

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

YENİ NESİL ÖKC SAYISAL SERTİFİKA YAŐAM DÖNGÜSÜ

Doküman Kodu

REH.01.03

Revizyon No

06

Revizyon Tarihi

08.11.2022

TASNİF DIŐI

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk çıkıő.	21.05.2013
01	Tanımlar alanında ve Őekillerde güncelleme yapılmıőtır.	01.07.2015
02	Doküman yeni Őablona aktarılmıőtır. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde REHB-001-012 kodu ile yer almaktadır.	28.05.2018
03	İmla hataları düzeltilmiőtir.	20.06.2018
04	Logo güncellendi. Tanımlar, kısaltmalar ve Őekillerde düzenleme yapıldı. Soft ÖKC Sertifikalarının iletirme süreci ve Sertifika başvuru süreci güncellendi. Niteliksiz Elektronik Sertifika kullanımını kaldırıldı.	23.09.2022
05	Tanımlar ve Kısaltmalar kısmında düzenleme yapıldı. İçindekiler bölümü güncellendi.	14.10.2022
06	YN ÖKC sertifika ömrü güncellendi.	08.11.2022

Tablolar Listesi

Tablo 1: Sistemde Kullanılacak Sertifikalar..... 5

Őekiller Listesi

Őekil 1: Anahtar ve Sertifikalar 6

İÇİNDEKİLER

1	<i>Amaç ve Kapsam</i>	4
2	<i>Sorumluluklar</i>	4
3	<i>Tanımlar ve Kısaltmalar</i>	4
4	<i>Uygulama</i>	5
4.1	Sistemde Tanımlı Sertifikalar	5
4.2	Sertifikaların Talep Edilmesi	6
4.3	Sertifika Üretim Süreci ve Müşteriye Teslimi	7
4.3.1	Sertifika Üretimi.....	7
4.3.2	Soft Sertifika Üretimi ve Elektronik Ortamda Teslimi.....	7
4.3.3	Akıllı Kartta Üretim ve Teslim	7
4.4	Aynı YN ÖKC İçin Yeniden Sertifika Üretilmesi	7
4.5	Sertifikaların İptal Edilmesi	8
4.6	Sertifikaların Amacı Dışında Kullanılması	8
4.7	Diğer Sertifikalar	8

1 Amaç ve Kapsam

Bu dokümanda, YN ÖKC'lerin güvenli haberleşmesinde kullanılacak sayısal sertifikaların YN ÖKC üreticileri tarafından TÜBİTAK BİLGEM Kamu SM'den talep edilmesi, bu sertifikaların Kamu SM tarafından oluşturulması, güvenli olarak YN ÖKC üreticisine gönderilmesi ve iptal edilmesi ile ilgili süreçler ayrıntılı olarak anlatılmaktadır.

2 Sorumluluklar

Bu sürecin yürütülmesinden Elektronik Sertifika Hizmetleri ve Müşteri İlişkileri Birimi; koordinasyon ve takibinden ise Elektronik İmza Teknolojileri Birimi sorumludur.

3 Tanımlar ve Kısaltmalar

ECDSA(Elliptic Curve Digital Signature Algorithm):	Eliptik Eğrili Sayısal İmza Algoritması
GİB:	Gelir İdaresi Başkanlığı
Güvenli Alan:	YN ÖKC'lere anahtar ve sertifika yükleme yapılacak olan ve kural koyucular ile TÜBİTAK tarafından denetlenen güvenlik seviyesi belirlenmiş özel yerler
Kamu SM:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.
NES:	5070 sayılı Elektronik İmza Kanunu'nun 9'uncu maddesinde sayılan nitelikleri haiz Nitelikli Elektronik Sertifika
ÖKC Üreticisi Sertifika Talep Yetkilisi:	YN ÖKC Üreticisi adına Kamu SM'den sertifika talebinde bulunabilecek kişi
PKF:	PKCS#12 standardında tanımlanmış dosya biçimi
PKCS#10:	Sertifika isteği için tanımlanmış dosya biçimi standardı
PKCS#12:	X.509 sertifikasıyla gizli/özel anahtarın elektronik ortamda güvenli olarak saklanması ve dağıtılması için tanımlanmış dosya biçimi standardı
SHA(Secure Hash Algorithm):	Güvenli Özet Algoritması
TSM(Trusted Service Manager):	Üretici firmanın YN ÖKC'leri kontrol edip yönettiği merkez
YN ÖKC:	Mükellefe ait mali verileri elektronik ortamda güvenli olarak ileten Yeni Nesil Ödeme Kaydedici Cihazı

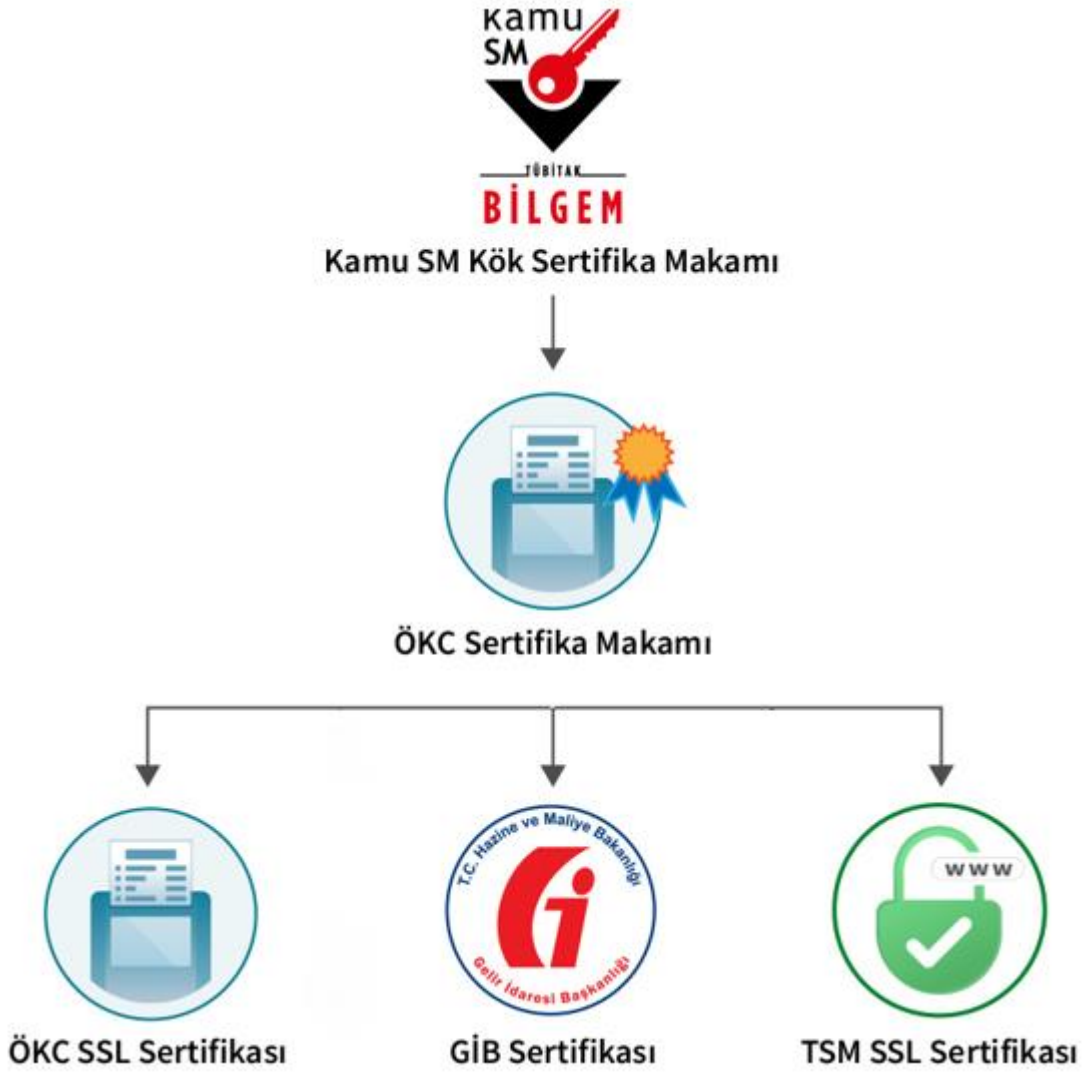
4 Uygulama

4.1 Sistemde Tanımlı Sertifikalar

Sistemde kullanılacak sertifikalar Tablo 1: Sistemde Kullanılacak Sertifikalar'da, kurumlarla iliŐkileri ise Őekil 1: Anahtar ve Sertifikalar'da verilmiŐtir.

Sertifika İsmi	Sertifika Ömrü	İmzalama Algoritması	Kullanılan Anahtar	Açıklama
YN ÖKC Sertifikası	11 yıllık üretilmektedir.	SHA384 with ECDSA	384 bit ECDSA	YN ÖKC'nin kimliĐini doĐrulayan ve güvenli haberleŐmesini saĐlayan sertifikadır.
GİB Sertifikası	3 yıllık üretilmektedir.	SHA384 with ECDSA	384 bit ECDSA	GİB kimliĐini doĐrulayan ve güvenli haberleŐmesini saĐlayan sertifikadır.
ÖKC TSM SSL Sertifikası	3 yıllık üretilmektedir.	SHA384 with ECDSA	384 bit ECDSA	ÖKC TSM'in kimliĐini doĐrulayan SSL sertifikasıdır. ÖKC TSM, YN ÖKC'ler ile tek taraflı SSL kullanarak haberleŐecektir. Böylelikle sadece yetkili TSM YN ÖKC'ye erişecektir.
YN ÖKC Test Sertifikaları	6 aylık üretilmektedir.	SHA384 with ECDSA	384 bit ECDSA	YN ÖKC üreticilerinin YN ÖKC geliŐtirirken kullanacakları sertifikalardır. Soft ve kartlı olarak üretilebilmektedir.

Tablo 1: Sistemde Kullanılacak Sertifikalar



Őekil 1: Anahtar ve Sertifikalar

4.2 Sertifikaların Talep Edilmesi

TÜBİTAK BİLGEM tarafından yapılacak denetimlerden (cihazların YN ÖKC Teknik Kılavuzlarında belirtilen şartlara uyumluluk denetimi ve soft sertifikaların YN ÖKC'lere yükleneceđi Güvenli Alan'ın YN ÖKC Sayısal Sertifika Koruma Kılavuzu'nda belirtilen şartlara uyumluluk denetimi) başarıyla geçmiş, GİB tarafından onaylanmış ve onay yazısı Kamu SM'ye gönderilmiş YN ÖKC(ler) için YN ÖKC üreticileri, Kamu SM'den ÖKC Sertifika talebinde bulunabilecektir. Kamu SM'den ilk defa YN ÖKC Sertifika talep edecek YN ÖKC Üreticisi, firma bilgilerinin ve ÖKC Üreticisi Sertifika Talep Yetkilisi olarak atanacak kişinin bilgilerinin yer aldığı YN ÖKC Üreticisi Başvuru Formu'nu Kamu Sertifikasyon Merkezi TÜBİTAK Gebze Yerleşkesi Gebze-KOCAELİ adresine gönderecektir.

YN ÖKC sertifikası talebinde bulunmak için ÖKC Üreticisi Sertifika Talep Yetkilisinin, YN ÖKC Sertifika Başvuru Listesini doldurup, kendisine ait Nitelikli Elektronik Sertifikası (NES) veya ıslak imza ile imzladıktan sonra okc[at]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.

ÖKC Üreticisi Sertifika Talep Yetkilisi tarafından doldurulmuş ve imzalanmış olarak Kamu SM'ye iletilen YN ÖKC Sertifika Başvuru Listesi, Kamu SM'de ilgili kişiler tarafından incelenecektir. YN ÖKC Sertifika Başvuru Listesinde sertifikalandırılacak YN ÖKC'lerin seri numaralarının ve sertifika tipinin (soft/kartlı) belirtilmesi zorunludur.

YN ÖKC Üreticisi Başvuru Formu'nun ve YN ÖKC Sertifika Başvuru Listesinin gönderilmemiş olması ya da beyan edilen bilgilerin ve imzanın yapılan kontroller ardından eksik veya yanlış olduğunun anlaşılması halinde ÖKC Üreticisi Sertifika Talep Yetkilisi e-posta yoluyla bilgilendirilecektir. Yetkili, gerekli düzeltmeleri yaptıktan sonra Kamu SM üretimi gerçekleştirecektir.

4.3 Sertifika Üretim Süreci ve Müşteriye Teslimi

4.3.1 Sertifika Üretimi

ÖKC Üreticisi, Sertifika Talep Yetkilisi tarafından YN ÖKC Sertifika Başvuru Listesinin tam ve doğru bir şekilde doldurulup imzalı olarak Kamu SM'ye iletilmesinin ardından YN ÖKC sertifikaları talebe göre soft veya kartlı olarak üretilmektedir.

4.3.2 Soft Sertifika Üretimi ve Elektronik Ortamda Teslimi

YN ÖKC'ler için üretilen soft sertifikalar, PFX (PKCS#12) formatında üretilmektedir. Başvuru listesinde belirtilen seri numaralarına göre her bir YN ÖKC için bir adet .pfx dosyası oluşturulur. .pfx dosya içeriğinde özel-açık anahtar çifti ve sertifika bulunmaktadır. Oluşturulan .pfx dosyaları sunucuya yüklenerek firmaya güvenli şekilde iletilir. 10 iş günü sonunda soft sertifikalar Kamu SM tarafından geri alınamayacak şekilde silinir.

Soft olarak YN ÖKC üreticisi firmaya iletilen sertifikalar YN ÖKC'lere Güvenli Alan'da yüklenmelidir. Güvenli Alan dışındaki alanlarda YN ÖKC'lere sertifika yüklenmesi yasaktır.

4.3.3 Akıllı Kartta Üretim ve Teslim

YN ÖKC'ler için üretilen sertifikalar akıllı kartlara yüklendikten sonra akıllı kartlar ilgili üretici firmaya kurye aracılığıyla teslim edilir.

4.4 Aynı YN ÖKC İçin Yeniden Sertifika Üretilmesi

YN ÖKC Sertifikasının silinmesi/bozulması gibi sertifikanın kullanılamaz hale geldiği durumlarda YN ÖKC'ye yeni bir sertifikanın yüklenmesi gerekmektedir.

Sertifikanın akıllı karta yüklü olarak verildiđi bir YN ÖKC'ye yeni bir sertifikanın yüklenmesi söz konusu olduđunda, Kamu SM tarafından YN ÖKC için yeni bir sertifika üretilecek ve yeni bir akıllı karta yüklenerek kurye ile gönderilecektir.

Sertifikanın soft olarak yüklendiđi bir YN ÖKC'ye sertifikanın yeniden yüklenmesi söz konusu olduđunda ise YN ÖKC için yeni bir sertifika üretilecek ve iletilecektir. Soft olarak YN ÖKC üreticisi firmaya iletilen sertifika YN ÖKC'ye Güvenli Alan'da yüklenecektir.

4.5 Sertifikaların İptal Edilmesi

YN ÖKC'ler için üretilecek sertifikanın geçerlilik süresi GİB tarafından belirlenmiŐtir ve bu süre 11 yıldır. Fakat bir mükellefin ticari faaliyetlerini sonlandırması, YN ÖKC'nin tamir edilemeyecek şekilde arızalanması durumunda cihaz üzerindeki sertifikanın kötüye kullanılmasının engellenmesi için ivedi olarak iptal edilmesi gerekmektedir.

YN ÖKC sertifikasının iptal edilmesi gerektiđi durumda, iptal edilecek cihazın/cihazların seri numarasının/numaralarının bulunduđu sertifika listesi ÖKC Sertifika Talep Yetkilisi tarafından yetkiliye ait NES ya da ıslak imza ile imzalanarak e-posta ile Kamu SM'ye iletilecektir. İmza dođrulama işlemleri yapıldıktan sonra sertifika/sertifikalar Kamu SM tarafından iptal edilecektir. Böylelikle belirtilen sertifika/sertifikalar, sertifika iptal listesine girecektir ve bilinçli veya bilinçsiz olarak kötüye kullanımın önüne geçilecektir.

4.6 Sertifikaların Amacı DıŐında Kullanılması

YN ÖKC üreticileri, aldıkları sertifikaların güvenli olarak kullanılmasından sorumludur. Üreticilere teslim edilen sertifikaların amacı dıŐında kullanılması durumunda oluşacak olumsuz duruma neden olan kiŐi veya kurumun tespit edilebilmesi amacıyla Kamu SM ürettiđi sertifikalara ait kayıtları tutacaktır. Gerektiđi durumda bu bilgileri GİB ve adli kurumlarla paylaşacaktır.

4.7 Diđer Sertifikalar

GİB Sertifikası ve ÖKC TSM SSL Sertifikası Kamu SM tarafından üretilecektir. Bu sertifikaların üretilebilmesi için GİB ve YN ÖKC üreticileri kullanacakları HSM'lerinde anahtar çiftlerini ve bu anahtarlardan PKCS#10 istek dosyalarını oluşturacak ve istek dosyalarını Kamu SM'ye iletceklerdir. Kamu SM bu istek dosyalarını işleyerek sertifikaları oluşturacak, GİB ve YN ÖKC üreticilerine iletacaktır.

Kamu SM, YN ÖKC üreticilerinin talep etmesi durumunda soft ve kartlı olarak YN ÖKC Test Sertifikası SM üretecektir.