YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT

ÖKC TSM MERKEZİ

TEKNİK KILAVUZU

Sürüm 2.0

23 Eylül 2016

YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARA AİT
ÖKC TSM MERKEZİ
TEKNİK KILAVUZU

Amaç

MADDE 1 – Bu kılavuzun amacı, yeni nesil ödeme kaydedici cihazlara ait ÖKC TSM Merkezleri'nin kurulması, işletilmesi, yönetimi ve denetimine ilişkin usul ve esasları ve kapsama dahil olanların bu kılavuzda belirtilen hususlardaki sorumluluklarını düzenlemektir.

Kapsam

MADDE 2 –Yeni nesil ödeme kaydedici cihaz üreticileri, üye işyeri anlaşması yapan kuruluşlar, dış hizmet sağlayıcıları ve faaliyetlerinde yeni nesil ödeme kaydedici cihaz kullanan işyerleri bu kılavuz kapsamındadır.

Dayanak

MADDE 3 –Bu Kılavuz, 213 sayılı Vergi Usul Kanunu'nun Mükerrer 257'nci maddesinin birinci fıkrasının 1,3 ve 6 numaralı bentleri ile 3100 sayılı Katma Değer Vergisi Mükelleflerinin Ödeme Kaydedici Cihazları Kullanmaları Mecburiyeti Hakkında Kanunu'nun 10'uncu maddesi ve 426 Sıra No'lu Vergi Usul Kanunu Genel Tebliği'ne dayanılarak düzenlenmiştir.

Tanımlar ve Kısaltmalar

MADDE 4 – Bu Kılavuzda yer alan;

a) **GİB**: Gelir İdaresi Başkanlığı'nı,
b) **GİB BS**: Gelir İdaresi Başkanlığı, Yeni Nesil Ödeme Kaydedici Cihazlar Bilgi Sistemleri'ni,
c) **BDDK**: Bankacılık Düzenleme ve Denetleme Kurumu'nu,
ç) **ÖKC**: Yeni Nesil Ödeme Kaydedici Cihazları,
d) **Yeni Nesil ÖKC**: GİB BS ve üye işyeri anlaşması yapan kuruluşlar ile **çevrimiçi çalışabilen** IP tabanlı ödeme kaydedici cihazları,
e) **IP**: İnternet Protokolünü,
f) **EFT-POS Özellikli Yeni Nesil ÖKC:** Üzerinde EFT-POS özelliği bütünleşik halde bulunan ÖKC'leri,
g) **Basit / Bilgisayar Bağlantılı Yeni Nesil ÖKC:** Üzerinde EFT-POS özelliği bütünleşik halde bulunmayan ve harici kablolu bağlantı yoluyla EFT-POS/PinPad cihazı bağlanabilen ÖKC'leri,
ğ) **ÖKC ÜRETİCİSİ**: Maliye Bakanlığı'ndan onay alan ve Yeni Nesil ÖKC ile ÖKC TSM Merkezinden sorumlu olan üretici firmayı,
h) **ÖKC TSM MERKEZİ (Trusted Service Manager-Güvenli Servis Sağlayıcı)**: Yeni Nesil Ödeme Kaydedici cihazlara yazılım-parametre yükleme, yazılım güncelleme, bu cihazları ve bu cihazlar ile birlikte veya üzerinde gerçekleştirilen kartlı işlemleri yönetme, cihazlar ile ilgili güvenli anahtar yönetimi gerçekleştirme, ön kontrol işlemlerini yapma, banka uygulaması yazılım ve parametrelerini cihaza yükleme, cihaz yaşam döngüsünü kontrol etme ve yönetme, ÖKC mesajlarının GİB BS'ye ve üye işyeri anlaşması yapan kuruluşlara GMP'lerde belirlenen iletişim protokolleri çerçevesinde aktarılmasını sağlama amacıyla kurulan ve ÖKC üreticilerine ait

terminal yönetim merkezini ifade eder.

ÖKC TSM Merkezi tamamen ÖKC üreticisi tarafından kurulabileceği gibi, ÖKC üreticisinin yetki ve sorumluluğunda kısmen veya tamamen bir Dış Hizmet Sağlayıcıdan hizmet temin etmek suretiyle de kurulabilir.

ÖKC TSM Merkezi'ne ilişkin hizmetlerin kısmen veya tamamen bir dış hizmet sağlayıcısından temin edilmesi halinde; TSM Merkezi'nce yerine getirilmesi beklenen faaliyetlerin gerçekleştirilmesinden müşterek ve müteselsil sorumluluk esasında olmak üzere dış hizmet sağlayıcısı ÖKC üreticisi ile birlikte sorumludur.

ÖKC TSM Merkezleri ÖKC Üreticileri için münhasıran kurulmuş donanım, yazılım ve işletimi içermeli ve sunulacak olan sertifikalar bu sistem için alınmış olmalıdır.

ı) GÜVENLİ ODA: Yeni Nesil ÖKC'lere PIN güvenlik kuralları ile anahtar ve sertifika yükleme yapılacak olan ve Kural koyucular ile TÜBİTAK tarafından denetlenen güvenlik seviyesi belirlenmiş özel yerleri,

i) DIŞ HİZMET SAĞLAYICI: ÖKC üreticisine, ÖKC TSM Merkezi'ne ilişkin hizmet veren kuruluşu,

j) EFT-POS (Electronic Funds Transfer at Point Of Sale): Kart kullanılarak elektronik fon transferi ile ödeme yapmaya yarayan satış terminalini,

k) Akıllı PINPAD Cihazı : Kart kullanılarak elektronik fon transferi ile ödeme yapmaya yarayan satış terminalini,

l) PCI DSS (Payment Card Industry Data Security Standard): PCI SSC tarafından yayımlanan Veri Güvenliği Standardını,

m) PCI SSC (Payment Card Industry Security Standards Council): Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyini,

n) PIN (Personal Identification Number) Güvenliği: Kart hamilinin kimliğini doğrulama amaçlı kullanılan, sadece kart hamilinin bildiği en az dört rakamdan oluşan değerin güvenliğini belirleyen esasları,

o) Kural Koyucular: GİB, BDDK

ö) ISO 20000: Bilgi Teknolojileri Servis Yönetim Sistemini,

p) ISO 22301: Uluslararası İş Sürekliliği Yönetimini,

r) ISO 27001: Bilgi Güvenliği Yönetim Sistemini,

s) İKİNCİL MERKEZ: Kanun ve ilgili mevzuatında, kuruluş için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği anda erişim sağlayan yedek sistemlerin kullanıma hazır olacak şekilde tesis edildiği, herhangi bir kesinti durumunda tüm işlemlere ilişkin faaliyetlerin iş sürekliliği planında ve toplam kullanılabilirlik kurallarına uygun olarak belirlenen kesinti süreleri içerisinde sürdürülür hale getirilmesine ve kuruluşun faaliyetleri sürdürmede kullandığı asıl sistemlerin tesis edildiği yapı ile aynı riskleri taşımayacak şekilde oluşturulmuş ve yurt içinde, birincil sistemden farklı bir il sınırında ve en az 300 km mesafede yer alan merkezi**,**

ş) KORUNAKLI SİSTEM: Bünyesindeki hassas verilere fiziksel ve yazılımsal olarak erişimi kısıtlayan, şifreleme anahtarlarının korunmasını ve yönetimini sağlayan, yetkisiz erişimleri fark eden ve bunlara tepki veren, birimlerinin yetkisiz olarak değiştirilmesi ve çıkarılması ile yeni birim eklenmesi faaliyetlerini algılamaya ve bunlara tepki vermeye yönelik kontroller içeren, çevresel ve operasyonel şartların değiştirilmesi, normal çalışma şartlarının dışına çıkılması veya yazılımsal anormallikler oluşturulması dolayısıyla sağladığı güvenlik seviyesinin azalmayacağına ilişkin makul güvence sunan sistemi ve bu sisteme destek hizmetini gerçekleştirebilecek yönetici ile yeterli sayı ve nitelikte personelin çalıştığı merkezi,

t) DENETİM İZİ: Operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini

sağlayacak kayıtları,

u) **GÜVENLİ ŞİFRELEME**: Kimlik doğrulama, veri bütünlüğünü sağlama, gizlilik ve mahremiyeti temin etme ve inkâr edememe şartlarını sağlama amaçlarıyla kullanılabilen, literatürde kabul görmüş ve güvenilirliğini yitirmemiş güçlü bir algoritma ile yeterli uzunlukta ve güvenliği kriptografik anahtar yönetimi süreci ile sağlanmış anahtarlar kullanılarak gerçekleştirilen, anahtar kullanılmaksızın şifrelenmemiş verinin elde edilmesi teorik olarak mümkün olsa bile pratikte gerektirdiği zaman ve kaynaklar dikkate alındığında uygulanabilir olmayan şifreleme faaliyetlerini,

ü) **KRİPTOLOJİK ANAHTAR YÖNETİM SÜRECİ**: PIN güvenlik kuralları ile anahtarın ve başlangıç vektörleri, sayaçlar gibi ilgili diğer güvenlik parametrelerinin oluşturulması, dağıtımı, saklanması, yüklenmesi ve kullanılması, ömrünü tamamlamasının ardından veya güvenliği zedelendiğinde yeni bir anahtar oluşturularak eski anahtarın imhası veya arşivlenmesinin yazılı ve etkin bir biçimde yönetilmesi sürecini,

v) **GMP**: Gelir İdaresi Başkanlığı Mesajlaşma Protokollerini,

y) **YETKİLENDİRİLMİŞ ESHS**: ESHS (Elektronik Sertifika Hizmet Sağlayıcısı) Yeni Nesil ÖKC'lere, ÖKC TSM Merkezlerine ve GİB BS'ye yüklenecek sertifikaların üretimi, dağıtımı ve sonrasında yönetimini ve denetimini gerçekleştirecek kurum (TÜBİTAK Kamu SM) ya da GİB tarafından yetkilendirilmiş sertifika otoritesi olan kurum.

z) **SERTİFİKA**: Yetkilendirilmiş ESHS tarafından üretilen; ÖKC'lere, ÖKC TSM Merkezine ve GİB BS'ye iletilen X509 sertifikalarını,

aa) **ÖKC MESAJLARI**: ÖKC Durum Verisi ve GİB Hassas ÖKC Verisinden oluşan mesajları,

bb) **ÖKC DURUM VERİSİ**: ÖKC'ler tarafından ÖKC TSM Merkezi'ne cihaz yaşam döngüsü kontrollerinin ve yönetiminin yapılması için gönderilen, detayları GMP'lerde belirlenmiş cihaz saha durum verilerini,

cc) **GİB HASSAS ÖKC VERİSİ**: ÖKC'lerden ÖKC TSM Merkezi'ne, ÖKC TSM Merkezi'nden GİB BS'ye, Yetkilendirilmiş ESHS'ye ait kriptografik anahtarlarla şifrelenerek iletilen ve ancak GİB BS'de açılabilen, detayları Teknik Kılavuzlarda ve GMP'lerde belirlenmiş Z raporu, fiş bilgileri, fiş iptal mesajları, kurulum ve anahtar değiştirme mesajları içerisinde yer alan verileri,

çç) **TEKNİK KILAVUZLAR**: GİB tarafından Yeni Nesil ÖKC'ler ile ilgili yayınlanmış olan Teknik Kılavuzları,

dd) **SIZMA TESTİ**: ÖKC TSM Merkezi'nin güvenlik açıklarını, istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen testi,

ee) **SİMETRİK ŞİFRELEME**: Hem veriyi şifrelemek hem de şifreli veriyi açmak için aynı anahtarın kullanıldığı şifreleme yöntemini,

ff) **ÜYE İŞYERİ ANLAŞMASI YAPAN KURULUŞ**: 5464 Sayılı Banka ve Kredi Kartları Kanunu ile 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkındaki Kanundan yetki almış kuruluşları ve 382 Sıra No'lu Vergi Usul Kanunu Genel Tebliği'nde belirtilen kurallara göre faaliyet gösteren Özel Kart ve Yemek Çeki Kuruluşlarını,

gg) **BSDHY:** 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,

ifade eder.

ÖKC TSM Merkezlerinin Kuruluş Esasları

MADDE 5 – (1) ÖKC Üreticileri, bu Kılavuzun Tanımlar ve Kısaltmalar maddesinde belirtilen PCI DSS, ISO 20000, ISO 22301, ISO 27001 standartlarını haiz olarak bir ÖKC TSM Merkezi kurmak veya bu standartları sağlayan bir Dış Hizmet Sağlayıcısının sunduğu ÖKC TSM Merkezi'ne ilişkin hizmetinden yararlanmak zorundadır.

(2) Kurulan veya dış hizmet sağlayıcıdan faydalanılan ÖKC TSM Merkezleri'nin, bu maddede belirtilen standartları faaliyetleri süresince sağlamaları zorunludur. Söz konusu standartlardan herhangi birinin, ÖKC TSM Merkezleri'nin denetimi sırasında karşılanmadığının tespiti halinde; GİB tarafından yazı ile bildirilecek tamamlama süresi içinde eksikliklerini tamamlamayan ÖKC TSM Merkezleri'nin (Dış Hizmet Sağlayıcıları dahil) izinleri GİB tarafından iptal edilebilir.

(3) ÖKC TSM Merkezi tamamen ÖKC üreticisi tarafından kurulabileceği gibi ÖKC üreticisinin yetki ve sorumluluğunda kısmen veya tamamen bir Dış Hizmet Sağlayıcıdan hizmet temin etmek suretiyle de kurulabilir.

(4) ÖKC TSM Merkezi'ne ilişkin hizmetlerin kısmen veya tamamen bir dış hizmet sağlayıcısından temin edilmesi halinde; TSM Merkezi'nce yerine getirilmesi beklenen faaliyetlerin gerçekleştirilmesinden müşterek ve müteselsil sorumluluk esasında olmak üzere dış hizmet sağlayıcısı ÖKC üreticisi ile birlikte sorumludur.

ÖKC TSM Merkezi Başvuru, Test, Denetim ve Onay Süreçleri:

MADDE 6 – (1) ÖKC TSM Merkezleri'nin başvuru, test ve onay denetimi, sadece ÖKC üretici onayı almış üreticiler için yapılır.

ÖKC üreticisi, TSM Merkezi'ne ilişkin hizmetleri kısmen veya tamamen bir Dış Hizmet Sağlayıcıdan temin etmesi halinde; TSM Merkezi Başvurusunda Dış Hizmet Sağlayıcıdan temin edilen hizmet unsurları detaylı olarak belirtilmeli ve TSM Merkezi'ne ilişkin test ve onay süreçlerinde Dış Hizmet Sağlayıcıdan temin edilen hizmet unsurları da test ve değerlendirmeye tabi tutulmalıdır.

TSM Merkezi başvurularının başvuru ve testleri ÖKC üretici onayı almış bir ÖKC üreticisi tarafından yapılmak zorunda olup bir ÖKC üreticisi ile birlikte olmaksızın yapılan ÖKC TSM Merkezi başvuruları dikkate alınmayacaktır.

(2) ÖKC TSM Merkezi test işlemlerine başlanabilmesi için, ÖKC Üreticileri ve Dış Hizmet Sağlayıcıları ÖKC TSM Merkezi hizmetlerine ilişkin gerekli sertifikalara sahip olmalı ve bu sertifikalar GİB'e yapılan yazılı başvuru ekinde sunulmuş olmalıdır. Bu yazılı başvuruda ÖKC TSM Merkezi'nin sahip olduğu donanımların marka, model, kapasite ve özellikleri ile yazılımlarının işleyiş süreçlerini anlatan teknik bir rapor da eklenecektir.

(3) ÖKC TSM Merkezi'nin gerekli şartları haiz olup olmadığının tespiti için, onay denetimi, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca veya TÜBİTAK tarafından yerinde yapılmak zorundadır.

Onay denetimi, Başkanlıkça yayınlanan "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezleri'nin Başvuru, Test, Denetim ve Onay Teknik Kılavuzu" nda yer alan "ÖKC TSM Merkezi Onay Denetimi ve Yıllık Denetim Süreçleri Akışı"na uygun olarak yürütülür ve "Bilgi Sistemleri Denetim Adımları" ile "Güvenli Haberleşme Denetim Adımları" olmak üzere iki aşamadan oluşur.

ÖKC TSM Merkezi'nin GİB tarafından onaylanmasını müteakip yapılacak yıllık denetim faaliyetleri, "Bilgi Sistemleri Denetim Adımları"na göre "ÖKC TSM Merkezi Yıllık Denetim Raporu" tanzimi ile gerçekleştirilir.

"Güvenli Haberleşme Denetim Adımları" onay sürecine münhasıran uygulanır. Ancak, GİB tarafından

GMP dokümanlarında değişiklik yapılması halinde, bu denetimlerin yıllık denetim faaliyetleri kapsamında tekrar edilmesi GİB tarafından istenebilir.

GİB, gerek görmesi halinde yerinde denetimi kendisi de yapabilir.

(4) GİB gerekli belge ve olumlu denetim raporu kontrollerini yaptıktan sonra, ÖKC TSM Merkezi tarafından GİB BS test ortamına bağlanılarak uçtan uca test çalışmalarına başlanır.

(5) ÖKC TSM Merkezi'nin testleri, öncelikle GİB tarafından üreticilere verilen simülatör ile kendileri tarafından gerçekleştirmeleri beklenmektedir. Simülatör üzerinde başarılı olarak sağlanan test sonrasında, ÖKC TSM Merkezi GİB tarafından verilecek olan fiili test tarihinde GİB BS ile birlikte fiili teste tabi tutulacaktır. GİB BS ile testler, GİB tarafından her bir ÖKC TSM Merkezi'ne özel takvimlendirilen test slotları zaman aralığında gerçekleştirilir. Ayrılan slot zaman aralığında testlerini tamamlayamayan ÖKC TSM Merkezi için GİB tarafından farklı bir takvimlendirme sağlanır.

(6) Tüm test süreçlerini başarılı şekilde tamamlayan ÖKC TSM Merkezleri'ne GİB tarafından yazılı olarak "ÖKC TSM Merkezi Onayı" verilir. ÖKC TSM Merkezi, söz konusu onay yazısında belirtilen tarih itibari ile GİB BS'ye veri gönderme işlemine başlamak zorundadır.

(7) GMP dokümanlarına uygun olarak hazırlanan ÖKC TSM Merkezi Uçtan Uca Test Senaryoları GİB tarafından ÖKC Üreticileri ile olumlu denetim raporu sonrasında paylaşılır.

(8) ÖKC TSM Merkezleri, ÖKC Üreticisi için münhasıran kurulmuş donanım, yazılım ve işletimi içermeli ve sunulacak olan sertifikaların bu sistem için alınmış olması gerekmektedir.

ÖKC TSM Merkezlerinin Yönetim Esasları

MADDE 7 – (1) Yeni Nesil ÖKC'lerin yaşam döngüsünün (Terminal ve Mesaj Yönetim Sistemi) ve ÖKC TSM Merkezi'nin yönetim, yetki ve sorumluluğu ÖKC üreticilerindedir.

(2) ÖKC üreticileri ÖKC TSM Merkezi hizmetlerini Dış Hizmet Sağlayıcıdan da temin edebilir. Bu hizmetin Dış Hizmet Sağlayıcıdan temin edilmesi ÖKC üreticisinin, ÖKC TSM Merkezi hizmetlerine ilişkin sorumluluklarını ortadan kaldırmaz.

(3) Yeni Nesil ÖKC'ler GİB BS'ye ÖKC TSM Merkezleri üzerinden bağlanacak olup, cihazların doğrudan veya ÖKC TSM Merkezleri haricinde başka bir hat üzerinden GİB BS'ye bağlanması mümkün değildir. ÖKC TSM Merkezleri ile ÖKC'ler ve GİB BS arasındaki kurulacak olan güvenli alt yapı, ağların sorumluluğu ve sahipliği ÖKC üreticilerinde olacaktır. ÖKC'lerin ÖKC TSM Merkezleri'ne erişmeleri için gereken alt yapı, erişim hatlarının sorumluluğu ve sahipliği ise ÖKC kullanan mükelleflere aittir.

(4) ÖKC GMP Mesajı ağ (network) iletim seviyesi, ÖKC TSM Merkezi'nde sonlandırılacak olup, GMP Mesajı üzerinde gerekli ön kontroller yapıldıktan sonra GİB BS'ye GMP Mesaj formatında iletilecektir.

(5) ÖKC TSM Merkezleri, Yeni Nesil ÖKC'leri yönetme, ayakta tutma, her işlemde cihazdan gelen GMP Mesaj bilgilerinin format ve doğruluğunu değerlendirme, bu mesaj bilgilerinin içerisindeki hassas mali verilerin kaynağını, doğruluğunu, değişmezliğini ve bütünlüğünü kontrol etmekle yükümlüdür. Bu kontrol işlemi sırasında GİB Hassas ÖKC verisinin ve Üye İşyeri Anlaşması Yapan Kuruluşlara ait hassas verilerin ÖKC TSM Merkezi tarafından açılmaması ve saklanmaması

gerekmektedir. GİB BS'nin cihazları yönetme, ayakta tutma, gelen bilgilerin doğruluğunu değerlendirme veya Yeni Nesil ÖKC'lerin durumu ile ilgili üreticiye veya ÖKC TSM Merkezleri'ne geri bildirim yapma görevi bulunmamaktadır. Bu sorumluluk ÖKC üreticileri ile birlikte ÖKC TSM Merkezleri'ne aittir.

(6) ÖKC Üreticileri, cihazda oluşturularak ÖKC TSM Merkezleri üzerinden GİB BS'ye gönderilen GİB ÖKC mesajlarının kaynağının doğruluğundan, değişmezliğinden ve bütünlüğünden sorumludur. GİB ÖKC mesajlarının teknik kılavuzlarda ve protokollerde öngörülen zaman ve sıralamaya uygun olarak GİB BS'ye gönderilmesi gerekmekte olup, bozuk, hatalı veya atak içeren mesajların gönderilmesi halinde sorumluluk ÖKC Üreticilerine aittir.

(7) Yeni Nesil ÖKC'lerin ÖKC TSM Merkezleri üzerinden GİB BS'ye gönderecekleri mesajların doğrudan GİB BS tarafından kayıt ve analiz edilebilecek mahiyette olması esas olup, bu mesajlar üzerinde GİB BS'nin ilave bir çalışma yapılmasına ihtiyaç gerektirmeyecek yapıda ve ilgili mesajlaşma protokollerine uygun şekilde olması esastır.

(8) ÖKC TSM Merkezleri, EFT-POS özellikli ÖKC'ler ve EFT-POS cihazları ile entegre çalışan Yeni Nesil ÖKC'ler de dahil, üzerlerinden bankacılık mesajlarının da geçecek olması nedeniyle BDDK ve PCI SSC düzenleme ve standartlarının gereklerini karşılaması zorunludur.

(9) Üye İşyeri Anlaşması Yapan Kuruluşlara ait olanlar da dahil olmak üzere Yeni Nesil ÖKC'ler üzerinde çalışan tüm uygulamalar ÖKC TSM Merkezi üzerinden Yeni Nesil ÖKC'lere bağlanacaktır. Üye İşyeri Anlaşması Yapan Kuruluşun yetkilendireceği kişi veya kurumlar, Yeni Nesil ÖKC ile birlikte çalışacak bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM Merkezleri'ne bildireceklerdir. Bu işlemler ÖKC TSM Merkezleri aracılığıyla gerçekleştirilecektir. Yeni Nesil ÖKC'lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntıları vb.) ÖKC üreticileri sorumludur.

(10) ÖKC TSM Merkezleri (Dış Hizmet Sağlayıcılar dahil) vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmak zorundadır.

ÖKC TSM Merkezlerinin Güvenlik Esasları

MADDE 8 – (1) ÖKC TSM Merkezleri'nin güvenlik gereksinimleri Başkanlıkça yayınlanan "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezlerinin Başvuru, Test, Denetim ve Onay Teknik Kılavuzu" nda belirtilen kurallar çerçevesinde sağlanacaktır. ÖKC TSM Merkezleri'nin sistem güvenliğinde ve sisteminin düzgün işlemesinde önemli ve dikkat edilmesi gereken temel hususlar bu doküman içerisinde yer almaktadır. Güvenlik gereksinim ana başlıkları aşağıdaki gibidir;

a- Kritik Varlıklar: Sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu ve erişilebilirliğini olumsuz yönde etkileyecek varlıklardır.

b- Aktörler:

1. Yetkili Kullanıcılar (İç personel)
2. Yetkisiz Kullanıcılar (Hacker, Siber Terörist, vb.)
3. Teçhizat ve Yazılımlar
4. Çevresel Koşullar

c- **Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale**: ÖKC TSM Merkezi'nin sistem güvenliğinin oluşturulması, gerçeklenmesi, bakımının yaptırılması ve sürekli geliştirilmesi için ISO 27001 sertifikasını alması gerekmektedir. Sistemin iş sürekliliğini ve felaketten kurtarma gereksinimlerinin standardizasyonunu sağlamak için ISO 22301 sertifikalarının alınması gerekmektedir.

ç- **Kullanılan Donanımların Güvenliği**: ÖKC TSM Merkezi; GİB BS ve ÖKC ile haberleşmek için kriptografik anahtarlar kullanılması ve bu anahtarların ÖKC TSM Merkezler'inde FIPS 140-2 level 3 ve üzeri sertifikası almış HSM'ler ile saklanması gerekmektedir.

d- **Kullanılan Yazılımların Güvenliği:** ÖKC TSM Merkezleri'nin kullandığı yazılımlarının güvenli olması gerekmektedir.

e- **Güvenlik Denetimi**: Yılda bir kez GİB ve ÖKC Üreticisi mutabakatıyla belirlenecek tarihlerde bağımsız firmalar tarafından gerçekleştirilecek sızma testleri ile proje genelinde hedeflenen bilgi güvenliği standardına ulaşılıp ulaşılmadığı sınanacak, tespit edilen açıklıkların kapatılmasına yönelik tavsiyeler detaylı bir şekilde bu firmalar tarafından kural koyuculara raporlanacaktır.

ÖKC TSM Merkezlerinin Risk Yönetim Esasları

MADDE 9 – (1) ÖKC TSM Merkezi ÖKC Mesajlarına dair işlemlerde kullandığı bilgi sistemlerine ve tüm operasyon süreçlerine ilişkin riskleri tespit etmek, analiz etmek, ölçmek, izlemek, kontrol etmek ve raporlamak üzere kapsamlı bir risk yönetim planı oluşturur.

(2) ÖKC TSM Merkezi altyapısının bir parçası olan veya herhangi bir noktada ÖKC Mesajlarını yöneten donanım, yazılım, uygulama geliştirme, değişim yönetim süreçleri, iletişim alt yapıları ve operasyon süreçleri risk yönetim planına dâhil edilir.

(3) ÖKC üreticisi, ÖKC TSM Merkezi'nin uyguladığı risk yönetim planı çerçevesinde, faaliyetlerinde kullandığı bilgi teknolojisi varlıklarının risk analizini, Dış Hizmet Sağlayıcılarından kaynaklanabilecek riskleri de dikkate alarak gerçekleştirir. Bu kapsamda varlık envanteri hazırlar, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemleri belirler, yazılı hale getirir.

(4) Bilgi sistemlerine ilişkin risk analizleri, hizmetleri etkileyen önemli güvenlik olayları sonrasında, önemli bir değişiklik öncesinde ve yeni tehditlerin tespiti halinde gözden geçirilir ve yılda en az bir defa olmak üzere güncellenir.

ÖKC TSM Merkezi İş Sürekliliği Yönetimi

MADDE 10 – (1) ÖKC TSM Merkezi, ÖKC'ler üzerinden sunduğu hizmetin sürekliliğini ve kesinti halinde faaliyetlerinin sürdürülebilmesini amaçlayan üst yönetim (ÖKC TSM Merkezi'nin imzaya yetkili yönetimi) tarafından onaylanmış iş sürekliliği yönetim sürecini tesis eder. Bu kapsamda, iş sürekliliği planı ve planının bir parçası olan bilgi sistemleri süreklilik planını hazırlar.

(2) ÖKC TSM Merkezi, iş sürekliliği planlamasına yönelik olarak iş etki analizi yapar ve kurtarma stratejilerini belirler. Bu kapsamda, iç ve dış bağımlılıklar belirlenir ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve

bunların potansiyel etkileri ÖKC TSM Merkezi tarafından değerlendirilir.

(3) İş sürekliliği yönetimi sürecinde, bilgi sistemleri varlıklarının ve tutulan verilerin önem düzeyleri dikkate alınarak iş etki analizi çerçevesinde kabul edilebilir kesinti süreleri belirlenir ve bu süreler içinde servislerin tekrar erişime açılabilmesini sağlamak amacıyla, alternatifli kurtarma prosedürleri ile yetki ve sorumlulukları içeren iletişim prosedürleri ÖKC TSM Merkezi tarafından geliştirilir. Süreç kapsamında; performans takip teknikleri kullanılır, kapasite planlaması yapılır, işlem hacmi tahminleri doğrultusunda stres testleri gerçekleştirilir, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif kanallar oluşturulur. Ayrıca, servis dışı bırakma atakları göz önünde bulundurulur ve buna karşı gerekli önlemler ÖKC TSM Merkezi tarafından alınır.

(4) ÖKC TSM Merkezi tarafından, süreç kapsamında yurt içinde bir İkincil Merkez tesis edilir. Veri ve sistem yedekleri kurulan bu İkincil Merkezde kullanıma hazır bulundurulur.

(5) ÖKC TSM Merkezi, bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra iş sürekliliği planını gözden geçirir ve günceller. Mevcut planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa bir günlük operasyonlarının tamamını İkincil Merkez üzerinden gerçekleştirecek şekilde testler yapar, test sonuçlarını ve hizmet sürekliliğini etkileyen olayları üst yönetime raporlar.

(6) ÖKC TSM Merkezi, bilgi sistemlerine ilişkin beklenmedik olayları yönetmek ve bunların etkilerini en aza indirmek üzere acil ve beklenmedik durum planı oluşturarak gerekli önlemleri alır. Faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci ile beklenmedik olayları erken haber almayı sağlayacak mekanizmaları tesis eder. Acil ve beklenmedik durum planı kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulma, hasarı tespit etme, olayın potansiyel boyutunu ve etkisini gösterme, yetkili yönetim birimine ulaştırılmasını sağlama ve etkilenen müşterileri tespit etme süreçlerini ele alır. Bilgi sistemlerine ilişkin beklenmedik olayların sonradan incelenmesine imkân tanıyacak, yetkili merciler tarafından talep edildiğinde kullanılabilecek nitelikte kayıt ve bilgileri toplayan bir mekanizma oluşturur.

(7) ÖKC TSM Merkezi, ÖKC'ler üzerinden sunduğu hizmete ilişkin Üye İşyeri Anlaşması Yapan Kuruluşa sözleşmede taahhüt ettiği düzeyde servis sürekliliği sağlar ve raporlar.

(8) ÖKC TSM Merkezi, ÖKC TSM Bilgi Sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde, mimari tasarımın ve testlerin yapıldığına dair güvence sunar. Bu kapsamda sunulacak güvence ve raporlamalar asgari olarak Uptime Institue Tier 2 standartlarını sağlamalı/yerine getirmelidir. Kesinti süreleri yıllık plansız toplam 18 saati ve planlı bir defada 1,5 saati aşmayacak şekilde yılda 4 defadan (toplam 6 saatten) fazla olamaz. Planlı kesintilerin ÖKC TSM Merkezi'nden hizmet almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara 15 gün önceden gerekçeleri ile birlikte bildirilmesi zorunlu olup planlı kesintilerin günün yoğun olmayan saatlerinde gerçekleştirilmesi gerekmektedir. ÖKC TSM Merkezi aylık olarak kullanılabilirlik raporunu hazırlayacak ve GİB'e ve ÖKC TSM Merkezi hizmeti almakta olan Üye İşyeri Anlaşması Yapan Kuruluşlara sunacaktır. Bu rapor aylık olarak denetimlerde sunulmak üzere hazır bulundurulur.

Değişiklik Yönetimi

MADDE 11 – (1) ÖKC TSM Merkezi, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve ÖKC Mesajlarını yöneten donanım ve yazılımlara ilişkin her türlü bakım, yama ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak yazılı ve etkin bir değişiklik yönetimi süreci işletir.

(2) ÖKC TSM Merkezi, ÖKC Mesajını yöneten yazılımlar için, yazılım geliştirilen ortamların ve geliştirilen yazılımların canlı ortama aktarılmadan önce test edildiği ortamların canlı ortamlardan ayrılmasını ve bu ortamların herhangi birinde değişiklik yapma yetkisine sahip personelin diğerlerinde değişiklik yapma yetkisinin bulunmamasını sağlar, test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleştirilemez nitelikte olmasını temin eder.

(3) ÖKC TSM Merkezi, ÖKC Mesajını yöneten sistemlere ilişkin değişikliklerde etki analizi yapılmasını, değişikliğin yetkili kişi veya kişilerce onaylanmasını ve değişikliği geri çekme prosedürünün oluşturulmasını sağlar.

ÖKC Mesajlarının (ÖKC Durum Verisi ve GİB Hassas ÖKC Verisi) Yönetimi

MADDE 12 – (1) ÖKC'ler, ÖKC TSM Merkezi ile GMP'lerde belirtilen güvenli ilklendirme yapılmadan yaşam döngüsüne başlayamaz.

(2) ÖKC Durum Verisi ÖKC'den gelen her bir mesaj için ÖKC TSM Merkezi'nde tutarlılık kontrollerinden geçirildikten sonra, GİB Hassas ÖKC verisi ise ÖKC TSM Merkezi üzerinden GİB BS'ye GMP'lere uygun olarak ve anahtarları korunarak iletilir.

(3) ÖKC TSM Merkezleri ÖKC ilklendirilmesiyle birlikte her mesaj için mesaj işlem kontrolleri yapmalıdır. Mesaj işlem kontrollerinin; mesajların sıralamalarında, formatlarında, geliş kaynaklarında, zamanlarında vb. unsurlarda tutarsızlıkları ve atakları önlemek için yapılması şarttır. Bu tutarsızlıkları ve atakları analiz ederek gerekli düzeltmeleri sağlamak ve problemleri çözmek ÖKC TSM Merkezleri ile birlikte ÖKC Üreticilerinin görevidir.

(4) Tutarsızlık ve atak içeren mesajlar ÖKC TSM Merkezleri tarafından geçersiz mesaj kabul edilecek olup bu mesajlar gerekli araştırmaya tabi tutulmadan ve ÖKC Üreticilerince ÖKC üzerinde düzeltme işlemleri yapılmadan GİB BS'ye iletilmeyecektir. Ancak gönderilmesi gereken mesajlar, durumun oluştuğu tarihten itibaren en geç ÖKC onarım süresi içerisinde ÖKC üreticisi tarafından düzeltilip ÖKC TSM Merkezi üzerinden GİB BS'ye düzeltilmiş mesaj formatında aktarılacaktır.

(5) ÖKC TSM Merkezleri tarafından yapılan mesaj kontrolleri sırasında karşılaşılan tüm tutarsızlıklar ve ataklar GİB'e bildirilmek zorundadır.

(6) GİB Hassas ÖKC Verisi, Yetkilendirilmiş ESHS tarafından sağlanan sertifikalar kullanılarak GİB BS sunucuları tarafından ÖKC'ye iletilen anahtarlar ile ÖKC'de şifrelenir ve GİB BS'de gelen verinin imza kontrolü yapıldıktan sonra belirlenmiş anahtarlar ile açılır.

(7) ÖKC'ler GMP protokollerine uygun olarak, sadece ÖKC TSM Merkezleri'ne bağlı olarak çalışmak ve ÖKC TSM Merkezleri üzerinden GİB BS ve Üye İşyeri Anlaşması Yapan Kuruluşlar ile haberleşmek zorundadırlar.

Denetim İzlerinin Oluşturulması

MADDE 13 – (1) ÖKC TSM Merkezleri, GİB Yeni Nesil ÖKC Mesajlarının yönetildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, işlem altyapısını kullanan yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması tesis eder.

(2) Denetim izi, kullanıcılara sorumluluk atayan, yeterli detay içeren ve şüpheli bir olayı izleme imkânı

sunan nitelikte tutulur.

(3) Denetim izleri asgari olarak aşağıdaki bilgileri içerir:
a) İşlemi gerçekleştiren uygulama,
b) İşlemi gerçekleştiren ve varsa onaylayan kişiler,
c) İşlemin açıklaması,
ç) Yapılan işlemin zaman bilgisi,
d) İşlemin olumlu veya olumsuz sonucu,
e) Etkilenen veri ve sistemlerin bilgisi.

(4) Denetim izleri asgari 5 yıl süreyle denetime hazır bulundurulacak şekilde ÖKC TSM Merkezleri tarafından saklanır.

(5) Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır.

(6) Denetim izleri, yetkisiz değiştirilmeye karşı ayrıcalıklı yetkiye sahip kullanıcıların kendi faaliyetlerine ilişkin denetim izlerine müdahale edemeyeceği şekilde ÖKC TSM Merkezleri tarafından korunur.

(7) Denetim izi mekanizmalarının geçici veya sürekli olarak durdurulmasını önlemeye ve durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(8) Denetim izlerinin yeterli güvenlik seviyesi bulunan ortamlarda saklanması, yedeklerinin alınması ve olası bir mücbir sebep ya da olağanüstü hal sonrasında erişilebilir olması gerekmektedir.

(9) Bilgi Sistemleri faaliyetleri kapsamında dış hizmet alınıyor olması durumunda ÖKC üreticisi, dış hizmet sağlayıcısı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve kendisinin bu denetim izlerine erişebilirliğini temin eder.

(10) ÖKC Üreticisi, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin iç süreçlerini oluşturur.

(11) ÖKC'lere ÖKC TSM Merkezi'nde Denetim izi oluşturulmadan bir yazılım veya parametre yükleme işlemi yapılamaz.

Dış Hizmet Alımı

MADDE 14 – (1) Dış Hizmet Alan ÖKC Üreticisi, bu Kılavuz kapsamında almak zorunda olduğu ISO 20000, 22301, 27001 ve PCI DSS belgelerine Dış Hizmet Sağlayıcısının uyumluluk onay durumunu izler ve aldığı hizmetin herhangi bir kapsam kısıtlamasına gitmeksizin mezkûr standartlar ile uyumlu olduğunun yılda bir defa belgelendirildiğinden emin olur.

(2) ÖKC Üreticileri, Dış Hizmet Sağlayıcısının bu Kılavuzda belirlenen koşullar ile uyumlu olduğuna ve sistem altyapısının güvenlik seviyesini düşürmediğine ilişkin, Dış Hizmet Sağlayıcısı nezdinde gerçekleştirdiği denetimlerle veya başka taraflarca gerçekleştirilen yerinde denetimler sonucunda oluşturulan onay belgelerinden faydalanarak emin olur ve buna ilişkin belgelendirme dokümanlarını kendisinde muhafaza eder ve talep edilmesi halinde GİB'e sunar.

(3) ÖKC TSM Merkezleri'nin birincil ve ikincil sistemleri (Dış Hizmet Sağlayıcıdan temin edilenler

dahil) yurt içinde olmak zorundadır. TSM Merkezlerine ilişkin ikincil sistemler; birincil sistemden farklı bir il sınırları içinde ve aralarında en az 300 km mesafe bulunacak şekilde kurulmuş olması zorunludur.

(4) ÖKC üreticileri, kendi kuracakları ÖKC TSM Merkezleri'ne ait birincil merkezinin donanım altyapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil merkezin tüm işletim ve operasyon süreçlerini ÖKC üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personel nitelik ve niceliği ile ilgili "TSM Merkezi Personel Gereksinimleri" başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir kısmının ÖKC üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC TSM Merkezi Dış Hizmet Sağlayıcısının verdiği bu hizmetler bakımından da test, değerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC üreticileri kendi kuracakları ÖKC TSM Merkezleri'ne ait ikincil merkezinin; sadece donanım alt yapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım alt yapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC üreticine ait kendi personeli ile yürütmek zorundadır.

Dış Hizmet Sağlayıcı, ÖKC TSM Merkezleri'ne ait ikincil merkezinin; sadece donanım alt yapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım alt yapısının yönetimi ile tüm işletim ve operasyon süreçlerinin yönetiminin ilgili DHS/ ÖKC üreticisine ait personel tarafından yürütülmesi zorunludur.

ÖKC TSM Merkezleri'nin Denetim Esasları

MADDE 15 – (1) Onay Denetimi; ÖKC TSM Merkezi olmak üzere GİB'e başvuruda bulunan ÖKC üreticilerinin kurmuş oldukları sistemin GİB tarafından talep edilen gerekli şartları haiz olup olmadığının tespiti için gerçekleştirilen denetim sürecidir. ÖKC TSM Merkezleri'nde gerçekleştirilecek Onay Denetim faaliyetleri esas itibariyle "Bilgi Sistemleri Denetimi" ve "Güvenli Haberleşme Denetimi" olarak isimlendirilen iki kısımdan oluşmaktadır.

(2) Yıllık Denetim; ÖKC TSM Merkezi'nin GİB tarafından onayını takip eden 1 yılın sonunda gerçekleştirilmesi gereken ve devam eden her yıl en az 1 defa olmak kaydı ile gerçekleştirilecek olan denetim sürecidir. ÖKC TSM Merkezleri'nde gerçekleştirilecek yıllık denetim faaliyetleri, TSM Merkezi onay denetiminde de yer alan "Bilgi Sistemleri Denetimi" sürecini kapsamaktadır.

(3) Bilgi sistemleri denetimi; ÖKC TSM Merkezleri'nin bu Kılavuzda belirtilen hükümlere uyum durumunun tespit edilmesi amacıyla ÖKC Durum verisi ve GİB Hassas ÖKC verisini ve kural koyucular tarafından hassas veri olarak kabul edilen verileri yöneten kişiler, süreçler, yazılımlar, donanımlar ile bu kapsamda tesis edilen iş süreçleri ve iç kontrollerin kural koyucular tarafından belirlenen bağımsız denetim kuruluşları (ÖKC TSM Merkezi ve ÖKC üreticisi ile doğrudan veya dolaylı yönetim, temsil görevi bulunmayan) tarafından değerlendirilmesi sonucunda, söz konusu iç kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir. Bilgi Sistemleri Denetiminin uygulama ve raporlama esasları "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezleri'nin Başvuru, Test, Denetim ve Onay Teknik Kılavuzu"nda detaylı olarak belirtilmiştir.

(4) Güvenli haberleşme denetimi; ÖKC TSM Merkezleri'nin bu Kılavuzda belirtilen hükümlere uyum durumunun tespit edilmesi amacıyla, ÖKC TSM Merkezleri'nin Yeni Nesil ÖKC ve GİB BS ile olan

mesajlaşma yönetiminin; Başkanlıkça yayınlanan/paylaşılan ve ÖKC TSM Merkezlerine doğrudan veya dolaylı olarak etki eden mesajlaşma protokolü dokümanlarının (GMP-1, GMP-2, GMP-3 vb.) isterlerine uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir. Bilgi Sistemleri Denetiminin uygulama ve raporlama esasları "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezleri'nin Başvuru, Test, Denetim ve Onay Teknik Kılavuzu"nda detaylı olarak belirtilmiştir.

(5) GİB, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir.

(6) Yıllık denetimler sonucunda düzenlenen raporda tespit edilen sorun ve eksiklikler ÖKC TSM Merkezleri tarafından ivedilikle giderilir.

(7) ÖKC TSM Merkezi, herhangi bir kapsam kısıtlamasına gidilmeden ve işlem sayısından bağımsız olarak, PCI DSS ile uyumlu olduğunu, asgari yılda bir defa, standartları PCI SSC tarafından tanımlanmış olan yerinde denetimler ile ispatlar.

(8) ÖKC TSM Merkezi, gerçekleştirilen denetimler sonucunda oluşturulan Denetim Mektubunu ve PCI DSS onay belgelerini, hizmet verdiği bütün Üye İşyeri Anlaşması Yapan Kuruluşlar ile paylaşmak zorundadır.

(9) ÖKC TSM Merkezleri'nde gerçekleştirilecek Denetim Faaliyetlerine ilişkin detaylar Başkanlıkça yayınlanan "Yeni Nesil Ödeme Kaydedici Cihazlara Ait ÖKC TSM Merkezleri'nin Başvuru, Test, Denetim ve Onay Teknik Kılavuzu" nda açıklanmıştır.

EFT POS Özellikli ÖKC'ler / PinPad veya EFT-POS Cihazı İle Çalışan ÖKC'ler İle İlgili ÖKC Üreticileri ve Üye İşyeri Anlaşması Yapan Kuruluşlara İlişkin Esaslar

MADDE 16 – (1) ÖKC üreticileri, ÖKC'ler üzerinde veya ÖKC'lerle birlikte çalışacak cihazlarda (EFT-POS, PinPad), Üye İşyeri Anlaşması Yapan Kuruluşlara ait uygulamaların ÖKC'ler ile Teknik Kılavuz ve GMP dokümanlarında belirtilen şekilde uyumlu olarak çalıştırılmasını temin etmek zorundadır.

(2) Bu zorunluluğun yerine getirilmesi amacıyla ÖKC üreticisi, Üye İşyeri Anlaşması Yapan tüm kuruluşlardan uygulamalarının (yazılım ve donanım dahil) Teknik Kılavuz ve GMP dokümanlarında belirtilen şekilde ÖKC ile uyumlu çalışabilir hale getirilmesini yazılı olarak talep eder. Bu talep üzerine Üye İşyeri Anlaşması Yapan Kuruluşlar yazılı talep tarihinden itibaren en geç 120 gün içerisinde uygulamalarını ÖKC ile uyumlu şekilde çalışabilir hale getirmek zorundadır.

(3) Ticari hayatın devamlılığını ve kartlı ödeme işlemlerinin aksatılmadan yürütülmesini sağlamak bakımından ÖKC üreticileri ve Üye İşyeri Anlaşması Yapan Kuruluşların, her marka ve model yeni nesil ödeme kaydedici cihaz ile her marka model EFT-POS/PinPad cihazının ve bunlara ait uygulamaların birlikte Teknik Kılavuz ve GMP dokümanlarında belirtilen şekilde uyumlu olarak çalıştırılabilir olmasını temin etme zorunlulukları bulunmaktadır. Üye İşyeri Anlaşması Yapan Kuruluşların, sadece üye işyeri anlaşması yaptıkları işyerlerinde uygulamalarının çalıştırılacağı tabiidir.

(4) Üye İşyeri Anlaşması Yapan Kuruluşun ÖKC yaşam döngüsü kapsamındaki yazılım geliştirme, yükleme, güncelleme, parametre yükleme, kartlı işlemlerin yönetimi, güvenli anahtar yönetimi, terminal güvenlik kontrolleri, işlemlerin yönlendirilmesi, çalıştırılması ve sonuçlarının sözleşmelere ve

sözleşmelerde belirtilen kriterlere (SLA- Service Level Agreement) uygun şekilde iletilmesi vb. faaliyetlerinin yetki ve sorumluluğu ÖKC Üreticilerindedir.

(5) ÖKC'ler üzerinde veya ÖKC'ler ile birlikte çalışacak cihazlar (EFT-POS, Pinpad) yoluyla Üye İşyeri Anlaşması Yapan Kuruluşun uygulamalarının çalıştırılmasına ilişkin sahada yapılması gereken tüm servis ve saha operasyonlarının yetki ve sorumluluğu ÖKC üreticilerindedir.

(6) ÖKC Üreticileri, Üye İşyeri Anlaşması Yapan Kuruluşa vereceği hizmetler kapsamında kural koyucuların koymuş oldukları standartlara uymak ve ilgili sertifikalara sahip olmak zorundadır.

(7) Üye İşyeri Anlaşması Yapan Kuruluş, hizmet aldığı ÖKC TSM Merkezi'nin PCI DSS ile uyumlu olduğuna ve işlem altyapısının güvenlik seviyesini düşürmediğine ilişkin, gerçekleştirdiği denetimlerden veya geçerliliğini yitirmemiş denetim raporu, sertifika gibi belgelerden faydalanarak makul güvence oluşturur.

(8) Üye İşyeri Anlaşması Yapan Kuruluşlar, sahtecilik ve dolandırıcılık faaliyetlerinin önlenmesine yönelik olarak, anlaşması bulunan üye işyerleri ve ÖKC'ler için takip mekanizmaları tesis eder. Takip ettiği alanlarda olağan dışı değişiklik meydana gelen üye işyerleri ile ÖKC'ler için, gerekli incelemeleri gerçekleştirerek uygun aksiyonları alır, ÖKC üreticisine ve ÖKC TSM Merkezi'ne bu konuda gereken bilgilendirmeleri yapar.

(9) ÖKC TSM Merkezleri, GİB ve yasalarca yetkili kılınmış diğer kurumlardan gelen talimatlar doğrultusunda ÖKC'lerin fonksiyonlarının tümünü veya belli bir kısmını durdurabilir veya değiştirebilir.

(10) ÖKC üreticileri ve bunlara ait ÖKC TSM Merkezleri kural koyuculardan gelen talimatlar doğrultusunda veya ÖKC üreticilerinin oluşturduğu sahtekarlık senaryolarına göre otomatik izleme mekanizmalarını ve raporlamalara uygun şekilde sahtekarlık önleme ve izleme sistemini kurmakla yükümlüdür.

(11) EFT-POS Özellikli ÖKC'ler ile PinPad bağlanmış Basit/Bilgisayar Bağlantılı ÖKC'lerde terminal yönetim ve Üye İşyeri Anlaşması Yapan Kuruluşlar ile iletişim, ÖKC ve ÖKC TSM Merkezi üzerinden şifreli olarak GMP'lerde belirtilen kurallara göre gerçekleşecektir.

(12) EFT-POS cihazlarının Basit/Bilgisayar Bağlantılı ÖKC'ye haricen bağlı olması halinde aşağıdaki esaslara da uyulması gerekmektedir.

a) EFT-POS cihazı ile Basit/Bilgisayar Bağlantılı ÖKC arasındaki iletişim ÖKC-Harici Donanım ve Yazılım Haberleşme Protokolü (GMP3) kurallarına göre gerçekleştirilecektir.

b) EFT-POS cihazı ÖKC TSM Merkezi üzerinden yapılan yönlendirme ile Üye İşyeri Anlaşması Yapan Kuruluş bilgi sistemleri ile haberleşecektir.

c) ÖKC TSM Merkezi, EFT-POS cihazı verilerini şifreli olarak Üye İşyeri Anlaşması Yapan Kuruluşlara, sözleşmelerinde belirtilen kriterlere (SLA- Service Level Agreement) ve PCI-DSS kurallarına uygun şekilde iletecektir.

ç) Finansal işlemler ÖKC'den başlayacak ve EFT-POS cihazı GMP3 kurallarına göre

tetiklendikten sonra provizyon işlemlerini gerçekleştirmek amacıyla ÖKC TSM Merkezi üzerinden bağlanarak Üye İşyeri Anlaşması Yapan Kuruluşlar ile şifreli olarak haberleşecektir. Bu suretle provizyon alındıktan sonra ödeme işlem bilgisi GMP3 kurallarına göre EFT-POS cihazından Basit/Bilgisayar Bağlantılı ÖKC'ye aktarılacaktır.

d) Basit/Bilgisayar Bağlantılı ÖKC'deki fiş bilgisi (Ekü Numarası, İşlem Sıra Numarası ve Z Raporu numarası) ile Harici EFT-POS cihazı ödeme verilerinin uyumu ve TÜBİTAK tarafından onaylanmış olan yazılım versiyonu kontrolü ÖKC TSM Merkezi tarafından kontrol edilecektir. Karşılaştırmada kullanılan değerler iz kaydı olarak tutulacaktır. Basit/Bilgisayar Bağlantılı ÖKC belli bir süre çevrimdışı kaldığında ise bu kontrol ilk gün sonunda yapılacaktır.

(13) Üye İşyeri Anlaşması Yapan Kuruluşlara ait kural koyucular tarafından hassas veri olarak kabul edilen verilerin ÖKC TSM Merkezi tarafından her halükarda açılmaması ve saklanmaması gerekmektedir.

(14) ÖKC TSM Merkezleri'nin, müşteriler (kart hamilleri) ile ilişkilendirilebilecek hiçbir veriye ve kural koyucular tarafından hassas veri olarak tanımlanan verilere erişebilme kabiliyeti bulunamaz. Bu Kılavuzda yer verilen sorumlulukları esnasında söz konusu veriye erişmesinin gerekmesi halinde, erişilebilen verinin anonim olması ve herhangi bir müşteri ile ilişkili olmaması sağlanır.

Üye İşyeri Adına Verilecek Olan Katma Değerli Hizmetler

MADDE 17 – (1) Faaliyetlerinde Yenil Nesil ÖKC kullanan mükellefler (üye işyeri) adına ve bir sözleşmeye bağlı olmak koşulu ile ÖKC TSM Merkezi ve ÖKC üreticisi üye işyerine yönelik katma değerli özel uygulamalar geliştirebilir, ÖKC üzerindeki bu uygulamalara ait verileri ÖKC veya ÖKC TSM Merkezi üzerinde sözleşmede belirtilen kurallar çerçevesinde işleyebilir, iletebilir, saklayabilir ve raporlayabilir.

(2) Tüm katma değerli uygulamalar Teknik Kılavuzlara ve GMP dokümanlarına uygun olarak geliştirilir ve işletilir.

(3) Üye İşyeri ile ÖKC Üreticisi ve ÖKC TSM Merkezi hizmetini veren kuruluş arasında yapılacak olan sözleşmelerde; işlenecek, saklanacak ve raporlanacak olan verilerin içeriği, saklama süresi, gizlilik kuralları ile ilgili yetki ve kapsamın açıkça belirtilmesi zorunludur.

(4) Bu sözleşmelerin elektronik ortamdaki bir örneğinin, sözleşmenin imzalandığı tarihten itibaren 15 gün içinde GİB BS'ye elektronik ortamda aktarılması gerekmekte olup buna ilişkin sorumluluk ÖKC üreticilerindedir.

Güvenli Odaların Kurulması, Denetimi ve Yönetimi

MADDE 18 - (1) Anahtar ve sertifika yüklemesi yapılacak olan güvenli odaların, TÜBİTAK Güvenli Oda Kriterlerine ve bankacılık sektörüne özel anahtarlar da yüklenecek ise "PCI – Pin Security Requirements" dokümanın ilgili bölümlerinde yer alan kriterlere uygun olması zorunludur.

(2) Güvenli Odaların denetimi yılda bir kere yaptırılarak, denetimlerinin belgeleri ÖKC Üreticisi tarafından GİB'e teslim edilir.

(3) Güvenli Oda yönetimi ve sorumluluğu tamamen ÖKC üreticisindedir.

Mevcut Teknik Kılavuz ve GMP Dokümanlarının Uyumlandırılması

MADDE 19- Bu Kılavuz'da belirlenen kurallar çerçevesinde ihtiyaç duyulması halinde mevcut Teknik Kılavuzlar ve GMP dokümanları GİB tarafından güncellenecek ve gizlilik esasları da göz önünde bulundurularak GİB internet sitesinde yayımlanacaktır.

Yürürlük ve Geçiş Hükümleri ile Sorumluluklar

MADDE 20 – (1) Bu Kılavuz GİB tarafından www.gib.gov.tr internet adresinde yayınlandığı tarihte yürürlüğe girer.

(2) ÖKC TSM Merkezi onay başvurusu GİB tarafından kabul edilen ÖKC üreticilerinin, ÖKC TSM Merkezi onay denetimlerini GİB tarafından belirtilen süre içerisinde tamamlatmaları zorunludur.

(3) ÖKC TSM Merkezi onayı almamış veya GİB tarafından belirlenen süre içerisinde denetimlerini tamamlatamamış olan ÖKC üreticilerinin; Yeni Nesil ÖKC'lerinin mühürleme ve satış işlemleri GİB tarafından durdurulabilir ve/veya ÖKC Üreticisi izinleri iptal edilebilir. İzni iptal edilen üreticiler tarafından satılmış ve mükelleflerce kullanılmakta olan ÖKC'lerin mali hafızalarında kayıtlı bilgiler ÖKC Yetkili Servislerince raporlanır ve bu raporlar mükellef tarafından ilgili Vergi Dairesine verilerek cihaz hurdaya ayrılma işlemine tabi tutulur. Hurdaya ayrılan cihazın rayiç veya emsal bedelinin mükellefe geri ödenmesinden ilgili ÖKC üreticisi yükümlüdür. Bu yükümlülüklerin ÖKC üretici onaylarının iptal edildiğinin GİB tarafından duyurulduğu tarihten itibaren en geç 60 gün içerisinde gerçekleştirilmesi gerekmektedir.

(4) Yeni Nesil ÖKC'lerin sahada bulunduğu süre içerisinde belirlenen kurallar dâhilinde tüm saha ve bakım hizmetlerinin sorumlusu ÖKC üreticisidir.

(5) Üye İşyeri Anlaşması Yapan Kuruluşun uygulamalarının Yeni Nesil ÖKC üzerinde çalışması için sahada yapılması gereken tüm kurulum, servis ve operasyonların sorumlusu ÖKC üreticisidir.

(6) Güvenilir Sertifika Otoritesi ile anlaşma yapılması, sertifika temini, sertifikaların yüklenmesi, bunun için uygun yapıların kurulması ve işletilmesi sorumluluğu ÖKC üreticisine aittir.

(7) Yeni Nesil ÖKC'ye bağlı olarak çalışacak olan bütün çevre birimlerinin ve buralarda çalışan yazılımların GMP kurallarına uygun olarak çalışmasına yönelik saha ve servis hizmetlerinin verilmesinin sorumlusu ÖKC üreticisidir.

(8) Yeni Nesil ÖKC'ler sadece kendi ÖKC TSM Merkezi ile haberleşecektir. Bu kuralın hayata geçirilmesi ve korunması yetki ve sorumluluğu ÖKC üreticisine aittir.

(9) ÖKC TSM Merkezi'nin GİB BS ile haberleşmesinin yönetilmesi sorumluluğu ÖKC TSM Merkezleri ile birlikte ÖKC üreticisine aittir.

(10) ÖKC TSM Merkezi'nin Üye İşyeri Anlaşması Yapan Kuruluş ile haberleşmesinin sorumluluğu ÖKC TSM Merkezleri ile birlikte ÖKC üreticisine aittir.

(11) Yeni Nesil ÖKC'ye bağlı olarak çalışacak olan Barkod, EFT-POS, PINPAD, otomasyon veya harici diğer tüm sistemlerin uyumlaştırma, entegrasyon işlemlerinin GMP'lerde belirtilen kurallara göre sağlanması yetki ve sorumluluğu ÖKC üreticisine aittir.

Yürütme

MADDE 21 – Bu Kılavuz hükümlerini Gelir İdaresi Başkanlığı yürütür.