TRAFICOM

Finnish Transport and Communications Agency

DNSSEC

Ensuring a secure internet

Route secured by

DNSSEC

What is DNSSEC?

DNSSEC is an extension of the Domain Name System (DNS), that ensures the authenticity and integrity of the data in DNS replies. Technical measures have been implemented which mean that the computer submitting a query (e.g. an internet browser) can now see whether the reply provided for an internet address in the DNS actually comes from the server that is registered with us as being the competent server. At the same time, DNSSEC ensures that this response is not modified as it is transported through the internet. Expressed in simple terms: DNSSEC is a type of insurance which guarantees that people using the internet are only shown the actual website that they intended to call up. This guarantee is achieved through cryptographic signatures. No information is encrypted in DNSSEC. All the data remains publicly accessible, as with the existing DNS.

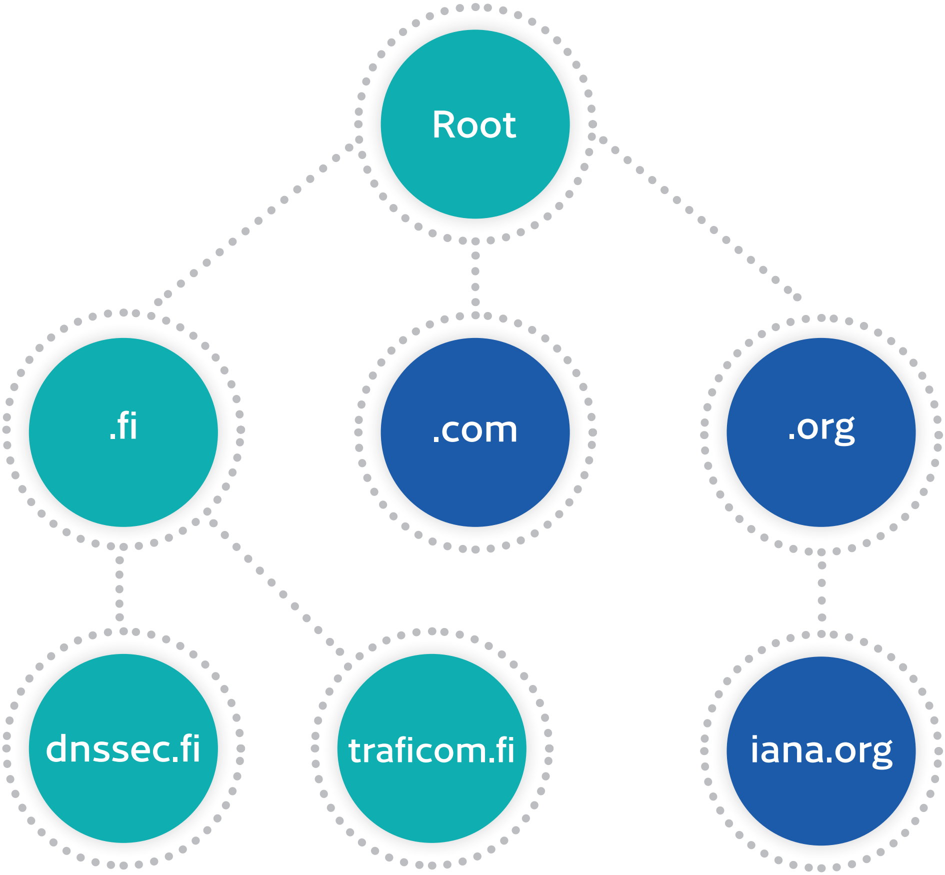
Why is DNSSEC necessary?

Observant readers will doubtless have noticed that internet browsers already incorporate a technology designed to ensure that the user arrives at the ‘correct’ website. Websites of this type are generally encrypted with SSL (Secure Sockets Layer) and are indicated in the browser by means of a key symbol.

DNSSEC was not developed in order to replace SSL encryptation. On the contrary, DNSSEC has been introduced to supplement SSL and to prevent a situation where the user lands at an incorrect server even before the connection has been secured by SSL.

How does the DNS (Domain Name System) work?

The internet as we know it today is based on the global Domain Name System. We will briefly outline the way this system works below. The DNS can be pictured as a globally distributed telephone directory, which allocates the globally unique domain names (www.dnssec.fi) to the globally unique internet addresses (87.239.124.120). The internet addresses, or domain names, are used simply because they are easier to write. To make sure that the different queries do not all land up on the same server, the DNS is designed with a hierarchical structure. The name space is divided up into so-called zones. In the case of www.dnssec.fi, the top level of the hierarchy (root), would be followed by the servers for Finland ('fi'), and then the DNSSEC servers ('dnssec.fi'). The competences of the individual zones are divided up (delegated) within the hierarchy. If you wish to call up the www.dnssec.fi website from your computer, your internet provider's name server will poll all the levels of the hierarchy, one after the other. Each level that does not know the answer to the target address will send notification to the next-lower level. The server on the lowest level of the hierarchy will then finally be able to provide the answer for the address.

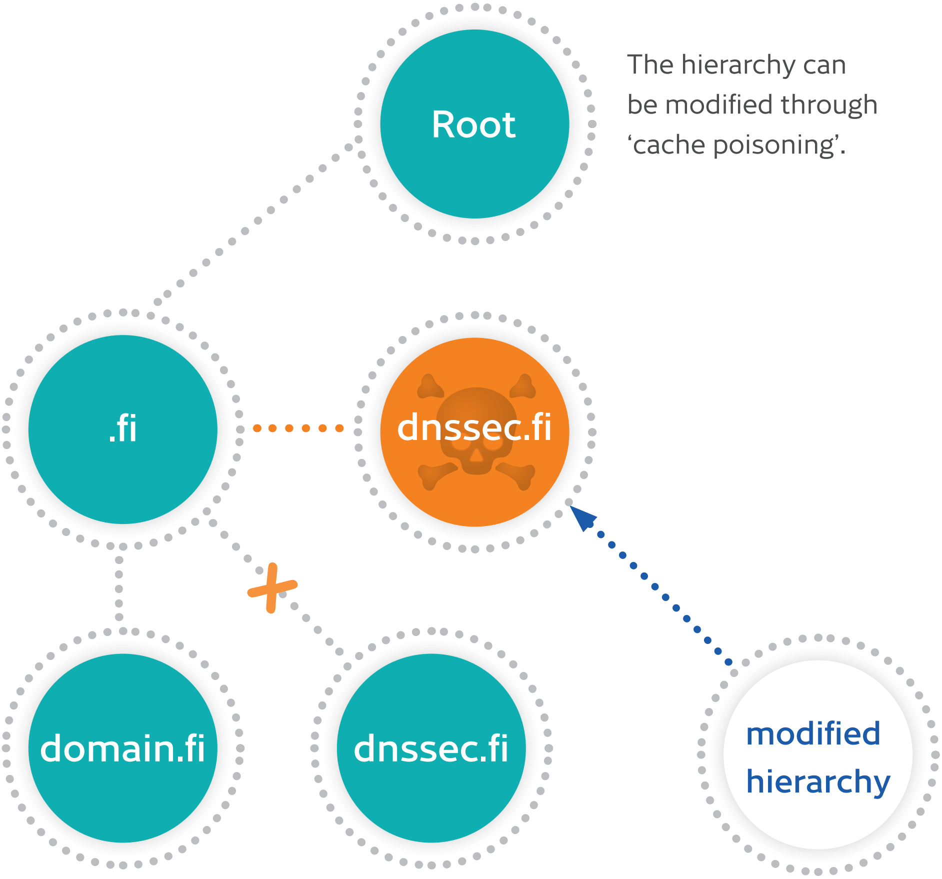


The Domain Name System (DNS) has a hierarchical structure. The name servers for '.fi' automatically forward requests for domain names ending in .fi (e.g. dnssec.fi) to the correct address.

What is the purpose of DNSSEC?

Imagine a situation where someone succeeds in changing entries in the telephone directory. You thus look up the number for the Traficom domain names helpdesk and find the wrong number listed there. Would you have had any means of recognising this non-permitted abuse? Not really. Such a scenario would be possible in the internet if an attacker were to change the hierarchy described above.
If an attacker succeeds, for instance, in smuggling incorrect datapalvelimelle. into your provider's server (cache poisoning), then you would land at a different website when you called up www.dnssec.fi. It's best not to try and imagine what could happen if the forged website was your bank. Or if you were to send your company's latest strategy to a Partner's 'forged' mail server.

Since the internet is used for a whole range of different purposes today, hacker attacks can have far-reaching implications. DNSSEC provides fundamental protection against attacks of this type – and not only when websites are called up. DNSSEC cannot protect against phishing attacks on a general basis. It does, however, provide efficient protection against attacks on the DNS. This is what is important, since most phishing attacks can be recognised and prevented by alert internet users. Even experts, however, can scarcely detect attacks on the DNS.



The hierarchy can be modified through ‘cache poisoning’.

DNSSEC in detail

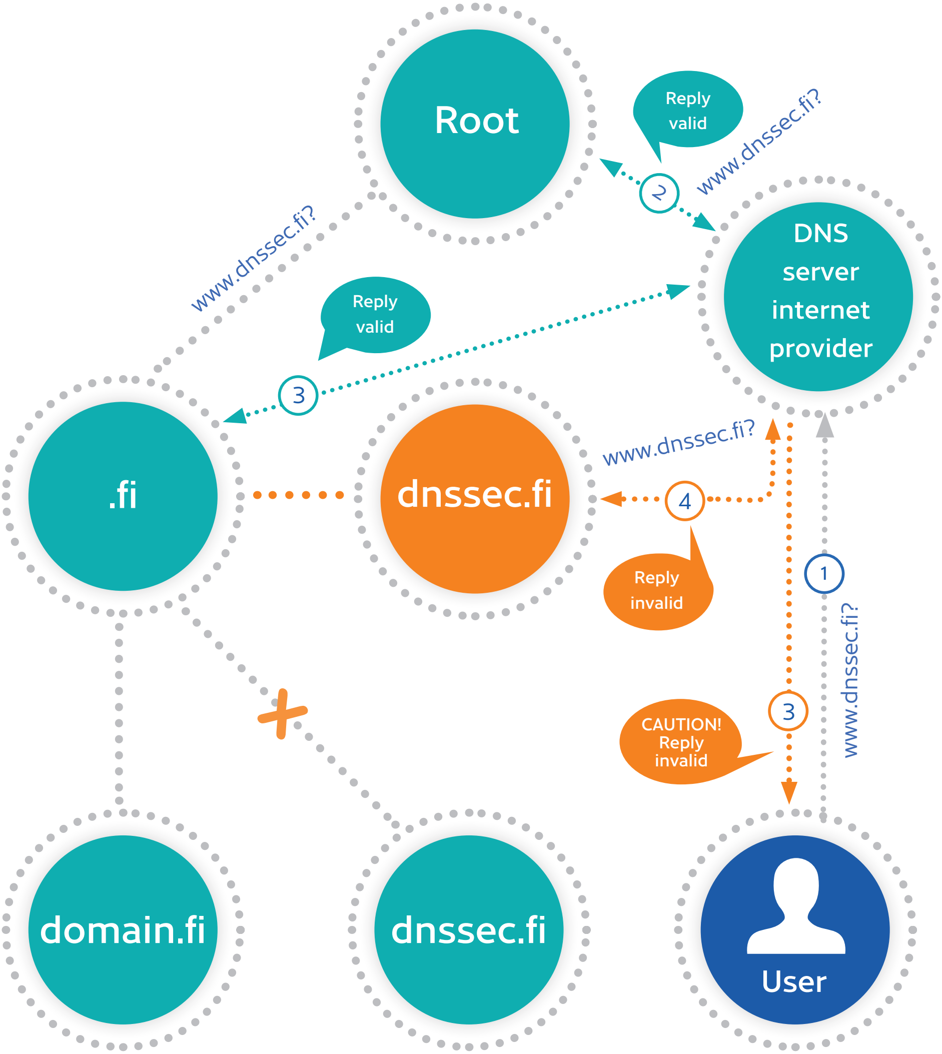
As already mentioned, DNSSEC is based on cryptographic signatures with which the current DNS entries are signed. Anyone who is responsible (authoritative) for a domain name in the internet can protect their information by means of DNSSEC. All the information for which a service provider holds responsibility is signed with this service provider's private key, and the signatures are written in the DNS (RRSIG record).

An example with DNSSEC:

Your internet provider's name server once again follows the familiar hierarchy in order to resolve a query. This time, however, it can check on the basis of the signatures received whether the origin of the answers is correct and whether an answer has been modified en route. The name server will only answer if all the information is correct.ovat oikein.

How is it possible for all these signatures to be checked?

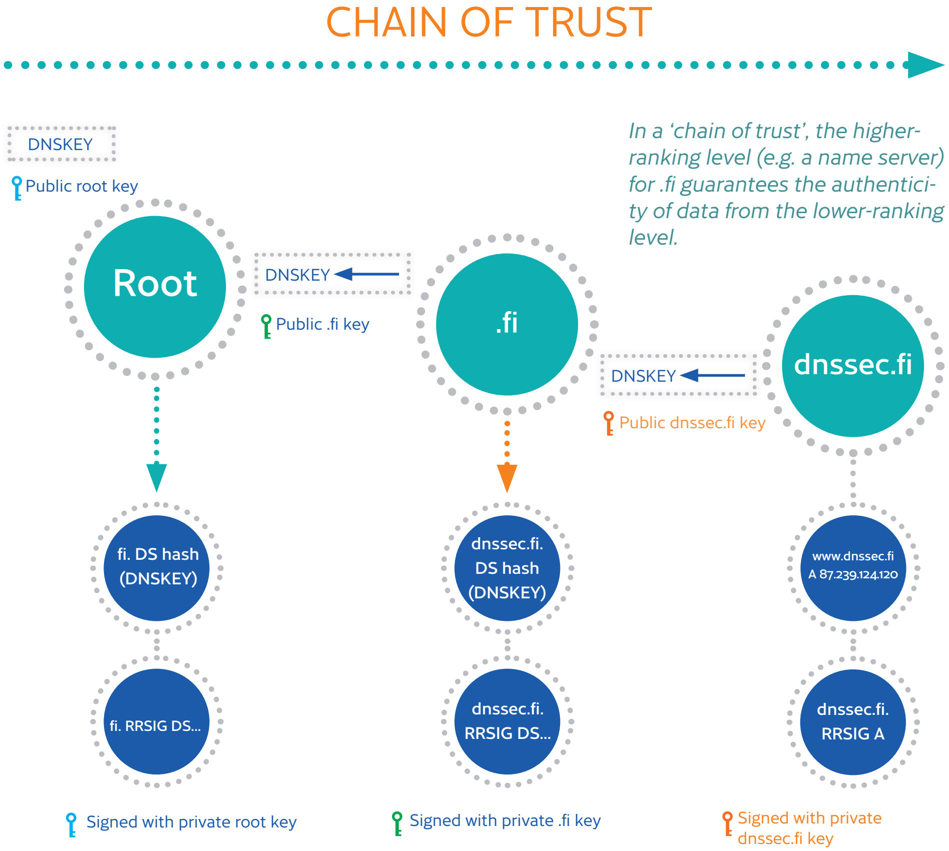
To compile digital signatures, a pair of keys is generated. A pair of keys of this type is made up of a private and a public key (asymmtric cryptosystem). As the name suggests, the private part is secret and remains with the owner.
The public part is published in the DNS (DNSKEY record). Using the public key, it is now possible to check and validate a signature that has been signed with the private key. It is thus necessary to trust a public key before you can check a signature. Since it is not possible to trust all the keys in the internet, use is made of a key hierarchy similar to the DNS hierarchy ('chain of trust'). This looks somewhat confusing at first sight, but its sole purpose is to ensure that all signatures can be verified with a single public key.



With DNSSEC, your internet provider's name server is able to recognise a hierarchy that has been modified by 'cache poisoning'.

The ‘chain of trust’ in detail

An image of the public key is notified to the next level of the hierarchy in each case. The higher level writes this image into its zone (DS record) and guarantees its authenticity by signing it. This public key for this level is then, in turn, notified to the next higher level.



In a ‘chain of trust’, the higher-ranking level (e.g. a name server) for .fi guarantees the authenticity of data from the lower-ranking level.

What do I need in order to use DNSSEC?

As an internet user, there is no need for you to do anything. If your ADSL or cable modem provider supports DNSSEC, all signature checks will be made on their DNS servers.
If you are the holder of a domain name, your website operator must set up DNSSEC for you.

Since DNSSEC will not be very widespread precisely in the initial phase, it will probably be the case that only operators of websites requiring protection (e.g. banks) will protect their domain names with DNSSEC to begin with.

Thanks to SWITCH who have produced the ”What is DNSSEC?”
SWITCH = the Swiss education and research network (www.switch.ch)

Customer service
p. 0295 345 656 / Domain Name Service / Mon-Fri 9-15
p. 0295 34 5000 / Switchboard / Mon-Fri 8-16.15

Finish Transport and Communications Agency
Kumpulantie 9
Helsinki, Finland
00059 TRAFICOM
domain.fi / traficom.fi

TRAFICOM
Finnish Transport and Communications Agency