

DNSSEC Politika ve Uygulama Beyanı

Yayınlayan Kuruluş: Atak Domain Bilgi Teknolojileri A.Ş.

Belge Tipi: DNSSEC Politika ve Uygulama Beyanı (DPS)

Kapsam: Atak Domain tarafından sunulan tüm alan adı kayıt hizmetleri

Standartlar: ICANN DNSSEC, RAA 2013/2019, RFC 6841, RFC 4033–4035, registry-specific DNSSEC policies

1. Amaç ve Kapsam

Bu DNSSEC Politika ve Uygulama Beyanı (“DPS”), Atak Domain’in sunduğu alan adı kayıt hizmetlerinde DNS Security Extensions (DNSSEC) kullanımına ilişkin tüm teknik, idari ve operasyonel süreçleri tanımlamak amacıyla hazırlanmıştır.

Bu beyan:

- DNSSEC desteğinin nasıl uygulanacağını,
- müşteri tarafında DNSSEC anahtar yönetiminin nasıl yapılacağını,
- DS kayıtlarının işleme süreçlerini,
- güvenlik, anahtar rotasyonu ve imzalama yöntemlerini

1

açıklar.

Bu DPS; .COM, .NET, .ORG, .BIZ, .INFO, gTLD’ler ve DNSSEC destekleyen ccTLD’ler için geçerlidir.

2. DNSSEC Hakkında Genel Bilgi

DNSSEC:

- DNS kayıtlarının bütünlüğünü korur,
- cevapların doğruluğunu garanti eder,
- sahte DNS yanıtlarını (cache poisoning, spoofing) engeller.

DNSSEC **şifreleme amaçlı değildir**, yalnızca imzalama ve doğrulama mekanizması sağlar.

3. Roller ve Sorumluluklar

3.1. Atak Domain (Registrar)

Atak Domain:

- müşteriden alınan DS kayıtlarını ilgili registry’e iletmekten,

- DNSSEC destekleyen domainler için teknik olduğu ölçüde aracılık etmekten,
- veri bütünlüğünü korumak için gerekli kontrolleri yapmaktan

sorumludur.

Atak Domain **DNS imzalama hizmeti sunmaz** (DNS hosting kayıt operatöründe veya müşteridedir).

3.2. Müşteri (Registran / Domain Sahibi)

Müşteri:

- DNSSEC anahtarlarını üretmekten, yönetmekten ve saklamaktan,
- hatalı veya eksik DS kayıtları nedeniyle oluşacak kesintilerden,
- kendi DNS sağlayıcısının imzalama altyapısını yönetmekten

sorumludur.

3.3. Registry Operatörleri

TLD'ye göre değişir (Verisign, PIR, Identity Digital, Nominet vb.).

Registry:

- DS kayıtlarını kök zone'a yayınlam,
- DNSSEC zincirinin üst seviyesini oluşturur.

2

4. DNSSEC Desteklenen TLD'ler

Atak Domain aşağıdaki DNSSEC destekli uzantılarla çalışır:

- .com, .net, .org
- .biz, .info, .mobi
- birçok yeni gTLD (.online, .app, .shop vb.)
- DNSSEC destekleyen ccTLD'ler

Destek listesi registry politikalarına göre değişebilir.

5. DS Kaydı İşleme Süreci

5.1. DS kaydı gönderimi

Müşteri aşağıdaki bilgileri sağlar:

- Key Tag
- Algorithm

- Digest Type
- Digest Hash

Atak Domain bu bilgiyi ilgili registry'ye iletir.

5.2. Doğrulama

Atak Domain şu kontrolleri yapar:

- DS formatının doğru olup olmadığı
- DNSSEC desteklenip desteklenmediği
- alan adının aktif durumda olması

5.3. Yayınlama

Registry, DS kaydını zone'a ekler.

DNSSEC zinciri tamamlanır.

5.4. DS kaydı kaldırma

Müşteri talep ettiğinde DS kaydı registry'den silinir.

Bu işlem, doğrulama zincirinin kopmasına sebep olabilir.

6. Güvenlik ve Anahtar Yönetimi Politikası

3

Atak Domain:

- müşterinin KSK/ZSK anahtarlarını saklamaz,
- anahtar üretmez veya yönetmez,
- yalnızca DS kaydının registry'e aktarılması için bir arayüz sağlar.

6.1. Registry güvenlik gereklilikleri

Registry operatörleri:

- HSM (Hardware Security Module)
- güvenli anahtar depolama
- düzenli anahtar rotasyonu
- 7/24 izleme

gibi endüstri standardı güvenlik önlemleri kullanır.

6.2. Müşteri tarafı güvenlik sorumluluğu

Müşteri:

- güçlü anahtarlar kullanılmalıdır,
- DNS sağlayıcısının desteklediği algoritmaları seçmelidir,
- anahtarlarını güvenli ortamda saklamalıdır,
- anahtar rotasyonu gerektiğinde DS kaydını güncellemelidir.

7. Anahtar Algoritmaları ve Teknik Standartlar

DNSSEC için geçerli algoritmalar:

- RSA/SHA-256 (Algoritma 8)
- RSA/SHA-512 (Algoritma 10)
- ECDSA Curve P-256 (Algoritma 13)
- ECDSA Curve P-384 (Algoritma 14)
- Ed25519 / Ed448 (Algoritma 15/16 – TLD destek durumuna bağlı)

Atak Domain yalnızca registry'nin desteklediği algoritmaları kabul eder.

8. Hatalı DS Kaydı ve Kesinti Durumları

Aşağıdaki durumlar alan adının tamamen erişilemez olmasına neden olabilir:

- yanlış DS kaydı girilmesi
- DNS sağlayıcısının imzasız DNS sunucusu kullanması
- KSK rotasyonunda DS kaydının güncellenmemesi
- zone imzalama hataları

Bu durumlarda Atak Domain:

- teknik inceleme yapar,
- doğru kayıtları müşteriye bildirir,
- ancak imzalama altyapısını yönetmediği için doğrudan düzeltme yapamaz.

9. Veri Koruma ve Gizlilik

DNSSEC sürecinde:

- yalnızca teknik DS verileri işlenir,
- kişisel veri içermeyen bir süreçtir,
- tüm işlemler Atak Domain Gizlilik Politikası ve DPA'ya uygundur.

10. Operasyonel Süreçler ve Erişilebilirlik

Atak Domain:

- DS kayıtlarını **7/24** teknik operasyon merkezi üzerinden işler,
- DNSSEC ile ilgili taleplere makul süre içinde yanıt verir,
- registry sistemleri erişilebilir olmadığında müşteriyi bilgilendirir.

11. Müşteri Destek Süreçleri

DNSSEC ile ilgili talepler için iletişim adresleri:

E-posta:

support@atakdomain.com

destek@atakdomain.com

Destek verilen işlemler:

- DS kaydı ekleme
- DS kaydı güncelleme
- DS kaydı kaldırma
- TLD destek bilgisinin doğrulanması

Destek verilmeyen işlemler:

- DNS imzalama
- anahtar üretimi
- zone yönetimi
- hosting/dns sağlayıcısının teknik ayarları

12. Politika Güncellemeleri

Atak Domain, bu DPS belgesini:

- ICANN gereklilikleri,
- registry politikaları,
- teknik standartlar değiştiğinde

güncelleme hakkını saklı tutar.

Güncellemeler web sitesinde yayınlandığı anda yürürlüğe girer.

13. Yürürlük

Bu DPS, Atak Domain üzerinden DNSSEC kullanarak alan adı yöneten tüm müşteriler için geçerlidir.