TCP.

4.5 ICANN формирует группу разработчиков процедуры обновления KSK корневой зоны

В декабре 2014 года ICANN пригласила добровольцев из сообщества принять участие вместе с RZM-партнерами в работе группы разработчиков плана обновления ключа для подписей ключей корневой зоны, представленного в настоящем документе.

5 Высокоуровневое описание процедуры обновления ключа KSK

Подготовленный в июле 2013 г. план, который не сильно отличается от планов обновления любых других ключей KSK, подразумевает следующие этапы.

1) Формирование новой пары ключей KSK (открытый и секретный ключ).

2) Новый открытый ключ KSK размещается в корневой зоне и/или предоставляется другим сторонам взаимодействия.

3) В отличие от других зон новый открытый ключ KSK корневой зоны находится в таком состоянии, что все начинают принимать его в качестве нового ключа KSK. Помимо пассивного принятия, новый открытый ключ KSK корневой зоны предоставляется на различных электронных и неэлектронных носителях, что позволяет операторам распознавателей и разработчикам, серверы которых не поддерживают RFC 5011, выигрывать дополнительное время для включения нового якоря доверия в свои системы и продукты. (Для других зон этот этап заменяется информированием держателей записей DS о поступающем новом ключе KSK.)

4) Процесс подписания переключается с использования старого секретного ключа KSK на новый секретный ключ KSK.

5) Теперь новый ключ KSK находится в переходном состоянии до того, как подписи, сформированные с использованием старого ключа KSK, не станут недействительными или иным образом исчезнут из операционной среды.

6) Старый открытый ключ KSK удаляется из корневой зоны (без отзыва).

7) Еще одно отличие от обычных операций заключается в повторном вводе старого ключа KSK корневой зоны для того, чтобы пометить его как отозванный в соответствии с рекомендациями, изложенными в документе RFC 5011. Этот отдельный этап призван учесть специфику операций с ключом подписания зоны (ZSK), которые подразумевают обновление такого ключа без чрезмерного увеличения ответов DNS для полного набора ключей корневой зоны.

6 Подход группы разработчиков

Группа разработчиков рассмотрела несколько аспектов обновления ключа KSK корневой зоны и подготовила рекомендацию по каждой из рассмотренных областей для помощи в разработке плана реализации партнерами по корневой зоне.

- Операционные соображения: воздействие на конечных пользователей Интернета и операторов систем DNS, а также на службы, используемые такими конечными пользователями
- Соображения протокола: в какой степени существующие документированные элементы протокола достаточны для учета особенностей обновления ключа KSK корневой зоны
- Воздействие на управление ключом KSK корневой зоны: воздействие на процессы, задействованные оператором функций IANA для задач управления ключом KSK
- Соображения криптографической защиты: обеспечение достаточной прочности криптографической защиты системы в целом
- Обмен информацией и координация усилий между всеми задействованными сторонами.

Каждая из этих областей рассматривается отдельно в следующих разделах. Кроме того, представлено также подробное техническое описание решения по обновлению ключа, которое призвано служить иллюстрацией того, каким образом можно выполнить рекомендации, а также исходной точкой для RZM-партнеров в подготовке ими окончательного плана реализации.

6.1 Операционные соображения

Ожидается, что воздействие на конечных пользователей Интернета и операторов систем DNS будет оказываться во время двух из перечисленных выше этапов. Когда новый открытый ключ KSK добавляется в корневую зону, увеличивается размер ответа на запрос набора ключей DNSKEY корневой зоны. Когда старый секретный ключ KSK больше не будет генерировать подписи, проверка подлинности с использованием соответствующего открытого ключа перестанет работать ожидаемым образом.

Увеличенный размер ответов на запросы DNSKEY может привести к образованию фрагментации пакетов UDP с результатами, которые будут несколько отличаться для IPv4 и IPv6. Некоторые подключения в Интернете уже считают фрагменты аномалий и отфильтровывают их. Для системы DNS, которая не ведет контроля состояния отправляемых ответов, это означает, что клиент может не получить ожидаемый ответ. Кроме того, существует потенциальная возможность того, что ответ UDP большего размера может превысить указанный размер буфера передаваемых данных DNS для соответствующего запроса, что приведет к повышению уровня неполных ответов и формированию последующих повторных запросов с помощью TCP.

Когда старый ключ KSK перестанет подписывать ключ подписания зоны, при условии, что новый ключ KSK будет генерировать подписи, средство проверки DNSSEC, для которого в качестве якоря доверия настроен только старый ключ KSK, не сможет проверить подлинность подписанных ответов DNSSEC. Такое средство проверки уйдет в отказ, то есть будет считать все подписанные ответы DNS недействительными.

Конечный клиент, использующий исключительно распознаватели со средствами проверки подлинности, которые не смогут переключиться на новый ключ KSK или принимать ответы большего размера во время процесса обновления ключа, не смогут подтверждать подлинность всех подписанных ответов DNS. Со стороны конечного клиента это будет выглядеть как какое-то отключение Интернета, когда не будет работать разрешение доменных имен. Когда аналогичные ситуации имели место в прошлом, побочным эффектом было увеличение количества обращений в центры поддержки клиентов, то есть дополнительная нагрузка на службы поддержки клиентов и управления операциями интернет-провайдеров.

ICANN следует спланировать при вводе в эксплуатацию нового ключа KSK координацию обмена информацией, а также переключениями с использования старого на новый ключ KSK для генерирования подписей (см. Рекомендацию 8).

6.2 Соображения протокола

6.2.1 Конфигурация якоря доверия корневой зоны

Необходимо учесть два вида конфигурации якорей доверия:

- якори доверия в онлайн-распознавателях с проверкой подлинности;
- якори доверия в устройствах или системах, которые не подключены к Интернету во время обновления ключа и будут подключены позже.

Онлайн-распознаватели с проверкой подлинности могут использовать *автоматическое обновление якорей доверия* расширений безопасности DNS (DNSSEC), описанное в документе RFC 5011, если используемое программное обеспечение DNS поддерживает этот механизм и настроено на использование этого механизма для обновления ключа подписания ключей корневой зоны.

Онлайн-распознаватели с проверкой подлинности, которые не могут или не хотят использовать автоматическое обновление якорей доверия расширений безопасности DNS, во время обновления ключа подписания ключей необходимо будет обновлять вручную. Такие обновления вручную должны будут отвечать графику механизма RFC 5011 — новый якорь доверия должен быть добавлен в конфигурацию такого распознавателя с проверкой в период публикации (PUBLISH) процесса обновления ключа (подробнее см. в разделе 11), а старый якорь доверия не должен удаляться до тех пор, пока корневая зона не будет подписана с помощью нового ключа KSK корневой зоны. Более того, с точки зрения разумной операционной практики старый якорь доверия не следует удалять до тех пор, пока не будет отозван старый ключ KSK корневой зоны. Механизмы получения нового якоря доверия аналогичны механизмам, применяемым для неподключенных устройств, и описаны далее в настоящем документе.

Рекомендация 1. Обновление ключа на подписание ключей корневой зоны должно соответствовать процедурам, описанным в документе RFC 5011 для обновления якорей доверия во время обновления ключа для подписания ключей.

Устройства, которые во время обновления ключа KSK не подключены к Интернету, необходимо будет обновить вручную, когда они будут подключены после завершения обновления ключа. По сути, для таких устройств необходимо будет провести процедуру первоначальной настройки, как если бы они устанавливались впервые.

В общем случае процедура подготовки любого устройства для выполнения проверки DNSSEC должна основываться на подходе, позволяющем снизить вероятность использования неправильного якоря доверия. В настоящее время рассылаются общие рекомендации для таких устройств в виде проекта интернет-документа IETF[13], озаглавленного «*Публикация якоря доверия DNSSEC для корневой зоны*», однако необходимо провести дополнительный анализ, чтобы прийти к некой стабильной согласованной версии документа с рекомендациями по реализации.

Группа разработчиков поддерживает обсуждение и рассмотрение сообществом проекта интернет-документа в IETF с целью опубликовать некую стабильную спецификацию, прошедшую рассмотрение специалистами, в виде документа RFC.

Существует несколько практических сценариев получения актуальных якорей доверия, которые кратко объясняются далее в настоящем документе.

6.2.1.1 Дальнейшее обсуждение документа RFC 5011

Ранее в тексте упоминались распознаватели, которые «не могут или не хотят» полагаться на подход, определенный в документе RFC 5011. В данном разделе приводится объяснение такой формулировки.

Идея таймера добавления и удержания ключей, предусмотренная документом RFC 5011, имеет большое значение. Такой таймер призван не допустить принятия ложно представленного ключа. Иными словами, если какая-то организация захочет представить ложный ключ KSK, она может успешно опубликовать этот ключ. В таком случае подлинная организация, выпускающая ключи, сможет заявить о недостоверности ложного ключа еще до того, как от него будут зависеть какие-то операции.

Сопротивление распознавателей идее документа RFC 5011 вызвано не вопросами, касающимися структуры механизма обновления. Скорее корни такого сопротивления нужно искать в нескольких различных практиках выполнения операций. Управление конфигурацией является важным фактором, вызывающим озабоченность, в тех случаях, когда речь идет об эксплуатации множества серверов, управление конфигурацией которых основано на push-рассылке файлов конфигурации. Механизм обновления, предусмотренный документом RFC 5011, основан на противоположном принципе, в соответствии с которым множество должным образом настроенных компьютеров самостоятельно получают и используют новые

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

данные, что отличает такой подход от централизованного управления конфигурацией.

С учетом этого у крупных операторов может использоваться некий ручной процесс, позволяющий использовать различные автоматизированные механизмы. Какая-то из авторизованных систем может оказаться именно тем инструментом, который отвечает принципам механизма обновления, предусмотренного документом RFC 5011. В ходе краткого неофициального опроса крупные операторы заявили, что они рассчитывают на несколько различных способов проверки и подтверждения подлинности нового ключа KSK корневой зоны, в том числе на обмен информацией между людьми для установления доверительных отношений. Именно по этой причине предлагаются альтернативы стандарту RFC 5011.

При более глубоком анализе операционных аспектов RFC 5011 было выявлено несколько пробелов. Первый пробел касается дистанционного подтверждения успешного выполнения процедуры RFC 5011. Второй пробел касается возможности тестировать обновление ключей с учетом использования таймера добавления и удержания.

Необходимо обеспечить некий способ, посредством которого можно было бы сообщать источнику доверия о якорях доверия, которые используются на распознавателях. В контексте озабоченности темой тотального наблюдения цель в данном случае заключается не в том, чтобы узнать конфигурацию и возможности конкретного распознавателя, а в том, чтобы сначала убедиться в достаточном соблюдении процедуры RFC 5011 и составить представление о том, когда будет приемлемо перейти к использованию нового ключа KSK корневой зоны.

Также была определена и необходимость обеспечить возможность оперативного проведения функционального тестирования, в ходе которого можно было бы наблюдать выполнение этапов процесса RFC 5011, не соответствующих необходимой модели безопасности. В частности, необходимы инструменты, которые могли бы переназначать указанные значения таймера добавления и удержания, чтобы иметь возможность использовать меньшие значения во время тестирования. Желательно предусмотреть некий защитный механизм для недопущения использования тестовых значений таймера добавления и удержания в реальной производственной среде. Эта рекомендация направлена на разработчиков инструментов и поставщиков программного обеспечения DNS.

6.2.1.2 Другие форматы якорей доверия

С момента первоначального подписания корневой зоны ICANN опубликовала на веб-сайте якорь доверия в форматах, отличных от DNS[14]. Такие якори доверия представляют собой некритический путь для распространения и получения якорей доверия корневой зоны с помощью инструментов, находящихся вне пределов операций DNS. Для доступа к файлам на данном веб-сайте не нужно обращаться к DNS. С учетом соображений использования некритического пути это позволяет распространять новые якоря доверия. В будущем, чтобы подчеркнуть необходимость в новых возможностях, можно будет добавлять якори доверия, использующие различные криптографические алгоритмы[15] DNSSEC. Это также можно будет использовать в качестве средства заблаговременной, предварительной передачи данных на распознаватели на случай экстренного обновления ключей в чрезвычайных ситуациях.

6.2.1.3 Поставщики программного обеспечения DNS

Якори доверия могут объединяться поставщиками в пакеты с программным обеспечением DNS (с открытым или закрытым/коммерческим исходным ходом). Для поддержания актуальности программного обеспечения поставщик ПО должен будет выпустить новую версию якоря доверия.

Важно, чтобы распространенные таким образом якоря доверия были настоящими и использовали все существующие механизмы проверки и подтверждения для обеспечения целостности ПО конечных систем. Поставщики ПО нуждаются в надежной и эффективной методике для обеспечения подлинности якорей доверия, которые они распространяют со своим ПО, поскольку последствия распространения ненастоящих ключей могут быть потенциально очень большими, в особенности если в рамках стратегии обновления ПО поставщиками используются ключи для подписания кода.

Рекомендация 2. ICANN следует определить ключевых поставщиков программного обеспечения DNS и работать в тесном контакте с ними для формализации процедур, которые позволили бы обеспечить надежность и безопасность распространения якорей доверия по каналам конкретных поставщиков.

[14] https://www.iana.org/dnssec/files
[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

6.2.1.4 Системные интеграторы

Одним из способов распространения якорей доверия DNSSEC является распространение через системных интеграторов, таких как поставщики пакетов и операционных систем. В таком случае системный интегратор предоставляет обновленные пакеты для всех экземпляров якорей доверия в системе. Ряд дистрибьюторов Linux прилагают усилия для того, чтобы предоставлять пакет с одним главным экземпляром якоря доверия.

Рекомендация 3. ICANN следует определить ключевых системных интеграторов DNS и работать в тесном контакте с ними для формализации процедур, которые позволили бы обеспечить надежность и безопасность распространения якорей доверия по каналам конкретных интеграторов.

6.2.1.5 Системные администраторы

Системные администраторы могут вручную загружать якори доверия DNSSEC с поддерживаемого ICANN веб-сайта IANA при установке или обновлении ПО. Текущие якоря доверия корневой зоны предоставляются оператором функций IANA через специальный веб-сайт[16], посвященный информации о DNSSEC в корневой зоне. Определение подлинности загружаемых якорей доверия является важнейшим фактором установления доверия в DNSSEC. Для поддержки проверки подлинности различных типов подписей на том же специальном веб-сайте публикуются сертификаты в форматах OpenPGP, PKCS#7 и X.509, содержащие ключ подписания корневой зоны.

Несмотря на то, что определение подлинности крайне важно, ему часто не уделяется достаточно внимания, а вопросы, связанные с ним, недостаточно проработаны. Когда процедуры поддержки проверки подлинности были опубликованы для общественного обсуждения, было получено незначительное количество комментариев по сути. Это ставит под угрозу усилия по обеспечению надлежащей поддержки проверки подлинности. Представляется целесообразным провести дополнительное рассмотрение этого вопроса (с внесением при необходимости изменений при сохранении обратной совместимости). Как уже было сказано ранее, группа разработчиков поддерживает обсуждение и рассмотрение сообществом ранее упомянутого проекта интернет-документа, озаглавленного «*Публикация якоря доверия DNSSEC для корневой зоны*», в IETF с целью опубликовать некую стабильную

[16] См. список по адресу: //www.iana.org/dnssec/files

спецификацию, прошедшую рассмотрение специалистами, в виде документа RFC.

Более того, из наблюдений за получением цифровых подписей с поддержкой подлинности можно сделать вывод, что лишь немногие (или вовсе никто) из сторон взаимодействия используют цифровые подписи. Для обеспечения доверия недостаточно просто предоставить цифровые подписи, необходимо активно продвигать соответствующие методики.

Рекомендация 4. ICANN следует играть активную роль в продвижении надлежащих методов проверки подлинности якорей доверия корневой зоны, в том числе за счет подчеркивания важности информации, публикуемой на веб-сайте ICANN, посвященном функциям IANA.

6.3 Последствия для управления ключом KSK корневой зоны

Как описано в документе *«Практическое заявление DNSSEC для оператора KSK корневой зоны»* оператор KSK корневой зоны подписывает все наборы записей DNSKEY RRset верхушки корневой зоны с помощью ключа KSR, предоставленного оператором ключа ZSK корневой зоны. Результатом этого является ключ SKR, который содержит набор подписанных записей DNSKEY RRset и который передается специалисту по обслуживанию корневой зоны.

Эти процедуры хорошо документированы и, что касается действий, предпринимаемых в ходе церемонии подписания ключа KSK, открыты для внешнего аудита и широкого наблюдения; группа разработчиков считает крайне важным избегать любых существенных изменений этих процедур в результате изменения ключа KSK во избежание нарушения процедуры, которая в ее нынешней форме предоставляется совершенно понятной.

Рекомендация 5. Обновление ключа для подписания ключей для корневой зоны не должно требовать существенных изменений существующих процессов для сохранения связанных с такими процессами высоких стандартов прозрачности.

Каждый ключ KSR охватывает период времени в один календарный квартал (3 месяца или приблизительно 90 дней) и делится на 9 слотов по 10 дней каждый. Если в период времени входит более 90 дней, то последний слот в этом периоде продлевается до конца периода. По этой причине все изменения набора записей ресурсов DNSKEY RRset коревой зоны, например, добавление и/или удаление ключей, что необходимо при обновлении ключа, должны

соответствовать таким 10-дневным периодам, чтобы свести к минимуму любые существенные изменения процессов, которые используются для публикации подписанной корневой зоны.

Рекомендация 6. Все изменения наборов записей RRset DNSKEY корневой зоны должны быть согласованы с 10-дневными временными слотами, описанными в заявлении DPS оператора ключа KSK.

В рамках стандартных периодов размер ответов на запросы записей ресурсов DNSKEY RRset корневой зоны увеличивается в каждый первый и последний слот каждого временного цикла. Первый слот содержит ключ ZSK после публикации из предыдущего временного цикла, а последний слот содержит ключ ZSK перед публикацией для следующего временного слота.

Чтобы свести к минимуму возможные проблемы, связанные с увеличенным размером ответов DNS, рекомендуется спланировать график обновлений ключей таким образом, чтобы поддержать минимальный возможный размер ответов на запросы DNSKEY RRset. Проблемы, связанные с размером ответов, подробно рассматриваются далее в настоящем документе; там же приводятся соответствующие документации. Кроме того, далее в настоящем документе также приводится пример графика обновления ключа KSK корневой зоны, составленный с учетом приведенных выше соображений.

6.4 Соображения криптографической защиты

Группа разработчиков рассмотрела вопрос о том, существует ли достаточно убедительное основание для рассмотрения изменения размера ключа или алгоритма создания ключа KSK. Убедительные основания могут появиться в связи с вопросами, связанные с прочностью криптографической защиты для выбранного размера или алгоритма создания ключа.

После первоначальной публикации в 2005 году документа SP 800-57, часть 1 (*Рекомендации по отношению управления ключами*), Национальный институт стандартов и технологий США (NIST) объявил о намерении повысить минимальный уровень прочности криптографической защиты. Однако за 5 лет, прошедших после публикации и до предлагаемой конечной даты, технологии факторизации прогрессировали не так быстро, как ожидалось. В настоящее время ничто не свидетельствует о насущной необходимости использовать ключи большей длины для ключа KSK корневой зоны.

6.4.1 Криптография конечного поля

В опубликованном в 2012 году ежегодном отчете инициативы ECRYPT II по алгоритмам и размерам ключей асимметричный ключ RSA длиной 2048 бит считается эквивалентным симметричному ключу длиной 103 бита[17]. В том же отчете рекомендуется для защиты в течение приблизительно 10 лет использовать ключи с длиной не менее 96 бит. В документа NIST *«Рекомендации в отношении управления ключами — часть 1: общие положения (редакция 3)»*[18] ключ RSA длиной 2048 бит считается эквивалентным защите уровня 112 бит, а такой уровень прочности защиты считается приемлемым для использования в период с 2014 года по 2030 год. В документе *«Référentiel Général de Sécurité»*[19] французского агентства Agence nationale de la sécurité des systèmes d'information (ANSSI) ключ RSA длиной 2048 бит также считается безопасным для использования до 2030 года.

Как правило, срок жизни подписанного содержания в корневой зоне невелик, поскольку периоды подписей DNSKEY измеряются днями (приблизительно 15 дней), и группа разработчиков считает, что ключ RSA длиной до 2048 бит будет безопасно использовать в течение еще 5 дней, если в области факторизации больших целых чисел не произойдет какого-то существенного технологического прорыва.

6.4.2 Эллиптическая криптография

Еще одним алгоритмом, который можно использовать в DNSSEC, является алгоритм цифровой подписи на основе эллиптической кривой (ECDSA), который определен в документе RFC 6605[20]. Некоторые характеристики алгоритма ECDSA делают желательным его использование в качестве алгоритма ключа для подписания ключей корневой зоны. Такие ключи отличаются гораздо меньшим размером при сохранении прочности, аналогичной ключам RSA. По текущим оценкам ключ ECDSA с кривой P-256 обладает прочностью, приблизительно эквивалентной прочности ключей RSA с длиной ключа 3072 бита (NIST) или 3248 бит (ECRYPT II). Однако этот алгоритм был стандартизирован для использования в DNSSEC только относительно недавно — документ RFC 6605 был опубликован в 2012 году — а в ходе измерений, описанных далее в настоящем документе, было отмечено, что средства проверки поддерживают алгоритм ECDSA не настолько широко, как RSA (см. раздел 7 — Операционные соображения).

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
[20] https://tools.ietf.org/html/rfc6605

Кроме того, исследовательская группа криптографического форума IETF (CFRG) также работает над новым документом RFC «Эллиптические кривые в области безопасности», призванным повысить надежность шифрования с использованием методов на основе эллиптических кривых, и эта группа выражает определенную озабоченность сообщества специалистов в области криптографии в отношении генерирования и потенциальной слабости кривых, которые используются ECDSA. Прежде чем переходить на использование нового алгоритма на основе эллиптических кривых для подписания корневой зоны, желательно дождаться, пока группа CFRG завершит свою работу над этим документом.

6.4.3 Выводы

Руководствуясь описанной выше информацией, группа разработчиков пришла к выводу об отсутствии насущной необходимости в изменении алгоритма или размера ключа KSK с 2048-битного RSA. Кроме того, группа разработчиков также узнала о реализации распознавателя DNS с проверкой подлинности, требующей, чтобы корневая зона была подписана всеми алгоритмами, отвечающими настроенным якорям доверия, в результате чего обновление ключа для других алгоритмов потребовало бы применения другого подхода, отличного от того, который используется при обновлении ключа KSK. Это еще одна практическая причина, по которой не следует спешить с изменением алгоритма в настоящее время. Группа разработчиков связалась с поставщиком по поводу данной проблемы и требований этого поставщика, и ожидается, что эта проблема будет устранена в будущем для еще не запланированных операций по обновлению ключа KSK.

По этим причинам в новом ключе KSK для первого обновления ключа KSK следует использовать 2048-битный ключ RSA, однако изменение алгоритма и/или длины ключа стоит рассмотреть для будущих операций обновления ключа KSK.

Рекомендация 7. Группа разработчиков рекомендует для первого изменения ключа для подписания ключей корневой зоны поддерживать существующий алгоритм и размер ключа для поступающего нового ключа для подписания ключей.

Рекомендация 8. Для поступающих обновлений ключа для подписания ключей корневой зоны в будущем следует пересмотреть выбор алгоритма и размера ключа.

6.5 Координация и обмен информацией

6.5.1 Координация усилий с техническим сообществом и партнерами по каналам распространения

ICANN следует разработать и выполнить план по обмену информацией для повышения осведомленности об обновлении ключа KSK корневой зоны. Для повышения осведомленности следует использовать технические форумы, например, те, на которых было представлено первоначальное развертывание DNSSEC в корневой зоне.

Новым термином «партнеры по каналам распространения» называются внешние организации, содействующие в использовании DNSSEC независимо от управления корневой зоной. Такие партнеры как бы распространяют по своим каналам преимущества подписания корневой зоны от RZM-партнеров далее в глобальный общедоступный Интернет.

Партнеры по каналам распространения распределены по трем основным областям. Первые — это те, кто делает возможным использование DNSSEC, кто разрабатывает ПО для проверки DNSSEC и занимается в том числе реализацией RFC 5011. Вторые — это дистрибьюторы программного обеспечения и систем, в том числе ПО для проверки DNSSEC, которые занимаются прежде всего распространением экземпляров ключа KSK корневой зоны. Третьи — это операторы систем, обеспечивающих проверку подлинности в DNSSEC и использующих ключ KSK корневой зоны.

Для содействия обмену информацией группа разработчиков рекомендует хранить в файле контактные данные каждого партнера по каналам распространения, если такой партнер не возражает против этого, и рассылать по таким контактным данным обновления ключа KSK. Такой контактный список не должен быть эксклюзивным или использоваться для обмена материалами, которые отсутсвуют в свободном доступе. Данный список контактов призван помочь в обеспечении осведомленности о различных этапах обновления ключа KSK корневой зоны. При этом такой список должен оставаться закрытым, чтобы партнеры по каналам распространения могли управлять доступностью своей избранной контактной информации.

Рекомендация 9. ICANN в сотрудничестве с RZM-партнерами должна подготовить и выполнить план информационной работы для повышения осведомленности об обновлении ключа для подписания ключей корневой зоны, включающий информирование глобального технического сообщества в рамках соответствующих технических конференций, а

также по каналам партнеров, в частности, определенных в настоящем документе.

6.5.2 Координация с операторами корневых серверов

Любые структурные изменения содержимого корневой зоны потенциально могут воздействовать на операционное поведение отдельных корневых серверов. Первоначальный ввод в эксплуатацию AAAA-записей адресного пространства IPv6 в корневой зоне и последующее развертывание DNSSEC могут служить примером изменений, которые были осуществлены в рамках консультаций и тесной координации усилий с операторами корневых серверов, поскольку такие изменения вызвали изменения в структуре запросов. С учетом этого благоразумие в отношении критически важной инфраструктуры требует использования консервативного подхода к любым изменениям на случай неожиданных последствий, которые могут отрицательно сказаться на производительности всей системы корневых серверов в целом.

Эксперименты, проведенные в рамках подготовки настоящего документа, свидетельствуют о том, что обновление ключа KSK не приведет к отрицательным последствиям, однако, как и в случае с предыдущими примерами структурных изменений, упомянутыми выше, рекомендуется использовать консервативный подход.

Группа разработчиков рекомендует отдельным операторам корневых серверов относиться к тем или иным конкретным событиям в рамках периода обновления ключа KSK так же, как они отнеслись бы к важным запланированным операционным событиям, то есть публиковать открытые уведомления о состоянии и координировать свои действия с другими операторами корневых серверов с использованием обычных каналов обмена информацией в режиме реального времени, которые используются в таких случаях. К таким событиям следует отнести период до и после добавления нового ключа KSK к набору DNSKEY RRSet верхушки корневой зоны, а также удаление текущего ключа KSK из того же набора RRSet.

Группа разработчиков предлагает таким же образом использовать для таких событий каналы обмена информацией в режиме реального времени между отдельными операторами корневых серверов и ICANN и другими RZM-партнерами с тем, чтобы обеспечить своевременное определение и оперативное информирование о любых ожидаемых последствиях.

Перед подготовкой окончательной версии и публикацией подробного графика периода обновления ключа KSK его должны рассмотреть операторы корневых серверов, чтобы убедиться, что он не противоречит любым другим планам,

которые могут отрицательно сказываться на способности отдельных операторов корневых серверов обеспечивать желаемый уровень операционного покрытия. Необходимо предпринять практически осуществимые усилия по корректировке графика обновления ключа для недопущения операционных конфликтов.

Рекомендация 10. ICANN следует поручить комитету RSSAC координировать рассмотрение подробного графика на период обновления ключа KSK перед его публикацией и удовлетворить разумные запросы изменения такого графика в тех случаях, когда это понадобится по каким-либо операционным причинам того или иного оператора одного из корневых серверов.

Рекомендация 11. ICANN следует координировать свои усилия с комитетом RSSAC и RZM-партнерами и обеспечить использование каналов связи в режиме реального времени для обеспечения операционной осведомленности системы корневых серверов о каждом изменении корневой зоны, подразумевающем добавление или удаление ключа KSK.

Содействовать пониманию операционных последствий обновления ключа KSK для средств проверки и самих операторов корневых серверов будет сбор данных операторами корневых серверов в ходе обновления ключа KSK. Поскольку система корневых серверов отличается разнообразием как по своей архитектуре, так и по распределению в Интернете, существует понимание того, что возможности сбора данных отдельными операторами корневых серверов в долгосрочной перспективе будут сопряжены с различными ограничениями, которые затруднительно охарактеризовать в краткой форме для всей системы в целом. Существует также понимание того, что уже существуют базовые возможности сбора данных для удовлетворения тактических требований в части мониторинга условий обслуживания в режиме реального времени по мере выполнения обновления ключа KSK.

В ходе первоначального развертывания DNSSEC в корневой зоне выполнялась обширная операция по сбору данных, и собранные в результате данные пригодились для неинтерактивного анализа реакции системы DNS в целом на структурные изменения, происходящие в корневой зоне, в том числе независимого анализа, который проводился при поддержке DNS-OARC[21]. В ходе первого обновления ключа KSK намечено провести аналогичную операцию.

[21] https://www.dns-oarc.net

Рекомендация 12. ICANN следует координировать с комитетом RSSAC, чтобы поручить операторам корневых серверов осуществлять сбор данных, призванных служить информационной основой для последующего анализа и определения характеристик операционных последствий обновления ключа для подписания ключей, а также обеспечить доступность планов и продуктов такого сбора данных для независимого анализа.

6.5.3 Координация действий между оператором ключа подписания ключей (KSK) и оператором ключа подписания зоны (ZSK)

Ответственность за управление ключом KSK корневой зоны возлагается отдельно соответственно на оператора функций IANA и специалиста по обслуживанию корневой зоны. Управление этими двумя ролями осуществляется по отдельности.

В качестве ключа ZSK корневой зоны в настоящее время используется 1024-битный ключ RSA, как указано в заявлении DPS специалиста по обслуживанию корневой зоны[22]. Возможно, в будущем специалист по обслуживанию корневой зоны увеличит размер ключа ZSK.

Ключ ZSK регулярно обновляется по 90-дневному графику, и ожидается, что в период обновления ключа KSK эта работа будет продолжаться в штатном режиме; поскольку ожидается, что период обновления ключа KSK продлится дольше, чем 90 дней, могут быть периоды, в течение которых набор записей ресурсов DNSKEY RRSet верхушки корневой зоны будет содержать 4 ключа в зависимости от итогового плана.

Увеличение размера ключа ZSK во время выполнения обновления ключа может вызывать различное поведение средств проверки на протяжении части периода обновления ключа ZSK, возрастет также размер ответов. Это может затруднить усилия по определению, пониманию и устранению возможных операционных проблем.

Любое решение, касающееся ключа ZSK, выходит за рамки настоящего документа. Однако мы рекомендуем ICANN координировать действия со специалистом по обслуживанию корневой зоны с тем, чтобы гарантировать, что любое возможное изменение размера ключа ZSK в будущем будет тщательно координироваться с обновлением ключей ZSK, чтобы эти две операции не выполнялись одновременно.

[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

Рекомендация 13. RZM-партнеры должны сделать так, чтобы любое увеличение размера ключа подписания зоны в будущем тщательно координировалось с обновлением ключа для подписания ключей с тем, чтобы эти две операции не выполнялись параллельно.

7 Влияние на распознаватели с проверкой подлинности

7.1 Соображения, касающиеся размера пакетов

Система DNS задумывалась для работы на основе транспортных протоколов UDP и TCP. В концепции протокола DNS предпочтение отдавалось протоколу UDP в связи с меньшими накладными расходами в сравнении с протоколом TCP, в особенности в том, что касается сохранения состояния подключений на сервере. Однако такой выбор протокола накладывает определенное ограничение. В первоначальном определении DNS в стандарте RFC 1035 ответы UDP были ограничены 512 октетами. Такое ограничение в 512 октетов по-прежнему соблюдается в программном обеспечении, используемом сегодня.

В рамках механизма расширения DNS и EDNS(0), который был впервые определен в документе RFC, опубликованном в августе 1990 года [RFC 2671, дополненный и измененный документом RFC 6891], клиент, отправляющий запрос DNS, может информировать сервер DNS о том, что он может обрабатывать ответы UDP, размер которых превышает 512 октетов. Клиент, отправляющий запрос, помещает в него максимальный размер полезной нагрузки UDP (это не размер пакета IP, а размер сообщения DNS), а сервер должен отправить ответ UDP, в котором полезная нагрузка DNS не должна превышать указанный размер буфера. Если это невозможно, сервер устанавливает в ответе специальный бит усечения, который указывает на то, что данные были усечены. Если усеченный ответ содержит действительное сообщение DNS, получатель может принять решение использовать усеченный ответ. В противном случае автор запроса открывает сеанс связи с сервером по протоколу TCP и повторяет запрос с использованием протокола TCP.

Системы DNS, использующие DNSSEC, должны сигнализировать о своей способности с помощью флага DO (DNSSEC OK) в псевдозаголовке EDNS. Поскольку операционные последствия, рассматриваемые в настоящем документе, касаются исключительно систем, поддерживающих DNSSEC, такие системы могут также использовать EDNS(0) (поскольку EDNS требует поддержки EDNS(0), поэтому они не ограничены лимитом в 512 октетов.

Клиент может инициировать операцию по протоколу TCP, однако распространенным вариантом поведения является инициирование операции по протоколу UDP и использование бита усечения для указания на то, что отправитель запроса должен использовать TCP.

Фрагментация пакетов UDP по-разному обрабатывается в протоколах IPv4 и IPv6. Если пакет слишком большой для передачи с помощью используемого транспортного протокола передачи IP-пакетов, IP-пакет может быть фрагментирован. В таком случае последующие фрагменты используют тот же заголовок уровня IP (в том числе поле номера протокола UDP), однако явным образом исключают псевдозаголовок UDP. В протоколе IPv4 фрагментировать IP-пакет может первоначальный отправитель или любой промежуточный маршрутизатор, если не установлен флаг IP Don’t Fragment. В протоколе IPv6 фрагментировать IP-пакет может только первоначальный отправитель. Если какой-либо промежуточный маршрутизатор не может переслать пакет на следующий сегмент маршрутизации, то в протоколе IPv6 такой маршрутизатор сформирует диагностический пакет ICMPv6 с размером MTU от следующего сегмента маршрутизации и начальной частью пакета и отправит эту информацию назад отправителю пакета.

При использовании UDP отправитель не поддерживает буфер неподтвержденных данных, поэтому при получении такого сообщения отправитель пакета IPv6 не сможет повторно отправить первоначальные данные. Эмпирическим путем можно прийти к предположению, что во многих вариантах реализации IPv6 стандартный ответ заключается в создании записи узла в локальной таблице маршрутизации IPv6 и записи полученного значения MTU в эту таблицу на какое-то определенное время кэширования, которое определяется локально. Это означает, что при всех последующих попытках отправить пакет UDP протокола IPv6 по указанному адресу такое значение MTU будет использоваться для определения способа фрагментации отправленного пакета.

7.1.1 Опыт измерения

Был подготовлен и проведен эксперимент, призванный воспроизвести ситуацию в среде корневого сервера для оценки влияния больших размеров пакетов на распознаватели и на пользователей.

Для этого одна из платформ онлайн-рекламы использовалась для того, чтобы побудить распознаватели DNS отправлять уникальные запросы на полномочный сервер, настроенный таким образом, чтобы отправлять на запросы для двух зон ответы разного размера. Считается, что распознаватели,

отправляющие запросы на полномочный сервер имен в рамках этого теста, примерно совпадают с набором распознавателей, которые, как ожидается, будут отправлять запросы в корневую зону.

Чтобы протестировать возможность получения распознавателями больших ответов, рекламная платформа выдавала запросы целевого доменного имени. Само это целевое доменное имя возвращало ответы обычного размера. Однако для того, чтобы получить конечный ответ, распознаватель сначала должен получить большой промежуточный ответ. Если распознаватель мог успешно хотя бы запросить информацию о целевом доменном имени, то для целей теста считалось, что распознаватель продемонстрировал способность обрабатывать большие промежуточные ответы.

Кроме того, тест включал получение веб-объекта с веб-сервера эксперимента, что позволяло экспериментаторам сопоставить адреса, которые использовались для чтения данных веб (IP-адреса конечных пользователей) с адресами, которые использовались распознавателями имен при отправлении запросов к DNS.

В этом тесте использовался ответ DNS размером 1444 октета.

7.1.2 Результаты теста

За период в 5 дней в мае 2015 года приблизительно 7,26 млн конечных систем успешно получили небольшую контрольную запись, а из них 7,17 млн систем успешно получили тестовую запись. Разница составила приблизительно 90 000 пользователей, или 1% от тестового набора — это системы, которые не смогли получить тестовую запись DNS размером 1444 октета.

Эти конечные системы использовали приблизительно 83 000 различных IP-адресов распознавателей DNS. 90% таких распознавателей успешно получили как контрольную запись, так и тестовую запись. Из 4251 распознавателей, которые получили контрольную запись, 3396 распознавателей использовали расширение EDNS(0) с установленным битом DNSSEC OK, что инициировало отправку размером 1444 октета. Из таких не справившихся с задачей распознавателей 3110 наблюдались только один раз в течение эксперимента, а 826 распознавателей не справились с задачей более одного раза. Это означает, что 1% распознавателей, наблюдавшихся в ходе данного эксперимента, не смогли получить ответ большого размера два или более раз, а еще 3% распознавателей, не справившихся с получением большого ответа, наблюдались только один раз, чего недостаточно, чтобы сколько-нибудь уверенно утверждать, что они не смогут постоянно обрабатывать большие ответы. Такой 1% распознавателей, которые не справились с задачей два или

более раз, использовались менее чем 3000 конечных систем, участвовавших в тесте.

5237 распознавателей использовали в этом тесте адреса IPv6 (6% от общего количества), при этом 830 из таких распознавателей не смогли получить тестовую запись (21% от распознавателей, не справившихся с задачей). Такие данные могут свидетельствовать о существовании потенциальной проблемы, связанной с распознавателями, использующими IPv6, и тем, как они обрабатывают значение размера MTU.

Что касается измерения изменения нагрузки, связанной с запросами при использовании ответов большого размера, контрольное имя (с размером ответа 93 октета) запрашивалось 16,4 млн раз, при этом наблюдалось 475 запросов с использованием TCP. Тестовое имя (с размером ответа 1444 октета) запрашивалось 18,6 млн раз, при этом 1,2 млн из таких запросов осуществлялись по протоколу TCP — это 6,5% от общего количества запросов тестового имени. Существует разница между общим количеством запросов, сделанных к контрольной записи, и общим количеством запросов к тестовой записи. Эту разницу можно объяснить тем, что распознаватели реагировали на получение усеченных ответов на запросы к тестовой записи отправлением еще одного запроса по протоколу TCP. Такой результат относительно неплохо коррелирует с распространением размеров буфера UDP, которые обеспечиваются для запросов UDP расширениями EDNS(0). Выдавая ответы больших размеров, полномочный сервер может ожидать повышения нагрузки в результате запросов, а также увеличение доли запросов, использующих протокол TCP.

7.1.3 Выводы

Приблизительно 1% распознавателей DNS, устанавливающих в своих запросах флаг DNSSEC OK, по всей видимости, не могут получать ответ DNS размером 1444 октета (с учетом факторов экспериментальной неопределенности верхним пределом такого количества можно считать 6% от всех распознавателей). В таком наборе распознавателей непропорционально широко представлены распознаватели, использующие в качестве транспортного протокола IPv6. Возможно, такое количество распознавателей, не справившихся с задачей, вызвано присутствием различных форм промежуточного ПО, перехватывающего запросы DNS, или, в случае IPv6, — возможной неправильной обработкой сообщений ICMP6 *Packet Too Big*, однако в точности определить природу таких ошибок в рамках данной экспериментальной методики невозможно.

Распознаватели, которые не смогли получить ответы, обслуживают очень незначительное количество пользователей. Количество пользователей, использующих распознаватели DNS, которые стабильно демонстрируют неспособность разрешить доменное имя в DNS в тех случаях, когда ответ DNS достигает такого размера, составляет 0,04% от всех пользователей (с учетом факторов экспериментальной неопределенности верхним пределом такого количества можно считать 1% от всех пользователей).

В ходе этих экспериментов тестировалась обработка ответов DNS размеров 1444 октета. Отмечается, что другие части DNS уже предоставляли ответы, размеры которых существенно превышали рассматриваемый здесь размер, и что ответы такого размера, по всей видимости, не привлекали внимания широкой публики и не вызывали заметных комментариев. К примеру, сравнимый запрос DNSKEY для имени в зоне .org привел 6 июня 2015 к формированию ответа размером 1625 октетов, который содержал два 2048-битных ключа RSA для подписания ключей, два 1024-битных ключа RSA для подписания зоны и три подписи — по одной для каждого ключа для подписания ключей и одну для одного их ключей подписания зоны. Все распознаватели с проверкой подлинности, которые не могут принимать такие большие ответы DNS, не смогут проверить подлинность подписи как для записи DS, так и для записи NSEC3 (которые используются, чтобы сигнализировать о несуществующей записи DS) для каждой операции делегирования в зоне .org, что, по сути, вызовет ошибки разрешения DNS для имен, делегированных в зоне .org.

Группе разработчиков не известно о каких бы то ни было операционных проблемах, которые могли бы испытывать держатели доменных имен в зоне .org в связи с размером пакетов ответов DNS DNSKEY на запросы имен в зоне .org. Даже с учетом крайне незначительного количества подписанных зон в зоне .org такое отсутствие каких бы то ни было операционных отчетов об ошибках разрешения доменных имен зоне .org свидетельствует о том, что размер такого отчета вряд ли может представлять собой существенную операционную проблему при обновлении ключа KSK корневой зоны.

Одним из отличий между сценарием тестирования и реальной ситуацией в зоне .org является то, что выдавать запросы к большому запросу записей ресурсов DNSKEY RRset будут только те распознаватели, которые на самом деле выполняют проверку подлинности. В случае данного тестирования все распознаватели, устанавливающие флаг DNSSEC OK, пытались получить ответ большого размера. Как описано в разделе 8,2 менее чем 30% распознавателей, которые устанавливают в исходном запросе бит DNSSEC OK, впоследствии выполняют проверку ответа. Возможно, операторы

распознавателей, которые включали проверку, более тщательно отнеслись к определению и исправлению всех сетевых проблем, которые могли помешать им получать большие пакеты ответов, поскольку такие распознаватели в большей степени подвержены таким проблемам. Другие распознаватели, которые не выполняли проверку, могли сталкиваться с большими пакетами ответов только при относительно редких обстоятельствах и могли не знать о таких ограничениях, накладываемых на них их сетевым окружением.

Разумным представляется вывод, что подавляющее большинство тех, кто не смог принять ответ большого размера в ходе тестов, — это распознаватели, не выполняющие проверку подлинности, которые не влияют на увеличение размера записи ресурсов DNSKEY корневой зоны.

Подводя итоги, можно сказать, что испытать последствия увеличения размера ответов во время обновления ключа KSK могут менее 0,04% пользователей, однако это оценочное значение с большим коэффициентом неопределенности, а на основании наблюдения тенденции в доменах TLD с большими наборами ключей можно сделать вывод, что это верхний предел количества пользователей, на которых может сказаться увеличение размера ответов.[23]

7.2 Работа функции проверки DNSSEC

Существует три подлежащих измерению аспекта работы функции DNSSEC. Первый аспект — это получение цифровых подписей DNSSEC (установка флага DNSSEC OK в параметрах EDNS(0) запроса), второй — это функция проверки, когда создается цепочка доверия от ключа корневой зоны до проверяемого имени, а третий — это то, будет ли пользовательская конфигурация разрешения имен считать ошибку проверки DNSSEC окончательной ошибкой или же запрос будет направлен на другой распознаватель.

7.2.1 Результаты теста

В рамках описанного выше эксперимента (раздел 7.1.1) в мае 2015 года наблюдалась ситуация, в которой приблизительно 85-90% пользователей, при этом в наблюдаемых на полномочном сервере имен запросах результирующих для некэшированного имени запрос содержал параметр EDNS(0) и установленный флаг DNSSEC OK.

[23] Более подробные сведения о данном эксперименте и его результатах см. на странице http://www.potaroo.net/ispcol/2015-05/ksk.html.

Приблизительно 24% от этой же выборки пользователей впоследствии выполнили запросы, демонстрирующие, что распознаватель выполнял проверку ответов с помощью DNSSEC, следуя по цепочке взаимосвязанных подписей назад по иерархии делегированных имен к ключу KSK корневой зоны.

Приблизительно 11% из той же выборки пользователей отвечали тому варианту пользовательского поведения, при котором реакция на ошибку проверки DNSSEC из предыдущего прохода заключается в передачи запроса на другой распознаватель, не выполняющий проверку подлинности DNSSEC.

Из этого можно сделать вывод о том, что любые изменения в процессах проверки подлинности DNSSEC потенциально могут иметь последствия для приблизительно четверти от всех пользователей Интернета.

Из них несколько менее половины таких пользователей уже восприняли ошибки проверки DNSSEC (о чем сигнализирует флаг SERVFAIL) как сигнал для направления такого же запроса на другой распознаватель, который не выполняет проверку подлинности SERVFAIL. Для этих 11% пользователей Интернета изменение ключа KSK корневой зоны потенциально может приводить к невозможности распознавания ключа KSK корневой зоны и ошибкам проверки, однако такие пользователи продемонстрировали, что они уже интерпретируют флаг SERVFAIL как сигнал для отправки запроса на альтернативный распознаватель. Потенциальным результатом этого может быть увеличение времени разрешения имен, использующих подписи DNSSEC, однако это не приведет к невозможности разрешения имен вообще.

Остальные 13% пользователей, которые при получении ответа SERVFAIL не переключаются на распознаватель, не выполняющий проверку, потенциально могут быть подвержены риску невозможности разрешения имен с подписями DNSSEC, если используемые такими пользователями распознаватели не смогут выполнять сигналы, получаемые в процессе обновления ключа согласно спецификации RFC 5011.

7.2.2 Выводы

Данный процесс измерения невозможно использовать для проверки того, способны ли распознаватели следовать процедуре RFC 5011 для автоматического выбора значения нового ключа KSK корневой зоны. Максимум того, что можно сделать, — это оценить количество пользователей, которые используют распознаватели, выполняющие проверку DNSSEC, то есть используют распознаватели, которые либо поддерживают спецификации

RFC 5011, либо требуют ручного вмешательства для загрузки нового ключа KSK корневой зоны в соответствующий момент времени.

Приблизительно 24% пользователей используют распознаватели, выполняющие проверку DNSSEC, и, следовательно, могут столкнуться с последствиями обновления ключа KSK корневой зоны. Ошибка проверки возвращает ответ SERVFAIL и 11% всех пользователей используют такой набор распознавателей, для которого ответ SERVFAIL, получаемый от одного распознавателя, означает сигнал направить запрос для повторной попытки разрешения на распознаватель, не выполняющий проверку. Это означает, что 13% всех пользователей могут столкнуться с последствиями обновления ключа KSK корневой зоны, если их распознаватель не поддерживает спецификацию RFC 5011, а администратор распознавателя не загрузит новый ключ KSK корневой зоны в соответствующий момент времени.

Однако многие из таких пользователей используют одну из крупных служб распознавателей с проверкой подлинности, которые должны поддерживать спецификацию RFC 5011 (например, распознаватели DNS Comcast), так что такая цифра в 13% представляет собой своего рода верхний предел количества пользователей, которых могут таким образом затронуть последствия обновления ключей.

8 Тестирование

Есть два элемента, имеющих отношение к тестированию. Один из них — это действия по измерению влияния обновления ключа KSK на общую работу Интернета для того, чтобы отслеживать уровень негативных последствий, которые могут привести к остановке работы. Другой — это действия, касающиеся подготовки задействованных сторон к этой операции, в том числе выделение ресурсов на организацию опытной площадки для самотестирования. Самотестирование может проводиться партнерами по каналам распространения посредством разработки программного обеспечения и/или операторами посредством развертывания парка серверов, или же любыми другими заинтересованными лицами.

8.1 Тестирование влияния

В ходе проведения испытаний для измерения успешного выполнения проверки для целей настоящего отчета была обнаружена определенная реакция на ошибки проверки DNSSEC. Одним из способов оценить ущерб может быть использование свидетельств того, что некоторые запросы начинают с DNSSEC, а затем переключаются на DNS, и измерение возможного роста (или

снижения) частоты таких операций при обновлении ключа KSK. Этот так называемый ущерб мог бы остаться незамеченным, однако его можно использовать в качестве ценного показателя при наблюдении влияния операции по обновлению ключа KSK корневой зоны. Пользователи, сидящие за экранами своих компьютеров, скорее всего, не заметят этого и не обратятся с жалобами и с заявками на исправление неполадок в службу поддержки провайдера.

Тесты, позволяющее определить это, должны проводиться регулярно (ежемесячно) с настоящего времени и до завершения (успешного или не успешного) операции по обновлению ключа KSK корневой зоны. Проведение тестов перед обновлением ключа позволит определить базовый уровень показателей для дальнейшего сравнения.

Помимо автоматического тестирования во время обновления ключа KSK корневой зоны необходимо будет поддерживать контакт с партнерами по каналам распространения для обмена полной информацией в режиме реального времени или почти реального времени. Это будет служить фактором мотивации для заблаговременного уведомления сторон, подвергающихся воздействию, а также для того, чтобы избегать времени неполного присутствия персонала на рабочих местах и выбирать время, когда проще устанавливать и поддерживать контакт.

8.2 Ресурсы для проведения самотестирования

Для содействия участвующим сторонам в проведении самотестирования следует организовать испытательную платформу, воспроизводящую условия операционной платформы с ускоренными темпами обновления ключей. Помимо выполнения на серверах процедуры RFC 5011 в ускоренном режиме с подписанными имитационными моделями корневых зон, необходимо представить якоря доверия из раздела «прочие структуры данных» с такими же путями. Это будет содействовать созданию более эффективных инструментов, например, инструментов для проверки ключа, инструментов для обнаружения содержимого средств проверки (для локального или дистанционного потребления).

Это может помочь лучше понять новые алгоритмы за счет возможности вставлять и удалять ключи с различными параметрами.

Важной задачей является определение графика выполнения операций. Режим быстрее реального времени необходим для достоверного наблюдения за процессом. При этом режим реального времени также имеет свои преимущества, позволяя снизить эффект тестирования.

И наконец, необходимо решить вопрос соответствия характеристикам корневой системы. Следует рассматривать вопрос о том, будет ли использоваться в качестве данных вся корневая зона или же имитационная зона с репрезентативной выборкой данных.

Существуют примеры таких испытательных площадок,[24,25] которые могут использоваться в качестве моделей для будущего тестирования.

8.3 Тестирование операционной совместимости модификации ПО и процессов операторов ключей KSK и ZSK

Поскольку процесс обновления ключа KSK требует изменения существующих графиков, процессов и, возможно, программного обеспечения поддержки работы KSK, перед началом обновления ключа необходимо провести тщательное тестирование таких изменений, в том числе в том, что касается генерирования ключа, создания подписанного набора записей ресурсов DNSKEY RRset, проверки подлинности DNSSEC, обмена ключами KSR/SKR и всех возможных механизмов возврата к предыдущему состоянию, а также репетиции церемонии создания ключей.

9 Реализация

Предлагаемая процедура обновления ключа была впервые задумана в июле 2013 года и с тех пор изучалась и дорабатывалась. Описанную здесь процедуру следует считать черновым вариантом, который может дорабатываться RZM-партнерами перед реализацией.

Эта процедура делится на три этапа:

1) публикация нового ключа KSK корневой зоны;
2) переход на подписание с помощью нового ключа KSK корневой зоны (обновление ключа);
3) отзыв старого ключа KSK корневой зоны.

Отзыв старого ключа KSK корневой зоны намеренно задерживается, чтобы иметь возможность вернуться к предыдущему состоянию, если после удаления старого ключа KSK корневой зоны из набора ключей возникнут какие-либо проблемы с новым ключом KSK корневой зоны. Эта процедура должна отвечать спецификации RFC 5011 с расширенными окнами для добавления нового ключа и отзыва старого ключа KSK. Эта процедура явным образом позволяет возможность откладывать отзыв старого ключа KSK корневой зоны

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

на неопределенный период на тот случай, если в процессе обновления ключа возникнут непредвиденные проблемы, которые потребуют внести изменения в запланированный процесс обновления ключа.

На Рис. 1 ниже показана общая схема выполнения этой процедуры по трем кварталам. Необходимо учесть, что нумерация кварталов указана относительно начала процесса, а не в порядке календарного года. То есть I квартал и кв. I не обязательно означает время с января по март. Новый ключ KSK обозначен как KSK-NEW, а старый — KSK-2010.

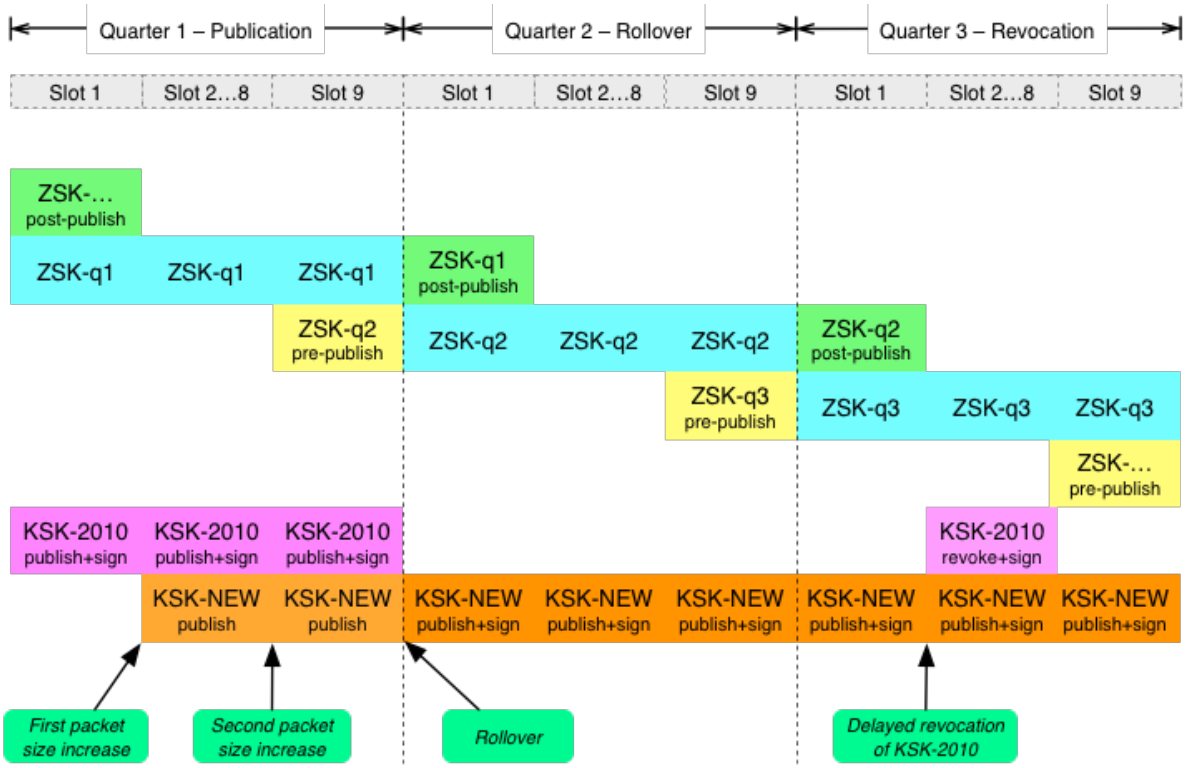

Рис. 1. Планирование графика обновления

9.1 Публикация нового ключа KSK

Новый ключ KSK добавляется в набор DNSKEY RRset в слот 2 кв. I, однако пока не используется для подписания. Это этап подготовительной публикации, позволяющей средствам проверки, совместимым со спецификациями RFC 5011, выбирать новый ключ KSK. Новый ключ KSK публикуется (и подписывается старым ключом KSK) в корневой зоне в течение в общей сложности 80 дней, прежде чем он будет использоваться для подписания. Ожидается, что настроенные вручную якори доверия будут обновлены для включения в них нового ключа KSK до или во время этого периода времени.

Для обновления ключа в соответствии со спецификацией RFC 5011 необходимо, чтобы новый ключ был опубликован в течение не менее чем 30 дней (время добавления и удержания) Если длительность предполагаемого 80-дневного периода публикации будет признана недостаточной, здесь можно вставить один или несколько дополнительных кварталов публикации перед обновлением ключа.

Во время квартала публикации нового ключа KSK распознаватели, выполняющие проверку DNSSEC, будут видеть увеличение размера пакетов ответа на запрос набора ключей DNSKEY RRset корневой зоны (размер пакета ответов) с 736 октетов до 1011 октетов. Такое условное увеличение основывается на сравнении размера ответов DNS на данном этапе при условии, что обновление ключа не выполняется, с размером ответа во время процесса обновления ключа. Во время последнего слота кв. I размер пакета ответов увеличивается с 833 октетов до 1158 октетов.

9.2 Переход на новый ключ KSK

После того как новый ключ KSK будет представлен, он будет использоваться для подписания набора ключей DNSKEY RRset корневой зоны, начиная с слота 1 кв. II. Этот квартал ничем не отличается от других кварталов за исключением того, что все наборы DNSKEY RRset подписываются только новым ключом KSK. Единственный раз, когда набор ключей DNSKEY RRset подписывается и старым, и новым ключом KSK, — это во время необязательного периода отзыва, который описывается ниже.

9.3 Отзыв старого ключа KSK

Если старый ключ KSK нужно отозвать, как описано в спецификации RFC 5011, старый ключ KSK публикуется с установленным битом отзыва и подписывается как старым, так и новым ключом KSK.

Отзывать старый ключ KSK необязательно. Если желательно отозвать ключ, публикация отзываемого старого ключа KSK выполняется начиная со слота 2 III кв. по слот 8 III кв.

Во время отзыва размер пакетов ответа возрастает с 736 октетов до 1297 октетов.

9.4 Влияние размера пакетов ответа

Желаемой целью является избежать фрагментации UDP, насколько это возможно. Далее приведены некоторые ограничения на размер ответа:

Размер	Ограничение
512 октетов	Минимальный размер полезной нагрузки DNS, который должен поддерживаться DNS
1232 октетов	Максимальный размер полезной нагрузки DNS для нефрагментируемого пакета IPv6 DNS UDP
1452 октета	Максимальный размер полезной нагрузки DNS для нефрагментированного пакета IPv6 DNS UDP
1472 октета	Максимальный размер полезной нагрузки DNS для нефрагментированного пакета IPv4 DNS UDP

Таблица 4. Ограничения на размеры пакетов

Представленные ранее результаты тестирования указывают на потенциальные проблемы с некоторыми распознавателями IPv6 и тем, как они обрабатывают большие ответы. Таким образом первым и самым распространенным ограничением по размеру является максимальный размер пакета IPv6 DNS UDP, который подразумевает размер пакета ответа DNSKEY не более 1232 октетов.

Первое ограничение достигается только во время необязательного этапа отзыва, когда необходимо повторно представить ключ KSK корневой зоны и отметить его битовым флагом отзыва. Для обеспечения полной совместимости со спецификацией RFC 5011 предусмотрено требование двойного подписания набора ключей DNSKEY RRset на этапе отзыва как новым ключом KSK корневой зоны, так и старым ключом KSK корневой зоны. Двойное подписание набора ключей RRset приводит к тому, что размер ответа превышает 1232 октетов.

Самым большим отдельным пакетом ответа для корневой зоны является подписанный набор ключей DNSKEY RRset. В следующей таблице представлены общие сведения о размерах пакетов ответа DNSKEY во время предлагаемого обновления ключа, а также сравнение с размерами пакетов ответа вне периода обновления ключа.

Время	DNSKEY во время обновления	RRSIG во время обновления	Размер ответа DNSKEY во время обновления	Размер ответа DNSKEY вне периода обновления
I кв., слот 1	1x KSK + 2xZSK	1x KSK	883 октета	883 октета
I кв., слот 2...8	2x KSK + 1xZSK	1x KSK	1 011 октета	736 октета
I кв., слот 9	2x KSK + 2xZSK	1x KSK	1158 октетов	883 октета
II кв., слот 1	1x KSK + 2xZSK	1x KSK	883 октета	883 октета
II кв., слот 2...8	1x KSK + 1xZSK	1x KSK	736 октетов	736 октетов
II кв., слот 9	1x KSK + 2xZSK	1x KSK	883 октета	883 октета
III кв., слот 1	1x KSK + 2xZSK	1x KSK	883 октета	883 октета
III кв., слот 2...8	2x KSK + 2xZSK	2x KSK	1297 октетов	736 октетов
III кв., слот 9	1x KSK + 2xZSK	1x KSK	883 октета	883 октета

Таблица 5. Размеры пакетов во время обновления ключа

(Цветовое кодирование в таблице выше соответствует графику ниже.)

Риски, связанные с избежанием отзыва старого ключа, подробно не обсуждались, однако на данный момент этап отзыва ключа можно рассматривать как необязательный. В качестве одного из возможных вариантов решения можно было бы изменить в этом отношении стандарт RFC 5011 и не требовать двойного подписания для отзыва старого ключа. Такая поправка обеспечила бы к тому же дополнительное преимущество — возможность отзывать утерянный или уничтоженный ключ. Отсутствие необходимости в двойной подписи для старого ключа также упростило бы обновление ключа в будущем, а также изменение алгоритма или длины ключа. Однако по причине времени, которое необходимо для повторного определения, публикации, разработки и распространения кода, а также внедрения такого кода в работу, этот вариант не представляется осуществимым для данного обновления ключа KSK.

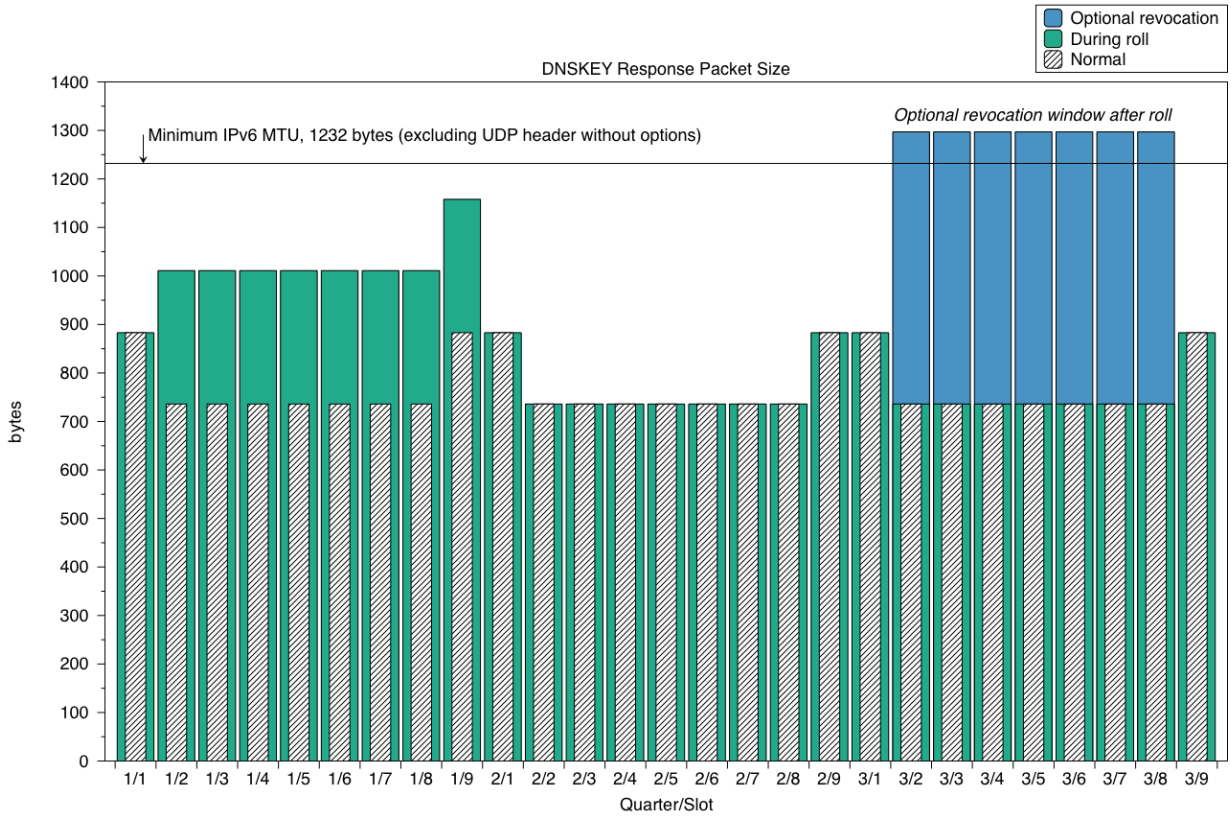

Рис. 2. Размеры пакетов ответа DNSKEY

9.5 Развертывание по отдельным корневым серверам

Введение в 2010 году расширений безопасности DNSSEC осуществлялось отдельно для каждого корневого сервера. Предварительная версия зоны, подписанной с помощью DNSSEC, появилась на одном сервере в январе 2010 года, на другом корневом сервере — в феврале, еще на двух корневых серверах — в марте, и т. п. Задачей было предоставить рекурсивным серверам (или другим отправителям запросов на корневые серверы) возможность сначала испытать работу DNSSEC и вернуться к предыдущему состоянию в случае неприемлемых результатов.

Такая стратегия предлагалась для обновления ключа KSK корневой зоны, однако от этой идеи быстро отказались по целому ряду причин. Что касается устранения последствий проблем, связанных с новым ключом KSK корневой зоны, и способности измерить принятие нового якоря доверия с течением времени, следующие обстоятельства могут служить препятствиями.

В ситуации ошибки проверки DNSSEC реакция рекурсивных серверов, осуществляющих проверку, неодинакова у разных инструментов. Некоторые инструменты известны более агрессивной стратегией повторных попыток,

некоторые действуют менее агрессивно, некоторые вовсе не повторяют попытки проверки.

Определить, принял ли тот или иной рекурсивный сервер (или любой источник запроса) явное решение о предпочтении одного корневого сервера другому, не представляется практически возможным. В обычных обстоятельствах источники запросов на корневых серверах отслеживаются в недостаточной степени для того, чтобы определить рекурсивные серверы, которые предпочитают обращаться к определенным, а не каким-то другим корневым серверам. Сбор данных DITL,[26] который проводит ежегодно центр DNS-OARC, выполняется в течение непродолжительного периода времени, это огромная по своим масштабам операция, которой тем не менее еще никогда не удалось охватить все корневые серверы в любой период времени.

Окончательным соображением является время, которое можно выделить для постепенного ввода нового якоря доверия. В любом квартале за пределами ключа ZSK корневой зоны остается только 70 дней. Для добавления нового ключа KSK (на первый сервер) необходимо 40 дней, то есть остается еще 30 дней для выполнения задачи в рамках одного периода ключа обновления ключа ZSK. Первоначальное поэтапное развертывание растянулось на больше чем 4 месяца.

10 Откат

В случае обнаружения возникновения серьезных проблем после ввода нового ключа KSK необходимо подготовить к развертыванию наборы ключей DNSKEY RRset, подписанные только старым ключом KSK. Такие наборы ключей RRset представлены в формате *подписанного ответного ключа* (SKR) и могут создаваться в рамках тех же церемоний создания ключа KSK корневой зоны, что и наборы ключей RRset, не предназначенные для отката к предыдущему состоянию. Критерии определения необходимости такого отката должны быть подробнее определены RZM-партнерами.

Рекомендация 14. Чтобы свести к минимуму время, необходимое для восстановления после затруднений, возникающих в связи с поступающим ключом для подписания ключей, SKR, генерируемый с использованием только действующего ключа KSK, должен генерироваться параллельно SKR, генерируемого с использованием нового KSK.

[26] https://www.dns-oarc.net/ditl/2011

Рекомендация 15. RZM-партнеры должны разработать процесс, подразумевающий использование ключа SKR, сформированного новым KSK.

Ключи SKR для отката, содержащие наборы записей ресурсов DNSKEY RRset, должны быть подготовлены для всех кварталов процесса. Во время I и II кварталов ключи SKR для отката состоят из набора DNSKEY RRset со старым ключом KSK и текущим ключом или ключами ZSK, подписанными старым ключом KSK. Новый ключ KSK опускается. Во время III квартала ключи SKR для отката состоят из набора DNSKEY RRset с новым ключом KSK и текущим ключом или ключами ZSK, подписанными новым ключом KSK. Отозванный старый ключ KSK опускается.

Порог срабатывания

Проведенные к этому времени тесты развертывания DNSSEC указывают на то, что погрешность измерения в таких тестах составляет приблизительно 5%. Это означает, что любое заявление об наносимом ущербе должно учитывать погрешность в 5% от количества пользователей или рекурсивных серверов (в зависимости от того, как именно проводятся измерения), которые могут столкнуться со снижением производительности без обнаружения. Исходя из этого определение тех или иных конкретных показателей не рассматривается как единственный способ определить порог срабатывания отката.

Более того, непонятно, в какой форме будет нанесен ущерб. Это могут быть ошибки развертывания, ошибки в коде, ошибки в процедурах или спонтанная реакция Интернета. По этой причине первым этапом должно стать установление контактов с партнерами по каналам развертывания и реализация инструментов для сообщения о проблемах, после чего можно будет выносить суждение в отношении реагирования на сообщения о проблемах.

Помимо серьезности и распространения ущерба существование множества различных сценариев использования не позволяет судить о том, не принесет ли откат больше вреда, чем продолжение обновления ключа с устранением проблем по мере их возникновения.

11 Когда?

С учетом существующей операционной среды в году есть четыре дня, когда можно перейти на использование нового ключа KSK корневой зоны вместо старого. Эти четыре дня — это первые дни кварталов, или первые числа

января, апреля, июля и октября. Выбор конкретной даты для изменения ключа зависит от двух компонентов — операционной целесообразности и совместимости с проходящими в настоящее время дискуссиями по поводу передачи координирующей роли в исполнении функций IANA.[27]

Операционная целесообразность означает, что такие даты не должны приходиться на выходные и праздники, от которых зависит график работы, а также на время неполного присутствия персонала на рабочих местах. С учетом необходимости выбрать эти три дня для аудитории по всему миру выполнить все из этих условий может быть нереально. Задача усложняется еще и тем, что в 2016 и 2017 годах все кварталы начинаются с пятницы, субботы или воскресенья. До 2018 года начало квартала не приходится ни на один другой день. (Четвертый квартал 2015 года начинается в четверг 1 октября, однако к тому времени еще не будет готов план и тем более не будет проведено необходимое тестирование, что не позволит выполнить обновление ключа в этот день.)

Одним из факторов нетехнического характера является запланированная передача координирующей роли в исполнении функций IANA. По этой причине рекомендовать ту или иную конкретную дату на данный момент нельзя.

12 Анализ рисков

12.1 Риски, связанные с недостаточной подготовкой

Описание	Последствия	Вероятность	Снижение
Обновление ключа KSK с таким же алгоритмом, контрольной суммой и размером может выглядеть недостаточным в глазах заинтересованных сторон	Низкая	Очень низкая	Начать планировать следующее обновление сразу же после завершения этого; при необходимости использовать другие параметры — изменить параметры

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Описание	Последствия	Вероятность	Снижение
Операторы сетей не будут знать об изменениях (то есть сетевой операционный центр (NOC) будет получать сообщения о неисправностях и должен знать, как на них реагировать)	Умеренная	Высокая	В плане обмена информацией; фокус на операторов
Операторы сетей и разработчики ПО (или все партнеры по каналам распространения) не будут иметь доступа к испытательной среде, адекватной условиям изменений	Умеренная	Высокая	Настроить тестовую площадку ICANN в соответствии со спецификацией RFC 5011 с ускоренным и своевременным обновлением ключа; прочие тесты
Осуществлять централизованное тестирование по ходу выполнения невозможно	Низкая	Высокая	Разработать подходы на основе модели распределенного тестирования; разработать список контактов

Описание	Последствия	Вероятность	Снижение
Отсутствие детерминиро-ванных критериев для принятия решения о выполнении или отказе от выполнения	Низкая	Высокая	Необходимо подготовить механизмы обмена информацией и тестирования; анализ осуществимости механизмов, используемых в полевых условиях; долгосрочные усилия по разработке изменения принятия измененных якорей доверия

12.2 Автоматический механизм якорей доверия не работает или работает неправильно

Описание	Последствия	Вероятность	Снижение
RFC 5011 поддерживается не повсеместно	Умеренная	Высокая	Альтернативные подходы к управлению якорями доверия
Неполная реализация RFC 5011	Умеренная	Очень низкая	Связаться с разработчиками ПО; проверить понимание RFC 5011
Процедура начальной настройки средств проверки реализована не полностью	Умеренная	Очень низкая	Связаться с системными интеграторами и обработчиками якорей доверия
Набор якорей доверия недоступен с веб-сайта ICANN, посвященного функциям IANA	Низкая	Очень низкая	Мониторинг доступности

Оборудование с якорями доверия, не синхронизированными из-за ненадлежащего технического обслуживания	Низкая	Высокая	План обмена информацией

12.3 Удаление старого ключа KSK приводит к ошибкам проверки

Описание	Последствия	Вероятность	Снижение
Протокол автоматических якорей доверия выполняется в недостаточной мере (любым участником этого процесса)	Низкая	Высокая	Тестирование, обмен информацией; предоставление операторам ресурсов для содействия скорейшему исправлению
Рост трафика вследствие повторяющихся неудачных попыток	Низкая	Очень низкая	Изучить[28] последствия сбоев после обновления ключа; рекомендации в отношении отрицательного кэширования

[28] http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf, http://www.potaroo.net/ispcol/2010-02/rollover.html

12.4 Добавление нового ключа KSK приводит к тому, что размер сообщения DNS превышает допустимые пределы

Описание	Последствия	Вероятность	Снижение
Передача наборов ключей приводит к увеличению размеров дейтаграмм	Умеренная	Очень низкая	Тщательное планирование передачи на основе изучения размера сообщений
Путаница с вопросом обработки фрагментации IPv6 в ПО DNS	Низкая	Очень низкая	Изучение и тестирование ПО DNS

12.5 Возникновение операционных ошибок

Описание	Последствия	Вероятность	Снижение
Некачественно выполненное обновление ключа KSK придаст импульс принятию DNSSEC	Высокая	Очень низкая	Тщательное планирование и анализ
Если бесконечно откладывать обновление ключа, в случае срочного обновления последствия могут быть более серьезными	Высокая	Очень низкая	Приверженность обновлению ключа KSK корневой зоны

Если начать, вернуться к текущему приемлемому состоянию будет невозможно	Высокая	Очень низкая	Определить план возврата к предыдущему состоянию
Старый ключ KSK (секретный компонент) уничтожен не до конца	Низкая	Очень низкая	Обязательство выполнить план

13 Список членов группы разработчиков

13.1 Добровольные участники от сообщества

- Джо Эбли (Joe Abley), Dyn, Inc., Канада
- Яап Аккергиус (Jaap Akkerhuis), NLNetLabs, Нидерланды
- Джон Дикинсон (John Dickinson), Sinodun Internet Technologies, Великобритания
- Джефф Хьюстон (Geoff Huston), APNIC, Австралия
- Онджей Суры (Ondrej Sury), CZ.NIC, Чехия
- Пауль Вултерс (Paul Wouters), No Hats/Red Hat, Нидерланды
- Йоширо Йонея (Yoshiro Yoneya), JPRS, Япония

13.2 Партнеры по управлению корневой зоной

- Дэвид Конрад (David Conrad), ICANN
- Эдвард Льюис (Edward Lewis), ICANN
- Ричард Лэмб (Richard Lamb), ICANN
- Ален Дюран (Alain Durand), ICANN
- Хейли Лафрамбуа (Hayley Laframboise), ICANN
- Элиза Герих (Elise Gerich), ICANN
- Ким Дейвис (Kim Davies), ICANN
- Рой Арендс (Roy Arends), ICANN
- Якоб Шляйтер (Jakob Schlyter), ICANN
- Фредрик Люнггрен (Fredrik Ljunggren), ICANN
- Брэд Верд (Brad Verd), Verisign

- Дуэйн Уэсселс (Duane Wessels), Verisign
- Дэйвид Блэка (David Blacka), Verisign
- Эл Боливар (Al Bolivar), Verisign
- Тим Полк (Tim Polk), NIST, Министерство торговли США
- Скотт Роуз (Scott Rose), NIST, Министерство торговли США
- Даг Монтгомери (Doug Montgomery), NIST, Министерство торговли США
- Эшли Хайнеман (Ashley Heineman), NIST, Министерство торговли США
- Вернита Харрис (Vernita Harris), NIST, Министерство торговли США

14 Ссылки

- RFC 5011: Автоматическое обновление якорей доверия расширений безопасности DNS (DNSSEC)
  https://tools.ietf.org/html/rfc5011
- SAC063: Информационное сообщение SSAC об обновлении ключа DNSSEC в корневой зоне
  https://www.icann.org/en/system/files/files/sac-063-en.pdf
- Практическое заявление DNSSEC для оператора KSK корневой зоны
  https://www.iana.org/dnssec/icann-dps.txt
- Практическое заявление DNSSEC для оператора ZSK корневой зоны
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf
- Публикация якоря доверия DNSSEC для корневой зоны
  https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- Установление надлежащего якоря доверия DNSSEC для корневой зоны в момент запуска
  https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 Приложение: партнеры по каналам распространения

Термином «партнеры по каналам распространения» называются внешние организации, которые независимо участвуют или содействуют в управлении ключом KSK корневой зоны. Такие организации не состоят в официальных отношениях с RZM-партнерами, однако в определенной степени координируют свои действия. Для каждой организации необходимо поддерживать соответствующие контакты для обмена сообщениями о статусе и прочей информацией, касающейся изменения ключа KSK корневой зоны.

Партнеры по каналам распространения перечислены в случайном порядке.

15.1 Производители программного обеспечения

Обмен важной информацией с такими партнерами относится к реализации (или отсутствии поддержки) функций управления якорями доверия RFC 5011 в программном обеспечении. В этот набор партнеров входят организации, выпускающие рекурсивные кэширующие сервера с проверкой подлинности. Контактные данные этих организаций в настоящем документе не указаны.

- ISC BIND (http://www.isc.org)
- NLNetLab Unbound (https://nlnetlabs.nl)
- Microsoft Windows Server (https://www.microsoft.com/)
- Nominum Vantio (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/
- Secure64 DNS Cache (http://www.secure64.com/)

15.1.1 Ожидается

В следующий набор партнеров входят организации, которые обсуждали, но еще не выпустили рекурсивные кэширующие сервера с проверкой подлинности DNSSEC. Они внесены в список и будут включены в перечень партнеров, если код будет распространен. (Другие рекурсивные кэширующие сервера DNS без поддержки DNSSEC не зависят от ключа KSK корневой зоны)

- Будет указано позже — рекурсивный сервер CZ.NIC (помимо Knot)
- Будет указано позже — PowerDNS

15.2 Системные интеграторы

Эти партнеры по каналам распространения в некоторых случаях передают ключи KSK корневой зоны в составе данных конфигурации ранее перечисленного ПО DNS. Ожидается, что эти организации проанализируют новый ключ KSK корневой зоны и включат его в обновления для своего программного обеспечения.

15.2.1 Linux

- Red Hat Enterprise Linux (RHEL) (RPM-пакеты)
- Micro Focus International SUSE (RPM-пакеты)
- Fedora
- CentOS
- APT Debian и Canonical (Ubuntu)
- Montavista Linux

15.2.2 BSD

- Порты FreeBSD
- NetBSD (pkgsrc)
- Порты FreeBSD

15.2.3 Другие

- Apple iOS, OS X
- Google Android, ChromeOS
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco / Linksys
- Wind River (RTOS)
- QNX (RTOS)
- OpenVMS
- OpenWRT

15.3 Операторы общедоступных распознавателей

Это партнеры, которые поддерживают работу рекурсивных серверов DNS, в некоторых случаях с поддержкой проверки подлинности DNSSEC. Ожидается, что эти партнеры включат ключ KSK корневой зоны в свои конфигурационные

данные, поэтому им может понадобиться провести внутренний анализ с учетом использования нового ключа KSK корневой зоны.

- Google Public DNS
- OpenDNS
- Neustar DNSAdvantage
- Symantec ConnectSafe
- Level 3
- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

Помимо приведенного выше списка операторов с общедоступными распознавателями, определенными как распознаватели, принимающие любой трафик из Интернета (насколько это представляется стороннему наблюдателю на данный момент), существуют партнеры, поддерживающие работу общедоступных распознавателей с определенными ограничениями по базе клиентов, которые могут их использовать. По мере определения таких партнеров им будет предложено получать уведомления о событиях, касающихся ключа KSK корневой зоны.