DNSSEC

By default, DNS entries in domain names are not encrypted during a simple query, so they may be denied access to or change the response. DNSSEC uses a cryptographic procedure to sign the domain names zone to give you a credible response that a third party can not access, can not modify it.

> Using the DNSSEC settings incorrectly for the domain name may result in the domain name being inoperable.

WHAT IS THE DNSSEC?

DNSSEC stands for the abbreviation of Domain Name System Security Extensions. Essentially, an extension of DNS that is intended to improve security vulnerabilities and vulnerabilities in the creation of DNS.

OPERATION OF DNSSEC

DNSSEC protects against data forgery by adding digital signatures to DNS records during queries. When querying domain names signed with DNSSEC, the digital signature stored in the name server set at the domain name is authenticated to ensure that the data stored in the zone during the period between the query and the response has not changed. Using DNSSEC, you can ensure that you actually query the web page that the visitor has typed into the browser’s address bar.

DNSSEC uses the public or secret key authentication. Public keys can be digitized in DNS as RRSIG type, these records can be retrieved the same way as any other type of record. The secret keys belonging to the domain names are stored by the name server and, during a query, they also send back the signed data with the secret key to the interviewee, who can unlock it using the public key. In case a third party interferes with the query and modifies the data sent in the response, it will not be possible to reverse it with the public key when decrypting it, but the recipient will know that it is fake.

DNSSEC does not encrypt data – in the absence of algorithms – but only ensures that the data you are querying is genuine. As a result, DNSSEC can not be used, for example, to prevent DDoS attack.

MANAGE DNSSEC KEYS

Naturally, like any cryptographic procedure, the private and open keys used for DNSSEC are also known and can be broken up over time. In order to make it easier to know the keys used and then

to crack it, an additional key has been introduced. For DNSSEC, the KSK and ZSK keys are used. The KSK keys are relatively rarely changed, but the ZSK keys often, ensuring that a possible break is much more time consuming, and this makes it more difficult.

Key type	Key description
KSK	Use this to sign the zone signing key
ZSK	which means that each record is signed

TROUBLESHOOTING DNSSEC

Use the following pages to check the correct setting for DNSSEC:

- Verisign DNSSEC Debugger
- DNSViz

Revision #1
Created 20 October 2023 09:59:18 by Judit Pásztor
Updated 20 October 2023 10:05:46 by Judit Pásztor