.SK Domain Registry

Automated DNSSEC activation through a CDS record

(technical implementation)

From 1st January 2020 an automated DNSSEC activation is being introduced, on the basis of the data on the NS servers (so called CDS scanning). The CDS scanning service is an alternative to entering of DS records (records for DNSSEC) into the Central .sk domain registry through the EPP interface or through the registrar console

This system scans the zones of all .sk domains in an automated way and looks for the CDS records in them.

The CDS scanning service in the .sk domain works in the following way:

- If at least one or more CSD records is found for a domain which in the Central domain registry does not have an existing DS record (ie. does not have DNSSEC activated), it is saved and during the following 72 hours its stability is being periodically watched (it must not stop existing or be changed). After the successful passing of this period it is entered to the domain as a valid DS record for DNSSEC.
- There is a similar principle also in the case the domain already has in the Central domain registry DNSSEC activated (ie. it has one or more DS records) and a different record is identified on the name server. In this case all existing records are overwritten with the newly found.
- In case that the existing record in the register and a CDS record found match, no action is performed.
- For removing the existing DS records also a so called „kill record“, ie. a special CDS record for complete deletion of records for DNSSEC. Here, in the same way like earlier stated a rule about watching the stability of the CDS record is being applied.

After a successful completion of each from the earlier mentioned variants (except for not performing any action when a match is found) a notification email will be sent to the technical contact of the domain.

Note: For using this service it is necessary to publish in the zone of a given domain a valid (or more) CDS record by the administrator of a name server.

By this service SK-NIC implements a CDS scanning in accordance with the technical specification RFC 8078 (see https://tools.ietf.org/html/rfc8078, which is available in English).

Except for basic functioning we add also several other rules, which apply for this system in the .sk domain:

- CDS records have to be valid, in order to be used by the system - algorithm and the type of the digest have to contain valid value from the IANA registers, the digest have to have a correct length for the given algorithm and so on,
- if the CDS record is stable and valid for the period of 72 hours, the records in the Central domain registry are accordingly updated - whatever existing DS records will be replaced by new records derived from the DS record,
- for using the “kill record“ it is necessary to set up the data in the CDS record to zero values - subsequently all existing DS records will be removed from the domain in the register, *example.tld. 38400 IN CDS 0 0 0 0*
- any data recorded in the DS records of the domain via EPP or registrar console will be, in the case of existence of a CDS record for the domain and in the case of being different from the records in the register replaced by the data in the CDS records.