

**TASNİF DIŐI**



**TÜBİTAK BİLGEM  
KAMU SERTİFİKASYON MERKEZİ**

**YENİ NESİL ÖKC SAYISAL SERTİFİKA KORUMA KILAVUZU**

**Doküman Kodu**

REH.06.01

**Revizyon No**

01

**Revizyon Tarihi**

31.07.2024

**TASNİF DIŐI**

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk Çıkıő.	26.10.2015
01	Doküman Őablonu güncellenmiőtir.	31.07.2024

## İÇİNDEKİLER

<b>1</b>	<b><i>Amaç ve Kapsam</i></b> .....	<b>3</b>
<b>2</b>	<b><i>Sorumluluklar</i></b> .....	<b>3</b>
<b>3</b>	<b><i>Tanımlar ve Kısaltmalar</i></b> .....	<b>3</b>
<b>4</b>	<b><i>Uygulama</i></b> .....	<b>4</b>
<b>4.1</b>	<b>Güvenlik Yönetimi</b> .....	<b>4</b>
<b>4.2</b>	<b>Güvenlik Gereksinimleri</b> .....	<b>4</b>
4.2.1	Ağ ve Bilgisayar Güvenliđi .....	4
4.2.2	Taşınabilir Bellek Güvenliđi .....	7
4.2.3	Fiziksel ve Çevresel Güvenlik .....	8
4.2.4	Personel Güvenliđi .....	9
<b>4.3</b>	<b>Güvenlik Olay Yönetimi</b> .....	<b>9</b>
<b>4.4</b>	<b>Güvenli Oda Denetimi</b> .....	<b>9</b>

## 1 Amaç ve Kapsam

Bu Kılavuz, Yeni Nesil ÖKC'ler için talep edilen anahtar çiftleri ve sertifikaların Yeni Nesil ÖKC üreticisine ulaşmasından, Yeni Nesil ÖKC'lere yüklenmesine kadarki sürecin güvenli bir şekilde gerçekleştirilmesini ve Yeni Nesil ÖKC üreticisi tarafından oluşturulan Güvenli Odalarla ilgili sorumlulukların belirlenmesini amaçlamaktadır.

## 2 Sorumluluklar

Bu dokümanın hazırlanmasından ve güncellenmesinden Kamu Sertifikasyon Merkezi sorumludur.

## 3 Tanımlar ve Kısaltmalar

<b>API:</b>	Application Programming Interface
<b>BİLGEM:</b>	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
<b>Firma Yetkilisi:</b>	Güvenli Oda ile ilgili tüm işlemlerden sorumlu yetkili
<b>GİB:</b>	Gelir İdaresi Başkanlığı
<b>Güvenilir Personel:</b>	Kamu SM'ye resmi yazıyla bildirilen personel
<b>Güvenli Oda:</b>	Yeni Nesil ÖKC'lere anahtar ve sertifika yükleme yapılacak olan ve kural koyucular ile TÜBİTAK tarafından denetlenen güvenlik seviyesi belirlenmiş özel yerler
<b>IP:</b>	Internet Protocol
<b>İhlal Olayı:</b>	Bir kesintiye, kayba, acil bir duruma veya krize neden olan veya olabilecek durumlar
<b>Kamu SM:</b>	TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde elektronik sertifika hizmet sağlayıcısı olarak kurulmuş olan Kamu Sertifikasyon Merkezi
<b>TÜBİTAK:</b>	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
<b>UPS:</b>	Uninterruptible Power Supply
<b>USB:</b>	Universal Serial Bus
<b>Yeni Nesil ÖKC:</b>	Mükellefe ait mali verileri elektronik ortamda güvenli olarak ileten Ödeme Kaydedici Cihaz

## 4 Uygulama

### 4.1 Güvenlik Yönetimi

GİB'den onay almış olan Yeni Nesil ÖKC üreticisi, Kamu SM tarafından üretilen sertifikaların Yeni Nesil ÖKC'lere yüklenmesi için gerekli olan güvenlik önlemlerini almalı ve devamlılığını sağlamalıdır. Bunun için gerekli yatırımları yapmalı ve güvenlik yönetimini sürdüreceği personeli atamalıdır. Atamadan sonra bu dokümanda belirtilmiş olan güvenlik önlemlerini asgari olarak uygulamalıdır. Mevcut güvenlik önlemlerini sürekli değerlendirerek olası iyileştirmeleri yapmalıdır. Sayısal sertifikaların Kamu SM sisteminden Yeni Nesil ÖKC üreticisi sistemine indirilmesi, Yeni Nesil ÖKC cihazlarına yüklenmesi ve sonrasındaki işlemlerin ayrıntılı olarak dokümanla edilmesi gerekmektedir. Güvenli Oda yönetimi ve sorumluluğu tamamen ÖKC üreticisindedir.

### 4.2 Güvenlik Gereksinimleri

#### 4.2.1 Ağ ve Bilgisayar Güvenliği

Sertifika ve anahtar çiftlerini işleyecek ve iletecek bilgisayarların ve ağ altyapısının belli güvenlik fonksiyonlarını yerine getirmesi gerekmektedir. Sertifika İndirme ve Sertifika Yükleme Bilgisayarının sağlaması gereken genel ve işletim sistemi güvenlik gereksinimleri ayrı ayrı tanımlanmıştır.

##### 4.2.1.1 Sertifika İndirme Bilgisayarı

Kamu SM'den sayısal sertifika ve anahtar çiftlerini pfx formatında indirecek bilgisayarın sağlaması gereken güvenlik özellikleri aşağıda verilmiştir:

- Bilgisayar Güvenli Odada bulundurulacaktır.
- Bilgisayar, sertifika ve anahtar çiftlerini indirmek için ağa bağlanacaktır. Bunun dışındaki zamanlarda bilgisayar ile herhangi bir ağ arasında bağlantı kurulmayacaktır (ağ kablosu takılı olmayacak ve hiçbir kablosuz iletişimi bulunmayacaktır).
- Bilgisayarda işletim sistemi dışında sadece antivirüs ve güvenlik duvarı programı bulunacaktır.
- Antivirüs, işletim sistemi güncellemeleri ve Kamu SM dışında herhangi bir yerle haberleşme yapmayacak şekilde ayarlanacaktır. Eğer Güvenli Oda ağ mimarisinde bir donanımsal güvenlik duvarı çözümü de mevcutsa, ilgili güvenlik duvarı sertifika indirme işlemi harici amaçlarla kullanılmayacaktır.
- Kamu SM'ye erişim yapan IP adresi statik olacaktır. Bu IP adresi Firma Yetkilisi tarafından resmi yazı ile Kamu SM'ye bildirilecektir.
- Bilgisayarlar üzerinde bulunan antivirüs ve işletim sistemi sürekli güncel tutulacaktır.
- Bilgisayar, takılan taşınabilir bellek ünitelerini otomatik olarak virüs taramasından geçirecek şekilde ayarlanacaktır.
- Yönetici ve sınırlı kullanıcı olmak üzere iki hesap içerecektir. Yönetici hesabının şifresi ve sınırlı kullanıcı hesabı, en az bir büyük harf, bir küçük harf, rakam ve sembol içerecek şekilde en az 8 karakterden oluşacaktır. Fakat, bu iki şifre birbirinden farklı olacaktır. Şifreler anlamlı kelimelerden, sıralı sayılardan veya harflerden oluşmayacaktır. Şifreler ayda bir kere değiştirilmelidir. "S#t94AE3r" şifresi örnek olarak verilebilir. Bilgisayardaki işlemler sınırlı kullanıcı hesabı ile yapılacaktır.

- Bilgisayarın şifresi yalnızca Kamu SM'ye bildirilen, ilgili işlemlerden sorumlu personel tarafından bilinecektir.
- Bilgisayara sertifika ve anahtar çiftlerinin taşınmasında kullanılacak harici bellek dışında herhangi bir cihaz takılmayacaktır. Firma bu bilgisayarı belirlenmiş harici bellek dışındaki cihazları tanımayacak şekilde ayarlamalıdır.
- Sertifika ve anahtar çiftleri bilgisayarın belleğine değil, doğrudan taşınabilir belleğe indirilecektir.
- Bilgisayarın değiştirilmesi durumunda, bilgisayara ait sabit disk güvenli bir şekilde imha edilecektir. İmha işlemi en az iki güvenilir personel tarafından kameraların önünde gerçekleştirilecektir. İmha edilen bütün depolama aygıtlarının kayıtları, imha edenlerin imzasını da içerecek şekilde tutulacaktır. İmha işleminden, en üst yöneticinin haberdar olması için imha işleminden önce izin alınacak ve imha sonrasında tutanak imzalanacaktır.
- Tuzak yönetici kullanıcısı olmalıdır.
- Yönetici hesapları varsayılan değerden değiştirilmelidir.
- Administrators, PowerUsers ve Guests yerel kullanıcı grupları üyeleri arasında gereksiz ve yetkisiz kullanıcılar devre dışı bırakılmalıdır.
- Bilgisayarda Lanman şifre özeti tutulmamalıdır.
- Bilgisayar giriŐ (logon) ekranında son kullanıcı ismi görölmesini engelleyecek ayar yapılmalıdır.
- Anonim kullanıcı hesabına erişim yapılmamalıdır.
- Bilgisayarda paylaşılmış klasörler bulunmamalıdır.
- Bilgisayar üzerinde gerekli olmayan tüm servisler durdurulup devre dışı bırakılmalıdır.
- Bilgisayar mavi ekran hatası verdiĐi zaman sabit diske hafıza içeriĐinin atılmamasını sağlayacak ayarlama yapılmalıdır.
- Bilgisayar, CD okuma sürücüsüne takılan CD ve USB portuna takılan USB bellek medyaları otomatik olarak çalıştırmamalıdır.
- Bilgisayar kapanırken takas dosyasının silinmesini sağlayacak ayar yapılmalıdır.
- Bilgisayarın CDRom'dan veya USB bellekten başlatılma özelliĐi kapatılmalıdır.
- Servis Dışı Bırakma saldırılarına karşı uygun korumanın sağlanabilmesi amacıyla gerekli kütük (registry) ayarları yapılmalıdır.
- Kullanıcı bilgisayar başından uzaklaŐtıktan sonra 5 dakika içinde oturumu kilitleyen ekran koruyucu devreye girmelidir.
- Bilgisayar açıldığında (startup) sadece gerekli olan program ve servisler çalıştırılmalıdır.

#### 4.2.1.2 Sertifika Yükleme Bilgisayarı

Yeni Nesil ÖKC'lere, Güvenli Oda içinde sayısal sertifika ve anahtar çiftlerini pfx formatından yükleyecek bilgisayarın sağlanması gereken güvenlik özellikleri aşağıda verilmiştir:

- Bilgisayar Güvenli Odada bulundurulacaktır.
- Anahtar ve sertifikayı Yeni Nesil ÖKC'ye yükleyecek olan bilgisayar, hiçbir ağa bağlı olmayacaktır.
- Yönetici ve sınırlı kullanıcı olmak üzere iki hesap içerecektir. Yönetici hesabının şifresi ve sınırlı kullanıcı hesabı bir büyük harf, bir küçük harf, rakam ve sembol içerecek şekilde en az 8 karakterden oluşacaktır. Fakat bu iki şifre birbirinden farklı olacaktır. Şifreler anlamlı kelimelerden, sıralı sayılardan veya harflerden oluşmayacaktır. Şifreler ayda bir kere değiştirilecektir. "S#t94AE3r" şifresi örnek olarak verilebilir. Bilgisayardaki işlemler sınırlı kullanıcı hesabı ile yapılacaktır.
- Bilgisayarın şifresi Kamu SM'ye bildirilen, ilgili işlemlerden sorumlu personel tarafından bilinecektir.
- Bilgisayarın 1.5 metre yakınlarında Yeni Nesil ÖKC dışında elektronik sistem, hat vs. (bilgisayar için gerekli olan elektrik kabloları vs. hariç) bulunmayacaktır.
- Bilgisayara, şifreli pfx dosyalarının işlenmesi ve Yeni Nesil ÖKC'lere yüklenmesi süreçlerine ait iş ihtiyaçlarını karşılama amacı haricinde herhangi bir yazılım yüklenmeyecektir.
- Bilgisayara hiçbir şekilde başka bir bilgisayar, telefon, mp3 player vb. elektronik aygıtlarla bağlantı kurulmayacaktır.
- Bilgisayarın değiştirilmesi durumunda, bilgisayara ait sabit disk güvenli bir şekilde imha edilecektir. İmha işlemi en az iki güvenilir personel tarafından kameraların önünde gerçekleştirilecektir. İmha edilen bütün depolama aygıtlarının kayıtları, imha edenlerin imzasını da içerecek şekilde tutulacaktır. İmha işleminden, en üst yöneticinin haberdar olması için imha işleminden önce izin alınacak ve imha sonrasında tutanak imzalanacaktır.
- Pfx formatında şifreli olarak indirilen anahtarlar ve sertifikalar taşınabilir bir bellek yardımıyla bu bilgisayara yüklenecek ve sertifikaların Yeni Nesil ÖKC'ye yüklenmesinden sonra güvenli silme programları ile bilgisayardan silinecektir.
- Pfx formatındaki anahtarlar ve sertifikaların şifreleri yükleme esnasında çözülecektir. Şifresiz olarak taşınabilir belleklerde veya yükleme bilgisayarında saklanmayacaktır.
- Pfx formatında şifreli olarak indirilen anahtarlar ve sertifikaların, Yeni Nesil ÖKC cihazlarına yüklenmemesi durumunda 10 iş günü sonunda taşınabilir belleklerden ve yükleme bilgisayarından güvenli silme programları ile silinecektir. Anahtarlar ve sertifikalar 10 iş günü içerisinde Yeni Nesil ÖKC cihazlarına yüklendiğinde, yüklemeden hemen sonra taşınabilir belleklerden ve yükleme bilgisayarından güvenli silme programları ile silinecektir.
- Şifreli pfx dosyalarının şifresini çözecek şifre çözme uygulama programından dolayı bilgisayar Windows işletim sistemine sahip olacaktır.
- Tuzak yönetici kullanıcısı olmalıdır.
- Yönetici hesapları varsayılan değerden değiştirilmelidir.
- Administrators, PowerUsers ve Guests kullanıcı grupları üyeleri arasında gereksiz ve yetkisiz kullanıcılar devre dışı bırakılmalıdır.
- Bilgisayarda Lanman şifre özeti tutulmamalıdır.
- Bilgisayar giriŐ (logon) ekranında son kullanıcı ismi görülmesini engelleyecek ayar yapılmalıdır.
- Anonim kullanıcı hesabına erişim yapılmamalıdır.
- Bilgisayarda paylaşılmıŐ klasörler bulunmamalıdır.
- Bilgisayar üzerinde gerekli olmayan tüm servisler durdurulup devre dışı bırakılmalıdır.
- Bilgisayar mavi ekran hatası verdiĐi zaman sabit diske hafıza içeriĐinin atılmamasını sağlayacak ayarlama yapılmalıdır.

- Bilgisayar CD okuma sürücüsüne, CD ve USB portuna takılan USB bellek medyaları otomatik olarak çalıştırmamalıdır.
- Bilgisayar kapanırken takas dosyasının silinmesini sağlayacak ayar yapılmalıdır.
- Bilgisayarın CDRom'dan veya USB bellekten başlatılma özelliđi kapatılmalıdır.
- Kullanıcı bilgisayar başından uzaklaştıktan sonra 5 dakika içinde oturumu kilitleyen ekran koruyucu devreye girmelidir.
- Bilgisayar açıldığında (startup) sadece gerekli olan program ve servisler çalıştırılmalıdır.

#### 4.2.2 Taşınabilir Bellek Güvenliđi

Saklanması gereken tüm elektronik ve fiziksel kayıtlar/bilgiler, řu şekilde saklanmalıdır:

- Kamu SM tarafından üretilmiş olan anahtar çiftlerinin ve sertifikanın taşınması için kullanılacak olan taşınabilir bellek (CD, DVD, USB, external hardisk vs.) hiçbir şekilde ve hiçbir zaman (bu iş için kullanımı sona erdikten sonra da geçerli olmak üzere) başka bir amaç için kullanılmamalıdır. Sadece yükleme yapılacak olan bilgisayara, şifreli anahtar çiftlerinin ve sertifikanın taşınmasında kullanılmalıdır.
- Taşınabilir belleklerin (CD, DVD, USB, external hardisk vs.) deđiştirilmesi söz konusu olduđu durumlarda, taşınabilir bellekler güvenli bir şekilde imha edilmelidir. İmha işlemi kameraların önünde gerçekleşmeli, taşınabilir bellekler en az iki güvenilir personel tarafından imha edilmeli ve imha edilen bütün depolama aygıtlarının kayıtları, imha edenlerin imzasını da içerecek şekilde tutulmalıdır. İmha işleminden, en üst yöneticinin haberdar olması için imha işleminden önce izin alınmalı ve imha sonrasında tutanak imzalatılmalıdır.
- Taşınabilir bellekler hiçbir şekilde Güvenli Oda dışına çıkarılmamalıdır.
- Taşınabilir bellekler, yetkisiz kişilere teslim edilmemelidir ve Yeni Nesil ÖKC üreticisi firmaların oluşturacakları Güvenli Oda içindeki çelik kasada saklanmalıdır.
- Taşınabilir belleklerin içerisindeki anahtar çiftleri ve sertifikalar, yükleme bilgisayarına yüklendikten sonra en az 2 güvenilir personel tarafından, güvenli silme programları ile silinmelidir. Eğer taşınabilir bellek, silmeye olanak tanıyan bir depolama aygıtı deđil ise depolama aygıtları güvenli bir şekilde imha edilmelidir. İmha işlemi kameraların önünde gerçekleşmeli, en az iki güvenilir personel tarafından imha edilmeli ve imha edilen bütün depolama aygıtlarının kayıtları, imha edenlerin imzasını da içerecek şekilde tutulmalıdır. İmha işleminden en üst yöneticinin haberdar olması için, imha işleminden önce izin alınmalı ve imha sonrasında tutanak imzalatılmalıdır.
- Güvenli Oda içinde saklanan her türlü kayıt, bilgi depolama aygıtı, anahtar çiftleri ve sertifikanın taşındığı taşınabilir bellekler çelik kasa içinde saklanmalıdır. Çelik kasa ise güvenlik kameralarının rahatlıkla görebildiđi bir yerde olmalıdır. Çelik kasanın en az iki anahtarının olması gerekir. Anahtarların farklı kişilerde olması ve kasanın açılması için iki anahtarın aynı anda kullanılması gerekmektedir.
- Kasa her açıldığında, kimler tarafından, neden ve ne zaman açıldığı açıkça kayıt altına alınmalı ve kayıtlar kasanın içinde saklanmalıdır.



### 4.2.3 Fiziksel ve Çevresel Güvenlik

Anahtar çiftleri ve sertifika yüklenmeden önce, Yeni Nesil ÖKC'nin Güvenli Odaya alınması gerekmektedir. Fiziksel ve çevresel güvenlik için gerekli olan asgari özellikler Őu Őekildedir:

- Güvenli Oda sadece Kamu SM'den alınan anahtar çiftleri ve sertifikaların güvenli bir Őekilde Yeni Nesil ÖKC'lere yüklenmesi iŐlemi için kullanılmalıdır.
- Güvenli Odayı kör nokta (kamaralar klavye üzerindeki tuŐ kombinasyonlarını izleyemeyecek Őekilde ayarlanmalı, kiŐinin varlığını ve genel hareketlerini net olarak göstermesi yeterlidir) kalmayacak Őekilde izleyen ve Güvenli Odada 7/24 kayıt yapan güvenlik kameraları bulunmalıdır. Bu kameraların kayıtları geriye dönük olarak en az 1 yıl saklanmalıdır.
- Kameraların düzgün çekim yapabilmesi için yeterli ıŐıklandırma olmalıdır.
- Kamera kayıtlarının düzenli olarak yedekleri alınmalı ve kayıtlar fiziksel olarak faklı bir yerde saklanmalıdır.
- Güvenli Odaya izinsiz eriŐimin engellenmesi için kapalı bir alanda olması gerekmektedir Seri üretim yapılması durumunda Güvenli Odaya yürüyen bant vb. sistemler alan içine girebilir. Böyle bir sistemin Güvenli Odanın içine girmesi durumunda, Güvenli Odaya bant üzerinde yapılan giriŐ ve çıkıŐlar dıŐarıdan ve içeriden 7/24 kameralar ile izlenmelidir. Seri üretim yapılmadıŐı durumlarda bu giriŐ ve çıkıŐlar kapalı olmalıdır.
- Güvenli Odaya giriŐ çıkıŐlar elektronik kimlik doŐrulaması ile yapılmalıdır. Güvenli Odaya giriŐlerde; giriŐ çıkıŐ saatleri, giren kiŐinin ismi ve giriŐ amacı kayıt altına alınmalıdır. Bu kayıtlar en az 10 yıl saklanmalıdır.
- Güvenli Odaya yalnızca yetkilendirilmiŐ personeller girebilir. Bu personeller dıŐında hiŐ kimsenin Güvenli Odaya eriŐim yetkisinin bulunmaması gerekir. YetkilendirilmiŐ personellerin gözetiminde gerekli olan kiŐi veya kiŐiler Güvenli Odaya giriŐ yapabilir. Ancak bu kiŐiler Güvenli Odada yalnız baŐına bırakılmamalıdır.
- Güvenli Odaya yetkisiz giriŐlerin önlenmesine yönelik alarm sisteminin kurulması ve alarm durumlarında gerekli kiŐilere (bu kiŐilerin önceden belirlenmesi gereklidir) haber verilmesi saŐlanmalıdır.
- Güvenli Odaya giriŐ en az iki yetkili personel tarafından birlikte yapılmalıdır.
- Güvenli Odaya giriŐ yapıldıŐktan sonra, iŐlemlerin tek kiŐi tarafından yapılmaması en az iki personel tarafından gerçekteŐirilmesi gerekmektedir. Bu personelden bir tanesi iŐlemi yapan kiŐi, diŐeri ise gözetleme yapan kiŐi olabilir.
- Güvenli Odanın dıŐarıdan gelecek olan fiziksel saldırılara (yangın, patlama vs.) karŐı özel koruma sistemleri ile korunması gerekmektedir. Yangın için FM200 gazlı veya benzeri yangın söndürme sistemi olmalıdır.
- Güvenli Oda mevcut elektrik sistemindeki elektrik kesintilerine karŐı, tüm sistemden baŐımsız olarak kendini besleyebilecek yedekli UPS ile desteklenmelidir.
- Yeni Nesil ÖKC'ler haricinde Güvenli Oda içine konulacak veya Güvenli Odadan çıkarılacak her Őey kayıt altına alınmalıdır.
- YetkilendirilmiŐ olan personelin görevinden ayrılması veya iŐten çıkarılması durumunda Kamu SM'ye bilgi verilmeli ve bu personelin Güvenli Odaya eriŐimleri iptal edilmelidir.
- Güvenli Odaya girecek olan kiŐilerin üzerinde cep telefonu, çaŐrı cihazı gibi elektronik kayıt yapma yeteneŐi olan cihazlar bulunmamalıdır.

#### 4.2.4 Personel Güvenliđi

- Güvenli Odaya giriş yapan personel isimleri gerekli olmadıkça kimse ile paylaşılmamalıdır.
- Personelin sabıka kaydı bulunmamalı ve adli sicil kayıtları her yıl yenilenmelidir.
- Personelden gizlilik beyanı alınmalıdır.
- Personele yaptıkları işin hassasiyetini ve güvenlik gereksinimlerini içeren farkındalık eğitimleri verilmelidir.
- Güvenli Odaya yetkili personel gözetiminde giriş çıkış yapacak bütün kişilere Güvenli Oda hakkında gerekli bilgilendirme yapılmalıdır.

#### 4.3 Güvenlik Olay Yönetimi

- Güvenli Odada oluşabilecek ihlal olayları sonrası; tespit edici, önleyici ve kontrol edici altyapı bulundurulmalıdır.
- Acil durumlarda Güvenli Odadaki bilgilerin güvenli bir şekilde korunması ve panik anında güvensiz/yetkisiz erişimlerin kısıtlanması için plan yapılmalıdır.

#### 4.4 Güvenli Oda Denetimi

- Yeni Nesil ÖKC üreticileri tarafından Yeni Nesil ÖKC'ler için Kamu SM'den talep edilen anahtar çiftleri ve sertifikaların Yeni Nesil ÖKC'lere yüklenmesi amacıyla oluşturulan Güvenli Odaların SSKK'ya uygunluğu, Gelir İdaresi Başkanlığı "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezi Teknik Kılavuzu 18. Maddesi ile Yeni Nesil Ödeme Kaydedici Cihazlar Teknik Kılavuzu TK-2 6. Maddesi" hükmünce Kamu SM tarafından denetlenecektir.
- Kamu SM tarafından denetlenmiş ve uygun bulunmuş Yeni Nesil ÖKC Güvenli Odalarına, Kamu SM tarafından yılda bir kere gözetim denetimi yapılır.
- Kamu SM tarafından gerekli görülmesi durumlarda haberli veya habersiz denetimler gerçekleştirilebilir.
- Yapılan denetimlerde, tespit edilen uygunsuzlukların giderilmesine yönelik düzeltici faaliyetler veya alınacak aksiyonlara ilişkin detaylı planlar, Kamu SM'ye bildirilecektir.
- Yapılan denetimlerin raporu GİB ve ÖKC üreticisi ile paylaşılacaktır. Denetimde uygunsuzluk tespit edilmesi durumunda, Yeni Nesil ÖKC üreticisine yeni sertifika üretimi durdurulacak ve durum GİB'e bildirilecektir. Yeni Nesil ÖKC üreticisinin uygunsuzluğu gidermesi ve giderilen uygunsuzlukların Kamu SM tarafından uygun bulunmasına müteakip, Yeni Nesil ÖKC üreticilerinin sertifika talepleri karşılanmaya devam edilecektir.