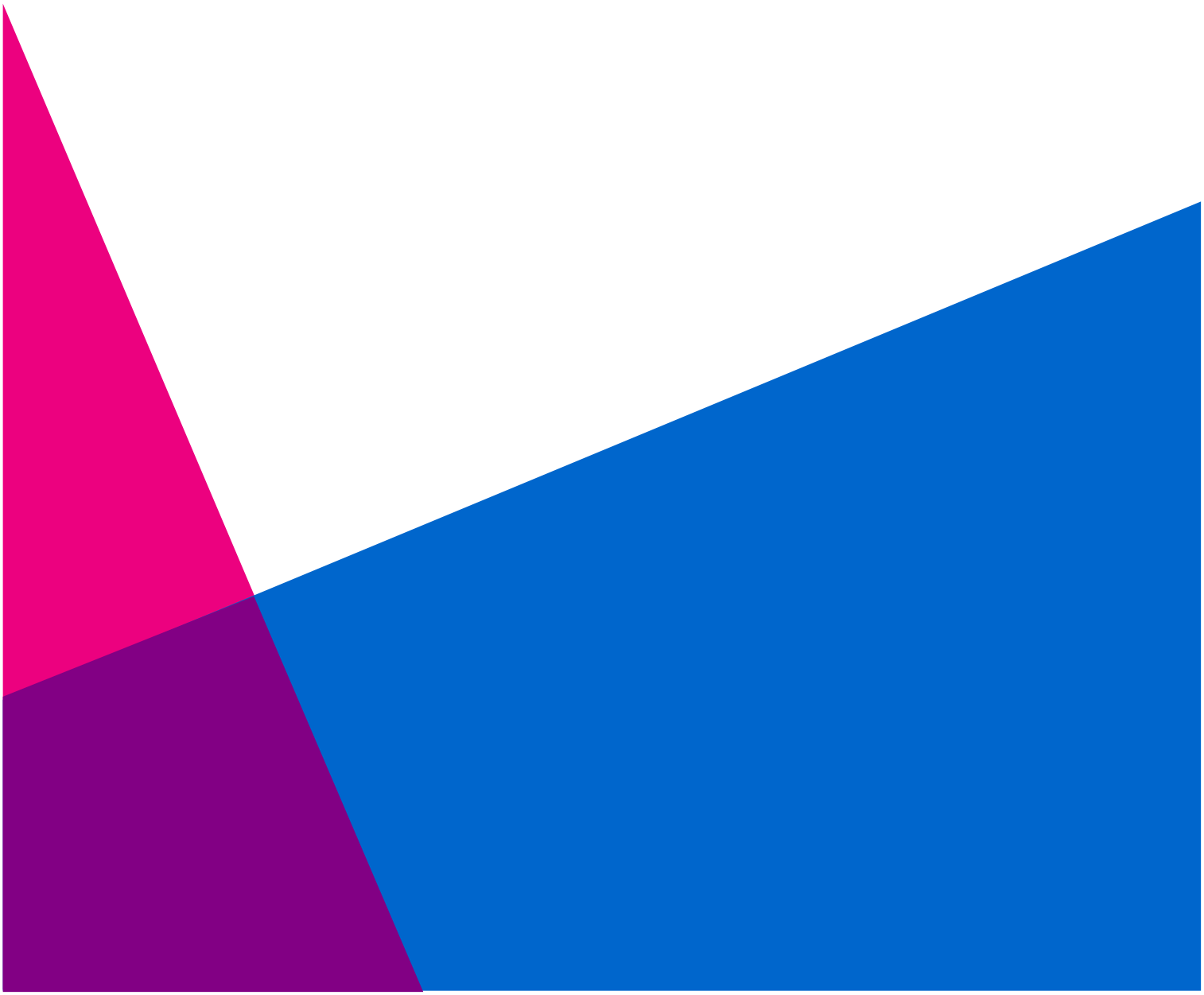
TRAFICOM
Liikenne- ja viestintävirasto

Secure domain name management

A guide for domain name registrars and holders

FI Domain Team



Contents

Introduction

If an organisation's domain name ends up in the hands of a malicious operator, they can potentially prevent access to the organisation's website, stop e-mail traffic, redirect VPN traffic elsewhere and gain access to encryption keys, user account information and other important data. As such, these types of security breaches may end up having major financial or political consequences as well.

This publication provides recommendations that can help organisations keep their domain names safe. The recommendations can help organisations reduce the risk of negative impacts on their image online, improve the usability and reliability of systems and increase the credibility and security of communications.

An organisation's online identity is strongly tied to their domain name. Most forms of online interaction with an organisation, from visiting their website to sending e-mails, are dependent on their domain name being findable. Because of this, it is important for organisations to be able to keep their domain names safe and secure.

This guide is intended primarily for the managers and technical staff of organisations' information management departments. The hope is that the recommendations will support organisations in developing their existing practices and ensuring that domain names are handled in a way that does not cause undue risks for the organisations.

General recommendations

This section provides general recommendations and details good practices for the safe and secure management of domain names. These recommendations can help organisations manage the risks associated with managing domain names.

The general recommendations and the principles mentioned below should be considered examples instead of an exhaustive list:

- An organisation should be aware of all of its domain names.
- The changing of domain name registration information must be secured via authentication.
- The changing of domain name registration information should always follow a standard procedure.
- Domain name registration information should be reviewed regularly.
- Name servers should be set up in a way that protects the organisation's domain names and ensures their usability.
- All domain names should be protected with Domain Name System Security Extensions (DNSSEC).
- DNS queries should be validated with DNSSEC.

Background

The Domain Name System (DNS) was implemented in the early 1980s. Its aim was to create a powerful and reliable, decentralised naming system that could process the requests made by a growing computer network.

This network eventually developed into what we now know as the global internet. Even today, the Domain Name System is still a prerequisite for the functioning of the countless services of the internet, but unfortunately security was not an area that was given much thought during its inception. One of the consequences of this is that nowadays we have to contend with a wide range of risks associated with domain names and the management thereof.

Traficom has observed an increase in attacks targeting domain name databases, domain name holders and name services in recent years (see concept definitions in Annex A: Concepts).

Examples of attack types

- breaching of domain name database and domain name registrar data
- breaching of domain administrator accounts maintained by registrars
- DNS hijacking of name servers and domain name databases
- using name servers for distributed denial-of-service attacks
- man-in-the-middle attacks and cache poisoning
- tampering with the DNS settings of home routers and computers.

Distributed denial-of-service attack: A distributed denial-of-service attack (DDoS) is a cyberattack in which hackers use hijacked computers to cause an unusually high amount of traffic for a specific website (web server) or network. This causes the website or network to go down and become unavailable for real users during the attack.

Man-in-the-middle attack: A type of attack in which a third party intercepts and potentially also alters communications between two parties.

Cache poisoning: An attack on a DNS service in which invalid entries are placed in a DNS server's cache for the purpose of redirecting traffic to an incorrect address.

Reading instructions

The guide is divided into two main sections, both of which have their own target audiences. The sections contain grouped recommendations that can help organisations reduce the risks associated with the above-mentioned types of attacks.

1. Recommendations concerning domain name management Target group: managers of information management departments

The recommendations provided in this section can help the managers of information management departments to safely and securely manage domain names and prevent attempts to compromise domain name security and hijack DNS servers (sections 2 and 3).

2.1 Recommendations concerning the design of name servers and 2.2 Recommendations concerning DNSSEC

Target group: Information system experts and the technical staff of information management departments

The recommendations provided in this section can help information system experts and the technical staff of information management departments to design and administer secure name servers. The measures can reduce the risk of DNS hijacking, prevent the utilisation of name servers in DDoS attacks and provide protection against man-in-the-middle attacks that utilise the Domain Name System.

The guide does not cover attacks targeting domain name databases (WHOIS services, OData) and registrars or attempts to tamper with the DNS settings of home routers and computers.

1 Recommendations concerning domain name management

Although domain names are one of the cornerstones of an organisation's online visibility, they are often forgotten about after being configured following registration. Traficom recommends that all organisations should systematically manage their domain names and actively monitor and administer their user accounts and domain name registrations.

The active and secure management of domain names can prevent external attempts to influence an organisation's systems, such as DNS hijacking attempts and attempts to tamper with domain name holders' user accounts.

1.1	**Domain name management**	Summary of domain names
Document the domain names in your organisation's possession and the domain name registrars used.		

If your organisation has registered domain names via multiple domain name registrars, you should consider consolidating them to a single registrar to make the administration and usage monitoring of the domain names easier.

When evaluating domain name registrars, you should also consider the security measures offered by the registrars, such as the possibility of enabling two-factor authentication for domain administrator accounts.

1.2	**Domain name management**	Domain name administration
Review the list of domain names regularly and evaluate the need to preserve or relinquish each domain name.		

Registering a domain name is easy and affordable, but registered domain names should be managed and their security should be monitored. If a domain name is no longer being used, you should consider relinquishing it to both ease the administrative burden on your organisation and reduce the 'surface area' susceptible to attacks. A .fi domain name can also be registered without name servers.

Registering a domain name without name servers is recommended if you want to keep a domain name in reserve, so to speak, for future use.

If a domain name that you are planning on relinquishing has been closely connected to your organisation's identity or brand, you should consider extending its registrations for the duration of a transition period to prevent it from being claimed by others. This way you can also monitor whether your old website is still getting traffic by checking the domain name's logs.

The relinquishing of a domain name should follow a standardised process so as to ensure that all references to the domain name are deleted from firewalls, encryption certificates and network and e-mail servers, for example. In some cases, it may be a good idea to hold on to a domain name for the time being even if it is no longer being used. The relinquishing of a domain name should always be a conscious decision.

1.3	**Domain name management**	Domain administrator accounts
Regularly review which domain administrator accounts are being used in your organisation and evaluate whether they should be kept separate or combined.		

.fi domain names are registered via a domain name service administered by Traficom. **Domain name registrars** can access a self-service portal in the domain name service using their own user accounts. The portal allows registrars to register and take control of domain names, change domain names' authoritative name servers and update the contact information of domain name holders, among other things. A domain name registrar can have multiple user accounts under their registrar account that have access to the system.

It is very important for domain name registrars to regularly review their domain name service accounts. If, for example, an employee is transferred to another position, yet still needs access to the registrar account in a different role, their user account's access rights must be adjusted to correspond to the employee's new position.

The largest domain name registrars typically use the domain name service's EPP interface to administer domain names. EPP makes it possible for domain name registrars to connect their own systems to the domain name service. By doing so, a registrar can offer their customers access to a self-service interface for registering and administering domain names. Using the EPP interface allows changes to be updated almost in real time.

A domain name holder's administrator account can be used to administer one or multiple domain names. Some organisations connect multiple administrator

accounts to a registered domain name for the purpose of administering it from multiple departments, for example. However, the existence of multiple administrator accounts increases the overall administrative burden, and the more accounts there are, the more potential targets there are for attacks.

1.4	**Domain name management**	User accounts on domain name registrars' systems
Regularly review which administrators have the right to administer your organisation's domain names on their registrars' systems. Make sure that access rights are up to date.		

Access to an organisation's accounts on registrars' systems should be restricted to persons who genuinely need to access them. The administrators must be aware of their responsibilities and role and the risks associated with phishing attempts. If a scammer manages to obtain the user information of a person who has access to a domain name registrar's system, they can potentially hijack the organisation's domain names or make any number of changes to name server configurations.

If a person leaves the organisation or their duties change, their access rights should be immediately revoked in accordance with the organisation's access rights management process.

1.5	**Domain name management**	Passwords to user accounts on domain name registrars' systems
Make sure that administrators use secure passwords in accordance with your organisation's password policy. If the domain name registrar offers the possibility of using two-factor authentication, using it is highly recommended.		

User names and passwords to registrar's systems are sensitive information and should be treated as such.

1.6	**Domain name management**	Contact information
Make sure that the contact information associated with all domain names is up to date and that the billing information provided to domain name registrars is up to date, if applicable.		

You should consider creating position-specific e-mail addresses so that important information is not missed due to possible personnel changes. If you do so, you should make sure that the relevant employees actively monitor the addresses in question. Using employees' private e-mail addresses to register the organisation's domain names should be avoided.

1.7	**Domain name management**	Recovery
Familiarise yourself with the domain name registrar's procedures for recovering hijacked domain names. Make sure that you have access to all the required documentation.		

Note that the procedures for recovering hijacked domain names vary considerably depending on the domain name registry. As regards .fi domain names, you should contact your own domain name registrar and, if necessary, the Finnish Transport and Communications Agency Traficom.

In general, the following documents can be useful for recovering hijacked domain names:

- a printout of the domain name registration
  (WHOIS search or screenshot / export of the domain name registrar's information)
- invoice or receipt of the payment transaction
- correspondence with the registrar concerning the registered domain names
- possible legal documents that show a connection between the organisation and the domain name.

1.8	Domain name management	Domain name renewal
Monitor the validity periods of all registered domain names and extend the registration of domain names in good time when necessary.		

Many domain name registrars offer the possibility of renewing domain names automatically. This reduces the risk of the domain name expiring. Billing information should be kept up to date to facilitate domain name renewal.

Although domain name registrars usually remind domain name holders about expiration in advance, organisations should have their own processes for ensuring renewal. If a domain name registration is not renewed in time and subsequently expires, it will become available for others after a grace period.

1.9	Domain name management	Changes and review
If there is a need to change the information on a domain name registrar's system, follow a formal change management process. Review current information regularly to ensure that no unauthorised changes have been made.		

To avoid unpleasant surprises, organisations should be very vigilant when making changes to domain name registrations. Invalid configurations can cause problems in regard to e-mail traffic, for example, and even cut off access to the organisation's website. Planned changes should be reviewed and approved in advance in accordance with the organisation's change management process.

1.10	Domain name management	Registration of new domain names
Organisations should have a formal procedure in place for the registration of new domain names, and it must be complied with.		

In order for an organisation to remain aware of all of the domain names in its possession and to ensure that the registration of new domain names is safe and secure, the organisation should establish a formal registration procedure and follow it.

A formal procedure can also help ensure that new domain names are accepted, that they are registered with the correct information on the correct accounts on the domain name registrar's system, that they are administered by the correct persons responsible and that their safety and security are ensured in accordance with the organisation's policies.

1.11	Domain name management	Prevention measures on the domain name registrar's system and name database
Protect domain names from unauthorised transfers, updating and deletion using the prevention measures offered by the domain name registrar.		

The changing of domain name information on Traficom's domain name service can be prevented with a so-called registry lock. The registry lock must be deactivated before any changes to the domain name information can be made. The lock can only be deactivated using a code sent to phone numbers specified in advance. The details of activating and deactivating registry locks should be discussed in advance with the domain name registrar.

2 Requirements concerning the design of name servers

This section and the recommendations provided in it are aimed at information system designers and the technical staff of information management departments. The reader is subsequently expected to possess a basic understanding of the Domain Name System. For more information on the concepts used and the DNS query process, please see Annexes A and B.

There are certain basic rules that should be followed in the design of name servers regardless of whether an organisation uses their own name servers, purchases a name service from a service provider or uses a combination of these two options.

A name server that is designed to be safe and secure ensures both the reliability of the organisation's DNS records and the functionality of systems. Safe and secure implementation can also reduce the risk of name servers being used for DNS-based denial-of-service attacks and the risk of successful cache poisoning.

The provided recommendations primarily concern name servers that are used to resolve external domain name queries, but many of the principles also apply to internal name servers.

Figure 1 below presents an example of a simple name service solution used by the fictional company Example Ltd:

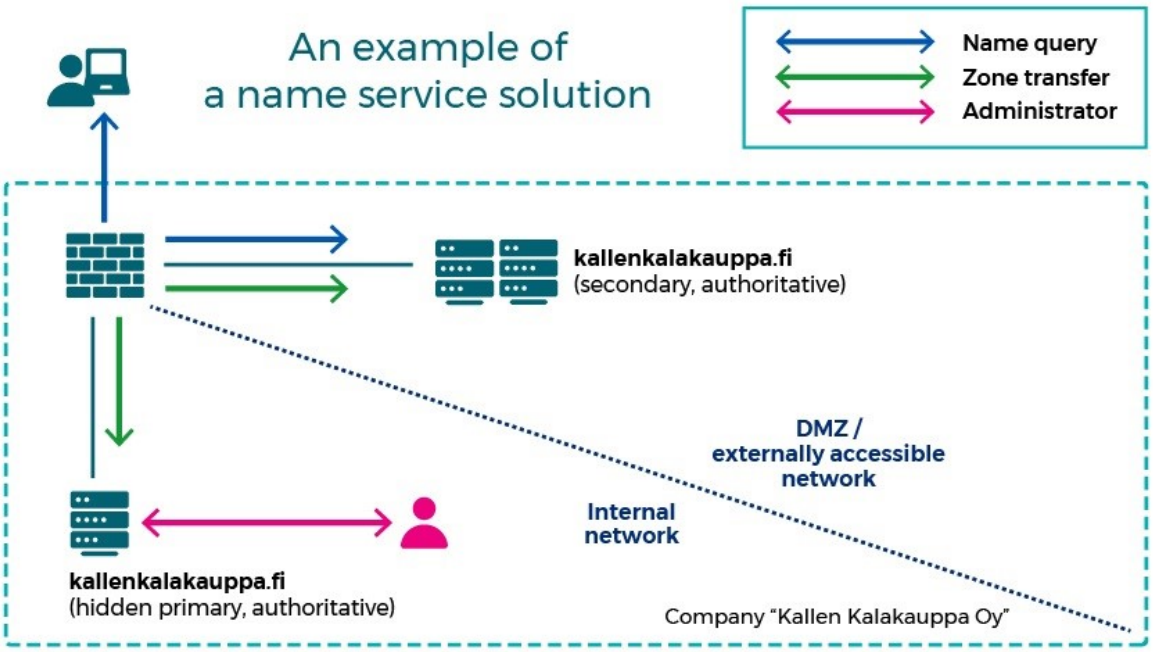


Figure 1: An example of a name service solution

The figure only presents an example, not an actual recommendation for implementing a name service solution. The optimal solution for each organisation depends on factors such as the size of the organisation, the hosting service, available resources and the geographic location of users who use the organisation's online services.

Traficom provides the following recommendations concerning the design of a name service for domain names usable over the internet:

2.1.1	Name server design	Differentiation of name server roles
Configure authoritative name servers so that they do not accept recursive queries.		

Authoritative name servers connected to the internet should not process recursive queries. Recursive queries increase server load and can make servers vulnerable to DNS reflection attacks and cache poisoning attempts. Recursive name queries should be handled by separate name servers that are only accessible to internal or known clients.

2.1.2	Name server design	Internal and external domain names
Information on internal domain names or server names should not be available on externally accessible name servers.		

The names and IP addresses of internal systems that outsiders are not meant to access should not be stored in the zones of external name servers.

Distributing internal resources across one or multiple sub-domains makes it possible to differentiate the administration of internal and external domain names and reduces the amount of information on internal structures that can be accessed via the internet.

2.1.3	Name server design	Name server redundancy
Secure the functioning of your name service by using multiple external name servers.		

It might be a good idea to let an external service provider that is not dependent on your organisation's internal structures to handle some or all of your organisation's external name servers. Name service providers can usually offer effective protection against denial-of-service attacks, geographically decentralised name server locations, around-the-clock monitoring and specialised technical support services. Some name services also support Anycast, which ensures that client requests are processed by a geographically distributed network of name servers. This also minimises the response time for the client.

The Finnish Transport and Communications Agency Traficom offers a free-of-charge service to provide Anycast secondary DNS for .fi domains. Further information on Traficom's Anycast service is available at https://www.traficom.fi/en/anycast-dns-registrars.

Domain name holders can enable Traficom's Anycast services for their .fi domain names via their own domain name registrar.

2.1.4	Name server design	The specialised task of name servers
Do not use external name servers for any other purpose than operating a name service.		

Name servers should not be used for any other tasks, and they should only run the software necessary for operating the name service. This reduces susceptibility to attacks and the risk of software vulnerabilities endangering the security of the name server.

2.1.5	Name server design	Hiding the primary name server
Do not use the primary name server as the name server of externally visible domain names. Prevent the primary name server from being accessible via the internet.		

The primary name server contains the primary copy of the zone file, and access to it via the internet should be prevented. The primary server should only be used for zone administration and the exchange of zone data with secondary name servers accessible over the internet. Access to primary servers should be restricted to approved name service administrators. Figure 1 presents an example of a name service solution in which the primary name server is hidden.

2.1.6	Name server design	Location of secondary name servers
Place secondary name servers in a separate network segment that only allows appropriate inbound and outbound traffic.		

Isolating name servers accessible via the internet to a separate, firewall-protected network segment can reduce the risk of a compromised server being used as a 'springboard' for tampering with other services. An example implementation in which name services accessible via the internet have been isolated to a demilitarised zone (DMZ) is presented in Figure 1. However, the functioning of the name service should be ensured by duplicating structures and/or using external name service providers.

2.1.7	Name server design	Firewall protection of name servers
Protect name servers with firewalls that only allow essential data traffic.		

Ideal firewall configurations depend on the selected hosting model and the organisation's other IT structures.

The following factors should be taken into consideration when assessing whether data traffic between different clients, servers and network segments is essential:

- The system must make it possible to accept DNS queries only from specified clients (internal/external depending on the role of the name server) using TCP and UDP over port 53.
- Recursive name servers serving internal users must be able to send DNS queries to the internet using TCP and UDP over port 53.
- Authoritative secondary name servers must be able to receive notifications from the primary name server and exchange zone data only with the primary name server.
- Data traffic to and from a centralised log service (SIEM) and essential for the administration of servers must be restricted to essential IP addresses and ports.
- The implementation of DNS validation should be considered if supported by the firewall used. This can ensure that only traffic that complies with official DNS requirements is allowed. It should be noted, however, that activating DNSSEC may require the allowing of large DNS packets and the use of TCP for resolving and responding to queries.

Firewall configurations must be thoroughly tested before deployment.

2.1.8	Name server design	Secure communication between name servers
Secure zone transfers between the primary and secondary name servers with TSIG.		

If zone data is shared to secondary name servers via zone transfers from the primary name server, the communications should be protected with a TSIG signature[1]. TSIG ensures that zone transfers can only be carried out to authenticated secondary servers and that the actual updating of the data is carried out appropriately. Each name server pair must have unique TSIG keys, and the TSIG must be subject to appropriately strict firewall configurations (see above). The keys are generated using name server software that is configured to sign all data traffic with other name servers.

2.1.9	Name server design	Utilisation of name servers in denial-of-service attacks
Configure name servers and network segments so that the risk of DNS reflection-based denial-of-service attacks is minimised.		

Name servers can be utilised in DNS reflection attacks in which the sender's IP address is spoofed for the purpose of making DNS queries with the victim's IP address instead of the sender's address. Since the response packets sent by a name server are larger than the queries, this method can be used to overload the victim's server or network resources. When using DNSSEC, response packets are larger than usual because they also include a digital signature. This makes name servers using DNSSEC particularly appealing in the eyes of those who carry out denial-of-service attacks. The risk can be reduced with the following additional measures:

- prohibiting recursive queries from the internet
- prohibiting AXFR queries (zone transfers) from other than authoritative name servers
- limiting the number of queries from the same IP address over a specified time frame (*rate limiting*)
- configuring routers and firewalls to only accept packets from IP addresses that have been approved in the network used to send packets (IP address spoofing prevention)
- prohibiting ANY queries (all records), if the name service software supports this.

2.1.10	Name server design	Version information
Configure name servers so that their response records do not include the name or version number of the software used.		

If a name server provides the name or version number of the software that it is running, an attacker can easily target known vulnerabilities and tailor their attack to the specific software version. Hiding the name and version number does not actually eliminate vulnerabilities, but it can force hackers to make additional enquiries, which may be spotted by your organisation's monitoring system. It is good practice not to disclose unnecessary information, but it is even more important to ensure that name servers and their operating systems are always kept updated (see below).

[1] https://tools.ietf.org/html/rfc2930

2.1.11	Name server design	Updates
Always keep name servers and their operating systems updated to the latest versions.		

Security updates for the name server software and the supporting hosting environment remove discovered vulnerabilities and help secure domain name data and the usability of your organisation's name service. If your organisation's name service is handled entirely or partially by an external service provider, you should make sure that security updates are tested and installed in a timely manner and according to a clearly defined procedure approved by your organisation.

2.1.12	Name server design	Changing configurations
Follow a formal change management process when changing name server configurations or the basic structures of the DNS solution.		

All planned changes to DNS structures or configurations should be reviewed and approved in advance in accordance with the organisation's change management process. A systematic approach to change management can reduce the risk of unexpected consequences and improve usability.

2.1.13	Name server design	Logs
Maintain a log of administrative actions concerning name servers in accordance with your organisation's logging policy. Review the logs regularly for actions indicative of unauthorised use.		

At minimum, you should maintain a log of rejected and approved login attempts and changes to configurations and zones. Good logs help locate errors and process security incidents.

2.1.14	Name server design	Hiding the primary name server
Review zones regularly to ensure that records are in order and that no unauthorised changes have been made to them.		

Records should be reviewed regularly to ensure that they are in order and that their content is correct. Unused records and records referencing IP addresses other than those associated with registered locations should be deleted. If you notice signs of unauthorised changes, you should immediately contact the person responsible for information security.

2.1.15	Name server design	Using DNSSEC
Use DNSSEC with all of your external domain names, if possible.		

DNSSEC prevents the spoofing of DNS query responses and ensures that received responses come from authenticated name servers.

Even if a domain name is not in active use, without DNSSEC responses to queries can still be spoofed. The sender of the query can thus be redirected to a phishing site maintained by an external party. In the case of .fi domain names, name servers should be completely removed from unused domain names. .fi domain names do not necessarily need to have any name servers.

2.1 Recommendations concerning DNSSEC

Since the Domain Name System is essential for locating services on the internet, attackers can look to spoof DNS query responses via man-in-the-middle attacks or cache poisoning. When successful, such attacks can redirect users from the website that they intended to visit to another website where they can be coaxed into disclosing login information or other sensitive information, for example. These types of attacks usually target external domain names on the internet.

DNSSEC (*Domain Name System Security Extensions*) is a suite of extensions to the DNS standard that uses cryptographic methods to ensure that the maker of a DNS query can trust that

- the response to the DNS query comes from the correct name server
- the response is not spoofed along the way
- a response stating that the queried name does not exist can be authenticated.

It should be noted that DNSSEC does not encrypt the actual DNS traffic. DNS encryption, such as *DNS over TLS* or *DNS over HTTPS* techniques, is not covered in this guide.

DNSSEC validation

The query process for domain names protected with DNSSEC is largely the same as the regular query process (see Annex B: DNS query process), but includes both the cryptographic validation of individual responses and the authentication of the hierarchical position of the name servers taking part in the process.

Response validation

DNS query responses are validated using the following record types:

- **RRset (resource record set):**
  Groups together all resource records of the same type (such as A or MX records)
- **RRSIG (resource record signature):**
  The signed hash value of the RRset based on a private ZSK
- **ZSK (zone signing key):**
  A public signing key for RRSIG validation
- **DNSKEY:**
  A record type used to store public signing keys

Response validation in a DNSSEC-signed zone is illustrated in Figure 2 below:

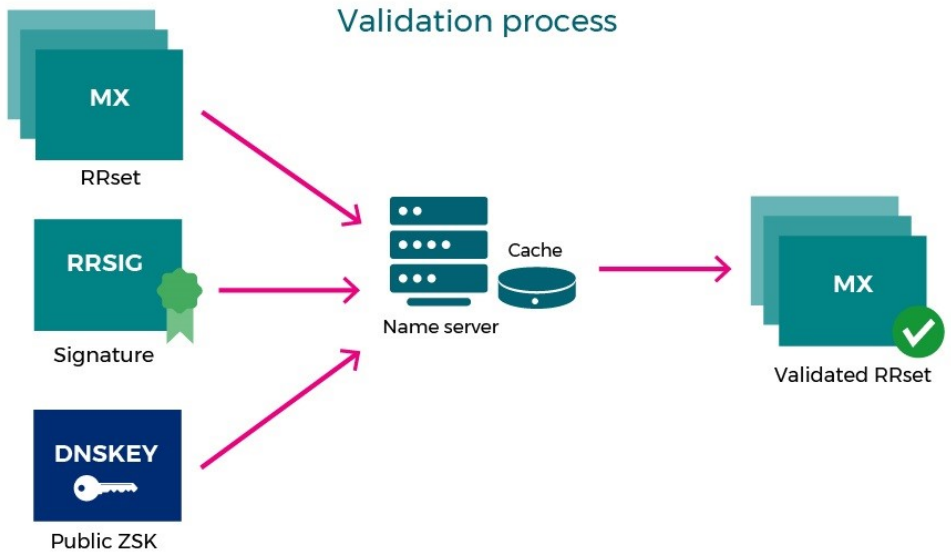


Figure 2. Resource record validation process (using an MX record as an example)

With the help of a public ZSK (zone signing key), the name server resolving the query can validate the signature (RRSIG) of the resource record set (RRset) of the requested record. This ensures that invalid responses are identified as such.

Validation of responding servers

To confirm that a validated response originated from a valid name server that is authorised to respond on behalf of the domain name, the public ZSK (marked in blue) used in the process depicted above must also be validated. This is done using the following records:

- **KSK (key signing key):**
  A public signing key for authenticating the RRSIG of the DNSKEY's RRset, such as a ZSK.

- **DS (delegation signer):**
  The hash value of the public KSK, which is saved in the zone responsible for domain name delegation (*parent zone*).

The process is similar to the one detailed above, but chained into a *chain of trust* via a TLD to the root of the DNS (see Figure 3). The public ZSK is validated with a public KSK, the hash value of which is stored in the parent zone's DS record.

The DS records of .fi domain names are stored in the domain name service administered by Traficom. The register's own KSK is stored as a hash value at the root of the hierarchy[2]. This way the fact that only authenticated name servers provide signed responses to DNS queries can be cryptographically ensured throughout the zone hierarchy. The process is illustrated in Figure 3 below.

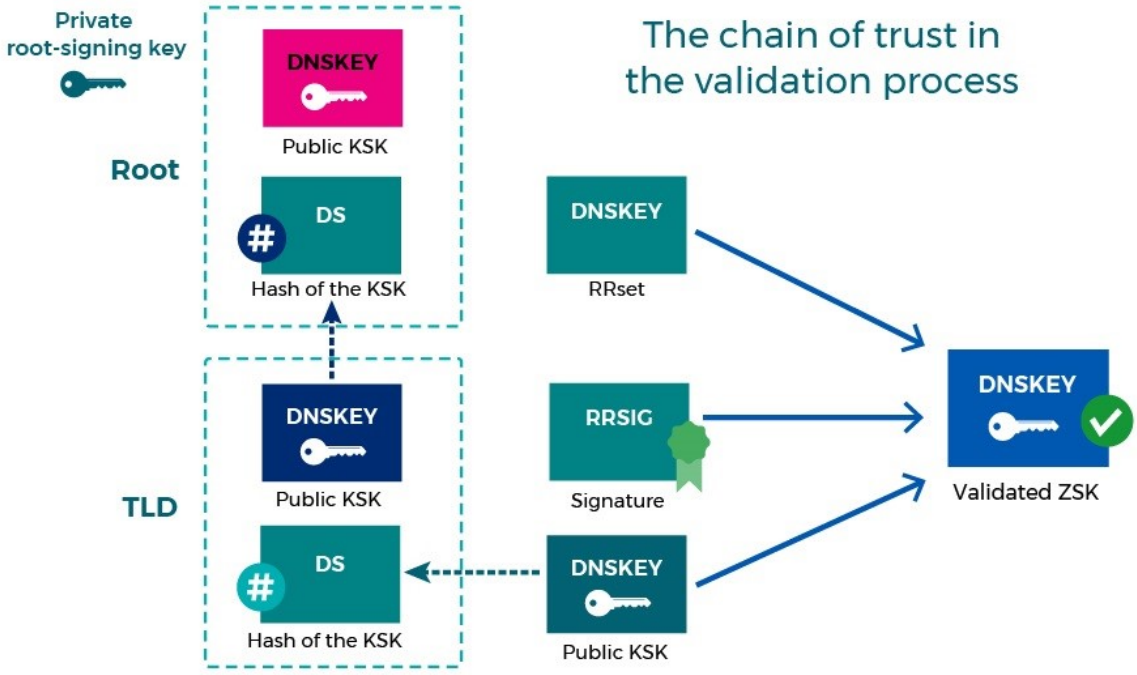


Figure 3. Overview of the DNSSEC validation process

Although the validation process may seem complicated, deploying DNSSEC for an organisation's domain names is usually simple. It can be deployed via a name service provider (often the same as the domain name registrar) or activated by the organisation's own name server administrator. In both cases, it is essential for the name server administrator to plan the necessary key management processes with care.

Regardless of whether DNSSEC is used for the organisation's external domain names, Traficom provides the following recommendations:

2.2.1	Name server design	Using DNSSEC
Use DNSSEC with all of your external domain names, if possible.		

2 The public KSK and ZSK of the hierarchy's top-level domain names (root zone) are signed with a private *root signing key* in a complex process that is repeated four times a year. The aim is to maintain the reliability of root keys.

To protect an organisation's own users against responses sent by spoofed or unauthorised name servers, the name servers resolving DNS queries on behalf of the organisation's users should be configured to validate responses concerning domain names that use DNSSEC. A response not passing DNSSEC validation can be a sign that the response has been tampered with, but it can also be caused by the DNSSEC-signed zone being incorrectly configured.

The following tools can help with troubleshooting:

https://dnssecdebugger.verisignlabs.com/

https://dnsviz.net/

2.2.2	DNSSEC	Deployment of DNSSEC on all authoritative name servers
All name servers should support DNSSEC.		

If there are name servers in a DNSSEC-signed zone that do not support DNSSEC, validation can fail, which can lead to usability problems.

2.2.3	DNSSEC	Signature renewal
Automatically renew signatures in good time before they expire.		

Zones that do not use DNSSEC are usually only updated when records are changed, deleted or created. When using DNSSEC, it should be noted that signatures are only valid for a limited time and must thus be renewed in good time before they expire. It should also be noted that records based on old signatures can remain in the cache, and their validation remains possible until they are deleted from the cache (when their *time to live* (TTL) ends). An active signature expiring will render clients validating the DNSSEC signature unable to access the resource. Signature renewal is usually automatic, but the process should be monitored.

2.2.4	DNSSEC	Responding to DNS queries concerning domain names that do not exist
Use NSEC3 to respond to queries concerning non-existent domain names. NSEC3 prevents zone walking, which makes it impossible to ascertain the full content of the zone.		

As with responses to queries concerning existing domain names, it must also be possible to validate responses that concern non-existent domain names with DNSSEC. NSEC3 is ideal for this purpose: it can be used to chain all of the domain names located in the same zone together and prove that domain names not included in the chain do not exist. To prevent the retrieval of a record containing full actual domain names by going through the chain from start to finish, NSEC3 presents the hash values of the names in encrypted form instead of as plain text.

2.2.5	DNSSEC	Changing keys
Renew KSKs and ZSKs regularly and automatically whenever there is reason to suspect that their security has been compromised.		

KSKs and ZSKs have finite validity periods. They must also be renewed regularly so that their security is not compromised. Most name server solutions provide a way of automating this process. Please note, however, that the renewal of KSKs requires exchanging updated DS records with the parent zone. In practice, with .fi domains the new DS records must be updated to the .fi root zone.

It is essential to take into account the validity periods of previously created signatures, the time to live (TTL) of data in the cache and the replication of DNS records throughout the Domain Name System in the process.

2.2.6	DNSSEC	Generating and storing KSKs
Generate and store KSKs in a safe environment.		

The ZSKs of zones protected with DNSSEC are based on KSKs, so KSKs must be generated and stored in a safe environment. If your organisation has a high security level requirement or encryption needs, you should consider using an HSM (*hardware security module*) for creating and storing encryption and signing keys.

2.2.7	DNSSEC	Key and hash algorithm
Use only algorithms that are generally considered safe.		

The algorithm most commonly used as the basis for the encryption of DNSSEC-signed .fi zones is, by a large margin, RSA/SHA-256 (8). Algorithm number 8 is generally considered safe.

Conversely, algorithm numbers 5 (RSA/SHA-1), 6 (DSA-NSEC3-SHA1) or 7 (RSASHA1-NSEC3-SHA1) should NOT be used.

Keys and signatures based on ECDSA (algorithm number 13 ECDSAP256SHA256 can be used for .fi domain names) are much shorter than those based on RSA, as a result of which they take up less space in the zone or name queries. Signing with them is quicker, but their validation is slower.

If security and speed need to be emphasised differently, algorithm numbers 8 (RSA/SHA-256) and 10 (RSA/SHA-512) can also be considered. Contrary to what one might think, algorithm number 10 is no more secure in practice than algorithm number 8. However, there are no practical obstacles to using algorithm number 10.

The newest DNSSEC algorithms are algorithm numbers 15 (Ed25519) and 16 (Ed448). These algorithms are still fairly new and not supported by all resolver name servers. Support for algorithm number 15 is coming for .fi domain names, but it cannot be used yet.

Regardless of the algorithm used, DNSSEC-signed responses are often so large that they must be sent using TCP. As previously stated, because of this it is important to always allow DNS queries over TCP.

2.2.8	DNSSEC	Network support for DNSSEC traffic
Make sure that the network solution used for the name service supports DNSSEC.		

Since DNS queries are larger than normal in a DNSSEC-signed zone, you should make sure that the network configuration and firewalls support them. This must be tested before deploying DNSSEC so that the usability of services is not endangered. For example, EDNS0 is no longer a problem for most firewalls and other network devices, but it is still a good idea to take the matter into consideration.

3 Other useful measures

The technical solutions mentioned below are not covered by this guide, but they should be taken into consideration as useful additional measures that can improve the protection of an organisation's infrastructure and communications:

- DANE: DNS-based Authentication of Named Entities
  A method similar to DNSSEC that is suitable for the following tasks:
  - indicating which certificate issuer the owner of the domain name allows to issue certificates concerning the domain name's resources
  - indicating the approved encryption certificates used by the domain name's resources
  - indicating to the senders of e-mails that they should encrypt the message traffic to the domain name's e-mail server.
- SPF: sender policy framework
  DKIM: domain keys identified mail

  DMARC: domain-based message authentication, reporting and conformance DNS-based measures for preventing the delivery of spoofed e-mail messages to the recipient.

4 References

The Finnish Transport and Communications Agency Traficom would like to thank the Danish *Centre for Cyber Security (CFCS)* for the source material.

Content-related tips were received from the following sources, among others:

https://www.icann.org/en/system/files/files/sac-044-en.pdf https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
https://www.enisa.europa.eu/publications/gpgdnssec

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-81-2.pdf

https://tools.ietf.org/html/rfc6781

5 Annex 1: Concepts

Below are a number of concepts with definitions and a description of the DNS query process to serve as background information for the recommendations provided in this guide:

- DNS (Domain Name System): A system and network protocol, the primary purpose of which is to facilitate the translation of domain names into IP addresses in a network. The Domain Name System is hierarchical in nature and administered with a decentralised network of name servers.
- Top-level domain (TLD): A domain at the highest level in the hierarchical Domain Name System. Top-level domains can be generic top-level domains (gTLD), such as .com, .org and .edu, or country-code top-level domains (ccTLD), such as .fi or .se.
- Domain name database: A database of all the domain names, their holders and authoritative name servers of a given top-level domain. The database of Finnish .fi domain names is maintained by Traficom.
- Registrar: A registrar offering domain name registration services. Many domain name registrars also offer website space and name server services, but these are not a mandatory part of the services of a registrar.
- Domain name holder: A person or organisation who has the right to use a specific domain name.
- Administrator: A person or organisation that has been authorised by the domain name holder to carry out actions concerning the domain name.
- Name server: A server or service that translates domain names into the corresponding IP addresses using the DNS protocol.
    - Recursive name server: A name server that helps resolve DNS queries from client machines by checking whether the name is already in the server's cache. If not, the server will send queries to relevant name servers until it receives an authoritative answer.
    - Authoritative name server: A name server that has been granted authoritative responsibility for a specific zone.
- Zone: A zone encompasses all the information about a domain name that a name server has authoritative responsibility for. If there are no sub-domains handled by other name servers associated with a domain name, then its zone equals the domain name. If there are one or more sub-domains handled by other name servers associated with a domain name, then the domain name has multiple zones.
- Resource record (RR): A zone's resource record usually contains a specific name, type and value. Example of an A-type resource record in the zone kallenkalakauppa.fi:
    - www A 193.163.102.58 – an address/host record (A) that returns the IP-address 193.163.102.58 when queried for host www.kallenkalakauppa.fi.

6 Annex 2: DNS query process

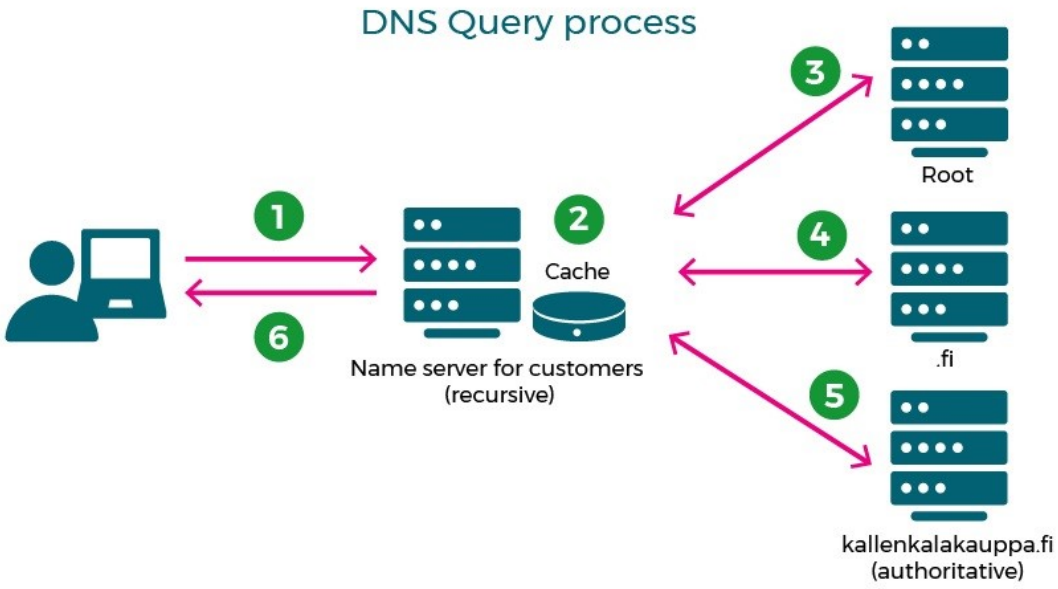


Figure 4: DNS query process

1. When a client wants to visit a website named www.kallenkalakauppa.fi, the request is first sent to the name server that the computer has been configured to use. In the case of companies, this is usually a name server operating in the company's own network. In the case of private users, the name server used is usually provided by an ISP.
2. The name server searches its cache to check whether it already knows the answer to the query based on previous queries.
   If the answer is found in the name server's cache, it is returned to the client, and the process ends here.
3. If the answer is not found in the cache and the name server does not know which name servers are responsible for the domain name kallenkalakauppa.fi or the top-level domain .fi, it queries a name server that it is familiar with at the root of the DNS hierarchy for name servers responsible for .fi domain names.
   If the root name server is familiar with name servers responsible for the domain name kallenkalakauppa.fi, the process continues with step 5. If the root name server is familiar with name servers responsible for .fi domain names, the process continues with step 4.
4. After this, the original name server queries one of the .fi name servers that it was informed about for name servers responsible for the domain name kallenkalakauppa.fi.
5. After this, the original name server queries one of the kallenkalakauppa.fi

name servers that it was informed about and receives a response containing the IP address for the domain name kallenkalakauppa.fi.

6. The answer is returned to the client and stored in the name server's cache for a specific period of time. As a result of this, queries for the same domain name or other name servers included in the chain can be answered without going through the whole process from start to finish again.

The client's name server sends a recursive query on the client's behalf (steps 3–5) and thus ensures that a response is received even if it requires querying multiple name servers.

The organisation responsible for the authoritative name service of a given domain name (in this example a fictional company, Example Ltd, with the domain name kallenkalakauppa.fi) is responsible for supplying recursive name servers with the information concerning all the names of the domain name.

Finnish Transport and Communications Agency Traficom

PO Box 320, FI-00059 TRAFICOM
tel. +358 (0)29 534 5000

traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto