The DNSSEC extension REGULATIONS

version 1.1

March 24, 2025

1. General Provisions

This document (the “Regulations”) describes main principles of the DNSSEC extension usage.

To activate DNSSEC for a domain the DNSKEY RR must be included in this domain and correspondent DS RR must be included in the parent domain. The publishing DS RR sets the chain of trust from the parent domain to the child domain.

2. Terms and Definitions

Registry - an information technology system for data processing that contains information regarding domain names, network addresses, Registrars, Registrants and Registrants’ contact persons and provides an interface for the operation of Registrars in accordance with the established Policy.

Public Domain Administrator - an entity that carries out administrative maintenance and ensures a public domain operability.

Registry Operator - an entity that carries out technical maintenance of the Registry.

Registrar - an entity that provides Registrant with services of registration and support of a domain name.

Registrant - a person/entity for whose benefit registration and delegation of a private domain name are carried out.

Domain - a character representation of areas on the Internet which is based on a hierarchic structure and is used to designate domain names.

Domain name - a character representation that is used for addressing hosts of the Internet and network resources located on such hosts (web-sites, e-mail servers, network services) in a human-friendly form.

Name Server (NS) - a dedicated software and hardware facility on the Internet that maps domain names and IP addresses.

DNS - a distributed computer system for obtaining information on domains.

DNSSEC - an extension of the existing DNS system that provides DNS data authentication and enables to check the consistency of DNS reply.

DNSKEY - a resource record (RR) that contains the open key of signature and can be used to check the DNSSEC signature.

DS - a Delegation Signer record that contains the digital signature information for the domain name and is used to identify the DNSKEY signing key.

3. The interface to the DNSSEC extension.

The common specification of the DNSSEC extension is defined in RFC5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP).

The “DS Data Interface” version is implemented on the EPP server of the

Registry (according to RFC5910). The full scheme of the DNSSEC extension is located at https://hostmaster.ua/epp/secDNS-1.1.xsd .

The Registry accepts DS RRs from registrars via the EPP interface or via the web interface. DS RRs must comply with the standards specified in Chapter 11 of this Regulation.

The DNSSEC extension interface allows following operations:

- receiving information about DS records of the delegated domain
- creation of a domain with DS record
- addition the DS record to the previously delegated domain
- deleting DS record in the delegated domain
- deleting all DS records in the delegated domain

The DNSSEC extension interface does not provide operations with keys ("Key Data Interface" according to RFC5910). The interface does not support "maxSigLife" and "urgent" options.

The DNSSEC extension changes the server reply to the <domain:info> request in case of using the DNSSEC in the requested domain.

The DNSSEC extension implies the changes to the <domain:create> and <domain:update> requests in case of using DNSSEC.

The extension does not change the <domain:transfer> command. But if registrant tries to transfer domain with DNSSEC enabled to a registrar that does not support the DNSSEC extension, transfer will be refused.

The extension does not affect on the <domain:check>, <domain:delete>, <domain:renew> and <domain:restore> commands. If the <domain:restore> command is applied to the domain that has DS records, the domain will be restored with the DS records.

4. Receiving information about DS records of the delegated domain

The information about the DS RR[s] is provided in the server response to the <domain:info> request according to the RFC5910.

5. Creation of the domain with DS RR

The creation domain request may contain the DS RR corresponding to the DNSKEY RR of the child domain. While the domain is registering the name servers that specified in the request must contain the domain and the DNSKEY RR corresponding to the DS RR in request. The EPP server checks the correspondence between the received DS RR and DNSKEY RR on all specified name servers. The domain is delegated in any case but if the received DS RR does not correspond to the DNSKEY RR of the child domain the warning about missing the correspondent DNSKEY RR in the child domain is sent to the registrar.

The maximum amount of the DS RRs for a domain are six records. If the client command resultes in more than 6 DS records for the domain, the operation is refused and the error message is sent to client.

6. Addition the DS record to the previously delegated domain

To add a new DS RR to the previously delegated domain the <domain:update> command is used. After addition of the new record the check of correspondence between the DS RR and the DNSKEY RR in the child domain is performed. If the received DS RR does not correspond to the DNSKEY RR of the child domain the warning about missing the correspondent DNSKEY RR in the child domain is sent to the registrar.

Additionally the command may contain the DNSKEY RR of the child domain corresponding to the DS RR in the request. In this case the correspondence check between received DS and DNSKEY RRs is performed before the operation. If the check fails the DS RR does not add to the domain and the error message is sent to the client.

The maximum amount of the DS RRs for a domain are six records. If the client command resultes in more than 6 DS records for the domain, the operation is refused and the error message is sent to client.

7. The DS record changing for previously delegated domain

The DS record changing for previously delegated domain is made by the sequence of commands: the DS RR removing followed by adding a new DS RR. Also this can be done by one <domain:update> command. In this case the extension should contain the remove command (with specific DS RR or all DS RRs) followed by the add command with the new DS RR[s] in the same extension. The resulting number of the DS RRs must not exceed 6. If the client command resultes in more than 6 DS records for the domain, the operation is refused and the error message is sent to client. After changing of the DS RRs the check of correspondence between the parent DS RR and the child DNSKEY RR is performed.

Additionally the command may contain the DNSKEY RR of the child domain corresponding to the DS RR in the request. In this case the correspondence check between received DS and DNSKEY RRs is performed before the operation. If the check fails the DS RR does not add to the domain and the error message is sent to the client.

8. The NS record changing for the domain with a DS record

While the NS RR is changing the server checks that the correspondent DNSKEY RR on the new name servers exists. If there is no the correspondent RR the changes is performed the warning about missing the correspondent DNSKEY RR in

the child domain is sent to the registrar.

9. Features of the transfer command for the domain with a DS record

In case when the registrar that provides DNSSEC transfers the domain with DS record to another registrar that does not provide DNSSEC initially the current registrar must delete all DS records for this domain from the parent zone and then the new registrar may send the transfer request. Otherwise the transfer request will be refused with the error message.

10. The DS record deletion

The DS RR is deleted from the parent domain after the request from the registrar is received.

The DS record deletion is accomplished by the extension in the <domain:update> command according to the RFC5910. Sprcified or all records can be deleted.

The deletion of all DS RRs (without addition of new DS RR) causes the DNSSEC deactivation for the domain.

11. Features of operations with DS record for the web interface

If registrar uses the web interface, only the operations of adding a DS RR to a previously delegated domain and deleting a DS RR are available. Before performing the operation of adding a DS RR, additional check of correspondence between the DS RR and the DNSKEY RR on domain name servers of the child domain is performed. In case of non-compliance, the operation is not performed and the error message is returned.

12. Standards supported by the Registry

The algorithm numbers that are standardized to use for the DNSSEC are listed on the IANA site by the following link:
https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

The Registry accepts the DS RRs if the corresponding DNSKEY is created by the algorithms:

- 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

The algorithm numbers that are standardized for the digest of DS records are listed on the IANA site by the following link:
https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml

The Registry accepts the DS records that is created by the algorithms:

2 SHA-256
4 SHA-384

13. The procedure for changing of the Regulations

If necessary, the Registry Operator may make changes to the Regulations. The changes are published on the site of the Registry Operator simultaneously with notification the Public domains administrators and Registrars. The Regulations changes should be published 30 days before the implementing of the changes.

In case of urgency the Regulations changes may be implemented simultaneously with the Regulations changes publishing and notification of the Public domains administrators and Registrars. The term of “urgency” means the conditions under which the Registry can not provide further service without the Regulations changing.