

DNSSEC Frequently Asked Questions

1. What are DNS Security Extensions (DNSSEC)?

DNSSEC is an addition to the Domain Name System (DNS) protocols, which provide origin authentication of DNS data, data integrity and authenticated denial of existence. DNSSEC is designed to add security to the DNS by protecting the Internet from certain types of attacks, such as any data modification attack (e.g. cache poisoning).

2. What does DNSSEC protect against?

DNSSEC is not a solution for all cyber security threats. It is designed to protect Internet resolvers (clients) from forged DNS data, such as that created by DNS cache poisoning. Currently, a DNS resolver sends a query out to the Internet and then accepts the first response it receives, without question. If a malicious system were to send back an incorrect response, the resolver would use this address until its cache expired. This is bad enough if it's a single user's computer that gets this bad data, it's much worse if it's another name server that answers queries for an ISP – affecting thousands of users.

3. How does DNSSEC protect against this attack?

DNSSEC, when deployed and utilized, ensures that the answer you receive came from a trusted name server by using public key cryptography to digitally sign DNS data when it comes into the system and then validated at its destination. In practice, this will come into effect when a registrant registers a domain name on the Internet with a registrar that supports DNSSEC, they will also then be able to have the domain name secured via DNSSEC. By sending in additional information to their registrar, domain name holders can “sign” a domain name. By checking the digital signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server.

4. What does it mean to say that the Root Zone will be “signed”?

Zone signing is the process of cryptographically signing the authoritative data within a zone file. This process adds new records to the zone, which allows verification of the origin authenticity and integrity of data. The zone-signing function for the root zone is being carried out by VeriSign. Key maintenance (key generation, storage, and rollover) and publishing the public portion of the root key (trust anchor) are separate but equally-necessary functions, and is being carried out by ICANN.

5. Can Top-Level Domain (TLD)s benefit from DNSSEC in the Root Zone?

Yes! TLD Managers can now submit their trust anchors (references to the cryptographic keys used to secure their own zones) through the normal IANA root zone management process. The presence of TLD trust anchors in the root zone simplifies key management operations for TLDs, and allows end users to benefit from DNSSEC without having to specify any special configuration for each signed TLD.

6. What is a key?

A key pair contains two digital keys — a private key (held only by the organization responsible for signing data) and a public key (distributed to the public). ICANN and VeriSign each use a private / public key pair; the key pair used by VeriSign (the "zone-signing key", or ZSK) is used to sign the zone, and the key pair used by ICANN (the "key-signing key", or KSK) is used to provide a cryptographic chain of trust between validators and the signed root zone records. End users' validators (or the validators at their ISPs) use the KSK public key to verify that signatures are correct and that the answers they receive in response to DNS queries are authentic.

7. Where can I find more information about DNSSEC?

For DNSSEC information specific to the root zone, see <http://www.root-dnssec.org>. For DNSSEC technical information broader than the root, the [dnssec.net](http://www.dnssec.net) <http://www.dnssec.net> and [dnssec-deployment.org](http://www.dnssec-deployment.org) <http://www.dnssec-deployment.org> web sites are both excellent resources to learn more about DNSSEC. You may also access visit the .ORG Advantage section of our website to see our DNSSEC Information Data Sheet http://pir.org/index.php?db=content/Website&tbl=ORG_Advantage&id=2.1.