DNSSEC Policy and Practice Statement (DPS)

Publishing Entity: Atak Domain Bilgi Teknolojileri A.Ş.
Document Type: DNSSEC Policy and Practice Statement (DPS)
Scope: All domain name registration services provided by Atak Domain
Standards: ICANN DNSSEC, RAA 2013/2019, RFC 6841, RFC 4033–4035, registry-specific DNSSEC policies

1. Purpose and Scope

This DNSSEC Policy and Practice Statement ("DPS") has been prepared to define all technical, administrative, and operational processes related to the use of DNS Security Extensions (DNSSEC) within Atak Domain's domain registration services.

This statement explains:

- How DNSSEC support is implemented
- How DNSSEC key management is handled by the customer
- The DS record processing workflow
- Security, key rotation, and signing methods

This DPS applies to .COM, .NET, .ORG, .BIZ, .INFO, gTLDs, and any DNSSEC-enabled ccTLDs.

2. Overview of DNSSEC

DNSSEC:

- Protects the integrity of DNS records
- Ensures the authenticity of DNS responses
- Prevents forged DNS responses (cache poisoning, spoofing)

DNSSEC is **not** an encryption system; it provides signing and validation mechanisms only.

3. Roles and Responsibilities

3.1. Atak Domain (Registrar)

Atak Domain is responsible for:

destek@atakdomain.com atakdomain.com İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR

- Submitting DS records received from the customer to the respective registry
- Facilitating DNSSEC-supported domain operations to the extent technically possible
- Performing integrity checks to ensure correct data submission

Atak Domain does **not** provide DNS signing services (DNS hosting remains with the registry operator or the customer).

3.2. Customer (Registrant / Domain Owner)

The customer is responsible for:

- Generating, managing, and storing DNSSEC keys
- Issues arising from incorrect or incomplete DS records
- Managing the DNS signing infrastructure of their DNS hosting provider

3.3. Registry Operators

Registry operators vary by TLD (Verisign, PIR, Identity Digital, Nominet, etc.).
Registries:

- Publish DS records into the parent zone
- Form the upper layer of the DNSSEC trust chain

4. DNSSEC-Supported TLDs

Atak Domain works with the following DNSSEC-enabled extensions:

- .com, .net, .org
- .biz, .info, .mobi
- Many new gTLDs (.online, .app, .shop, etc.)
- DNSSEC-enabled ccTLDs

The supported list may vary according to registry policies.

5. DS Record Processing Workflow

5.1. Submission of DS Records

The customer provides the following:

- Key Tag
- Algorithm
- Digest Type
- Digest Hash

Atak Domain submits this information to the relevant registry.

5.2. Validation

Atak Domain performs checks including:

- Correct format of the DS record
- DNSSEC support availability for the TLD
- Domain status (must be active)

5.3. Publication

The registry publishes the DS record in the TLD zone.
The DNSSEC trust chain is completed.

5.4. Removal of DS Records

Upon customer request, DS records may be removed.
This may break the DNSSEC validation chain.

6. Security and Key Management Policy

Atak Domain:

- Does not store customer KSK/ZSK keys
- Does not generate or manage DNSSEC keys
- Only provides an interface for submitting DS records to the registry

6.1. Registry Security Requirements

Registry operators use industry-standard security measures, including:

- Hardware Security Modules (HSM)
- Secure key storage
- Regular key rotation
- 24/7 monitoring

6.2. Customer-Side Security Responsibilities

The customer must:

- Use strong cryptographic keys
- Select algorithms supported by their DNS provider
- Store keys in a secure environment
- Update the DS record during key rotation

7. Key Algorithms and Technical Standards

Supported DNSSEC algorithms include:

- RSA/SHA-256 (Algorithm 8)
- RSA/SHA-512 (Algorithm 10)
- ECDSA Curve P-256 (Algorithm 13)
- ECDSA Curve P-384 (Algorithm 14)
- Ed25519 / Ed448 (Algorithms 15/16 – depending on TLD support)

Atak Domain accepts only algorithms supported by the registry.

8. Incorrect DS Records and Outage Conditions

The following may cause the domain to become completely unreachable:

- Incorrect DS record submission
- DNS provider using an unsigned DNS server
- Failure to update DS records during KSK rotation
- Zone signing errors

In such cases, Atak Domain:

- Performs technical analysis
- Provides correct record information to the customer
- Cannot directly fix signing infrastructure issues (as it does not manage DNS hosting)

9. Data Protection and Privacy

Within the DNSSEC process:

- Only technical DS data is processed
- No personal data is involved
- All operations comply with the Atak Domain Privacy Policy and Data Processing Agreement

10. Operational Processes and Availability

Atak Domain:

- Processes DS records via a 24/7 technical operations center
- Responds to DNSSEC requests within a reasonable timeframe
- Notifies customers if registry systems are temporarily inaccessible

11. Customer Support Processes

DNSSEC request contact details:

Email:
support@atakdomain.com
destek@atakdomain.com

Supported operations:

- Adding a DS record
- Updating a DS record
- Removing a DS record
- Verifying TLD DNSSEC support

Unsupported operations:

- DNS signing
- Key generation
- Zone management
- Technical settings of the hosting/DNS provider

12. Policy Updates

Atak Domain reserves the right to update this DPS in line with:

- ICANN requirements
- Registry policy changes
- Technical standard updates

Updates take effect immediately upon publication on the website.

13. Effective Date

This DPS applies to all customers who use DNSSEC for domain management through Atak Domain.