РЕГЛАМЕНТ

расширения DNSSEC

версия 1.0

4 октября 2019

1. Общие положения

Этот документ (далее Регламент) описывает основные принципы работы расширения DNSSEC.

Для активации DNSSEC в домене необходимо указать DNSKEY запись в этом домене и соотвествующую ей DS запись в Реестре соответствующего домена верхнего уровня. Опубликованная DS запись устанавливает цепочку доверия от домена верхнего уровня к подрядному домену.

2. Термины и определения

Реестр - информационно-техническая система обработки данных, которая содержит информацию о доменных именах, адресах сети, Регистраторах, Регистрантах и контактных лицах Регистрантов, а также предоставляет интерфейс для работы Регистраторов согласно принятого Регламента.

Администратор публичного домена - лицо, которое осуществляет мероприятия по административному сопровождению публичного домена и обеспечению его работоспособности.

Оператор Реестра – лицо, которое осуществляет мероприятия по техническому сопровождению Реестра.

Регистратор - лицо, которое предоставляет Регистранту услуги по регистрации и сопровождению доменного имени.

Регистрант – лицо, в интересах которого осуществляется регистрация и делегирование приватного доменного имени.

Домен – символьное обозначение областей в сети Интернет, которое базируется на иерархической структуре и позволяет определять доменные имена.

Доменное имя – символьное обозначение, которое служит для адресации узлов сети Интернет и размещенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты, сетевых сервисов) в удобной для человека форме.

Сервер имен (NS) - специализированный программно-аппаратный комплекс в сети Интернет, который обеспечивает взаимосвязь доменных имен и IP адресов.

DNS - компьютерная распределенная система для получения информации о домене.

DNSSEC – расширение существующей системы DNS, которое обеспечивает аутентификацию данных DNS и позволяет проверить, что содержимое ответа DNS не было изменено.

DNSKEY – запись, содержащая открытый ключ подписи, который можно использовать для проверки подписей DNSSEC.

DS – запись подписанта делегирования (Delegation Signer), которая содержит данные цифровой подписи для доменного имени и используется для идентификации ключа подписи DNSKEY.

3. Интерфейс работы с расширением DNSSEC

Общая спецификация расширения DNSSEC определена в RFC5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).
В Реестре реализован тип интерфейса DS Data Interface (согласно RFC5910).
Полная реализация схемы расширения DNSSEC:
https://hostmaster.ua/epp/secDNS-1.1.xsd

Реестр принимает DS записи от регистраторов через EPP интерфейс либо через web-интерфейс. DS запись должна соответствовать стандартам, указанным в разделе 11 данного Регламента.

Интерфейс работы с расширением DNSSEC позволяет выполнять операции:

- получение информации о DS записи делегированного домена
- создание домена с DS записью
- добавление DS записи к ранее делегированному домену
- изменение DS записи в делегированном домене
- удаление DS записи в делегированном домене

Интерфейс работы с расширением DNSSEC не предусматривает работу с ключами (Key Data Interface согласно RFC5910). Интерфейс не поддерживает опции maxSigLife и urgent.

Расширение DNSSEC вносит изменения в ответ сервера на запрос <domain:info> при условии использования DNSSEC в домене, в отношении которого выполнен запрос.

Расширение DNSSEC, при условии его использования, вносит изменения в команды клиента <domain:create> и <domain:update>.

Расширение DNSSEC не вносит изменений в команду <domain:transfer>, однако при попытке перевода доменного имени, подписанного DNSSEC, к регистратору, который не поддерживает это расширение, трансфер будет отклонен.

Указаное расширение никак не влияет на работу команд <domain:check>, <domain:delete>, <domain:renew> и <domain:restore>. В случае выполнения команды <domain:restore> относительно домена, который имел DS записи, они восстанавливаются вместе с доменом.

4. Получение информации о DS записи делегированного домена

В ответе EPP-сервера на запрос <domain:info> предоставляется

информация о DS записи делегированного домена согласно RFC5910.

5. **Создание домена с DS записью**

В заявке на регистрацию доменного имени может быть указана DS запись, которая соответствует DNSKEY записи подрядного домена. При регистрации домена, на серверах имен, которые указаны в запросе, уже должен существовать соответствующий домен и сформированная DNSKEY запись, которая соответствует отправленной в запросе DS записи. EPP-сервер выполняет проверку соответствия отправленной DS записи и записи DNSKEY подрядного домена на всех указанных серверах имен. Домен делегируется независимо от результатов проверки, однако в случае, если отправленная DS запись не соответствует DNSKEY записи подрядного домена, кроме сообщения о регистрации домена, регистратору отправляется предупреждение об отсутствии соответствующей DNSKEY записи в подрядном домене.

Максимальное количество записей DS для одного домена – шесть. Если отправленная клиентом команда приведет к созданию более 6 записей DS, то операция не выполняется, а клиенту возвращается сообщение об ошибке.

6. **Добавление DS записи к ранее делегированному домену**

Для добавления новой DS записи к ранее делегированному домену используется команда <domain:update>. После добавления DS записи выполняется проверка соответствия DS записи и DNSKEY записи подрядного домена. Если DNSKEY запись не соответствует отправленной записи DS, то регистратору отправляется предупреждение об отсутствии соответствующей DNSKEY записи в подрядном домене.

В команде возможно дополнительно указать DNSKEY запись подрядного домена для отправленной DS записи. В таком случае проверка соответствия DS записи и DNSKEY записи подрядного домена проводится до выполнения операции. В случае не прохождения проверки, операция добавления DS записи не выполняется, а клиенту возвращается сообщение об ошибке.

Максимальное количество записей DS для одного домена – шесть. Если отправленная клиентом команда приведет к созданию более 6 записей DS, то операция не выполняется, а клиенту возвращается сообщение об ошибке.

7. **Изменение DS записи в ранее делегированном домене**

Изменение записи в ранее делегированном домене можно произвести при помощи последовательности операций: удаления DS записи и добавления новой DS записи. Также это действие можно выполнить при помощи одной операции <domain:update>. В этом случае в расширении необходимо указать команду удаления опеределенных либо всех DS записей, после этого в рамках того же расширения добавляется одна либо несколько новых DS записей. В результате внесения изменений в DS записи, максимальное количество DS

записей не должно превысить шести. Если отправленная клиентом команда приведет к созданию более 6 записей DS, то операция не выполняется, а клиенту возвращается сообщение об ошибке. После проведения операции изменения DS записей выполняется проверка соответствия отправленной DS записи и записи DNSKEY подрядного домена.

В команде возможно дополнительно указать DNSKEY запись подрядного домена для отправленной DS записи. В таком случае проверка соответствия DS записи и DNSKEY записи подрядного домена проводится до выполнения операции. В случае не прохождения проверки, операция добавления DS записи не выполняется, а клиенту возвращается сообщение об ошибке.

8. Изменение NS записей в домене с существующей DS записью

При изменении NS записей выполняется проверка наличия на новых серверах имен соответствующей(их) DNSKEY записи(ей). В случае ее отсутствия, изменения вносятся, а регистратору отправляется предупреждение об отсутствии соответствующей DNSKEY записи в подрядном домене.

9. Особенности команды transfer для домена с DS записью

В случае, если домен с существующей DS записью передается от регистратора, который поддерживает работу с расширением DNSSEC, к регистратору, не поддерживающему работу с таким расширением, сначала текущий Регистратор должен удалить все DS записи в домене верхнего уровня, а потом новый регистратор должен подать запрос на трансфер данного домена. Если на момент поступления запроса на трансфер от регистратора, который не поддерживает расширение DNSSEC, в домене существуют DS записи, то такой запрос отклоняется с сообщением об ошибке.

10. Удаление DS записи в делегированном домене

При получении от регистратора запроса на удаление DS записи, данная запись удаляется из домена верхнего уровня.

Удаление DS записи в делегированном домене выполняется при помощи расширения в команде <domain:update> согласно RFC5910. Записи DS могут быть удалены выборочно либо все одновременно.

Удаление всех DS записей (без добавления новых) приводит к деактивации DNSSEC для данного домена.

11. Особенности операций с DS записью для web-интерфейса

При работе через web-интерфейс доступны операции добавления DS записи в ранее делегированом домене и удаления DS записи. Перед выполнением операции добавления DS запись дополнительно проверяется на соответствие DNSKEY записи на серверах имен подрядного домена. В случае

несоответствия – операция не выполняется, а клиенту возвращается сообщение об ошибке.

12. Стандарты, которые поддерживает реестр

Номера алгоритмов, которые стандартизированы для использования в DNSSEC, приведены на сайте IANA по следующему адресу: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml
Реестр принимает DS записи, если соответствующий DNSKEY создан по алгоритмам:

- 8 RSA/SHA-256
- 10 RSA/SHA-512
- 13 ECDSA Curve P-256 with SHA-256
- 14 ECDSA Curve P-384 with SHA-384
- 15 Ed25519

Номера алгоритмов, которые стандартизированы для DS записей приведены на сайте IANA по следующему адресу: https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml
Реестр принимает DS записи, созданные по алгоритмам:

- 2 SHA-256
- 4 SHA-384

13. Порядок внесения изменений в Регламент

У случае необходимости Оператор Реестра может вносить изменения в Регламент расширения DNSSEC. Изменения в Регламент публикуются на сайте Оператора Реєстра для ознакомления одновременно соответсвующим уведомлением Администраторов публичных доменов и Регистраторов. Изменения в Регламент могут вноситься за 30 дней до введения их в действие.

У случае насущной необходимости, внесение изменений в Регламент может осуществляться одновременно с их публикацией на сайте Оператора Реестра одновременно с соответствующим уведомлением Администраторов публичных доменов и Регистраторов. Под понятием насущной необходимости понимаются условия, при которых дальнейшее предоставление услуг Оператором Реестра невозможно без внесения соответствующих изменений.