KUZEY KIBRIS TÜRK CUMHURİYETİ

# RESMÎ GAZETE

| Sayı : 276 | 22 Aralık 2021, Çarşamba | Sayfa: 1063 |
|---|---|---|

**BİLDİRİ**

Resmi Gazete'nin bu sayısı aşağıdaki Ek'leri ihtiva etmektedir.

**Sayfa**



KKTC Devlet Basımevinde basılmıştır.

KUZEY KIBRIS TÜRK CUMHURİYETİ
RESMÎ GAZETE

Sayı : 276 EK III 22 Aralık, 2021
TEBLİĞ VE İLANLAR

Sayı : 969

**Trafik Bilgisi Teknik Detay Uygulama Usullerine İlişkin Tebliğ**

**Bilişim Suçları Yasası**

**32/2020 Sayılı Yasa**

Bilgi Teknolojileri ve Haberleşme Kurumu Yönetim Kurulu, 32/2020 sayılı Bilişim Suçları Yasası uyarınca hazırlanan ve 07.09.2021 tarih ve R.G 197 sayısı ile Resmi Gazete'de yayımlanarak yürürlüğe giren Bilişim Suçları Tüzüğü'nün 13'üncü maddesinin kendisine verdiği yetkiyi kullanarak aşağıdaki Tebliği yapar:

**Kısa İsim**

**Madde -1**

Bu Tebliğ "**Trafik Bilgisi Teknik Detay Uygulama Usullerine İlişkin Tebliğ**" olarak isimlendirilir.

**Amaç ve Kapsam**

**Madde - 2**

Bu tebliğ, trafik bilgisini içeren dosya ve/veya dosyaların isimlendirme standartları, veri alanları, açıklamaları ve formatı ile dosya yapılandırılmasında dikkat edilecek hususların ayrıntılı olarak açıklanması amacıyla Kurul kararı ile yayımlanmıştır.

**Tefsir**

**Madde - 3**

(1) "Erişim Sağlayıcı", kullanıcılarına elektronik haberleşme şebekesine erişim olanağı sağlayan elektronik haberleşme hizmet sağlayıcılarını anlatır.
"Kurum", Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK)'nu anlatır.
"NAT", Ağ Adres Dönüşümü (Network Address Translation) anlatır.
"NTP Sunucu", Ağ zaman sunucusu (Network Time Protocol Sunucusu) anlatır.
"RFCs" , İnternet için başlıca standart belirleme kuruluşu (Request for Comments) anlatır.

"Trafik Bilgisi", içerik hariç olmak üzere, elektronik haberleşme şebekesinde gerçekleştirilen her türlü erişime ilişkin olarak tarafları, zamanı, süreyi, yararlanılan hizmetin türünü, aktarılan veri miktarı ve bağlantı noktalarını anlatır.

"Tüzük"; Bilişim Suçları Tüzüğü'nü anlatır.

"Yasa", 32/2020 sayılı Bilişim Suçları Yasası'nı anlatır.

(2) Bu Tebliğ'de geçen ve yukarıda yer almayan tanım ve kısaltmalar için Yasa ve Tüzükte yer alan tanım ve kısaltmalar geçerlidir.

**Erişim Sağlayıcıları Tarafından Uyulması Gereken Hususlar**

**Madde - 4**

(1) Abonelerini NAT'layarak internete çıkaracak olan erişim sağlayıcıları her bir kullanıcı için haberleşmenin gerçekleştiği zaman aralığında diğer herhangi bir kullanıcıya tahsis edilmemiş benzersiz (unique) portlar atamaları gerekmektedir.

(2) Trafik bilgisi üreten veya bu süreçte kullanılan cihazlar, NTP sunucusu ile senkronize olarak çalışması zorunludur. Trafik dosyalarına işlenecek zaman bilgisi NTP sunucusundan alınan gerçek zaman olacaktır.

(3) Dosyaların isimlendirilmesine ve içeriğinin oluşturulmasına ait format (desen) bu dokümanda belirtildiği şekilde uygulanacaktır.

(4) Trafik dosyaları işbu Tebliğ'de belirtilen usul ve esaslara uygun olarak oluşturulacak ve kaydedilecektir.

(5) Dosya isimlerinde ve kayıtlarında yer alan tarih değerleri KKTC yerel saatine uygun olarak kaydedilmelidir.

(6) Trafik bilgilerini içeren ve GNU zip (gzip) ile sıkıştırılmış dosyalar, dosya içerisinde ilk oluşturulan trafik bilgisine ait tarih ve saatten itibaren en fazla 12 saat içerisinde zaman damgalı olarak imzalanıp saklanması gerekmektedir.

**Trafik Bilgisi Dosyalarının isimlendirilmesi**

**Madde - 5**

(1) **Trafik Dosyası İsimlendirme Formatı:** Trafik dosyası aşağıda sunulan şablona uygun olarak oluşturulmalıdır. Dosya isimlendirmesinde Türkçe karakter **kullanılmamalıdır.**

"ERISIMSAGLAYICINO_TRAFIK_YYYYMMDDHHMISS_MINTAR_MAXTAR_CNT.log.gz"

Trafik dosyası isimlendirme formatında geçen alanlar:

(A) ERISIMSAGLAYICINO: Trafik bilgisini oluşturan erişim sağlayıcıyı belirtmektedir. Kurum tarafından yetkilendirilen internet servis sağlayıcıya (erişim sağlayıcının) Kurum tarafından verilen numarayı anlatmaktadır. (Örn: 12345_ISS)

(B) TRAFIK: Bu ifade belirtildiği şekilde kalmalıdır.

(C) TARIH_ZAMAN: Bu alana girilecek olan tarih değeri "YYYYMMDDHHMISS" deseninde olmalıdır.

(a) YYYY deseni dört basamak olarak yılı (örneğin 2021 gibi)

(b) MM deseni iki basamak olarak ayı (örneğin 06 gibi)

(c) DD deseni iki basamak olarak günü (örneğin 05 gibi)

(d) HH deseni iki basamaklı ve 24 saat formatında saati (örneğin 18 gibi)

(e) MI deseni iki basamak olarak dakikayı (örneğin 18)

(f) SS deseni iki basamak olarak saniyeyi (örneğin 18)

(D) Örnek bir tarih değeri "20210605181221" şeklindedir.

(E) MINTAR: Bu alana girilecek olan tarih değeri "YYYYMMDDHHMISS" deseninde olmalıdır, dosya içeriğindeki kayıtların minimum başlangıç zamanını bildirir.

(F) MAXTAR: Bu alana girilecek olan tarih değeri "YYYYMMDDHHMISS" deseninde olmalıdır, dosya içeriğindeki kayıtların maksimum başlangıç zamanını bildirir.

(G) CNT (Count): Bu değer aynı gün içinde birden fazla dosya atılması durumunda her dosya için arttırılmalıdır. Rakamla üç hane olacak şekilde yazılmalıdır (Örn:002). Bu dosyayı üretecek birden fazla şebeke elemanı olması halinde CNT bilgisinin başına 5 haneyi geçmeyecek şekilde erişim sağlayıcı şebeke elemanı kodunu girecektir. (Örn: PRSR1_002)

(H) Örnek dosya isimi:

"12345_ISS_TRAFIK_20210315162500_20210315162501_20210415162530_001.log.gz"

**(2) Trafik Dosyası Uzantısı:** Trafik dosyasının uzantısı ".log" olmalıdır. Dosya uzantısı küçük harfler ile yazılmalıdır.

**(3) Trafik Dosyası Sıkıştırma Formatı:** Dosyalarda yer alan kayıtlar, öncelikle, en eski zaman ve tarihten en yeni zaman ve tarihe göre sıralanmalı, ardından GNU zip (gzip) sıkıştırma algoritması ile sıkıştırılmalıdır. Sıkıştırma işlemi yapıldıktan sonra dosyanın isim formatı aşağıda görüldüğü gibi olmalıdır.

"12345_ISS_TRAFIK_20210315162500_20210315162500_20210415162500_001.log.gz"

**(4) Trafik Dosyalarının İçeriği**

(A) Trafik dosyalarının içinde bulunan kayıtlar için;

(a) Her kayıt için bir satır oluşturulmalıdır.

(b) Bir kaydın, birden fazla satırda olmaması gerekmektedir.

(c) Trafik kayıtları ortadan bölünmeden, bir bütün olarak kaydedilmelidir.

(B) Kayıtlardaki kolonlar "|" (pipe) işareti ile ayrılmalı ve bu "|" (pipe) işareti ayraç alanı dışında kesinlikle kullanılmamalıdır.

(C) Her bir anlamlı kayıt satırı "\n" (satır sonu) karakteri ile ayrılmalıdır.

(D) IP adresleri noktalı olarak (dotted decimal, Örn: 8.8.8.8) yazılmalıdır.

(E) Port numaraları rakamla girilmelidir.

(F) Sadece Delete (Stop) paketleri değil, Create (Start) ve Interim paketleri de gönderilmelidir.

(G) Trafik bilgilerinin içerisinde yer alan verilerde aşağıdaki özel karakterler kesinlikle bulunmamalıdır.

(a) (;) Noktalı Virgül, (') Single Quote, (") Double Quote, (\) Backslash, Newline, Tab, Backspace, Form Feed, Vertical Tab, Carriage Return (\r, satır başı)

**Trafik Bilgisi Veri Deseni Yapısı ve Dosya İçerikleri**

**Madde - 6**

(1) Her bir satır 16 kolondan oluşmalıdır.

(2) Her kolon "|" (pipe) karakteri ile (hexadecimal değeri 7C) ayrılmalıdır.

(3) Boş bırakılan alan olması durumunda bu alan yine "pipe" kullanılarak belirtilmelidir.

(4) Dosya içerikleri UTF-8 karakter kodlaması kullanılarak hazırlanmalıdır.

**Trafik Bilgisi Formatı Ve Detayları**

**Madde- 7**

(1) Trafik bilgileri içerisinde yer alan her bir satır aşağıda belirtilen desen formatında saklanmalıdır. Aşağıda belirtilen desen tek bir anlamlı trafik bilgisi satırını belirtmektedir.

**KULLANICI_ADI@ERISIMSAGLAYICINO|OZEL_IP|OZEL_PORT|GERCEK_IP|GERCEK_PORT|TRAFIK_BASLAMA_TARIH|TRAFIK_SURE|HEDEF_IP|HEDEF_PORT|NETWORK_PROTOKOL|DOWNLOAD_BYTES|UPLOAD_BYTES|OTURUM_ID|NAT_CIHAZ_IP |PACKET_TYPE|DIRECTION**

(A) **KULLANICI_ADI:** Bu alan, trafiği başlatan aboneyi erişim sağlayıcı ağında işaret eden benzersiz ibaredir. Bu ibare, aboneye sözleşmede atanan benzersiz bir numara veya kimlik bilgisi olacaktır. "KULLANICI_ADI" bilgisine yazılacak

olan numara veya kimlik bilgisi, abonenin kim olduğunu ispatlayacak nitelikte olacaktır. Bu alanda yer alan "KULLANICI_ADI" bilgisi, erişim sağlayıcı tarafından Kuruma hali hazırda düzenli bir şekilde gönderilen verilerde bulunuyor ise, bu alanda yer verilecek kullanıcı adı bilgisi Kuruma hali hazırda gönderilen verilerdeki ile aynı olmalıdır. "ERISIMSAGLAYICINO" bilgisi trafik dosyası isimlendirme bölümünde yer alan tanımdaki numara kullanılacaktır.

**(B) OZEL_IP:** Erişim sağlayıcı ağı içerisinde NAT yöntemi ile IP atayan erişim sağlayıcıları için kullanıcıya ait özel (private) IP adresini ifade eder. NAT yöntemi kullanan erişim sağlayıcıları **bu alanı boş bırakamaz ve standart dışı ifadeler kullanamaz.** NAT yöntemi kullanmayan erişim sağlayıcıları bu alanı boş göndermelidir.
(Örn: 10.0.0.10)

**(C) OZEL_PORT:** Özel IP adresinin kaynak port numarasıdır. NAT yöntemi kullanan erişim sağlayıcıları bu alanı **boş bırakamaz ve standart dışı ifadeler kullanamaz.** NAT yöntemi kullanmayan erişim sağlayıcıları bu alanı boş göndermelidir.

**(Ç) GERCEK_IP:** Abonenin internet ortamına çıkarken kullandığı gerçek (public) IP adresini ifade eder.
(Örn: 99.99.99.99)

**(D) GERCEK_PORT:** Gerçek IP adresinin port numarasını ifade etmektedir. Bu alana doğrudan trafiğin gerçekleştiği port değeri yazılmalıdır.
(Örn: 53254)

**(E) TRAFIK_BASLAMA_TARIH:** Trafiğin başlama zamanını ifade eder. YYYYMMDDHHMISS formatında gönderilmelidir.
(Örn: 20210418163000)

**(F) TRAFIK_SURE:** Saniye cinsinden trafiğin süresini ifade eder. Sürenin küsuratlı olması ve/veya küsuratlı saniye olması durumunda, süre yukarı yuvarlanacaktır.

**(G) HEDEF_IP**: Kullanıcının bağlantı yapmak istediği hedef IP adresini ifade eder.
(Örn: 100.100.100.100)

**(H) HEDEF_PORT**: Kullanıcının bağlantı yapmak istediği hedef port numarasını ifade eder.
(Örn:53254)

**(İ) NETWORK_PROTOCOL:** Trafiğin network seviyesindeki protokol bilgisini ifade eder. Asgari TCP ve UDP olmak üzere network seviyesindeki protokollerin bu alanda girilmesi gerekmektedir. UDP: **"17"**, TCP: **"6"**, ICMP: **"1"**, ESP: **"50"** vb.

olarak ilgili RFC'de belirtildiği şekilde gönderilmelidir. **TCP, UDP, ICMP, ESP gibi ifadeler kullanılamaz.**

**(I) DOWNLOAD_BYTES:** Trafiğin "byte" cinsinden indirilen veri miktarını ifade eder (download bilgisi).

**(J) UPLOAD_BYTES:** Trafiğin "byte" cinsinden yüklenen veri miktarını ifade eder (upload bilgisi).

**(K) OTURUM_ID:** Bu alan, belli bir oturum için verilmiş olan tekil değeri (session_id) ifade eder. **Devam eden bir oturum içindeki tüm trafik kayıtları aynı oturum id değerine sahip olmalıdır.**

**(L) NAT_CIHAZ_IP:** NAT kaydının oluştuğu NAT cihazı veya NAT işlevi için kullanılan cihazın IP adresini ifade eder. **NAT cihazı üzerinden trafik kaydı oluşturan erişim sağlayıcılar bu alanı boş gönderemez ve standart dışı ifadeler kullanamaz.**
(Örneğin 10.250.0.10)

**(M) PACKET_TYPE:** Trafiği oluşturan paketin türünü ifade eder. Start:"**1**", Stop:"**2**", Interim-Update:"**3**". Bu alana 1, 2 veya 3 değerlerinden biri girilmelidir. **Start, interim ve stop ifadeleri kullanılamaz.**

**(N) DIRECTION:** Trafiğin akış yönünü ifade eder. Akış yönü; erişim sağlayıcı abonesinin "start ve stop" paketleri yönünden trafiğin kaynağı olması durumunda "Çıkış", trafiğin hedefi olması durumunda ise "Giriş" şeklinde değerlendirilmelidir. Giriş: "**0**", Çıkış: "**1**". Bu alana 0 veya 1 değerlerinden biri girilmelidir. **"Giriş" ya da "Çıkış" ifadeleri kullanılamaz.**

(2) Örnek Trafik Bilgisi Kaydı aşağıda gösterildiği şekilde olmalıdır.

aboneX@12345_ISS|10.0.0.10|45555|99.99.99.99|54444|20210418000000|200|100.100.100.100|80|17|250|83|DDFR-65AC-12EE-FFFF|10.250.0.10|1|0

aboneY@12346_ISS|10.0.10.10|55555|99.11.11.11|50001|20210418000000|200|100.100.100.100|80|6|250|83|DDFR-65AC-12EE-FFFD|10.250.0.10|0|1

**Yürürlüğe Giriş**

**Madde – 8**

İşbu Tebliğ, Resmi Gazete'de yayımlandığı tarihten başlayarak yürürlüğe girer.