OpenDNSSEC

helping to secure the Internet

Open source solution for a fast and easy DNSSEC deployment

OpenDNSSEC is an open source, easily deployable solution for implementing DNSSEC. It is a tool intended to drive adoption of Domain Name System Security Extensions (DNSSEC) to further enhance the security of domain names and the Internet.

What is DNSSEC?

Many Internet protocols hinge on the Domain Name System (DNS) but the data in DNS caches has been proven to be vulnerable to attack.

DNSSEC, which stands for DNS Security Extensions provides DNS with authentication for responses from DNS servers and thereby aims to prevent DNS spoofing, which is a common technique used by hackers.

The added authenticity in DNSSEC makes sure that such attacks have no effect if zones are verified and secured. Whilst easy-to-deploy software exists to cover verification (Unbound or properly configured Bind9) there was no open source solution that handled all aspects of securing zone files using DNSSEC.

As a result, the OpenDNSSEC project was formed to create such a solution and it is now available for use.

What is OpenDNSSEC?

OpenDNSSEC is a tool that simplifies the process of signing one or more zones with DNSSEC. OpenDNSSEC handles the entire process from an unsigned zone to a signed zone automatically, including secure key management and timing issues. With OpenDNSSEC, fewer manual operations are needed by the operator.

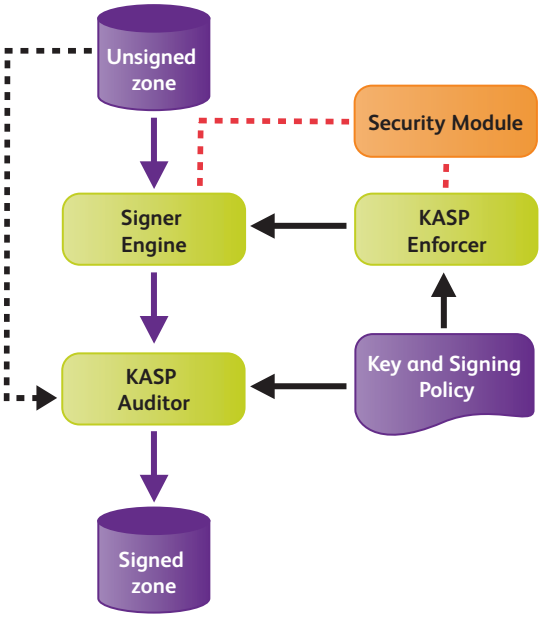
OpenDNSSEC makes sure that all the steps in the signing process are done in the correct order and at the same time, making sure that nothing breaks. The issue of handling the private keys associated with DNSSEC signing has been addressed by keeping the keys in so-called HSMs (Hardware Security Modules) so that they cannot be leaked to an unauthorised third party.

OpenDNSSEC removes the manual aspect of deploying DNSSEC, lowering the threshold for Internet Service Providers, hosting companies and Name Server Operators to deploy secure DNS. This will significantly increase the number of DNSSEC users.

What does OpenDNSSEC do?

OpenDNSSEC takes in unsigned zones, adds the signatures and other records for DNSSEC and passes it to the authoritative name servers for that zone.

DNS is complicated, as is digital signing, so it is no surprise that combining the two in DNSSEC is complex as well. The idea of OpenDNSSEC is to handle these complexities so that the administrator does not have to worry about them.



Who should use OpenDNSSEC?

OpenDNSSEC works with all different versions of the Unix operating systems and is suitable both for those who will need to sign a few very large zones (for example Top Level Domains) and for those who are responsible for a large number of smaller zones (for example Internet Service Providers and Registrars).

About the OpenDNSSEC Project

The OpenDNSSEC Project is a collaboration between .SE (The Internet Infrastructure Foundation), NLNetLabs, Nominet, Kirei, SURFnet, SIDN and John Dickinson.

For further information about the OpenDNSSEC technology or to download the software, go to our web site at: www.opendnssec.org

Key features of OpenDNSSEC

Overview

- Single piece of software for signing DNS zones that can be seamlessly integrated into an existing system without needing to overhaul the entire existing infrastructure.
- Can be configured to sign zone files or to sign zones transferred in via AXFR.
- Fully automatic – once set up, no manual intervention is needed.
- Open source software supplied with a licence so suppliers of commercial products can use the open source code in them whilst retaining the IPR of their own software.

Scalable

- Able to sign zones containing anything from a few records up to millions of records.
- Single instance of OpenDNSSEC can be configured to sign one or many zones.

Flexible

- Able to define zone signing policy (length of key, key lifetime, signature interval etc.); can set the system up for anything between one policy to cover all zones to one policy per zone.

Secure

- OpenDNSSEC stores sensitive cryptographic data in an HSM, communicating with it using the industry-standard PKCS#11 interface.
- SoftHSM – a software emulation of an HSM – is available if use of an HSM is not necessary, or to set up a DNSSEC testbed before purchasing a real HSM.
- Facility to check whether HSMs are compatible with OpenDNSSEC.
- Includes an auditing function that compares the incoming unsigned zone with the outgoing signed zone, so you can check that no zone data has been lost and that the zone signatures are correct.