FREQUENTLY ASKED QUESTIONS ABOUT DNSSEC

What is DNS?

Equipment or machines are identified on the Internet through IP addresses or names which must be unique in order to function correctly. The DNS system (Domain Name System) is responsible for establishing correspondence between names (www.example.es) and IP addresses (192.168.2.15).

The original DNS does not include security measures, something that became evident in 2008 when Dan Kaminsky published the document "*Multiple DNS implementations vulnerable to cache poisoning*" (http://www.kb.cert.org/vuls/id/800113). From that moment, organisations like ICANN began promoting the mass implementation of **DNSSEC**, the specifications of which were established in 1995.

What is DNSSEC?

DNSSEC is a set of security extensions that uses asymmetric encoding developed for the DNS system. It provides the following benefits:

- It authenticates the origin of the data on a DNS server
- It maintains the integrity of data between DNS servers
- Authenticated denial of existence

What is DNSSEC not?

- DNSSEC is not a new protocol to replace DNS.
- It does not protect against denial of service attacks.
- It does not give confidentiality to DNS data: the responses provided by DNSSEC are authenticated but are not encoded.

How are the data authenticated and how is their integrity maintained?

DNSSEC uses public key asymmetric cryptography which means that the authorship of anything signed with one key can be checked against the other. There will be one public key for each domain, which will be distributed (DS and Trust-Anchor Records) and published using DNS (DNSKEY Record) in the secure domain zone. The records are authenticated by checking the digital signatures against the public keys distributed. A more detailed explanation of how digital signatures work can be found at http://www.cert.fnmt.es/index.php?cha=cit&sec=3&page=219&lang=es.

In order for the system to be reliable, a private key is required that needs to be kept safely and securely because, if it is compromised, an attacker could use it to forge the domain data.

What are the KSK and ZSK keys?

KSK stands for *Key Signing Key (*a long term key) and **ZSK** stands for *Zone Signing Keys* (a short term key).

DNSSEC blocks potential threats using a short term key (ZSK) to routinely calculate the signatures in the DNS records and a long term key (KSK) to calculate a signature in the ZSK to permit validation. The ZSK key is frequently changed or renewed to make it harder for the attacker to find it, while the longer KSK key is changed after much longer periods of time (the current best practices set this period at about a year).

The two keys KSK and ZSK are stored in the zone. The ZKS key signs all the records in the zone and the KSK signs all the keys in the zone. To be able to resolve the issue properly both keys are necessary.

What are the security extensions?

The security extensions consist of a new set of records and modifications to the current DNS protocol.

The new records are:

- DNSKEY: DNS Public Key
- RRSIG: Resource Record Signature.
- DS (Delegation Signer): Hash of a DNSKEY
- NSEC/NSEC3 (Next Secure): Used to deny existence
- NSEC3PARAM: Configuration parameters of NSEC3

With regard to modifications to the protocol, these include new calls and record requests for each DNS query performed, making it possible to authenticate the domains.

What is a chain of trust?

The chain of trust is a list of **DNSKEY** records (Public keys) and DS (Delegation Signer) records that enable chains of trust to be created between domains. This makes it possible to validate any domain within that chain using a single public key. To do this, the DS record, which is a hash (a function or method for generating codes or keys that unequivocally represent a document, record or file) generated from a DNSKEY record, are published on the parent domain. For example, if we have the domain red.es with its associated key, and we generate the DS record of this and publish it on the .es domain, we can authenticate the red.es domain using the public key for the .es domain.

As an end user, what do I need in order to protect myself using DNSSEC?

To use the record validation in DNSSEC, you need equipment that is compatible with this system and you need to sign up to a service with a DNS provider that has a DNS resource server where the validation is activated.

This DNS resource server must contain the public keys of the domains you wish to validate. It is also possible to use one of the resource servers with DNSSEC that certain organisations such as OARC's (https://www.dns-oarc.net) make available to everyone.

What happens if you consult a DNS record and the DNSSEC validation fails?

When a resource server that has the **DNSSEC** validation activated receives a manipulated or false response from the DNS, the client who requested that name resolution will not obtain any records and an error code will be returned (RCODE) SERVFAIL which means that an error has occurred while responding to the query.

As the owner of a domain, what steps do I need to take to make the domain use DNSSEC?

To secure the domain with DNSSEC the authoritative DNS servers available to you need to publish the signed domain. If the DNS servers are BIND you can use OpenDNSSEC (http://www.opendnssec.org), which uses an unsigned zone file (with BIND format) to generate its signed equivalent (with BIND format); or the tools that BIND provides such as dnssec-signzone. For more information go to http://www.nlnetlabs.nl/publications/dnssec_howto/.

What are the main problems we might come across in a DNSSEC deployment?

The main issues to be resolved are:

- The network hardware must support **EDNS0** (largest extension mechanism for DNS).
- Increase in hardware resources (The increase in resources will depend on the volume of information to be managed):
    - the resource servers will require more bandwidth and CPU
    - the authoritative servers will need more memory, bandwidth and CPU
- At an operational level, there is an additional workload as the implementation of DNSSEC brings with it a series of procedures such as: the renewal of keys and monitoring of the signature system.
- It is recommended that you understand in detail how DNSSEC works and that you have some knowledge of cryptography. A fault or an error could render the whole domain inaccessible.

Where can I find more information on DNSSEC?

You will find technical information in the **RFCs** (Internet standard) of the Internet Engineering Task Force:

- RFC 2535 Domain Name System Security Extensions
- RFC 3833 A Threat Analysis of the Domain Name System
- RFC 4033 DNS Security Introduction and Requirements (*DNSSEC-bis*)
- RFC 4034 Resource Records for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4035 Protocol Modifications for the DNS Security Extensions (*DNSSEC-bis*)
- RFC 4398 Storing Certificates in the Domain Name System (DNS)
- RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 4641 DNSSEC Operational Practices