Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi

İşletici Kuruluş Sistemi Güvenlik Test Süreçleri Dokümanı

Versiyon 1.0

(21.05.2020)

1) GİRİŞ

Bu doküman, İşletici Kuruluşlar ile Başkanlık tarafından Sistemi test etmek üzere yetkilendirilmiş test kuruluşları için düzenlenmiştir. İşletici Kuruluşların Sistemlerine ait güvenlik testleri bu doküman temel alınarak yapılmalı ve raporlanmalıdır.

Test Kuruluşu raporunu oluştururken bu doküman yanında Güvenli Mobil Ödeme ve Elektronik Belge Yönetim Sistemi Başvuru, İzin, Onay ve Denetim Süreçleri Kılavuzundan ("Kılavuz") da yararlanmalı ve ürettiği sonuçların Kılavuz ile uyumlu olduğunu dikkate almalıdır.

Test Kuruluşu, raporuna temel oluşturacak testlerini yaparken en az Test Gereksinimleri ve Adımları başlığında tanımlanan test adımlarını uygulamalı ancak sadece bunlara bağlı kalmak zorunda olmadığından testini bunlarla sınırlamamalıdır. Test Kuruluşu yapmış olduğu testler sonucunda ilgili konulardaki uyumluluğun sağlandığını teyit edeceğinden, kendisinin uygun göreceği ya da test esnasında ortaya çıkan ve detaylandırılması gereken konularda ek testler yapması beklenmektedir. Test Kuruluşu, Kılavuz ve bu doküman gereksinimleri ile bütünlük içinde değerlendirmesi sonucunda düzenlemiş olduğu raporun eksiklik, belirsizlik ve tutarsızlık içermeyen doğru bilgilerle oluşturulduğunu taahhüt eder.

Test Kuruluşu tarafından düzenlenecek raporlar, sunulan Sistemin istenilen güvenlik gereksinimlerine uygun olduğuna dair kanıtları sunmalıdır. Bu nedenle, Test Kuruluşunun kapsamlı bir teknik ve kalite güvence incelemesi yapması gerekir.

İşletici Kuruluş, test süre ve süreçlerinin uzamasından kaçınmak amacıyla, Test Kuruluşu ile gerekli işbirliğini yapmalı, Test Kuruluşu tarafından talep edilen bilgi ve belgeleri zamanında ve eksiksiz şekilde sağlamalıdır. Test Kuruluşunun yapacağı kod analizi testleri için; İşletici Kuruluş bu analize katılarak kodlarını açabileceği gibi dilerse kodlarını Test Kuruluşuna teslim ederek kod analizinin Test Kuruluşu tarafından yapılmasını sağlayabilir.

2) AMAÇ

Sistem üzerinde gerçekleşen tüm mali ve finansal işlemlerin güvenli bir şekilde yapılması ve hassas verilerin güvenli bir şekilde saklanabilmesi gerekmektedir. Bu doküman ile tüm bunlara yönelik testlerin yapılarak Sistemin bu doküman ve Kılavuza uygunluğunun bir sınamadan geçirilmesi amaçlanmaktadır.

Bu dokümanda hem uç cihazlar için hem de Merkezi Bilgi Sistemi için gerekli temel güvenlik gereksinimlerinin test edilmesi hedeflenmektedir.

İşletici Kuruluşlar, bu doküman ve Kılavuz içerisinde tanımlanan güvenlik gereksinimlerine aynen uymak koşuluyla, Başkanlık tarafından yetkilendirilmiş Test Kuruluşuna Güvenlik Gereksinimi Testlerini yaptırmak ve onaylatmak zorundadır.

Uç noktada kullanılan cihazların güvenlik gereksinimi açısından cihaz üreticisi tarafından sağlanan güvenlik önlemleri, sertifikaları ve/veya çözümleri de İşletici Kuruluş tarafından Test Kuruluşuna sunulabilir. Test Kuruluşu test ve değerlendirmelerini bu yönde yapmalıdır.

Açıkça ifade edilmelidir ki; Uç noktada cihaz, ödeme uygulaması veya farklı bir uygulama ile ilgili bir sertifika veya güvenlik testi yapılmış olması(PCI PTS, CPoC, vb..); Kılavuz kapsamında geliştirilmiş olan GMU'nun, ödeme uygugulamalarını, satış uygulamalarını ve e-Belge entegrasyonlarını güvenli bir şekilde yaptığı anlamına gelmemektedir. Bu sebeple GMU için uygulanacak güvenlik testleri aynen geçerli olacaktır. Şöyle ki; diğer sertifikasyonlar, kullanılan Secure Element, SAM kart, WBC vb. kripto altyapılarının GMU için de kullanılması, sistem güvenliği için büyük oranda katkı sağlayacak ve testlerde temel alıncaktır.

3) TEST RAPORU ve İÇERİĞİ

Test Kuruluşunun yapacağı testler sonucunda düzenleyeceği rapor, güvenlik gerekliliklerine uygunluğu göstermelidir. Tüm test gereklilikleri için Test Kuruluşu, herhangi bir sonucun nasıl elde edildiğini göstererek sonuçları doğrulamak için doğrudan testler ve teorik iddialar hakkında yeterli bilgi sunmalıdır. Test uzmanı uygun testleri belirlemeli ve test gerekliliklerinin ve yöntemlerinin test gerekliliklerine dayanarak neden geçerli olduğunu belgelemelidir. Her test gereksinimi için raporda belirtilen değerlendirme sonuçları, anlaşılması ve doğrulanması için yeterli kanıtla desteklenmelidir. Bu kanıtlar, bunlarla sınırlı olmamak üzere, aşağıdakileri içermelidir:

- İşletici Kuruluş tarafından sağlanan bilgiler ve test gereksinimlerine dair referanslar,
- Test edilen bileşenin, güvenlik gereksinimlerine uygun olduğuna dair kanıtların açıklamaları,
- Uygulanan koruma yöntemleri, yazılım mimarisi ve işletim sistemi dâhil ancak bunlarla sınırlı olmamak üzere ilgili sistem özelliklerinin doğru tanımları,
- Beyaz kutu (White-box) yaklaşımları kullanılması durumunda, bu yaklaşımların neler olduğu ve bunların nedenleri dâhil olmak üzere test faaliyetlerinin kapsamı ve odağı ve saldırı hipotezlerinin ayrıntılı açıklamaları,
- Kaynak kod analizi ve sonuçları,
- Sızma testi yapmak için alınan kararların detayları, kullanılan yöntemler ve sızma testi sonuçları,
- Uygulamalı test yerine teorik analize dayalı her türlü sonuca ilişkin açıklamalar,
- İstisnai durumlarda geçerli olmak üzere, doğrudan test faaliyetlerinden elde edilmeyen, ancak İşletici Kuruluş tarafından sunulan kanıt veya taahhütlere güvenmenin gerekçesi ya da gerekçeleri.

Test raporunun, değerlendirmeyi açıklayan ekran görüntüleri ve / veya diğer grafikler, resimler de dâhil edilerek zenginleştirilmesi talep edilmektedir. Ekran görüntüsü, grafik ve resimlerin yeterli kalitede olması gerekmektedir.

Test Kuruluşu üstlenmiş olduğu görevin bilinci ile yapacağı testler ve düzenleyeceği rapordan Başkanlığa karşı sorumludur.

Test raporunda güvenlik test sonuçları maddeler halinde yer almalıdır. Ancak test sonucuna ilişkin bir hüküm yer almamalıdır. Varsa kritiklik seviyelerine göre bulgular ve bulgulara sebep olan açıklamalar yer almalıdır.

Yine test raporunda bulgulara ilişkin çözüm önerileri ve yönlendirmelere ilişikin açıklamalar da yer alabilir.

Test Kuruluşu tarafından düzenlenen ve Başkanlığa iletilen raporun sonucunda Başkanlık aşağıdaki üç duruma karar verebilir:

- İşletici Kuruluş güvenlik testlerinin başarılı bulunup, test onayının verilmesi.
- İşletici Kuruluş güvenlik testlerinin kısmen başarılı bulunup, geçici onay verilmesi ve 3 ay içerisinde tekrar test sürecine girilmesini talep etmesi.
- İşletici Kuruluş güvenlik testlerinin başarısız bulunup, tekrar test sürecine girilmesini talep etmesi.

4) GEREKLİ EN DÜŞÜK TEST GEREKSİNİMLERİ VE ADIMLARI

Sistem uç nokta ve arka uçta yer alan yazılımlardan, bunların birbirleriyle ve diğer Sistem bileşenleriyle uyumlu şekilde çalışmasından ve bu çalışma esnasında işlenen ve üretilen verilen güvenli bir şekilde saklanmasını sağlayan birimlerden oluşmaktadır. Her İşletici Kuruluş, Sistemin güvenliğini, verilerin doğruluğunu, bütünlüğünü ve değiştirilemezliğini taahhüt ettiğinden, kendisine ait Sistem topolojisi içerisinde kendi mimarisini oluşturur.

Bu bölümün amacı, Sistemin Kılavuzda tanımlandığı şekilde çalıştığını güvence altına almak için bir takım ilke ve gereksinimleri uygun şekilde test edilmesini sağlamaktır. Bu bölümde açıklanan güvenlik gereksinimlerine dair testler, işlemlerin bütünlüğü ve güvenliğini ön planda tutarak, Sistemde işlenen hassas mali ve finansal verilerin gizliliğini ve bütünlüğünü korumak için bir güvenlik çerçevesi sağlandığını sınar. Test Kuruluşu, bu bölümde ana hatları verilen test gereksinimlerini baz alarak kendi yöntem ve araçları ile testlerini yaparlar. Test Kuruluşunun görevi yaptığı sınamalardan elde ettiği sonucu objektif bir şekilde sonuç raporuna yansıtmasıdır.

Güvenlik gereksinimleri, Kılavuzun yayınlandığı tarih itibariyle bilinen saldırı senaryoları ile güvenlik açıklarına yönelik olarak düzenlenmiştir. Başkanlık, yeni tehdit ve/veya güvenlik açıklarının ortaya çıkması ile veya uygun gördüğü durumlarda, burada tanımlanan güvenlik testi gereksinimlerini gözden geçirmeye, değiştirmeye, ek testler talep etmeye karar verebilir.

Güvenlik testi gereksinimleri birden fazla bölümde toplanmaktadır. İşletici Kuruluşun Sisteminin aşağıda sıralanan tüm bu bölümlerdeki testleri başarı ile tamamlaması beklenmektedir.

a. Temel Güvenlik Gereksinimleri
b. Güvenli İletişim
c. Anahtar ve Sertifika Yönetimi
d. Veri güvenliği

A. TEMEL GÜVENLİK GEREKSİNİMLERİ

1. Operasyonel Yönetim

1.1. Test Kuruluşu, İşletici Kuruluşun ilgili kılavuzları hazırladığını ve bu kılavuzların test edilen Sistem ile uyumlu ve kullanıcılar için de yeterli olduğunu test etmelidir.

1.2. Test Kuruluşu, uç nokta güvenliğine yönelik hazırlanan gerekli doküman ve diyagramların Kılavuz ve bu doküman kapsamında geçerli ve yeterli olduğunu test etmelidir.

1.3. Test Kuruluşu, Güvenli Mali Uygulama yaşam döngüsü içerisinde; geliştirme ortam güvenliği, kaynak kod güvenliği, versiyon yönetimi, değişiklik yönetimi, erişim kontrolü için gerekli prosedürlerin tanımlandığını test etmelidir.

1.4. Test Kuruluşu, Sistem ile ilgili olası uygulama hataları ve güvenlik açıklarının İşletici Kuruluşa bildirilebileceği bir ara yüz (portal, e-posta adresi, vb.) sunulduğunu test etmelidir.

Bu ara yüzden yapılan bildirimlerin İşletici Kuruluşa iletildiği test edilir.

Bu iletimden sonra da ilgili kişi ve birimlere dağıtımlarının yapıldığı bir yöntem tanımlı olmalıdır.

1.5. Test Kuruluşu, İşletici Kuruluşun risk değerlendirme, yazılım ve son kullanıcı kullanım kılavuzu güncelleme politikası, iç test gibi operasyonel süreçlerini belgelendirdiğini ve bunların uygunluğunu test etmelidir.

2. Uygulama Bütünlüğü

2.1. Test Kuruluşu, Güvenli Mali Uygulamanın uç noktaya güvenli bir şekilde kurulabildiğini test etmelidir.

2.2. Test Kuruluşu, GMU'nun bileşenlerinin GMU kontrolünde güvenilir bir uygulama mağazasından yüklenip yüklenmediğini test eder. Güvenli olmayan bir mağazadan indirilen uygulamanın çalıştırılmamasının sağlandığı test etmelidir.

2.3. Test Kuruluşu, GMU'nun aşağıdaki güvenlik kontrollerini doğru bir şekilde yaparak merkezi sistemine iletebildiğini test etmelidir:

2.3.1. Cihaz "rooted" olarak tabir edilen yöntemle manipüle edilmekte midir?

2.3.2. Cihaz "jailbreak" olarak tabir edilen yöntemle manipüle edilmekte midir?

2.3.3. Cihaz üzerinde bir hata ayıklayıcı (debugger) yüklü ve/veya çalışmakta mıdır?

2.3.4. Uygulama kurcalaması yapılmış mıdır?

2.4. Test Kuruluşu, GMU'nun çalışma zamanı bütünlüğü kontrolleri (run-time integrity checks) yaptığını ve işlevsel bir değişiklik tespit etmesi halinde kontrollerin sonuçlarını Merkezi Sistemine ilettiğini test etmelidir.

2.5. Test Kuruluşu, GMU'nun uygulama dosyalarını tersine mühendislikten koruduğunu test etmelidir.

2.6. Test Kuruluşu, GMU'nun hassas ve referans olarak kullanılan verileri yetkisiz değişiklikleri önlemek için uygulama içerisinde güvenli bir şekilde sakladığını test etmelidir.

3. İşlem Sırasında Hassas Verilerin Korunması

3.1. Test Kuruluşu, GMU'nun mali ve finansal işlemler sırasında Kişisel Veri, Tutar, Mali Veri, TCKN vb. gibi hassas verilerin alınma anı ile ilgili güvenlik önlemlerini sağladığını test etmelidir.

3.2. Test Kuruluşu, GMU'nun hassas veriler kullanımı sonrasında güvenli bir şekilde sildiğini ve işlem sırasındaki izinler dışında uygulama belleğinde tutmadığını test etmelidir.

3.3. Test Kuruluşu, GMU'nun hassas verileri Sistemin bir paydaşı olan ilgili taraflar dışında üçüncü partilerin sistemleri ya da yazılımları ile paylaşmadığını test etmelidir.

GMU'nun, hassas verileri Sistem paydaşları ilgili veri – paydaş ilişkisi çerçevesinde paylaşım yapıldığı, paydaşlara kendilerini ilgilendirmeyen verilerin iletilmediğini test etmelidir.

3.4. Test Kuruluşu, GMU'nun hassas verileri kaynak koduna gömmediğini test etmelidir.

3.5. Test Kuruluşu, GMU'nun diğer uygulama ve kullanıcıların erişimini engellemek amacıyla çalışma zamanı veri koruması (run-time data protection) yaptığını test etmelidir.

3.6. Test Kuruluşu, kullanıcı arayüzü koruması (UI Protection) yapıldığını test etmelidir.

GMU tarafından oluşturulan kullanıcı arayüzüne, hassas bilgilere GMU dışındaki yetkisiz kişi, işlem ve uygulamaların erişilemeyeceği şekilde yalıtım sağlandığını ve verilerin güvence altına alındığını test etmelidir.

3.7. Test Kuruluşu, GMU'nun web tabanlı bir arayüze sahip olması durumunda, HTML üzerinden yapılan tüm yetkisiz ve harici URL isteklerini durdurulduğunu ve bu isteklerin işletim sistemine veya internete iletilmesinin engellendiğini test etmelidir.

3.8. Test Kuruluşu, GMU'nun web tabanlı bir arayüze sahip olması durumunda, kendisine ait olmayan herhangi bir Java Script kodunun başka bir kişi/uygulama/işlem tarafından enjeksiyonunun ve yürütülmesinin önlendiğini test etmelidir.

4. Uç Nokta Güvenliği

4.1. Test Kuruluşu, GMU'nun desteklediği platform ya da platformların (Android, iOS, Linux vb. gibi) neler olduğunu teyit etmeli ve bunu raporlamalıdır.

4.2. Test Kuruluşu, Sisteme bağlı olarak uç noktada çalışan her bir uygulamanın çalıştığı ortama ait parmak izi (fingerprint) verilerini kullanarak, GMU'nun ve bağlı bileşenlerinin uç noktada güvenli bir şekilde çalışmasını ve uç nokta doğrulamasını sağlayabildiğini test etmelidir.

4.3. Test Kuruluşu, uç noktadaki cihaz üzerinde bir veri tutulması durumunda bu verinin saklanmasında anahtar kullanıldığını test etmelidir.

4.4. Test Kuruluşu GMU'nun ve bağlı bileşenlerinin kullanıcı adı, şifre, anahtar, kişisel veriler, mali veriler vb. hassas bilgiler saklanıyorsa veya işleniyorsa bu verilerin güvenli bir şekilde saklanabildiğini ve korunabildiğini test etmelidir.

4.5. Test Kuruluşu GMU ve bağlı bileşenleri için Root Detection yapıldığını ve GMU'nun rootlanmış cihazlarda çalışmadığını test etmelidir.

4.6. Test Kuruluşu GMU ve bağlı bileşenleri için, kurulduğu cihazı tanımlayabilecek veriler sağlandığını (Device Identification) test etmelidir.

4.7. Test Kuruluşu GMU ve bağlı bileşenleri için, başarılı kurulmuş bir uygulama gibi davranıp farklı lokasyondan işlem yapmasına müsaade etmemesini sağlayacak (Geolocation) bir mekanizmaya sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.8. Test Kuruluşu GMU ve bağlı bileşenleri için, uygulama ile kurulduğu cihazı birbirine bağlayan eşsiz bir imza üreten ve yapılan bir işlemin ilgili cihaza kurulu uygulamadan gerçekleştirildiğini garanti eden bir mekanizma (Device Binding) olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.9. Test Kuruluşu GMU ve bağlı bileşenleri için, yazılımsal veya donanımsal kriptografik depolama / güvenli depolama yapıldığını test etmelidir.

Uygulamalar üzerinde saklanması gereken hassas verilerin güvenli şifreleme algoritmaları ile şifreli ve sadece uygulamanın güvenli bir şekilde okunabileceği ve başka hiç şekilde ulaşılamayan bir alt yapı ile saklandığı test etmelidir.

4.10. Test Kuruluşu GMU ve bağlı bileşenlerinin, herhangi bir debugger ile analiz edilmesini engelleyecek bir mekanizmaya (Anti-Debugging) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.11. Test Kuruluşu GMU ve bağlı bileşenlerinin, emulatör üzerinde çalışmasını engelleyecek bir mekanizmaya (Detect Emulator) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.12. Test Kuruluşu GMU ve bağlı bileşenlerine ait fonksiyonlarının harici bir fonksiyonla çalışma zamanında değiştirilmesini engelleyecek bir mekanizmaya (Detect Hooking) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.13. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulama kodlarının çözülüp yeniden paketlenmesini tespit ederek çalışmasını engelleyecek bir mekanizmaya (Detect Repacking) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.14. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulamanın çalışma zamanında kullandığı hafıza alanından hassas verilerin alınmasını engelleyecek şifreleme, karıştırma ve diğer sisteme bağlı tedbirleri içeren bir mekanizmaya (Secure Runtime Memory) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.15. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulama çalışma zamanında yüklenen uygulama kodunun değişmesini kontrol edip çalışmasını durduracak ve bu durumu Merkezi Bilgi Sistemine bildirecek bir mekanizmaya (Runtime CRC Check) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.16. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulamanın ihtiyaç duyduğu işlemlerde OTP doğrulama yapabildiğini test etmelidir.

4.17. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulamanın ihtiyaç duyduğu işlemlerde, cihazın izin vermesi durumunda Push Notification doğrulaması yapabildiğini test etmelidir.

4.18. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulama içerisindeki fonksiyonların dışarıdan izinsiz bir şekilde tetiklenmemesini, fonksiyonların kendi uygulamasının dışında bir uygulama ile çalışmamasına yönelik bir mekanizmaya (Application Binding) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.19. Test Kuruluşu GMU ve bağlı bileşenlerinin, uygulama kodları tersine mühendislik ve statik kod analizleri ile açığa çıkmamasını sağlamak amacıyla önlemlere (Code Obfuscation and Diversification / Code Lifting) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

4.20. Test Kuruluşu GMU'nun, işlemlerin takibi için dijital olarak her işlemi imzalayacağı ve bu imzayı Merkezi Bilgi Sisteminde saklayacağı bir mekanizmaya (Transaction Data Signing) sahip olduğunu ve bunu başarılı bir şekilde uygulayabildiğini test etmelidir.

B. GÜVENLİ İLETİŞİM

1. Test Kuruluşu, Sistem üzerindeki kritik noktalar arasındaki (GMU, Merkezi Sistem, Özel Entegratör Kuruluş ve (varsa) Üye İşyeri Yapan Kuruluş) ve İşletici Kuruluş tarafından sunuluyor ise GMU'nun Harici Donanım ve/veya Harici Uygulamalar arasındaki iletişimin şifreleme yapılarak kurulduğunu ve iletişimlerin bu sayede korunduğunu test etmelidir.
2. Test Kuruluşu, kurulan güvenli iletişim kanallarının yapısını ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
3. Test Kuruluşu, hassas verilerin ele geçirilmesini engellemek amacıyla birbirleri ile işlem yapan arabirimler arasındaki trafiğin izlenmesini önlemek amacıyla kullanılan yöntemleri ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
4. Test Kuruluşu, güvenli iletişim kanallarında kimlik doğrulama yöntemi içerdiğini teyit ederek, uygulamasını ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
5. Test Kuruluşu, her bir güvenli iletişim kanalı için Ortadaki Adam (Man in the Middle) ve Tekrarlayan Saldırısı (Replay Attacks) engellenme yöntemini ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
6. Test Kuruluşu, Sistemin farklı bileşenleri arasında güvenli iletişim kanalı oluşturmak amacıyla kullanılan anahtarların sadece ilgili bileşene ait olduğunu teyit etmeli ve GMU ile diğer bileşenler arasındaki güvenli iletişimin nasıl oluşturulduğunu ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
7. Test Kuruluşu, TLS vb. gibi standart iletişim protokollerinin kullanıldığı yerlerde Sürüm Düşürme Saldırısı (Downgrade Attack / Rollback Attack) yönteminin mümkün olamayacak şekilde engellenmesine yönelik alınan tedbirleri ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.
8. Test Kuruluşu, kullanılan standart iletişim protokollerinin ve versiyonlarının genel olarak bilinen bir güvenlik açığına yol açmadığını denetlemeli ve bunu raporlamalıdır.

C. ANAHTAR ve SERTİFİKA YÖNETİMİ

İşletici Kuruluşun sunmuş olduğu Sistemde işlemlerin güvenli bir şekilde yapılması, işlem verilerinin korunması, gizliliği ve bütünlüğünün sağlanması kritik önemde bir role sahiptir. Bu amaçlarla kullanılan anahtarlar ve sertifikaların yönetimi, Sistemin güvenliği üzerinde önem arz edecektir.

1. Sertifika Yöntemi

   1.1. Test Kuruluşu İşletici Kuruluşun Kılavuza uygun şekilde;

   - Tübitak KamuSM için uygun formatta sertifika talep dosyası üretme,
   - Tübitak KamuSM tarafından üretilen sertifikayı güvenli bir şekilde alarak saklama ve gerekmesi durumunda imha edilme,

- Güvenli bir şekilde sakladığı İşletici Kuruluş Güvenli Mali Sertifikasından, yapılan her bir işlemin imzalanmasını ve kullanılan yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.

1.2. Test Kuruluşu yapılan her bir işlem için imza yöntemi ile Güvenli Mali Sertifika, mükellef VKN, cihaz marka – model ve seri numarası eşleşmesini güvenli bir şekilde kayıt alabildiğini ve saklayabildiğini test etmelidir.

1.3. Test Kuruluşu, Güvenli Mali Uygulamanın her bir işlemi kendisinden beklendiği şekilde imzalayabildiğini test etmelidir.

1.4. Test Kuruluşu, GMU tarafından imzalanarak Merkezi Sistemde saklanan işlemlere ait imzaların doğrulanabildiğini test etmelidir.

1.5. Test Kuruluşu, yapılan her bir işleme ait imzanın, işleme ait kılavuzda yer alan bilgileri içerdiğini test etmelidir.

2. Anahtar Yönetimi

2.1. Test Kuruluşu, Sistem içerisinde sadece onaylı ve doğruluğu kanıtlanmış ve Başkanlık tarafından tanınan algoritmalar kullanıldığını test etmelidir.

2.2. Test Kuruluşu, İşletici Kuruluş tarafından kullanılan tüm anahtarlar için anahtar amaç ve bütünlüğün sağlanma yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.

2.3. Test Kuruluşu, GMU tarafından kullanılan rastgele sayıların üretilmesinde kullanılan onaylı rastgele sayı üretme (RNG) algoritmaları veya kütüphanelerini ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.

2.4. Test Kuruluşu, whitebox kriptoloji tekniği kullanılması durumunda bu amaçla kullanılan anahtarlar hariç olmak üzere, diğer tüm gizli şifreleme anahtarlarının ve özel şifreleme anahtarlarının benzersiz olduğunu test etmelidir.

2.5. Test Kuruluşu, Sistemde kullanılan her bir anahtara ait yükleme yöntemi ve prosedürünü ayrıntılı olarak raporlamalı ve uygunluğunu test etmelidir.

2.6. Test Kuruluşu, tüm simetrik ve asimetrik kök/ana anahtarların güvenli bir şekilde saklanma yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.

2.7. Test Kuruluşu, Sistemde kullanılan asimetrik anahtarların her biri için anahtarın iptal edilme yöntemini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.

2.8. Test Kuruluşu, tüm anahtar yönetim işlemleri için yetkisiz değişikliklere veya silinmelere karşı bütünlük koruması içerek şekilde denetim amaçlı iz kayıtları oluşturma yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.

D. VERİ GÜVENLİĞİ

Sistem mali ve finansal hassas veriler içermesi ve bu verilerin sızmasının bilgi gizliliğini ihlal etmesi yanında verilerin açığa çıkmasının ulusal güvenlik problemi yaratabilme potansiyelinden dolayı veri güvenliğinin sağlanması kritik derecede önemlidir.

1. Test Kuruluşu, veri bütünlüğünün uç noktadan merkezi sisteme kadar uçtan uca ve güvenli bir şekilde sağlanma yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.
2. Test Kuruluş, TCKN, e-posta, telefon numarası, adres, kart numarası gibi her tür hassas verinin anahtar kullanılarak şifreli bir şekilde güvenli ortamlarda saklanma yöntemlerini ayrıntılı bir şekilde raporlar ve uygunluğunu test eder.
3. Test Kuruluşu, her tür hassas veriye yetki bazlı erişimin sağlanma ve bu erişimlerinin iz kayıtlarının saklanma yöntemlerini ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.
4. Test Kuruluşu, her bir tür hassas verinin açık metin olarak değil, maskeli ve özet değerleri gösterildiğini test etmelidir.
5. Test Kuruluşu, hassas verilerin korunması ve yönetilmesine dair İşletici Kuruluş ve/veya Dış Hizmet Sağlayıcısı tarafından sağlanan belgelendirilmiş politikaları ayrıntılı bir şekilde raporlamalı ve uygunluğunu kontrol etmelidir.
6. Test Kuruluşu, hassas verilerin saklandığı ortamın güvenliğinin sağlanması, izlemesi ve bunların sürdürülebilir olması için alınan önlemleri ayrıntılı bir şekilde raporlamalı ve uygunluğunu kontrol etmelidir.
7. Test Kuruluşu, hassas verilerin işlenmesinden, yönetiminden sorumlu şirket içi personel değişikliklerinde, Sisteme yeni donanım ve/veya ağ bağlantıları eklenmesi gibi durumlarda hassas verilerin korunması ve güvenliğinin sağlanması amacıyla alınan tedbir ve uygulanan yöntemleri ayrıntılı bir şekilde raporlamalı ve uygunluğunu kontrol etmelidir.
8. Test Kuruluşu, sistem mimarisi ve güvenlik kontrol noktalarını destekleyen ağ ve veri akış diyagramlarını ayrıntılı bir şekilde raporlamalı ve uygunluğunu test etmelidir.
9. Test Kuruluşu, açık metin şeklindeki verilerin yetkilendirilmemiş / izin verilmemiş bir kanal ya da yöntem üzerinden Merkezi Sistemden dışarı çıkartılmasını anlayacak, ayrı verecek ve bunu engelleyecek mekanizmaları ayrıntılı bir şekilde raporlamalı ve yeterliliğini test etmelidir.
10. Test Kuruluşu İşletici Kuruluş tarafından her 6 ayda bir sızma testleri yapılması için alınan tedbirleri ayrıntılı bir şekilde raporlamalı ve uygunluğunu kontrol etmelidir.
11. Test Kuruluşu, Merkezi Sistemde saklanan verilere için dosya bütünlüğü izleme mekanizmalarına ait yöntemleri ayrıntılı bir şekilde raporlamalı ve yeterliliğini test etmelidir.

12. Test Kuruluşu, Merkezi Sistem üzerinde kötü amaçlı yazılımların çalışmasını tespit etmek, önlemek ve kaldırmak için alınan tedbirleri ayrıntılı bir şekilde raporlamalı ve yeterliliğini test etmelidir.
13. Test Kuruluşu, Merkezi Sistemin güvenlik açıklarını derecelendirme ve oluşması durumunda tespit etmeye dayalı yöntemlerini ayrıntılı bir şekilde raporlamalı ve yeterliliğini test etmelidir.