GELİR İDARESİ BAŞKANLIĞI

Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi

Başvuru, İzin, Onay ve Denetim Süreçleri Kılavuzu

Versiyon 1.2
(10.07.2020)

Versiyon	Yayım Tarihi	Açıklama
1.0	30.12.2019	Kılavuzun ilk yayım tarihi
1.1	21.05.2020	Sistem kapsamında düzenlenecek ve tutarı 500 TL ye kadar olacak e-Arşiv Faturalarla ilgili 515 SN VUK Genel Tebliği ile yapılan değişikliklerin işlenmesi, Güvenli Mali Sertifika yönetimi teknik süreçlerinin açıklığa kavuşturulması, GMÖEBYS Uyumluluk Test Adımları Tablosunun güncellenmesi, İşletici Kuruluş Faaliyet İzni Başvuru Formunun eklenmesi, İşletici Kuruluş Sistemi Fonksiyonel Test Süreçleri Dokümanının hazırlanması, İşletici Kuruluş Sistemi Güvenlik Test Süreçleri Dokümanının hazırlanması, amacıyla düzenleme yapılmıştır.
1.2	10.07.2020	İşletici Kuruluş İzin Başvurusu, Uyumluluk Testleri Denetimi ve İznin Verilmesi bölümü güncellenmiştir.

İÇİNDEKİLER

1. Giriş 4
2. Tanımlar ve Kısaltmalar 4
3. Sistemin Temel Özellikleri 7
   a. Güvenli Mali Uygulama (GMU) 8
   b. e-Belge Entegrasyonu 14
   c. Ödeme Kabul Eden Araç 15
   ç. Mali Raporlar 17
   d. Güvenli Mali Sertifika ve İmza Yönetimi 17
   e. Yazılım Güvenliği 22
   f. Erişim Kontrolü 22
   g. Kimlik Doğrulama 23
   ğ. Oturum Açma ve Oturum Kimliği Doğrulama 23
   h. Uçtan Uca Güvenlik 24
   ı. Olay Kayıt Özelliği 24
   i. PCI Güvenlik Sertifikası 24
   j. EMV Sertifikaları 25
   k. Satış Yazılımı ve Harici Satış Uygulamaları ile Entegrasyonu 25
4. Sistemin Genel Güvenlik Gereksinimleri 25
5. Mülkiyet 31
6. Sistem Üzerinden Düzenlenebilecek e-Belgeler 32
7. Ödeme Türleri 34
8. Avans Ödeme ve Cari Hesap Tahsilatı İşlemleri 35
9. Fatura Tahsilatı İşlemleri 35
10. İşletici Kuruluş İzin Başvurusu, Uyumluluk Testleri Denetimi ve İznin Verilmesi 36
11. Sistemden Yararlanmak İsteyen Mükelleflerin Üyelik Başvurusu ve Sisteme Dahil Edilmesi 38
12. Sistem İle Birlikte ÖKC/YNÖKC Kullanımı 39
13. Denetim 39
14. Sorumluluk ve Ceza Uygulaması 40
15. Dış Hizmet Alımı 42
16. Değişiklik Hakkı 42

1. Giriş

Bu Teknik Kılavuz, Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemine (Sistem) ilişkin 01.06.2019 tarih ve 30791 sayılı Resmi Gazete'de yayımlanan 507 Sıra No'lu Vergi Usul Kanunu Genel Tebliğinin 4 üncü Maddesinin 5 inci fıkrası hükmü uyarınca hazırlanmış olup, Sisteme ilişkin teknik gereklilikler ile Sistem kapsamında hizmet sunacak İşletici Kuruluşların izin başvuru, onayı süreçleri ve Sistem işletilmesi sürecinde güvenlik, denetim, sorumluluk ve uygulamaya ilişkin uyulması gereken diğer usul ve esasları düzenlemektedir.

2. Tanımlar ve Kısaltmalar

TANIM	AÇIKLAMA
Bakanlık	Hazine ve Maliye Bakanlığı
Başkanlık	Gelir İdaresi Başkanlığı
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
TCMB	Türkiye Cumhuriyet Merkez Bankası
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
Diğer Regülasyon Otoriteleri	Başkanlık dışında kalan, Merkez Bankası ile Uluslararası Ödeme Sistemleri Güvenlik Sertifikasyon ve Regülasyon kuruluşları olan PCI (*Payment Card Industry*) ve EMVCo ile TROY veya Türkiye sınırları dahilinde kart işlemi kabul edilen Uluslararası (VISA, Mastercard, Amex, JCB vb.) şema sahibi kuruluşlar ı
EFT-POS	EMV Sertifikaları ile uyumlu kartlı ödeme sistemleri terminali *(Electronic Funds Transfer – Point of Sale)*

Elektronik Belge (e-belge)	Usul ve esasları Vergi Usul Kanunu genel tebliğleri ile belirlenen elektronik ortamda düzenlenebilen belgeler
EMV Sertifikaları	EMVCo kuruluşu tarafından verilen EMV sertifikaları
Finansal Kuruluş	507 Nolu VUK Genel Tebliği kapsamında; 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununa göre faaliyet gösteren Bankalar ile 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanuna göre faaliyet gösteren elektronik para kuruluşları ve ödeme kuruluşlarından Hazine ve Maliye Bakanlığınca yetkilendirilen ve bu Tebliğde belirtilen sistemin işletilmesi nedeniyle Bakanlık, Başkanlık ve sistem kapsamındaki hizmetlerden yararlananlara karşı asli sorumlu olan kuruluşları,
Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi (Sistem) (GMÖEBYS)	Finans kuruluşları ya da ÖKC üreticileri ile birlikte özel entegratör kuruluşlar tarafından bu Tebliğde belirtilen usul ve esaslara uygun gerçekleştirilen satış, ödeme/tahsilat işlemleri ile bu işlemlere ilişkin mali belgelerin elektronik belge olarak oluşturulması, iletilmesi, muhafaza ve ibraz edilmesi süreçlerine ilişkin olarak Bakanlıkça izin verilen sistemi,
Güvenli Mali Uygulama (GMU)	e-Belgelendirme Sisteminde yapılan tüm işlemlerin güvenli bir şekilde başlamasını ve güvenli bir şekilde sonlanmasını sağlayan ve ayrıca diğer uygulamaların bağlı olarak çalıştığı merkezi sistem ve uç nokta yazılımlarının tamamını içeren ana uygulama
İşletici Kuruluş	507 Sıra Nolu Tebliğde tanımlanan Finans Kuruluşu veya Ödeme Kaydedici Cihaz Üreticilerinden, sistemi işletmek üzere Hazine ve Maliye Bakanlığınca yetkilendirilen ve Sistemin işletilmesi nedeniyle Bakanlık, Başkanlık ve sistem kapsamındaki hizmetlerden yararlananlara karşı asli sorumlu olan kuruluşlardan her biri
Mali Raporlar	Başkanlık tarafından bu kılavuzda belirtilen ve İşletici Kuruluşlardan istenebilecek raporlar

Mobil İmza	Cep telefonu ve GSM SIM kart kullanılarak 5070 sayılı Elektronik İmza Kanunu ve ilgili yasal mevzuata uygun olarak ıslak imza niteliğinde güvenli bir biçimde elektronik imza işlemi yapılmasına imkân sağlayan uygulama
Ödeme Aracı	Bankalar, elektronik para kuruluşları ve ödeme kuruluşlarınca ödeme işlemlerinin yapılmasına olanak sağlayan fiziki/sanal kartları ya da bu kuruluşların hesaplarından ödemeyi gerçekleştirebilecek bilgileri barındıran ve fiziki niteliği bulunmayan yazılımsal uygulamalar (QR, NFC vb.)
Ödeme Kabul Eden Araç	Bir fiziki donanım üzerinden, Ödeme Aracını kabul ederek ödemeyi gerçekleştirebilen yazılımsal uygulamalar.
ÖKC / YNÖKC	3100 sayılı Kanunun 2 nci maddesinde ve 213 sayılı Kanunun mükerrer 257 nci maddesi hükümleri uyarınca yayımlanan 426 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinde belirtilen teknik dokümanlardaki nitelikleri haiz cihazlar
ÖKC Üreticisi	426 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinde belirtilen yeni nesil ödeme kaydedici cihazların üretim ve ithalatına ilişkin Bakanlıktan onay alan ve bu Tebliğde belirtilen sistemin işletilmesi nedeniyle Bakanlık, Başkanlık ve sistem kapsamındaki hizmetlerden yararlananlara karşı asli sorumlu olan kuruluşlar
Özel Entegratör Kuruluş	Elektronik belgelerin (*e-Fatura, e-Arşiv Fatura, e-Serbest Meslek Makbuzu vb. diğer elektronik belgeler*) düzenlenmesi, iletilmesi, alınması ve saklama hizmetleri ile ilgili mükelleflere hizmet verme konusunda Başkanlıktan alınmış özel entegratörlük izni bulunan kuruluşlar
PCI Güvenlik Sertifikası	

	PCI (*Payment Card Industry*) SSC (Security Standarts Counciel) tarafından **PCI PTS** (*PIN Transaction Security*) ve / veya Software-based PIN Entry on COTS (SPoC), PCI Contactless Payments on COTS (CPoC) vb. çözümleri kapsamında verilen güvenlik sertifikaları
Üye İşyeri Anlaşması 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 Kuruluşları
Yetkili Servis	İşletici Kuruluş tarafından, sorumluluğu kapsamındaki yazılımları için kurulum, güncelleme, anahtar yükleme, bakım, eğitim gibi hizmetleri vermek üzere yetkilendirilen servisler

3. Sistemin Temel Özellikleri

Sisteminin amacı, vergi doğuran mal ve hizmet satış işlemleri ile bunlara bağlı olarak yapılan ödemeleri / tahsilatları vergi kayıp ve kaçağına yol açmayacak şekilde, donanım bağımsız güvenli mobil uygulamalar aracılığıyla gerçekleştirmek ve sonuçlarını işlemin mahiyetine uygun düzenlenecek mali nitelikli e-Belgeler yoluyla kayıt altına almaktır.

Sistem üzerinden yapılacak her tür işlemin, Güvenli Mali Uygulama üzerinden (veya Güvenli Mali Uygulama ile entegrasyonu İşletici Kuruluş sorumluluğunda gerçekleştirilmiş ve satışa başlama işleminin güvenli mali uygulama tarafına yapılan başlangıç bildirimi ile tetiklendiği harici satış uygulama yazılımları üzerinden) başlaması ve ödeme/tahsilat da dâhil olmak üzere ilgili e-Belgelendirme süreçlerinin Güvenli Mali Uygulama aracılığıyla sonlandırılması esastır. Sistem bünyesinde bulunan satış uygulaması tarafından ya da Güvenli Mali Uygulama ile entegrasyonu İşletici Kuruluş sorumluluğunda sağlanmış harici satış uygulama yazılımları tarafından satışa ve müşteriye ait verilerinin girişi yapılarak güvenli mali uygulama da tetiklenebilir.

İzin verilen Sistem, üzerinde çalıştığı fiziki donanım tipine göre değişmek üzere iki farklı versiyon olarak sunulabilir. Bu versiyonlar ve bunlara ait temel özellikler aşağıdaki "**Temel Teknik Özellikler Tablosu**"nda gösterilmektedir:

Sisteminin Temel Teknik Özellikler Tablosu

Temel Teknik Özellikler	Sertifikalı Cihazlar üzerinden çalışan Sistem	Sertifikasız Cihazlar üzerinden çalışan Sistem
Güvenli Mali Uygulama	X	X
e-Belge Entegrasyonu	X	X
Ödeme Kabul Eden Araç	X	X
Mali Raporlar	X	X
Güvenli Mali Sertifika	X	X
Yazılım Güvenliği	X	X
Erişim Kontrolü	X	X
Kimlik Doğrulama	X	X
Oturum açma ve oturum kimliği doğrulama	X	X
Uçtan Uca Güvenlik	X	X
Olay Kayıt Özelliği	X	X
PCI Güvenlik Sertifikası	X	İ
EMV Sertifikaları	X	İ
Harici Uygulamalar ile Entegrasyon	İ	İ

X = Zorunlu **İ** = İhtiyari - = Yok

a. Güvenli Mali Uygulama (GMU)

Güvenli Mali Uygulama, İşletici kuruluşların 507 Sıra No.lu VUK Genel Tebliği, bu Kılavuz, 509 Sıra No.lu e-Belge uygulamalarına ilişkin VUK Genel Tebliği ve İlgili Teknik kılavuzları, satış uygulaması ve ödeme süreçleri ile Sistem kapsamında sürdürülmesi gereken iş, işlem ve entagrasyon süreçlerini sağlayan merkezi ve uç nokta yazılım sistemlerinin bütününü ifade etmekte olup, Sistem içindeki tek bir modül veya fonksiyonu tariflememektedir.

Sistem kapsamında gerçekleştirilen tüm işlemler ile bu işlemlere bağlı olarak yapılan ödeme / tahsilat işlemleri ve ilgili işlem uyarınca düzenlenmesi gereken e-Belgenin oluşturulması, vergi kayıp ve kaçağına yol açmayacak şekilde vergi ve ödeme / tahsilat güvenliğini sağlanması amacıyla Güvenli Mali Uygulamanın kontrolü ve yönetimi altında yapılır. İşletici Kuruluş bu sistem içerisinde, dâhili bir satış uygulaması çalıştırabileceği gibi isterse harici satış uygulaması da sunabilir. Harici Satış Uygulamalarının, İşletici Kuruluş sorumluluğunda, Güvenli Mali Uygulama ile entegre edilmesi zorunludur.

İşletici Kuruluş Güvenli Mali Uygulamasını (veya bu uygulamanın bir parçası olan Satış Uygulamasını), kendisine ait bir bilgi işlem merkezinden olmak koşuluyla Web tarayıcılar üzerinden erişilebilecek şekilde web tabanlı veya bulut sistemler yoluyla da sunabilir. Ancak ilgili satış uygulaması, uygulama marketleri ya da Yetkili Servisler aracılığı ile bir cihaza indirilerek / kurularak çalıştırılan bir uygulama ise, bu tip satış uygulamaları dâhili satış uygulaması olarak değerlendirilir. Güvenli mali uygulamanın bir parçası olmayan ve mükelleflerin faaliyetlerinde halihazırda kullandığı harici satış uygulama yazılımlarının işletici kuruluşa ait bilgi işlem sistemlerinde kurulması ve işletilmesi zorunluluğu bulunmamaktadır. Bu tür harici satış uygulama yazılımlarının güvenli mali uygulama ile entegrasyonu sağlanarak (satışa başlama işleminin güvenli mali uygulama tarafına yapılan başlangıç bildirimi ile tetiklenecek şekilde) ödeme ve mali e-belgeye dönüştürülmesi işlemlerinin işletici kuruluşlar tarafından yapılması gereği bulunmaktadır.

İster dâhili ister harici olsun, Satış uygulamalarının mali anlamdaki asli görevi ilgili işleme ait verilerin girişinin sağlanmasıdır.

Sistem üzerinden yapılacak satış ve diğer tüm işlemlerin, Güvenli Mali Uygulama üzerinden (veya Güvenli Mali Uygulama ile entegrasyonu İşletici Kuruluş sorumluluğunda gerçekleştirilmiş ve satışa başlama işleminin güvenli mali uygulama tarafına yapılan başlangıç bildirimi ile tetiklendiği harici satış uygulama yazılımları üzerinden) başlaması ve Güvenli Mali Uygulama üzerinden / aracılığıyla sonlandırılması esastır. Buna tahsilat işlemleri de dâhildir. Bu çerçevede, sistem kapsamında yapılan tahsilatların da vergisel işlemle ilişkilendirilmesi zorunludur. Satış ve diğer tüm işlemlerin Güvenli Mali Uygulama ile İşletici Kuruluş tarafından entegre edilen harici satış uygulama yazılımları üzerinden başladığı ve Güvenli Mali Uygulama üzerinden / aracılığıyla sonlandırıldığı durumlardaki işlemlerin güvenliği ve mali sorumluluğu İşletici Kuruluşa aittir. Ancak bu durum İşletici Kuruluşa e-Belge ile ilgili tüm süreçlerin gerçekleştirilmesine hizmet veren özel entegratör kuruluşların kendi görev, yetki ve hizmet sunumundan kaynaklanan idari, mali ve güvenlik sorumluluğundan İşletici kuruluşa karşı sorumlu olup, ayrıca GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır.

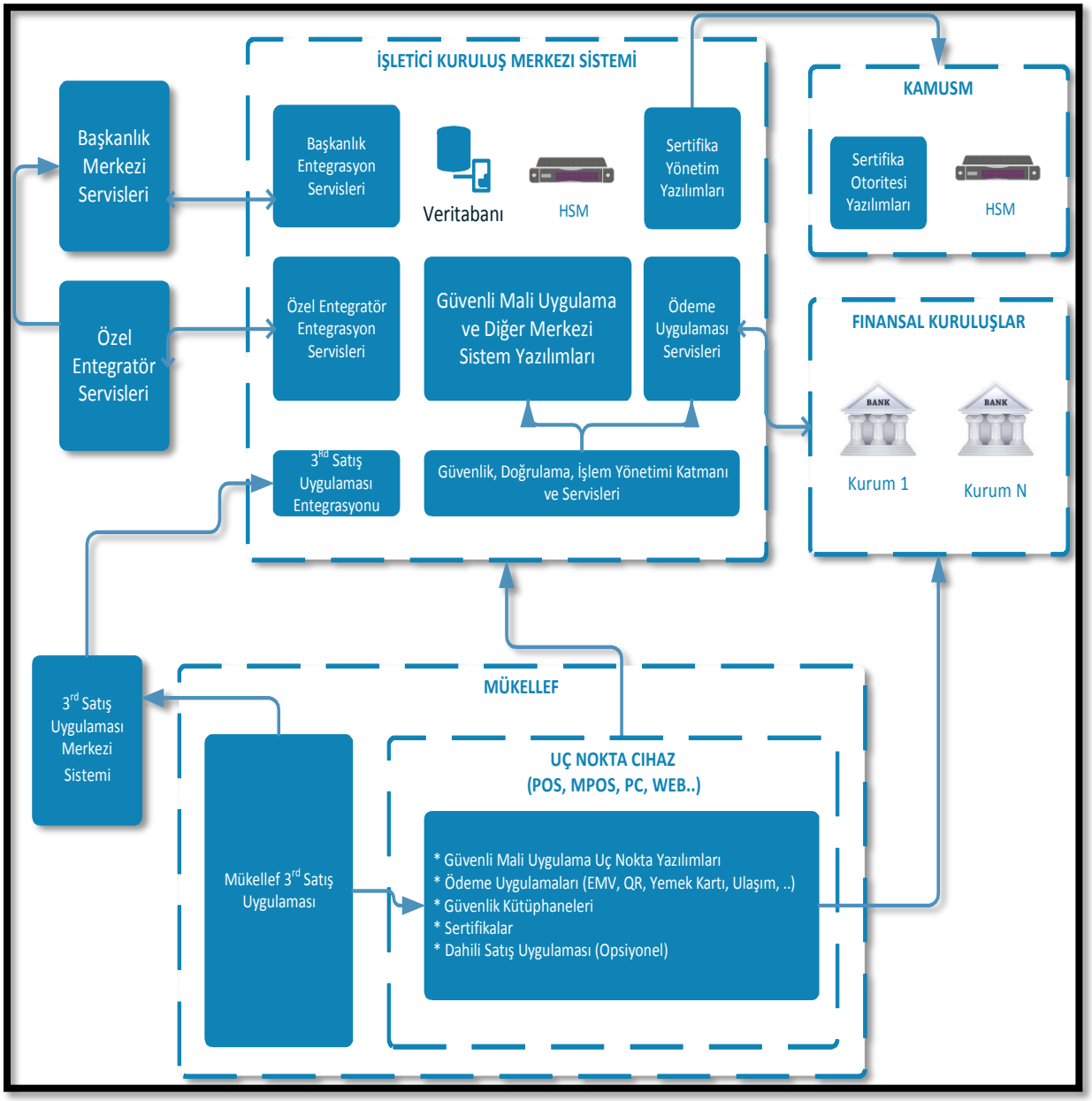
Güvenli Mali Uygulamanın İdareye karşı asli sorumlusu İşletici Kuruluştur. İşletici Kuruluş sorumluluğunda Güvenli Mali Uygulama ile entegrasyonu gerçekleştirilerek Sistem kapsamında kullandırılan harici satış uygulama yazılımından alınan e-Belge verilerini doğru şekilde e-Belgeye (bilgi fişi düzenlenmesi gereken hallerde bilgi fişlerine) dönüştürülmesinden (İşletici Kuruluşlar satış uygulamasından-harici satış uygulamaları dahil- alınan verileri doğru bir şekilde özel entegratöre iletmekten ve özel entegratörün de kendisine iletilen verileri doğru bir şekil ve şemada e-Belge'ye yerleştirerek dönüştürmesi ve e-Belgeyi oluşturmasından) asli olarak İşletici Kuruluşlar sorumlu olup, bununla birlikte e-Belge ile ilgili süreçlerin gerçekleştirilmesine hizmet veren özel entegratör kuruluşlar da GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır. Güvenli mali uygulamanın aşağıdaki özellikleri desteklemesi gerekir:

- Düzenlenecek e-Belgenin türüne uygun zorunlu bilgileri kendi üzerinden ya da satış uygulaması vasıtasıyla temin edecek nitelikte olmalı,

- Satışı gerçekleştirilecek mal ve hizmetlere ilişkin bilgiler ile vergi oran veya tutarları tanımlanabilmeli veya satış uygulamasından gelen bilgileri desteklemeli,
- Mal ve hizmet detayları, tutarları ile vergi hesapları doğru bir şekilde yapılabilmeli,
- İndirim/Artırımların vergi hesabı doğru dağılımında yapılabilmeli
- Yazılım versiyon kontrolü yapabilmeli (İşletici kuruluş uç noktada yapılan işlemlerin hangi güvenli mali uygulama yazılımı versiyonu ile yapıldığını takip edebilir, gösterebilir olmalıdır),
- Güvenli Mali uygulama sistem kapsamında gerçekleştirilen satış/ödeme/tahsilat işlemleri (iptal ve gerçekleşmeme dâhil) ve e-Belge düzenleme ve iptal etme ile ilgili log kayıtlarının oluşturulmasına ve işletici kuruluş tarafından takip edilmesine imkân sağlayacak nitelikte olmalı,
- Özel Entegratör ile güvenli iletişim sağlamalı,
- Kılavuzda tanımlanan tüm ödeme türlerini desteklemeli, Kılavuzda belirtilen mali Raporları üretebilmelidir.

Güvenli Mali Uygulamanın cihazlar ve web tarayıcı üzerinden çalıştığı durumların genel örnek topolojisi aşağıda gösterilmektedir. Ancak bu topoloji içinde yer alan her bir modül (mavi kutular), işletici kuruluş tarafından alt modüller olarak kırılabilir, detaylandırılabilir, yeni topolojiler tasarlanabilir.

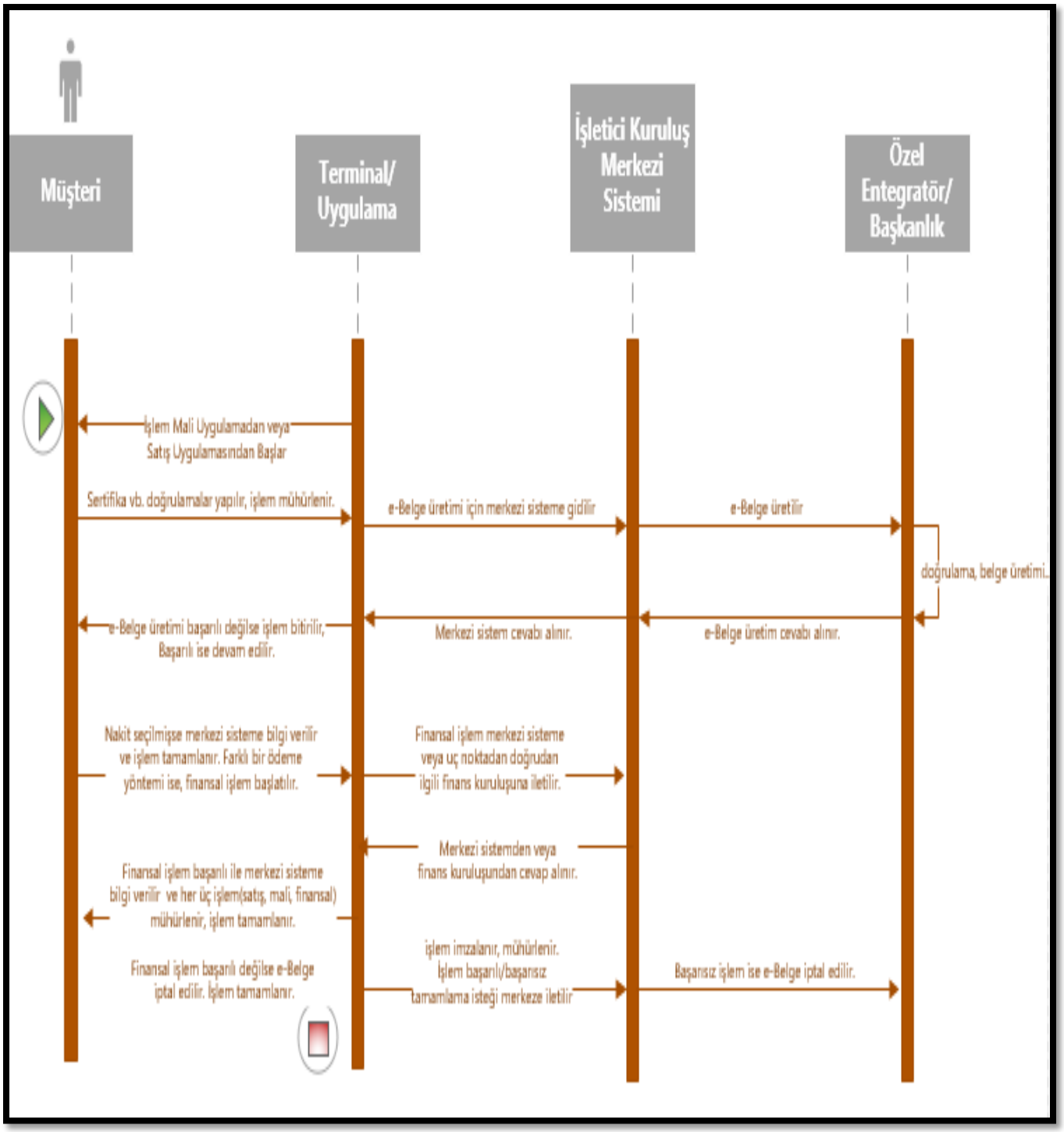
Genel Sistem Topolojisi:



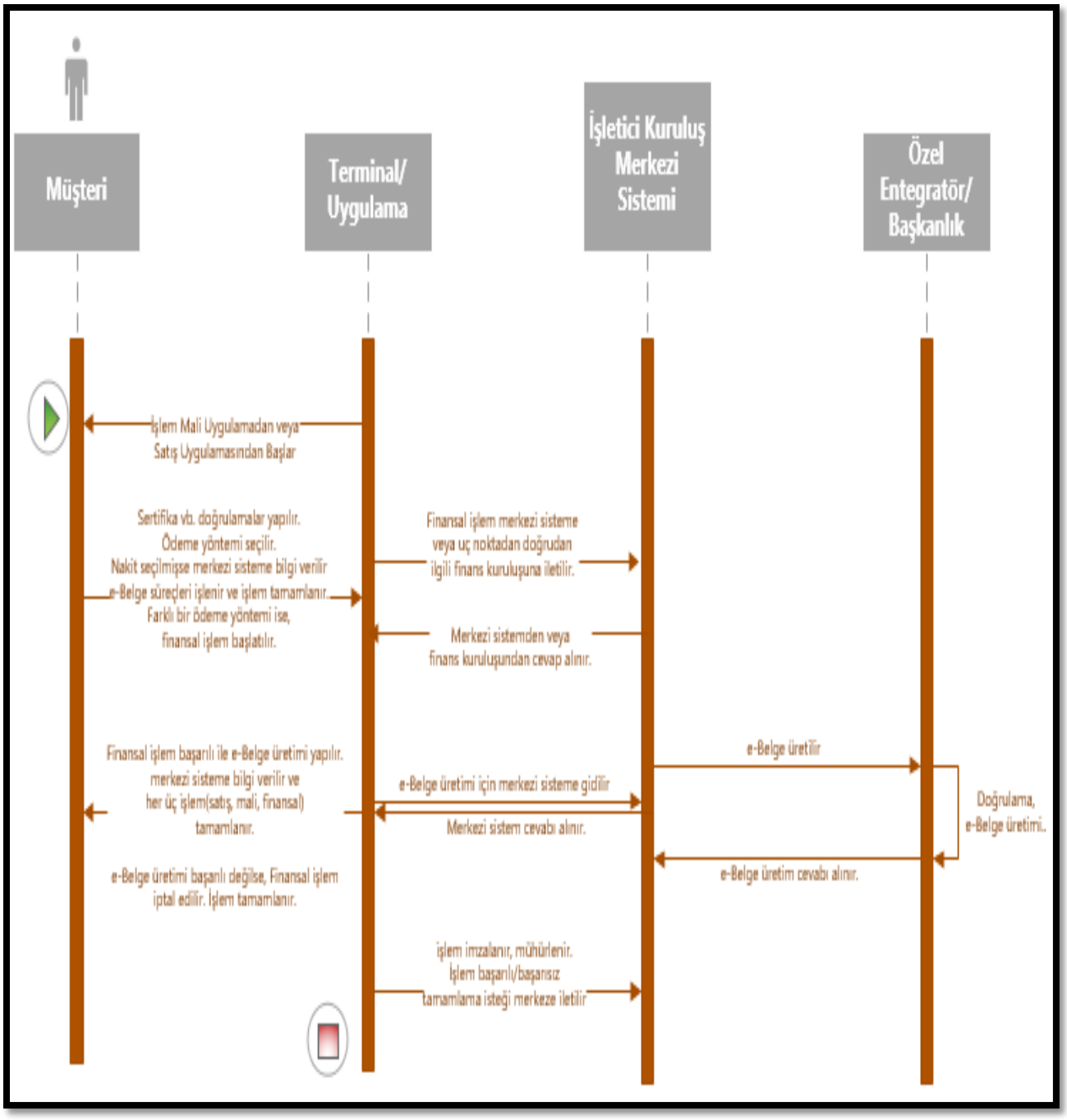
Genel İşlem Akışı:

Güvenli Mali Uygulama işlem akışları, aşağıdaki iki farklı senaryoda da yapılabilecektir. İşletici kuruluş bu senaryolardan dilediğini uygulayabilir.

Senaryo 1: Ödeme Onayından Önce **e-Belge Taslağının** Oluşturulduğu Senaryo:



Senaryo 2: Ödeme Onayından Sonra **e-Belgenin** Oluşturulduğu Senaryo:



b. e-Belge Entegrasyonu

Güvenli Mali Uygulama tarafından yapılan tüm mali ve finansal işlemlerin, belge düzenleyecek mükellefin mükellefiyet türüne uygun şekilde, İşletici Kuruluşun sorumluluğunda ve Özel Entegratör aracılığıyla anlık olarak, mevzuatta öngörülen elektronik belgelere dönüştürülmesi ve düzenlenen bu belgenin elektronik (ticari sır, müşteri sırrı, kişisel veri vb. ilgili mevzuatlarında uygunluğu belirtilen e-posta, sms, bankacılık uygulamaları vb.) veya kâğıt ortamda muhatabına iletilmesi zorunludur.

e-Belge'lerin düzenlenmesi, iletilmesi, sunulması, erişime açılması, raporlanması saklanması vb. süreçlerindeki sorumluluk, asli olarak İşletici Kuruluşta olmakla birlikte Özel

Entegratör Kuruluşların da GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır.

İşletici Kuruluş Güvenli Mali Uygulamasını Sistem kapsamında anlaşmalı olduğu Özel Entegratör kuruluş / kuruluşlar ile entegre etmek ve kesintisiz şekilde çalıştırılmasını temin etmek zorundadır. Sisteminin çevrimiçi çalışması esastır. Bir başka ifade ile Sistem kapsamında gerçekleştirilen mali ve finansal işlemlerin, Güvenli Mali Uygulama aracılığıyla tamamlanmasıyla birlikte anlık olarak Özel Entegratör kuruluşa iletilmesi ve yine anlık olarak e-Belge oluşturularak müşteriye elektronik veya kâğıt ortamda iletiminin / sunumunun gerçekleştirilmesi zorunludur. Özel Entegratör ile çevrim içi olunmayan durumlarda Güvenli Mali Uygulamanın, mali ve finansal işlemleri gerçekleştirmemesi; çevrim içi olunması ile birlikte mali ve finansal işlemler ile bunlara bağlı olarak ilgili e-Belge düzenleme işleminin gerçekleştirilmesi gerekmektedir. İşletici Kuruluş, Güvenli Mali Uygulama ile Özel Entegratör sistemleri arasındaki iletişimin ve Özel Entegratörün e-Belge servislerinin aylık %99,75 kullanılabilirlik oranı ile hizmet sunacağını taahhüt etmeli ve bunu sağlamalıdır. Her iki kurum bu taahhüdün yerine getirilebilmesi için gerekli kendi servislerini taahhüde uygun şekilde çalıştırmaktan sorumludur. İşletici Kuruluş, uçtan uca güvenli çalışma esaslarını tanımlaması, oluşturması ve taahhüt etmesi koşuluyla, sistemin çevrimdışı çalışmasına yönelik usuller hususunda da Başkanlıktan izin alabilir. Bu durumda İşletici Kuruluş, Çevrimdışı Sistem Mimarisini ve Çevrimdışı İş Akışlarını ayrı bir doküman ile Başkanlığa sunacak ve uyumluluk onayı alacaktır.

Sistem kapsamında düzenlenen e-Belgeler, ödeme türü ve detaylarına (ilgili mevzuatlarında belirtilen şekilde) ilişkin bilgileri de içermelidir. Ödeme kredi kartı/banka kartı gibi slip belgesi ile belgelendirilmesi gereken ödeme tipi ile yapılmış ise, bu ödemeye dair slipte yer alan temel ödeme bilgileri de e-Belgenin içerisinde bulunmalıdır.

Bunun yanı sıra, her e-Belge üzerinde işlemi gönderen Güvenli Mali Uygulamanın sürüm numarası da yer almak zorundadır.

İşletici Kuruluş ve bu kuruluşla birlikte çalışacak Özel Entegratör Kuruluşları, Sistem kapsamında düzenlenen e-Belgelerin (Bilgi Fişleri dâhil), değiştirilemeyecek ve silinemeyecek şekilde 507 Sıra No.lu Tebliğde öngörülen sürelerde muhafaza edilmesini taahhüt etmeli ve sağlamalıdır. Bu işlemlerin sorumluluğu, asli olarak İşletici Kuruluşta olmakla birlikte Özel Entegratör Kuruluşların da GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır.

c. Ödeme Kabul Eden Araç

Ödeme Kabul Eden Araç, bir fiziksel donanım üzerinde çalışan ve Ödeme Aracını kabul ederek ödemeyi gerçekleştirebilen yazılımsal uygulamalardır.

Sistem kapsamında, Ödeme Kabul Eden Araçların yüklenebileceği / kullanılabileceği fiziksel donanımlar aşağıdaki şekilde iki tipte olabilir:

I. **Sertifikalı Fiziki Donanımlar**: Bir Ödeme Kabul Eden Araç aracılığıyla, Ödeme Araçlarını kabul etmek ve ödeme işlemlerini, üzerinden güvenli bir şekilde gerçekleştirmek amacıyla özel olarak tasarlanmış, bu nedenle de diğer Regülasyon Otoriteleri tarafından

sertifika zorunluluğu getirilen cihazlardır. Bu cihazlara örnek olarak, PCI ve EMV sertifikaları bulunan EFT-POS cihazları gösterilebilir.

II. **Sertifikasız Fiziki Donanımlar**: Asıl kullanım amacı Ödeme Aracı kabul etmek olmayan, ancak finansal kuruluşlar tarafından sağlanan yazılımsal uygulamalar ile bu işlemleri de yapabilen, bu işlemleri yapmak için kendisine ait bir sertifikasyon gerekmeyen tablet, cep telefonu gibi cihazlardır.SoftPOS, TaptoPhone, TapOnPhone gibi isimlerle adlandırılan yazılım tabanlı yeni ödeme teknolojilerinin sertifikasız cihazlar üzerinde çalışacağı kabul edilir. Ancak bu ödeme teknolojilerin kullanımında, Diğer Regülasyon Otoriteleri tarafından belirlenen ödeme sistemleri için gerekli olan izin ve onayların alınması ve Başkanlığa bildirilmesi gerektiği açıktır.

Ödeme Kabul Eden Araç, Güvenli Mali Uygulama ile aynı **fiziki ortamda** bulunmak ve buna bağlı olarak çalışmak zorundadır. Ödeme Kabul Eden Araç, Güvenli Mali Uygulamadan bağımsız olarak ve farklı bir fiziki ortamda çalışamaz. Fiziki ortam kavramından; aynı cihaz ya da donanım kastedilmemektedir.

İşletici kuruluş, kendi sorumluluğunda olmak üzere, gerekli güvenlik önlemlerini alınması koşulu ile sahibi olduğu güvenli mali uygulamaya harici Ödeme Kabul Eden Araç bağlantısını kablolu veya kablosuz olarak dilediği protokol ile yapabilir.

İşletici Kuruluşlar, Sistem kapsamında kullanılabilecek tahsilat yöntemi (ödeme türleri) olarak sadece belli ödeme türleri ile sınırlandırarak değil bu kılavuzun "Ödeme Türleri" başlığı altında tanımlanan diğer ödeme türlerini tanımlamak zorundadır. İşletici Kuruluşların, bu kılavuzun "Ödeme Türleri" başlığı altında tanımlanan nakit dışındaki diğer ödeme türlerinde; uygulamadan yararlanan mükelleflerin ilgili ödeme türünden tahsilat yapmasına ilişkin ilgili üye işyeri anlaşması yapan kuruluşlarla gerekli üye işyeri anlaşmalarının bulunup bulunmadığını göz önünde bulundurarak, bu ödeme tipi için bir başka uygulama kullanılmak ve bu uygulama ile entegrasyon yapılmak zorunlu ise İşletici kuruluş gerekli entegrasyonu sağlamadan söz konusu ödeme/tahsilat yöntemini müşterinin kullanımına açamaz. Bir başka ifade ile İşletici Kuruluşların, bu kılavuzun "Ödeme Türleri" başlığı altında tanımlanan nakit dışındaki diğer ödeme türlerini sunabilmeleri için; sistemden yararlanan mükellefin, üye işyeri anlaşması yapan kuruluşlarla üye işyeri anlaşmasının bulunması ve ayrıca buna ilişkin Ödeme Kabul Eden Araç gerekmesi durumunda, öncelikle ilgili kuruluş ile buna ait entegrasyonun İşletici Kuruluş tarafından sağlanması gerekmektedir. Bu entegrasyon sağlanmadan bu ödeme türleri mükellefe sunulamaz. Mükellefin ilgili Ödeme Kabul Eden Aracı kullanabilmesi için ise, Üye İşyeri Anlaşmasının bulunup bulunmadığı göz önüne alınmak zorundadır.

Ayrıca, Sistemden faydalanmak isteyen ya da faydalanmaya başlayan mükellefler, belli bir Ödeme Kabul Eden Araç kullanmaya zorlanamazlar. Mükellef, sahibi olduğu sertifikalı ya da sertifikasız fiziki donanımı üzerinden kabul edeceği ödeme türlerini özgür iradesi ile seçmekte serbesttir. İşletici kuruluşlar, Sistemlerini kullanmayı talep eden ve hizmet sunumu konusunda anlaştığı mükelleflerin, mülkiyetine sahip olduğu fiziki donanımları üzerine (işletici kuruluş sisteminin çalıştırılmasına teknik bir engeli bulunmayan cihazlar olmalıdır) Güvenli Mali Uygulamalarını kurmak zorundadırlar.

Sertifikalı cihazlar üzerinden çalışan sistemi sunmak isteyen İşletici Kuruluşlar, bu iş için mükellefin sahibi olduğu EFT-POS, mPOS gibi özel bir fiziki donanım üzerinden bu işlemleri yapacağından, ilgili fiziki donanımın diğer Regülasyon Otoritelerinin uygulamaları nedeniyle, PCI Güvenlik Sertifikası ve EMV sertifikasyonlarına sahip olması zorunludur.

Sistem kapsamında gerçekleştirilen tüm ödeme / tahsilat işlemlerinin ilgili vergisel işlemle (e-Belgeyle veya mevzuata uygun düzenlenmiş Bilgi Fişi ile) eşlenme zorunluluğu, vergi güvenliği bakımından önemli ve gereklidir. Bu eşleme Güvenli Mali Uygulama aracılığıyla yapılır. İşletici Kuruluş, uçtan uca güvenlikten sorumlu olacağından, ödeme sistemleri ile yapılacak entegrasyonun yazılımsal metodunu seçmekte özgür ve bağımsızdır.

ç. Mali Raporlar

Sistemi sunan İşletici Kuruluş, sistemi üzerinden gerçekleştirilen satışlara ait verileri içeren aşağıdaki mali raporları destekleyecek yapıda bir sisteme sahip olmalı ve güvenli mali uygulama aracılığı ile bu raporları uygulamadan yararlanan mükelleflere sunabilmeli ve talep edildiğinde Gelir İdaresi Başkanlığına elektronik ortamda iletebilmelidir.

a) **Günlük Satış Raporu** (Belge Türü, Ödeme Türü, KDV oranları itibariyle Toplam Adedi, Toplam Satış Tutarı ile Toplam KDV Tutarları)

b) **Aylık Satış Raporu** (Belge Türü, Ödeme Türü, KDV oranları itibariyle Toplam Adedi, Toplam Satış Tutarı ile Toplam KDV Tutarları)

c) **İki Tarih Aralığı Satış Raporu** (Belge Türü, Ödeme Türü, KDV oranları itibariyle Toplam Adedi, Toplam Satış Tutarı ile Toplam KDV Tutarları)

ç) **Düzenlenen Belgeler Raporu** (Belgenin Türü, Tarihi, Belge No'su, Kime Düzenlendiği, Belge Toplam Tutarı (Vergi Hariç), Oranlar İtibariyle Belgedeki KDV Tutarları ve Toplamı)

d) **Bilgi Fişleri Raporu** (Günlük/Aylık/İki Tarihi Aralığı) (Bilgi Fişi Türü –Yemek Kartı Çeki / Fatura Tahsilatı / Cari Hesap Tahsilatı-, Tarihi, Belge No'su, Tutarı)

e) Başkanlıkça belirlenebilecek, mükellefler veya sektörler bazında anlık veya dönemsel verilere ait raporlar

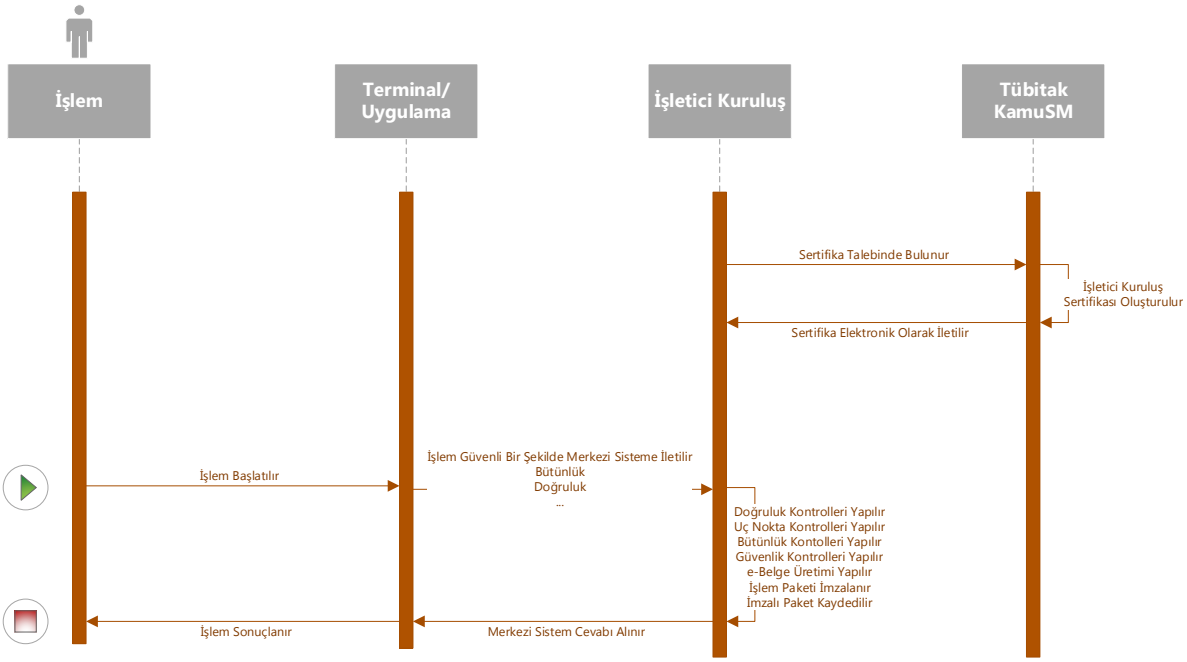
d. Güvenli Mali Sertifika ve İmza Yönetimi

İşlem, Güvenli Mali Uygulama, İşletici Kuruluş ve Sertifika Otoritesi süreçleri uçtan uca yürütülürken, içerik/kimlik doğrulaması ve bütünlük kontrollerinin yapılabilmesi için bu başlık altında detayları açıklanan Güvenli Mali Sertifika ve İmza Yönetimi tasarlanmıştır.

Sertifika ve imza kullanımı ile yapılan her bir işlem için; işleme ait bilgiler, işlemin yapıldığı uygulama, uygulamanın ait olduğu İşletici Kuruluş ve uygulamayı kullanan mükellef bilgileri ile mühürlenmiş olacaktır.

Sertifika ve imza altyapısı temel olarak; kimlik doğrulama, işlem bilgileri doğrulama, mükellef doğrulama, Güvenli Mali Uygulama doğrulama, İşletici Kuruluş doğrulama ve uygulama lisansının geçerlilik süresini denetleme amacıyla kullanılacaktır.

Genel sertifika ve imza süreç akışı aşağıdaki şekildedir:



İşletici Kuruluş yapacağı işlemleri imzalamak amacı ile kullanılmak üzere, Kamu SM 'den en fazla **3 yıl süreli** X.509 standardında bir son kullanıcı sertifikası tedarik edecektir. Bu sertifikanın ismi İşletici Kuruluş Güvenli Mali Sertifikası olarak adlandırılacaktır. İşletici Kuruluş Güvenli Mali Sertifikası içerisinde aşağıdaki veriler bulunacaktır.

İşletici Kuruluş sertifika talep dosyasını Kamu SM'ye PKSCS#10 standardında elektronik olarak gönderecektir. İşletici Kuruluş sertifika talep dosyasını oluştururken "**Subject"** alanı altına aşağıdaki değerleri set edilecektir:

- Common Name alanına, İşletici Kuruluş Adı
- Serial Number alanına, İşletici Kuruluş Vergi Kimlik Numarası

Sertifika alanlarıyla ilgili düzenlemeleri yapmaya yetkili kuruluş Kamu SM'dir.

İşletici Kuruluş Dijital İşlem İmzası:

İşletici Kuruluşlar kendi yönettikleri platformlarda, verilerin uç noktadan merkezi sistemlerine doğrulanarak, güvenli ve bütünlüğü korunarak ulaşmasından sorumludurlar. İşletici Kuruluş kendi sertifikasına(İşletici Kuruluş Güvenli Mali Sertifikası) ait özel anahtarı(private) ile yaptığı her bir işlemi kendi sunucularında imzalamak zorundadır. Bu imzanın ismi, İşletici Kuruluş Dijital İşlem İmzası olarak adlandırılacaktır. İşletici Kuruluş Dijital İşlem İmzası içeriği başkanlık tarafından belirlenecek olup, aşağıdaki veriler bulunacaktır:

- Versiyon
- İmza Algoritması
- Güvenli İmza Özet Algoritması
- İşletici Kuruluş Vergi Kimlik Numarası
- Mükellef Vergi Kimlik Numarası/TCKN
- Terminal Numarası
- Uygulama Versiyon Numarası
- Uygulama Tekil Numarası
- e-Belge Numarası
- Özel Entegratör Numarası
- Satış Sipariş Numarası (Satış Uygulamasından Alınan)
- Ödeme Provizyon Kodu (Bankacılık Kanalları İçin)
- İşlem Numarası
- İşlem Tutarı
- İşlem Zamanı
- Rasgele Sayı
- Sertifika Özet Değeri
- İmza Özet Değeri

İşletici Kuruluş tarafından yapılan her bir işlem için yukarıdaki bilgileri de ihtiva eden bir işlem paketi (xml) oluşturulacak olup, asgari XADES-BES standardı kullanılarak imzalanacaktır. İmzalama için "Enveloped" tekniği kullanılmalıdır. "Enveloping" ve "Detached" teknikleri kabul edilmeyecektir.

Gün içinde tekil bazda oluşturulan ve XADES-BES standardı ile imzalanmış bu işlem paketleri, gün sonunda yine bir pakete (xml) eklenmeli ve bu paket (tüm güne ait XADES-BES imzalı işlem paketlerini ihtiva eder) XADES-A standardı kullanılarak zaman damgalı olarak imzalanmalıdır. Böylelikle imza için kullanılan elektronik imza içerisindeki sertifikaların ve iptal bilgilerinin süreleri dolsa dahi işlemlerin içinde bulunduğu paketin imza doğrulaması yapılabilecektir.

Güvenli Mali Sertifika Temin ve Kullanım Süreci aşağıdaki şekilde yürütülür:

- İşletici Kuruluş, Başkanlıktan gerekli izni alır.
- İşletici Kuruluş, Ortak Kriterler EAL4+ Sertifikalı HSM Cihazları kullanarak anahtar çifti üretir. Bu anahtar çiftinin Private olan eşleniği HSM cihazından çıkarılamaz özellikte tanımlanmalıdır. Başkanlık veya Tübitak Kamu SM tarafından yayınlanacak formatta sertifika talep dosyası üretir ve elektronik ortamda Tübitak Kamu SM' ye iletir.

- Tübitak Kamu SM; Başkanlık tarafından İşletici Kuruluş'un izin almış olması şartı ile, İşletici Kuruluş Güvenli Mali Sertifikası'nı üretir ve İşletici Kuruluşa elektronik ortamda iletir.
- İşletici Kuruluş, Sertifikayı doğrular ve HSM Cihazlarına bu sertifikayı yükler.
- İşletici Kuruluş, merkezi sisteminde kendisine ait Private anahtar ile her bir işlemin HSM üzerinde imzalanmasını sağlar.
- Yapılan her bir işleme ait imza, İşlem Verileri ile birlikte İşletici kuruluş merkezi sisteminde saklanacaktır ve istenildiğinde Başkanlığa iletilecektir.

Sertifika ve imza yönetimi teknik olarak aşağıdaki şekilde açıklanmıştır:

KSMpub : Kamu SM otorite public anahtarı.
KSMpri : Kamu SM otorite private anahtarı.

Asimetrik Anahtar Çiftleri: Algoritma ve anahtar boyutları aşağıdaki şekilde olmalıdır:

- **RSA için;**
  - 2048 bit ve üzeri anahtar boyutu, exponent olarak 65537(0x10001) kullanılacaktır.

- **ECC için;**
  - 256 bit, NIST-secp256r1 curve
  - 384 bit, NIST-secp384r1 curve

Özet Algoritması olarak kullanılabilecek algoritmalar: SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512

İşletici Kuruluş;

- RSA kullanması durumunda, Özet algoritması olarak SHA2-256 veya SHA2-512 kullanmalıdır.
- ECC kullanması durumunda, Özet algoritması olarak;
  - ECC 256 için, SHA2-256 veya SHA3-256
  - ECC 384 için, SHA2-384 veya SHA3-384

kullanmalıdır.

İKpub : İşletici Kuruluş public anahtarı.
İKpri : İşletici Kuruluş private anahtarı.

İKcert : İşletici Kuruluş Setifikası

TXNsign: İşletici Kuruluş Güvenli Mali Uygulama İşlem İmzası

İşlem Adımları:

1. Kamu SM; otorite anahtar çiftini HSM cihazında üretecektir.
    a. **KSM**pub
    b. **KSM**pri
2. İşletici Kuruluş; kendisine ait anahtar çiftini HSM cihazında üretecektir.
    a. **İK**pub
    b. İKpri
3. İşletici Kuruluş; sertifika talep dosyasını Kamu SM ile paylaşacaktır.
4. Kamu SM; Teknik olarak, sertifika dosyasında yer alan **İK**certInput verilerini **KSM**pri ile Sign edecek(**İK**cert) ve oluşturduğu sertifikayı(**İK**cert) İşletici Kuruluş ile paylaşacaktır.
5. İşletici Kuruluş; Kamu SM'den aldığı sertifikasını(**İK**cert) kendi sisteminde tanımlayacaktır.
6. İşletici Kuruluş; **Kendi sisteminde** yapılan her bir işlemi İşletici Kuruluş'a ait **özel anahtar** ile(**İk**pri) imzalayacaktır. Teknik olarak, **TXN**singInput verilerini **İK**pri ile Sign edecek(**TXN**sign) ve oluşturduğu dijital imzalı veriyi(**TXN**sign) merkezi sisteminde kaydedecektir. (Talep edildiğinde Başkanlığa gönderilecek veri,

Böyleyece; yapılan her bir işlem için;

- İşletici Kuruluş'a ait bir Güvenli Mali Uygulama tarafından,
- İşletici Kuruluş'a ait bir terminalde,
- İşletici Kuruluş'tan hizmet alan mükellefte,
- İlgili İşlem Zamanında,
- İlgili İşlem Tutarında,
- ...
- Kamu SM' tarafından sertifikalanmış bir İşletici Kuruluş'a,

ait olduğu kayıt altına alınmış olacaktır. Bu kayıt, hem İşletici Kuruluşu hem de mükellefi korumak amaçlıdır.

Mükellefin birden fazla İşletici Kuruluş ile çalışmayı tercih ettiği durumlarda bir cihaz üzerine birden fazla Güvenli Mali Uygulama kurulabilir. Bu durumda her bir uygulamanın kendine özel ayrı bir sertifikası olması gerekmektedir.

Güvenli Mali Sertifikaların, mükellefin Sistemi kullanacağı ve aynı zamanda Güvenli Mali Uygulama ile Ödeme Kabul eden Aracın bulunacağı fiziki donanım üzerinde olması ve doğrulanması zorunluluğu vardır. Satış Uygulamasının harici ya da dâhili olması, bu zorunluluğu değiştirmez.

İşletici Kuruluş tarafından sunulan Sistem, özel bir uygulama olmadan sadece standart web tarayıcılar üzerinden (Internet Explorer, Chrome, Firefox vb.) erişilebilen bir altyapı üzerinden çalışıyor ise, oturum açma ve kimlik doğrulama koşullarını sağlaması durumda, Güvenli Mali Sertifika, Güvenli Mali Uygulama ve Ödeme Kabul Eden Aracın da kendisine ait olan Bilgi İşlem Merkezi'nde çalışacağı tabiidir. Bu durumda, söz konusu bilgi işlem merkezi

servislerinin aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde mimari tasarımının ve testlerinin yapıldığını taahhüt eder. Bu kapsamda sunulacak taahhüt ve raporlamalar asgari olarak Uptime Institute Tier 2 standartlarını sağlamalı/yerine getirmelidir. Web sunucularının Türkiye Cumhuriyeti sınırları içerisinde olması gerektiği tabidir.

Elektronik ortamda sertifikaları teslim alacak olan İşletici Kuruluşlar, söz konusu sertifikaların güvenli olarak saklanması, HSM cihazlarına yüklenmesi, gerekmesi durumunda imha edilmesi gibi işlemleri güvenli bir şekilde yapabilmek için gerekli altyapıyı kurmak zorundadır.

e. Yazılım Güvenliği

İşletici Kuruluş, sunmuş olduğu Sistem içerisinde var olan uygulamalar ve bunların güvenli mali uygulama ile entegrasyonundan sorumludur. İşletici kuruluşun sunmuş olduğu uygulamalar vasıtasıyla üretilen ve iletilen verilerin güvenliği önemlidir.

Bu kapsamda, İşletici Kuruluş sunmuş olduğu sisteme ait Güvenli Mali Uygulama, Ödeme Kabul Eden Araç ve e-Belge Entegrasyon yazılımları için;

- Güvenli şekilde yüklenme yöntemini sağlanmasından,
- Bu yazılımların arşivlenmesinden,
- Yazılım sürümü takibinden,
- Yazılım sürümünü tekil olarak ifade etmek üzere yazılım özet bilgisi değeri (HASH) oluşturmaktan ve saklamaktan,
- Yazılım sürüm güncellemesinin amacına ve yapılan değişikliklere dair bilgileri saklamaktan,
- Yazılım sürümünü onaylayan yetkili personel bilgisini saklamaktan,
- Talep edildiği anda ilgili yazılımları (*geçmiş sürümleri de dahil olmak üzere*) denetime açmak üzere güvenli bir merkezde saklamaktan sorumludurlar.

Başkanlık, gerek görmesi halinde yazılımların güncel ve geçmiş tüm sürümlerine ait kaynak kodlarını yerinde inceleyebilir.

Bu maddede sayılan şartları karşılamayan ve Sistem kapsamındaki yazılımın vergi ziyaına yol açılacak şekilde kullandırıldığı tespit edilen İşletici Kuruluşlar hakkında Vergi Usul Kanununda yer alan cezai hükümler uygulanabileceği gibi yapılan yazılı uyarıya rağmen gerekli önlemleri almayan işletici kuruluşların Bakanlıkça verilen faaliyet izinleri belli bir süreyle durdurulabileceği gibi iptal de edilebilir.

f. Erişim Kontrolü

Sisteminin temel araçları olan Güvenli Mali Uygulama, Ödeme Kabul Araç ve e-Belge Entegrasyonuna ait olan yazılımların yüklenmesini, güncellenmesini, anahtar yüklemelerini,

gerekmesi durumunda sistemin yerinde kurulumunu, bakım ve onarım gibi hizmetleri İşletici Kuruluş kendisi sağlayabileceği gibi asli sorumluluk İşletici Kuruluş'ta olmak kaydı ile Yetkili Servisleri üzerinden de sağlayabilir.

Sistem ile ilgili teknik destek vermek için sadece yetkili kişilerin erişimi olmalı ve bu kişilerin yaptığı tüm iş ve işlemlerin log kaydı tutulmalıdır. Sistemde hem mali hem de finansal işlemler söz konusu olduğu için, İşletici Kuruluşların farklı yetkilendirme tipleri ile erişim yetkileri ve alanları tanımlamaları mümkündür. Ancak bu durum, İşletici Kuruluş'un sistemin uçtan uca güvenliğine ilişkin asli sorumluluğunu ortadan kaldırmaz.

Kullanım esnasında, Sistemin ana yazılım bileşenleri olan Güvenli Mali Uygulama, Ödeme Kabul Eden Araç ve Özel Entegratör Kuruluş ile olan entegrasyon üzerinde yapılacak manipülasyonlar, tahsilat ile düzenlenen e-Belge arasındaki uyumsuzluklar, usulsüz işlemler için kullanıma uygun çalışma ortamı gibi durumlardan İşletici Kuruluş aslen sorumludur.

Sistemin üzerinde çalışacağı cihazın kendi özel işletim sistemine ait otomatik bir saat ayarı yok ise, her açılışta NTP ile saatlerinin doğruluğunu kontrol etmesi gerekir.

g. Kimlik Doğrulama

Sistemden yararlanmak isteyen mükelleflerin bilgilerinin doğruluğundan, bu bilgilerin sisteme doğru kaydedilmesinden ve Başkanlığa bildirilmesinden İşletici Kuruluşlar sorumludur.

İşletici kuruluşlar, ister sertifikalı ister sertifikasız cihazlar üzerinden çalışan sistemin lisans ve mükellef eşlemesini yaptığı cihazların, marka, model ve seri numarası kaydının tutulmasından sorumludur. Herhangi bir Uygulamanın kayıtlı olmadığı bir cihaz üzerinde Sistemin çalışmaması gerektiğinden, İşletici Kuruluş buna yönelik tedbirleri almak ve uygulamak zorundadır.

İşletici Kuruluş, bu bilgileri kaydedecek bir altyapı kurmakla yükümlüdür. Başkanlıkça talep edilmesi halinde işletici kuruluş tarafından Başkanlığa iletilmesi zorunludur.

ğ. Oturum Açma ve Oturum Kimliği Doğrulama

Tablet, cep telefonu gibi mobil Sertifikasız Cihazlar Üzerinde Çalışan Sistemlerini sunan İşletici Kuruluşlar, sistemin kusursuz ve manipülasyona yol açmayacak şekilde çalışmasından sorumludurlar.

Kötü niyetli kullanımlara engel olmak ve işlemi gerçekleştiren kişileri kayıt altına almak amacıyla, sertifikasız cihazlar üzerinde çalışacak olan Güvenli Mali Uygulamanın ilgili mükellefini kullanımına sunulduğunun doğrulanması amacıyla; mobil imza, tek kullanımlık şifre (OTP) ya da İşletici Kuruluşun belirlediği güvenli doğrulama metodu gibi güvenlik yöntemi kullanım zorunluluğu vardır. Bu sayede uygulamanın ilgili mükellefe yüklenmiş ve işlemi yapan mükellefin işlemi ilişkin rızasının olduğu kayıt altına alınmış olacaktır.

İşletici Kuruluş, sadece Web tarayıcısı üzerinden erişilebilen bir Sistem sunuyor ise, İşletici Kuruluş Sisteme giriş yöntemini kendi sorumluluğunda olmak koşuluyla serbestçe belirleyebilir. Bu durumda, bir oturum açıldıktan sonra işlem yapılmama süresi 180 saniyeyi geçemez. Bu süre dolduktan sonra oturum otomatik olarak kapatılmak zorundadır.

h. Uçtan Uca Güvenlik

İşletici Kuruluş sistemin uçtan uca güvenli şekilde çalışmasından aslen sorumludur. Bu sorumluluk kapsamında işlemlerin vergi kaybı ve kaçağına sebep vermeyecek ve güvenli şekilde yapıldığını ve sürdürüleceğini taahhüt eder.

İşletici Kuruluş, satış işlemenin başlayıp, ödemenin alınarak, mükellefiyet ve işlemin türüne uygun e-Belgenin düzenlenerek satışın sonlandırılmasından ve düzenlenen e-Belgenin Özel Entegratör Kuruluşa iletilmesine kadar geçen süreçte uçtan uca güvenli bir zincir ve iletim sistemi kurmakla mükelleftir.

İşletici kuruluş, uçtan uca kurulan bu güvenli zincir ile hassas mali verilerin kaynağının, doğruluğunun, değişmezliğinin ve bütünlüğünün kontrolünü ve bu arada bir manipülatif işlemin gerçekleştirilmemesini sağlamaktan sorumludur.

İşletici Kuruluş, uçtan uca güvenliği taahhüt ederken kullanacağı yazılımsal metotları seçmekte özgür ve bağımsızdır.

ı. Olay Kayıt Özelliği

Usulsüzlük iddiası olması durumunda gerekli kontrollerin yapılabilmesi için, bu konuda sorumluluğu bulunan İşletici Kuruluşun bazı kritik olay kayıtlarını sisteminde saklaması ve kamu otoritelerinin talep etmesi halinde de sunması zorunludur. Bu nedenle, aşağıda listelenmiş olan kritik olay kayıtları İşletici Kuruluş tarafından ilgili kanun ve tebliğlerde belirtilen süre boyunca saklanmalıdır:

a) İlgili mali işleme ait Güvenli Mali Uygulama sürüm numarası
b) İlgili mali işlem sonunda üretilen e-Belge tipi, tarih ve numarası
c) İlgili mali işlemin Özel Entegratör Kuruluşa iletim zamanı
ç) İlgili mali işlem için Özel Entegratörden dönen cevap zamanı
d) Harici uygulamalar ile entegrasyon mevcut ise bağlantının yapıldığı ve kesildiği / koptuğu zaman bilgileri
e) Mükellefin kullandığı Güvenli Mali Uygulamanın güncelleme bilgileri
f) Mükellefin kullandığı, Ödeme Kabul Aracının güncelleme bilgileri

i. PCI Güvenlik Sertifikası

Sertifikasız cihazlar üzerinde çalışan, Ödeme Kabul Araçlar kısıtlı işlem yapabilme hakları olan araçlardır. Buna mukabil tablet, cep telefonu şeklinde olabilen bu cihazların PCI Güvenlik

Sertifikası zorunluluğu yoktur. Ancak sertifikasız cihazlar üzerinde ödeme teknolojilerin kullanımında, Diğer Regülasyon Otoriteleri tarafından belirlenen ödeme sistemleri için gerekli olan izin ve onayların alınması ve Başkanlığa sunulması gerektiği açıktır.

Ticari hayatın devamını sağlamak amacıyla, ticari işletmelerin çok büyük bir kısmı için sertifikalı cihaz kullanma zorunluluğu doğacağı açıktır. Sertifikalı Cihazlar için diğer Regülasyon Otoritelerinin koymuş olduğu kurallar gereğince, PCI Güvenlik Sertifikası bir zorunluluktur.

j. EMV Sertifikaları

Sertifikalı Cihazlar üzerinden çalışan Sisteminin çalışacağı fiziki donanımların, diğer Regülasyon Otoritelerinin koymuş olduğu kurallar gereğince gerekli EMV sertifikalarına sahip olması gerekmektedir.

k. Satış Yazılımı ve Harici Satış Uygulamaları ile Entegrasyonu

Sistem, kendi bünyesinde, mal ve hizmet satışı yapan mükelleflerin satış işlemini gerçekleştiren (mal ve hizmetlerin tanımlanması, satışa başlama, müşteri seçimi, satılan mal ve hizmet seçimi, belgede yer alan tutarların hesaplaması ve işlem sonucunda e-Belge düzenlenmesi için gerekli olan bilgileri temin eden) temel bir satış uygulama yazılımını barındırmalıdır.

İster sertifikalı ister sertifikasız cihazlar üzerinden çalışan Sistem olsun, her iki tipteki sistemde de İşletici Kuruluşlar, harici satış yazılımları, perakende otomasyon yazılımları, stok ve muhasebe programları gibi uygulamalarla entegrasyon da yapabilirler.

Burada önemli olan nokta, bu entegrasyonun Güvenli Mali Uygulama aracılığıyla yapılmasının ve harici / dâhili satış uygulamaları üzerinden (satışa başlama işleminin güvenli mali uygulama tarafına yapılan başlangıç bildirimi ile tetiklendiği harici satış uygulama yazılımları üzerinden) tetiklenecek işlemlerin Güvenli Mali Uygulama aracılığıyla başlatılması ve sonlanması kuralına riayet edilmesinin zorunlu olmasıdır. Bunun dışında, sistemin uçtan uca güvenliğini taahhüt eden İşletici Kuruluş entegrasyonun hangi yazılımsal metotlarla yapılacağı konusunda özgür ve bağımsızdır. Bu tip harici uygulamalar ile yapılan entegrasyonlar sonucu gerçekleşen iş ve işlemlerden de İşletici Kuruluş aslen sorumludur.

4. Sistemin Genel Güvenlik Gereksinimleri

Güvenli ve güvenilir mali/satış/finansal işlemlerin yapılmasını sağlamak için, Hassas bilgileri korumak için, “rooted” veya “jailbroken” cihazlara ilişkin tehditleri, kötü niyetli veya yetkisiz kullanıcılardan gelen tehditleri ve aynı ortamda çalışan (ve paylaşılan kaynaklara erişimi olan) diğer uygulamalardan gelen tehditleri önlemek için, sistemde kullanılan veri ögelerinin bütünlüğünü korumak için, önleyici ve koruyucu mekanizmalar uygulanmalı/geliştirilmelidir.

Bu başlık altındaki maddeler, güvenlik gereksinimleri ile ilgili yalnızca temel prensipleri içermektedir. Bu temel prensiplere ait detaylar; Ortak Kriterler, OWASP, PCI, EMVCo vb. kuruluşlar tarafından yayınlanan standart dokümanlarında da mevcuttur. Başkanlık ve Uyumluluk Testi Yapmaya Yetkili Kuruluşlar, değişen/güncellenen güvenlik gereksinimlerine istinaden ek güvenlik testleri uygulayabilir.

Bu madde kapsamında Güvenli Mali Uygulamanın sağlaması gereken uç nokta cihaz güvenlik önlemlerinin uygulanabilirlik durumu Web tabanlı uygulamalar için test otoritesi tarafından değerlendirilecektir.

Uç noktada kullanılan cihazların güvenlik gereksinimi açısından cihaz üreticisi tarafından sağlanan güvenlik önlemleri, sertifikaları, ve/veya çözümleri de İşletici Kuruluş tarafından test otoritesine sunulabilir.

a) Bir Bütün Olarak Sistemi Korumaya Yönelik Mekanizmalar:

1. İşletici Kuruluş, uygulamalarına yönelik güvenli kullanım kılavuzu hazırlamalı ve bu kılavuzu kullanıcılarının erişimine açmalıdır.
2. Güvenli Mali Uygulama yaşam döngüsü içerisinde; geliştirme ortam güvenliği, kaynak kod güvenliği, versiyon yönetimi, değişiklik yönetimi, erişim kontrolü için gerekli prosedürler tanımlanmalı ve uygulanmalıdır.
3. Güvenli Mali Uygulama konfigürasyon yönetimi kapsamında olası uygulama hataları ve güvenlik açıklarının İşletici Kuruluşa bildirilebileceği bir arayüz (portal, e-posta adresi, vb.) sunulmalıdır. İşletici Kuruluş, bu bildirimleri değişiklik yönetimi prosedürleri kapsamında yönetir.

b) Uygulama Bütünlüğünü Korumaya Yönelik Mekanizmalar:

4. Güvenli Mali Uygulama; güvenilir bir uygulama mağazasından yüklenip yüklenmediğini kontrol eder. Bu mağaza İşletici kuruluşun kendi uygulama yönetim sistemi olabileceği gibi, Google Play, iTunes ve Microsoft App store, vb. de olabilir. Kontrollerin sonuçlarını Merkezi Sistemine iletir.
5. Güvenli Mali Uygulama; Aşağıdaki cihaz güvenlik kontrollerini yapar kontrollerin sonuçlarını Merkezi Sistemine iletir.
   - Cihaz “rooted” veya “jailbroken” yapılmış mı?
   - Uygulama emülatör, sanal makina veya simülatör ortamda çalışıyor mu?
   - Bir hata ayıklayıcı(debugger) ekli mi?
   - Uygulama kurcalaması yapılmış mı?
6. Güvenli Mali Uygulama; Çalışma zamanı bütünlüğü kontrolleri yapmalıdır. (run-time integrity checks) Fonksiyonal değişiklik tespit etmesi halinde kontrollerin sonuçlarını Merkezi Sistemine iletir.
7. Güvenli Mali Uygulama; uygulama dosyaları tersine mühendislikten korunmalıdır.

8. Güvenli Mali Uygulama; hassas ve referans olarak kullanılan verileri yetkisiz değişiklikleri önlemek için uygulama kodu içerisinde güvenli bir şekilde saklamalıdır.

c) Hassas Verileri Korumaya Yönelik Mekanizmalar:

Güvenli Mali Uygulama tarafından işlenen veriler doğası gereği oldukça hassastır ve yetkisiz erişimlerden korunmalıdır. Bu bilgiler arasında mali veriler, finansal veriler, kişisel veriler, kimlik doğrulama verileri, şifreleme anahtarları ve tüketici cihazı bilgileri vb. veriler yer alabilir.

1. Güvenli Mali Uygulama; Kişisel Veri, Tutar, Mali Veri, TCKN vb. hassas verinin alınma anı ile ilgili güvenlik önlemlerini sağlamalıdır. Bu her veri için ayrı bir hassasiyet içerebilir. (Örn: ödeme bilgisinin satış uygulaması, finansal uygulama ve mali uygulama arasındaki güvenli girdi oluşturma yöntemi)
2. Güvenli Mali Uygulama; hassas veriler kullanımı sonrasında güvenli bir şekilde silmelidir. İşlem sırasındaki izinler dışında asla uygulama belleğinde tutmamalıdır.
3. Güvenli Mali Uygulama; hassas verileri sistemin bir parçası olanlar(özel entegratör, finans kuruluşu vb.) dışında hiç bir şekilde üçüncü parti sistem ve yazılımlar ile paylaşmamalıdır.
4. Güvenli Mali Uygulama; hassas verileri kaynak koduna gömemez.
5. Güvenli Mali Uygulama; diğer uygulama ve kullanıcıların erişimini engellemek amacıyla çalışma zamanı veri koruması (run-time data protection) yapmalıdır.
6. Güvenli Mali Uygulama tarafından oluşturulan (hem native/yerel hem de web/HTML modlarında) kullanıcı arayüzü (UI), hassas bilgilere güvenli mali uygulama dışındaki yetkisiz kişi, işlem ve uygulamaların erişilemeyeceği şekilde izolasyon sağlar ve verileri güvence altına alır. (UI Protection)
7. Güvenli Mali Uygulama, Web tabanlı bir arayüze sahipse, HTML üzerinden yapılan tüm yetkisiz ve harici URL isteklerini durdurmalıdır. Bu isteklerin işletim sistemine veya internete iletilmesini engellemelidir.
8. Güvenli Mali Uygulama, Web tabanlı bir arayüze sahipse, kendisine ait olmayan herhangi bir JavaScript kodunun başka bir kişi/uygulama/işlem tarafından enjeksiyonunu ve yürütülmesini önlemelidir.

ç) Şifreleme Mekanizmaları:

Temel güvenlik gereksinimi olarak, kriptografik algoritmaların ve uygun anahtar yönetim tekniklerinin doğru şekilde uygulanması gereklidir. Bu uygulama, bilgilerin bütünlüğünü ve gizliliğini sağlamak için kritik öneme sahiptir. Yalnızca onaylı ve doğruluğu kanıtlanmış ve başkanlık tarafından tanınan algoritmalar ve anahtar yönetimi teknikleri kullanılmalıdır. Özel algoritmalar kullanılmamalıdır.

1. Yalnızca onaylı ve doğruluğu kanıtlanmış ve başkanlık tarafından tanınan algoritmalar kullanılmalıdır. Örneğin: Tübitak, NIST, ANSI, ISO, EMVCo, vb.

2. Güvenli Mali Uygulama tarafından kullanılan tüm rastgele sayılar, yalnızca onaylı (Tübitak, Ortak Kriterler, NIST vb.) rastgele sayı üretme (RNG) algoritmaları veya kütüphaneleri kullanılarak üretilmelidir.
3. Merkezi Sistemde Seritifka yönetimine ilişkin işlemler için ve veritabanında saklanan hassas veriler için donanımsal şifreleme yöntemleri kullanılmalıdır. Bunun için Ortak Kriterler EAL4+ Sertifikalı HSM cihazları kullanılmalıdır.
4. Tüm simetrik ve asimetrik kök/ana anahtarlar Doğrudan İşletici Kuruluşu temsil ettiği için güvenli bir şekilde HSM cihazları içerisinde saklanmalıdır.
5. Uç nokta yazılımlarında şifreleme ve anahtar yönetimi için SAM, Secure Element vb. donanımsal güvenlik ortamları varsa bu alanlar kullanılabilir. Mobil Telefon, tablet, PC vb. uç noktalar için donanımsal bir güvenlik ortamı yoksa yazılımsal kütüphane ve ortamlar ile belirtilen tüm güvenlik adımları sağlanmalıdır.

d) Güvenli İletişim Mekanizmaları:

1. Güvenli Mali Uygulamaya ait tüm bileşenler güvenli iletişim kanalları üzerinden haberleşmelidir.
2. Güvenli Mali Uygulama uç nokta yazılımları ve merkezi sistemi haberleşirken tcp, ssl, tls vb protokollerin içinde akan veriler için şifreli olarak özel bir kanal oluşturmalıdır ve bu kanal içerisinden giden/gelen veriler özel anahtarlarla şifrelenmelidir.
3. Güvenli Mali Uygulama ve özel entegratör sistemleri merkezi sistemleri üzerinden iletişim kurmalıdır. Bu sayede, merkezi sistemler arasında IP tanımı yapılmalı ve güvenli bir kanal üzerinden veri iletişimi sağlanmalıdır. (Host-To-Host)
4. Harici satış uygulamaları ile entegrasyon uç nokta üzerinde veya merkezi sistemler arasında olabilir. Verinin uygulamalar arasında şifreli aktarılması ve güvenli kanal oluşturulması gerekmektedir.

e) Uç Nokta Güvenliği:

1. Sisteme ait uç nokta güvenliği ile ilgili; gerekli dokümanlar ve akış diagramları Başkanlığa ve test otoritesine sunulmalıdır.
2. Sistem bir bütün olarak; uç noktada çalışan (web tabanlı olsun veya olmasın) her bir uygulama için, uygulamanın çalıştığı ortama ait fingerprint verilerini kullanarak, mali uygulamanın uç noktada güvenli bir şekilde çalışmasını ve uç nokta doğrulamasını sağlayabiliyor olmalıdır.
3. Uç nokta ile merkezi sistemin SSL iletişiminde en az TLS 1.2 vb. güvenlik seviyesindeki mekanizmalar kullanılmalıdır.
4. Uç nokta ile merkezi sistemin iletişiminde TLS 1.2 vb. iletişim mekanizmaları içerisinde akan verinin şifrelenmesi için işleme özel türetilmiş minimum 128 bit ve üzeri AES bir anahtar kullanılmalıdır.
5. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalar bir veri tutuyorsa, bu verilerin saklanmasında anahtar kullanılmalıdır.

6. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda; kullanıcı adı, şifre, anahtar, kişisel veriler, mali veriler vb. hassas bilgiler saklanıyorsa veya işleniyorsa bu veriler güvenli bir şekilde saklanmalıdır/korunmalıdır.
7. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Root Detection yapılmalıdır. (Uygulamanın rootlanmış cihazlarda çalışması engellenmelidir.)
8. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Device Identification yapılmalıdır. (uygulama kurulduğu cihazı tanımlayabilecek veriler sağlamalıdır)
9. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Geolocation yapılmalıdır. (Başarılı kurulmuş bir uygulama gibi davranıp farklı lokasyondan işlem yapmasına müsade etmemeli)
10. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Device Binding yapılmalıdır. (Uygulaması ile kurulduğu cihazı birbirine bağlayan eşsiz bir imza üretmeli ve yapılan bir işlemin ilgili cihaza kurulu uygulamadan gerçekleştirildiğini garanti etmelidir)
11. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Yazılımsal veya Donanımsal Güvenli Alan/Cryptography Storage/Secure Storage yapılmalıdır. Uygulama üzerinde saklanması gereken hassas verileri güvenli şifreleme algoritmaları ile şifreli ve sadece uygulamanın güvenli bir şekilde okuyabileceği ve başka hiç şekilde ulaşılamayan bir alt yapı ile saklar) (Uygulama güvenli sanal veri deposu alanı oluşturabilecek, uygulamaya ait gizli özel anahtarı ve sertifikayı (X509) burada saklayacaktır. Uygulama, uygulamaya ait özel anahtarı güvenlik sunucusu ile ilişkilendirecek, hiçbir şekilde açık olarak veya çevrim dışı şifreleme yöntemler ile cihaz üzerinde depolamayacaktır.)
12. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Secure Channel kurulmalıdır. (Uygulamanın sunucu ile olan iletişimini gizlilik ve bütünlük açısından gerekli asimetrik ve simetrik şifreleme algoritmaları ile koruyacağı güvenli bir kanal üzerinden sağlar)
13. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Anti-Debugging yapılmalıdır. (uygulamasının herhangi bir debugger ile analiz edilmesini engellemelidir)
14. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect Emulator yapılmalıdır. (uygulamasının herhangi bir emulator üzerinde çalışmasını engellemelidir)
15. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect-Hooking yapılmalıdır. (uygulamasına ait fonksiyonlarının harici bir fonksiyonla çalışma zamanında değiştirilmesini engeller)
16. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect Repackaging yapılmalıdır. (uygulamasının kodlarınının çözülüp tekrar paketlenmesini tespit edip çalışmasını engeller)
17. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Secure RunTime Memory yapılmalıdır. (uygulamasının çalışma zamanında kullandığı hafıza alanından hassas verilerin alınmasını engelleyecek şifreleme, karıştırma ve diğer sisteme bağlı tedbirleri içerir)

18. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Runtime CRC Check yapılmalıdır. (Uygulama, uygulama çalışma zamanında yüklenen uygulama kodunun değişmesini kontrol edip çalışmasını durduracak ve bu durumu uzak sunucuya raporlayacaktır)
19. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, gerekli durumlarda ve cihaz izin veriyorsa Soft OTP yapılmalıdır. (uygulama ihtiyaç duyduğu işlemlerde Soft OTP doğrulamasını yapabilmelidir)
20. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, gerekli durumlarda ve cihaz izin veriyorsa Push Notification yapılmalıdır. (uygulama ihtiyaç duyduğu işlemlerde Push Notification doğrulaması yapabilmelidir)
21. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Application-binding yapılmalıdır. (Uygulama içerisindeki fonksiyonlar dışarıdan izinsiz bir şekilde tetiklenmemelidir. Fonksiyonlar kendi uygulamasının dışında bir uygulama ile çalışmamalıdır.)
22. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Code Obfuscation and Diversification / Code Lifting yapılmalıdır.(Uygulama kodları tersine mühendislik ve statik kod analizleri ile açığa çıkmamalıdır)
23. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, SSL-pining yapılmalıdır. (Uygulamasının sunucu ile olan iletişiminde kendi özel sertifikalarını kullanacak ve bunların güvenliğini ve bütünlüğünü garanti edecektir. Uygulama, kendi şifreli sertifika deposunu kullanacak, işletim sistemine ait sertifika deposunu kullanmayacak ve tanımlı kök sertifika otoritelerine güvenmeyecektir)
24. Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Transaction Data Signing yapılmalıdır. (Uygulama, işlemlerin takibi için dijital olarak her işlemi imzalayacak ve bu imzayı sunucuda saklayacaktır)

f) Genel Gereksinimler:

1. İşlemler; satış, ödeme, e-Belge oluşturma süreçleri bütüncül olarak yönetilmelidir.
   - Satış İşlemleri (Satışın başarılı olabilmesi için her üç işlemin de başarılı olduğu)
   - İptal İşlemleri (İptal işleminin her üç işlem için de ortak yapıldığı; satış iptal, ödeme iptal, e-Belge iptal.)
   - İade İşlemleri (İade işleminin her üç işlem için de ortak yapıldığı; satış iade, ödeme iade, e-Belge iptal.)
2. Veri bütünlüğü uç noktadan merkezi sisteme, oradan da 3rd servislere kadar, uçtan uca ve güvenli bir şekilde sağlanmalıdır. (Uç noktadaki verilerin, (örneğin tutar verisi) merkezi sistemde ve verinin aktığı her yerde aynı değerde olması kontrolü sağlanmalıdır.)
3. TCKN, email, telefon numarası, adres, kart numarası gibi hassas veriler saklandığı noktalarda anahtar kullanılarak şifreli bir şekilde güvenli ortamlarda saklanmalıdır.
4. TCKN, email, telefon numarası, adres, kart numarası gibi hassas verilerin yetki bazlı olarak erişilebildiği, erişen sistem kullanıcının iz takibinin yapılabildiği bir altyapı kurgulanmalıdır.

5. TCKN, email, telefon numarası, adres, kart numarası gibi hassas verilerin raporlara veya yetki bazlı olmayan erişimlere açık değer olarak değil, maskeli olarak veya özet/hash değerleri ile yansıtılması sağlanmalıdır.
6. Sisteme ait Sertifika Yönetimi ile ilgili; gerekli dokümanlar ve akış diagramları sunulmalıdır.
7. Sertifikasyon sürecinde kullanılmak üzere, İşletici Kuruluşa ait anahtarlar güvenli olarak oluşturulmalıdır.
8. GİB'in belirlediği sertifika otoritesine gönderilmek üzere sertifika talebi güvenli bir şekilde yapılabilmelidir.
9. GİB'in belirlediği sertifika otoritesinden gelen sertifika sisteme güvenli bir şekilde yüklenebilmelidir.
10. Sistem bir bütün olarak; uç noktada çalışan (web tabanlı olsun veya olmasın) her bir uygulama için sertifika üretebilmelidir.
11. Sistem bir bütün olarak; uç noktada çalışan (web tabanlı olsun veya olmasın) her bir uygulama için ürettiği sertifikaları, GİB'in belirlediği sertifika otoritesinden aldığı sertifikadan türetebilmelidir.
12. "Sistem bir bütün olarak; uç noktada çalışan (web tabanlı olsun veya olmasın) her bir uygulama için ürettiği sertifika içeriği Bu kılavuzda geçen zorunlu verileri kapsamaldır.
13. Üretilen tüm sertifikalar kılavuzda belirtilen formatlar ile uyumlu olmalıdır.
14. Sistem ve güvenli mali uygulama, sertifikalar için sertifika geçerlilik süresi kontrolü yapmalıdır.
15. Sistemin kurulu olduğu merkezde tüm anahtar yönetimi ve şifreleme işlemleri için HSM cihazları kullanılmalıdır.
16. Kullanılan HSM cihazları Ortak Kriterler EAL4+ veya üzeri sertifikaya sahip olmalıdır.

5. Mülkiyet

Mükelleflerin Sistem kapsamında kullanacakları **fiziki donanımın mülkiyeti**, cihazların üzerinde çalışabilecek Ödeme Kabul Eden Araç da dâhil her türlü uygulamanın mükellefler tarafından serbestçe belirlenebilmesi bakımından (İşletici Kuruluşlar, bankalar ya da ödeme kuruluşları tarafından talep edilen ücret, komisyon vb. gibi ücretlerin değişkenliği ve rekabet koşulları içinde istenilen uygulamaların seçiminin serbestçe yapılabilmesi bakımından) uygulama kapsamına dâhil olan mükelleflere ait olması esastır. Bununla birlikte, kullanılacak fiziki donanımda diğer İşletici Kuruluşların Sistemlerine ilişkin uygulamalarının çalıştırılmasına işletici kuruluşlar arasında cihazın ortak kullanımına ilişkin ticari anlaşmanın yapılmış olması ve herhangi bir engel konulmaması şartıyla, söz konusu cihazların mülkiyeti İşletici Kuruluşa ait olarak mükellefe bedeli mukabilinde ya da bedelsiz olarak kullandırılması da mümkündür.

Güvenli Mali Uygulamanın mülkiyeti İşletici Kuruluşlarda olacaktır. İşletici Kuruluş ile mükellef arasındaki hizmet ilişkisinin sona ermesi durumunda, cihaz üzerindeki Güvenli Mali Uygulamanın İşletici Kuruluş tarafından kullanıma kapatılması gerekmektedir.

Sistemden faydalanmak isteyen mükellefler, bir cihaza ve / veya İşletici Kuruluşa bağımlı olmadan ticari birlikteliklerini ve iş ortaklıklarını kendi özgür iradeleri ile belirleyebilmesi bakımından uygulama kapsamında kullanacağı fiziki donanımın mülkiyetine sahip olması ya da mülkiyeti İşletici Kuruluşta bulunsa dahi fiziki donanım üzerinde İşletici Kuruluş tarafından diğer İşletici Kuruluşların uygulamalarının çalıştırılabilmesine işletici kuruluşlar arasında cihazın ortak kullanımına ilişkin ticari anlaşmanın yapılmış olması halinde her hangi bir engel konulmamış olması gereklidir.

Mükelleflerin özgür iradelerini kısıtlayıcı, pazarlık gücünü düşürücü ve cihaz bağımlılığı üzerinden zorunlu ticari birlikteliğe yol açmaya dayalı iş modeli 507 Sıra No'lu Vergi Usul Kanunu Genel Tebliğinin özüne ve amacına aykırıdır. Bu nedenle mükellefleri cihaz bağımlılığı üzerinden zorunlu ticari birlikteliğe zorunlu kılmamak üzere, ister sertifikalı ister sertifikasız olsun Sisteminin üzerinde çalıştığı tüm fiziki donanımların mülkiyeti mükelleflerin kendisine ait olmalı ya da fiziki donanım üzerinde diğer İşletici Kuruluşların uygulamalarının da çalıştırılabilmesine yönelik her hangi bir engel konulmamış olması işletici kuruluşlar arasında cihazın ortak kullanımına ilişkin ticari anlaşmanın yapılmış olması halinde zorunludur.

Ayrıca mükellefler, İşletici Kuruluşlar tarafından bir Ödeme Kabul Eden Araç entegrasyonu yapmaya zorlanamazlar. Mükellefler, nakit ya da Ödeme Kabul Eden Araç dışında kalan diğer yöntemlerle tahsilat yapabilir, mülkiyeti kendisinde olan sertifikalı ya da sertifikasız cihazından Ödeme Kabul Eden Araç uygulaması ve / veya buna yönelik entegrasyonun kaldırılmasını talep edebilirler.

6. Sistem Üzerinden Düzenlenebilecek e-Belgeler

Sistem kapsamında düzenlenecek olan e-Belgelerin veri girişi, işletici kuruluş tarafından sunulan Güvenli Mali Uygulama üzerinden ya da İşletici kuruluş sorumluluğunda Güvenli Mali Uygulama ile entegrasyonu yapılmış harici satış uygulama yazılımları ile birlikte Güvenli Mali Uygulama aracılığıyla yapılabilir. İşletici Kuruluşlar, sistem kapsamında hizmet sunacakları mükelleflerin mükellefiyet türüne uygun olarak mevzuatta öngörülen ilgili e-Belgeleri desteklemek zorundadır. Bu sorumluluk Asli olarak işletici kuruluşa ait olmakla birlikte Özel Entegratör kuruluşların da e-Belge ile ilgili süreçlere ilişkin GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır.

Güvenli Mali Uygulama üzerinden ya da Güvenli Mali Uygulama ile entegrasyonu ile düzenlenecek olan e-Belgelerin, e-Belge uygulamalarına ilişkin olarak ilgili mevzuatlarında (Kanun, Genel Tebliğ ve Teknik Kılavuzlarda) belirtilen şekil şartlarına uyması zorunludur. İlgili mevzuatlarında belirtilen ve e-Belgelerde yer alması zorunlu tutulan bilgilerin, e-Belgenin düzenlenebilmesi için Özel Entegratör Kuruluşa güvenli bir şekilde iletilmesi ve e-Belgenin doğru içerikle oluşturulması sorumluluğu asli olarak işletici kuruluşa ait olmakla birlikte Özel Entegratör kuruluşların da e-Belge ile ilgili süreçlere ilişkin GİB'e karşı İşletici Kuruluşla birlikte müşterek ve müteselsil sorumluluğu da bulunmaktadır.

e-Belgelerde bulunması gereken bilgilerin hiç ya da gerektiği gibi Sistem tarafından Özel Entegratör kuruluşlara iletilmemesi, uygulamayı kullanan mükelleflerin kusurundan kaynaklanmaması ve işletici kuruluş veya Özel Entegratör kuruluşun gerekli önlemleri almamasından kaynaklaması halinde, işletici kuruluşların ve Özel Entegratör Kuruluşların Bakanlıkça veya Başkanlıkça verilen faaliyet izinleri, Başkanlıkça yapılan değerlendirme ve kontroller çerçevesinde belli bir süreyle durdurulabileceği gibi iptal de edilebilir.

Sistemin, vergiden muaf esnaflara kullandırılması durumunda, gerçekleştirilen satış işlemi için vergiden muaf esnafın, belge düzenleme zorunluluğu bulunmadığından, satış işlemine ait bilgilerin (Satışı gerçekleştiren vergiden muaf esnafın bilgileri, satışa konu mal veya hizmetin bilgileri, tutarları) yer alacığı ve mali değeri bulunmayan, bilgi amaçlı "Bilgi Fişi" düzenlenmesi gerekecek olup, Güvenli mali uygulamanın bunu sağlaması gerekmektedir.

Ayrıca, ticari kazancı basit usulde tespit edilen gelir vergisi mükelleflerin ve gerçek usulde vergiye tabi olmayan çiftçilerin de gerçekleştirdikleri mal teslimleri ile hizmet ifaları KDV den istisna olduğundan, bu durumdaki mükelleflerce tanzim olunacak fatura, müstahsil makbuzu belgelerde KDV tutarının yer almamasının sağlanması gerekmektedir.

Ayrıca Sistem kapsamında düzenlenecek e-belgelerde; malın ve/veya işin nev'i genel ve soyut isimlerle (yiyecek, içecek, giyecek, gıda, meyve, temizlik malzemesi, ilaç gibi) tanımlanmaması ve satışı gerçekleştirilen mal veya hizmetin özel ve somut adıyla tanımlanması esas olmakla birlikte, 509 Sıra No.lu Vergi Usul Kanunu Genel Tebliği'nde 515 Sıra No.lu Vergi Usul Kanunu Genel Tebliği ile yapılan değişiklik uyarınca; vergiler dahil toplam satış tutarı 500 TL'ye kadar olan perakende mal ve hizmet satışlarına ait düzenlenen e-Arşiv Faturalarda "müşterinin adı, ticaret unvanı, adresi, vergi dairesi ve hesap numarası" bilgileri yerine, müşterinin adı bölümünde "NİHAİ TÜKETİCİ" açıklamasına yer verilerek düzenlenmesine imkanı Sistem kapsamından yararlanan mükellefler için de verilmiş ve bu şekilde düzenlenen e-Arşiv Faturaların **perakende satış fişi** veya **ÖKC fişi** olarak kabul edileceği belirtilmiştir. Mezkûr düzenlemede ayrıca bu kapsamda düzenlenecek e-Arşiv Faturaların düzenlenmesinde uyulacak usul ve esaslar ile e-Arşiv Faturanın şekli, formatı, içeriği ve uygulamaya yönelik diğer hususlarını ebelge.gib.gov.tr adresinde yayımlanacak kılavuzlarla Başkanlığın belirlemeye yetkili olduğu hüküm altına alınmıştır.

Yapılan bu düzenlemeyle Başkanlığımıza verilen yetki çerçevesinde; Sistemden yararlanan mükelleflerce, Sistem kapsamında vergiler dahil toplam tutarı 500 TL ye kadar olan düzenlenecek e-Arşiv Faturalarda, alıcının (müşterinin) adı-soyadı, ünvanı, adresi, vergi dairesi ve vergi kimlik numarası veya TCKN bilgisine yer verilme zorunluluğu olmadan müşterinin adı bölümünde "Nihai Tüketici" açıklamasına yer verilmesi ve bu belgelerin mal ve hizmetlerin nev'i (cinsi) bilgisi alanında; mal ve hizmetlerin ait olduğu **KDV oranlarına göre gruplandırarak genel ifadelere** (Yiyecek, İçecek, Ekmek, Temizlik Malzemesi, Temel Gıda, Muhtelif Gıda, vb.) yer verilmek suretiyle düzenlenmesi mümkün bulunmaktadır. İşletici kuruluş tarafından sunulan sistemin bu gereksinimleri sağlaması gerekmektedir. İşletici kuruluşun sunacağı sisteme mükellef kendi ürün/mal/iş listesini ekleyebileceği gibi KDV departmanları ve genel mal/hizmet ifadelerini de ekleyebilmeli ya da harici satış uygulamaları

üzerinden de bu bilgiler sisteme aktarılabilmelidir. Malın ve/veya hizmetin (işin) nev'inin doğru şekilde tanımlanması ve belge üretiminde kullanılması sorumluluğu satış uygulamasını kullanan mükellefe aittir.

Bu çerçevede uygulamayı kullanacak mükelleflerin vergi mükellefiyet durumlarına uygun şekilde Belge düzeninin sağlanmasına yönelik olarak Güvenli Mali Uygulamanın oluşturulması ve sunulması sorumluluğu işletici kuruluşlara aittir.

7. Ödeme Türleri

İşletici Kuruluşlar tarafından sunulan Sistemde, tüm mali ve finansal işlemlerin Güvenli Mali Uygulama üzerinden (veya Güvenli Mali Uygulama ile entegrasyonu İşletici Kuruluş sorumluluğunda gerçekleştirilmiş harici satış uygulama yazılımları üzerinden) başlaması ve Güvenli Mali Uygulama üzerinden / aracılığıyla sonlandırılması esastır. Mali işlemin sonlanması, satışa ait oluşacak e-Belgedeki bedelin hangi ödeme türü ile gerçekleştirileceğinin seçilmesi ile devam etmeli ve bu ödeme türüne göre işlemler sonlandırılarak e-Belge oluşturulmalıdır.

Güvenli Mali Uygulamaların aşağıdaki ödeme türlerinin tamamı tanımlı olmalıdır. Ancak, söz konusu ödeme türlerinden, mükellefin ilgili finansal kuruluşlarla bir üye işyeri anlaşması olmaması nedeniyle kullanılması mümkün olmayanların aktif edilmemesi, üye işyeri anlaşması gerçekleştiğinde ise aktif edilmesi sorumluluğu işletici kuruluşa aittir.

a) **Nakit:** Para ile gerçekleştirilen ödemelerdir.

b) **Banka / Kredi Kartı:** Banka vb. kuruluşlara ait; ön ödemeli, banka veya kredi kartları ile gerçekleştirilen ödemelerdir. Fiziki, sanal veya dijital ortamdan oluşturulmuş kartlar (NFC/HCE/QR vb.) ile yapılan tahsilatlar bu gruptadır.

c) **Diğer:**

1) Senet/Çek/Açık Hesap/Kredili: Çek, senet teslimi veya açık hesap/kredili (vadeli) olarak gerçekleştirilen satışlarda kullanılan ödeme türüdür.

2) Havale/EFT: Banka hesapları arasında havale veya EFT işlemi ile gerçekleştirilen ödemelerdir.

3) Hediye Kartı: Hediye kartları ile gerçekleştirilen satışlarda kullanılan ödeme türüdür. İndirim çekleri de bu gruptandır.

4) Belediye Ulaşım Kartları, Yardım Kartları ve Çekleri: 5393 sayılı Belediye Kanununa uygun olarak; Belediyeler tarafından ihraç edilen ulaşım kartları veya ihtiyaç sahiplerine verilmiş olan yardım kartları ve çekleri ile gerçekleştirilen satışlarda kullanılan ödeme türüdür.

5) Yemek Kartı ve Çekleri: Yemek Kartı ve çekleri ile gerçekleştirilen satışlar için kullanılacak ödeme türüdür. Yemek kartı ve çekleri ile yapılan ödemeler için mali değeri bulunmayan bilgi fişi düzenlenecektir. YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARDAN "BİLGİ FİŞLERİ" DÜZENLENMESİNE

DAİR USUL VE ESASLARA İLİŞKİN TEKNİK KILAVUZ'un 9.2 bölümünde yer verilen açıklamalar ve ilgili bölümde belirtilen bilgi fişi belge örnekleri dikkate alınacaktır. Bu husus, bilgi fişinin düzenlenmesinde yeni nesil ödeme kaydedici cihazın kullanılması ve ÖKC ile özgülenen bilgilerin (Z No, EKÜ No, Fiş No, YN ÖKC Seri No) belge üzerinde yer verilmesi zorunluluğunu getirmemektedir.

6) Finansal kuruluşlar tarafından sunulan/sunulabilecek diğer ödeme yöntemleri.

İşletici Kuruluş, her bir ödeme/tahsilat işleminde düzenlenecek olan ilgili e-Belgenin hangi ödeme türü ile işlem gördüğünü Özel Entegratör Kuruluşa bildirmek ve mali verilerin doğruluğunu sağlamak zorundadır. Sistem, mali bir işlem ile eşleşmeyen hiçbir ödeme / tahsilatın yapılmasına müsaade etmemelidir.

8. Avans Ödeme ve Cari Hesap Tahsilatı İşlemleri

Ticari hayatın doğal akışı içerisinde yer alan mal ve hizmetlerin satışının gerçekleştirilmesinden önce ön ödeme (Avans, depozito, kaparo) Tahsilatı ve Cari Hesap Tahsilatı (Müşteriye önceden teslim edilmiş bir mal veya sunulmuş hizmet karşılığında ödemeleri alınmamış ve karşılığı 213 sayılı Vergi Usul Kanunu uyarınca düzenlenmiş resmi evraklar ile tevsik edilebilen alacakların ödeme / tahsilat işlemleri), Sistemi kapsamında Güvenli Mali Uygulama içeriğinde olmak üzere işletici kuruluşlar tarafından sunulabilir.

Avans ve Cari Hesap Tahsilatlarına ilişkin, Sistem kapsamında düzenlenecek belgelerin format ve içeriği ile uygulama usulü hakkında YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARDAN "BİLGİ FİŞLERİ" DÜZENLENMESİNE DAİR USUL VE ESASLARA İLİŞKİN TEKNİK KILAVUZ'un 9.3 ve 9.6 bölümlerinde yer verilen açıklamalar ve bu bölümlerde yer verilen bilgi fişi belge örnekleri dikkate alınacaktır. Bu husus, bilgi fişinin düzenlenmesinde yeni nesil ödeme kaydedici cihazın kullanılması ve ÖKC ile özgülenen bilgilerin (Z No, EKÜ No, Fiş No, YN ÖKC Seri No) belge üzerinde yer verilmesi zorunluluğunu getirmemektedir.

Bu bilgi fişlerinin Güvenli Mali Uygulama üzerinden düzenlenmesi ve bu belgelerin de e-Belge olarak düzenlenmek amacıyla Özel Entegratör Kuruluşa iletilmesi ve bunlar tarafından muhafaza edilmesi, Başkanlık tarafından talep edildiğinde Başkanlığa elektronik ortamda raporlanması gerekmektedir.

9. Fatura Tahsilatı İşlemleri

6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunun 12 nci maddesinin (1) numaralı fıkrasının (e)

bendi uyarınca fatura ödemelerine aracılık edilmesine yönelik hizmetleri yerine getirme amacıyla faaliyet gösteren kuruluşlar ile bu kuruluşların resmi temsilcileri, fatura tahsilat işlemlerini bu kılavuzda belirtilen Sistem aracılığıyla da gerçekleştirebilir.

Sistem kapsamında gerçekleştirilen Fatura Tahsilatı İşlemlerinde;

Gerçekleştirilen fatura tahsilat işlemi sonucunda müşteriden ek bir ücret / komisyon alınmıyor ise, bu durumda YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARDAN "BİLGİ FİŞLERİ" DÜZENLENMESİNE DAİR USUL VE ESASLARA İLİŞKİN TEKNİK KILAVUZ'un 9.5. bölümünde yer alan açıklamalar dikkate alınacak ve söz konusu kılavuzun 7 numaralı ekinde yer verilen format ve içerikteki bilgi fişinin e-Belge olarak düzenlenmesi zorunludur. Bu husus, bilgi fişinin düzenlenmesinde yeni nesil ödeme kaydedici cihazın kullanılması ve ÖKC ile özgülenen bilgilerin (Z No, EKÜ No, Fiş No, YN ÖKC Seri No) belge üzerinde yer verilmesi zorunluluğunu getirmemektedir.

Müşteriden ilave bir ücret / komisyon alınmadan yapılan fatura tahsilat işlemlerine ait olmak üzere, faturası tahsil edilen kurum veya kuruluşlardan daha sonra ücret, komisyon, ciro primi vb. adlar altında tahakkuk eden alacaklar için ise genel esaslar çerçevesinde KDV'li faturanın, faturası tahsil edilen kuruma kesilmesi gerektiği açıktır.

Gerçekleştirilen fatura tahsilat işlemi sonucunda müşteriden ek bir ücret / komisyon alınıyor ise, bu durumda alınan komisyon tutarında faturanın e-Belge olarak düzenlenmesi zorunludur.

İlgili kuruluş ve temsilcilerinin, fatura tahsilat işlemlerinde işbu kılavuzda tanımlanan Sistemi tercih etmeyerek, YNÖKC kullanması ve tahsilatların banka / kredi kartı ile yapılması durumunda, tahsilatın yapıldığı pos cihazının ÖKC ya da YNÖKC ile entegre ve bağlantılı bir yapıda (*satış işleminin ÖKC'den başlatılıp, tahsil edilecek tutarın EFT-POS cihazına ÖKC'den otomatik olarak gönderilmesi ve satış işleminin ÖKC'den sonlandırılması*) ve ÖKC'den bütünleşik fişi YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARDAN "BİLGİ FİŞLERİ" DÜZENLENMESİNE DAİR USUL VE ESASLARA İLİŞKİN TEKNİK KILAVUZ'unda belirtilen şekilde düzenlemeleri zorunludur.

10. İşletici Kuruluş İzin Başvurusu, Uyumluluk Testleri Denetimi ve İznin Verilmesi

507 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinin Tanımlar bölümünde yer verilen "Finansal Kuruluş" ya da "ÖKC Üreticisi" şirketlerden dileyenler, Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemini işletmek üzere "**İşletici Kuruluş**" yetkisi almak için, Başkanlığa yazılı olarak başvuruda bulunurlar.

İşletici Kuruluş izni almak isteyen kuruluşlar, Sisteme dair e-Belge düzenlenmesi konusunda işbirliği yaptığı özel entegratör ile imzaladığı protokolü de Başkanlığa başvuru ile birlikte iletir.

Bu başvuruda, işbu kılavuzda tarif edilen Sistemi işletmek için gerekli olan yazılımlar ile teknik alt yapıyı hazırladığını gösteren bilgi ve belgeleri ve sistem mimarisini, alacağı denetim raporuna baz teşkil etmesi amacıyla sunar. Sistem mimarisi; network topolojisi, uçtan uca güvenlik altyapısı ile sertifika ve anahtar saklama yöntemini içerir. Başkanlık, gerek görmesi durumunda İşletici Kuruluştan ek ve açıklayıcı doküman ve bilgiler talep edebilir.

İşletici Kuruluşlar, izin başvuruları ile birlikte Sistemi bu kılavuzda tariflenen şekilde kurarak işleteceklerini ve aynı zamanda bu kılavuz içerisindeki tüm sorumlulukları eksiksiz yerine getireceklerini gayrikabili rücu şekilde kabul, beyan ve taahhüt etmek zorundadırlar.

Başvurusu değerlendirmeye alınan kuruluşlara, Sistemin işleyişi ve sistem kapsamında e-Belgelerin düzenlenme, iptal/iade edilme, saklanma hususları ile çeşitli ödeme türlerinin uygulama esaslarını ve diğer gereklilikleri gösteren ve bu Kılavuz ekinde yer alan "**GMÖEBYS Test Adımları Tablosu**" verilir.

Başvuru yapan kuruluş, bu kılavuz içerisinde tariflenen şekilde bir dosya hazırlayarak, **GMÖEBYS Test Adımları Tablosu'na uygun** uyumluluk testleri için hazır olduğunu beyan eder. Uyumluluk testleri; TÜBİTAK Devlet Üniversitelerinden Teknik Üniversitelerin ilgili bölümlerince ya da BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarının gerekli yetkinliğe haiz personeli tarafından, sorumlulukları kendilerine ait olmak üzere yapılması/yaptırılması gerekmektedir. Bununla birlikte kapsam ve içeriğini belirleyeceği testleri Başkanlık kendi bilgi işlem ekipleri ile de yapabilir. Uyumluluk testini gerçekleştirilen kuruluşlar, test sonuçlarını Başkanlığa bir Rapor ile bildirir. Bu birimler tarafından testlerin yapılması, gerek görülmesi halinde Başkanlık birimleri tarafından da ayrıca test yapmasına mani teşkil etmez. Uyumluluk testlerini başarıyla gerçekleştiren kuruluşların sistemlerinin çalışabilirliğini göstermiş oldukları kabul edilir. Ancak bu kabul hiçbir şekilde Uçtan Uca Güvenlik ve Vergi Güvenliği ile ilgili sorumluluklarında kısıtlama ya da Başkanlığa devri anlamına gelmez.

Başkanlık izin başvurularının değerlendirilmesi sürecinde ek bilgi ve belge talep edebilir, açıklama ve sistemin işleyişine ilişkin demo sunum isteyebilir, diğer kamu kurum ve kuruluşlarından uygunluk sorgulaması yapabilir.

Başkanlık tarafından yapılan değerlendirme süreçlerini başarılı şekilde tamamlayan ve Bakanlık tarafından da izin verilen kuruluşlar, kendilerine izin yazısında bildirilen tarihten geçerli olmak üzere mükelleflere Sistem kapsamında İşletici Kuruluş olarak hizmet verebilirler.

İşletici Kuruluş izni verilen kuruluş ile anlaşmalı olduğu Özel Entegratör Kuruluşuna ilişkin bilgiler ebelge.gib.gov.tr internet adresinde yayınlanır. İşletici kuruluş, izin aldıktan sonra, farklı bir özel entegratör ile de e-Belge entegrasyonu sağlamak istediği durumda, Başkanlığa yeniden izin için başvuru yapmasına gerek bulunmamakta olup entegrasyon yaptığı Özel entegratör ile aralarında düzenlenen protokol örneğini Başkanlığa yazılı olarak sunmaları

yeterlidir. Başkanlık gerek görmesi durumunda, işletici kuruluşun izin sonrası entegrasyon yaptığı Özel entegratör ile Sistemin uyumluluk testlerinin yeniden yapılmasını talep edebilir.

İşletici Kuruluşlar, izin aldıkları sistem mimarisine yönelik değişiklik yapmak istemeleri halinde, bu durum Başkanlık iznine bağlıdır. Başkanlık yazılı izni olmadan Sistem mimarisinde değişikliğe gidilemez. Bunun için ilk izin başvurusunda bulundukları kapsamda bir dosya hazırlayarak;

a) Sistem Mimarisinde değişikliğe gitme ihtiyacının nedenlerini,
b) İzin almak istedikleri yeni sistem mimarisi ile izin aldıkları sistem mimarisi arasındaki farkları,

gösteren iki ek ile başvurularını yaparlar.

Başkanlık sistem mimarisinde gerçekleştirilecek değişikliğe izin vermek için, yapılacak değişiklikler nedeniyle oluşan fark unsurların sistemin ana yapısında bir zafiyete yol açılmadığını uyumluluk testi raporu ile belgelendirilmesini talep eder. Söz konusu raporun uygun görüş içermesi durumunda sistem mimarisine ilişkin değişikliğe Başkanlık izin verir. Yeni sistem mimarisinin verilen izin tarihinden itibaren, sahaya uygulanması mümkündür.

Başkanlık belirli aralıklarla işletici kuruluşların test ve canlı networkleri üzerinde veya İşletici kuruluş bünyesinde test ve canlı ortamlarda Uyumluluk Testleri yaptırılmasını talep edebilir. Bu kapsamda Uyumluluk Testi Yapmaya Yetkili Kuruluşlar tarafından fonksiyonalite, performans ve güvenlik test araçları kullanılabilir ve oluşan raporlar Başkanlığa sunulur. Başkanlık bu raporların sonuçlarına göre işletici kuruluşların sistemlerinde kılavuza uygun düzenlemeler yapmalarını talep edebilir.

11. Sistemden Yararlanmak İsteyen Mükelleflerin Üyelik Başvurusu ve Sisteme Dahil Edilmesi

507 Sıra No'lu Vergi Usul Kanunu Genel Tebliği 5 nci maddesi, 1 nci fıkrasında tanımlanan vergi mükelleflerinin tümü Sistemden faydalanabilir. Bunun için Başkanlık tarafından İşletici Kuruluş olarak yetkilendirilmiş şirketler ile üyelik anlaşmaları yapmaları ve Başkanlık tarafından sunulan İnteraktif Vergi Dairesi üzerinden 507 sıra no.lu VUK Genel Tebliği kapsamında e-Belge uygulamalarına dahil olacaklarını beyan etmeleri ve hizmet alacakları işletici kuruluşu seçmeleri gerekmektedir.

Söz konusu başvuruyu müteakip hizmet alacakları işletici kuruluşun çalışmakta olduğu ve mükellefe e-Belge hizmet sunacak özel entegratör tarafından "e-Fatura Uygulaması Özel Entegrasyon Kılavuzunda" açıklanan şekilde mükellef hesabının açılması için HR.xml dosyası elektronik ortamda Başkanlığa iletilecek ve Başkanlıktan gelen onay mesajını müteakip Sistemden faydalanmaya başlayabilirler.

Başkanlık, üyelik başvurusu ve sisteme dahil edilme sürecinde elektronik imza, mali mühür dışında diğer doğrulama ve onaylama mekanizmalarını kullandırmaya ve bunu işletici kuruluşlara yazı ile bildirmeye yetkilidir.

İşletici kuruluşlar, sisteme dahil ettiği veya sistemden çıkardığı (sözleşmesin feshi veya sona ermesi nedeniyle) mükelleflerin bilgilerini yine "e-Fatura Uygulaması Özel Entegrasyon Kılavuzunda" açıklanan şekilde mükellef hesabının kapatılması için HR.xml dosyası elektronik ortamda Başkanlığa aynı gün iletilmek zorundadır.

Üyelikten çıkış prosedürü ve süresi, üyelik başvuru prosedüründen ve süresinden uzun ve farklı olmamalı ve ayrıca işletici kuruluş ile uygulamadan yararlanan mükellef arasındaki ticari alacak ve borç ilişkisi, mükellefin sistemden çıkma talebinin yerine getirilmesine engel teşkil etmemelidir.

12. Sistem İle Birlikte ÖKC/YNÖKC Kullanımı

Sisteme dahil olan ve tüm mükelleflerin, faaliyetlerinde ödeme kaydedici cihaz kullanma mecburiyetleri bulunmamaktadır. Ancak sisteme dahil olan mükelleflerden hali hazırda ödeme kaydedici cihaz kullanmakta olanlar, söz konusu cihazlarını perakende satış fişi ile belgelendirilebilecek satışlarında kullanmaları mümkündür.

Bununla birlikte söz konusu ödeme kaydedici cihazların Sistem kapsamında gerçekleştirilen ve e-Belge düzenlenen hallerde kullanılması durumunda, elektronik belgelere ilişkin olarak "Bilgi Fişi" (*usul ve esasları Başkanlıkça www.ynokc.gib.gov.tr internet adresinde yayımlanan YENİ NESİL ÖDEME KAYDEDİCİ CİHAZLARDAN "BİLGİ FİŞLERİ" DÜZENLENMESİNE DAİR USUL VE ESASLARA İLİŞKİN TEKNİK KILAVUZ'da belirtilen*) düzenlemeleri gerekmektedir.

Sisteme dahil olan mükellefler, sistem kapsamında verilmeyen banka vb. kuruluşlara ait EFT-POS cihazlarını, ödeme kaydedici cihazlarla 483 Sıra No.lu Vergi Usul Kanunu Genel Tebliğinde ve bu Tebliğe dayanılarak Başkanlık tarafından yayımlanan Teknik Kılavuzlar, Protokol dokümanları ve Başkanlık tarafından www.ynokc.gib.gov.tr internet adresinde yapılan duyurularla belirlenen kurallara uygun kullanılması şartıyla kullanmaya devam edebilirler.

13. Denetim

Başkanlık tarafından işletici kuruluş izni verilen firmalar, kurmuş oldukları ya da yararlandıkları dış hizmet sağlayıcıların sistemlerinin uçtan uca güvenli haberleşme ve bilgi sistemleri denetimini, izin tarihinden en geç 1 yıl içerisinde BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kurumları veya Devlet Üniversitelerinden Teknik Üniversitelerin ilgili bölümlerince ya da TÜBİTAK tarafından denetlenmelerini tamamlamak ve ilgili raporların Başkanlığa iletimini sağlamak zorundadır.

Bu süre içerisinde denetim raporları Başkanlığa ulaşmamış olan işletici kuruluşların izinleri önce askıya alınır ve bu durum ebelge.gib.gov.tr adresinden duyurulur. Bunun üzerine İşletici Kuruluşa denetim raporlarını teslim etmesi için 6 ay ek süre verilir. Bu süre zarfında da denetim raporlarını teslim etmeyen ya da edemeyen İşletici Kuruluşların izni iptal edilir.

İşletici Kuruluşlar, Sistemi yönetmek ve işletmek amacıyla kurdukları altyapının (Dış Hizmet Sağlayıcıdan yararlanılması halinde bunların altyapılarının) Güvenli Haberleşme ve Bilgi Sistemleri denetimlerini, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşları veya Devlet Üniversitelerinden Teknik Üniversitelerin ilgili bölümlerince ya da TÜBİTAK tarafından her 3 yılda bir yaptırmak zorundadır.

Bakanlık ya da Başkanlık gerek görmesi durumunda, İşletici Kuruluşu ve bu kılavuz kapsamında işletici kuruluş sorumluluğunda e-Belge ile ilgili hizmet sunacak Özel Entegratörlerin kurmuş olduğu altyapı sistemlerini dilediği anda ve dilediği şekilde denetleyebilir veya denetletebilir.

İşletici Kuruluş ve Özel Entegratör kuruluşlar, sistem kapsamındaki altyapılarını geriye doğru 10 yıllık bir denetime elverişli halde kurmak ve tutmakla yükümlüdür. Bu sebeple İşletici Kuruluş ve Özel Entegratör kuruluşları tarafından sağlanacak olan sistem iz kayıtlarının doğruluğundan, bütünlüğünden ve değiştirilmezliğinden İşletici Kuruluş sorumludur.

14. Sorumluluk ve Ceza Uygulaması

Sistem uçtan uca bir bütündür. Bu bütünün güvenlik zincirini sağlamak da İşletici Kuruluşun sorumluluğu altındadır. Sistemin asli sorumlusu İşletici Kuruluş olsa da Bakanlık ve Başkanlık'a karşı tüm iş ortakları aldıkları izin kapsamındaki faaliyetlerden müteselsilen sorumludur.

e-Belgeleri, gerek bu kılavuzda gerek ilgili e-Belge Teknik kılavuzlarında açıklandığı şekilde üretmeyen İşletici Kuruluş hakkında Vergi Usul Kanununda yer alan cezai hükümler uygulanabileceği gibi yapılan yazılı uyarıya rağmen gerekli önlemleri almayan işletici kuruluşların Bakanlıkça verilen faaliyet izinleri belli bir süreyle durdurulabileceği gibi iptal de edilebilir.

İşletici Kuruluşlar, uçtan uca güvenliğin sağlanmasında kullandıkları yazılımsal metodlardan sorumludur.

Güvenli Mali Uygulama, Ödeme Kabul Eden Araç ve e-Belge entegrasyonları İşletici Kuruluş adına üçüncü taraflarca da geliştirilebilir ve işletilebilir. Ancak bu durum İşletici Kuruluşun Sistemi için sahip olduğu münhasır ve asli sorumluluğu ortadan kaldırmadığı gibi, Sistemin ana omurgasını oluşturan bu üç yazılımın tamamının ya da bir kısmının üçüncü (dış hizmet sağlayıcı) taraflarca geliştirilmiş olması, ya da Sistemin işletilmekte olması diğer taraflarla sorumluluk paylaşımı anlamına gelmez.

İşletici Kuruluşlar, Sistemin uçtan uca güvenliğinin sağlanması amacıyla aşağıda belirtilenlerle sınırlı olmamak üzere, sorumludurlar:

- Her ödeme türü için, e-Belgenin düzenlenmesini sağlamaktan,
- Ödeme / Tahsilat işlemlerinin güvenliğinden,
- Satış işlemlerinin ve e-Belgenin vergi mevzuatındaki düzenlemelerine uyumluluğunun sağlanmasından, (asli olarak İşletici Kuruluşta olmakla birlikte Özel Entegratör Kuruluşların da müşterek ve müteselsil sorumluluğu bulunmaktadır.)
- Güvenli Mali Uygulama, Ödeme Kabul Eden Araç ve Özel Entegratör Kuruluş ile entegrasyon yazılımlarının her birinin üzerinde ayrı ayrı ya da birbirleri olan entegrasyonlar arasında yapılan her tip ve türdeki manipülasyonları önlemekten,
- Tahsilat ile düzenlenen e-Belge arasındaki mutabakatsızlıkları kontrol ve önlemekten,
- e-Belge düzenlemeye esas verilerin Özel Entegratör Kuruluşa, ilgili Genel Tebliğlerde ve Teknik Kılavuzlarında tariflenen belge düzenleme esas ve şartlarına riayet edilerek iletilmesini sağlamaktan,
- Mali verilerin kaynağının, doğruluğunun, değişmezliğinin ve bütünlüğünün kontrolünü sağlamaktan,
- Bozuk, hatalı ve atak içeren verilerin muhataplara iletilmesini önlemekten,
- Sisteme ilişkin verilerin güvenliği ve gizliliği zarar görmeyecek şekilde 10 yıl süre ile saklanmasını sağlamaktan,
- Denetime uygunluk verecek şekilde sistem loglarının tutulmasını sağlamaktan,
- Harici Uygulamalar ile Güvenli Mali Uygulama arasında yapılan entegrasyonların vergi kayıp ve kaçağına yol açılmayacak şekilde yapılmasını sağlamaktan,
- Yetkili Servislerin yaptığı iş ve işlemlerin bu kılavuz ve ilgili diğer mevzuatlarda belirlenen kurallara uygunluğunu sağlamaktan,

sorumludur.

İşletici Kuruluşlar işbirliği yaptığı özel entegratör kuruluşlar ile birlikte müşterek ve müteselsilen Sistem kapsamında düzenlenen e-Belgeleri, asgari 10 yıl süre ile gizlilik ve güvenliğini sağlayacak şekilde saklama ve talep edilmesi halinde Başkanlığa elektronik ortamda iletme yükümlülüğü bulunmaktadır. İşletici kuruluşların yukarıda sayılı sorumluluklarını yerine getirmemeleri durumunda; 213 sayılı Vergi Usul Kanununda yer alan cezai hükümler uygulanabileceği gibi yapılan yazılı uyarıya rağmen gerekli önlemleri ivedilikle almayan işletici kuruluşların Bakanlıkça verilen faaliyet izinleri belli bir süreyle durdurulabileceği gibi iptal de edilebilir.

İşletici Kuruluşlar ve bunlarla e-Belge düzenlenmesi konusunda işbirliğinde bulunan özel entegratör kuruluşlar, merkezi sunucularını Türkiye Cumhuriyeti sınırları içerisinde kurmak ve barındırmak zorundadırlar. Sistem üzerinden geçen gerek mali gerekse finansal hiçbir verinin yedekleme amacıyla da olsa yurtdışına çıkarılmayacağını taahhüt ederler.

Ayrıca, İşletici Kuruluşlar ve bunlarla e-Belge düzenlenmesi konusunda işbirliğinde bulunan özel entegratör kuruluşlar, kurmuş ve işletmiş oldukları Sistem üzerinden geçen işlemlere dair ticari, mali ve finansal verileri Başkanlık dışında, uygulamadan yararlanan mükelleflerin ve işleme taraf olanların yazılı izni olmadan hiçbir şekilde ve amaçla işleyemezler, üçüncü taraflara iletemezler, kullandıramazlar ve raporlayamazlar. Verilen hizmetler kapsamında elde edilen her tür ticari, mali ve finansal verilerin güvenliğinden ve gizliliğinden İşletici Kuruluşlar sorumludurlar. Sistem kapsamında düzenlenen e-Belgelerin, uygulamadan yararlanan mükellefler tarafından yazılı bir onayla finansal bir işleme (faktöring, kredi teminatı, alacak sigortası vb. e-Belgeye bağlı finansal/bankacılık işlemlerine) konu edilmesini sağlamak üzere ilgili finansal kuruluşlara belirtilen finansal işlemlerin gerçekleştirilmesi amacıyla iletilmesi mümkündür.

Söz konusu sorumluluklara uymadığı tespit olunan İşletici Kuruluş veya özel entegratörlerin Bakanlıkça verilen faaliyet izinleri belli bir süreyle durdurulabileceği gibi tamamen iptal de edilebilir. Faaliyet izinleri iptal edilen işletici kuruluş veya özel entegratörlere ve bunların yöneticilerinin kanuni temsilciliğini yürüttüğü kuruluşlara, Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi kapsamında tekrar faaliyet izni verilmez.

İşletici Kuruluşlar, münhasıran Sistemden yararlanan mükellefin kendi bilgilerini kendisine katma değerli hizmetler sunmak maksadıyla ve yazılı bir sözleşme yapılmış ve katma değerli hizmetin kapsamı açıkça belirtilmiş olmak kaydıyla işleyebilir, raporlayabilir. Ancak bu durumda da Sistem kapsamındaki ticari, mali ve finansal verilerin üçüncü kişilerle herhangi bir şekilde paylaşılması ve bu amaçla işlenmesi mümkün değildir.

15. Dış Hizmet Alımı

İşletici Kuruluşlar, tebliğ konusu sistemlerin temini ve işletimi konusunda dış hizmet alımı yapabilirler. Ancak bu durum İşletici Kuruluş'un tebliğ kapsamındaki sorumluluklarını ortadan kaldırmaz.

16. Değişiklik Hakkı

Başkanlığın bu Teknik Kılavuz üzerinde her türlü değişiklik ve güncelleme hakkı bulunmakla birlikte, dijitalleşen süreçler, ödeme sistemlerindeki gelişmeler, güvenlik ihtiyaçlarındaki değişimler, ek gereksinim, fonksiyonalite vb. durumlarda teknik kılavuzda değişiklik yapmadan yazılı bildirim yapmak suretiyle İşletici Kuruluşlardan bu değişiklikleri yapmasını talep edebilecektir.

EKLER:

1- GMÖEBYS Test ve Doğrulama Adımları Tablosu