Технический
Центр
Интернет

Политика DNSSEC реестров RU, РФ

Техническая политика

На 19 страницах

Информация о документе

Индекс документа	ТП
Статус документа	Технические нормы
Дата начала действия документа	29.09.2017
Версия	1.2
Дата окончания действия документа	

Содержание

1 Введение

Данный документ является частью системы технической документации; центральный документ этой системы – «Технические условия взаимодействия с системой регистрации доменов».

Документ описывает основные процедуры и меры, принятые для внедрения DNSSEC в доменах верхнего уровня (далее – ДВУ) .RU и .РФ.

1.1 Сообщество и применимость

1.1.1 Регистратура

Регистратура ДВУ обладает полномочиями по выработке правил регистрации доменных имен в ДВУ, в том числе выработку политики DNSSEC, а также отвечает за аккредитацию регистраторов. Регистратура использует реестр на стороне внешнего субподрядчика, а именно, АО "Технический Центр Интернет" (далее – ТЦИ). ТЦИ отвечает за: функционирование реестра и систему регистрации в ДВУ; проверку и обработку данных DNSSEC, полученных от аккредитованного регистратора; формирование и подписание ресурсных записей в файле ДВУ; управление ZSK и распространение ДВУ по надлежащим серверам DNS.

1.1.2 Регистратор

Регистратор - юридическое лицо, аккредитованное регистратурой ДВУ. Регистрация новых доменных имен и размещение DS записей для них в ДВУ осуществляется аккредитованными регистраторами. Аккредитованные регистраторы несут ответственность за проверку принадлежности ключа KSK администратору доменного имени.

1.1.3 Администратор домена

Администратор домена – лицо, заключившее договор о регистрации доменного имени с регистратором и осуществляющее администрирование данного домена.

Администраторы доменных имен, размещенных в ДВУ, вносят необходимые изменения с помощью аккредитованных регистраторов и несут ответственность за правильность подписи своей доменной зоны, а также за актуальность размещенных в реестре открытых ключей в виде DS-записей в соответствии со своими потребностями.

1.1.4 Заинтересованные стороны

Заинтересованные стороны – участники сети Интернет, которые полагаются на работу DNSSEC, например, валидирующие DNS-серверы. Заинтересованные стороны несут ответственность за настройку и обновление надлежащих доверенных открытых ключей на своем оборудовании.

1.1.5 Применимость

Данная политика DNSSEC применяется ДВУ XN--P1AI (РФ) и .RU, и описывает процедуры и меры, принятые для внедрения DNSSEC в этих ДВУ. Применение DNSSEC в субординатных доменах выходит за рамки данного документа и описывается администраторами этих доменов.

1.2 Управление документом

Данный документ будет периодически пересматриваться и обновляться в случае необходимости.

2 Публикация открытых ключей и репозитарии

2.1 Репозитарии

ТЦИ публикует техническую документацию, относящуюся к функционированию DNSSEC в ДВУ, на официальном сайте компании в соответствующем разделе, доступном по адресу:

- https://www.tcinet.ru/documents.

2.2 Контроль доступа к документации

Информация, опубликованная на официальном сайте ТЦИ, защищена от несанкционированного удаления или модификации. При доступе к официальному сайту ТЦИ рекомендовано проверять сертификат SSL.

2.3 Публикация ключа для подписи ключей

ТЦИ составляет цепочку доверия DNSSEC, публикуя открытый KSK в форме DS-записи непосредственно в корневой зоне DNS.

3 Эксплуатационные требования

3.1 Активация DNSSEC для субординатного домена

Для активации DNSSEC в субординатном домене необходимо разместить DNSKEY запись и соответствующую ей DS запись в реестре ДВУ. ТЦИ проверяет данные на корректность, выполняя следующие тесты:

- Проверка поддержки реестром алгоритма, по которому сформирована DS-запись;
- Проверка подписи;
- Проверка тега ключа.

Если домен делегирован и проверка DS-записи прошла успешно, то DS-запись для данного домена будет опубликована в DNS. Опубликованная DS-запись устанавливает цепочку доверия к субординатному домену.

3.2 Идентификация и аутентификация администратора домена

Надежная идентификация и аутентификация администратора субординатного домена входит в обязанности регистратора, с помощью подходящих для этого способов.

3.3 Регистрация DS-записей

ТЦИ принимает DNSKEY-записи и соответствующие им DS-записи от регистраторов, используя EPP-интерфейс.

DS и DNSKEY записи должны быть корректными и отправлены в формате, описанном в RFC 4310. Реестр принимает следующие алгоритмы подписи для DNSKEY-записей:

№ алгоритма[1]	Наименование алгоритма	Код алгоритма	Стандарт
3	DSA/SHA-1	DSA	RFC3755
5	RSA/SHA-1	RSA/SHA-1	RFC 3110, RFC 4034
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	RFC 5155
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	RFC 5155
8	Secure Hash Algorithm Version 2 (RSA/SHA-256)	RSASHA256	RFC 5702
10	Secure Hash Algorithm Version 2 (RSA/SHA-512).	RSASHA512	RFC 5702
12	ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. (GOST R 34.10-2001)	ECC-GOST	RFC 5933
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	RFC 6605
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384	RFC 6605

Табл. 1. Алгоритмы, допустимые для DNSKEY-записи

[1] См. https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml.

Реестр принимает DS-записи по следующим дайджест-алгоритмам:

№ алгоритма[2]	Наименование алгоритма	Код алгоритма	Стандарт
1	US Secure Hash Algorithm 1	SHA-1	RFC 3174
2	Secure Hash Algorithm Version 2, 256	SHA-256	RFC 4634
3	ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хеширования (принят в качестве межгосударственного стандарта ГОСТ 34.311-95).	GOST R 34.11-95	RFC 5933
4	Secure Hash Algorithm Version 2, 384	SHA-384	RFC 6605

Табл. 2. Алгоритмы шифрования DS-записей

3.4 Способ определения владельца закрытого ключа

ТЦИ не выполняет дополнительных проверок с целью достоверного определения, что администратор субординатного домена владеет закрытым ключом.

3.5 Удаление DS-записей

ТЦИ удаляет из реестра DS-запись при получении от регистратора соответствующего запроса через EPP-интерфейс. Удаление всех DS-записей для субординатного домена деактивирует DNSSEC для этого домена. Только администратор субординатного домена или сторона официально уполномоченная представлять интересы администратора субординатного домена могут при помощи регистратора отправить запрос на удаление DS-записи для этого домена.

[2] См. https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml.

4 Средства управления и эксплуатационный контроль

4.1 Физические средства управления

4.1.1 Площадка проведения процедур и её конфигурация

ТЦИ располагает несколькими объектами на территории России. Эти объекты включают в себя: Защищенные от несанкционированного доступа серверные стойки в центрах обработки данных, подготовленное основное помещение для проведения процедур в офисе ТЦИ и резервное помещение в одном из центров обработки данных.

4.1.2 Физический доступ

К объектам ТЦИ организован ограниченный доступ, который предоставляется только уполномоченному персоналу.

4.1.3 Электропитание и кондиционирование воздуха

Объекты ТЦИ оснащены источниками бесперебойного питания и системами кондиционирования воздуха. Оборудование ТЦИ расположенное в центрах обработки данных имеет резервные источники питания, на случай выхода из строя одного из них.

4.1.4 Подверженность затоплению

ТЦИ предприняты меры предосторожности для минимизации влияния водного воздействия на оборудование.

4.1.5 Пожарная безопасность

Объекты ТЦИ оснащены пожарными датчиками и централизованной системой пожаротушения.

4.1.6 Хранение информации

Критичные носители информации размещаются в сейфах, доступ к которым предоставляется только уполномоченному персоналу.

4.1.7 Уничтожение информации

Критичные документы уничтожаются способом измельчения. Электронные носители информации перед утилизацией подвергаются специальному форматированию, для исключения возможности восстановления информации, ранее записанной на эти носители.

4.1.8 Резервная копия

ТЦИ создает резервные копии критических системных данных. Резервные носители критичной информации располагаются на резервных площадках. Эти носители информации защищены от несанкционированного доступа.

4.2 Процедурные средства управления

Для работы с закрытым KSK созданы две доверенные роли: крипто-офицер и крипто-оператор, каждая из которых состоит минимум из двух допущенных лиц. Каждое из допущенных лиц имеет персональный идентификатор и пароль к нему. Для работы с закрытым KSK необходимо наличие минимум двух крипто-офицеров и одного крипто-оператора. Сотрудник, привлеченный к работе с закрытым KSK, не может одновременно совмещать роли крипто-офицера и крипто-оператора.

Для работы с ZSK создана доверенная роль: **администратор доменной зоны,** которая состоит минимум из двух допущенных лиц. Для контроля и управления ключами ZSK в полуавтоматическом режиме необходимо хотя бы одно допущенное лицо.

Для контроля над ходом выполнения ключевых процедур создана роль «Наблюдатель», которая состоит минимум из двух допущенных лиц.

4.3 Средства управления персоналом

4.3.1 Квалификация и опыт

Выше описанный персонал является сотрудниками ТЦИ, либо лицами, специально утвержденными регистратурой на роль крипто-офицера. Персонал, участвующий в процедурах, должен иметь опыт в области применения DNSSEC.

4.3.2 Требования к подготовке

Новые сотрудники, перед вступлением в вышеописанные роли, должны изучить внутреннюю документацию, описывающую реализацию DNSSEC в ТЦИ. Они также должны принять участие в ключевых процедурах в качестве наблюдателей перед началом исполнения своих обязанностей.

4.3.3 Переподготовка

ТЦИ периодически проверяет готовность персонала к проведению процедур и осуществляет переподготовку по мере необходимости.

4.3.4 Документация

Документация, описывающая порядок выполнения процедур, доступна для всех вовлеченных сотрудников.

4.4 Учет доступа

Каждый факт доступа в специально отведенную зону работы с критичной информацией DNSSEC сохраняется в автоматизированной системе учета. В тех зонах, где автоматизация невозможна факты доступа протоколируется в специальных журналах. Журналы и сохраненные протоколы автоматизированной системы учета доступа регулярно просматриваются и анализируются. Периодичность анализа определяется политикой информационной безопасности ТЦИ. При анализе журналов доступа строго выполняется разделение ролей между лицом (лицами), проводящим (и) анализ, и теми, чьи действия подвергаются мониторингу.

4.5 Компрометация и восстановление после сбоя

Если некоторое событие привело или может привести к нарушениям безопасности, то проводится внутреннее расследование с целью выявления причин произошедшего и их устранения. Если

данное событие компрометирует критичную информацию DNSSEC, то происходит аварийная замена ключей. Инициирует процедуру аварийной замены ключей крипто-оператор. В случае компрометации ключа ТЦИ продолжит эксплуатацию этого ключа до завершения процедуры аварийной замены ключей.

5 Технические средства безопасности

5.1 Генерация ключей и их внедрение

5.1.1 Генерация ключей

Создаваемые ключи KSK генерируются и хранятся в специализированном устройстве, называемом HSM (Hardware Secure Module – аппаратный модуль защиты), у которого отсутствует подключение к сетевой инфраструктуре. Все операции с использованием криптографических преобразований, требующие участия закрытого KSK, выполняются на этом устройстве или на идентичном ему, которое используется в качестве резервного. Для обеспечения безопасности закрытый KSK может покидать устройство только в зашифрованном виде.

Создаваемые ключи ZSK генерируются и хранятся на сервере подписания, который подключен к внутренней сети реестра доменов верхнего уровня. Все операции с использованием криптографических преобразований, требующие участия закрытого ZSK, выполняются на этом устройстве или на идентичном ему, которое используется в качестве резервного. Для обеспечения безопасности закрытый ZSK может покидать устройство только в зашифрованном виде.

5.1.2 Распространение открытого ключа

Открытый KSK распространяется средствами протокола DNS.

5.1.3 Параметры генерации открытого ключа и проверка качества

Задание параметров и проверка качества ключевой информации осуществляется ТЦИ.

5.1.4 Применение ключа

ТЦИ использует ключевую информацию исключительно для подписи зоны домена верхнего уровня.

5.2 Средства защиты закрытого ключа

5.2.1 Контроль несколькими людьми за использованием закрытого ключа

Операции, требующие закрытой части KSK, выполняются крипто-офицерами и крипто-операторами в порядке, определённом в секции «Процедурные средства управления». Персональный идентификатор крипто-офицера содержит часть парольной фразы, необходимой для получения доступа к защищённому диску на HSM. Для восстановления пароля достаточно участия крипто-офицеров в количестве $m<n$, где n – общее количество частей парольной фразы (крипто-офицеров).

5.2.2 Резервное копирование закрытого ключа

Периодически выполняется резервное копирование закрытого ключа. Закрытый ключ покидает устройство исключительно в зашифрованном виде. Резервная копия закрытого KSK содержится в зашифрованном виде отдельно от HSM в хранилище, доступ к которому контролируется крипто-оператором, и может быть расшифрована крипто-офицерами.

Резервная копия закрытого ZSK хранится на резервном сервере подписания с горячим подключением, расположенном на резервной площадке, и включается в каждую резервную копию базы данных реестра.

5.2.3 Архивация закрытого ключа

Выведенные из использования закрытые ключи хранятся исключительно в виде резервных копий.

5.2.4 Перемещение закрытого ключа

Закрытые ключи могут быть извлечены из устройств подписания в зашифрованном виде и восстановлены на резервных системах уполномоченным персоналом в порядке, определённом в секции «Процедурные средства управления».

5.2.5 Способ активации закрытого ключа

Доступ к закрытому KSK открывается после открытия доступа к HSM и после дешифрования защищённого диска. Крипто-оператор обеспечивает доступ крипто-офицеров к консоли HSM. Крипто-офицеры используют персональные идентификаторы для дешифрования защищённого диска.

Доступ к закрытому ZSK обеспечивается Администратором доменной зоны из интерфейса управления DNSSEC.

5.2.6 Способ деактивации закрытого ключа

Доступ к закрытому KSK прекращается автоматически немедленно после проведения операции подписания.

Доступ к закрытому ZSK прекращается после выключения сервера подписания.

5.2.7 Способ уничтожения закрытого ключа

Не предполагается уничтожение закрытых ключей. Они могут быть удалены из системы с целью недопущения их использования в будущем.

5.3 Примечания к управлению ключевыми парами

5.3.1 Резервное копирование открытых ключей

Открытые ключи подвергаются резервному копированию при проведении плановых процедур резервного копирования на устройствах.

5.3.2 Сроки использования ключей

Срок действия KSK устанавливается в один год, ZSK – три месяца. Оператор реестра при необходимости может изменить данные сроки. Устаревшие ключи не используются повторно.

5.3.3 Данные для активации

5.3.3.1 Генерация данных для активации и их внедрение

Данные для доступа к KSK представляют собой набор паролей к персональным идентификаторам крипто-офицеров и паролей к персональным идентификаторам крипто-операторов (PIN-коды).

5.3.3.2 Защита данных для активации

Крипто-офицеры и крипто-операторы обеспечивают сохранность данных для доступа в соответствии с рекомендациями по безопасности.

5.3.4 Примечания по работе с данными для активации

В качестве экстренной меры крипто-офицеры и крипто-операторы хранят копии парольных данных в индивидуальных опечатанных пеналах, хранящихся в безопасном месте.

5.4 Средства управления компьютерной безопасностью

Все критичные для деятельности ТЦИ компоненты располагаются на площадках, защищённых от несанкционированного доступа. Разграничение доступа проводится среди уполномоченного персонала в соответствии с их должностными обязанностями; осуществляется учёт фактов получения доступа.

5.4.1 Средства управления сетевой безопасностью

Онлайновая часть системы подписания присоединяется к внутренней сети ТЦИ, которая логически отделена от внешней сети. Подключение к данной онлайновой части возможно исключительно минуя межсетевой экран, при этом межсетевой экран предоставляет минимально необходимые для осуществления управления возможности.

Содержащая KSK часть системы подписания не имеет сетевого подключения. Передача запроса на подписание ключевого набора (KSR) осуществляется через съёмный носитель.

5.4.2 Метки времени

Онлайновая часть системы подписания осуществляет синхронизацию времени с доверенным источником во внешней сети. Установка времени в офлайновой части системы осуществляется вручную при каждом включении HSM.

5.5 Средства управления жизненным циклом

5.5.1 Системные средства управления разработкой

Разрабатываемые ТЦИ приложения используют системы контроля версий. Перед внедрением в рабочий реестр предоставляемые третьей стороной разработки проходят лабораторное тестирование на совместимость с разработками ТЦИ.

5.5.2 Средства управления безопасностью

ТЦИ проводит периодический аудит безопасности.

5.5.3 Средства управления безопасностью жизненного цикла

Системы подписания разработаны с учётом минимизации обслуживания. Критичные с точки зрения безопасности и функциональности обновления применяются после прохождения лабораторного тестирования.

6 Подпись доменной зоны

6.1 Длины и алгоритмы ключей

В системе подписания применяются необходимые с точки зрения безопасности на протяжении периода использования длины ключей и их алгоритмы. Текущим алгоритмом для KSK и ZSK является RSA-SHA256 с длиной ключа 2048 и 1024 бит соответственно.

6.2 Авторитетное подтверждение отсутствия домена

Для авторитетного подтверждения отсутствия домена используется механизм NSEC3 OPT-OUT, [RFC 5155].

6.3 Формат подписи

Подпись формируется по алгоритму RSA и хешированием по SHA256, см. [RFC 5702].

6.4 Ротация ZSK

Для ротации ZSK применяется схема с предварительной публикацией, см. [RFC 4641].

6.5 Ротация KSK

Для ротации KSK применяется схема с двойной подписью, см. [RFC 4641].

6.6 Время действия подписей и частота обновления подписи

Время жизни подписи для ключевого набора устанавливается в 20 дней. Для записей других типов время жизни подписей устанавливается в 45 дней. Обновление подписи зоны осуществляется каждые 2 часа.

Данные параметры могут быть изменены при необходимости.

6.7 Проверка набора ключей

При создании состоящего из открытых ключей KSK и ZSK ключевого набора (KSR) происходит подписание последнего при помощи содержащегося в онлайновой части системы ключа PGP реестра. Офлайновая часть системы автоматически проверяет подпись KSR при помощи предварительно импортированного открытого ключа PGP реестра перед принятием KSR на подпись.

6.8 Проверка ресурсных записей

ТЦИ проверяет ресурсные записи на соответствие стандартам.

6.9 Время актуальности ресурсных записей

Время жизни записей типа DNSKEY, DS и соотносящихся с ними RRSIG установлено в 345600 секунд (4 дня).

Время жизни записей типа NSEC3 установлено в 3600 секунд (1 час), что соответствует времени отрицательного кэша для зоны.

Данные параметры могут быть изменены при необходимости.

7 Аудит соответствия и правовые вопросы

В соответствии с внутренней политикой безопасности проводится регулярный аудит, результатом которого является устранение замечаний и недостатков работы системы и введение улучшений.

ТЦИ не несёт юридической ответственности за вопросы, описанные в данном документе.

В своей деятельности ТЦИ опирается на законодательство Российской Федерации и распорядительные документы Регистратуры.

Приложение 1. Список внесенных изменений

История изменения документа

Дата изменения	Номер версии	Описание изменения
22.07.2016	1.1	Расширен список поддерживаемых стандартов. Оформление документа приведено к стандарту.
21.09.2017	1.2	В документе приведены списки алгоритмов DNSKEY и DS-записей.

Контакты АО «Технический центр Интернет»

- 127083, Москва, улица 8 Марта, дом 1 строение 12.
- Телефон: +7 (495) 730-29-69.

Клиентская служба

Клиентская служба Технического центра Интернет:

- Телефон: +7 (495) 730-29-69.