CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DNSSEC INTEGRATION & IMPLEMENTATION.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Content

DOCUMENT CONTROL AND REVIEW

Document control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

GLOSSARY

DNS resolver	A DNS resolver is an essential part of the Domain Name System (DNS). It is software responsible for translating domain names into numeric IP addresses.
Amplification attacks	are a type of Distributed Denial of Service (DDoS) attack in which the attacker sends a small amount of traffic to a server or service, which then generates a much larger amount of traffic to a target. This results in "amplifying" the effect of the attack, allowing the target to be overwhelmed without the attacker needing many resources.

Introduction: why implement DNSSEC?

The Domain Name System (DNS) is an indispensable core of the Internet. Every online request-from opening a website to sending an e-mail-begins with a DNS query. Unfortunately, DNS was not originally designed with security as a priority, making it vulnerable to various cyber attacks. DNSSEC (Domain Name System Security Extensions) addresses these shortcomings and plays a vital role in ensuring the integrity of the modern internet. Here are the main reasons to implement DNSSEC:

1. Protection against critical DNS attacks

1.1 PROTECTION AGAINST MAN-IN-THE-MIDDLE ATTACKS

In a man-in-the-middle attack, an attacker intercepts DNS requests and modifies the responses to mislead users. With DNSSEC, DNS responses are cryptographically validated, making manipulation in transit impossible.
DNS spoofing, also known as DNS cache poisoning,.

- This leads to:
    - Traffic redirection: Users are directed to malicious websites without realising it.
    - Data interception: As a result of redirection, attackers can steal sensitive data such as passwords and credit card details.

DNSSEC prevents such attacks by providing DNS answers with digital signatures. This allows resolvers to verify that the data received is authentic

1.2 DEFENCE AGAINST BRUTE-FORCE ON NON-EXISTENT DOMAINS

DNS attacks, such as "NXDOMAIN flooding", try to overwhelm resolvers by asking for non-existent domains. DNS servers performing DNSSEC validation can use NSEC/NSEC3 records* to efficiently prove that a domain does not exist without additional burden.

2. Strengthening trust and credibility

2.1 TRUST AMONG USERS

Users want to be sure they are connecting to the real website or service they are referring to. By implementing DNSSEC, an organisation strengthens the credibility of its domain and reduces the risk of fraud. After all, an insecure Internet service causes both reputational and financial damage. This is important for internet users, this because the internet is increasingly used as a platform for storing valuable information and conducting financial transactions. Think of online banking, online investing and payments at online shops. DNSSEC is a guarantee for users that their internet traffic arrives at the right place.

2.2 LEGAL AND REGULATORY COMPLIANCE

In certain sectors, such as financial services, healthcare and government, security standards are often mandatory. DNSSEC can help meet compliance requirements, such as NIS2 by ensuring the integrity of DNS requests.

*See 9.3 in this guide for more details

3. Basis for advanced security protocols

DNSSEC is more than a stand-alone security technology. It provides a foundation for new and additional security protocols, such as:

3.1 DANE (DNS-BASED AUTHENTICATION OF NAMED ENTITIES).

DNSSEC enables DANE, a protocol that improves the trustworthiness of SSL/TLS certificates. DANE allows a domain owner to capture a specific TLS certificate chain in DNSSEC-signed records, which prevents certificate forgery.

3.2 AUTHENTICATION FOR EMAIL (E.G. WITH TLSA RECORDS)

DNSSEC allows mail servers to use cryptographically validated records, which strengthens security mechanisms such as MTA-STS and STARTTLS.

3.3 IOT SECURITY

With the growth of IoT, there is an urgent need for lightweight, scalable security solutions. DNSSEC fills this gap by securing DNS requests against tampering, which is essential for ensuring reliable communication between IoT devices and their servers. As a result, DNSSEC provides a robust layer of security in ecosystems where traditional methods are not feasible or effective.

4. Protecting corporate reputation

4.1 PREVENTING REPUTATIONAL DAMAGE

A successful DNS attack, such as redirecting a website to a fraudulent page, can cause serious damage to an organisation's reputation. Customers lose trust in the company's reliability, leading to immediate financial losses and long-term reputational damage.

4.2 LIMITING LEGAL LIABILITY

Organisations that fail to implement security measures such as DNSSEC risk being held liable for data breaches or fraud. By using DNSSEC, you reduce the risk of legal complications.

5. Operational benefits

5.1 STRENGTHENING INTERNAL IT PROCESSES

DNSSEC forces organisations to gain a detailed overview of their DNS infrastructure. This often leads to improved internal processes and management standards, such as key management and monitoring.

5.2 COMPATIBILITY WITH MODERN TECHNOLOGIES

With more and more devices and applications supporting DNSSEC, DNSSEC is crucial to ensure the authenticity of DNS messages.

6. Future-proofing

6.1 EXPECTED STANDARDISATION

With the growing threat of cyber attacks, it is likely that DNSSEC will eventually become a mandatory standard for all domains. By implementing early, organisations can get a head start and minimise future migration costs.

6.2 READINESS FOR QUANTUM COMPUTING

The cryptographic algorithms that DNSSEC supports can be adapted to quantum-resistant variants, making it a sustainable long-term investment.

7. Summary of benefits

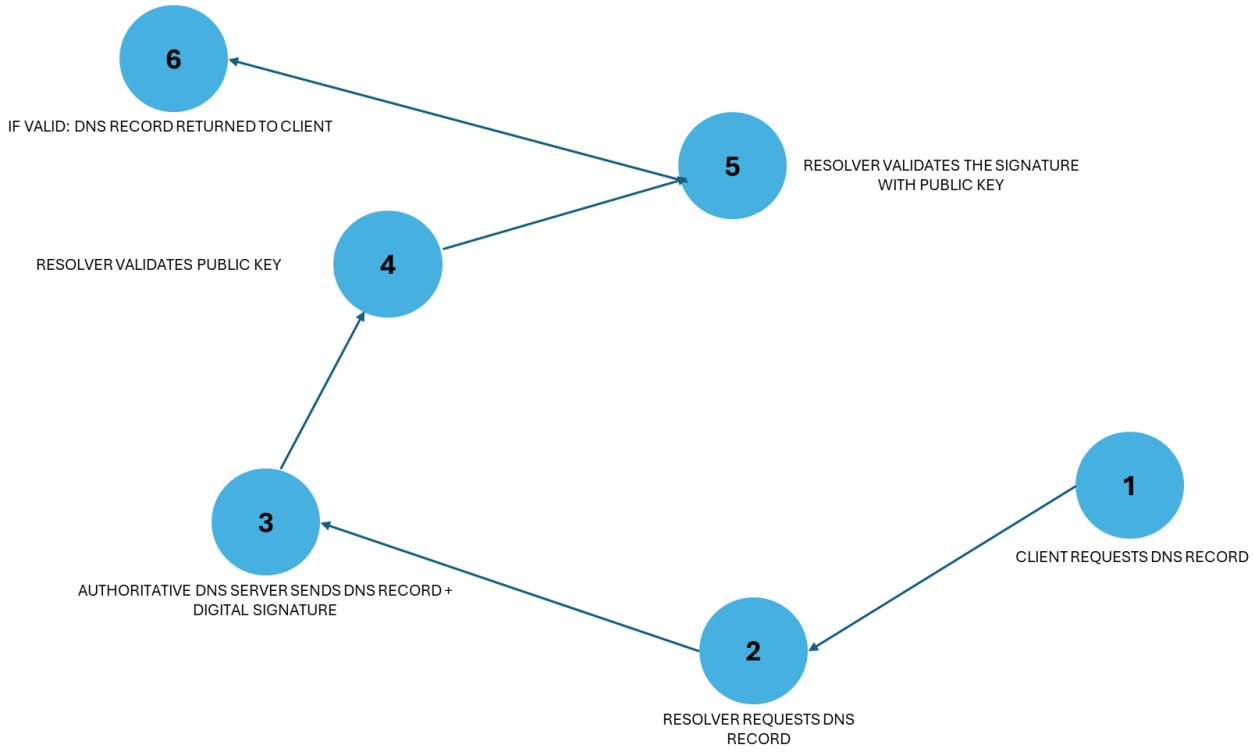
Category	Benefits
Security	Protection against DNS spoofing, cache poisoning and man-in-the-middle attacks
Trust	Increases user trust, regulatory compliance
Innovation	Foundation for technologies such as DANE and IoT security
Reputation	Prevents damage from DNS-related incidents.
Future-proofing	Readiness for future standards.

8. Decision

With DNSSEC, an organisation invests in robust security and strengthens the reliability of its domain. In an era of increasing cyber threats, DNSSEC is not just an addition to existing security measures, but a basic requirement

9. How does DNSSEC work technically?

Technical diagram: How DNSSEC works



9.1 SCHEME EXPLANATION

1.CLIENT REQUESTS DNS RECORD

The **client** (e.g. a web browser) sends a request to a DNS resolver to retrieve the IP address information of a domain name (e.g. example.com).

- **Role of DNSSEC**: No security applied yet in this step; the request is a standard DNS query.

2. RESOLVER REQUESTS DNS RECORD

The resolver (often an ISP's DNS server) forwards the request to the **authoritative DNS server** responsible for the domain.

- **Role of DNSSEC**: The authoritative server is configured with DNSSEC and knows that the DNS record must be secure.

3. AUTHORITATIVE DNS SERVER SENDS DNS RECORD + DIGITAL SIGNATURE

The authoritative DNS server returns the requested DNS record along with a **digital signature** (an RRSIG record). This signature is generated using a private key.

- **Important**:
  - The signature guarantees that the DNS record is authentic and has not been modified in transit.
  - The public key required to verify this signature is published in a DNSKEY record.

4. RESOLVER VALIDATES PUBLIC KEY

The resolver does the following actions:

- The resolver retrieves the corresponding **public key** (DNSKEY record) via DNS.
- The **DS** (Delegation Signer) **records** and respective signature in the parent zone (e.g. .be) prove that the public key is valid.
- This process repeats up to the **root zone**, whose public key is already established as trustworthy (the "trust anchor").

- The resolver retrieves the corresponding **public key** (DNSKEY record) via DNS.

5. RESOLVER VALIDATES THE SIGNATURE WITH PUBLIC KEY

The resolver validates the received signature. To do this, the resolver checks whether the signature is valid.

6. IF VALID: DNS RECORD RETURNED TO CLIENT

If all checks are successful, the resolver returns the original DNS record to the client.

If the validation fails (e.g. due to a signature mismatch), an error is returned and the client does not receive a DNS response

9.2 THE BASIC PRINCIPLES

DNSSEC works through a hierarchical system of digital signatures and public keys:

1. **Zone lists and records**:
    - DNS records are provided with a digital signature. The signature is generated with a private key.
    - The corresponding public key is stored in a DNSKEY record in the same zone.
2. **Validation through a chain of trust**:
    - To ensure the integrity of DNS responses, dnssec-enabled resolvers validate the signature against the public key.
    - This process goes up hierarchically in the DNS tree structure (e.g. from domain → TLD → root).

9.3 TECHNICAL COMPONENTS

1. **DNSKEY records**:
    - Contains the public key of the zone.
    - Two types of keys:
        - **ZSK (Zone Signing Key)**: Signs DNS records within the zone.
        - **KSK (Key Signing Key)**: Signs the ZSK to strengthen the chain of trust.
2. **RRSIG records**:
    - Each DNS record in a zone has an associated RRSIG record that contains the digital signature.
3. **Delegation Signer (DS) records**:
    - Are used to create a chain of trust between a child zone and the parent zone (e.g. between a domain and its TLD).
4. **NSEC/NSEC3 records**:
    - Used to cryptographically verify that a record does not exist.
    - Provide security against brute-force attacks on non-existent domains. (not globally enabled by default)
    - NSEC displays the next available domain, while NSEC3 uses hashing for additional security.

9.4 THE VALIDATION PROCESS

1. A DNS resolver asks for the DNS records of a domain.
2. The records are returned along with their RRSIG records.
3. The resolver checks:
    - Whether there is one or more DS for the zone in the parent
    - Whether the signature matches the DNSKEY.
    - Whether the DNSKEY is legitimate, by validating it via the DS records in the parent zone.
    - No DS => NO validation
4. The process repeats until the root zone, whose public key is known and serves as a trusted anchor.

10. Implementation steps

10.1 PREPARATION

1. **Check DNSSEC support**:
    - Make sure your DNS provider or nameserver software supports DNSSEC (e.g. BIND, Knot or NSD as authoritative DNS software and BIND or Unbound as DNS resolver software).).
2. **Generate keys**:
    - Create a KSK and ZSK using DNSSEC tools. With BIND, this can be done via the command:

      dnssec-keygen -a RSASHA256 -f KSK -b 2048 -n ZONE example.com
      dnssec-keygen -a RSASHA256 -b 2048 -n ZONE example.com

3. **Publish the public key**:
    - Add the DNSKEY records to your DNS zone file.

10.2 CONFIGURATION

1. **Sign the zone**:
    - Use a tool such as dnssec-signzone to sign the zonefile:

      dnssec-signzone -K /path/to/keydir -o example.com -t example.com.zone

      example: If you have stored the keys in /etc/dnssec/keys/ and have a zone file example.com.zone, the command looks like this:

      dnssec-signzone -K /etc/dnssec/keys/ -o example.com -t example.com.zone

2. **Configure the parent zone**:
    - Upload the DS record to your TLD provider to form the chain of trust.
3. **Update resolvers**:
    - Configure your resolvers to use DNSSEC validation. For Unbound, you can enable this with:

      server: auto-trust-anchor-file: "/var/lib/unbound/root.key"

10.3 TEST AND CHECK THE STATUS OF A DNS ZONE (DNSVIZ.NET)

CHECK THE CONFIGURATION WITH TOOLS SUCH AS:

- dnssec-debugger.verisignlabs.com
- dig +dnssec example.com

11. Advantages and disadvantages

11.1 ADVANTAGES

1. **Protection against tampering**:
    - DNSSEC prevents attacks such as cache poisoning and DNS spoofing.
2. **Foundation for further security**:
    - DNSSEC is a foundation for technologies such as DANE (e.g. for email security via TLSA records).
3. **Increased trust**:
    - Users and systems can trust that DNS data is authentic.

11.2 DISADVANTAGES

1. **Complexity**:
    - Key management and zone signing require expertise.

2. **Larger DNS packets**:
    - Additional records (RRSIG, DNSKEY, NSEC) make DNS responses larger, causing potential problems with legacy systems.

3. **Amplifications** attacks can take advantage of this.
   How DNSSEC is specifically used in amplification attacks

    - High responses due to DNSSEC:

        - DNSKEY records: Contains the public keys and can be very large (especially when using strong cryptography such as RSA 2048).
        - RRSIG records: Digital signatures for each DNSSEC-protected zone.
        - NSEC/NSEC3 records: Recordsets indicating the next name in the zone, used for protection against zone-walking, but also large in size.

    - Open resolvers:

        - Attackers use poorly configured open resolvers, which accept DNS queries from anyone.
        - These resolvers send responses back to the target with the large DNSSEC records.

    - Amplification factor:

        - The ratio between the size of the input (DNS query) and the output (DNS response) is called amplification factor.
        - With DNSSEC, these amplification factors can be as high as 50x or more. For example, a query of 60 bytes can generate a response of 3000 bytes.

4. **No encryption**:
    - DNSSEC only protects integrity and authenticity; data is not encrypted.
5. Zone walking:
    - Because of NSEC, there is the possibility that zone content can be enumerated. In some situations, this may not be desirable. NSEC3 makes zone enumeration significantly more difficult.

12. Best practices for DNSSEC

1. **Use secure algorithms**:
   - Choose modern algorithms in accordance with recommendations RFC 8624 (e.g. ECDSAP256SHA256.)

2. **Regular key management**:
   - Rotate ZSKs every 3-6 months and KSKs annually.

3. **Check configuration regularly**:
   - Implement active monitoring to check for expired signatures and keys.

4. **Implement fallback options**:
   - Configure resolvers to handle DNSSEC validation issues without service interruptions.

13. Cost and maintenance

- **DNSSEC configuration**:
  - Initial configuration: 5-15 hours of work depending on complexity.
  - Maintenance: Periodic rotation of keys, updates to zone files.

- **Cost indication**:
  - **Small domains**: ~€100-€300 per year.
  - **Large organisations**: Additional costs for staff, training and monitoring.

Disclaimer