Ulusal Taşıt Tanıma Sistemi Kapsamında
YN Pompa ÖKC ile Tabanca İletişim Modülü Arasında
Güvenli İletişim Protokolü

(Sürüm 1.0)

27 AĞUSTOS 2024

İÇİNDEKİLER

1. Giriş

Bu Teknik Kılavuz, 05/10/2023 tarihli ve 32330 sayılı Resmî Gazete ’de yayımlanan 1 Sıra No.lu Ulusal Taşıt Tanıma Sistemi Uygulama Genel Tebliği’nin 5 inci maddesinin ikinci fıkrası uyarınca TTO’nun TTB’yi okuması sonucunda taşıt plakasının otomatik olarak YN Pompa ÖKC’ye güvenli olarak iletilmesinin sağlanması, YN Pompa ÖKC ile TTO arasında gerçekleşecek güvenli haberleşmenin donanımları, metotları, kuralları ve diğer hususları belirlenmek amacıyla hazırlanmıştır.

Akaryakıt satış işleminin YN Pompa ÖKC’de başlatılması ve sonlandırılması esastır.

2. Tanımlar ve Kısaltmalar

Bu Teknik protokolde geçen;

Başkanlık: Gelir İdaresi Başkanlığını,
Darphane: Darphane ve Damga Matbaası Genel Müdürlüğünü,
Veri Merkezi: UTTS kapsamında oluşan verilerin kaydedilip, saklanacağı veri merkezini,
Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihaz (YN Pompa ÖKC): Elektronik ortamda anlık veri aktarımı yapabilen, güvenlik seviyesi yükseltilmiş ve 527 sıra no'lu Vergi Usul Kanunu Genel Tebliği ve ilgili teknik kılavuzlarda diğer özellikleri belirlenen Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazı,
YN Pompa ÖKC Üreticisi: YN Pompa ÖKC'lerin ithali/üretimi, satışı ve satış sonrası bakım onarım hizmetlerinin yürütülmesi için Hazine ve Maliye Bakanlığından onay alan firmayı,
YN Pompa ÖKC Yetkili Servisi: YN Pompa ÖKC'ler için Hazine ve Maliye Bakanlığından onay alan üretici/ithalatçı firmaların bu cihazların bakım ve onarım hizmetlerini yapmaya yetkili kıldığı kişi veya kurumu,
TİM: TTO'lardan gelen sinyali çözümleyip Veri Merkezi ile iletişime geçerek TTB'ye ait bilgileri alan ve bunları YN Pompa ÖKC'ye ileten, üzerinde Güvenlikli Haberleşme Anahtarı/Kodu ve özel yazılım bulunan, harici olarak YN Pompa ÖKC'ye bağlanmış veya YN Pompa ÖKC içine entegre edilmiş modülü,
TTB: Yakıt verilen taşıtların yakıt depo girişine monte edilebilen ve söküldüğünde tekrar kullanılamayan, taşıta ait plaka bilgisi, mükellefe ilişkin bilgiler gibi hususları hafızasında muhafaza eden ve bu bilgilerin akaryakıt alımı sırasında TTO vasıtasıyla pompa ünitelerinin bağlı olduğu YN Pompa ÖKC'lere otomatik olarak iletilmesine imkân sağlayan pasif bir devre ve anteni içeren Taşıt Tanıma Birimini,
Taşıt Tanıma Okuyucusu (TTO): TTB üzerindeki bilgileri okuyabilen, okunan bilgilerin YN Pompa ÖKC'lere otomatik olarak iletilmesine imkân sağlayan Taşıt Tanıma Okuyucu Cihazı,
ACK: Bir mesajın veya verinin başarıyla alındığını onaylayan kontrol karakterini,
CRC16-ARC: Veri iletimi sırasında meydana gelebilecek hataları tespit etmek için yaygın olarak kullanılan bir çevrimsel artıklık denetimi algoritmasını,
ETX: Metin Sonu anlamına gelen ve mesajın bittiğini gösteren kontrol karakterini,
EOT: Bir ileti serisinin sonunu belirten kontrol karakteridir. Veri iletiminde, göndericinin veri iletim serisinin tamamladığını ve artık veri göndermeyeceğini,
Güvenlikli Haberleşme Anahtarı (SAM Kart): UTTS Donanımları arasındaki güvenli iletişimin sağlanmasını temin eden ve sadece Darphane'den temin edilebilen dijital ve/veya fiziksel teknolojik unsuru,
NAK/NACK: Bir mesajın veya verinin hatalı olduğunu veya alınamadığını belirten bir kontrol karakterini,
Poll: İletişim protokollerinde, veri yolu üzerindeki cihazların düzenli olarak kontrol edilmesini sağlayan; bir cihazın diğer cihazlardan veri veya durum bilgisi istemek için gönderdiği sorgulama işlemini,
RSA: Asimetrik şifreleme yöntemlerinden biridir. Kamu anahtarı kriptografisinde veri güvenliğini sağlamak amacıyla veri şifreleme ve dijital imzaların doğrulanması için kullanılan; biri açık biri gizli olan 2 anahtarı,

RTC (Real-Time Clock): Gerçek zamanlı saat anlamına gelen, sistemlerin doğru tarih ve saat bilgisini takip etmesini sağlayan, genellikle bilgisayarlar, gömülü sistemler ve çeşitli elektronik cihazlarda bulunan ve sistem kapalıyken bile zamanı takip edebilmesi için bir batarya ile çalışan donanım bileşenini,
Soket: Ağ üzerindeki iki cihaz arasında iletişim kurmak için kullanılan bir uç noktadır. Belirli bir IP adresi ve port numarası ile ilişkilendirilen, veri alışverişi için kullanılan, hem bağlantı tabanlı (TCP) hem de bağlantısız (UDP) protokollerde kullanılabilen ve bir uygulamanın ağ üzerinden veri göndermesi veya alması için gereken arabirimi,
STX: Veri iletiminde metnin başlangıcını belirtmek için kullanılan kontrol karakterini,
TCP/IP: İnternet ve diğer bilgisayar ağlarında veri iletimi için kullanılan, verilerin güvenilir ve sıralı bir şekilde iletilmesini sağlayan (TCP); verilerin doğru hedefe yönlendirilmesi (IP) için kullanılan, ağ üzerinde bilgisayarlar arasında iletişimin temelini oluşturan temel protokol setini,
TLS 1.2: İnternet üzerinden veri iletiminde güvenliği sağlamak için kullanılan verilerin gizliliğini ve bütünlüğünü koruyarak yetkisiz erişim ve müdahaleleri önleyen şifreleme protokolünü,
TLV: Veri yapılandırma formatıdır. Bir verinin türünü (Type), uzunluğunu (Length) ve içeriğini (Value) belirten özellikle iletişim protokollerinde esnek ve düzenli veri iletimi sağlamak için kullanılan veri yapılandırma formatını,

ifade eder.

3. Güvenli İletişim Protokol Açıklamaları

TİM ve YN Pompa ÖKC arasındaki haberleşme RS-485 veya ethernet ile gerçekleştirilebilir. Haberleşme RS-485 ile gerçekleştiriliyorsa, RSA güvenli haberleşme protokolü ile veri güvenliği sağlanır. Haberleşme ethernet ile gerçekleştiriliyorsa, TLS 1.2 güvenli haberleşme protokolü ile veri güvenliği sağlanır.

- **Mesaj Listesi**
  - TİM'den YN Pompa ÖKC'ye Giden Mesajlar

Mesaj Adı	**Şifreli mi?**
TİM: TTB Bağlantı & Veri (0x61)	Evet
TİM: Durum Yanıtı (0x67)	Evet
TİM'den YN Pompa ÖKC'ye Başlatma (INIT) Yanıtı (0x7D)	Hayır
TİM'den YN Pompa ÖKC'ye Anahtar (Key) Yanıtı (0x7E)	Hayır (anahtar şifreli)
TİM'den YN Pompa ÖKC'ye Şifreli Kapatma (Close) Yanıtı (0x7F)	Evet

  - YN Pompa ÖKC'den TİM'e Giden Mesajlar

Mesaj Adı	**Şifreli mi?**
TTB Verisini Yeniden Gönder (0x71)	Evet
RTC'yi Güncelle (0x75)	Evet
Durum İsteği (0x77)	Evet
İşlem Raporu (0x7B)	Evet
YN Pompa ÖKC'den TİM'e Başlatma (INIT) İsteği (0x6D)	Hayır
YN Pompa ÖKC'den TİM'e Anahtar (Key) İsteği (0x6E)	Hayır (anahtar şifreli)
YN Pompa ÖKC'den TİM'e Şifreli Kapatma (Close) İsteği (0x6F)	Evet

3.1 TCP/IP Haberleşme

TİM ve YN Pompa ÖKC iletişimi, çift yönlü veri alışverişi olarak tek bir TCP/IP soketi üzerinden gerçekleşir. Bu soket, güvenlik seviyesi TLS 1.2 olan bir bağlantı kullanır.

TİM, YN Pompa ÖKC'nin bağlantıyı kurduğu ve her zaman açık tuttuğu sunucu tarafıdır. Varsayılan TİM TCP port numarası 8000'dir ve bu numara TİM web arayüzü üzerinden tanımlanabilir.

TİM ve YN Pompa ÖKC arasındaki bilgi alışverişi, bu dokümanda açıklandığı gibi yapılandırılmış mesajlarla gerçekleştirilir.

3.2 RS-485

3.2.1 İletişim Protokolü

TİM ve YN Pompa ÖKC iletişimi, RS-485 veri yolu arayüzü üzerinden gerçekleştirilir. YN Pompa ÖKC, TİM ile önceden tanımlanmış benzersiz bir adres aracılığıyla iletişim kurar ve RS-485 veri yolu üzerinde poll mekanizması kullanır. Protokol, YN Pompa ÖKC'nin TİM'e bir istek mesajı göndererek iletişimi başlattığı ve TİM'in YN Pompa ÖKC'ye bir yanıt mesajı ile cevap verdiği komut-yanıt mesaj çiftlerine dayanır.

3.2.2 Arayüz Tanımı

RS-485 arayüzü, saniyede 57600 sembol hızı (baud rate), 8 bit veri genişliği, parite olmadan ve 1 dur bitine (stop biti) sahip olacak şekilde yapılandırılmıştır.

3.2.3 Zamanlama

TİM, 200 ms (milisaniye) içinde bir yanıt mesajı gönderir.

Bir yanıt ile bir sonraki istek arasında en az 30 ms gecikme olması gerekir.

3.2.4 RS-485 İşlem Sırası

TİM, YN Pompa ÖKC tarafından gönderilen komutlara yanıt verir ve bir mesaj iletmek için YN Pompa ÖKC'den gelecek bir sonraki poll komutunu bekler.

Durum	**YN Pompa ÖKC**		**TİM**
TİM'den veri yok	Poll		→ TİM'den Veri yok
			← EOT
TİM'den YN Pompa ÖKC'ye veri	Poll	→	
			← Veri 1
	ACK	→	
			← Veri 2
	ACK	→	
		•••	
			← EOT
YN Pompa ÖKC'den TİM'e veri (Poll gerekli değil)	Veri 1	→	
			← ACK
	Veri 2	→	
			← ACK
YN Pompa ÖKC'den TİM'e hatalı veri	Veri1-Hata	→	
Sonsuz döngülerden kaçınmak için YN Pompa ÖKC hata sayımı yapacaktır.			← NACK
YN Pompa ÖKC'den TİM'e hatalı veri	Veri 1	→	

		←	ACK
TİM'den YN Pompa ÖKC'ye hatalı veri	Poll	→	
YN Pompa ÖKC hata sayımı yapacak ve sonsuz döngülerden kaçınmak için bir ACK gönderecektir.		←	Hata-Veri 1
TİM'den YN Pompa ÖKC'ye hatalı veri	Poll	→	
		←	Veri 1
	ACK	→	
		←	EOT

3.2.5 RS-485 Mesaj Formatı

3.2.5.1 Mesaj Formatı

- Her mesaj aşağıdaki alanları içerir:

FDh	ADDR	DIR	YN Pompa ÖKC MSG ID	TİM MSG ID	OPCODE	Length	Data	CRC	FEh

Kod	**Açıklama**	**Boyut**
FDh	Mesaj Başlangıcı	Bir Bayt
ADDR	Cihaz Adresi	Bir Bayt
DIR	Yön Baytı	Bir Bayt
YN Pompa ÖKC MSG ID	YN Pompa ÖKC Mesaj ID'si	Bir Bayt
TİM MSG ID	TİM Mesaj ID'si	Bir Bayt
OPCODE	İşlem Kodu	Bir Bayt
Length	Veri Uzunluğu	İki Bayt
Data	Veri	Uzunluk Bayt
CRC16	Standart CRC16-ARC	İki Bayt
FEh	Mesaj Sonu	Bir Bayt

- İletişimi başlatan her zaman YN Pompa ÖKC'dir. TİM, yanıt mesajını 200 ms içinde gönderir.

3.2.5.2 Mesaj Formatı

- CRC, ADDR alanından DATA alanına kadar (dahil) hesaplanır. Örneğin:

FDh	**ADDR**	**DIR**	**YN Pompa ÖKC MSG ID**	**TİM MSG ID**	**OPCODE**	**Length**	**Data**	**CRC**	**FEh**
FDh	01h	80h	32h	31h	08h	0000h		B9FAh	FEh

- Yukarıdaki örnekte, veri uzunluğu sıfırdır, bu nedenle Veri alanı boştur. Aşağıdaki veri içeren bir mesajın örneği yer almaktadır:

FDh	ADDR	DIR	YN Pompa ÖKC MSG ID	TİM MSG ID	OPCODE	Length	Data	CRC	FEh
FDh	01h	00	47h	4Ah	26h	0018h	01 A3 30 32 31 30 30 30 30 2E 32 32 36 30 30 30 30 30 2E 37 36 32 30 30	D923h	FEh

3.2.5.3 Mesaj Bileşenlerinin Açıklaması

Cihaz Adresi Alanı (ADDR): TİM'in önceden tanımlanmış RS-485 veri yolu adresidir (istek ve yanıt mesajlarında aynıdır).

Yön Baytı (DIR): Sıra numaralandırma için kullanılır- D XXX XXXX - burada:

- D = Yön Biti; 1 = Ana cihazdan (YN Pompa ÖKC), 0 = Alt cihazdan (TİM)
- XXXXXXX = Gelecek kullanım için ayrılmıştır.

TİM MESAJ ID (TİM MSG ID): Sıra Numarası, 1..FF arasında sayar; FF'den 1'e geçiş yapar.

- Her mesaj ilgili mesaj isteğinin YN Pompa ÖKC MSG ID'sini içerir.
- TİM, her giden mesaj için TİM MSG ID'sini arttırır.
- TİM, gelen veri mesajlarındaki TİM MSG ID'sinin geçerliliğini kontrol eder.
    - Eğer veri mesajının TİM MSG ID'si önceki ile aynı ise TİM ek bir mesaj işlemeden ilgili ACK mesajını gönderir.
    - Eğer bir mesajın TİM MSG ID'si önceki ile aynı ise TİM protokole göre işlem yapar (arttırılmış TİM MSG ID ile veri yanıtı tekrarı veya EOT gönderir).

YN Pompa ÖKC MESAJ ID: Sıra Numarası, 1..FF arasında sayar; FF'den 1'e geçiş yapar.

- Her mesaj, son TİM mesajının TİM MSG ID'sini içerir. YN Pompa ÖKC mesajı bir TİM isteği olmadan gönderilmiş ise TİM MSG ID sıfır olarak ayarlanır (başlatma).
- YN Pompa ÖKC giden her mesaj için YN Pompa ÖKC MSG ID'sini arttırır.
- YN Pompa ÖKC gelen veri mesajlarındaki YN Pompa ÖKC MSG ID'sinin geçerliliğini kontrol eder.
    - Yanıt mesajı doğru alınmadığında (örneğin; NACK, Hatalı CRC, Yanıt Yok) tekrar mesaj gönderilir. Tekrar mesajı, arttırılmış YN Pompa ÖKC MSG ID'sini içerir.

3.2.6 RS-485 Mesaj Açıklamaları

3.2.6.1 RSA Eşleştirme Mesajları (02)

Kaynak: TİM, YN Pompa ÖKC

Format: Aşağıdaki tabloya bakınız.

Tablo 3-1: RSA Eşleştirme Mesajı Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	02
Mesaj Uzunluğu	2	Bayt	xx
Veri		TLV	

- Bu komut, başlatma ve anahtar isteği mesajları ile eşleştirme sürecindeki NACK mesajları için kullanılır. Bu mesajların TLV veri bloğu şifrelenmemiştir (belirli şifreli veri öğeleri içermesine rağmen). Başarılı anahtar değişim komutundan sonra, TİM ve YN Pompa ÖKC arasındaki iletişim 03h komutu (Şifreli Veri modu) ile şifrelenir.

3.2.6.2 Şifreli Veri Mesajı (03)

Kaynak: TİM, YN Pompa ÖKC

Format: Aşağıdaki tabloya bakınız.

Tablo 3-2: Veri Modu Mesaj Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	03
Mesaj Uzunluğu	2	Bayt	xx
Veri	n x 16	Şifreli	

- Bu komut, TİM ve YN Pompa ÖKC arasında RS-485 üzerinden şifreli veri alışverişi için kullanılır ve TİM- YN Pompa ÖKC Mesajları'nda açıklanan TİM-YN Pompa ÖKC mesajlarına göre çalışır. Şifreli veri mesajları, "RS-485 RSA eşleştirme özeti" olarak tanımlanan başarılı bir eşleştirme ve anahtar değişim süreci tamamlandıktan sonra değiştirilebilir.

3.2.6.3 POLL Mesajı (08)

Kaynak: YN Pompa ÖKC

Format: Aşağıdaki tabloya bakınız.

Tablo 3-3: POLL Mesajı Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	08
Mesaj Uzunluğu	2	Bayt	0
Veri			

3.2.6.4 EOT Mesajı (04)

Kaynak: TİM

Format: Aşağıdaki tabloya bakınız.

Tablo 3-4: EOT Mesajı Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	04
Mesaj Uzunluğu	2	Bayt	0
Veri			

3.2.6.5 ACK Mesajı (06)

Kaynak: TİM, YN Pompa ÖKC

Format: Aşağıdaki tabloya bakınız.

Tablo 3-5: ACK Mesajı Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	06
Mesaj Uzunluğu	2	Bayt	0
Veri			

3.2.6.6 NACK Mesajı (15h)

Kaynak: TİM

Format: Aşağıdaki tabloya bakınız.

Tablo 3-6: NACK Mesajı Özellikleri

İsim	Boyut (bayt)	Format	Değer
Mesaj Türü	1	Bayt	15h
Mesaj Uzunluğu	2	Bayt	1
Hata Kodu	1	Bayt	Aşağıdaki tabloya bakınız

- Aşağıdaki tablo, TİM ve YN Pompa ÖKC arasındaki hata kodlarını listeler.

Hata Adı	Açıklama	Format	Değer
Geçersiz Mesaj	Opcode desteklenmiyor/Mevcut değil	Bayt	01h

Hata Adı	Açıklama	Format	Değer
Geçersiz Mesaj Uzunluğu	Yanlış mesaj uzunluğu	Bayt	02h
Cihaz eşlenmedi	Cihaz eşlenmedi. Eşleştirme süreci gerekli	Bayt	03h
CRC hatası	Yanlış CRC	Bayt	05h
ETX bulunamadı	Çerçeve sonu baytı (0xFE) bulunamadı	Bayt	06h

4. TİM-YN Pompa ÖKC Mesajları

TİM ve YN Pompa ÖKC arasındaki mesajlar senkronize değildir ve bu mesajlar, herhangi bir sırayla ve herhangi bir zamanda iletilebilir. Gelen bir mesaj sonrasında, yanıt verilmeden önce başka mesajlar araya girebilir. Her mesaj, protokolde belirtilen ilgili yanıt mesajı, ACK veya NACK/HATA ile yanıtlanmalıdır. Bir istek üzerine yanıt alınamazsa, mesaj 1 saniye zaman aşımından sonra yeniden gönderilmelidir. Mesajı iptal etmeden önce üç kez yeniden gönderme denemesi yapılmalıdır. Bilinmeyen mesajlar, hatalı çerçeve ve yanlış CRC ile gelen mesajlar yok sayılır.

4.1 Mesaj Bileşenleri

Mesajlar üç bölümden oluşur:

- Mesaj başlığı
- Veri alanı
- Mesaj sonlandırıcısı

Mesaj başlığı, bir bayt açılış karakteri (STX) ve iki bayt döngüsel sayaçtan oluşur. Döngüsel sayaç, TİM ve YN Pompa ÖKC tarafından ayrı ayrı korunur. Veri alanı, bir bayt Mesaj Türü, iki bayt Veri alanı uzunluğu ve TLV (Etiket, Uzunluk, Değer) olarak yapılandırılmış çok baytlı veri alanından oluşur. Veri alanı olmayan mesajlar için, Veri alanı uzunluğu sıfıra eşittir. Etiket değeri, mesaj başına alan türü başına benzersizdir; bu, bir mesajdaki tekrarlanan alanların aynı Etiket ID'sine sahip olduğu ve Etiket ID'sinin iki farklı mesajda tekrar edilebileceği anlamına gelir. Uzunluk bilgisini kodlamak için TLV format kuralları uygulanacaktır. Uzunluk bilgisi aşağıdaki gibi tanımlanacaktır:

Uzunluk	Örnek
0..127	00..7F
128..255	81 80..FF
256..65535	82 01..FF 00..FF

Uzunluk 'xx' olarak işaretlenmişse, değer alanının gerçek uzunluğuna göre değişkendir.

Not: Gelecekteki uyumluluk için bilinmeyen TLV etiketleri yok sayılmalıdır.

Mesaj sonlandırıcısı, iki baytlık CRC ve bir baytlık mesaj sonlandırıcısından (ETX) oluşur.

4.2 TİM/YN Pompa ÖKC Mesajının Genel Yapısı

Alan Adı	Açıklama	Değer	Uzunluk
Mesaj Başlığı			
STX	Mesaj başlangıcı	0x02	1
MSG ID	Mesajı başlatan tarafından oluşturulan ardışık numara	Int16 (LSB önce)	2
Veri Alanı			
MSG Türü	TİM / YN Pompa ÖKC protokolünde genel komut		1
Veri alanı uzunluğu	Maksimum uzunluk 1600 bayt	Int16 (LSB önce)	2
Veri alanı	Mesaj verisi, iç yapısına bağlıdır	TLV	xx
Mesaj Sonlandırıcısı			
CRC-16/ARC	STX'ten (dahil) CRC alanına kadar (dahil değil)	Int16 (LSB önce)	2
ETX	Mesaj sonu	0x03	1

4.3 RS-485 Mesaj Şifrelemesi

RS-485 üzerinden iletilen tüm veri mesajları (mesaj türü 03), eşleşme sürecinde oluşturulan anahtarlar ve IV kullanılarak şifrelenir. Tüm veri yükü, STX (0x02) ve ETX (0x03) arasında yer alır ve AES256-CBC algoritması kullanılarak şifrelenir.

PKCS#7 formatında dolgu, verinin uzunluğunu 16 bayt (AES blok boyutu) katı olacak şekilde tamamlamak için verinin sonuna (sağ tarafına) eklenmelidir. Örneğin, 11 bayt eksikse, açık metin 0x0B değeri ile 11 bayt dolgu ile tamamlanmalıdır. Verinin uzunluğu 16'nın katı ise, 0x10 değeri ile tam 16 baytlık bir blok eklenmelidir.

- **Şifreleme Yöntemi**: AES256-CBC
- **Dolgu Formatı**: PKCS#7
- **Mesajlar**:
    - **YN Pompa ÖKC'den Gelen Mesajlar**: TİM tarafından aynı anahtar/IV ile şifrelenir ve çözülür.
    - **TİM'den Gelen Mesajlar**: Kenc-tim ve IVtim kullanılarak şifrelenir ve YN Pompa ÖKC tarafından aynı anahtar/IV ile çözülür.

5. Protokol Mesajlari

5.1 TİM'den YN Pompa ÖKC'ye Mesajların Veri Alanı

5.1.1 TİM: TTB Bağlantı ve Veri (0x61)

Bu mesaj, her TTO-TTB bağlantı değişikliğinde veya YN Pompa ÖKC'nin “TTB verilerini yeniden gönder” isteğine yanıt olarak gönderilir.

YN Pompa ÖKC'den ACK alınmalıdır. Eğer ACK alınmazsa, mesaj 1 saniye sonra tekrarlanır. Tekrarlama sayısı: 3’dür.

Eğer ACK alınmadan önce TTB bağlantı durumu değişirse, mevcut mesaj iptal edilir ve yeni bir mesaj gönderilir.

TİM: TTB Verisini Gönder- Mesaj Türü = 0x61

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
60h	2	Int16 (LSB önce) İlgili mesajın MSG ID'si	MSG ID	Mesaj 0x71'e yanıt olarak zorunlu
57h	4	String (ASCII hex)	TTO ID[1]	Zorunlu
42h	1	String ‘0’-‘9’	Bağlantı Durumu ‘0’= Bağlı değil[2] ‘1’= Yeni bağlı ‘2’= Aynı bağlı ‘3’= Yetkilendirme reddedildi[3]	Zorunlu
A8h	xx Max: 16	String (ASCII alfanümerik)	TİM Yazılım Sürümü	Zorunlu
85h	xx Max: 16	String (ASCII numerik)	Plaka Numarası	Zorunlu
8Ah	2	String (ASCII numerik)	Ürün ID	Zorunlu
91h	1	String (ASCII)	Sahip ID	Zorunlu
93h	1	String (ASCII)	UTTS-TTS (‘0’ Hayır ‘1’ Evet)	Zorunlu "Yetkilendirme türü" çevrimdışı olduğunda, varsayılan değeri '0': Hayır. (UTTS)

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
94h	1	String (ASCII)	Limit Türü (Para/Miktar) (‘0’: Hayır, ‘1’ ‘2’)	Zorunlu "Yetkilendirme türü" çevrimdışı olduğunda, varsayılan değeri '0': Hayır. (UTTS)
95h	xx Max: 9	String (ASCII)	Limit Değeri	Bağlantı durumu ‘1’ veya ‘2’ ise zorunlu Uzunluk pompa türü ile eşleşmelidir.
81h	1	String ‘0’ veya ‘1’	Yetkilendirme Türü ‘0’ çevrimiçi ‘1’ çevrimdışı	Bağlantı durumu ‘1’ veya ‘2’ ise zorunlu Eğer ödeme yöntemi Bitmap bit 0- VIS ve bit 4- UTTS-VIS ise (93h UTTS-TTS 1 (Evet) ise), işlem ve yetkilendirme türü 0 (çevrimiçi) olmalıdır.
82h	4	String (ASCII numerik)	İşlem Referans Numarası (0001-9999)	Bağlantı durumu ‘1’ veya ‘2’ ve yetkilendirme türü çevrimiçi ise zorunlu
8Dh	xx Max: 20	String (ASCII alfanümerik)	İstasyon Lisans ID	Zorunlu
8Fh	2	String (ASCII numerik)	Yetkilendirme Reddetme Kodu	Bağlantı durumu ‘3’ ise zorunlu
90h	xx Max: 30	String (ASCII alfanümerik)	Yetkilendirme Reddetme Açıklaması	Bağlantı durumu ‘3’ ise zorunlu

Notlar:

1. 1: **TTO ID**, nozul kurulumunda tanımlanan Pompa (Hex PPNN) değerini temsil eder. Örneğin, Pompa=26 Nozul=3 için TTO ID = “1A03” (=Hex 31 41 30 33).
2. 2: **Bağlantı durumu '0'**, hali hazırda bağlı olmayan bir nozul için alındığında YN Pompa ÖKC tarafından yok sayılır.
3. 3: **Bağlantı durumu ‘3’** olduğunda, işlem gerçekleştirilmez. TİM, YN Pompa ÖKC'ye plaka numarası ve reddetme nedenini bildirmek için TTB verilerini gönderir.

5.1.1.1 Sahip ID

Aşağıdaki tablo, mesajlarda kullanılan (yetkilendirme verisi, işlem raporu) sahip ID'lerini ve onların ondalık ve ASCII değerlerini listeler:

Sahip ID	Sahip Adı	Değerler (Ondalık)	ASCII Değeri
0	Bireysel Kiralama	“0”	0x30

Sahip ID	Sahip Adı	Değerler (Ondalık)	ASCII Değeri
1	Kurumsal Kiralama (Uzun Dönem)	“1”	0x31
2	Kurumsal Kiralama (Kısa Dönem)	“2”	0x32
3	Ayrılmış	“3”	0x33
4	Ayrılmış	“4”	0x34
5	Ayrılmış	“5”	0x35
6	Ayrılmış	“6”	0x36
7	Ayrılmış	“7”	0x37

5.1.1.2 Ürün ID Tanımları

- Aşağıdaki tablo, mesajlarda kullanılan (yetkilendirme verisi, işlem raporu) ürün ID'lerini ve onların ondalık ve ASCII değerlerini listeler:

Ürün ID	Ürün Adı	Değerler (ASCII)	ASCII Değeri
1	Kurşunsuz Benzin 95 Oktan	“01”	0x30 0x31
2	Kurşunsuz Benzin 95 Oktan E10	“02”	0x30 0x32
3	Kurşunsuz Benzin 98 Oktan	“03”	0x30 0x33
4	Motorin	“04”	0x30 0x34
5	Motorin 2 (Biyodizel Katkılı)	“05”	0x30 0x35
6	Otogaz LPG	“06”	0x30 0x36
7	Gazyağı	“07”	0x30 0x37
8	Yakıt Naftası	“08”	0x30 0x38
9	LNG	“09”	0x30 0x39
10	CNG	“10”	0x31 0x30
11	Elektrik	“11”	0x31 0x31
12	Adblue	“12”	0x31 0x32

13	Ayrılmış	“13”	0x31 0x33
14	Ayrılmış	“14”	0x31 0x34
15	Ayrılmış	“15”	0x31 0x35
16	Ayrılmış	“16”	0x31 0x36
17	Ayrılmış	“17”	0x31 0x37
18	Ayrılmış	“18”	0x31 0x38
19	Ayrılmış	“19”	0x31 0x39
20	Ayrılmış	“20”	0x32 0x30
21	Ayrılmış	“21”	0x32 0x31
22	Ayrılmış	“22”	0x32 0x32

- Aşağıda TTO-TTB bağlantı durumlarına ilişkin beklenen YN Pompa ÖKC davranışı verilmiştir (komut 0x61 Etiket 42h):

TTO-TTB Bağlantı Durumu	**YN Pompa ÖKC Beklenen Davranışı**
‘0’ = Bağlı değil	Pompayı durdur
‘1’ = Yeni bağlı	Pompayı başlat
‘2’ = Aynı bağlı	Pompa yakıt vermeye devam eder
‘2’-> ‘0’ = Bağlı değil	Pompayı durdur
‘2’-> ‘1’ = Yeni bağlı	Pompayı durdur
‘3’ = Yetkilendirme Reddedildi	YN Pompa ÖKC – Etiket 90h'ye göre hata mesajı gösterilmeli, işlem yapılmaz

5.1.2 TİM: Durum Yanıtı (0x67)

Bu mesaj Durum isteğine (0x77) yanıt olarak gönderilir.

TİM: Durum yanıtı gönder. Mesaj Türü = 0x67

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
60h	2	Int16 (LSB önce)	İlgili mesajın MSG ID'si	Zorunlu
A8h	xx Max: 16	String (ASCII alfanümerik)	TİM Yazılım Sürümü	Zorunlu
A1h	xx Max: 16	String (ASCII alfanümerik)	TİM Seri Numarası	Zorunlu
A9h	xx Max: 16	String (ASCII alfanümerik)	TİM Marka Adı	Zorunlu
AAh	xx Max: 16	String (ASCII alfanümerik)	TİM Üretici Modeli	Zorunlu
64h	4	Uint32 (LSB önce)	0x00000000 hata yoksa Hata Kodları bitleri. Hata mevcut olduğunda bit '1' olarak ayarlanır	Zorunlu

Hata kodları bitleri, hata mevcut olduğu sürece ayarlıdır.

Hata kodları bit tanımları:

Bit	Hata Kodu
Bit0	TİM_KAYITLI_DEĞİL
Bit1	ÇEVRİMDIŞI_İŞLEM_DEPOLAMASI_DOLU TİM'de saklanan maksimum çevrimdışıişlem sayısı 1000'dir. Bu limite ulaştığında veya 72 saat çevrimdışıolduğunda (hangisi önce gelirse), TİM yeni yakıt ikmalini kabul etmez.
Bit2	TİM_DEVRE_DIŞI_BIRAKILDI
Bit3	TİM_ÇEVRİMDIŞI_MODDA
Bit4	TİM_DEVRE_DIŞI_BIRAKILDI_YN_POMPA_ÖKC_SERİ_NUMARASI_EŞLEŞMİYOR
Bit5	TİM_YÜKSELTME_SÜRECİNİ_BAŞLAT
Bit6	HATALI_YN_POMPA_ÖKC_SÜRÜMÜ

Bit	Hata Kodu
Bit7-31	Ayrılmış

5.2 YN Pompa ÖKC'den TİM'e Mesajların Veri Alanı

5.2.1 YN Pompa ÖKC: TTB verilerini yeniden gönder (0x71)

Talep edilen TTO ID'sinin TTB verilerini yeniden gönderme isteği. TİM, "TTB Bağlantı ve Veri" mesajı (0x61) ile yanıt verir.

YN Pompa ÖKC: TTB verilerini yeniden gönder

Mesaj Türü = 0x71

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
57h	1 veya 4	String (ASCII hex) veya '0'	TTO ID	Zorunlu

4 TTO ID, nozul kurulumunda tanımlanan Pompa (Hex PPNN) değerini temsil eder. Örneğin, Pompa=26 Nozul=3 için TTO ID = "1A03" (=Hex 31 41 30 33).

Not: Bu mesaj, bağlantı durumu '0' olmayan herhangi bir TTO için (yani, aktif yakıt doldurma işlemi devam ediyorsa) düzenli aralıklarla (örneğin, 60 saniye) gönderilir. Eğer bu süre zarfında "FP bağlanma verisi" mesajı (0x61) alınmazsa, YN Pompa ÖKC nozul bağlantı durumu '0'a zorlanır; YN Pompa ÖKC, TTO durumunu "bağlı değil" olarak ayarlar.

YN Pompa ÖKC başlatıldığında veya TİM ile bağlantıyı yeniden kurduğunda, mevcut TTB bağlantı verilerini elde etmek için bu mesaj TTO ID '0' ile gönderilebilir. Bu, şu anda bağlı olan tüm TTO'lar için geçerlidir.

5.2.2 YN Pompa ÖKC: RTC'yi Güncelle (0x75)

YN Pompa ÖKC tarafından bağlantı kurulduktan sonra, her 24 saatte bir ve YN Pompa ÖKC tarafında zaman değiştirildiğinde TİM tarih ve saatini güncellemek için gönderilir. RTC-Verisi- YYYYMMDDhhmmss

YN Pompa ÖKC: RTC'yi Güncelle

Mesaj Türü = 0x75

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
59h	14	String – YYYYAAGGssddss	Mevcut YN Pompa ÖKC Tarih-Saat	Zorunlu

5.2.3 YN Pompa ÖKC: Durum İsteği (0x77)

YN Pompa ÖKC tarafından her n saniyede bir gönderilir. Varsayılan: n=1.

YN Pompa ÖKC: Durum Bilgisi

Mesaj Türü = 0x77

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
62h	1	String – '1'	Gelecek kullanım için değer	Zorunlu
A5h	xx Max: 16	String (ASCII alfanümerik)	YN Pompa ÖKC Yazılım Sürümü	Zorunlu
A0h	xx Max: 16	String (ASCII alfanümerik)	YN Pompa ÖKC Seri Numarası	Zorunlu
A6h	xx Max: 16	String (ASCII alfanümerik)	YN Pompa ÖKC Üretici Marka Adı	Zorunlu
A7h	xx Max: 16	String (ASCII alfanümerik)	YN Pompa ÖKC Üretici Modeli	Zorunlu

Not: TİM kayıtlı değilse, bir NACK mesajı ile yanıt verir ve TİM_KAYITLI_DEĞİL hata kodunu iletir. YN Pompa ÖKC'nin, TİM'in kayıtlı olmadığı durumu bildirmesi önerilir.

TTO ID = '0' olduğunda, TİM her bir mevcut TTB bağlantılı TTO için "TTB Bağlantı ve Veri" mesajı ile yanıt verir.

Not: YN Pompa ÖKC, TİM'den 4 saniye boyunca yanıt alamazsa yakıt doldurmayı askıya alır, çünkü TTO bağlantı durumu mevcut değildir.

TCP/IP için yalnızca aşağıdaki kurtarma prosedürü geçerlidir:

- **Durum Bilgisi Prosedürü:**

Üç ardışık Durum mesajına yanıt alınamaması durumunda, YN Pompa ÖKC bir kurtarma dizisine girer.

Kurtarma dizisi (YN Pompa ÖKC):

- Soketi kapatın.
- 1 saniye bekleyin.
- Soketi yeniden bağlayın.

5.2.4 YN Pompa ÖKC: İşlem Raporu (0x7B)

Bu mesaj, işlem tamamlandığında YN Pompa ÖKC tarafından gönderilir. YN Pompa ÖKC, TİM'den ACK alınana kadar bu mesajı göndermeye devam eder. YN Pompa ÖKC, işlemi TİM'in aldığı ve işlediğini belirten ACK mesajını gönderene kadar saklar

YN Pompa ÖKC: İşlem Raporu

Mesaj Türü = 0x7B

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
92h	4	String (ASCII numerik)	Fiş Numarası	Zorunlu
97h	4	String (ASCII numerik)	Z Numarası	Zorunlu
98h	4	String (ASCII numerik)	EKU Numarası	Zorunlu
A5h	xx Max: 16	String (ASCII alfanümerik)	YN Pompa ÖKC Yazılım Sürümü	Zorunlu
57h	4	String (ASCII hex)	TTO ID	Zorunlu Komut 0x61'de bildirilen değerle aynıdır.
85h	Xx Max: 11	String (ASCII alfanümerik) MSB solda	Plaka Numarası	Zorunlu Komut 0x61'de bildirilen değerle aynıdır.
59h	14	String – YYYYAAGGssddss	İşlem Tarih-Saat	Zorunlu
81h	1	Yetkilendirme Türü	‘0’ çevrimiçi, ‘1’ çevrimdışı	Zorunlu Komut 0x61'de bildirilen değerle aynıdır
82h	4	String (ASCII numerik) MSB solda	İşlem Referans Numarası (0001-9999)	Zorunlu Komut 0x61'de bildirilen değerle aynıdır.
83h	xx Max: 20	String (ASCII alfanümerik) MSB solda	Rezerve	Zorunlu
86h	xx Max: 10	String (ASCII numerik) MSB solda	Rezerve	Zorunlu
87h	xx Max: 12	String (ASCII numerik) MSB solda	Rezerve	Zorunlu
96h	xx Max: 12	String (ASCII numerik) MSB solda	KDV (Vergi Tutarı)	Zorunlu
88h	xx	String (ASCII numerik) MSB solda	Fiyat	Zorunlu

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
	Max: 8			
89h	xx Max: 40	String (ASCII alfanümerik) MSB solda	Ürün Adı	Opsiyonel Komut 0x61'de bildirilen değerle aynıdır.
8Ah	2	String (ASCII numerik) MSB solda	Ürün ID	Zorunlu Komut 0x61'de bildirilen değerle aynıdır.
8Bh	xx Max: 15	String (ASCII numerik) MSB solda	Rezerve	Zorunlu
8Eh	2	String (ASCII HEX) MSB solda	Rezerve	Zorunlu
91h	2	String (ASCII numerik) MSB solda	Sahiplik Türü	Zorunlu Komut 0x61'de bildirilen değerle aynıdır.

5.3 YN Pompa ÖKC ve TİM'in Ortak Mesajları

5.3.1 ACK (0x06)

YN Pompa ÖKC veya TİM: ACK

Mesaj Türü = 0x06

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
60h	2	Int16 (LSB önce) İlgili mesajın MSG ID'si	MSG ID	Zorunlu

5.3.2 NACK/HATA Raporu (0x15)

YN Pompa ÖKC veya TİM: NACK/HATA Raporu

Mesaj Türü = 0x15

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
60h	2	Int16 (LSB önce)	İlgili mesajın MSG ID'si	NACK için zorunlu, HATA raporu için isteğe bağlı
61h	4	Uint32 (LSB önce)	HATA Kodu	Zorunlu

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
63h	xx Max: 30	String (ASCII alfanümerik) MSB solda	HATA Kodu açıklaması (serbest metin)	Zorunlu

Mesajların Hata Kodları Listesi

Hata Kodu Tanımı	Değer
ZORUNLU_ETİKET_BULUNAMADI	0x00000001
GEÇERSİZ_VERİ	0x00000002
YANLIŞ_MESAJ_TİPİ (Yanlış Opcode)	0x00000003
YN_POMPA_ÖKC'DEN_TİM'E_YENİ_YAKIT_ALIMI_BAŞLATILAMIYOR*	0x00000004
EŞLEŞTİRME_HATASI (Eşleştirme Sonlandırıldı)	0x00000005

Bu hata, ilgili pompada TİM'e rapor edilmesi gereken, bekleyen bir işlem olduğunu belirtmek için YN Pompa ÖKC'den TİM'e gönderilir.

6. RS-485 RSA Eşleştirme Özeti

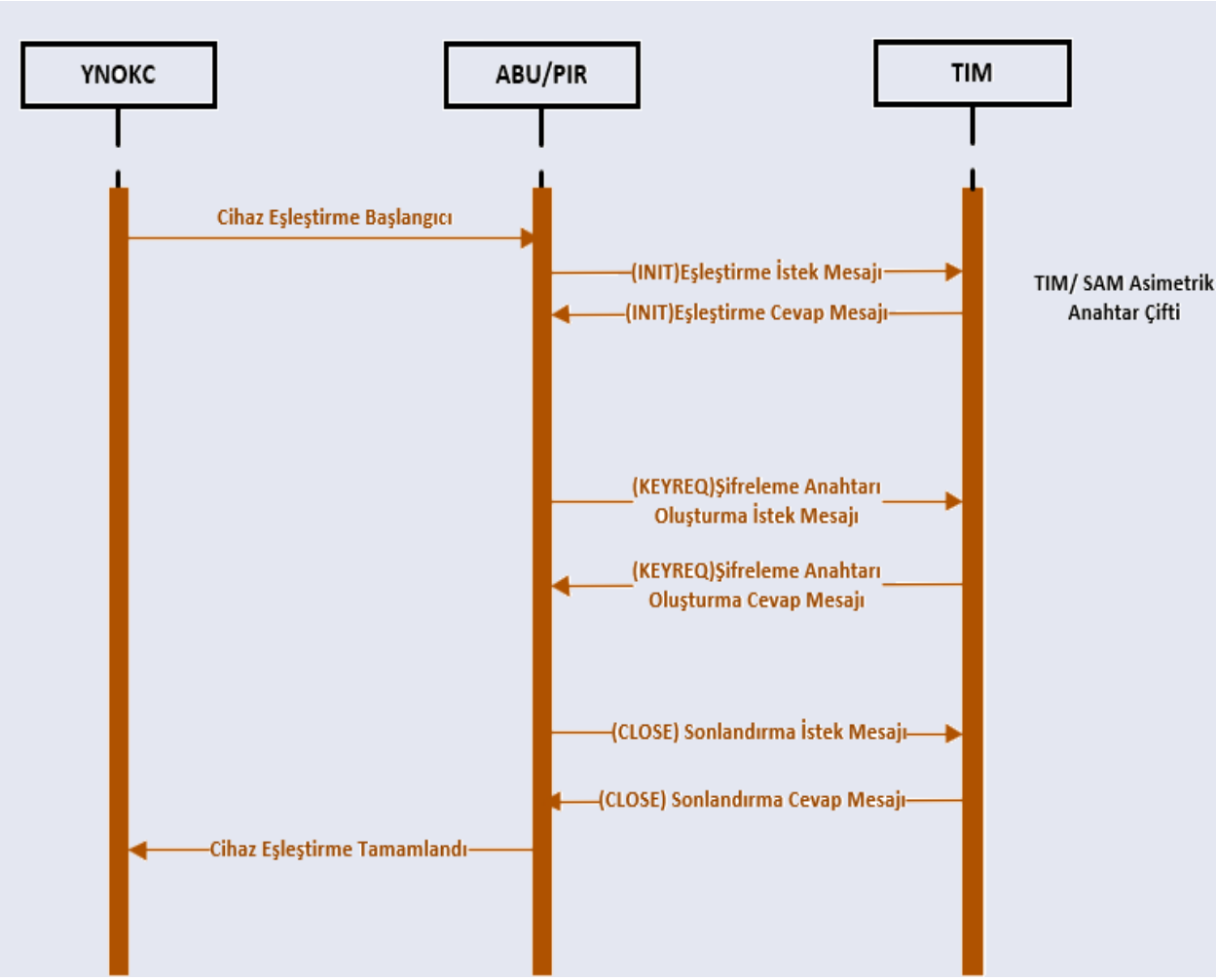
YN Pompa ÖKC -TİM RSA eşleştirme işlemi, cihazların RS-485 üzerinden kurulumu ve bağlantısı sonrasında gerçekleştirilmelidir. Eşleştirme işlemi, kimlik doğrulama ve anahtar değişimi için RSA şifrelemesini kullanır. Başarılı eşleştirmeden sonra, cihazlar eşleştirme işlemi ile oluşturulan anahtarları kullanarak şifreli veri mesajları alışverişi yapabilirler.

Eşleştirme işlemini başlatma ön koşulları:

- Veri merkezi ve/veya SAM Kart, TİM için bir RSA2048 anahtar çifti tahsis etmiştir.
- YN Pompa ÖKC seri numarası, yetkili servis teknisyeni tarafından TİM üzerinde yapılandırılır.
- TİM seri numarası YN Pompa ÖKC yetkili servis tarafından YN Pompa ÖKC üzerinde yapılandırılır.

6.1 Cihaz Eşleştirme İşlem Dizisi Diyagramı

Aşağıdaki diyagram, cihaz eşleştirme işleminde kullanılan istek ve yanıt dizisini tanımlar. RS-485 mesajları ve formatı, RS-485 Taşıma Sırasına uygun olmalıdır.



6.2 RS-485 Eşleştirme Mesajları

Yukarıdaki diyagramda detaylandırıldığı gibi, ilk iki eşleştirme mesajı şifrelenmemiştir. Bu iki mesaj alışverişinden sonra, cihazlar veri şifreleme anahtarlarını oluşturabilir ve üçüncü mesaj (Kapat) şifreli bir veri mesajı olarak gönderilir.

6.2.1 Eşleştirme Mesaj Formatı (02h)

- **INIT İstek/Yanıt (0x6D/0x7D)**
- **Anahtar (Key) İstek/Yanıt (0x6E/0x7E)**
- **NACK (0x15)** – Eşleştirme mesajında hata durumunda, NACK şifrelenmemiş olarak döndürülür.

Byte	Değer	Açıklama
1	FDh	Mesaj Başlangıcı Kodu
1	ADDR	Cihaz Adresi
1	DIR	Yön Baytı

Byte	Değer	Açıklama
1	YN Pompa ÖKC MSG ID	YN Pompa ÖKC Mesaj ID
1	TİM MSG ID	TİM Mesaj ID
1	02h	Mesaj Türü (INIT/Key/NACK)
2	Len	Veri Uzunluğu
xx	Data	Veri (Şifrelenmemiş)
2	CRC	CRC16-ARC
1	FEh	Mesaj Sonu Kodu

6.2.2 Şifreli Eşleştirme Mesaj Formatı (03h)

- **Kapat (Close) İstek/Yanıt (0x6F/0x7F)**

Byte	Değer	Açıklama
1	FDh	Mesaj Başlangıcı Kodu
1	ADDR	Cihaz Adresi
1	DIR	Yön Baytı
1	YN Pompa ÖKC MSG ID	YN Pompa ÖKC Mesaj ID
1	TİM MSG ID	TİM Mesaj ID
1	03h	Mesaj TÜRÜ (Şifreli Kapatma)
2	Len	Veri Uzunluğu
xx	Encrypted Data	Şifreli Veri
2	CRC	CRC16-ARC
1	FEh	Mesaj Sonu Kodu

6.3 Eşleştirme Mesajlarının Veri Alanı

6.3.1 YN Pompa ÖKC->TİM Başlatma İsteği (0x6D)

Bu mesaj, eşleştirme sürecini başlatmak için YN Pompa ÖKC tarafından gönderilir. TİM seri numaralarını doğrular, YN Pompa ÖKC versiyonunu, üretici ve model bilgilerini saklar ve Veri

Merkezi’nden bir RSA2048 genel anahtarı ister. Daha sonra Başlatma yanıtını (0x7D) döndürür. TİM verileri başarıyla doğrulamazsa, eşleştirme hata kodu ile NACK mesajı (0x15) döner.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx Max: 16	String (ASCII alfanumerik)	YN POMPA ÖKC Seri Numarası	Zorunlu
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TİM Seri Numarası	Zorunlu
A5h	xx Max: 16	String (ASCII alfanumerik)	YN POMPA ÖKC Yazılım Sürümü	Zorunlu
A6h	xx Max: 16	String (ASCII alfanumerik)	YN POMPA ÖKC Üretici Marka Adı	Zorunlu
A7h	xx Max: 16	String (ASCII alfanumerik)	YN POMPA ÖKC Üretici Modeli	Zorunlu

6.3.2 TİM-> YN Pompa ÖKC Başlatma Yanıtı (0x7D)

Bu mesaj, YN Pompa ÖKC'den gelen Başlatma isteğine yanıt olarak TİM tarafından gönderilir. YN Pompa ÖKC seri numaralarını ve genel anahtar parmak izini (isteğe bağlı) doğrular, TİM versiyonunu, üretici ve model bilgilerini saklar ve anahtar değişim adımına devam eder.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx Max: 16	String (ASCII alfanumerik) MSB sol	YN Pompa ÖKC Seri Numarası	Zorunlu
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TİM Seri Numarası	Zorunlu
A2h	xx Max: 500	ASCII Base64	TİM RSA2048 genel anahtarı, Base64 kodlanmış DER formatı	Zorunlu
A8h	xx Max: 16	String (ASCII alfanumerik)	TİM Yazılım Sürümü	Zorunlu
A9h	xx Max: 16	String (ASCII alfanumerik)	TİM Marka Adı	Zorunlu
AAh	xx	String (ASCII alfanumerik)	TİM Üretici Modeli	Zorunlu

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
	Max: 16			

6.3.3 YN Pompa ÖKC ->TİM Anahtar İsteği (0x6E)

Bu mesaj YN Pompa ÖKC tarafından gönderilir ve YN Pompa ÖKC tarafından üretilen bir anahtar (32 bayt) ile YN Pompa ÖKC rastgele (16 bayt) birleşimi içerir ve TİM genel anahtarı ile şifrelenmiştir. TİM bunu özel anahtar ile çözmek ve anahtarı ve YN Pompa ÖKC rastgele bilgisini almak için Veri Merkezi'ne gönderir, ardından Anahtar yanıtını (0x7E) döndürür. TİM verileri başarıyla doğrulamazsa, eşleştirme hata kodu ile NACK mesajı (0x15) döner.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx Max: 16	String (ASCII alfanumerik)	YN Pompa ÖKC Seri Numarası	Zorunlu
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TİM Seri Numarası	Zorunlu
A3h	256	Binary	Master Anahtar || YN Pompa ÖKC rastgele, TİM genel anahtarı ile RSA-OAEP ile şifrelenmiş	Zorunlu

6.3.4 TİM-> YN Pompa ÖKC Anahtar Yanıtı (0x7E)

Bu mesaj, YN Pompa ÖKC Anahtar isteğine yanıt olarak TİM tarafından gönderilir. TİM, YN Pompa ÖKC rastgele ile TİM rastgeleyi birleştirir ve anahtar ile AES256-CBC kullanarak şifreler. YN Pompa ÖKC bunu çözer ve rastgele bilgileri alır. YN Pompa ÖKC rastgele doğrulanır.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx Max: 16	String (ASCII alfanumerik) MSB sol	YN Pompa ÖKC Seri Numarası	Zorunlu
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TM Seri Numarası	Zorunlu
A4h	32	Binary	Master Anahtar || YN Pompa ÖKC rastgele, TİM genel anahtarı ile RSA-OAEP ile şifrelenmiş	Zorunlu

6.3.5 Veri Şifreleme Anahtarları ve IV Hesaplama

Başarılı anahtar değişim adımından sonra, her iki cihaz da anahtar ve YN Pompa ÖKC/TİM rastgele bilgilerine sahip olur ve veri şifreleme anahtarlarını oluşturabilir. Anahtar veri bloğu, TLS-PRF sahte rastgele fonksiyonunu kullanarak SHA256 hash ve aşağıdaki parametrelerle oluşturulur:

Secret = Anahtar (32 bayt)

Label = "YN Pompa ÖKC -TİM TİM_anahtarları"

Seed = YN Pompa ÖKC rastgele || TİM rastgele (32 bayt)

Output length = 96 bayt

Anahtar bloğu daha sonra veri anahtarlarını ve IV'leri aşağıdaki sırayla almak için bölünür:

Kenc-tim - TİM şifreleme anahtarı – 32 bayt

Kenc-ynpompaökc - YN Pompa ÖKC şifreleme anahtarı – 32 bayt

IVtim - TİM IV – 16 bayt

IVynpompaökc - YN Pompa ÖKC IV – 16 bayt

Her iki cihaz da şifreleme ve çözme için anahtarları ve IV'leri güvenli bir şekilde saklamalıdır.

6.3.6 YN Pompa ÖKC->TİM Şifreli Kapatma İsteği (0x6F)

Bu mesaj, eşleşme sürecini tamamlamak için YN Pompa ÖKC tarafından gönderilir. Eşleşme sürecinde oluşturulan anahtarlar kullanılarak şifrelenmiştir. TİM, mesajı çözer ve seri numaralarını doğrular, ardından şifreli bir Kapatma yanıtı (0x7F) döndürür. TİM verileri başarıyla doğrulamazsa, eşleştirme hata kodu ile NACK mesajı (0x15) döner.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx Max: 16	String (ASCII alfanumerik) MSB sol	YN Pompa ÖKC Seri Numarası	Zorunlu
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TİM Seri Numarası	Zorunlu

6.3.7 TİM-> YN Pompa ÖKC Şifreli Kapatma Yanıtı (0x7F)

Bu mesaj, YN Pompa ÖKC'den gelen Kapatma isteğine yanıt olarak TİM tarafından gönderilir. YN Pompa ÖKC, mesajı çözer ve seri numaralarını doğrular, ardından eşleştirme tamamlanır ve YN Pompa ÖKC, eşleştirmenin tamamlandığını TİM'e bildirir. Seri numaralarını doğrulamada başarısızlık durumunda, YN Pompa ÖKC'ye bir hata rapor edilmeli ve eşleştirme süreci baştan başlatılmalıdır.

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
A0h	xx	String (ASCII alfanumerik) MSB sol	YN Pompa ÖKC Seri Numarası	Zorunlu

Etiket	Uzunluk	Değer	Açıklama	Zorunlu
	Max: 16			
A1h	xx Max: 16	String (ASCII alfanumerik) MSB sol	TİM Seri Numarası	Zorunlu