



**BİLGİ  
TEKNOLOJİLERİ  
VE İLETİŞİM  
KURUMU**

# **İSS TRAFİK LOGU TEKNİK DETAY DOKÜMANI**

## **AÇIKLAMA:**

Bilindiđi üzere; Kurumumuz 5397 sayılı Kanun kapsamındaki önleyici-istihbari amaçlı ve 5271 sayılı Ceza Muhakemesi Kanununun 135'inci maddesi kapsamındaki adli amaçlı iletişimin tespit edilmesi, dinlenmesi, sinyal bilgilerinin deđerlendirilmesi ve kayda alınmasına yönelik işlemler kapsamında verilen görevleri süresinde, eksiksiz ve herhangi bir aksamaya sebebiyet vermeyecek şekilde yerine getirmekle yükümdür.

Bu bağlamda kullanıcılarına internet hizmeti sađlayan İSS operatörlerinden sundukları hizmet neticesinde oluşan IPDR veri dosyaları alınmaktadır. Hali hazırda alınan oturum verilerine ilave olarak her bir hedef bağlantısı için oluşan trafik kayıtları alınmaya başlanılacaktır. Bu dokümanda alınacak olan trafik kayıtlarını içeren dosyanın isimlendirme standartları, veri alanları, açıklamaları ve formatı ile dosya yapılandırılmasında dikkat edilecek hususlar ayrıntılı olarak açıklanmaktadır. Sunucu IP adresi, FTP/FTPS kullanıcı ve şifresi, abone verilerinin iletileceđi izin bilgileri işletmeciyeye Kurum tarafından bildirilecektir. Bu doküman dört ana bölümden oluşmaktadır.

1. Giriş
2. Trafik log kayıtları dosya isimlendirme standartları
3. Trafik log kayıt alanları
4. Dikkat edilmesi gereken hususlar

Doküman üzerinde anlaşılamayan veya tereddüt oluşturan kısımlar ile karşılaşılmaması halinde Kurum yetkilileri ile irtibata geçilerek problemler giderilmelidir.

**Yayınlama Tarihi** : Aralık 2020

**Versiyon** : Versiyon-2.1

# 1. BÖLÜM

## GİRİŞ

### 1.1. DOKÜMANIN AMACI

11/06/2016 tarih ve 29739 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren ELEKTRONİK HABERLEŞME SEKTÖRÜNE İLİŞKİN YETKİLENDİRME YÖNETMELİĞİ’nde yapılan değişiklikler ile ilgili yönetmeliğin 19. Maddesinin birinci fıkrasının (f) bendinde belirtilen trafik bilgilerinin alınması amaçlanmaktadır.

### 1.2. DOKÜMANIN KAPSAMI

Bu doküman, sunulan internet hizmetine yönelik işletmecilerin hizmetle ilgili Bilgi Teknolojileri ve İletişim Kurumu’na (Kurum) olan yükümlülüklerini belirtmekte, Kurum’a gönderilecek olan dosyaların ve verilerin desen bilgilerini ve veri iletim yapısını tanımlamaktadır.

### 1.3. TANIMLAR ve KISITLAMALAR

- **Kurum:** Bilgi Teknolojileri Ve İletişim Kurumu (BTK)
- **FTP:** File Transfer Protocol (Dosya İletim Protokolü)
- **FTPS:** Secure FTP (Güvenli FTP)
- **NAT:** Network Address Translation (Ağ Adres Dönüşümü)
- **NTP Server :** Network Time Protocol Sunucusu (Ağ zaman sunucusu)
- **IPDR:** Internet Protocol Detail Record (İnternet Protokol İletişim Kaydı)
- **İSS:** İnternet Servis Sağlayıcı

### 1.4. HUKUKİ GEREKÇE

- 14/07/1934 sayılı ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu Ek Madde 7, 10/03/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu Ek Madde 5, 01/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun 6’ncı maddesi.
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
- 11/06/2016 tarihli ve 29739 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği.
- Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar.

### 1.5. DOKÜMANIN KAPSAMI

Bu doküman, kullanıcılarına internet hizmeti sağlamakta olan İSS işletmecilerinin, verecekleri bu hizmetle ilgili Bilgi Teknolojileri Ve İletişim Kurumu’na (Kurum) olan yükümlülüklerini belirtmekte, Kurum’a gönderilecek olan verilerin desen bilgilerini ve veri iletim yapısını tanımlamaktadır.

Elektronik haberleşme hizmeti sunmak ve/veya şebekesi veya altyapısı kurup işletmek isteyen şirketlerin yetkilendirilmesine ilişkin usul ve esasları kapsayan “Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği” nin “İşletmecilerin Hak ve Yükümlülükleri” başlıklı 19’uncu maddesinin birinci fıkrasının (u) bendinde;

“5397 ve 5651 sayılı Kanunlar ve ilgili diğer kanunlarda getirilen yükümlülükler: İşletmeciler, elektronik haberleşme sistemleri üzerinden milli güvenlikle, 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik altyapıyı, elektronik haberleşme sistemini hizmete sunmadan önce Kurumca belirlenecek usul, esas ve standartlarda, tüm harcamaları kendine ait olmak üzere kurmak ve güncellemekle yükümlüdür. Halen elektronik haberleşme hizmeti sunan işletmeciler de; söz konusu teknik altyapıyı, Kurum tarafından belirlenecek usul, esas ve standartlarda, tüm harcamaları kendilerine ait olmak üzere kurmak ve güncellemekle yükümlüdürler. İşletmeciler, 5397 ve 5651 sayılı Kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili olarak, tüm harcamaları kendilerine ait olmak üzere; ilgili mevzuat gereği verilmesi gereken bilgi, belge ve veriyi Kurum tarafından belirlenecek usul, esas ve standartlarda eksiksiz ve zamanında kanunen yetkili mercie teslim etmekle, her türlü sistemin işletilmesi bakımından, altyapı kullanımının sağlanması ile söz konusu sistemlerin çalışır vaziyette tutulması için gerekli donanım, yazılım, bakım, onarım, teknik destek gibi gerekli tedbiri almakla ve bunları etkileyen donanım, yazılım, altyapı ve şebekeye ilişkin değişiklikleri Kurum onayını alarak yapmakla yükümlüdürler” denilmektedir.

## 1.6. GEREKSİNİMLER

İşletmeciler tarafından sistemin gerçekleştirilmesi için gerekli olan hususlar:

- Abonelerini NAT’layarak internete çıkaracak İşletmecilere her bir kullanıcı için bölünmemiş belirli bir port aralığı atamaları tavsiye edilmektedir.
- Örneğin işletmeci tarafından her bir kullanıcı için 1000 portluk bir aralık tahsis edildiği varsayıldığında, 10.0.0.1 özel IP adresine sahip bir abone gerçek IP üzerinden bir bağlantı yapmak istediğinde bu gerçek IP adresine ait 10001:11000 gibi bir port aralığı kullanıcıya tahsis edilerek bağlantı bu port aralığı üzerinden sağlanmalıdır.
- Yukarıda belirtilen şekilde gerçekleştirilen bir atamada belli bir kullanıcıya ait olan özel IP adresi, NAT’landığı gerçek IP üzerinde rastgele portları değil, sistem tarafından önceden bu kullanıcıya tahsis edilmiş olan belli bir port aralığını kullanmalıdır.
- Yukarıdaki örnekte olduğu gibi 10.0.0.1 özel IP adresli kullanıcının açtığı her bir oturum için örneğin 80.80.80.80 IP adresi üzerinde kendisine tahsis edilmiş olan 10001:11000 port aralığındaki bir portu kullanabilecektir.
- Bu durumda Kuruma gönderilecek olan oturum (NAT IPDR) kayıtlarında bir kullanıcının gerçekleştirmiş olduğu bütün trafiklerin özeti olarak; bu kullanıcının aktif olduğu süre içinde kendisine tahsis edilen özel IP adresini, bu IP adresinin NAT’landığı gerçek IP adresini ve port aralığını içeren tek bir kayıt yer alacaktır.

- Bir kullanıcıya tahsis edilen bir port veya port aralığı; boşa çıktıktan sonra en az bir saat bekletilerek farklı bir kullanıcıya tahsis edilmesi uygun görülmektedir. Bu sayede belli bir port veya port aralığının art arda farklı kullanıcılara kullandırılması sonucunda oluşabilecek hataların önüne geçilebilecektir.

## 1.7. Kalite ve İdame Gereksinimleri

Tasarlanan sistemin kesintiye uğramaması ve veri bütünlüğünün sağlanabilmesi için aşağıda belirtilen olası problemlerle ilgili işletmeciler tarafından gerekli kontroller yapılmalıdır. Hata oluşabilecek durumlar için işletmeci problemi tespit edip hızlı müdahale amacıyla alarmlar üretmelidir. Bu problemler;

### a- Teknik altyapı problemleri;

- Noktadan noktaya kiralık devrenin çalışmaması.
- Güvenlik duvarı ve sunucuya uzaktan erişimin olmasına rağmen bu cihazlarda erişimi engelleyici arızaların oluşması.
- Sunucu ve cihazların NTP sunucusu konfigürasyonlarının yapılmamış ya da eksik olması. Bir işletme içerisinde kullanılan tüm cihazların en azından bir NTP sunucusu üzerinden hizmet almasının sağlanması.
- Güvenlik duvarı ve DPI cihazlarının CPU, RAM kullanımının artmasından dolayı by-pass durumuna geçmesi.
- Kullanıcı haklarından kaynaklanan problemler.

### b- Dosya problemleri;

- Dosyaların belirlenen periyotlarla sunucuya bırakılmaması.
- Dosyaların eksik gönderilmesi (eksik satır veya kolon içermesi).
- Dosyaların veya trafik kayıtlarının "Veri Deseni" bölümünde belirtilen desenlerden farklı olması.
- Dosyaların gzip formatında sıkıştırılmadan gönderilmesi.
- Dosyanın "sort" komutuyla sıralanmadan gzip'lenmesi.
- Dosya isimlendirmesinin hatalı yapılması.

Ayrıca, Kuruma ait sunucuda oluşacak olan arızalar BTK tarafından gözlemlenerek, işletmeciden arızanın giderilmesi talep edilecektir.

## 2. BÖLÜM

### İSS TRAFİK LOG DOSYALARI

Bu bölüm trafik kayıtlarını içeren dosyaların isim formatını açıklamaktadır. İşletmeciler tarafından trafik kayıtlarını içeren dosyalar, bu alanda açıklanan yapıya uygun olarak isimlendirilmelidir.

**A. Gönderi Dosyası İsimlendirme Formatı:** Gönderi dosyası aşağıda sunulan şablona uygun olarak oluşturulmalıdır. Dosya isimlendirmesinde Türkçe karakter kullanılmamalıdır.

**“ISLETMECI\_ADI\_KODU\_ISS\_TRAFIK\_YYYYMMDDHH24MISS\_MINTAR\_MAXTAR\_CNT.log.gz”**

Gönderi dosya isim deseninde geçen alanlar:

- **ISLETMECI\_ADI:** Trafik verisini oluşturan işletmeciyi belirtmektedir. Kurum tarafından iletilen işletmecici\_adi değiştirilmeden kullanılmalıdır.
- **ISLETMECI\_KODU:** Trafik verisini oluşturan işletmecinin kodunu belirtmektedir. Kod rakamla üç hane olacak şekilde yazılmalıdır. Örneğin 002 gibi.
- **ISS\_TRAFIK:** Bu değer belirtildiği şekilde kalmalıdır.
- **TARİH\_ZAMAN:** Bu alana girilecek olan tarih değeri “YYYYMMDDHH24MISS” deseninde olmalıdır.
  - YYYY deseni dört basamak olarak yılı (örneğin 2012 gibi)
  - MM deseni iki basamak olarak ayı (örneğin 06 gibi)
  - DD deseni iki basamak olarak günü (örneğin 05 gibi)
  - HH deseni iki basamaklı ve 24 saat formatında saati (örneğin 18 gibi)
  - MI deseni iki basamak olarak dakikayı (örneğin 18)
  - SS deseni iki basamak olarak saniyeyi (örneğin 18)

Örnek bir tarih değeri “20120605181221” şeklindedir.

- **MINTAR:** Bu alana girilecek olan tarih değeri “YYYYMMDDHH24MISS” deseninde olmalıdır, dosya içeriğindeki kayıtların minimum başlangıç zamanını bildirir.
- **MAXTAR:** Bu alana girilecek olan tarih değeri “YYYYMMDDHH24MISS” deseninde olmalıdır, dosya içeriğindeki kayıtların maksimum başlangıç zamanını bildirir.
- **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 işletmecici tercihen şebeke elemanı kodunu girebilir. (Örn:PRSR1\_002)

Örnek dosya isimi:

**“ORNEKTELEKOM\_263\_ISS\_TRAFIK\_20170315162500\_20170315162500\_20170415162500\_001.log.gz”**

**B. Trafik Dosyası Uzantısı:** Trafik dosyasının uzantısı **“.log”** olmalıdır. Dosya uzantısı küçük harfler ile yazılmalıdır.

**C. Trafik Dosyası Sıkıştırma Formatı:** Dosyalarda yer alan kayıtlar öncelikle “sort” komutu ile sıralanmalı, ardından “gzip” komutu ile sıkıştırılmalıdır. Sıkıştırma işlemi yapıldıktan sonra dosyanın isim formatı aşağıda görüldüğü gibi olmalıdır.

**“ORNEKTELEKOM\_263\_ISS\_TRAFIK\_20170315162500\_20170315162500\_20170415162500\_001.log.gz”**

**D. Trafik Dosyalarının FTP Sunucusundaki Yeri:** Trafik dosyaları, FTP sunucusunda operatöre giriş hakkı verilen dizin içerisindeki **“TRAFIK”** klasörü altına gönderilmelidir.

**E. Trafik Dosyalarının Gönderim Periyodu:**

Trafik dosyaları (teslim edilen/alınan, işlemi süren tüm kayıtlar) yaklaşık 100 MB büyüklüğündeki dosyalar halinde ve azami bir saatlik periyotlar ile gönderilmelidir. Süre ve boyut limitinden hangisine önce ulaşılır ise dosya gönderim periyodu ona göre belirlenmelidir.

**F. Trafik Dosyalarının İçeriği:**

1. Trafik dosyalarının içinde bulunan kayıtlar için;

a) Her kayıt için bir satır oluşturulmalıdır.

**trafik1\_alan1|trafik1\_alan2|trafik1\_alan3|....|trafik1\_alan22**

**trafik2\_alan1|trafik2\_alan2|trafik2\_alan3|....|trafik2\_alan22**

**trafikN\_alan1|trafikN\_alan2|trafikN\_alan3|....|trafikN\_alan22**

b) Bir kaydın, birden fazla satırda olmaması gerekmektedir. Aşağıdaki kullanım yanlış bir örnektir.

**#**

**trafik1\_alan1|**

**trafik1\_alan2|**

**...**

**trafik1\_alan22**

**#**

```
trafik2_alan1|
trafik2_alan2|
...
trafik2_alan22
#
trafikN_alan1|
trafikN_alan2|
...
trafikN_alan22
#
```

c) Trafik kayıtları ortadan bölünmeden, bir bütün olarak gönderilmelidir. Aşağıdaki yanlış bir örnektir.

```
trafik1_alan1|trafik1_alan2|trafik1_alan3|...|trafik1_alan22
trafik2_alan1|trafik2_alan2
|trafik2_alan3|...|trafik2_alan22
trafikN_alan1|trafikN_alan2|trafikN_alan3|...|trafikN_alan22
```

2. Kayıtlardaki kolonlar “|” (pipe) işareti ile ayrılmalı ve bu “|” (pipe) işareti ayraç alanı dışında kesinlikle kullanılmamalıdır.
3. Her bir anlamlı kayıt satırı “\n” (satır sonu) karakteri ile ayrılmalıdır.
4. IP adresleri noktalı olarak (dotted decimal) yazılmalıdır.
5. Port numaraları rakamla girilmelidir.
6. Sadece Delete (Stop) paketleri değil, Create (Start) ve Interim paketleri de gönderilmelidir.
7. Hali hazırda Kurum ile paylaşılan oturum verilerinin gönderilmesine devam edilecektir.
8. İSS Trafik Log alanlarının içerisinde yer alan verilerde aşağıdaki özel karakterler kesinlikle bulunmamalıdır.  
(;) Noktalı Virgül, (') Single Quote, (") Double Quote, Backslash, Newline, Tab, Backspace, Form Feed, Vertical Tab, Accent Grave (backtick),\r (carriage return:satır başı)
9. Kayıtlarda hatalı ve eksik bilgiler, tarih formatı, kolon sayısı, geçersiz IP formatı vb. rutin olarak kontrol edilecektir. Kurum tarafından iletilen ve işletmeniz tarafından yapılacak rutin kontrollerde tespit edilen “Hata ve Eksiklikler” ivedilikle düzeltilecek ve yapılan çalışma hakkında, çalışma öncesi ve sonrasında Kuruma bilgi verilecektir.



## 3. BÖLÜM

### 3.1. İSS TRAFİK LOGU VERİ DESENİ

Bu bölüm; ISS işletmecileri tarafından gönderilecek olan trafik logu veri desen yapısını açıklamaktadır. Dosya içerikleri aşağıda belirtilen formata göre hazırlanmalıdır.

Trafik verileri aşağıdaki kurallara göre oluşturulmalıdır.

- Her bir satır 22 kolondan oluşmalıdır.
- Her kolon “|” (pipe) karakteri ile (16lık sistemde/hexadecimal değeri 7C) ayrılmalıdır.
- Boş bırakılan alan olması durumunda bu alan yine pipe kullanılarak belirtilmelidir.
- Dosya içerikleri UTF-8 karakter kodlaması kullanılarak hazırlanmalıdır.

### 3.2. İSS TRAFİK LOG FORMATI

Trafik kayıtları içerisinde yer alan her bir satır aşağıda belirtilen desen formatında gönderilmelidir. Aşağıda belirtilen desen tek bir anlamlı trafik log satırını belirtmektedir.

**KULLANICIADI@DOMAIN|OZEL\_IP|OZEL\_PORT|GERCEK\_IP|GERCEK\_PORT\_BASLANGIC|GERCEK\_P  
ORT\_BITIS|TRAFIK\_BASLAMA\_TARİH|TRAFIK\_SURE|HEDEF\_IP|HEDEF\_PORT|APP\_PROTOKOL|NE  
TWORK\_PROTOKOL|DOWNLOAD\_BYTES|UPLOAD\_BYTES|BAGLANTI\_PVC|OTURUM\_ID|SSG\_IP|N  
AT\_CIHAZ\_IP|DPI\_CIHAZ\_IP|TERMINATION\_CAUSE|PACKET\_TYPE|DIRECTION**

### 3.3. İSS TRAFİK LOG ALANLARI

**1. KULLANICI\_ADI:** Bu alan, trafiği başlatan aboneyi operatör networkünde işaret eden benzersiz ibaredir. Bu alana kullanıcı adı tahsisi yapılan hizmet tiplerinde (adsl vb.) kullanıcı adı, kullanıcı adı tahsisi yapılmayan hizmet tiplerinde (Metro Ethernet vb.) ise devre numarası vb. bilgiler girilmelidir. Bu alanda yer alan kullanıcı ad bilgisi ile işletmeci tarafından Kurumumuza hali hazırda gönderilen veya gönderilecek olan abone ve oturum dosyalarında yer alan kullanıcı ad bilgisi uyumlu olmalıdır. Yani işletmeci abone ve oturum dosyalarında **aboneX@ornektelekom** olarak geçen bir kullanıcı, İSS Trafik log kayıtlarında da **aboneX@ornektelekom** olacak şekilde yer almalıdır.

Kullanıcı adı tahsisi yapılan hizmet türlerinde domain bilgisi işletmecinin adıyla uyumlu olmalı ve gönderilen kullanıcı adında bu domain bilgisine yer verilmelidir. Bayi veya acente üzerinden yapılan aboneliklerde bayilik/acentelik veren işletmecinin (yetkilendirilmiş işletmecinin) domaini kullanılmalı, her bayi veya acente için farklı domain ismine bu alan içerisinde yer verilmemelidir.

**2. OZEL\_IP:** İşletme ağı içerisinde NAT yöntemi ile IP atayan işletmeciler için kullanıcıya ait özel (private) IP adresini ifade eder. **NAT yöntemi kullanan işletmeciler bu alanı boş gönderemez ve**

**standart dışı ifadeler kullanılmaz.** NAT yöntemi kullanmayan işletmeciler bu alanı boş göndermelidir.

(Örn: 10.0.0.10)

**3. OZEL\_PORT:** Özel IP adresinin kaynak port numarasıdır. NAT yöntemi kullanan işletmeciler bu alanı **boş gönderemez ve standart dışı ifadeler kullanılmaz.** NAT yöntemi kullanmayan işletmeciler bu alanı boş göndermelidir.

**4. GERCEK\_IP:** Abonenin internet ortamına çıkarken kullandığı gerçek (public) IP adresini ifade eder.  
(Örn: 99.99.99.99)

**5. GERCEK\_PORT\_BASLANGIC:** Gerçek IP adresinin port aralığının başlangıç değerini ifade eder. Port aralığının girilemediği durumlarda bu alana doğrudan trafiğin gerçekleştiği port değeri yazılmalıdır.  
(Örn: 53254)

**6. GERCEK\_PORT\_BITIS:** Gerçek IP adresinin port aralığının bitiş değerini ifade eder. Port aralığının girilemediği durumlarda bu alana yine doğrudan trafiğin gerçekleştiği port değeri yazılmalıdır.  
(Örn:53254)

**7. TRAFIK\_BASLAMA\_TARİH:** Trafiğin başlama zamanını ifade eder. YYYYMMDDHH24MISS formatında gönderilmelidir.  
(Örn: 20180418000000)

**8. TRAFIK\_SURE:** Saniye cinsinden trafiğin süresini ifade eder (Küsuratlı değer "ceiling" özelliği ile yukarı yuvarlanacaktır).

**9. HEDEF\_IP:** Kullanıcının bağlantı yapmak istediği hedef IP adresini ifade eder.  
(Örn: 100.100.100.100)

**10. HEDEF\_PORT:** Kullanıcının bağlantı yapmak istediği hedef port numarasını ifade eder.

**11. APP\_PROTOCOL:** Trafik kaydının uygulama seviyesindeki protokolünü ifade eder. Çözülen protokol için protokol bilgisi bu alana girilmelidir. **DPI üzerinden veya bu alanı çözebilecek benzer sistemler üzerinden trafik kaydı oluşturan işletmeler için bu alan boş gönderilemez ve standart dışı ifadeler kullanılmaz.**

(Örn: http, ftp, Whatsapp vb.)

**12. NETWORK\_PROTOCOL:** Trafiğin network seviyesindeki protokol bilgisini ifade eder. Asgari TCP ve UDP olmak üzere network seviyesindeki protokollerin bu alanda loglanması gerekmektedir. UDP: **"17"**, TCP: **"6"**, ICMP: **"1"**, ESP: **"50"**, IPv6 ICMP: **"58"** vb. olarak ilgili RFC'de belirtildiği şekilde gönderilmelidir. **TCP, UDP, ICMP, ESP gibi ifadeler kullanılmaz.**

**13. DOWNLOAD\_BYTES:** Trafiğin byte cinsinden indirilen veri miktarını ifade eder (download bilgisi). **Kuruma resmi yazı ile bilgi verilerek onay alınması şartı ile gereksiz kaynak kullanımının önüne geçilmesi adına; işletmenin kendi şebekesindeki bir CDN (Content Delivery Network) sisteminden gerçekleştirilecek download bilgisinin raporlanıp raporlanmaması işletmecinin tercihine bırakılmıştır.**

**14. UPLOAD\_BYTES:** Trafiğin byte cinsinden yüklenen veri miktarını ifade eder (upload bilgisi).

**15. BAGLANTI\_PVC:** Bu alan, kullanıcının bağlı olduğu router port bilgilerini ifade eder.  
(Örn: SSG\_ADI#8:5#13/5 gibi )

**16. 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.

**17.SSG\_IP:** Oturumun oluşturduğu SSG cihazının IP adresini ifade eder.  
(Örneğin 10.251.20.10)

**18. NAT\_CHAZ\_IP:** NAT kaydının oluşturduğu NAT cihazı veya NAT işlevi için kullanılan cihazın IP adresini ifade eder. **NAT cihazı üzerinden trafik kaydı oluşturan işletmeler için bu alan boş gönderilemez ve standart dışı ifadeler kullanılamaz.**  
(Örneğin 10.250.0.10)

**19.DPI\_CHAZ\_IP:** Trafiğin geçtiği DPI cihazının IP adresini ifade eder. **DPI üzerinden trafik kaydı oluşturan işletmeler için bu alan boş gönderilemez ve standart dışı ifadeler kullanılamaz.**

**20.TERMINATION\_CAUSE:** Trafiğin kapanma sebebini ifade eder. Kullanıcının trafik kaydı normal şekilde sonlandığında bu alan boş gelmelidir. Diğer durumların hepsinde bu alana kapanma sebebi (örn: timeout, error, handover, NAS error vb.) yazılmalıdır. **Trafiğin normal olarak sonlanmadığı durumlarda bu alan boş gönderilemez ve standart dışı ifadeler kullanılamaz.**

**21.PACKET\_TYPE:** Trafiği oluşturan paketin türünü ifade eder. Hali hazırda Oturum ve Nat IPDR kayıtlarında gönderilmekte olan Oturum Durum (Session Status) bilgisi ile karıştırılmamalıdır.  
start:"1", stop:"2" , interim-Update:"3"  
Bu alana 1, 2 veya 3 değerlerinden biri girilmelidir. **Start, interim ve stop ifadeleri kullanılamaz.**

**22.DIRECTION:** Trafiğin akış yönünü ifade eder. Akış yönü; ISS abonesinin "start ve stop" paketleri yönünden trafiğin kaynağı olması durumunda "Egress", trafiğin hedefi olması durumunda ise "Ingress" şeklinde değerlendirilmelidir.  
Ingress: "0" , Egress: "1"  
Bu alana 0 veya 1 değerlerinden biri girilmelidir. **Ingress ya da Egress ifadeleri kullanılamaz.**

### Örnek İSS TRAFİK LOG kaydı:

aboneX@ornektelekom|10.0.0.10|45555|99.99.99.99|54444|55443|20180418000000|200|100.100.100.100|80|HTTP|17|250|83  
|ORNEK-06-ERC-SSR-02#4/22#6:145|DDFR-65AC-12EE-FFFF|10.251.20.10 |10.250.0.10|10.250.15.10|Nas-Error|1|0

aboneY@ornektelekom|10.0.10.10|55555|99.11.11.11|50001|50001|20180418000000|200|100.100.100.100|80|HTTP|6|250|83  
|ORNEK-06-ERC-SSR-02#4/22#6:146|DDFR-65AC-12EE-FFFD|10.251.20.10 |10.250.0.10|10.250.15.10|Time-Out|0|1

---

## 4. BÖLÜM

### DİKKAT EDİLMESİ GEREKEN HUSUSLAR

İSS işletmecilerinin İSS Trafik Logu oluşturma ve Kuruma gönderme süreçlerinde aşağıda belirtilen açıklamaları göz önünde bulundurmaları gerekmektedir.

- Azami 1 saat olabilecek olan Trafik logu gönderim periyodu Kuruma yazılı olarak bildirilmeli, dosya isimlendirmesinde kullanılan zaman bilgisi ile dosyanın içerisinde yer alan logların zaman bilgisi tutarlı olmalıdır. Örneğin; İşletmecinin dosya gönderim periyodu süre ve boyut kısıtlarına göre 10 dk. ise, dosya oluşturma zamanı 13:00:00 iken bu dosya içerisinde gelecek verilerin 13:00:00 ile 13:09:59 arasında olması zorunludur.
- Gönderilecek dosyalar “Trafik Log Deseni” bölümünde belirtilen açıklama ve kısıtlamalara uygun olarak gönderilmelidir.
- Dosya isimlerinde ve kayıtlarda yer alan tarih değerleri Türkiye yerel saatine uygun olarak gönderilmelidir.
- Yukarıda belirtilen alanlarda yer alan desen yapısına ve kısıtlamalara uygun olarak iletilmeyen verilerin BTK tarafından yapılan incelemeler neticesinde tespit edilmesi, aynı problemin sık sık veya belli aralıklarla yaşanması halinde; Kurum tarafından ilgili işletmeciye resmi yazı ile problemin kalıcı olarak giderilmesi yönünde bildirim yapılacaktır. Problemin belirlenen süre içerisinde giderilememesi durumunda ilgili mevzuat hükümleri çerçevesinde gerekli cezai işlemler başlatılacaktır.
- İşletmeciler verilerini ve dosyalarını oluşturma süreçlerini gözlem altında tutmakla ve oluşacak problemleri en kısa zamanda gidermekle yükümlüdürler. Bu amaç doğrultusunda, işletmeciler tarafından oluşacak problemlerin erken tespiti ve giderilmesi için alarmların üretilmesinin, uygun bir çözüm olduğu değerlendirilmektedir.
- İşletmeciler dosyalarını düzenli olarak göndermekle, gönderdikleri verilerin doğruluğunu ve bütünlüğünü sağlamakla yükümlüdürler.