РЕГЛАМЕНТ

розширення DNSSEC

версія 1.1

24 березня 2025

1. Загальні положення

Цей документ (далі Регламент) описує основні принципи роботи розширення DNSSEC.

Для активації DNSSEC в домені необхідно розмістити DNSKEY запис в цьому домені та відповідний йому DS запис в Реєстрі домену вищого рівня. Опублікований DS запис встановлює ланцюжок довіри від домену вищого рівня до домену нижчого рівня.

2. Терміни та визначення

Реєстр - інформаційно-технічна система обробки даних, що містить інформацію про доменні імена, адреси мережі, Реєстраторів, Реєстрантів та контактних осіб Реєстрантів, та надає інтерфейс для роботи Реєстраторів згідно з прийнятим Регламентом.

Адміністратор публічного домену - особа, що здійснює заходи з адміністративного супроводу публічного домену та забезпечення його працездатності.

Оператор Реєстру – особа, що здійснює заходи з технічного супроводу Реєстру.

Реєстратор - особа, що надає Реєстранту послуги з реєстрації та супроводу доменного імені.

Реєстрант - особа, в інтересах якої здійснюється реєстрація та делегування приватного доменного імені.

Домен – символьне позначення областей в мережі Інтернет, що базується на ієрархічній структурі та дозволяє визначити доменні імена.

Доменне ім'я – символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі.

Сервер імен (NS) - спеціалізований програмно-апаратний комплекс в мережі Інтернет, що забезпечує взаємозв'язок доменних імен та IP адрес.

DNS - комп'ютерна розподілена система для отримання інформації про домени.

DNSSEC – є розширенням існуючої системи DNS, яка забезпечує аутентифікацію даних DNS та дозволяє перевіряти, що вміст відповіді DNS не було змінено.

DNSKEY – запис, що містить відкритий ключ підпису, який можна використовувати для перевірки підписів DNSSEC.

DS – запис підписувача делегування, що містить дані цифрового підпису

для доменного імені та використовується для ідентифікації ключа підпису DNSKEY. Містить тег ключа, алгоритм, тип дайджесту, дайджест

3. Інтерфейс роботи з розширенням DNSSEC.

Загальна специфікація розширення DNSSEC визначена в RFC5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).
В Реєстрі реалізований тип інтерфейсу DS Data Interface (згідно RFC5910).
Повна схема розширення DNSSEC: https://hostmaster.ua/epp/secDNS-1.1.xsd

Реєстр приймає DS записи від реєстраторів через EPP інтерфейс або через web-інтерфейс. DS запис має відповідати стандартам, зазначеним у розділі 11 даного Регламенту.

Інтерфейс роботи з розширенням DNSSEC дозволяє виконувати наступні операції:

- отримання інформації про DS записи делегованого домену
- створення домену з DS записом
- додавання DS запису до раніше делегованого домену
- видалення DS запису в делегованому домені
- видалення всіх DS записів в делегованому домені

Інтерфейс роботи з розширенням DNSSEC не передбачає роботу з ключами (Key Data Interface згідно RFC5910). Інтерфейс не підтримує опції maxSigLife та urgent.

Розширення DNSSEC вносить зміни у відповідь сервера на запит <domain:info> за умови використання DNSSEC у домені, щодо якого зроблено запит.

Розширення DNSSEC, за умови його використання, вносить зміни в команди клієнта <domain:create> та <domain:update>.

Розширення DNSSEC не вносить змін до команди <domain:transfer>, проте при спробі переведення доменного імені, підписаного DNSSEC, до реєстратора, який не підтримує це розширення, трансфер буде відхилено.

Зазначене розширення не впливає на роботу команд <domain:check>, <domain:delete>, <domain:renew> та <domain:restore>. У випадку виконання команди <domain:restore> щодо домену, який мав DS записи, вони відновлюються разом із доменом.

4. Отримання інформації про DS записи делегованого домену

У відповіді EPP-сервера на запит <domain:info> надається інформація про DS записи делегованого домену згідно RFC5910.

5. Створення домену з DS записом

В заявці на реєстрацію доменного імені може бути зазначений DS запис, що відповідає DNSKEY запису домену нижчого рівня. При реєстрації домену, на серверах імен, що вказані у запиті, вже повинен існувати відповідний домен та сформований DNSKEY запис, що відповідає надісланому в запиті DS запису. EPP-сервер виконує перевірку відповідності надісланого DS запису та запису DNSKEY домену нижчого рівня на всіх вказаних серверах імен. Домен делегується незалежно від результатів перевірки, але у випадку, якщо надісланий DS запис не відповідає DNSKEY запису домену нижчого рівня, крім повідомлення про реєстрацію домену, реєстратору надсилається попередження про відсутність відповідного DNSKEY запису в домені нижчого рівня.

Максимальна кількість записів DS для одного домену – шість записів. Якщо надіслана клієнтом команда призведе до створення більше 6 записів DS, то операція не виконується, а клієнту повертається повідомлення про помилку.

6. Додавання DS запису до раніше делегованого домену

Для додавання нового DS запису до раніше делегованого домену використовується команда <domain:update>. Після додавання DS запису виконується перевірка відповідності DS запису до DNSKEY запису домену нижчого рівня. Якщо DNSKEY запис не відповідає надісланому запису DS, то реєстратору надсилається попередження про відсутність відповідного DNSKEY запису в домені нижчого рівня.

В команді можна додатково зазначити DNSKEY запис домену нижчого рівня для надісланого DS запису. В такому випадку перевірка відповідності DS запису до DNSKEY запису домену нижчого рівня проводиться до виконання операції. У випадку не проходження перевірки, операція додавання DS запису не виконується, а клієнту повертається повідомлення про помилку.

Максимальна кількість записів DS для одного домену – шість записів. Якщо надіслана клієнтом команда призведе до створення більше 6 записів DS, то операція не виконується, а клієнту повертається повідомлення про помилку.

7. Зміна DS запису в раніше делегованому домені

Зміну запису в раніше делегованому домені можна провести за допомогою послідовності операцій: видалення DS запису та додавання нового DS запису. Також цю дію можна виконати за допомогою однієї операції <domain:update>. В такому випадку в розширенні необхідно зазначити команду видалення певних або усіх DS записів, після цього в межах того ж розширення додається один або декілька нових DS записів. В результаті внесення змін в DS записи, максимальна кількість DS записів не повинна перевищувати шести. Якщо надіслана клієнтом команда призведе до створення більше 6 записів DS,

то операція не виконується, а клієнту повертається повідомлення про помилку. Після проведення операції зміни DS записів виконується перевірка відповідності надісланого DS запису та запису DNSKEY домену нижчого рівня.

В команді можна додатково зазначити DNSKEY запис домену нижчого рівня для надісланого DS запису. В такому випадку перевірка відповідності DS запису до DNSKEY запису домену нижчого рівня проводиться до виконання операції. У випадку не проходження перевірки, операція додавання DS запису не виконується, а клієнту повертається повідомлення про помилку.

8. Зміна NS записів у домені з існуючим DS записом

При зміні NS записів виконується перевірка наявності на нових серверах імен відповідного(их) DNSKEY запису(ів). У випадку його відсутності, зміни вносяться, а реєстратору надсилається попередження про відсутність відповідного DNSKEY запису в домені нижчого рівня.

9. Особливості команди transfer для домену з DS записом

У випадку, якщо домен з існуючим DS записом передається від реєстратора, що підтримує роботу з розширенням DNSSEC, до реєстратора, що не підтримує роботу з таким розширенням, спочатку поточний Реєстратор має видалити усі DS записи в домені вищого рівня, а потім новий реєстратор має подати запит на трансфер домену. Якщо на момент надходження запиту на трансфер від реєстратора, який не підтримує розширення DNSSEC, у домені існують DS записи, то такий запит відхиляється з повідомленням про помилку.

10. Видалення DS запису в делегованому домені

При отриманні від реєстратора запиту на видалення DS запису, цей запис видаляється з домену вищого рівня.

Видалення DS запису в делегованому домені виконується за допомогою розширення в команді <domain:update> згідно RFC5910. Записи DS можуть бути видалені вибірково або всі одночасно.

Видалення всіх DS записів (без додавання нових) призводить до деактивації DNSSEC для цього домену.

11. Особливості операцій з DS записом для web-інтерфейсу

При роботі через web-інтерфейс доступні операції додавання DS запису в раніше делегованому домені та видалення DS запису. Перед виконанням операції додавання DS запис додатково перевіряється на відповідність DNSKEY запису на серверах імен домену нижчого рівня. У випадку невідповідності – операція не виконується, а клієнту повертається

повідомлення про помилку.

12. Стандарти, що підтримує реєстр

Номери алгоритмів, що стандартизовані для використання у DNSSEC, наведені на сайті IANA за наступною адресою:
https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml
Реєстр приймає DS записи, якщо відповідний DNSKEY створений за алгоритмами:

- 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
- 16 Ed448

Номери алгоритмів, що стандартизовані для DS записів наведені на сайті IANA за наступною адресою:
https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml
Реєстр приймає DS записи створені за алгоритмами:

- 2 SHA-256
- 4 SHA-384

13. Порядок внесення змін до Регламенту

У разі необхідності Оператор Реєстру може вносити зміни до Регламенту розширення DNSSEC. Зміни до Регламенту публікуються на сайті Оператора Реєстру для ознайомлення одночасно з відповідним повідомленням Адміністраторів публічних доменів та Реєстраторів. Зміни до Регламенту можуть вноситися за 30 днів до введення змін в дію.

У разі нагальної необхідності, внесення змін до Регламенту може здійснюватися одночасно з їх публікацією на сайті Оператора Реєстру одночасно з відповідним повідомленням Адміністраторів публічних доменів та Реєстраторів. Під поняттям нагальної необхідності розуміються умови, за яких подальше надання послуг Оператором Реєстру неможливе без внесення відповідних змін.