TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

YENİ NESİL AKARYAKIT POMPA ÖKC ELEKTRONİK SERTİFİKA YAŞAM DÖNGÜSÜ

Doküman Kodu

REH.01.07

Revizyon No

03

Revizyon Tarihi

24.04.2024

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk Çıkış.	04.06.2021
01	Tanımlar, kısaltmalar ve şekillerde düzenleme yapıldı. Niteliksiz Elektronik Sertifika kullanımı kaldırıldı.	13.10.2022
02	YN Pompa ÖKC sertifika ömrü güncellendi.	08.11.2022
03	Sistemde Kullanılacak Sertifikalar tablosu güncellendi. İptal başvurusu alınması ile ilgili detaylar verildi. Başvuru formu isimleri güncellendi.	24.04.2024

TABLO LİSTESİ

ŞEKİL LİSTESİ

İÇİNDEKİLER

1 Amaç ve Kapsam

Bu dokümanın amacı, Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlarının (YN Pompa ÖKC) güvenli haberleşmesinde kullanılacak elektronik sertifikaların YN Pompa ÖKC üreticileri tarafından TÜBİTAK BİLGEM Kamu SM'den talep edilmesi, bu sertifikaların oluşturulması, güvenli olarak gönderilmesi, üreticilerde saklanması, cihazlara yüklenmesi, kontrol edilmesi ve imha edilmesi süreçlerinin ayrıntılı olarak anlatılmasıdır.

2 Sorumluluklar

Bu dokümanın hazırlanmasından ve güncellenmesinden Kamu Sertifikasyon Merkezi sorumludur.

3 Tanımlar ve Kısaltmalar

BES(Basic Electronic Signature):	Basit Elektronik İmza
BİM:	Bilgi İşlem Merkezi
ECDSA(Elliptic Curve Digital Signature Algorithm):	Eliptik Eğrili Sayısal İmza Algoritması
GİB:	Gelir İdaresi Başkanlığı
HSM:	Hardware Security Module (Donanımsal Güvenlik Modülü)
Kamu SM:	TÜBİTAK Kamu Sertifikasyon Merkezi
Nitelikli Elektronik Sertifika:	5070 sayılı kanuna göre güvenli elektronik imza oluşturmaya yarayan sertifika
ÖKC Üreticisi Sertifika Yetkilisi:	ÖKC üreticisi adına Kamu SM'den sertifika talebinde bulunabilecek kişi
PKCS#10:	Sertifika isteği için tanımlanmış dosya biçimi standardı
RSA	Rivest Shamir Adleman (Algoritmayı bulan kişilerin baş harfleri)
SHA(Secure Hash Algorithm):	Güvenli Özet Algoritması
TSM(Trusted Service Manager):	Üretici firmanın YN ÖKC'leri kontrol edip yönettiği merkez
XAdES(XML Advanced Electronic Signature):	XML Gelişmiş Elektronik İmza
YN Pompa ÖKC:	Mükellefe ait mali verileri elektronik ortamda güvenli olarak ileten IP tabanlı Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazı

4 Uygulama

4.1 Genel Yaşam Döngüsü Yapısı

YN Pompa ÖKC'lerin GİB ve ÖKC üreticileri ile güvenli haberleşmesinde kullanılacak olan sertifikalar TÜBİTAK BİLGEM Kamu SM tarafından üretilecektir. Sertifikalar üretildikten sonra ÖKC üreticilerine teslim edilerek cihazlarının içerisine güvenli olarak yüklenmesi sağlanacaktır.

- YN Pompa ÖKC'nin GİB Sistemlerine mali verileri göndermesi amacıyla yapacağı haberleşmede YN Pompa ÖKC'nin BİM'i doğrulaması gerekmektedir. Bu doğrulama BİM'e verilecek SSL sertifikası ile sağlanacaktır. YN Pompa ÖKC ile BİM arasında tek taraflı bir kimlik doğrulama gerçekleşecektir.

- YN Pompa ÖKC sertifikası ise, BİM'e SSL üzerinden gönderilecek mali verinin değişmezliğinin sağlanması ve BİM'in gelen verinin YN Pompa ÖKC'den geldiğini doğrulaması için gönderilecek verinin YN Pompa ÖKC tarafından XAdES-BES (enveloped) formatında imzalanması amacıyla kullanılacaktır.

- ÖKC üreticisi TSM'nin paramatre yükleme vb. işlemler için YN Pompa ÖKC ile haberleşmesinde, YN Pompa ÖKC'nin ÖKC TSM'yi doğrulama gereksinimi vardır. Bu doğrulama ÖKC TSM'ye verilecek SSL sertifikası ile sağlanacaktır. ÖKC TSM ve YN Pompa ÖKC'ler arasında tek taraflı bir kimlik doğrulama gerçekleştirilecektir.

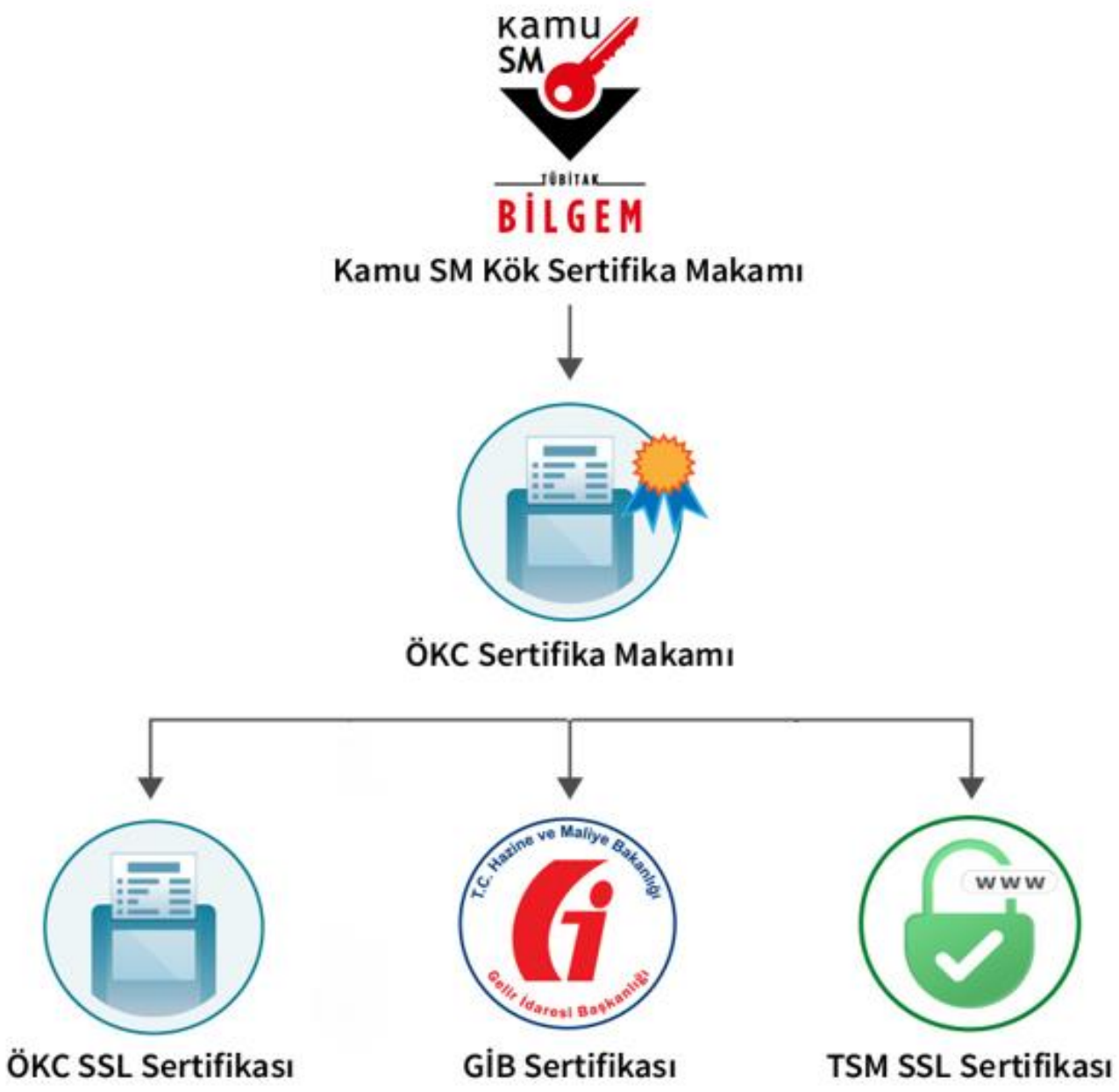
4.1.1 Sistemde Tanımlı Sertifikalar

Sistemde kullanılacak sertifikalar Tablo 1: Sistemde Kullanılacak Sertifikalar tablosunda, sertifikaların hiyerarşideki yerleri ise Şekil 1: Anahtar ve Sertifikalar alanında verilmiştir.

Sertifika İsmi	Anahtar Kullanımı	Gelişmiş Anahtar Kullanımı	İmzalama Algoritması	Kullanılan Anahtar	Açıklama
YN Pompa ÖKC Sertifikası	Digital Signature, Key Encipherment	Server Authentication, Client Authentication,	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	YN Pompa ÖKC'lerin GİB ile kuracağı bağlantıda mali verinin XAdES- BES (enveloped) formatında imzalanması için kullanılan sertifikadır.
BİM Uygulama Sunucusu SSL Sertifikası	Digital Signature, Key Encipherment	Server Authentication, Client Authentication	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	YN Pompa ÖKC'nin BİM ile kuracağı SSL bağlantısında BİM'i doğrulaması

					için kullanılacak sertifikadır.
ÖKC TSM SSL Sertifikası	Digital Signature, Non-Repudiation, Key Encipherment	Server Authentication, Client Authentication	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	ÖKC TSM'in kimliğini doğrulayan SSL sertifikasıdır. ÖKC TSM, YN Pompa ÖKC'ler ile tek taraflı SSL kullanarak haberleşecektir. Böylelikle sadece yetkili TSM YN Pompa ÖKC'ye erişecektir.
YN Pompa ÖKC Test Sertifikası	Digital Signature, Key Encipherment	Server Authentication, Client Authentication	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	YN Pompa ÖKC üreticilerinin YN Pompa ÖKC geliştirirken kullanacakları sertifikalardır. Soft ve kartlı olarak üretilebilmektedir.

Tablo 1: Sistemde Kullanılacak Sertifikalar



Şekil 1: Anahtar ve Sertifikalar

4.1.2 Sertifikaların Talep Edilmesi

Gelir İdaresi Başkanlığı tarafından yetkilendirilmiş YN Pompa ÖKC üreticileri Kamu SM'den sertifika talebinde bulunabilecektir. Kamu SM'den sertifika talep edecek olan YN Pompa ÖKC üreticisi, firma bilgilerini ve sertifika talep yetkilisi bilgilerini GİB'e bildirecektir. GİB'in bu bilgileri resmi olarak Kamu SM'ye iletmesiyle süreç başlayacaktır. YN Pompa ÖKC sertifikası talebinde bulunmak için YN Pompa ÖKC üreticisi Sertifika Talep Yetkilisinin, "Sırasız ÖKC Sertifika Başvuru Listesi"ni doldurup, kendisine ait Nitelikli Elektronik Sertifikası (NES)

veya ıslak imza ile imzaladıktan sonra okc@kamusm.gov.tr adresine e-posta ile göndermesi gerekmektedir. Islak imza ile yapılan başvurularda, listenin ıslak imzalı hali Kamu Sertifikasyon Merkezi TÜBİTAK Gebze Yerleşkesi Gebze-KOCAELİ adresine gönderilmelidir.

4.1.3 Sertifika Üretim Süreci ve Müşteriye Teslimi

4.1.3.1 Sertifika Üretimi

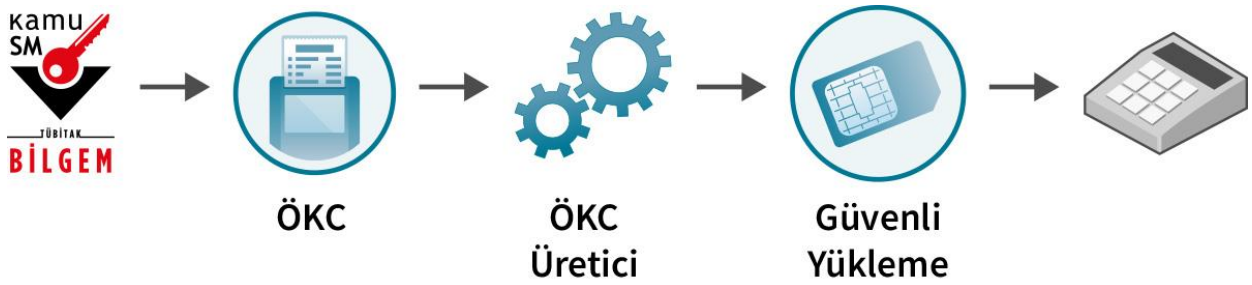
Kamu SM'ye ulaşan "ÖKC Sertifikası Talep Formu" incelenerek formdaki bilgiler ve imza kontrol edildikten sonra eksik veya yanlış bilgi var ise e-posta ile ilgili kısımlar bildirilerek düzeltilmesi talep edilecektir. Düzeltmeler tamamlandıktan sonra üretime başlanacaktır. Üretilecek YN Pompa ÖKC Sertifikası, YN Akaryakıt Pompa ÖKC Gelir İdaresi Başkanlığı Mesaj Protokolü (GMP) teknik şartnamelerinde belirtilen formata uygun olacaktır. Sertifika üretimi tamamlandıktan sonra ÖKC üreticisi sertifika yetkilisi eposta ile bilgilendirilecektir.

SSL Sertifikaları Kamu SM tarafından üretilecektir. SSL sertifikalarının üretilebilmesi için GİB ve ÖKC üreticileri kullanacakları HSM'lerde SSL anahtar çiftini oluşturacaktır. Açık anahtardan PKCS#10 istek dosyalarını oluşturacaklar ve Kamu SM'ye göndereceklerdir, istek dosyası oluşturamayan kurumlar destek talep edebilirler. Kamu SM HSM destek ekibi talep sahibi kurumun HSM'lerine bağlanarak anahtar çifti ve isteği oluşturulacak ve Kamu SM'deki ilgili birime iletilecektir. Kamu SM istek dosyalarını işleme alarak SSL sertifikalarını oluşturacak, GİB ve ÖKC üreticilerine teslim edecektir.

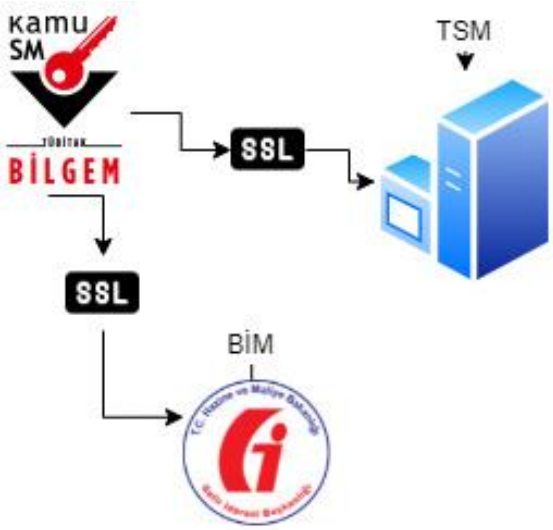
4.1.3.2 Akıllı Kartta Teslim

YN Pompa ÖKC'ler için üretilen sertifikalar akıllı kartlara yüklendikten sonra kurye aracılığıyla teslimatları sağlanacaktır.

Özet Akışlar

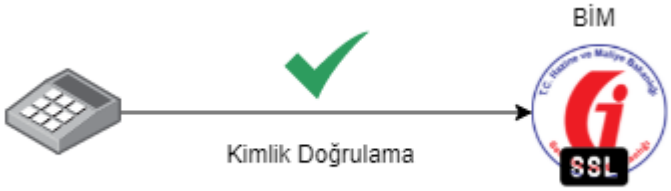


Şekil 2: TÜBİTAK'ın ürettiği ÖKC sertifikalarının ÖKC cihazına yüklenmesi



Şekil 3: TÜBİTAK, GİB-BİM ve TSM için SSL sertifikası üretir

a. *YN Pompa ÖKC'nin GİB Sistemlerine mali verileri göndermesi amacıyla yapacağı haberleşmede YN Pompa ÖKC'nin BİM'i doğrulaması gerekmektedir. Bu doğrulama BİM'e verilecek SSL sertifikası ile sağlanacaktır. YN Pompa ÖKC ile BİM arasında tek taraflı bir kimlik doğrulama gerçekleşecektir.*



Şekil 4: GİB-BİM'in kimliğinin SSL sertifikası ile doğrulanması

b. *YN Pompa ÖKC sertifikası ise, BİM'e SSL üzerinden gönderilecek mali verinin değişmezliğinin sağlanması ve BİM'in gelen verinin YN Pompa ÖKC'den geldiğini doğrulaması için gönderilecek verinin YN Pompa ÖKC tarafından Xades-Bes (enveloped) formatında imzalanması amacıyla kullanılacaktır.*

Şekil 5: ÖKC'nin GİB'e veri göndermesi

c. *ÖKC üreticisi TSM'nin paramatre yükleme vb işlemler için YN Pompa ÖKC ile haberleşmesinde, YN Pompa ÖKC'nin ÖKC TSM'yi doğrulama gereksinimi vardır. Bu doğrulama ÖKC TSM'ye verilecek SSL sertifikası ile sağlanacaktır. ÖKC TSM ve YN Pompa ÖKC'ler arasında tek taraflı bir kimlik doğrulama gerçekleştirilecektir.*

Şekil 6: GİB-BİM'in kimliğinin SSL sertifikası ile doğrulanması

4.1.4 Sertifikaların Üretici Tarafında Saklanması

Akıllı kartta verilen sertifikaların üretici firmalar tarafından yedeklenmesi söz konusu olmayacaktır. Olası olumsuz bir durumda ilgili YN Pompa ÖKC'ye yeni sertifika üretilecektir.

4.1.5 Sertifikaların Cihaza Yüklenmesi

Akıllı kartta verilen sertifikalar cihaza takılarak kullanılacaktır.

4.1.6 Bakım veya Arıza Durumunda Sertifikaların Yeniden Yüklenmesi

Sertifikanın akıllı karta yüklü olarak verildiği bir YN Pompa ÖKC'ye yeni bir sertifika yüklenmesi söz konusu olduğunda cihaz için yeni sertifika yeni bir akıllı karta yüklenecek ve üretici firmaya kurye ile iletilecektir.

4.1.7 Sertifikaların İptal Edilmesi

YN Pompa ÖKC'ler için üretilecek sertifikanın geçerlilik süresi GİB tarafından belirlenmiştir ve bu süre 11 yıldır. Fakat bir mükellefin ticari faaliyetlerini sonlandırması ya da YN Pompa ÖKC'nin tamir edilemeyecek şekilde arızalanması durumunda cihaz üzerindeki sertifikanın kötüye kullanılmasının engellenmesi için sertifikanın ivedi olarak iptal edilmesi gerekmektedir. YN Pompa ÖKC sertifikasının iptal edilmesi gerektiği durumda, bu cihazın seri numarasını, üretici firmanın ÖKC üreticisi sertifika yetkilisi Kamu SM'ye bildirecek ve Kamu SM bu sertifikayı iptal edecektir. Bu şekilde sertifikanın bilinçli veya bilinçsiz olarak kötüye kullanılmasının önüne geçilecektir.

Kamu SM'ye bildirim okc@kamusm.gov.tr veya bilgi@kamusm.gov.tr adresine iptal edilecek sertifikalara ait bilgilerin iletilmesi ile gerçekleştirilecektir. Bu bildirimlerde yetkili kişiden gelen ıslak imzalı dokümanın doğrulama işlemlerinden sonra sertifika iptal edilecektir.

4.1.8 Sertifikaların Amacı Dışında Kullanılması

Üreticilere teslim edilen sertifikaların amacı dışında kullanılması durumunda oluşacak olumsuz duruma neden olan kişi veya kurumun tespit edilebilmesi amacıyla Kamu SM ürettiği sertifikalara ait kayıtları tutacaktır. Gerektiği durumda bu bilgileri GİB ve adli kurumlarla paylaşacaktır.