ZBEÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI
ANAHTAR YÖNETİM PROSEDÜRÜ

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

1. AMAÇ:

Bu prosedürün amacı, Bilgi Güvenliği Yönetim Sistemi dâhilinde bilgilerin gizliliğinin, bütünlüğünün ve doğruluğunun korunması için kriptografinin düzgün ve etkili bir şekilde kullanılmasını sağlamak için gereken kontrolleri tanımlamaktır. Bilgiye erişimi kontrol etmek için yöntemlerin oluşturulmasıdır.

2. KAPSAM:

Kapsam dâhilindeki tüm bilgi varlıklarıdır.

3. TANIMLAR:

Bilgi: Kurum **s**üreçlerinin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir varlıktır.

Bilgi varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, yedeklemelerinde tutulan ve kurumun iş süreçlerindeki formlarda işlenen veridir.

Denetim Kaydı: Bir Bilgi varlığına kimin eriştiğini veya erişmeye çalıştığını ve erişim sağlayan kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtlar.

Genelge: 06.07.2019 Tarihli ve 30823 Sayılı Resmi Gazete 'de yayımlanan 2019/12 sayılı Cumhurbaşkanlığı Genelgesi.

Rehber: Bilgi ve İletişim Güvenliği Rehberi

NES: Nitelikli Elektronik Sertifika

Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları.

Fiziksel varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri).

Servisler (Hizmetler): Bilgi işleme ve haberleşme servisleri (web servisi, e-mail servisi, ftp servisi),

İnsan: Kurum çalışanları.

Süreçler: Kapsam dâhilinde ZBEÜ Bilgi İşlem Daire Başkanlığında ve ilgili gruplarda gerçekleştirilen ve bilgi varlıkları ile ilgili olan tüm süreçler.

Departman: Bilgi varlığının kurum içinde hangi birime ait olduğunu gösterir.

Varlık Adı: Departmandaki bilgi varlığının adı. (ör: yazıcı, form…)

Lokasyon: Bilgi varlığının hangi lokasyonda olduğunu gösterir. (ör: merkez, FKM)

Kategori: Varlığın kategorisinin belirtir. (ör: donanım, yazılım, uygulama, süreç, bilgi)

4. SORUMLULAR:

Bu prosedürün uygulanmasından Bilgi Güvenliği Kurulu başta olmak üzere tüm personel sorumludur.

5. KRİPTOGRAFİK ALGORİTMALAR ve KULLANIMI:

5.1. Kriptografik algoritma seçimi; algoritma kullanım amacı, algoritmayı kullanacak taraflar ve bu kapsamda işlenecek bilgi/verinin kritiklik seviyesi göz önünde bulundurularak yapılmalıdır. (Rehber:4.4.1.1) Ayrıca Kurum bünyesinde, standartlaştırılmış ve güvenli kriptografik algoritma takımında yer alan algoritmaları barındıran uygulama, cihaz ve sistemler kullanılmalıdır. Standartlaştırılmış ve güvenli kriptografik algoritmalara yönelik endüstri standartları ve en iyi uygulama örnekleri dikkate alınmalıdır.

5.2. Kullanılacak standart kriptografik algoritmaları içeren kripto modüllerinin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/EC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır. (Rehber:4.4.1.3)

5.3. Kritik bilgi/veri işleyen kurumların, kritiklik seviyesine uygun tipte milli kriptografik algoritmaların gerçeklendiği cihazlar temin edilmelidir. Yetkili kripto analiz laboratuvarından güvenli şekilde kullanılabileceğine dair kripto analiz raporu bulunan milli kriptografik algoritmaların donanımsal olarak gerçeklendiği bu kripto cihazların, yetkili laboratuvar tarafından yapılan COMSEC güvenlik testlerinden başarılı bir şekilde geçmiş olmaları gerekmektedir. (Rehber:4.4.1.4)

6. UYGULAMA:

6.1. Son kullanıcı sertifikaları Kamu Sertifikasyon Merkezinden alınır.

6.2. e-İmza, sayısal sertifika kullanılarak üretilir ve imzayı atan kişinin yaptığı işlemi inkâr etmesini önler. Nitelikli Elektronik Sertifika (NES) kullanılarak atılan imzalar, güvenli elektronik imza olarak adlandırılır ve 5070 sayılı Elektronik İmza Kanunu uyarınca elle atılan imza ile eşdeğerdir.

6.3. Tüm bu kriptografik işlemler (simetrik/asimetrik şifreleme, özetleme, e-İmza vb.) çeşitli yazılım ve bazen de donanımların kullanılması suretiyle yapılır. Yapılan kriptografik işlemin beklenen faydayı sağlaması için güçlü kriptolama algoritmaları seçmek ve seçilecek algoritmaya göre yeterli koruma sağlayacak uzunlukta anahtar kullanmak gerekir.

6.4. Güvenli ağların, güvensiz bir ağ üzerinden haberleşmesinin gerekmesi durumunda VPN teknolojileri kullanılmalıdır. (Rehber:4.4.3.1)

6.5. Kullanılan kriptografik ürünlerin işlediği verinin gizlilik derecesine uygun olarak kullanılmasını sağlamak amacıyla ilgili güvenlik değerlendirmesi ve gizlilik derecesi ile uyumlu olarak onay sürecinin işletilip işletilmediği kontrol edilmelidir.

6.6. Kriptografik algoritmaların ve protokollerin en güncel ve güvenli olan versiyonlarının kullanımı sağlanmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir. Sistemde kullanılan taşıma katmanı protokollerine ait sürümler belirli aralıklarla değerlendirilmeli ve denetlenmelidir.

6.7. Kullanılan kriptografik ürünlerin kullanım durumları, versiyon kontrolü, güvenlik değerlendirmesi ve onay durumu gibi bilgilerin takibi ve raporlaması envanter yönetim sistemi ile yapılmalıdır. Envanter yönetim sistemine yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.

7. ŞİFRELEME ve ANAHTAR YÖNETİMİ:

7.1. Kriptografik anahtarlar üretilirken; kullanım amacına uygun, bilgi güvenliği gereksinimlerini karşılayacak seviyede, ulusal ve uluslararası düzeyde kabul görmüş anahtar uzunlukları kullanılmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir.

7.2. Anahtar üretim aşamasında, anahtarın tahmin edilebilir olmasını engellemek için anahtarın entropisinin anahtar boyundan daha düşük olmaması sağlanmalıdır. Üretim esnasında ulusal ve/veya uluslararası standartlar kapsamında kabul görmüş ve yetkili test ve değerlendirme merkezi tarafından güvenlik testleri yapılmış bir gerçek rassal sayı üreteci "True Random Number Generator (TRNG)" veya sanki rassal sayı üreteci "**Pseudo Random Number Generator**" kullanılmalıdır.

7.3. Anahtar üretim ve dağıtım cihazlarının bulunduğu fiziksel ve elektronik ortamlara yalnızca erişim yetkisi olan tarafların erişimi mümkün kılınmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.

7.4. Anahtarın yedeğinin alındığı fiziksel ve elektronik ortamların güvenliği sağlanmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.

7.5. Kriptografik anahtarlara erişim sadece kullanım amacına özel olarak erişim yetkisi tanımlanmış personel ile sınırlandırılmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.

7.6. Kriptografik anahtarlar aşağıdaki maddelerin herhangi birisinin ortaya çıkması durumunda revize edilmelidir;

- ✓ Kriptografik anahtar ile ilgili herhangi bir zafiyet durumu oluşması ya da zafiyet şüphesinin olması
- ✓ Kriptografik anahtarlara erişim yetkisi olan personelin kurumdan ayrılması veya görev değiştirmesi
- ✓ Kriptografik anahtarların, kullanım periyodunun tamamlanması ile birlikte geçerlilik sürelerinin dolması

7.7. Anahtar dağıtım protokolünün analiz edilerek güvenli olması sağlanmalıdır. Gizli kriptografik anahtar bir ağ ortamından iletilecek ise trafik iki uç arasında şifreli ve araya girme saldırılarına karşı korumalı olmalıdır. Ayrıca, trafiğin şifrelemesi taşınan anahtarın gizlilik seviyesi ile uyumlu olmalıdır. Kullanım amacı ve içerdiği bilgi/verinin kritiklik derecesine göre anahtarın birden fazla parçaya ayrılarak farklı kanallarla iletilmesi sağlanmalıdır. Kriptografik anahtar dijital bir kanal ile iletilmiş ise iletilen anahtarın bütünlük kontrolü yapılmalı ve iletilen anahtarın orijinal anahtar ile aynı olduğu doğrulanmalıdır. Dijital kanal açık bir kanalsa, anahtarın şifrelenmesi de sağlanmalıdır. Anahtar dağıtımı ve üretimi için uygun görüldüğü durumlarda HSM tabanlı bir teknoloji tercih edilerek yukarıda bahsi geçen gereksinimler HSM aracılığı ile sağlanmalıdır. Bu durumda, HSM sistemi uygun şekilde yapılandırılmalı ve erişimleri kontrol altına alınmalıdır.

7.8. Anahtar taşıma cihazları güvenli alanlarda muhafaza edilmelidir. Anahtar taşıma cihazlarına ve depolama medyasına sadece yetkilendirilmiş personelin ulaşabilmesi sağlanmalıdır. Tüm erişim kayıtları tutularak takibinin yapılması sağlanmalıdır.

7.9. Anahtar üretim ortamlarına erişim HTTPS, SSH gibi şifreleme desteği sunan protokoller kullanılarak yapılmalıdır.

7.10. Yasal yükümlülükleri yerine getirmek, şüpheli davranışları tespit etmek ve güvenlik ihlali durumunda adli soruşturma yetenekleri sağlamak için anahtarlar üzerinde gerçekleştirilen yetkilendirme, yetki değişikliği, iptal etme, silme, yedekleme vb. tüm işlemler kayıt altına alınmalıdır.

7.11. Kriptografik anahtarlar, kabul edilebilir sınırlı bir geçerlilik süresine ve/veya kullanım sayısına sahip olmalıdır. Yaşam süresi devam ederken kaybedilen ve/veya saldırgan tarafından kısmen ya da tamamen ele geçirilen bir kriptografik anahtarın iptal işlemi gerçekleştirilmelidir. Yetkisini yitirmiş kriptografik anahtar ve/veya akıllı kart, token vb. kriptografik anahtar ihtiva eden donanımlar geri dönülemez biçimde yok edilmelidir.

7.12. Anahtar dağıtım ve teslim şeklinin imkân vermesi durumunda kriptografik anahtarların sadece gerekli ve geçerli iş amaçları için kullanılacağını, kriptografik anahtarlar ile yapılmış olan tüm işlemlerin sorumluluğunun kişiye ait olduğunu vurgulayan bir zimmet tutanağının hazırlanmalı, kriptografik anahtarların zimmetlendiği personele imzalatılmalıdır.

7.13. Üretilen anahtarların kullanım kabiliyetleri (şifreleme, şifre çözme, imzalama, doğrulama vb.) dokümante edilmeli ve yetkilendirme bu doğrultuda yapılmalıdır.

7.14. Anahtarların üretim yerinden sonra kontrolsüz şekilde kopyalanması ve çoğaltılması engellenmelidir. Anahtar kaç kopya üretildi ise o sayıda dağıtım ve kullanım sağlanmalıdır.

7.15. Anahtar malzemesi elektronik ortamda tutulduğu veri tabanında veya yayımlandığı taşıma ortamlarında açık olarak görülememelidir. (Anahtarı kullanan cihazlara aktarımın kâğıt üzerinde olması durumu kapsam dışıdır.) Açık anahtar görülmesi ihlal kapsamında değerlendirilmelidir ve anahtar kullanımdan çıkarılmalıdır.

7.16. Anahtarların ifşa olması ve anahtar kullanım süreçlerindeki ihlal durumlarını raporlama (compromise reporting) mekanizması kurulmalıdır.

7.17. Anahtar üretim ve dağıtımın hızlı olamadığı uygulamalarda, ihlal/ifşa durumlarında kullanılmak üzere yedek anahtarlar hazırlanmalıdır.

7.18. Kullanılacak anahtar üretim ve yönetim sistemleri ile kripto cihazların yerli ve milli üreticilerden temini tercih edilmelidir. Kullanılacak anahtar üretim ve yönetim sisteminin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/IEC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır.

7.19. Kriptografik anahtar şifreleme anahtarları ile veri şifreleme anahtarları birbirlerinden izole edilmiş ortamlarda saklanmalıdır. Her iki özellikteki anahtar da dışarıdan yapılabilecek müdahaleye karşı korunmuş modüllerde (TRSM) saklanmalıdır. Bu mümkün değilse bilgiyi parçalı olarak korumak gereklidir. Parçalı koruma işleminde parçalar ayrı yerlerde tutulmalı, bilgi kullanılacağı zaman bir araya gelmesi sağlanmalıdır. Üretilen anahtarlar özellikle güvenli saklama için tasarlanmış USB token, akıllı kart vb. teknolojilerde saklanmalıdır. Eğer yazılımsal token vb. bir teknoloji kullanılacak ise ilave olarak hard token da fiziksel olarak sağlanan sahip olma özelliğinin, kişinin bilgisayar, tablet vb. da sağlanması gerekmektedir. Soft token siber saldırılara karşı dayanıklı olmalı ve gizli anahtarı sızdırmamalıdır.