EK-1

GELİR İDARESİ BAŞKANLIĞI

Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi

Test ve Doğrulama Adımları Dokümanı

Versiyon 1.1

(21.05.2020)

1) GİRİŞ

Bu doküman, İşletici Kuruluşların geliştirdikleri sistemleri ön testlere tabi tutmaları ve yetkilendirilmiş test kuruluşları için rehber olması amacı ile düzenlenmiştir. İşletici Kuruluşların Sistemlerine ait doğrulama, fonksiyonel ve güvenlik testleri bu özet doküman temel alınarak yapılacaktır.

2) TEST VE DOĞRULAMA TABLOSU

KODU	TEST UNSURU	UYGULANACAK YÖNTEMLER
1	İzin Başvurusu Yapan Kuruluş Tebliğde belirtilen kuruluşlar kategorisinde midir?	Başvuru belgeleri kontrol edilecektir.
2	İşbirliği yapılacak Özel Entegratör Kuruluş ile İşletici Kuruluş arasında, Güvenli Mali Uygulama ile e-Belge entegrasyonu ve sorumluluğu konusunda protokol yapılmış mıdır?	Başvuru belgeleri kontrol edilecektir.
3	Sisteme dahil edilen kullanıcının, mükellefiyet durumu dikkate alınmakta mıdır?	Fonksiyonel testler esnasında; Mükellef/ Üye İşyeri Yönetim modülleri incelenecektir.
4	Basit Usul mükelleflerinin düzenleyeceği Fatura belgesinde KDV istisnası uygulanmakta mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
5	Sistem kapsamında düzenlenen e-Belgeler GİB şematron kontrollerinden geçmiş midir?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
6	Harici Satış Uygulama Yazılımı ile Güvenli Mali Uygulama Entegrasyonu sağlanmış mıdır?	Fonksiyonel testler esnasında; Eğer entegrasyon varsa; bilgi bütünlüğü, güvenliği ve doğruluğu iletişim protokolü incelenerek değerlendirilecektir.
7	Güvenli Mali Uygulama Yazılımında Mal ve Hizmetlerin Tanımlaması (Mal veya Hizmetin Adı, Birim Ölçüsü, Barkodu/Standart Kodu, Birim Fiyatı, KDV Oranı, ÖTV Oranı) yapılmakta mıdır?	Fonksiyonel testler esnasında; Sistem bünyesindeki temel satış uygulaması incelenerek değerlendirilecektir.
8	Belge üzerinde ödeme bilgisine de yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge ve müşteriye verilen/gönderilen belge ve çıktılar incelenerek değerlendirilecektir.

9	Belge üzerinde İçeriği GİB tarafından belirlenen Karekoda yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
10	KDV hesaplaması doğru şekilde yapılmakta mıdır?	Fonksiyonel testler esnasında; farklı oranlarda KDV barındıran işlemler yapılarak değerlendirilecektir.
11	Fatura altı ıskonto tutarları farklı KDV oranlarına göre dağıtımı yapılmakta mıdır?	Fonksiyonel testler esnasında; farklı oranlarda KDV barındıran işlemler yapılarak değerlendirilecektir.
12	Satır ıskontoları doğru uygulanmakta mıdır?	Fonksiyonel testler esnasında; farklı oranlarda KDV barındıran işlemler yapılarak değerlendirilecektir.
13	Belge üzerinde(alt kısmında) İşletici Kuruluş Güvenli Mali Uygulama Yazılım Sürüm bilgisine yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge ve müşteriye verilen/gönderilen belge ve çıktılar incelenerek değerlendirilecektir.
14	Ödeme/Tahsilat işlemi ile birlikte belge içerik bilgileri özel entegratör sistemlerine anlık olarak aktarılmakta mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
15	Ödeme/Tahsilat işlemi ile birlikte e-Belge özel entegratör sistemlerinde anlık olarak oluşturulmakta mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
16	Özel Entegratör sistemi ile çevrim içi olunmadığında Güvenli Mali Uygulama satış işlemini kesmekte midir?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
17	Güvenli Mali Uygulamanın Çevrimdışı çalışıyorsa; fonksiyonel gereksinimler karşılanmış mıdır? Gerekli güvenlik önlemleri alınmış mıdır?	Güvenlik testleri esnasında; Çevrimdışı sistemler için güvenlik testleri ayrıca değerlendirilecektir. Başvuru dokümanlarında İşletici Kuruluş tarafından iletilen Çevrimdışı mimari ve güvenlik altyapısı incelenecektir. Altyapının doğruluğu, verinin korunduğu ve Çevrimiçi olunduğunda güvenli bir şekilde merkeze iletildiği kontrol edilecektir. İşletici kuruluş sistemi bu akışları gösteren örnek işlemler yapmak ve Test kuruluşuna bu akışların doğru çalıştığını sunmalıdır. Fonksiyonel testler esnasında; çevrimdışı yapılan işlemlerin sistem çevrim içi olduğunda veri kaybına neden olmadığı ve doğru bir şekilde çevrimiçi iken olduğu gibi akışların aynen uygulandığı kontrol edilecektir.

18	Sistem kapsamında düzenlenecek e-Belgenin müşteriye iletim usulü belge üzerinde belirtilmekte midir?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
19	Sistem kapsamında düzenlenecek e-Belgenin müşteriye elektronik ortamda iletimi seçeneği arasında SMS var mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir. SMS var ise test edilecek ve SMS ile doğru bir şekilde belge aktarımı yapıldığı kontrol edilecektir.
20	Sistem kapsamında düzenlenecek e-Belgenin müşteriye elektronik ortamda iletimi seçeneği arasında e-Mail(e-Posta) var mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir. E-Posta var ise test edilecek ve E-Posta ile doğru bir şekilde belge aktarımı yapıldığı kontrol edilecektir.
21	İşletici Kuruluş Güvenli Mali Uygulama ile Özel Entegratör Sisteminin aylık olarak % 99,75 kullanılabilirlik oranı ile hizmet sunacağını taahhüt etmiş midir?	Başvuru belgeleri kontrol edilecektir.
22	e-Belge üzerinde ödeme türü bilgisine yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge ve müşteriye verilen/gönderilen belge ve çıktılar incelenerek değerlendirilecektir.
23	e-Belge üzerinde banka/kredi kartı ile yapılan tahsilatlara ilişkin slip temel bilgilerine de yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge ve müşteriye verilen/gönderilen belge ve çıktılar incelenerek değerlendirilecektir.
24	e-Belge üzerinde KDV oranlarına göre Toplam Satış Tutarı ve Toplam KDV Tutarı bilgisine ayrıca yer verilmiş midir?	Fonksiyonel testler esnasında; e-Belge ve müşteriye verilen/gönderilen belge ve çıktılar incelenerek değerlendirilecektir.
25	İşletici kuruluş, sisteminde yer alan, ödeme kabul eden noktalardaki yazılım ve donanım matrisini sunmuş mudur? Bu matrise ait her bir varyasyonun mali uygulama yazılımının güvenliğini sağlamış mıdır? Mali uygulama yazılımı güvenlik altyapısına ilişkin gerekli dokümanları ve akış diyagramlarını sunmuş mudur?	Başvuru belgeleri kontrol edilecektir. Test Kuruluşu her bir matris için ayrı ayrı sistem fonksiyonel ve güvenlik testlerini tekrar edecektir.
26	İşletici Kuruluş hangi Ödeme/Tahsilat Türlerini desteklemektedir?	Başvuru belgeleri kontrol edilecektir.
27	Üye işyeri anlaşması gerektiren ödeme/tahsilat türlerinde bu ödeme türünün aktif / pasif hale getirilmesi işletici kuruluş sorumluluğunda gerçekleştirilmekte midir?	Fonksiyonel testler esnasında; İşletici Kuruluşun desteklediği ödeme türleri için İşletici Kuruluş Sistemlerinden, aktif ve pasif yapılarak kontroller

		yapılmalıdır. Yalnızca aktif olan ödeme türleri ile işlem yapılabildiği değerlendirilmelidir.
28	a. Güvenli Mali Uygulama Günlük Satış Raporunu üretebilmekte midir? b. Bu raporları GİB ile GİB'in belirlediği yöntemlerle paylaşabilmekte midir?	Fonksiyonel testler esnasında; Fonksiyonel test süreçleri dokümanında yer aldığı şekli ile, İşletici Kuruluş arayüzleri, veritabanı ve merkezi sistemleri kontrol edilmelidir.
29	a. Güvenli Mali Uygulama Aylık Satış Raporunu üretebilmekte midir? b. Bu raporları GİB ile GİB'in belirlediği yöntemlerle paylaşabilmekte midir?	Fonksiyonel testler esnasında; Fonksiyonel test süreçleri dokümanında yer aldığı şekli ile, İşletici Kuruluş arayüzleri, veritabanı ve merkezi sistemleri kontrol edilmelidir.
30	a. Güvenli Mali Uygulama İki Tarih Aralığı Satış Raporunu üretebilmekte midir? b. Bu raporları GİB ile GİB'in belirlediği yöntemlerle paylaşabilmekte midir?	Fonksiyonel testler esnasında; Fonksiyonel test süreçleri dokümanında yer aldığı şekli ile, İşletici Kuruluş arayüzleri, veritabanı ve merkezi sistemleri kontrol edilmelidir.
31	a. Güvenli Mali Uygulama Düzenlenen Belgeler Raporunu üretebilmekte midir? b. Bu raporları GİB ile GİB'in belirlediği yöntemlerle paylaşabilmekte midir?	Fonksiyonel testler esnasında; Fonksiyonel test süreçleri dokümanında yer aldığı şekli ile, İşletici Kuruluş arayüzleri, veritabanı ve merkezi sistemleri kontrol edilmelidir.
32	a. Güvenli Mali Uygulama Düzenlenen Bilgi Fişleri Raporunu dönemsel olarak (Günlük/Aylık/İki Tarih Aralığı şeklinde) üretebilmekte midir? b. Bu raporları GİB ile GİB'in belirlediği yöntemlerle paylaşabilmekte midir?	Fonksiyonel testler esnasında; Fonksiyonel test süreçleri dokümanında yer aldığı şekli ile, İşletici Kuruluş arayüzleri, veritabanı ve merkezi sistemleri kontrol edilmelidir.
33	İşletici Kuruluş, Uygulamaya dahil edilen mükellef ile kurulan yazılım arasındaki kimliklendirmeyi sağlamakta mıdır?	Fonksiyonel ve güvenlik testleri esnasında; Test süreçleri dokümanlarında yer aldığı şekli ile, gerekli kimlik doğrulama ve oturum açma yöntemlerinin uygulandığı kontrol edilmelidir.
34	Güvenli Mali Uygulamayı kullanacak mükellefin, oturum açma ve kimlik doğrulaması için gerekli tedbirler alınmış mıdır?	Fonksiyonel ve güvenlik testleri esnasında; Test süreçleri dokümanlarında yer aldığı şekli ile, gerekli kimlik doğrulama ve oturum açma yöntemlerinin uygulandığı kontrol edilmelidir.
35	Yarım kalan-sonlanmayan- veya iptal edilen (Müşterinin vazgeçmesi, tahsilatın yapılamaması, işlemin iptali) satış işlemlerine ait bilgiler de güvenli şekilde saklanmakta mıdır?	Fonksiyonel ve güvenlik testleri esnasında; ilgili akış olasılıkları uygulanmalı ve bu olasılıklara ait sonuçlar test raporuna yansıtılmalıdır.

36	Satış işleminin Ödeme/Tahsilat aşaması gerçekleştirildikten sonra kapatılması sağlanmakta mıdır?	Fonksiyonel testler esnasında; satış uygulaması üzerinden işlem testleri yapıp gerekli kontroller yapılmalıdır.
37	a. Güvenli Mali Uygulama aracılığı ile oluşan satış bilgilerinin özel entegratör kuruluşa iletiminde güvenli iletişim yöntemi uygulanmakta mıdır? b. Kullanılan güvenli iletişim yöntemine ilişkin gerekli dokümanları ve akış diyagramlarını sunmuş mudur?	Başvuru belgeleri kontrol edilecektir. e-Belge entegrasyonu incelenmelidir. Kullanılan iletişim yöntemi ve güvenlik seviyesi test raporunda yer almalıdır.
38	e-Belge bilgilerinin özel entegratör aracılığı ile müşteriye iletiminde güvenlikli iletim yöntemi uygulanmakta mıdır?	e-Belge entegrasyonu incelenmelidir. Kullanılan iletişim yöntemi ve güvenlik seviyesi test raporunda yer almalıdır.
39	e-Belge bilgilerinin özel entegratör aracılığı ile satıcıya iletiminde güvenlikli iletim yöntemi uygulanmakta mıdır?	e-Belge entegrasyonu incelenmelidir. Kullanılan iletişim yöntemi ve güvenlik seviyesi test raporunda yer almalıdır.
40	e-Belge bilgilerinin GİB tarafından sorgulanması ve doğrulanmasına ilişkin web servis kurulmuş mudur?	Fonksiyonel testler esnasında; İşletici Kuruluşun bu servisleri hazırlayıp hazırlamadığı kontrol edilecektir. Servislerden örnek çağrımlar yapılarak sonuçları test raporuna yansıtılacaktır.
41	e-Belge örneklerinin GİB sistemlerine aktarımına ilişkin web servis-transfer sistemi kurulmuş mudur?	Fonksiyonel testler esnasında; İşletici Kuruluşun bu servisleri hazırlayıp hazırlamadığı kontrol edilecektir. Servislerden örnek çağrımlar yapılarak sonuçları test raporuna yansıtılacaktır.
42	İşletici kuruluş sistem kapsamında gerçekleştirilen satış, ödeme/tahsilat, e-Belge süreçlerinin, kılavuzun "Olay Kayıt Özelliği" başlığında belirtilen şekilde log kayıtlarının tutulmasına yönelik alt yapı kurmuş mudur?	Fonksiyonel testler esnasında; İşletici Kuruluşun merkezi sistemi ve uç nokta yazılımları kontrol edilecek, Olay Kayıt Özelliği test edilecektir. Geçmiş 10 yıl verisi için merkezi sistemde gerekli mimarinin kurgulanmış olduğu başvuru dokümanları ve merkezi sistem mimarisi incelenerek raporlanacaktır.
43	Avans tahsilat işleminde düzenlenen Bilgi Fişi'nde ilgili kılavuzda belirtilen gerekli bilgileri barındırmakta mıdır?	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa Bilgi Fişi ve çıktıları incelenecektir.
44	Cari Hesap Tahsilat işleminde düzenlenen Bilgi Fişi'nde ilgili kılavuzda belirtilen gerekli bilgileri barındırmakta mıdır?	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa Bilgi Fişi ve çıktıları incelenecektir.
45	Yemek Kartı ile Yapılan Tahsilat işleminde düzenlenen Bilgi Fişi'nde ilgili kılavuzda	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa Bilgi Fişi ve çıktıları incelenecektir.

	belirtilen gerekli bilgileri barındırmakta mıdır?	
46	Fatura Tahsilatı işleminde düzenlenen Bilgi Fişi'nde ilgili kılavuzda belirtilen gerekli bilgileri barındırmakta mıdır?	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa Bilgi Fişi ve çıktıları incelenecektir.
47	Sistemin Otopark uygulamalarında kullanılması durumunda, araç giriş işlemleri Otopark Giriş Bilgi Fişi ile belgelendirilmekte midir?	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa Bilgi Fişi ve çıktıları incelenecektir.
48	Sistemin Otopark uygulamalarında kullanılması durumunda, araç çıkış işlemleri e-Belge (e-Fatura ya da e-Arşiv Fatura) belgelendirilmekte midir?	Fonksiyonel testler esnasında; İşletici Kuruluş destekliyorsa e-Belge entegrasyonu ve çıktıları incelenecektir.
49	Vergiler dahil belli tutarı (500 TL) aşan e-Arşiv Faturalarda müşterinin Adı-Soyadı bilgisi için kontrol uygulanmakta mıdır?	Fonksiyonel testler esnasında; e-Belge entegrasyonu ve çıktıları incelenecektir.
50	Sistemden yararlanmak isteyen mükellefin sisteme kayıt bilgilerinin GİB'e elektronik ortamda bildirimi için alt yapı tesis edilmiş midir?	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. GİB'e ilgili bağlantılar sağlandığında iletilebileceğinin gösterilmesi yeterlidir.
51	İşlemler; satış, ödeme, e-Belge oluşturma süreçleri bütüncül olarak yönetilmekte midir? 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.)	Fonksiyonel testler esnasında; Tüm işlem türleri test edilecek ve sonuçları değerlendirilecektir. Uç noktadan yapılan işlemler merkezi sistemde İşletici Kuruluş arayüzleri üzerinde kontrol edilecek ve her üç işlemin de eşleştiği ve bu şekilde raporlanabildiği görülecektir.

52	Veri bütünlüğü uç noktadan merkezi sisteme, oradan da 3rd servislere kadar, uçtan uca ve güvenli bir şekilde sağlanmış mıdır? (Uç noktadaki verinin, (örneğin tutar verisi) merkezi sistemde ve verinin aktığı her yerde aynı değerde olması kontrolü sağlanmalıdır.)	Veri aktarımında; karşı taraf doğrulama, şifreleme, hash ve uç nokta doğrulama gibi yöntemler hangilerinin kullanıldığı tespit edilecek ve bu bilgilere ayrıntılı bir şekilde raporda yer verilecektir.
53	TCKN, e-posta, telefon numarası, adres, kart numarası gibi hassas veriler saklandığı noktalarda anahtar kullanılarak şifreli bir şekilde güvenli ortamlarda saklanmış mıdır?	İşletici Kuruluş Merkezi sistemi veritabanı ve dosya sunucuları üzerinde hassas verilerin tutulma yöntemleri incelenecektir. Verilerin saklandıkları yerde şifreli olduğu görülmelidir. Bu verilerin açık halde hiç bir ortamda saklanmadığı kontrol edilecektir. Bu bilgilere ayrıntılı bir şekilde raporda yer verilecektir.
54	TCKN, e-posta, telefon numarası, adres, kart numarası gibi hassas verilerin yetki bazlı olarak erişilebildiği, erişen sistem kullanıcının iz takibinin yapılabildiği bir altyapı kurgulanmış mıdır?	Hassas verilere erişim iz takibi ile erişim yapılabilmelidir. Kullanıcı arayüzü üzerinden yapılan erişimler test edilmeli, iz takibinin yapılabildiği görülmelidir. İz kayıtlarının da ayrıca korunduğu gözlemlenmelidir.
55	TCKN, e-posta, 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 sağlanmış mıdır?	Hassas verilere yetki bazlı olmayan, raporlama vb. amaçlı erişimler isteniyorsa; verinin saklandığı yerlerde yalnızca maskeli ve özet hali ile görülebildiği gözlemlenmelidir.
56	Sisteme ait Sertifika Yönetimi ile ilgili; gerekli dokümanlar ve akış diyagramları sunulmuş mudur?	Başvuru belgeleri kontrol edilecektir.
57	Sertifikasyon sürecinde kullanılmak üzere, sistem işleticisine ait private anahtarı güvenli olarak oluşturulabilmekte midir?	Kılavuzda yer alan HSM cihazları kullanılmalıdır. Anahtarlar doğrudan cihazlar üzerinde rasgele üretilmelidir. Anahtarın cihazdan yetkisiz bir şekilde çıkarılamayacak özellikte tanımlandığı kontrol edilmelidir.
58	GİB'in belirlediği sertifika otoritesine gönderilmek üzere sertifika talebi yapılabilmekte midir?	Kılavuzda yer alan sertifika talep dosyası üretimi gösterilmelidir. Talep dosyasının formatı ve doğruluğu kontrol edilmelidir.
59	GİB'in belirlediği sertifika otoritesinden gelen sertifika sisteme yüklenebiliyor mu?	Kılavuzda yer alan sertifikanın sisteme tanımlanabildiği gösterilmelidir. Sisteme tanımlanan sertifikanın formatı ve doğruluğu kontrol edilmelidir.

60	Sistem ve güvenli mali uygulama, sertifika geçerlilik süresi kontrolü yapıyor mu?	Sistem saati ileri alınarak sertifika geçerlilik kontrolü yapılıp yapılmadığı gözlemlenmelidir.
61	a. Sistemin kurulu olduğu merkezde anahtar yönetimi ve şifreleme işlemleri için HSM cihazları kullanılmakta mıdır? b. Kullanılan HSM cihazlarının Ortak Kriterler EAL4+ sertifikası var mıdır?	Hassas verilerin şifrelenmesi, sertifika yönetimi, işlem imzalama gibi İşletici kuruluş sistemleri tarafından yapılan kriptografik işlemlerde HSM cihazlarının kullanıldığı gösterilmelidir. Sistem testleri esnasında işlemler yapılarak; HSM Cihazına giden/gelen işlem logları incelenmelidir. Satış İşlemleri, Mükellef tanımlama işlemleri, Sertifika talebi işlemleri vb. yapılan işlem ve sonuçlarına raporda yer verilmelidir.
62	Sisteme ait uç nokta güvenliği ile ilgili; gerekli dokümanlar ve akış diyagramları sunulmuş mudur?	Başvuru belgeleri kontrol edilecektir.
63	Sistemim bir bütün olarak; uç noktada çalışan (web tabanlı olsun veya olmasın) her bir uygulama için, uygulamanın çalıştığı ortama ait fingerprint verilerini kullanılarak, mali uygulamanın uç noktada güvenli bir şekilde çalışmasını ve uç nokta doğrulamasını sağlayabiliyor mu?	Sistemde uç noktada kullanılan fingerprint verileri ve bunların kullanım yöntemleri incelenmelidir. Fingerprint veri ile bir anahtar kullanılarak verilerin korunma yöntemi yapılıp yapılmadığı kontrol edilmelidir. Kaynak kodlarda gömülü olarak anahtar tutulmadığı kontrol edilmelidir. Raporda kullanılan yöntemlere ve bu bilgilere açık bir şekilde yer verilmelidir.
64	Uç nokta doğrulamasında OTP, Push Notification vb. harici güvenlik önlemleri var mı?	Servis altyapısı incelenmelidir. Mimari incelenmelidir. İşlem testleri yapılarak kontrol edilmelidir.
65	Uç nokta ile merkezi sistemin iletişiminde en az TLS 1.2 kullanılıyor mu?	Merkezi sistemde SSL sonlandırma ortamında ilgili tanımlamaların yapıldığı kontrol edilmelidir. TLS 1.1 ve altına izin verilmediği tanımlarda görülmelidir.
66	Uç nokta ile merkezi sistemin iletişiminde TLS 1.2 içerisinde akan verinin şifrelenmesi için işleme özel türetilmiş AES 256 bir anahtar kullanılıyor mu?	Örnek bir işlemde TLS içerisinde akan verinin şifreli olduğu ve hangi yöntem kullanıldığına ilişkin detaylara yer verilmelidir.
67	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalar bir veri tutuyorsa, bu verilerin saklanmasında anahtar kullanılıyor mu?	Anahtar kullanılıp kullanılmadığı kontrol edilmelidir. Kullanılıyorsa kod analizinde anahtarın saklanma yöntemi kontrol edilmeli ve güvenlik derecesi raporlanmalıdır.

68	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 saklanıyor/korunuyor mu?	Hassas bilgi saklanıyorsa(ssl pinning sertifikası, user, pass, url, IP, TCKN, mali bilgiler, olay kayıtları..), kod analizinde verilerin saklanma yöntemi kontrol edilmeli ve güvenlik derecesi raporlanmalıdır. Veri saklanması esnasında anahtar kullanımı ve fingerprint kullanımına ilişkin detaylara raporda yer verilmelidir.
69	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Root Detection yapılıyor mu? (Uygulamasının rootlanmış cihazlarda çalışmasını engelleyebilmelidir.)	Uygulama web tabanlı değilse, Rootlanmış bir cihazda veya test tool u ile uygulamanın uç noktada çalışmadığı kontrol edilmelidir. Web tabanlı ise yapılabilecek kontrollerin yapılıp yapılmadığı raporlanmalıdır.
70	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Device Identification yapılıyor mu?	Hangi cihaz verilerinin nasıl kullanıldığına raporda detaylı bir şekilde yer verilmedilir. Cihaz verilerin merkezi sisteme aktarılması ve doğrulanması yöntemleri incelenmelidir. Uygulamasının kurulduğu cihazı tanımlayabilecek veriler kullanıldığı incelenmelidir. Kod analizi esnasında bu kısma yer verilmelidir.
71	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Geolocation yapılıyor mu?	Geolocation yapılıyorsa farklı bir lokasyonda çalışıp çalışmadığı test edilmeli ve sonuçları raporlanmalıdır. Uç nokta uygulaması başarılı kurulmuş bir uygulama gibi davranıp farklı lokasyondan işlem yapmasına müsaade etmemelidir.
72	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Device Binding yapılıyor mu?	Uygulaması ile kurulduğu cihazı birbirine bağlayan eşsiz bir imza üretmeli ve yapılan bir işlemin ilgili cihaza kurulu uygulamadan gerçekleştirildiğini garanti etmelidir
73	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Whitebox Cryptography Storage/Secure Storage kullanılıyor mu?	Bu yöntem ile uygulama; üzerinde saklanması gereken hassas verileri güvenli şifreleme algoritmaları ile şifreli ve sadece uygulamanın güvenli bir şekilde okuyabileceği ve başka bir şekilde ulaşılamayan bir alt yapı ile saklar. Merkezi sisteme bağlantı için kullanılan API anahtarı, API Kullanıcı kodu, API şifresi, Merkezi sistem adresi(URL, IP, Port) vb. bilgiler uç noktada güvenli bir şekilde saklanmalıdır. Çevrim dışı çalışan cihazlarda SAM kart, secure element vb. donanımsal bir kripto ortamı yoksa yazılımsal kripto kullanımı kontrol edilmeli ve

		raporlanmalıdır. Uygulama, uygulamaya ait özel anahtarı güvenlik sunucusu ile ilişkilendirecek, hiçbir şekilde açık olarak cihaz üzerinde depolamayacaktır.
74	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Secure Channel kuruluyor mu?	SSL içerisinde akan veri için ikinci bir şifreleme olarak; Uygulamanın sunucu ile olan iletişimini gizlilik ve bütünlük açısından gerekli asimetrik ve simetrik şifreleme algoritmaları ile koruyacağı güvenli bir kanal üzerinden sağlanıyor mu?
75	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Anti-Debugging yapılıyor mu?	Uygulamanın bir debugger ile analiz edilmesinin engellenmiş olduğu kontrol edilmelidir.
76	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect Emulator yapılıyor mu?	Uygulamanın bir emulator üzerinde çalışmasının engellendiği kontrol edilmelidir.
77	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect-Hooking yapılıyor mu?	Uygulamaya ait fonksiyonlarının harici bir fonksiyonla çalışma zamanında değiştirilmesini engellediği kontrol edilmelidir.
78	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Detect Repackaging yapılıyor mu?	Uygulamanın kodlarının çözülüp tekrar paketlenmesini tespit edip çalışmasını engellediği tespit edilmelidir. (özet vb. yöntemler ile)
79	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Secure RunTime Memory yapılıyor mu?	Uygulamanın çalışma zamanında kullandığı hafıza alanından hassas verilerin alınmasını engelleyecek şifreleme, karıştırma ve diğer sisteme bağlı tedbirleri içerdiği kontrol edilmelidir. Bu madde için kod analizi de yapılıp raporda yer verilmelidir.
80	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Runtime CRC Check yapılıyor mu?	Uygulama, uygulama çalışma zamanında yüklenen uygulama kodunun değişmesini kontrol edip çalışmasını durduracak ve bu durumu uzak sunucuya

		raporlayacaktır. Bu madde için kod analizi de yapılıp raporda yer verilmelidir.
81	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, OTP yapılıyor mu?	Uygulama ihtiyaç duyduğu işlemlerde OTP doğrulaması yapabilmelidir. Bu işlemler ilklendirme, ilk defa login, hassas veri işlemleri, büyük ölçülü işlemler vb. olabilir. SMS, Soft veya e-Mail ile OTP doğrulaması yapılabilir.
82	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Push Notification yapılıyor mu?	Sistem destekliyorsa, uygulama ihtiyaç duyduğu işlemlerde Push Notification doğrulaması yapabilmelidir. Örneğin login adımında Push Notification kullanılması gibi.
83	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Application-binding yapılıyor mu?	Uygulama içerisindeki kritik fonksiyonların dışarıdan izinsiz bir şekilde tetiklenmemesi, Fonksiyonların kendi uygulamasının dışında bir uygulama ile çalışmaması testleri yapılmalıdır. Raporda bu kısma yer verilmelidir.
84	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, Code Obfuscation and Diversification / Code Lifting yapılıyor mu?	Uygulama kodları tersine mühendislik ve statik kod analizleri ile açığa çıkmamalıdır. Bunun için kullanılan tool ve yöntemler incelenmelidir.
85	Uç noktada çalışan (web tabanlı olsun veya olmasın) uygulamalarda, SSL-pining yapılıyor mu?	Uygulamasının sunucu ile olan iletişiminde kendi özel sertifikalarını kullanacak ve bunların güvenliğini ve bütünlüğünü garanti edecektir. Uygulama, kendi güvenli ve şifreli sertifika deposunu kullanacak, işletim sistemine ait sertifika deposunu kullanmayacak ve tanımlı kök sertifika otoritelerine güvenmeyecektir. Bu kısım için test raporunda detaylı bilgi verilecektir.
86	GMU da, Transaction Data Signing yapılıyor mu?	Uygulama, işlemlerin takibi için dijital olarak her işlemi imzalayacak ve bu imzayı sunucuda saklayacaktır. İmzalı işlemler testler esnasında kontrol edilecektir.
87	Sisteme ait dışarıya açılan tüm servisler için sızma testleri yapılmış mıdır?	Sızma testi Test Kuruluşu tarafından da yapılabilir veya Sızma Testi raporları kontrol edilebilir.

88	Sisteme ait işlem esnasında kullanılan tüm servisler için yük testleri yapılmış mıdır?	Yük testi Test Kuruluşu tarafından da yapılabilir veya Yük Testi raporları kontrol edilebilir.
89	Sisteme ait servisler için fonksiyonalite testleri yapılmış mıdır?	Fonksiyonel test süreçleri dokümanında yer alan testler yapılmalıdır.
90	Sisteme ait servisler için selftest modülü var mıdır?	Self test modülleri ile testlerin yapılabildiği görülmelidir ve sonuçları incelenmelidir. Test raporunda self test sonuçlarına yer verilmelidir.
91	Sistem işleticisinin, test ortamı var mı?	Testler esnasında görülmelidir. Ortam gereksinimleri başvuru dokümanı ve Kılavuz bütüncül olarak incelenerek belirlenmelidir. Ortama ilişkin bilgiler raporlanmalıdır.
91	Sistem işleticisinin, canlı ortamı yedekli mi?	Başvuru belgeleri kontrol edilecektir.
93	Sistem işleticisinin, FKM ortamı var mı?	Başvuru belgeleri kontrol edilecektir.
94	Sistem işleticisi, GİB tarafından saklaması gereken verileri güvenli bir şekilde ve yedekli olarak saklayabilecek bir altyapı ve yazılım mimarisi kurgulamış mı?	Başvuru belgeleri kontrol edilecektir.
95	Sistem işleticisi, sakladığı verilere ilişkin hash değerlerini, zaman, tutar ve id alanlarını içerecek şekilde ve değişmezliğini temin edecek güvenlik seviyesinde, anahtar kullanarak saklıyor mu?	Sistemin merkez mimarisi ve veritabanı incelenecek kılavuzda geçen verilerin fonksiyonel ve güvenlik kriterlerine uygun şekilde saklandığı kontrol edilecektir.
96	Sistem işleticisi, GİB' in talep ettiği verileri sisteminden GİB'e ulaşana kadar güvenli bir şekilde iletilmesini sağlıyor mu?	GİB' e sunulan servislerin güvenliği ve kullanılan yöntemler incelenecektir.
97	Sistem işleticisi, GİB' in belirlediği otoritelere test ve doğrulama aşamalarında sunduğu verileri, kişisel verilerin güvenliğini bozmayacak şekilde ve güvenli bir ortamda sunuyor mu?	Denetçi ve otorite kuruluşlarına açılan verilerin, kişisel verilerin güvenliğini bozmayacak şekilde incelemeye sunulduğu gösterilmelidir.
98	Sistem işleticisi, 3rd entegrasyonlarında kendi sağladığı hizmetler için veri güvenliğini uçtan uca sağlıyor mu?	3rd entegrasyon servislerinin güvenliği ve kullanılan yöntemler incelenecektir.