Руководство по развертыванию DNSSEC для ccTLD

Офис технического директора ICANN

Язид Аканхо (Yazid Akanho) и Пол Мучене (Paul Muchene)
OCTO-029
12 ноября 2021

ICANN

СОДЕРЖАНИЕ

Настоящий документ входит в серию документов офиса технического директора ICANN (OCTO). Список документов этой серии см. на странице публикаций OCTO. Вопросы и предложения по любому из этих документов принимаются по адресу octo@icann.org.

Настоящий документ поддерживает стратегическую задачу ICANN — повысить общую ответственность за поддержание безопасности и стабильности системы доменных имен (DNS) за счет укрепления координации DNS в партнерстве с соответствующими заинтересованными сторонами. Это часть стратегической цели ICANN по укреплению безопасности DNS и системы корневых серверов DNS (RSS).

1 Введение

В последние годы безопасность становится все более серьезной проблемой в интернете. Что касается системы доменных имен (DNS), то за прошедшие годы было предложено и разработано несколько протоколов безопасности. Один из наиболее важных — это расширения безопасности системы доменных имен (DNSSEC). DNSSEC помогает защитить ответы DNS путем добавления процедуры аутентификации источника данных и обеспечения защиты целостности данных.

Корневая зона DNS, находящаяся под управлением ICANN, была впервые подписана с помощью DNSSEC в июле 2010 года. На момент публикации данного руководства все домены общего пользования верхнего уровня (gTLD) будут подписаны с помощью DNSSEC, отчасти благодаря контрактным обязательствам перед ICANN, а из национальных доменов верхнего уровня (ccTLD) на сегодняшний день подписано около 60%. Одной из причин такой тенденции на уровне ccTLD может быть недостаточный уровень понимания процесса обеспечения безопасности зон с помощью DNSSEC среди операторов регистратур национальных доменов.

В связи с этим офис технического директора ICANN (OCTO) опубликовал данное руководство, чтобы помочь операторам регистратур ccTLD лучше освоить процесс, призванный помочь им подписывать их зоны с помощью DNSSEC. В руководстве не охвачен второй аспект DNSSEC — проверка, которая выполняется в основном на рекурсивных резолверах DNS, обычно расположенных у интернет-провайдеров (ISP), крупных операторов общедоступных облачных сред или в корпоративных сетях.

1.1 Целевая аудитория документа

Данное руководство предназначено в первую очередь для того, чтобы предоставить регистратурам ccTLD, персоналу, заинтересованным сторонам, в частности регистраторам, владельцам доменов и всем остальным, общее представление о DNSSEC и о том, как этот протокол может быть применен регистратурой при подписании зоны. В документе не рассматриваются детали технической конфигурации; скорее, он является руководством для базового понимания протокола DNSSEC, предпосылок и аспектов его развертывания при подписании зон ccTLD.

Даже если вы уже используете TLD, подписанный DNSSEC, настоящий документ может помочь вам определить элементы, которые необходимо улучшить; например, воспользоваться лучшими практиками применения алгоритмов или документирования всей работы службы DNS. Если вы являетесь оператором ccTLD или управляете зонами подписанного ccTLD, это руководство поможет вам приступить к этой работе. Несмотря на то, что все операторы gTLD уже подписали свои зоны, они также могут почерпнуть информацию о передовых методах использования DNSSEC, описанных в этом документе, и использовать его в качестве основы для повышения осведомленности своих регистраторов и владельцев доменов о DNSSEC.

Существует множество документов по теоретическим, техническим и эксплуатационным аспектам DNSSEC, и в настоящем руководстве приводятся ссылки на некоторые из них. В связи с этим читателям предлагается ознакомиться с этими цитируемыми документами, если они хотят лучше разобраться в различных аспектах, связанных с DNSSEC.

2 DNSSEC и его значение для DNS

Система доменных имен (DNS) — это иерархическая, распределенная и децентрализованная система присвоения имен для интернета. Подобно телефонной книге, которая переводит имена в телефонные номера, DNS помогает преобразовать информацию о доменных именах в IP-адреса и наоборот. DNS считается критически важным сервисом в интернете, но изначально при ее разработке не были предусмотрены надежные механизмы безопасности, обеспечивающие целостность и подлинность ее данных. С течением времени был обнаружен ряд уязвимостей, угрожающих надежности DNS и доверия к ней, и DNSSEC-протокол помогает устранить некоторые из них.

Основные параметры DNSSEC-протокола определены и указаны в трех документах стандартов интернета: RFC 4033 *Безопасность DNS: введение и требования (DNS Security Introduction and Requirements)*; RFC 4034 *Ресурсные записи для расширений безопасности DNS* (Resource Records for the DNS Security Extensions) и RFC 4035 *Модификации протокола для расширений безопасности DNS (Protocol Modifications for the DNS Security Extensions)*. В DNSSEC используется криптография открытого ключа (генерация пар открытых и закрытых ключей) для добавления в DNS возможностей аутентификации источника данных, целостности данных, проверки и аутентифицированного отрицания существования. В частности, в DNS добавляются цифровые подписи и новый набор типов ресурсных записей и битов заголовка сообщения (флагов), которые можно использовать для проверки ответов DNS из подписанной зоны. Стоит отметить, что DNSSEC не шифрует данные DNS-сообщений и, следовательно, не обеспечивает конфиденциальность.

После подписи домена с помощью DNSSEC, администратор зоны генерирует цифровые подписи с помощью закрытого ключа, которые затем публикуются в виде цифровой подписи ресурсной записи (RRSIG) в файле зоны как часть файла корневой зоны домена. Когда рекурсивный резолвер, ориентированный на обеспечение безопасности, также известный как валидирующий резолвер, отправляет запрос DNS на авторитативный сервер подписанного домена, ответ DNS содержит ресурсную запись в открытом или незашифрованном виде и соответствующую цифровую подпись. Затем резолвер использует полученную цифровую подпись для проверки этого DNS-ответа. Для этого валидирующий резолвер также запрашивает другую информацию, связанную с DNSSEC, такую как открытый ключ, который хранится в записи DNSKEY и публикуется администратором домена в составе данных зоны.

3 Условия и требования, необходимые для развертывания DNSSEC

3.1 Документация существующей системы

В связи с той критической ролью, которую DNS играет в интернете и необходимостью предотвращения сбоев при любых обстоятельствах, важно поддерживать в актуальном

состоянии документацию, описывающую инфраструктуру, операции и процессы DNS. Одновременно DNSSEC-протокол повышает уровень сложности существующей инфраструктуры и функционирования DNS, и поэтому обеспечение актуальности документации имеет очень большое значение для обеспечения четкого представления о существующей системе. Это также позволяет обеспечить непрерывность работы в случае смены персонала или модернизации инфраструктуры.

Мы рекомендуем кратко излагать в документации два основных аспекта: политики управления ccTLD и эксплуатационные и технические аспекты обслуживания.

Кроме того, желательно, чтобы документ содержал максимально полную информацию, опуская при этом все конфиденциальные данные, такие как имена пользователей и пароли, которые могут использоваться для проведения атак на регистратуру.

Аспекты документа, связанные с управлением, могут касаться следующих тем:

- общий обзор и структура ccTLD;
- модели регистрации: 3R (регистратура, регистратор и владелец домена), 2R (только регистратура и владелец домена) или другие модели *[сокращения соответствуют первым буквам английских терминов]*;
- контактные лица регистратуры по техническим и административным вопросам;
- кадровые ресурсы, роли, обязанности и контактные данные людей, участвующих в принятии технических решений в регистратуре;
- список регистраторов и их контактная информация.

Технические и эксплуатационные аспекты документа могут охватывать следующие темы:

- количество первичных и вторичных авторитативных серверов имен (NS) с соответствующими IP-адресами, контактная информация TLD (телефоны и адреса электронной почты), протоколы взаимодействия между регистратурой и регистраторами, такие как протокол EPP (EPP), программное и аппаратное обеспечение, реализующее функции регистратуры, включая базу данных регистратуры, протокол доступа к регистрационным данным (RDAP) и/или серверы WHOIS, а также другая техническая информация;
- доступ пользователей и перечень привилегий, доступных только ограниченному числу уполномоченных лиц;
- процедуры резервного копирования и восстановления данных;
- безопасность: физический доступ, управление журналами, средства управления доступом, управление паролями, брандмауэры, целостность файлов корневой зоны, безопасность при передаче зон и многое другое;
- системы мониторинга: аппаратное и программное обеспечение, синхронизация зон (между NS);
- стратегия технического обслуживания;
- план обеспечения бесперебойной деятельности и послеаварийного восстановления.

3.2 Аудит существующей инфраструктуры

Как уже говорилось, развертывание DNSSEC повышает уровень сложности существующей инфраструктуры и функционирования DNS. Поэтому хорошей и безопасной практикой является проведение аудита текущей инфраструктуры, операций и процессов системы с привлечением сторонних или собственных специалистов,

достаточно компетентных и независимых, чтобы выявить все недостатки и подготовить выводы. Очень важно устранить все недостатки существующей системы до или в ходе подписания зоны. Это снижает риск того, что после внедрения DNSSEC система станет неуправляемой.

3.3 Подготовка политик и заявлений о практике использования DNSSEC

3.3.1 Что такое политика DNSSEC и заявление о практике использования DNSSEC?

При подписании домена необходимо учесть несколько соображений и определить параметры, например алгоритмы подписи DNSSEC, размеры ключей, срок действия и частоту обновления подписи. Для зон с большим количеством делегирований, хорошей практикой является полный учет и поддержание в актуальном состоянии применимых к зоне параметров и обеспечение открытого доступа к ним. В связи с этим здесь следует обратить внимание на две концепции:

- **Политика DNSSEC** (DP): Определяет требования и стандарты безопасности, которые должны быть реализованы для зоны, подписанной DNSSEC. DP представляет собой основу для аудита, аккредитации или оценки организации, например регистратуры. Каждая организация может быть оценена по одной или нескольким DP, которые, по ее словам, она реализует. Иначе говоря, в DP прописано, что необходимо сделать.
- **Заявление о практике использования DNSSEC** (DPS). Документ, раскрывающий операционную практику, который может служить дополнением к политике DNSSEC (если она существует). В нем приводится общая информация о том, как оператор зоны и его партнеры по управлению зоной, если таковые имеются, внедряют процедуры и средства контроля для выполнения требований применимой DP. В отличие от DP, в DPS прописываются реальные действия.

DP содержит общие принципы, а DPS — описание процедур и средств контроля, что делает его более подробным, чем DP. С другой стороны, политика обычно разрабатывается органом, определяющим политику (регистратурой TLD или регулирующим органом), и может быть применима к одной или нескольким зонам в иерархии DNS, а заявление о практике использования, относящееся к одной зоне, составляется оператором зоны и описывает ее соответствие требованиям конкретной политики или набора политик.

Например, в ситуации, когда контактные лица ccTLD по административным и техническим вопросам являются разными организациями, контактное лицо по административным вопросам может опубликовать политику с изложением стандартов и требований, которым необходимо следовать, и потребовать от контактного лица по техническим вопросам опубликовать заявление о практике с подробным описанием того, как эти стандарты и требования будут выполняться.

В качестве альтернативы оператор или управляющий зоны, который не руководствуется внешней политикой, может опубликовать DPS.

Публикация DPS наиболее актуальна для организаций, управляющих зоной с большим количеством делегирований, например TLD. Публикация DPS помогает повысить уровень прозрачности для укрепления доверия сообщества к функционированию TLD, но, как уже говорилось, DPS не должно содержать конфиденциальную информацию об эксплуатации.

RFC 6841 *Концепция политик DNSSEC и заявлений о практике использования DNSSEC (A Framework for DNSSEC Policies and DNSSEC Practice Statements)* — это документ, позволяющий получить глубокое понимание обширного списка тем, которые оператор TLD должен учитывать при составлении DP и DPS соответственно.

3.3.2 Принципы составления DP и DPS

Составление DPS — важный шаг на пути к подписанию ccTLD. Заявление DPS может быть коротким и простым или длинным и сложным, но в любом случае оно призвано помочь людям понять концепцию функционирования DNSSEC и причины, по которым они могут доверять процессу подписания ccTLD.

Следующая таблица представляет собой краткое описание набора положений из восьми описанных в RFC 6841 компонентов, которые могут быть приняты во внимание при составлении DP или DPS. Не все описанные в RFC 6841 компоненты обязательно реализовывать, поэтому вы можете выбрать те (под)компоненты, которые подходят для ваших нужд.

Название	Описание	Подкомпоненты
Введение	Определение и описание вышеуказанных положений, а также список типов организаций и приложений, на которые ориентирована политика или заявление о практике использования.	• Общие сведения • Название и идентификатор документа • Сообщество и применимость • Управление спецификациями
Публикация и репозитории информации	Описание требований к публикации организацией информации о своих практиках, открытых ключах, текущем состоянии этих ключей, а также сведения о репозиториях информации.	• Репозитории • Публикация открытых ключей
Производственные требования	Описание производственных требований при работе с зоной, подписанной DNSSEC.	• Значение доменных имен • Идентификация и аутентификация управляющего дочерней зоной • Регистрация ресурсных записей DS

		• Методы доказательства владения закрытым ключом • Удаление ресурсных записей DS
Средства управления объектом, управленческий и оперативный контроль	Описание нетехнических средств контроля безопасности, то есть физических, процедурных и кадровых средств, необходимых для выполнения функций, связанных с DNSSEC с соблюдением принципов обеспечения безопасности. Эти средства контроля — это физический доступ, управление ключами, послеаварийное восстановление, аудит и архивирование, и они имеют решающее значение для обеспечения доверия к подписям, созданным с помощью DNSSEC.	• Физические средства контроля • Процедурные средства контроля • Кадровые средства контроля • Процедуры регистрации аудита • Взлом и послеаварийное восстановление • Прекращение деятельности организации
Технические средства контроля безопасности	Определение мер безопасности, предпринятых для управления криптографическими ключами и данными активации, например, PIN-кодами, паролями или хранимыми вручную ключами совместного пользования, связанными с работой DNSSEC.	• Генерация и установка пары ключей • Защита закрытых ключей и инженерно-технические средства контроля криптографических модулей • Данные активации
Подписание зоны	Описание всех аспектов подписания зоны, включая криптографическую спецификацию, связанную с ключами подписания, схему подписания, методику обновления ключей и собственно подписание зон. Дочерние зоны и другие зависимые стороны могут нуждаться в информации в этом разделе, чтобы понимать, каких данных следует ожидать в	• Длина ключа, типы ключей и алгоритмы • Аутентифицированное отрицание существования • Формат подписи • Обновление ключа • Срок действия подписи и частота повторного подписания

	подписанной зоне и определить свои действия.	
Аудит выполнения требований	Описание порядка проведения аудита оператором зоны и, возможно, другими организациями-участниками.	• Частота проведения аудита выполнения требования организацией • Личность/квалификации аудитора • Темы аудита • Действия после аудита
Юридические вопросы	В разделе указана юрисдикции, в которой действует регистратура и даны ссылки на все действующие соглашения. В разделе «Юридические вопросы» может содержаться информация о всех выявленных последствиях для защиты личных данных.	• Упоминание соответствующей юрисдикции • Договорные обязательства и национальные, транснациональные или международные законы и нормативные акты • Защита данных и работа с личными данными

К этой концепции могут быть добавлены дополнительные компоненты для удовлетворения конкретных потребностей ccTLD. Примеры заявлений о практике использования DNSSEC приведены в Приложении A данного руководства.

3.3.3 Выбор криптографических алгоритмов для зоны

Область криптографии постоянно развивается. Новые алгоритмы заменяют существующие, когда выясняется, что те менее безопасны, чем считалось ранее. Поэтому требования к применению алгоритмов и руководство по использованию регулярно обновляются, чтобы отразить новые реалии.

Реализация DNSSEC требует выбора подходящего криптографического алгоритма. На момент публикации данного руководства в документе RFC 8624 *Требования к применению алгоритмов и руководство по их использованию с DNSSEC* (*Algorithm Implementation Requirements and Usage Guidance for DNSSEC)* содержатся рекомендации по применению алгоритмов и требования к параметрам подписи, относящиеся к DNSSEC.

В следующей таблице перечислены некоторые (неисчерпывающие) рекомендации из RFC 8624. Отдельные операторы могут иметь особые требования и решить внести соответствующие изменения.

Пункт	**Рекомендация**
Алгоритм DNSKEY	**Алгоритм 13 (ECDSAP256SHA256)** обеспечивает криптографическую стойкость и в настоящее время

	рекомендуется для использования в новых схемах развертывания DNSSEC, так как им используются более короткие ключи и подписи, что приводит к уменьшению размера DNS-пакетов. При этом **алгоритм 8 (RSASHA256)** также можно использовать, поскольку он широко распространен и уже несколько лет применяется по умолчанию из-за своей криптографической надежности.
Алгоритмы создания подписи делегирования (DS)	SHA-256 широко используется и является надежным хэш-алгоритмом, поэтому рекомендуется для новых и существующих схем развертывания DS.
Алгоритм безопасности DNSSEC (состоит из криптографического алгоритма и хэш-алгоритма)	В настоящее время рекомендуется использовать алгоритм 13 (ECDSAP256SHA256). В качестве альтернативы можно также использовать алгоритм 8 (RSASHA256).
Размер ключа подписания зоны (ZSK) и ключа для подписания ключей (KSK)	Алгоритм 13 (ECDSAP256SHA256) всегда генерирует ключи длиной 256 бит. Размер ключа алгоритма 8 (RSASHA256) может быть установлен в диапазоне 2048–4096 бит.
Период действия ZSK и KSK	Хорошего способа оценить индивидуальные потребности не существует, поскольку операторы корректируют периоды действия ключей на основе своего предыдущего опыта. Некоторые операторы используют ZSK в течение одного-трех месяцев и KSK в течение одного-пяти лет, прежде чем их обновить.
Хранение закрытых ключей	Автономные, не подключенные к сети, физически защищенные машины, такие как программно-аппаратные криптографические модули (HSM)

Примечание: Более длинные ключи увеличивают размеры записей RRSIG и DNSKEY, повышая тем самым вероятность переполнения UDP-пакетов DNS. Кроме того, при использовании более длинных ключей увеличивается время, необходимое для проверки и создания цифровых подписей ресурсных записей (RRSIG), поэтому ненужного увеличения размеров ключей следует избегать.

3.3.4 Отрицание существования: NSEC или NSEC3

Отрицание существования или доказательство того, что чего-то не существует — это механизм передачи резолверу информации о том, что определенного доменного имени

не существует (NXDOMAIN). Или наоборот, доменное имя существует, но в его настройках отсутствует соответствующая запрашиваемая ресурсная запись (NODATA). При аутентификации отрицания существования для подписания отрицательного ответа используется криптография. В DNSSEC это обеспечивается с помощью NSEC (следующая безопасная запись) или NSEC3 (следующая безопасная запись, версия 3), соответственно.

NSEC используется для описания интервала между именами. NSEC косвенно сообщает резолверу, какие имена отсутствуют в зоне, предоставляя в каноническом порядке имя перед ним и имя после него. Этот реализованный в NSEC механизм лежит в основе механизма аутентифицированного отрицания существования в DNSSEC и сопряжен с двумя проблемами:

- Записи NSEC уязвимы к обходу зоны, и эта слабость может позволить злоумышленнику обойти все имена в зоне. Это позволяет восстановить всю зону и, следовательно, преодолеть любые попытки административного блокирования передачи зоны.

- Вторая проблема, с которой сталкивается NSEC в зоне, ориентированной на делегирование, такой как TLD, заключается в том, что каждое имя в этой зоне получает запись NSEC и связанную с ней RRSIG. После подписания зоны это приводит к нежелательному увеличению ее размера. Вызванные этим увеличением накладные расходы могут негативно повлиять на производительность авторитативных DNS-серверов, например, ограничить ресурсы аппаратного хранилища или увеличить продолжительность операций передачи зон.

NSEC3, напротив, смягчает проблему обхода зон в NSEC за счет хэширования доменных имен с возможностью их усиления путем добавления случайной строки (соли). Более того, благодаря специальной функции явного отказа неподписанные доменные имена, делегированные в зону (т. н. небезопасное делегирование), не требуют записи NSEC3. Это означает, что если в зоне TLD активирована функция отказа от подписи, NSEC3 не может подтвердить или опровергнуть существование неподписанных доменов, зарегистрированных в этом TLD. Тем не менее, одним из недостатков NSEC3 является то, что ответы DNS больше, чем у NSEC.

Нет единственного правильного решения, когда речь идет о выборе между NSEC и NSEC3. Если вы предпочитаете использовать NSEC3 для предотвращения обхода зон, обычно рекомендуется применить NSEC3 без дополнительных итераций и добавить пустую соль, но для небольших зон использовать записи NSEC3 на основе функции явного отказа не рекомендуется. Для очень больших и редко подписываемых зон, в которых большинство записей представляют собой случаи небезопасного делегирования, можно использовать функцию отказа от NSEC3. Если не принимать во внимание вышеупомянутые соображения, устранять неисправности при использоовании NSEC проще, чем при использовании NSEC3.

3.4 Участие регистраторов

Привлекать регистраторов настоятельно рекомендуется на предварительных этапах подписания ccTLD, и это не только потому, что они являются посредниками между

регистратурой и владельцами доменов, но и потому, что развертывание DNSSEC на уровне ccTLD является отправной точкой для обеспечения безопасности пространства имен этого ccTLD. После подписания ccTLD владельцы доменов второго уровня могут приступить к защите своих доменов. При этом регистраторы должны иметь возможность получать от владельцев доменов второго или последующего уровней и отправлять в регистратуру записи нового типа. Этот новый тип записи называется «подпись делегирования» (DS).

В техническом плане DS представляет собой хэш ключа для подписания ключей (KSK) и помогает выстроить цепочку доверия между родительской и дочерней зонами в пространстве имен DNS. Наличие записи DS в родительской зоне создает надежную связь, которую внешнему злоумышленнику придется преодолеть, чтобы подделать данные ключа в дочерней зоне.

Обычно ccTLD передает свою запись DS Администрации адресного пространства интернета (IANA) для публикации в корневой зоне. Владельцы доменов и администраторы доменных имен в рамках ccTLD предоставляют свои записи DS в ccTLD напрямую или через регистратора. Регистраторы играют здесь две важные роли:

- **Предоставление безопасного и надежного интерфейса или механизма для получения записей DS** от владельцев доменов; если такого интерфейса или механизма еще не существует, регистраторы, готовые предоставить сервис поддержки DNSSEC своим владельцам доменов, должны как можно скорее приступить к его внедрению. Стандартного способа переноса записи DS между клиентом и регистратором не существует. У разных регистраторов разные механизмы, начиная от простых веб-интерфейсов и заканчивая различными API.
- **Передача DS в регистратуру**. Вместо публикации DS в родительской зоне вручную рекомендуется использовать автоматизированное решение. В модели «регистратура-регистратор» можно использовать расширения DNSSEC для EPP с целью передачи наборов ресурсных записей (наборов RRset) DS и, по желанию, наборов DNS-записей DNSKEY. В любом случае взаимодействие между оператором ccTLD и регистраторами необходимо протестировать, чтобы убедиться в том, что новые транзакции осуществимы с использованием существующей инфраструктуры.

Еще одним механизмом автоматического управления DS дочерней зоны из родительской является использование CDS (дочерняя подпись делегирования) или набора DNS-записей CDNSKEY (дочерний DNSKEY), если у родительской зоны есть политика принятия этих записей. Их можно использовать в следующих трех случаях:

- Первичная публикация DS
- Обновление ключа
- Возврат в незащищенное состояние

Проще говоря, CDS/CDNSKEY — это указание родителю изменить набор DNS-записей ресурса DS, если CDS/CDNSKEY и DS отличаются. В документе RFC 8078 *Управление записями DS из родительской зоны через CDS/CDNSKey (Managing DS Records from the Parent via CDS/CDNSKey)* подробно описано автоматизированное управление записями DS в дочерней и родительской зонах.

Наконец, привлечение регистраторов на ранних этапах процесса также позволяет им воспользоваться тренингами и практическими программами по DNSSEC, проводимыми ICANN и ее партнерами в интернет-сообществе.

4 Продолжительность процедуры развертывания

Строгого определения продолжительности процедуры развертывания DNSSEC нет, и она может быть от нескольких недель до месяцев или лет в зависимости от ряда факторов. При этом следует принять к сведению следующие рекомендации, чтобы избежать длительных задержек:

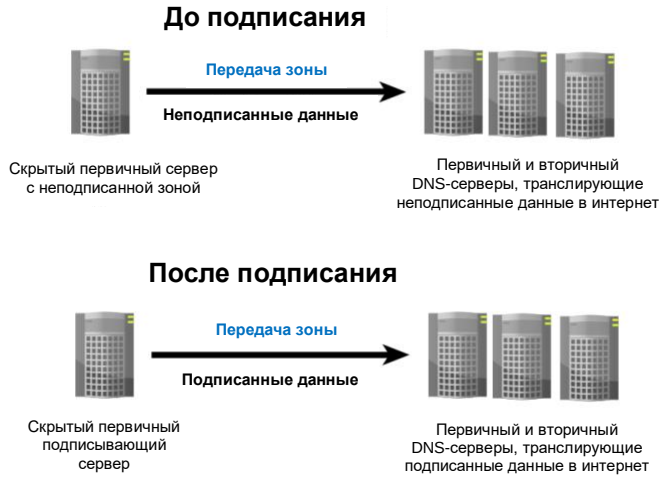
- Определите процесс как проект с четкой датой начала, ожидаемой датой окончания и обязательными промежуточными этапами. Кроме того, назначьте руководителя проекта или технического руководителя с соответствующими ресурсами.
- Определите и координируйте порядок взаимодействия с заинтересованными сторонами, в том числе с регуляторами, регистраторами, техническими и административными сторонами, подрядчиками, операторами программно-аппаратной части и всеми остальными сторонами. Необходимо также решить проблему коммуникации между различными заинтересованными сторонами ccTLD.
- Выявите риски и примите меры по надлежащему управлению ими.

5 Сценарии развертывания DNSSEC

Независимо от того, решите ли вы управлять зоной исключительно с помощью собственных ресурсов и инфраструктуры или наняв подрядчика, например оператора серверной части, скорее всего, архитектура технического развертывания будет соответствовать одному из двух основных сценариев, описанных в этом документе.

5.1 Первичный сервер для поточного подписания (скрытый первичный сервер)

В этом сценарии конфигурации скрытый первичный DNS-сервер, обычно неизвестный в интернете, передает зону на ряд авторитативных серверов DNS, обычно на один публичный первичный и несколько вторичных серверов. Скрытый первичный DNS-сервер — это требование, не связанное конкретно с DNSSEC, а скорее передовая практика работы DNS, которая предполагает наличие внеполосного авторитативного сервера имен, недоступного и неизвестного широкой публике, на котором могут производиться все обновления зоны. На этом сервере также должны быть реализованы более жесткие процедуры обеспечения безопасности и проведения аудитов. Примерная архитектура представлена на следующем рисунке:

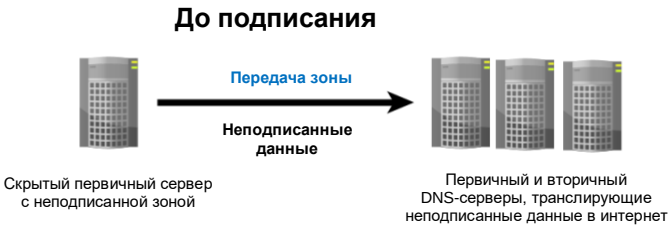


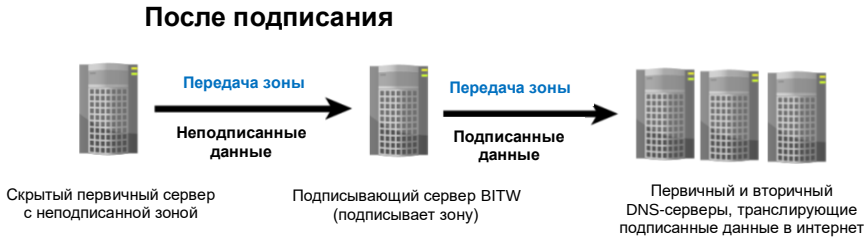
Этот скрытый первичный сервер настраивается на распознавание созданных ключей и их использование для создания и запуска подписанной зоны, следуя процессу, предусмотренному программным обеспечением DNS, на котором он работает. По завершении подписанная версия файла корневой зоны передается и синхронизируется со всеми соответствующими видимыми публике авторитативными DNS-серверами.

За исключением изменений конфигурации скрытого первичного сервера имен, в данной архитектуре нет необходимости вносить дополнительные изменения конфигурации или программного обеспечения.

5.2 Поточное подписание BITW

В этом сценарии конфигурации в существующую архитектуру вводится новый DNS-сервер (подписывающий), который размещается между скрытым первичным сервером и публичными DNS-серверами, обслуживающими зону в интернете. Этот новый сервер работает в качестве устройства BITW (bump-in-the-wire). Он получает неподписанный файл корневой зоны от скрытого первичного сервера, подписывает данные и отправляет подписанный файл корневой зоны для распространения среди публичных DNS-серверов домена.





Для этого можно предпринять следующие шаги:

1. Скрытый первичный сервер не должен указываться в списке ресурсов RRset DNS-сервера (NS) домена во избежание получения противоречащих друг другу ответов, то есть неподписанных ответов от скрытого первичного сервера и подписанных ответов от других DNS-серверов.
2. Конфигурация скрытого первичного сервера должна быть обновлена, чтобы только подписывающий сервер мог выполнять передачу зоны.
3. Подписывающий сервер использует неподписанный файл корневой зоны, полученный от скрытого первичного сервера, и закрытый ключ для подписания ресурсных записей. Наконец, он распространяет подписанный файл зоны на первичный и вторичные DNS-серверы, используя механизмы передачи зоны.
4. Конфигурация DNS-серверов также должна быть соответствующим образом обновлена для получения данных зоны только от подписывающего сервера.

Независимо от сценария развертывания, рекомендуется проверить подписанную зону, прежде чем распространять ее по всем серверам. Эту проверку можно провести на доменном имени, используя онлайн-инструменты, подобные описанным в разделе 10 настоящего документа. Также хорошей практикой является выполнение нескольких запросов на поиск подписей ресурсных записей DNSSEC и назначение дат истечения срока действия подписи и использование других параметров для каждой из администрируемых зон. Эти тесты следует включить в процедуру проверки результатов развертывания.

Подводя итоги, сравним этапы цепочки действий при создании зоны в обычной DNS и DNSSEC:

- **Обычная DNS**: Создание → Проверка → Публикация → Текущий контроль
- **С DNSSEC**: Создание → Проверка → Подписание → Проверка → Публикация → Текущий контроль

6 Подписание TLD

Как и при любом другом серьезном изменении, перед переходом к планированию развертывания нового механизма в производственной системе настоятельно рекомендуется провести глубокое тестирование. Это особенно необходимо в случае с DNSSEC, поскольку в зону вносятся новые изменения. Описанные ниже шаги представляют собой общий обзор процедуры подписания зоны TLD, но ваша среда и конкретные требования могут привести к необходимости их откорректировать.
В некоторых случаях для крупных ccTLD нецелесообразно подписывать весь файл корневой зоны сразу; вместо этого безопаснее выработать поэтапный подход к подписанию зоны. Другие ccTLD могут также предпочесть сначала подписать дочернюю зону на испытательной платформе, прежде чем добавлять запись DS в родительскую зону, что является подготовительным тестом перед подписанием реальной зоны ccTLD.

В любом случае, чтобы успешно завершить процесс подписания, целесообразно действовать осторожно, применив соответствующие планы развертывания и тестирования в сочетании со строгой методологией проверки.

1. Разверните и настройте испытательную платформу DNSSEC. В зависимости от модели развертывания испытательная платформа может содержать следующие элементы:
   - Один тестовый сервер подписи, DNS-сервер (тестовый NS), способный подписать файл корневой зоны. Этот сервер должен иметь возможность либо генерировать ключи подписи, либо получать сгенерированные ключи с другого сервера или программно-аппаратного криптографического модуля (HSM), подписывать зону и распространять подписанный файл корневой зоны (помимо других функций).
   - Один тестовый вторичный авторитативный DNS-сервер, который будет получать подписанную зону и обслуживать ее.
   - Один тестовый резолвер, который должен быть настроен на локальное выполнение DNSSEC-валидации для подписанной зоны.
2. Скопируйте файл неподписанной зоны со скрытого первичного сервера на тестовый сервер подписи. Распространение неподписанного файла корневой зоны на тестовую систему подписания можно автоматизировать позднее, на этапе тестирования.
3. Сгенерируйте ключи KSK и ZSK. Генерировать ключи рекомендуется вне системы подписания. Храните KSK в модуле HSM или автономно и используйте его только для подписания ресурсных записей DNSKEY.
4. Подпишите зону и опубликуйте ее на одном или нескольких тестовых вторичных DNS-серверах.
5. Сгенерируйте и импортируйте DS в качестве доверенных ключей в тестовый резолвер. В реальной жизни DS не будет распространяться среди рекурсивных резолверов по всему миру непосредственно администраторами TLD; скорее, он будет отправлен в IANA для публикации в корневой зоне. Все валидирующие рекурсивные резолверы по всему миру затем получат DS, соответствующую этому TLD, из корневой зоны.
6. Проверьте результаты, проведя пользовательские приемочные испытания (UAT) на основе заранее определенных контрольных примеров. Проверяться должны такие аспекты, как получение ключей и подписей, проверка срока действия

подписей, времени ответа на запрос и размера. Среди прочих задач выполните проверку DNSSEC.

7. Если процесс тестового подписания автоматизирован, проследите за истечением срока действия подписи и автоматической генерацией новых подписей. В противном случае ключ следует обновлять вручную, пока процесс тестового подписания не будет автоматизирован.
8. Обновите ключи ZSK и KSK. Чтобы обновить ключ KSK создайте новую DS и смоделируйте совместное использование с родительской зоной, добавив эту запись в тестовый резолвер с целью локальной валидации. В зависимости от различных временных параметров, таких как период действия ключа в тестовой среде, нужно будет удалить старую DS из тестового резолвера и старый KSK из зоны, чтобы завершить обновление ключа KSK.
9. Итеративно проводите новые тесты и уточняйте шаги с 1 по 8.
10. Освоив методологию тестирования, сосредоточьтесь на переходе к реальной работе и выборе подходящей среды и сценария развертывания: BITW или поточное подписание с использованием скрытого первичного сервера. Проведите новое пользовательское приемочное тестирование, чтобы убедиться, что все авторитативные DNS-серверы правильно обслуживают зону и соответствующие ей ресурсные записи DNSSEC.
11. Наконец, опубликуйте DS в корневой зоне в соответствии с руководством по управлению делегированием для TLD, согласно определениям IANA по адресу https://www.iana.org/domains/root/manage. После добавления в корневую зону подпись делегирования объявляет всем, что данный ccTLD подписан с использованием DNSSEC и любой резолвер, ориентированный на безопасность, должен выполнять проверку DNSSEC для записей DNS, исходящих из этой зоны. Настоятельно рекомендуется использовать такой инструмент, как https://dnsviz.net/ (подробнее см. в разделе 10) для фактической проверки цепочки доверия DNSSEC для зоны.
12. Чтобы цепочка доверия вступила в силу, сразу после «официального подписания» ccTLD планируйте предоставить доступ регистраторам для публикации записей DS владельцев доменов в регистратуре.

7 Обновление ключа и алгоритма

Когда зона защищена с помощью DNSSEC, менеджер зоны должен быть готов заменить (или «обновить») ключи, используемые для защиты зоны, независимо от того, делается ли это периодически в целях безопасности, по оперативным соображениям или в чрезвычайной ситуации. Для обновления ключа или алгоритма необходимо ввести новые ключи и удалить из зоны старые ключи. Очень важно учитывать, что данные, опубликованные для зоны, хранятся в различных кэшах резолверов. Игнорирование кэшированных данных может привести к существенному нарушению условий предоставления услуг. Например, рассмотрим данные зоны, подписанные старым ключом, которые проверяет резолвер, не имеющий в своем кэше старого ключа зоны. Если старого ключа в текущей зоне больше нет, валидация будет неудачной и соответствующие данные зоны будут помечены как фиктивные.

С другой стороны, если резолвер пытается проверить данные, подписанные новым ключом, а старый ключ все еще находится в кэше резолвера, это также приведет к тому, что данные будут помечены как фиктивные. Существуют различные методы обновления

ключей и алгоритмов, описанные в документах RFC 6781 *Практика эксплуатации DNSSEC, версия 2* и RFC 7583 *Соображения относительно сроков обновления ключей DNSSEC (DNSSEC Key Rollover Timing Considerations).* Примерами таких методов являются *предварительная публикация*, *обновление ZSK с двойной RRSIG, двойной KSK*, *двойная DS, двойной RRset* и другие.

В случае, когда требуется экстренно обновить ключи из-за подозрения на взлом пары ключей ZSK или KSK, рекомендуется иметь заранее задокументированную процедуру.

7.1 Обновление ключа ZSK

Во время обновления ключа ZSK необходимо убедиться в том, чтобы у всех кэширующих валидаторов, имеющих доступ к определенной подписи, также есть доступ к соответствующему действительному ZSK. В документе RFC 6781 *Практика эксплуатации DNSSEC, версия 2* описаны три метода обновления ключа ZSK: предварительная публикация, двойная подпись и двойная RRSIG.

В этом документе мы опишем только метод предварительной публикации, поскольку он позволяет свести к минимуму размеры зон и ответов в течение всего процесса обновления ключа. Согласно этому методу новый ZSK вводится в набор DNSKEY RRset по истечении времени, достаточного для того, чтобы все кэшированные наборы DNSKEY RRset содержали оба ключа. Затем зона подписывается с использованием нового ZSK, а старые подписи удаляются. Наконец, когда срок действия подписей, созданных со старым ZSK, истекает в кэше, старый ключ удаляется. Ниже описаны этапы этого процесса.

1. Новый ZSK A вводится в зону и появляется в DNSKEY RRset, но еще не используется для подписания записей в зоне. Текущий активный KSK заново подписывает DNSKEY RRset, который затем заново подписывается текущими активными KSK. Предполагается, что на этом этапе новый ZSK уже опубликован.
2. По истечении определенного срока ZSK A становится готовым к подписанию записей в зоне. Этот срок равен задержке распространения зоны плюс времени существования записей DNSKEY в зоне. Иными словами, это максимальное время истечения срока действия существующих записей DNSKEY в кэшах. ZSK A становится активным и фактически начинает подписывать записи зоны.
3. ZSK A будет продолжать подписывать и обновлять записи зоны до того момента, пока не нужно будет опубликовать новый ZSK B. Время публикации ключа B зависит от времени активации A и времени существования ZSK, установленного для зоны политикой управления ключами. ZSK B приводится в готовность и может использоваться для подписания записей, но ZSK A все еще активен.
4. По истечении времени существования ключа ZSK A его действие прекращается. Ключ B становится активным и используется для подписания зоны. При этом ключ с истекшим сроком действия должен сохраняться в зоне в течение некоторого времени (в течение «интервала отмены»), чтобы сгенерированная с использованием этого ключа RRSIG могла по-прежнему проверяться резолверами. Интервал отмены равен времени, необходимому для переподписания всех существующих наборов RRset ключом B, плюс задержка распространения зоны и максимальное TTL всех RRSIG, созданных в зоне со старым ключом.
5. Подписи, созданные с помощью прекратившего действие ключа, по истечении определенного срока исчезают из кэшей резолверов, и старый ключ считается аннулированным.

6. После аннуляции старого ключа его можно удалить из набора DNSKEY RRset, который необходимо переподписать текущим KSK зоны. На этом этапе ключ A объявляется удаленным.
7. Спустя некоторое время публикуется новый ключ, и весь процесс повторяется.

7.2 Обновление ключа KSK

При обновлении ключа KSK основная проблема заключается в том, чтобы гарантировать, что доверенный KSK существует для зоны в любое время, даже во время процесса обновления. В документе RFC 6781 *Практика эксплуатации DNSSEC, версия 2* также описаны три метода обновления ключа KSK: двойной KSK, двойная DS и двойной RRset. Метод двойного RRset является наиболее эффективным из них, так как новые записи DS и наборы DNSKEY RRset распространяются параллельно.

Согласно этому методу новые записи DNSKEY и DS публикуются одновременно в соответствующих зонах. По истечении времени, достаточного для истечения срока действия старых наборов DNSKEY и DS RRset в кэшах, они удаляются из соответствующих зон. Этапы обновления ключа описаны ниже:

1. Записи DS и DNSKEY присутствуют в соответствующих зонах. Соответствующий им KSK A активен и обеспечивает безопасность зоны.
2. Когда срок действия текущего KSK A истекает, в зону вводится новый KSK B, который используется для подписания DNSKEY RRset. DS KSK B отправляется родителю для публикации в родительской зоне.
3. Родитель может продолжить проверку новой DS, а затем опубликовать ее в родительской зоне.
4. По прошествии некоторого времени новые DS или DNSKEY уже успевают распространиться в кэшах валидирующих резолверов. Одновременно с этим из зоны удаляется ZSK A.
5. Позже также удаляются записи DS и DNSKEY, связанные с ZSK A.
6. Спустя некоторое время публикуется новый ключ, и весь процесс повторяется.

8 Другие соображения по поводу подписанных зон

При подготовке стратегии развертывания DNSSEC стоит обратить внимание на следующие моменты:

- **Создание программы наращивания потенциала**: Найдите и примите участие в семинарах, вебинарах, практических занятиях и любых других мероприятиях по наращиванию потенциала, которые могут помочь расширить знания и развить новые навыки в работе с DNSSEC. Отдел ICANN по взаимодействию с техническим сообществом проводит такие тренинги, в том числе семинары по DNSSEC, которые обычно проходят во время конференций ICANN.
  - Помимо ICANN, мероприятия, связанные с DNSSEC, также проводят Центр ресурсов для запуска сетей (NSRC), Общество Интернета и региональные интернет-регистратуры (RIR).
  - Наконец, участие в форумах, вебинарах и семинарах, на которых как опытные операторы, так и новички встречаются, представляют и обсуждают текущие и

будущие проекты по развертыванию DNSSEC, может значительно расширить знания о методах работы DNSSEC.

- **Подписка на листы рассылки NOG**: Это полезные форумы, где люди обсуждают и делятся своим техническим опытом и знаниями, а также обращаются за поддержкой и помощью в технических вопросах, так что их можно рассматривать как сообщество, которое при необходимости может помочь.
- **Генерация и управление ключами:** Программно-аппаратные криптографические модули (HSM) обычно предоставляют хорошие возможности для генерации и хранения закрытых ключей. При этом стоит учитывать затраты на покупку, обеспечение безопасности и обслуживание HSM. В зависимости от характеристик стоимость HSM может составить от нескольких сотен до тысяч долларов. HSM также могут потребовать дополнительных затрат на обучение, поскольку освоение любого нового оборудования сопряжено с трудностями. Использование HSM является хорошей практикой, но это не единственный метод генерации ключей. Еще одна заслуживающая внимания возможность — генерация, хранение и использование закрытых ключей на автономной, не подключенной к сети, физически защищенной машине. Документ RFC 6781 *Практика эксплуатации DNSSEC, версия 2* содержит более подробную информацию о генерации и управлении ключами.
- **Соображения относительно времени**: DNSSEC вводит понятие абсолютного времени в DNS. Подписи в DNSSEC имеют срок действия от даты начала до даты истечения действия, после чего подпись помечается как недействительная, а подписанные данные считаются фиктивными. Очень важно обеспечить правильное управление временем, чтобы подписи создавались с правильным сроком действия. Представьте себе подписанную зону, срок действия подписи которой истек — это приведет к сбою валидации на стороне резолвера. Именно поэтому для точного отсчета времени настоятельно рекомендуется настроить сервер протокола сетевого времени (NTP). Существуют и другие соображения, такие как минимальное и максимальное время существования зоны (TTL), период публикации подписи и период действия подписи, как описано в RFC 6781 *Практика эксплуатации DNSSEC, версия 2*.
- **Требования к программному обеспечению, оборудованию и сети**: В настоящее время поддерживаются как открытые, так и коммерческие реализации DNSSEC, в том числе BIND, PowerDNS, NLnet Labs Name Server Daemon (NSD), Knot DNS и другие. OpenDNSSEC — это решение для подписания зоны, которое по-прежнему широко используется, поскольку автоматизирует процесс учета ключей DNSSEC и подписания зон. Если вы планируете развернуть DNSSEC на авторитативном сервере, необходимо сгенерировать в системе криптографические ключи подписи. Период времени, необходимый для генерации ключей, зависит от источника случайности (энтропии) в системе. Такие системы, как виртуальные машины с недостаточной энтропией, могут потребовать гораздо больше времени для генерации ключей.
  - Аппаратные ресурсы, например процессор, накопитель и память, также являются областями, на которые стоит обратить внимание на предмет возможной оптимизации. Это связано с тем, что включение DNSSEC увеличивает нагрузку на накопитель, память и процессор, частично из-за генерации и подписания ключей. В результате подписи зоны всегда увеличивается файл корневой зоны.
  - Что касается политики сетевой безопасности, убедитесь, что правила брандмауэра и ACL, например, разрешают как большие пакеты DNS UDP, так и

DNS по TCP через порт 53. Кроме того, механизм расширения для DNS (EDNS0) должен быть активирован на серверах DNS и в конфигурации сети соответственно.

9 Отмена подписи TLD (при необходимости)

Система DNSSEC, как и многие другие вещи в этом мире, не лишена проблем. Усложнение DNS увеличивает вероятность того, что что-то может сломаться или пойти не так. Например, KSK или ZSK, или оба ключа одновременно могут быть утеряны или взломаны. Непредвиденная ошибка аппаратного или программного обеспечения может помешать подписанию и распространению зоны, в результате чего зона не будет обслуживаться должным образом.

В худшем случае вы можете решить отменить подписание зоны, чтобы исправить все проблемы и ошибки, прежде чем подписать ее снова. При этом отмена подписи домена сопряжена с накладками в связи с возвратом в незащищенное состояние.

Подписана зона или нет определяется по наличию записи DS в родительской зоне. Если записи DS нет, цепочка доверия не гарантируется. Поэтому возврат к неподписанному состоянию технически так же прост, как удаление всех записей DS из родительской зоны. В отношении ccTLD это подразумевает отправку запроса в IANA об удалении соответствующей записи (записей) DS из корневой зоны.

После решения всех проблем оператор TLD должен рассмотреть возможность генерации новых ключей и повторного подписания зоны. Кроме того, прежде чем публиковать новую запись DS в корневой зоне, оператор должен проверить, что вновь подписанная зона хорошо распределена и доступна на всех DNS-серверах. Как только IANA публикует DS, весь интернет узнаёт, что зона TLD снова подписана и все валидирующие резолверы начинают проверять все записи ресурсов, обслуживаемых этой зоной.

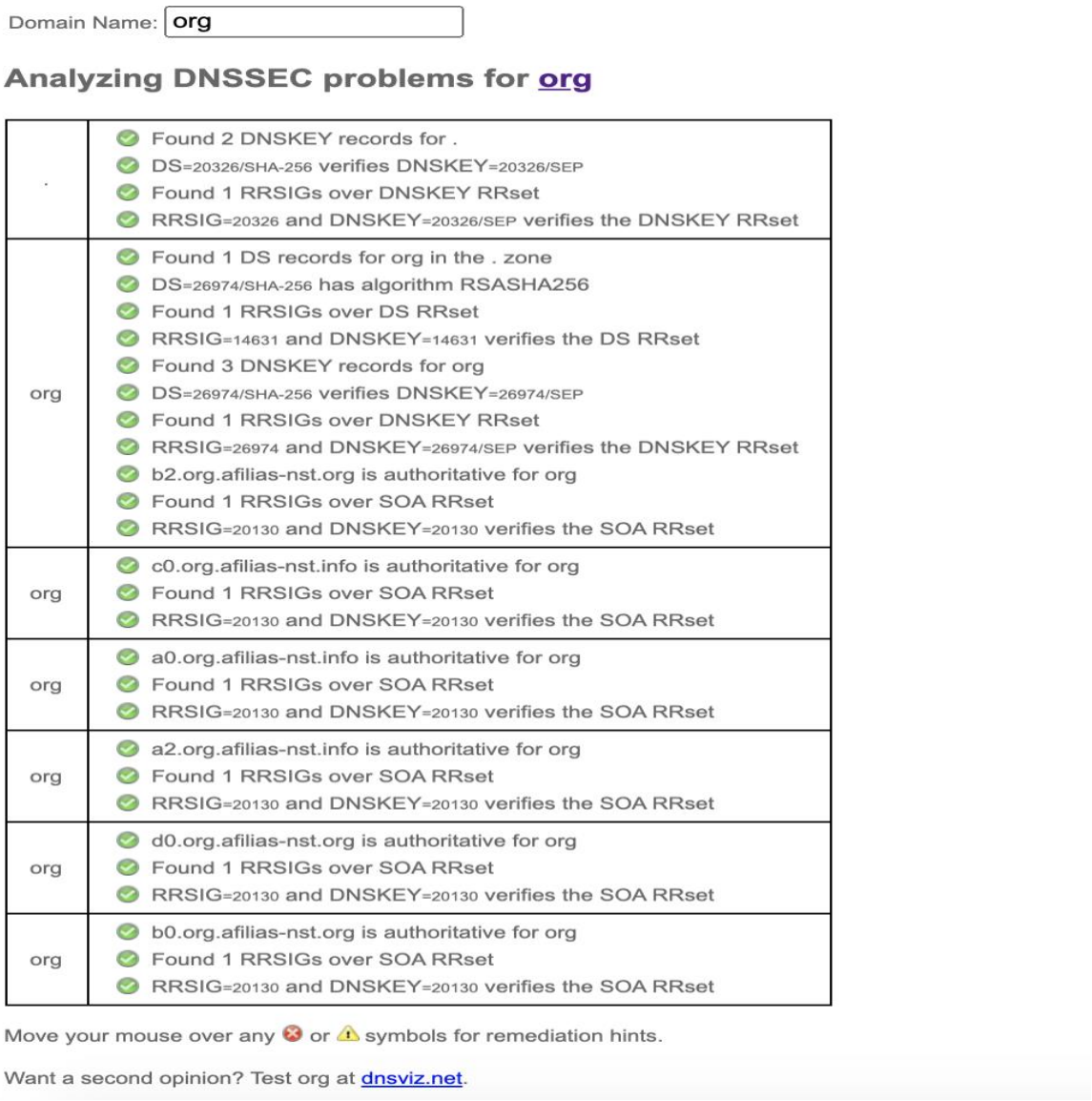
10 Полезные инструменты для DNSSEC

Следующие инструменты могут быть полезны для устранения неполадок DNSSEC.

10.1 Отладчик DNSSEC от Verisign

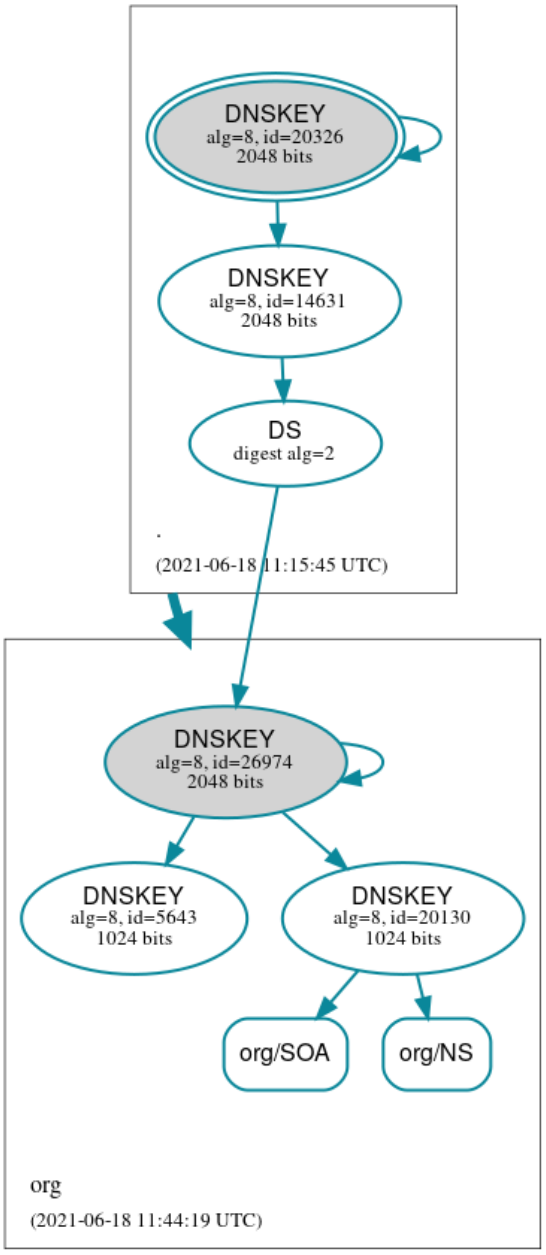
Отладчик DNSSEC, доступный по адресу https://dnssec-debugger.verisignlabs.com/, представляет собой веб-инструмент, который помогает убедиться в целостности «*цепочки доверия*» для того или иного доменного имени с поддержкой DNSSEC. Он отображает все этапы валидации заданного доменного имени и сообщает о всех найденных проблемах.

Ниже приведен пример выводимой информации:



10.2 DNSVIZ

DNSViz (https://dnsviz.net) — это инструмент для визуализации состояния зоны DNS. Он обеспечивает визуальный анализ цепочки аутентификации DNSSEC для доменного имени и цепочки его разрешения в пространстве имен DNS. Этот инструмент также составляет список обнаруженных ошибок конфигурации. Ниже приведена визуализация зоны .ORG:



11 Заключение

DNSSEC — это надежный протокол, который обеспечивает аутентификацию и целостность данных DNS. Подписание доменного имени с помощью DNSSEC многое меняет на операционном уровне, так как сопряжено с возникновением новых понятий и задач, которых не существовало в обычной DNS.

Настоящий документ представляет собой руководство, помогающее операторам регистратур ccTLD и любой другой стороне понять, что представляет собой подписание

ccTLD. О DNSSEC можно рассказывать долго, и в этом документе рассмотрены некоторые из наиболее важных аспектов его развертывания.

Как и в любом другом решении по обеспечению безопасности, во избежание неполадок рекомендуется следовать надлежащему процессу и подготовиться. Все стороны должны проанализировать собственную среду и связанные с ней угрозы и уязвимости, чтобы определить уровень риска, на который они готовы пойти при использовании DNSSEC для защиты своей зоны и доменов в ней.

По сути, скоординированные усилия и активное сотрудничество всех заинтересованных сторон остаются залогом успешного развертывания DNSSEC.

A Примеры политики DNSSEC и заявлений о практике использования DNSSEC

- Концепция политики и заявление о практике использования DNSSEC ZACR, версия 001, сентябрь 2016 года, ZACR: https://www.registry.net.za/downloads/u/zacr-dps-signed.pdf
- Заявление о практике использования DNSSEC зоны .fr, версия 1.2, июнь 2013 года, Afnic: https://www.afnic.fr/wp-media/uploads/2020/12/dps-english-fr.pdf
- Заявление о практике использования DNSSEC CIRA для зоны .CA, версия 1.5, август 2016 года, CIRA: https://www.cira.ca/cira-dnssec-practice-statement-ca
- Заявление о практике использования DNSSEC для зоны JP (JP DPS), версия 1.4, октябрь 2015 года, JPRS: https://jprs.jp/doc/dnssec/jp-dps-eng.v1.4.html
- Заявление о практике использования DNSSEC Verisign для зоны TLD/GTLD, версия 1.8, декабрь 2019,: https://www.verisign.com/assets/20191111_CTLD_VerisignDNSSECPracticeStatement_v1.8_finalized.pdf. Список зон, к которым это относится, можно найти по адресу https://www.verisign.com/assets/20190430-Verisign-Operated-TLD-GTLD-Zones-v1.04-Converted.pdf

B Пример неподписанной и подписанной зоны

B.1 Неподписанная зона

```
example.                  86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072300 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )
```

```
example.                    86400  IN     NS     a.nic.dns.blablabla.
example.                    86400  IN     NS     b.nic.dns.blablabla.
example.                    86400  IN     NS     d.nic.dns.blablabla.
example.                    86400  IN     NS     e.nic.dns.blablabla.
example.                    86400  IN     NS     f.nic.dns.blablabla.
aaa.example.                86400  IN     NS     ns1.reg.zzzz.
aaa.example.                86400  IN     NS     ns2.reg.zzzz.
bbb.example.                86400  IN     NS     ns1.reg.zzzz.
bbb.example.                86400  IN     NS     ns2.reg.zzzz.
ccc.example.                86400  IN     NS     ns1.reg.zzzz.
ccc.example.                86400  IN     NS     ns2.reg.zzzz.
ddd.example.                86400  IN     NS     ns3-l2.nic.zzzz.
```

B.2 Подписанная зона

```
example.                    86400  IN     SOA    a.nic.dns.blablabla.
hostmaster.dns.blablabla. (
                2017072305 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                2419200    ; expire (4 weeks)
                300        ; minimum (5 minutes)
                )

example.                    86400  IN     RRSIG  SOA 8 1 86400 20170724231821
20170618015310 660 example. nQ8H8StSRDoQgzwBNQ0k9+E1LGrV0tsCinoB6KxcyuHfGT4ehWsj5JI6
N01WpXqy/q1S/XlhqtjVoiti4zSOwIjFlSloug3W09eJnH9biwmb6U8B
JQoHf3edGvZtWNZdtcOKY1CFBI2ApceFn8KOYvT0qzpygOlF5lMrJvnO J5c=
example.                    86400  IN     NS     a.nic.dns.blablabla.
example.                    86400  IN     NS     b.nic.dns.blablabla.
example.                    86400  IN     NS     d.nic.dns.blablabla.
example.                    86400  IN     NS     e.nic.dns.blablabla.
example.                    86400  IN     NS     f.nic.dns.blablabla.
example.                    86400  IN     RRSIG  NS 8 1 86400 20170730192856
20170617025305 660 example. KNaF2jTPuCGq5FIzspbJL+TDBx/6z01E7+tkkzYRNh0xAKDnutcfb1It
D7XrNWPEbXsaafFyZ/M5DaDGzTzsVNm1h9h3md6o0vZNH07q8nmm+fYX
do8sx9aFxCgl9NsmG0cyrBbVnyrPKxDlAx69HJCh0kBb7PFKhr1hpnYY xGA=
example.                    86400  IN     DNSKEY 256 3 8
AwEAAasHjitdDurpevNLojD4Sp3609P+C9uOTR42DJel0NSSva/x38Ba
7gs0b4Q+tmKPI5cmxDhECiUfdzaRRA8vxPZK8x5LL/V1WZ5q6egFmH4x
eLxWaxlftFotev/T8kVe7jZUk7Hh3x7LPgGLajpjNNFELj42Xe6XBkkN 9FY1lQkB
example.                    86400  IN     DNSKEY 257 3 8
AwEAAY6HLDY5M5kjlrjVV9HQyWUkkrYZ2eB8KeJjUMN9qDM6FsA57pbS
5tmbGV1zxxqGon0pO7HYV06GZIgFOLBqDvgGsnKDQ5A2iktYNuSmTh+w
fd8ixgbYigtoBMBnNeqFozMK58c1yf7amui2cCOg9ibGZMpLQvjKOSyV
Jnlh0l8e3OE7Ul1GEa39XpVez2wkjImhsG0e7KAZPlFjEUpvwie8HEQV
jz3PK7Zr6SZVLLyet0rnN3prCHfvhNh6DycN/rt6/PopLvPQM8SaW+u8
zn6Z4S4AoTPTxKm5udzb7mWf7lT83PAbOvLu/WIRY6nqye+4SkJsrmjI xnLdk/Q54E8=
example.                    86400  IN     RRSIG  DNSKEY 8 1 86400 20170703000000
20170613000000 54322 example. B2riGYos+/q5RqXVBQKrrkVUuruDBH8ANNa8J6sMHUjf0MPZOuICd2kZ
PlAGMpZpp8LoaRoG2zaTVILZ8Vhi90FsyLsZVpPooAvmKlTFOrWoJoPo
XScLhb3ISRLOzKEnyLt5Ds3TxuabHLPlf8jpTXaHMFZCzYYtTJJQb+M3
BLeK+Lx4uCwU1pvxNkuR9StKa5tJquByIZCWZsSx5nKWPyrsGLtFJKrg
DXe8XlA8LxeER69OQgSZ1VXvK8Kd4p3wyvzUHCcsPYZzebxHXPqDrYB7
```

```
BU7eqsDUjCfThqbkC0Ju7koHROYRjGdoY/4f6nDOJEOICIFEgEDHJg2t w1nENQ==
example.                    0       IN      NSEC3PARAM 1 0 3 00FF

example.                    0       IN      RRSIG  NSEC3PARAM 8 1 0 20170716213640
20170606005304 660 example. a6Mp1NjW2/nnn+5i98AWzVrOX0yUvu/urP1cqY6zZjISReZOSLx6aorJ
lM9Nnx1fNVr2COtD71UVJI7kFUC5jVbmAitWdHHH/zyzK6WyyaN5Nsaf
cKW0Su8lLkctCHiqpKmuhOhnK1Dqmigx8YhyhPbN5nCzoST6lcnNjtV0 TwQ=
aaa.example.         86400  IN      NS      ns1.reg.zzzz.

aaa.example.         86400  IN      NS      ns2.reg.zzzz.

bbb.example.         86400  IN      NS      ns1.reg.zzzz.

bbb.example.         86400  IN      NS      ns2.reg.zzzz.

ccc.example.         86400  IN      NS      ns1.reg.zzzz.

ccc.example.         86400  IN      NS      ns2.reg.zzzz.

ddd.example.         86400  IN      NS      ns3-l2.nic.zzzz.

0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      NSEC3 1 1 3 00FF
464L7A368JEOCPKU9G34B9RQADEPKA14 NS DS RRSIG
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170703210235 20170602012306 660 example.
H+qdaHqnAgUa66VSKmMmfKWopeZQM0ridMUN2YN4rncHeWD8b0yA6O6N
hLF/ojpZoGrQN+G+p4SWJVb/pj2CkLk00E2AhloXXV0KaQIzUwPVNm7p
J9es7ohi5ErGtM1ClLpGggz05qNWboejbrXtS8TFdoTtn6Z2Omk4RNmj hG0=
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      NSEC3 1 1 3 00FF
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA NS DS RRSIG
464L7A368JEOCPKU9G34B9RQADEPKA14.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170715005821 20170610062309 660 example.
dk6WScB3zmJYig0w8LxFXoc9vj1leqFRBlET4YAVVmeAwcGf0ixa41T+
pKKcMHbXDsw+PHYZHaRLmA9lEgs+4lJMdA3fRroNSXyV2usHMdFaKUoG
UZKehVGdgrBRx4vx+o4w1ztdumY6MsD0ART6IrhUbr+cvGHAlxNSviCI BbE=
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      NSEC3 1 1 3 00FF
0KPQJ71AL5RHRST9HM8LEFLK0I0QN5N7 NS SOA RRSIG DNSKEY NSEC3PARAM
MLTMB5J4Q7T5R3GJBSBTMVD2LBMFU3KA.example.      3600 IN      RRSIG NSEC3 8 2 3600
20170706043605 20170604225320 660 example.
Ndq6p+Y8ztlgNN1vH12o5rxxh7QM8GLY3E1FPCX4h7N4RtnuoPpvEpsl
/K4XQ1p/8Uehe6Izg0BpvQ7A256/+UW3lkwlonR7UaOX/+gkEdxuxlC/
41nX5fI9G5QFrV7H8B7ezlVF/uLz4nXyH4mzz496x4iTMEoHfoAdMinL C7A=
example.                    86400  IN      SOA     a.nic.dns.blablabla.
hostmaster.dns.blablabla. 2017072305 86400 14400 2592000 3600
```

C Контрольный список по развертыванию DNSSEC

C.1 Инициация и подготовка

- ❑ Определить развертывание DNSSEC как проект

  Управление всем процессом как проектом с датой начала, намеченной датой окончания и четкими результатами с использованием методологии проектного управления.

- ❑ Подготовить документацию существующей системы

  Актуальная документация, описывающая систему и используемые процессы.

- ❑ Провести аудит существующей инфраструктуры

Устранение всех недостатков в текущей системе до развертывания DNSSEC.

- ❑ Привлечь заинтересованные стороны

  Обеспечение понимания принципов развертывания DNSSEC и подготовки к этой процедуре.

- ❑ Подготовить план обучения и следовать ему

  Обеспечение получения сотрудниками и заинтересованными сторонами знаний и навыков, необходимых для развертывания DNSSEC.

C.2 Развертывание и текущий контроль DNSSEC

- ❑ Подготовка DP или DPS

  Публикация применимой в зоне концепции функционирования DNSSEC

- ❑ Подготовка плана развертывания DNSSEC

  Описание стратегии и этапов глобального развертывания DNSSEC. В этом документе можно охватить несколько пунктов контрольного списка.

- ❑ Разработка и проверка процессов и рабочих процедур DNSSEC

  Описание процедур с учетом ваших требований и условий.

- ❑ Выбор сценария развертывания DNSSEC

  Определение модели развертывания DNSSEC

- ❑ Выбор и приобретение новых материалов и оборудования

  Приобретение нового оборудования и материалов

- ❑ Выбор параметров подписи DNSSEC

  Присвоение значений набору параметров DNSSEC

- ❑ Создание испытательной платформы DNSSEC

  Написание, выполнение и проверка тестовых примеров подписания зоны для ознакомления с процессами и операциями DNSSEC

- ❑ Планирование перехода в рабочий режим и подготовка плана нейтрализации неисправностей

  Подготовка и описание рабочего режима в производственной среде, а также процедур текущего контроля и нейтрализации неисправностей

- ❑ Рабочий режим и текущий контроль

  Подпись DNSSEC и текущий контроль работы DNSSEC в производственной среде

- ❑ План публикации DS владельцев доменов

  Продвижение DNSSEC, подготовка к получению и обработке записей DS поддоменов

- ❑ Публикация DS владельцев доменов

  Объявление DS поддоменов в зоне ccTLD

- ❑ Описание накопленного опыта

Сбор и сведение воедино информации об уроках и опыте, извлеченных на каждом этапе процесса

D Дополнительная литература

- *Major DNSSEC Outages and Validation Failures*, IANIX: https://ianix.com/pub/dnssec-outages.html
- *DNSSEC: The long and bumpy road of algorithm deployment*, APNIC, https://blog.apnic.net/2020/12/01/dnssec-the-long-and-bumpy-road-of-algorithm-deployment/
- *DNSSEC Infrastructure Audit Framework*, NLnet Labs, https://nlnetlabs.nl/downloads/publications/dns-audit-framework-1.0.pdf
- *Root DNSSEC information*, IANA, https://www.iana.org/dnssec
- *Frequently Asked Questions about DNSSEC*, SIDN, https://www.sidn.nl/en/faq/dnssec
- RFC 6781, *DNSSEC Operational Practices v2,* https://www.rfc-editor.org/rfc/rfc6781.html

1. RFC 6841, *A Framework for DNSSEC Policies and DNSSEC Practice Statements,* https://www.rfc-editor.org/rfc/rfc6841.html
2. RFC 8078, *Managing DS Records from the Parent via CDS/CDNSKey,* https://www.rfc-editor.org/rfc/rfc8078.html
3. RFC 8624, *Algorithm Implementation Requirements and Usage Guidance for DNSSEC,* https://www.rfc-editor.org/rfc/rfc8624.html