TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

YENİ NESİL ÖKC SAYISAL SERTİFİKA YAŞAM DÖNGÜSÜ

Doküman Kodu

REH.01.03

Revizyon No

07

Revizyon Tarihi

18.04.2024

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk çıkış.	21.05.2013
01	Tanımlar alanında ve şekillerde güncelleme yapılmıştır.	01.07.2015
02	Doküman yeni şablona aktarılmıştır. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde REHB-001-012 kodu ile yer almaktadır.	28.05.2018
03	İmla hataları düzeltilmiştir.	20.06.2018
04	Logo güncellendi. Tanımlar, kısaltmalar ve şekillerde düzenleme yapıldı. Soft ÖKC Sertifikalarının iletilme süreci ve Sertifika başvuru süreci güncellendi. Niteliksiz Elektronik Sertifika kullanımı 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
07	Sistemde tanımlı sertifikalar tablosu güncellendi. Başvuru formu isimleri güncellendi. Başvuru yöntemi düzenlendi. Diğer sertifikalar için istek üretim süreci güncellendi.	18.04.2024

Tablolar Listesi

Şekiller Listesi

İÇİNDEKİLER

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 dokümanın hazırlanmasından ve güncellenmesinden Kamu Sertifikasyon Merkezi sorumludur.

3 Tanımlar ve Kısaltmalar

ECDSA(Elliptic Curve Digital Signature Algorithm):	Eliptik Eğrili Sayısal İmza Algoritması
GİB:	**G**elir **İ**daresi **B**aşkanlığı
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 **N**itelikli **E**lektronik **S**ertifika
ÖKC Üreticisi Sertifika Talep Yetkilisi:	YN ÖKC Üreticisi adına Kamu SM'den sertifika talebinde bulunabilecek kişi
PFX:	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
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
YN ÖKC:	Mükellefe ait mali verileri elektronik ortamda güvenli olarak ileten **Y**eni **N**esil **Ö**deme **K**aydedici **C**ihazı

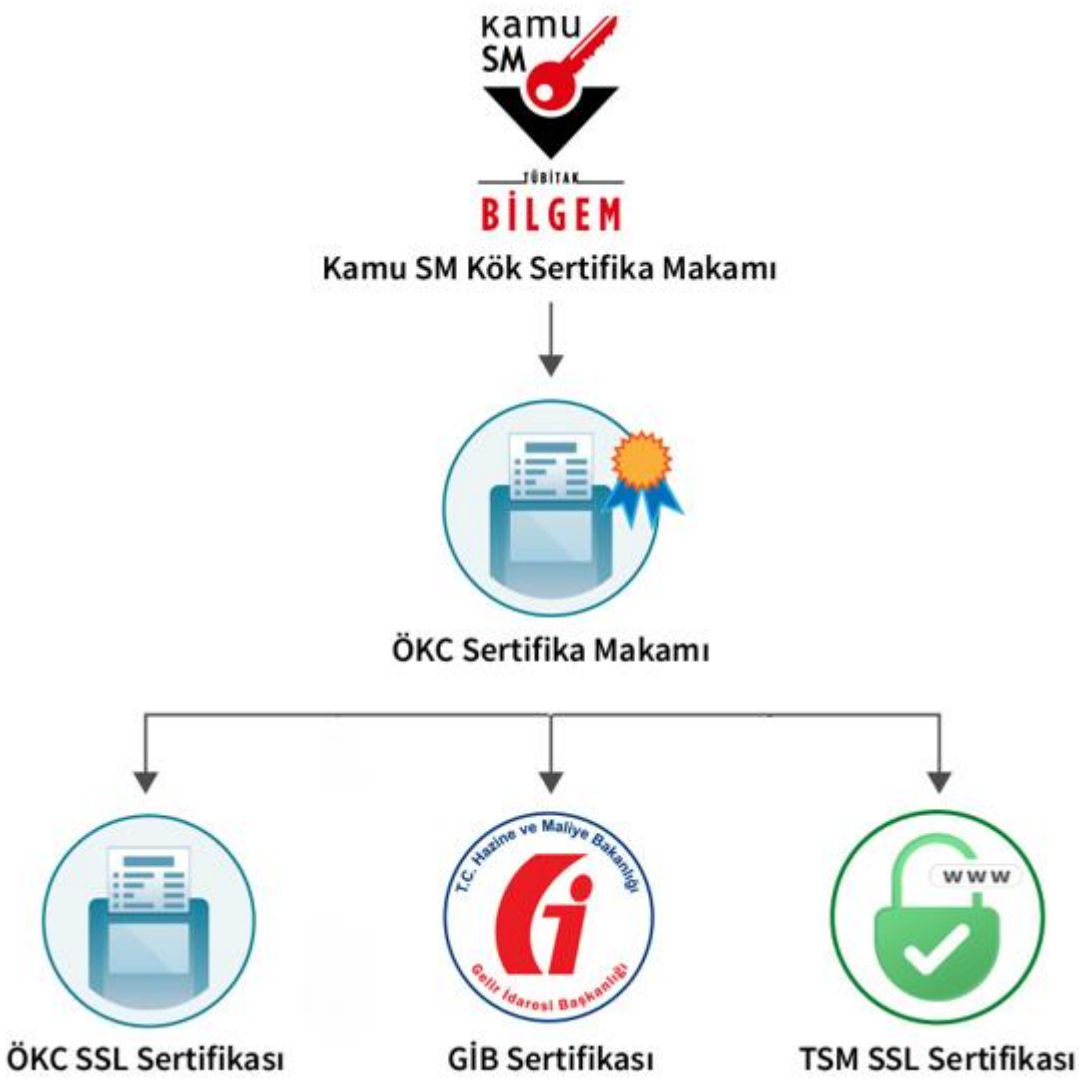
4 Uygulama

4.1 Sistemde Tanımlı Sertifikalar

Sistemde kullanılacak sertifikalar Tablo 1: Sistemde Kullanılacak Sertifikalar'da, kurumlarla ilişkileri ise Şekil 1: Anahtar ve Sertifikalar'da verilmiştir.

Sertifika İsmi	Anahtar Kullanımı	Gelişmiş Anahtar Kullanımı	İmzalama Algoritması	Kullanılan Anahtar	Açıklama
YN 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 ÖKC'nin kimliğini doğrulayan ve güvenli haberleşmesini sağlayan sertifikadır.
GİB Sertifikası	Digital Signature, Key Encipherment	Server Authentication, Client Authentication	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	GİB kimliğini doğrulayan ve güvenli haberleşmesini sağlayan 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 ÖKC'ler ile çift taraflı SSL kullanarak haberleşecektir. Böylelikle sadece yetkili TSM YN ÖKC'ye erişecektir.
YN ÖKC Test Sertifikaları	Digital Signature, Key Encipherment	Server Authentication, Client Authentication	SHA384 with ECDSA veya SHA256 with RSA	ECC (384 Bits) veya RSA (2048 Bits)	YN ÖKC üreticilerinin YN ÖKC geliştirirken kullanacakları sertifikalardır. Soft ve kartlı olarak üretilebilmektedir.

Tablo 1: Sistemde Kullanılacak Sertifikalar



Şekil 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 yükleneceği 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 Sertifikası talebinde bulunabilecektir. Kamu SM'den ilk defa YN ÖKC Sertifikası talep edecek YN ÖKC Üreticisi, firma bilgilerinin ve ÖKC Üreticisi Sertifika Talep Yetkilisi olarak atanacak kişinin bilgilerinin yer aldığı ÖKC Sertifikası Talep Formunu okc@kamusm.gov.tr adresine e-posta ile iletecektir ve asıllarını ise Kamu Sertifikasyon Merkezi TÜBİTAK Gebze Yerleşkesi Gebze-KOCAELİ adresine gönderecektir.

YN ÖKC sertifikası talebinde bulunmak için ÖKC Üreticisi Sertifika Talep Yetkilisinin, Sırasız ÖKC Sertifika Başvuru Listesini 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.

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

ÖKC Sertifikası Talep Formu ve Sırasız 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 Sırasız 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 üretilecektir.

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 verildiği bir YN ÖKC'ye yeni bir sertifikanın yüklenmesi söz konusu olduğunda, Kamu SM tarafından YN ÖKC için yeni bir sertifika üretilecek ve yeni bir akıllı karta yüklenerek kurye ile gönderilecektir.

Sertifikanın soft olarak yüklendiği bir YN ÖKC'ye sertifikanın yeniden yüklenmesi söz konusu olduğunda ise YN ÖKC için yeni bir sertifika üretilecek ve sunucuya yüklenerek firmaya güvenli şekilde 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 belirlenmiştir ve bu süre en fazla 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 gerektiği durumda, iptal edilecek cihazın/cihazların seri numarasının/numaralarının bulunduğu sertifika listesi ÖKC Sertifika Talep Yetkilisi tarafından yetkiliye ait NES ya da ıslak imza ile imzalanarak e-posta ile Kamu SM'ye iletilecektir. İmza doğrulama 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 Dışında Kullanılması

YN ÖKC üreticileri, aldıkları sertifikaların güvenli olarak kullanılmasından sorumludur. 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.

4.7 Diğer 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 ileteceklerdir. HSM üzerinden anahtar üretiminde destek almak isterlerse Kamu SM'nin HSM destek personeli üreticinin HSM 'ine bağlanarak anahtar çiftini ve anahtar çiftinden isteği üretecektir, istek dosyasını Kamu SM'nin ilgili ekibine iletecektir. Kamu SM bu istek dosyalarını işleyerek sertifikaları oluşturacak, GİB ve YN ÖKC üreticilerine iletecektir.

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