Политика DNSSEC для доменов .KZ и .ҚАЗ

1. ВВЕДЕНИЕ

1.1 В документе используются следующие основные понятия и сокращения:

1) DNS – специализированное программное обеспечение для обслуживания системы доменных имен, а также оборудование, на котором программное обеспечение выполняется;

2) DNSSEC – расширение DNS, которое добавляет поддержку аутентификации источника и проверку целостности данных для системы доменных имен;

3) DS-запись – запись указывает на ключ, который зона, расположенная на уровень ниже (делегируемая зона), должна использовать для удостоверения (подписывания) адресной информации.

4) DNSKEY-запись – содержит публичную часть ключа и его идентификаторы (ID, тип и используемая хеш-функция);

5) KSK – ключ для подписи ресурсной записи DNSKEY;

6) ZSK – ключ для подписи ресурсных записей;

7) HSM – аппаратный модуль защиты;

8) Субдомен – домен второго, третьего и более уровней.

2. ОБЩИЕ СВЕДЕНИЯ

2.1 Данный документ описывает основные процедуры для функционирования DNSSEC в доменах верхнего уровня .KZ и .ҚАЗ

2.2 Регистратура доменов верхнего уровня сама определяет политику функционирования DNSSEC:

1) Управляет KSK;
2) проверяет и обрабатывает данные DNSSEC, полученные от аккредитованного регистратора;
3) формирует и подписывает ресурсные записи в файле доменов верхнего уровня;
4) управляет ZSK и распространяет файл доменов верхнего уровня по авторизованным серверам DNS.

2.3 Регистратор осуществляет регистрационные действия в реестре от имени регистранта домена. Регистратор несёт ответственность за проверку ключа KSK, принадлежащему регистранту доменного имени.

2.4 Регистранты доменных имен, 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.

2.5 Заинтересованные стороны – участники сети Интернет, которые полагаются на работу

DNSSEC, например, валидирующие DNS-серверы, несут ответственность за настройку и обновление надлежащих доверенных открытых ключей на своем оборудовании.

2.6 Применение DNSSEC в субдоменах выходит за рамки данного документа и описывается регистраторами этих доменов.

3. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ

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

3.2 Для активации DNSSEC в субдомене необходимо разместить хотя бы одну DS-запись в реестре доменов верхнего уровня. Регистратура проверяет данные на корректность, выполняя проверку поддержки реестром алгоритма, по которому сформирована DS-запись тега ключа. Если проверка DS-записи прошла успешно, то DS-запись для данного домена будет опубликована в DNS. Опубликованная DS-запись устанавливает цепочку доверия к субдомену.

3.3 Надежная идентификация и аутентификация регистранта субдомена входит в обязанности регистратора, с помощью подходящих для этого способов.

3.4 Регистратура принимает DS-записи от регистраторов, используя EPP-интерфейс. DS и DNSKEY-записи должны быть корректными и отправлены в формате, описанном в RFC 4310. Реестр Регистратуры поддерживает размещение DS-записей, сформированных в соответствии с RFC 4034 и RFC 5933.

3.5 Регистратура не выполняет дополнительных проверок с целью достоверного определения, что регистрант субдомена владеет закрытым ключом. Выполнение надлежащих проверок возлагается на регистраторов.

3.6 Регистратура удаляет из реестра DS-запись при получении от регистратора соответствующего запроса через EPP-интерфейс. Удаление всех DS-записей для субдомена деактивирует DNSSEC для этого домена. Только регистрант субдомена или сторона, официально уполномоченная представлять интересы регистранта, могут при помощи регистратора отправить запрос на удаление DS-записи для этого домена.

4. СРЕДСТВА УПРАВЛЕНИЯ И ЭКСПЛУАТАЦИОННЫЙ КОНТРОЛЬ

4.1 Регистратура располагает Центром обработки данных (ЦОД) на территории Казахстана. ЦОД включает в себя защищенные от несанкционированного доступа серверные стойки. Оснащен источниками бесперебойного питания и системами кондиционирования воздуха. Подключена централизованная система пожаротушения.

4.2 В офисе подготовленно помещение для проведения процедур. К объектам Регистратуры организован ограниченный доступ, который предоставляется только уполномоченному персоналу.

4.3 Критичные носители информации и резервные копии размещаются в сейфах, доступ к которым предоставляется только уполномоченному персоналу. Критичные документы уничтожаются способом измельчения. Электронные носители информации перед утилизацией подвергаются специальному форматированию для исключения возможности восстановления информации, ранее записанной на эти носители.

4.4 Для работы с закрытыми KSK и ZSK ключами 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. Сотрудник, привлеченный к работе с закрытыми KSK и ZSK ключами, не может одновременно совмещать роли крипто-офицера и крипто-оператора.

4.5 Для контроля над ходом выполнения ключевых процедур создана роль: Наблюдатель, которая состоит минимум из двух допущенных лиц. Наблюдатели обеспечивают прозрачность процесса и тщательное соблюдение процедур при выполнении критически важных операций с секретными частями ключей KSK и ZSK.

4.6 Выше описанный персонал является сотрудниками Регистратуры. Персонал, участвующий в процедурах, должен иметь опыт в области применения DNSSEC. Новые сотрудники, перед вступлением в вышеописанные роли, должны изучить внутреннюю документацию, описывающую реализацию DNSSEC. Они также должны принять участие в ключевых процедурах в качестве наблюдателей перед началом исполнения своих обязанностей.

4.7 Каждый факт доступа в специально отведенную зону работы с критичной информацией DNSSEC сохраняется в автоматизированной системе учета. Автоматизированной системы учета доступа регулярно просматриваются и анализируются. Периодичность анализа определяется политикой информационной безопасности Регистратуры.

4.8 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 Регистратура продолжит эксплуатацию этого ключа до завершения процедуры аварийной замены ключей.

5. ТЕХНИЧЕСКИЕ СРЕДСТВА БЕЗОПАСТНОСТИ

5.1 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.

5.2 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.

5.3 Открытый KSK распространяется среди сообщества средствами протокола DNS. Задание параметров и проверка качества ключевой информации осуществляется Регистратурой.