TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

ELEKTRONİK BELGELERİ AÇIK ANAHTAR ALTYAPISI KULLANARAK GÜVENLİ İŞLEME REHBERİ

Doküman Kodu
REH.01.01

Revizyon No
06

Revizyon Tarihi
15.03.2023

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk Çıkış.	01.11.2011
01	Doküman içeriği güncellenmiştir.	05.12.2012
02	Doküman kodu güncellenmiştir.	18.03.2014
03	Doküman içerisinde referans verilen standartların yeni sürümlerinin yayımlanması sebebiyle doküman revize edilmiştir.	27.11.2014
04	Doküman içeriği güncellenmiştir.	09.06.2016
05	Doküman biçimi yeni şablona aktarılmıştır. Doküman kodu güncellenmiştir. Dokümanın eski revizyonları Kamu SM doküman yönetim sisteminde "REHB-001-001" kodu ile yer almaktadır.	01.06.2018
06	Kullanılmayan link ve referanslar güncellenmiş veya kaldırılmıştır. Risk değerlendirme kapsamına dahil olan varlıklar ve zayıflıklara ekleme yapılmıştır. Risk listesi güncellenmiştir. Şifreleme sırasında kullanılan algoritmalar ve örnek şifreleme ASN.1 yapısı güncellenmiştir. Doküman içeriği, CBDDO'nun internet adresinde yer alan 1.4 versiyonu ile paralel olacak şekilde güncellenmiştir.	15.03.2023

TABLOLAR

İÇİNDEKİLER

1 Amaç ve Kapsam

Bu rehber, güvenli bir açık anahtar altyapısı (AAA) kullanılarak üretilen elektronik sertifikaların, bilgisayar ortamında oluşturulan elektronik belgelerin güvenli işlenmesinde nasıl kullanılabileceğini tanımlamak için yazılmıştır.

Rehber, özellikle kamu kurumlarının Kamu Sertifikasyon Merkezi tarafından üretilen elektronik sertifikaları kullanarak elektronik imzalı ve şifreli belge işlemesine yönelik kural önerileri içermektedir. Bununla beraber başka bir güvenli AAA tarafından üretilmiş elektronik sertifikaları kullanan kurum ve kişiler de bu rehberde anlatılan yöntemlerden yararlanabilir.

Bir elektronik belgenin güvenliğini sağlamak için kullanılan uygulama yazılımlarının, akıllı kart, akıllı kart okuyucu vb. cihazların, bilgisayarların, işletim sistemlerinin, ağ altyapısı ve ilgili diğer tüm bileşenlerin güvenliği bu rehberin kapsamı dışındadır. Güvenliğin tam olarak sağlanabilmesi amacıyla bunlar için de güvenlik önlemleri alınmalıdır.

Elektronik belge güvenliğini sağlamak için kullanılan yöntemler bilişim sistemleri güvenliği, fiziksel güvenlik ve idari güvenlik gibi yöntemlerle beraber değerlendirilmelidir. Bu rehberde anlatılan yöntemler kullanılarak güvenliği sağlanacak belgelerin **Hizmete Özel** ve daha alt gizlilik seviyesinde olması önerilmektedir.

Hizmete Özel üstü gizlilik dereceli belgelerin tek başına bu rehberde anlatılan yöntemlerle şifrelenmesi ve kullanılması uygun değildir.

2 Referanslar

[R1] RFC 5652 Cryptographic Message Syntax, Internet Engineering Task Force, Eylül 2009 (www.rfc-editor.org/rfc/rfc5652.txt)

[R2] ETSI TS 101733 (v2.2.1) CMS Advanced Electronic Signatures (CADES), ETSI Electonic Signatures and Infrastructures (ESI), Nisan 2013 (https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf)

[R3] ETSI TS 101903 (v1.4.2) XML Advanced Electronic Signatures (XADES), ETSI Electonic Signatures and Infrastructures (ESI), Aralık 2010 (https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf)

[R4] RFC 3278 - Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS), Internet Engineering Task Force, Nisan 2002 (www.rfc-editor.org/rfc/rfc3278.txt)

[R5] SP800-56A Revision1, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logaritm Cryptography, NIST, Mart 2007

[R6] SECG, “Elliptic Curve Cryptography”, Standards for Efficient Cryptography Group, 2000 (https://www.secg.org/SEC1-Ver-1.0.pdf)

[R7] FIPS 180-3, Secure Hash Standard, NIST, Ekim 2008

[R8] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks

[R9] ETSI TS 119 312 (v1.4.1) Cryptographic Suites, Electronic Signatures and Infrastructures (ESI), Ağustos 2021

3 Tanımlar ve Kısaltmalar

Kamu SM: 2004/21 Sayılı Başbakanlık Genelgesi uyarınca, tüm kamu kurumlarının kurumsal sertifika ihtiyaçlarını karşılamak için TÜBİTAK BİLGEM tarafından kurulmuş olan Kamu Sertifikasyon Merkezi.

İŞA (İçerik Şifreleme Anahtarı): Elektronik belgenin içeriğini simetrik bir algoritmayla şifrelerken kullanılan simetrik anahtar.

AŞA (Anahtar Şifreleme Anahtarı): Elektronik belgede kullanılan İŞA'yı asimetrik bir algoritmayla şifrelemek için kullanılan asimetrik anahtar.

AAA (Açık Anahtar Altyapısı): Asimetrik kripto algoritmalara ait anahtar çiftlerinin yönetimi için oluşturulan genellikle elektronik sertifika kullanan sunucu ve son kullanıcı hizmetleri.

EC (Elliptic Curve): Eliptik eğri matematiğini kullanan asimetrik kripto algoritmaları ailesi.

RSA: Modüler üs alma yöntemlerini kullanan asimetrik kripto algoritması. İmza ve şifreleme için kullanılabilir.

ECDSA (Elliptic Curve Digital Signature Algorithm): Ayrık logaritma ve eliptik eğri kullanan imzalama algoritması.

ECDH (Elliptic Curve Diffie Hellman): Eliptik eğri kullanan anahtar anlaşma algoritması.

SHA (Secure Hash Algorithm): Herhangi bir uzunlukta veriyi girdi olarak alan ve sabit uzunlukta bir değer çıkaran FIPS 180-3[R7]'de tanımlanmış özet hesaplama fonksiyonu.

ASN.1 (Abstract Syntax Notation 1): Elektronik haberleşmede ve bilgisayarlarda veri yapılarını tanımlamak için kullanılan esnek ve standart bir veri kodlama yöntemidir. ISO/IEC X.680 serisi standart belgelerinde tanımı yapılmıştır.

4 Risk Değerlendirme

Bir elektronik belgenin oluşturulması ve kullanılması sırasında karşı karşıya kaldığı çeşitli tehditler bulunmaktadır. Bunlar:

- Kullanılan sistemlerdeki açıklık ve zayıflıklar
- Belge içeriğini yetkisiz kişilerin görmesi
- Belge içeriğini yetkisiz kişilerin değiştirmesi
- Belgeyi hazırlayanın bunu sonradan inkar etmesi
- Belgeyi hazırlayan kişinin kimliğinin doğru bir şekilde belirlenememesi
- Belgenin hazırlandığı tarihin saptanamaması

şeklinde sıralanabilir.

Bu tehditlerin oluşturduğu risklerin derecelendirilmesi, önlenmesi veya risk seviyesinin düşürülmesi için bu rehberde ISO 27005 standardında [R8] belirtilen yöntem temel alınmıştır. Bu yöntem aşağıdaki şekilde özetlenebilir:

- Varlıkları tanımla
- Varlıklarda bulunabilecek zayıflıkları tanımla
- Varlıklarda bulunan zayıflıkları kullanabilecek tehditleri tanımla
- Tehdit ve zayıflıkların varlıklar üstünde oluşturduğu riskleri tanımla
- Tehditlerin gerçekleşme olasılığını tanımla
- Tehditlerin etki derecesini tanımla
- Riskler için tahmini risk değerini belirle ve derecelendirme yap

Bu rehber kapsamında güvenliği sağlanmaya çalışılan varlıklar Bölüm 4.1'de listelenmektedir. Diğer varlıkların güvenliğinin sağlanması bu rehberin kapsamı dışındadır.

Bu rehberde anlatılan tehdit ve zayıflıklar/açıklıklar muhtemel tüm tehdit ve zayıflıkları kapsamamaktadır. Rehber söz konusu bu tehditlere yönelik riskleri azaltacak ya da ortadan kaldıracak önlemleri sunmaktadır.

4.1 Varlıklar

Bu rehber kapsamında güvenliği sağlanmaya çalışılan varlıklar aşağıda listelenmiştir.

- **Elektronik Belge (VAR-EB):** Elektronik ortamda hazırlanan ve elektronik formatta saklanan doküman.
- **Kriptografik Anahtarlar (VAR-KA):** Elektronik belge içeriğini şifrelemede, elektronik belgenin şifresini çözmede, elektronik belgeye elektronik imza eklemede ve elektronik belgenin elektronik imzasını doğrulamada kullanılan asimetrik ve simetrik kripto anahtarları.
- **Akıllı Kart (VAR-AK):** Elektronik belgenin güvenliği için kullanılacak asimetrik anahtarların saklanmasına ve kullanılmasına yarayan, yongaya ve işletim sistemine sahip karttır. Simetrik ve geçici asimetrik anahtarların üretiminde kullanılan güvenli bir donanımsal rasgele sayı üreteci içerir.
- **Donanım Güvenlik Modülü (VAR-DGM):** Elektronik belgenin şifrelenmesi için kullanılacak asimetrik/simetrik anahtarların saklanmasına ve kullanılmasına yarayan donanımsal modüldür. Simetrik ve geçici asimetrik anahtarların üretiminde kullanılan donanımsal rasgele sayı üreteci içerir.
- **Sertifikalar (VAR-SR):** Şifreleme, şifre çözme, elektronik imza oluşturma ve elektronik imza doğrulama işlemlerinde kullanılan sertifikalar ve bunları yayınlayan kök ve alt kök yayıncılara ait elektronik sertifikalar.
- **Uygulama Yazılımı (VAR-UY):** Şifreleme, şifre çözme, elektronik imza oluşturma ve elektronik imza doğrulama işlemlerinde kullanılan ve bilgisayarda koşan yazılım.

Güvenliği sağlanması gereken en önemli varlıklardan biri de Bilgi Sistemleri Altyapısıdır (**VAR-BS**). Elektronik belge, elektronik belgeyi işlemek için kullanılan uygulamayı barındıran işletim sistemleri, işletim sistemlerinin üzerinde çalıştığı donanımlar ve belgenin bir noktadan diğerine ulaştırılmasında kullanılan ağ altyapı bileşenleri bilgi sistemleri altyapısını oluştururlar. Bilgi sistemleri altyapısı ile ilgili riskler yönetilmediği sürece yukarıda belirtilen varlıkların güvenliğinin tam olarak sağlanması mümkün değildir. VAR-BS'nin güvenliğini sağlamak için alınacak önlemler bu rehberin kapsamı dışındadır.

4.2 Zayıflıklar

Zayıflıklar, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Zayıflıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir.

Bu rehberdeki varlıkların barındırabileceği zayıflıklar aşağıda listelenmiştir.

- **ZAY-BS-YGA:** Elektronik belgenin işlendiği bilgisayarda yazılım tabanlı güvenlik açıkları olması (virüslere ve diğer zararlı yazılımlara karşı koruma yazılımlarının yüklü ve/veya güncel olmaması, işletim sistemi sıkılaştırmasının yapılmamış olması, işletim sistemi yamalarının uygulanmamış olması). Bu zayıflığı barındırabilecek varlık VAR- BS'dir.
- **ZAY-BS-DGA:** Elektronik belgenin işlendiği bilgisayarda donanım tabanlı güvenlik açıkları olması (elektromanyetik veya optik ışınımla istenmeyen bilgi kaçakları olması, bilgisayara bağlı çevre donanımlarından bilginin dışarı sızması). Bu zayıflığı barındırabilecek varlık VAR -BS'dir.
- **ZAY-BS-AGA:** Elektronik belgenin işlendiği bilgisayarın bağlı olduğu ağda güvenlik açıkları olması (güvenlik duvarı, saldırı tespit sistemi gibi koruma sistemlerinin kullanılmaması, ağ bölgesine erişimde denetim uygulanmaması). Bu zayıflığı barındırabilecek varlık VAR -BS'dir.
- **ZAY-KR-ALZ:** Zayıf ve yetersiz kriptografik algoritmaların kullanılması veya kriptografik algoritmaların hatalı kullanılması. Bu zayıflığı barındırabilecek varlıklar VAR-AK, VAR-DGM ve VAR-UY'dir.
- **ZAY-KR-AÜY:** Kriptografik anahtar üretim yöntemlerinin güvenli olmaması. Bu zayıflığı barındırabilecek varlıklar VAR-AK ve VAR-DGM'dir.
- **ZAY-KR-GOS:** Kriptografik anahtarların güvensiz bir ortamda saklanması/işlenmesi. Bu zayıflığı barındırabilecek varlıklar VAR-EB, VAR-AK, VAR-DGM, VAR-SR ve VAR-UY'dir.
- **ZAY-KR-YSÖ:** Kriptografik anahtarların kullanıldığı donanımlarda yan kanal saldırılarına karşı önlem alınmamış olması. Bu zayıflığı barındırabilecek varlık VAR- AK'dır.
- **ZAY-AK-EVÇ:** Akıllı kart erişim verisinin (PIN) çalınmasına karşı yazılım ve donanım seviyesinde güvenlik önlemlerinin alınmaması. Bu zayıflığı barındırabilecek varlıklar VAR-BS ve VAR-UY'dir.
- **ZAY-UY-DEĞ:** Uygulama yazılımının elektronik belge, kriptografik anahtar ve sertifika kullanımıyla ilgili fonksiyonlarının değiştirildiğini kontrol etmemesi veya bu durumu fark etmemesi. Bu zayıflığı barındırabilecek varlık VAR-UY'dir.
- **ZAY-UY-SU**: Uygulama yazılımının kaliteli yazılım geliştirme standartlarına ve güvenli kod geliştirme metodolojilerine uygun geliştirilmemesi ve yeterince test edilmemesi. Bu zayıflığı barındırabilecek varlıklar VAR-AK, VAR-DGM ve VAR-UY'dir.

4.3 Tehditler

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar/kişiler ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır:

- **Doğal tehditler:** Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler
- **Çevresel tehditler:** Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.
- **Yasalara uyum ile ilgili tehditler:** Üçüncü taraflarla yaşanan anlaşmazlıklar, faaliyetlerin yasalara uyum göstermemesi vs.
- **İnsan kaynaklı tehditler:** İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılım yüklenmesi, yetkisiz erişimler vs.
- **Teknolojiden kaynaklanan tehditler:** Yazılım ve/veya donanım hataları, veri ve sistem kayıpları, ağ altyapı ve iletişim problemleri vs.

Bu rehber kapsamında belirtilen varlıklara karşı ele alınan tehditlerin kaynağı; teknolojik gelişmeler, varlıkların sahibi olan kişiler, kötü niyetli insanlar veya kötü niyetli kurumlar olabilir. Rehber kapsamında dikkate alınan tehditler aşağıda listelenmiştir.

- **TEH-EB-AHE:** Elektronik belgenin açık (şifresiz) halinin elde edilmesi
- **TEH-EB-VBB:** Elektronik belgenin veri bütünlüğünün bozulması
- **TEH-EB-KD:** Elektronik belgeyi hazırlayan kişinin kimliğinin değiştirilmesi
- **TEH-EB-TD:** Elektronik belgenin var olduğu tarihin değiştirilmesi
- **TEH-KR-ALZ:** Kriptografik algoritmaların zayıflaması
- **TEH-KR-ZYF:** Kriptografik anahtarların kolayca bulunması
- **TEH-KR-KPY:** Kriptografik anahtarların kopyalanması
- **TEH-KR-YAN:** Kriptografik anahtarların yan kanallardan elde edilmesi
- **TEH-AK-EVÇ:** Akıllı kart erişim verisinin (PIN) çalınması
- **TEH-AK-FİY:** Akıllı karta sahibinin isteğinden farklı işlem yaptırma
- **TEH-SR-KSD:** Uygulama yazılımının güvendiği kök sertifikaların değiştirilmesi
- **TEH-UY-DEĞ:** Uygulama yazılımının değiştirilmesi

4.4 Tehdit Gerçekleşme Olasılığı

Risk analizinde bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirmesi yapılır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi, mevcut önlemlerin varlığı ve etkinliği göz önünde bulundurulur.

Bu rehberde olasılık değerlendirmesi için **Tablo 1**'deki ölçütler kullanılmaktadır.

Tablo 1: Tehdit Olasılık Tablosu

	Değer	Açıklama
Çok Düşük (Uzak ihtimal)	**1**	Sadece olağanüstü durumlarda gerçekleşebilir. Tehdit kaynağının motivasyonu çok düşük seviyede ve/veya kabiliyeti az ya da yeterli önemler uygulanmış.
Düşük (Nadiren, Seyrek)	**2**	Tehdit kaynağının motivasyonu düşük seviyede ve/veya kabiliyeti az ya da önlemler kısmi olarak uygulanmış.
Orta (Ara sıra)	**3**	Tehdit kaynağı yeterli motivasyona sahip ve/veya kabiliyeti olumsuz etkilere yol açabilecek kapasitede ya da mevcut şartlarda yeterli önlemler uygulanmış.
Yüksek (Genellikle, Muhtemelen)	**4**	Tehdit kaynağının varlığa saldırma motivasyonu çok yüksek seviyede ve kabiliyeti yüksek ya da önlemler kısmi olarak uygulanmış ama çok yeterli değil.
Çok Yüksek (Sık sık)	**5**	Tehdit kaynağının varlığa saldırma motivasyonu çok yüksek seviyede, kabiliyeti yüksek ya da önlemler uygulanmamış.

4.5 Tehdit Etki Derecesinin Değerlendirilmesi

Etki değerlendirilmesinde, herhangi bir zayıflığın/açıklığın gerçeklenmesi halinde varlıklar üzerinde ortaya çıkabilecek gizlilik, bütünlük, erişilebilirlik kayıplarının olası olumsuz etki seviyesi belirlenir. Bunun için varlığın sahibi tarafından atanan değeri, görevi, kritikliği, varlığın etkilediği verinin hassasiyeti, varlığın mali değeri ve gizlilik, bütünlük, erişilebilirlik kayıplarının sebep olduğu etkiler göz önüne alınır.

Etki derecesinin değerlendirmesi için **Tablo 2**'deki ölçütler kullanılmaktadır.

Tablo 2: Tehdit Etki Değeri Tablosu

	Önemsiz (İhmal edilebilir düzeyde)	**Düşük Şiddette**	**Orta Şiddette**	**Yüksek Şiddette (Önemli)**	**Yıkıcı, Felaket düzeyinde**
	1	**2**	**3**	**4**	**5**
Kurum İmajı/Şöhreti	Kurum imajı etkilenmez. Kurum dışına yansıyacak düzeyde değildir.	Olumsuzluk kurum dışına yansıyabilir ama dikkat çekecek düzeyde kurumu etkileyecek seviyede değildir.	Olumsuzluk kurum dışına yansır, belirli gruplar ve kişiler tarafından tepkiyle karşılanır. Kurum imajı belirli oranda zarar görür.	Gazete sayfalarında veya televizyonlarda yayınlanacak şekilde kurum imajının zedelenmesi	Medyada ve halkın gözünde kurum faaliyetlerinin sonlandırılmasına varacak şekilde olumsuz tepkilerin oluşması. Kurumun çok ciddi itibar kaybına uğraması
Sistemler/ Servisler	Sistemler üzerinde işlerin aksamasına neden olmayacak düzeyde küçük hatalar veya performans sorunları	Belirli bir serviste yavaşlamaya ve işlerin küçük çapta gecikmesine yol açabilecek hatalar	7/24 hizmet vermesi gereken bir serviste 0-2 saat kesintiye yol açan ve müşterileri direkt etkileyen hatalar veya performans sorunları	7/24 hizmet vermesi gereken bir serviste 2-24 saat kesintiye yol açan ve müşterileri direk etkileyen hatalar veya performans sorunları	7/24 hizmet vermesi gereken bir serviste 1 günden daha uzun süreli kesintiye yol açan ve müşterileri direkt etkileyen hatalar veya performans sorunları
Finansal/ Mali	Bütçenin yüzde 1'inden küçük zararlar	Bütçenin yüzde 1'i ile 2,5'u arasında kalan zararlar	Bütçenin yüzde 2,5'i ile 5'i arasında kalan zararlar	Bütçenin yüzde 5'i ile 10'u arasında kalan zararlar	Bütçenin yüzde 10'undan büyük zararlar
Genel	İş, itibar kaybı, yasal yükümlülük ya da çalışanların morali açısından ciddi bir zarara yol açmayan ancak yapılan iş üzerinde az da olsa etkisi olabilecek / bir miktar gecikmeye neden olabilecek durumlar (Ör: Bir çalışanın kişisel bilgisayarı gibi araçların erişilebilirliği) Gizlilik, erişilebilirlik ve bütünlük ilkelerinden en az biri ihmal edilebilir derecede zarar görür. Zarar çok kısa vadede telafi edilebilir.	İş, itibar kaybı, yasal yükümlülük ya da çalışanların morali açısından bir zarara yol açmayan ancak yapılan işi bir miktar etkileyen / gecikmesine neden olan durumlar (Ör: Bir birime özgü ve kurumun asli fonksiyonlarına yönelik olmayan sistemlerin erişilebilirliği) Gizlilik, erişilebilirlik ve bütünlük ilkelerinden en az biri düşük derecede zarar görür. Zarar kısa vadede telafi edilebilir.	İtibar kaybı ve yasal yükümlülük açısından bir zarara yol açmayan ancak iş kaybına, ek maliyetlerin doğmasına ya da çalışanların motivasyonu üzerinde bir miktar olumsuz etkiye yol açan durumlar (Ör: E-posta sistemlerinde erişilebilirlik, bütünlük, gizliliği; İnternet erişilebilirliği; herhangi bir iş konusunda uzman insan kaynağının erişilebilirliği) Gizlilik, erişilebilirlik ve bütünlük ilkelerinden en az biri orta derecede zarar görür. Zarar kısa/orta vadede telafi edilebilir.	Kurumun yasal yükümlülük hariç itibar veya iş kaybına uğramasına, yüksek ek maliyetler doğmasına ya da çalışanların motivasyonu üzerinde ciddi olumsuz etkiye yol açan durumlar (Ör: Kritik iş uygulamalarının erişilebilirlik, bütünlük ve gizliliği) Gizlilik, erişilebilirlik ve bütünlük ilkelerinden en az biri kritik derecede zarar görür. Zarar orta vadede telafi edilebilir.	Kurumun çok ciddi itibar veya iş kaybına uğramasına, yasal yükümlülük altına girmesine, yüksek ek maliyetlerin doğmasına, çalışan motivasyonun iş kesintisine neden olacak şekilde etkilenmesine neden olabilecek durumlar. (Ör: Kurumun sözleşme ile hüküm altına alınmış gizlilik ilkelerini ihlal etmesi, işlerini tamamen durmasına neden olacak bir kesinti) Gizlilik, erişilebilirlik ve bütünlük ilkelerinden en az ikisi kritik derecede zarar görür. Zarar telafi edilemez ya da uzun vadede telafi edilebilir.

4.6 Riskler

Risk tanımı, bir tehdit kaynağı tarafından varlıkta bulunan zayıflığın kullanılarak ne tip bir zarar oluşturulabileceğinin ve varlıkla ilgili güvenlik öğelerine nasıl zarar verilebileceğinin tanımlanmasıdır.

Bu rehber kapsamında tanımlanan tehditlerin etki ettiği varlıklar ve bunun sonucunda ortaya çıkan riskler **Tablo 3**'de numaralandırılmıştır.

Tablo 3: Risk Listesi

	VAR-EB	VAR-KA	VAR-AK	VAR-DGM	VAR-SR	VAR-UY
TEH-EB-AHE	Risk01					
TEH-EB-VBB	Risk02					
TEH-EB-KD	Risk03					
TEH-EB-TD	Risk04					
TEH-KR-ALZ	Risk05	Risk13			Risk27	
TEH-KR-ZYF	Risk06	Risk14			Risk28	
TEH-KR-KPY	Risk07	Risk15				
TEH-KR-YAN	Risk08	Risk16	Risk19	Risk23		
TEH-AK-EVÇ	Risk09		Risk20	Risk24		
TEH-AK- FİY	Risk10		Risk21	Risk25		
TEH-SR-KSD	Risk11	Risk17			Risk29	
TEH-UY-DEĞ	Risk12	Risk18	Risk22	Risk26	Risk30	Risk31

Bu risklerin tek tek incelenmesi ve önlemlerin tanımlanması bu rehberin kapsamı dışındadır. VAR-BS ile ilgili risk değerlendirmesi/yönetimi, çok fazla ayrıntı içerdiği ve kurumların mevcut bilgi sistemleri altyapıları ile ilişkili olduğu için elektronik belgeyi üreten ve işleyen kurumların sorumluluğundadır. Kurumların bilgi sistemleri altyapılarını ISO 27005 vb. süreçlere uygun hale getirmeleri, süreçlerle ilgili risklerin belirlenmesine ve yönetilmesine imkan sağlayacaktır.

4.7 Tahmini Risk Değerinin Belirlenmesi

Risk, bir tehdidin bir açıklığı gerçekleme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan önlemlerin yeterliliğinin bir fonksiyonudur. Diğer bir deyişle risk, olasılık değerlendirmesinde ve etki değerlendirmede belirlenen değerlere bağlıdır. Bu rehberde risk değerinin belirlenmesinde aşağıdaki formül kullanılmıştır:

Risk Değeri = Tehdit Kaynağının Risk Oluşturma Olasılığı Değeri (**TKROD**) x Bilgi Sistemleri Güvenliği Önlem Seviyesi (**BSGÖS**) x Kripto Güvenlik Seviyesi (**KGS**)

Risk Değeri formülündeki Tehdit Kaynağının Risk Oluşturma Olasılığı Değeri, tehdit kaynağının amacı ve yeteneklerine göre belirlenen Tehdit Gerçekleşme Olasılığı ile ilişkilendirilmektedir. Buna göre çeşitli tehdit kaynakları için kullanılacak Tehdit Kaynağının Risk Oluşturma Olasılığı Değerleri **Tablo 4**'te gösterilmiştir.

Tablo 4: Tehdit Kaynağının Risk Oluşturma Olasılığı Değeri

Tehdit Kaynağı	Tehdit Gerçekleşme Olasılığı	TKROD
İstem dışı kullanıcı hatası	Çok Düşük (uzak ihtimal) / Düşük (Nadiren, Seyrek)	1-2
Kurum içi/dışı kötü niyetli kullanıcı	Düşük (Nadiren, Seyrek) / Orta (Ara sıra)	2-3
Kurum içi kötü niyetli sistem yöneticisi	Orta (Ara sıra) / Yüksek (Genellikle, Muhtemelen)	3-4
Kurum dışı uzman saldırgan (Hacker)	Yüksek (Genellikle, Muhtemelen) / Çok Yüksek (Sık sık)	4-5
Kötü niyetli kurumlar	Çok Yüksek (Sık sık)	5

Risk Değeri formülündeki Bilgi Sistemleri Güvenliği Önlem Seviyesi (**BSGÖS**), elektronik bilginin işlendiği bilgi sisteminin genel güvenlik seviyesine verilen bir puandır. Bu rehberde kullanılan puanlama **Tablo 5**'de gösterilmiştir.

Tablo 5: Bilgi Sistemleri Güvenliği Önlem Seviyesi

Bilgi Sistemi Ağ Tipi	Önlem Seviyesi	BSGÖS
Ağ Bağlantısı Yok	Tüm güvenlik önlemleri alınmış	1
Kapalı Ağ	Tüm güvenlik önlemleri alınmış	2
Kapalı Ağ	Güvenlik önlemleri kısmen alınmış	3
Açık Ağ	Tüm güvenlik önlemleri alınmış	4
Açık Ağ	Güvenlik önlemleri kısmen alınmış	5
Açık Ağ	Güvenlik önlemi alınmamış	6

Risk Değeri formülündeki Kripto Güvenlik Seviyesi (**KGS**), elektronik bilginin işlendiği bilgi sisteminde kullanılan akıllı kartlar, kripto algoritmaları ve uygulama yazılımlarının sağladığı güvenlik seviyesine göre verilen bir puandır. Bu rehberde kullanılan puanlama **Tablo 6**'da gösterilmiştir.

Tablo 6: Kripto Güvenlik Seviyesi

Kriptografik Önlem Seviyesi	KGS
Tasarım ve gerçeklemesi kapalı tutulan ve milli kripto onayı olan sistem	1
Bu rehberde anlatılan yöntemlerle çalışan sistem (elektronik imzalı-şifreli)	2
Bu rehberde anlatılan yöntemlerle çalışan sistem (elektronik imzalı)	3
Diğer AAA sistemleri	5

4.8 Belge İçeriğine Göre Risk Değerleri

Bölüm 5.7'de verilen Risk Değeri formülüne göre bir riskin değeri en az 1 (1x1x1), en fazla 150 (5x6x5) olabilir. Hizmete Özel ve daha alt gizlilik dereceleri için bu rehber tarafından yapılan değerlendirmeye göre oluşan risk değerleri **Tablo 7**'de gösterilmektedir.

Tablo 7: Hizmete Özel ve Daha Alt Gizlilik Dereceleri için Kabul Edilebilecek Risk Değerleri

Belge İçeriği	Kabul Edilebilecek En Yüksek Risk Değeri	TKROD (Tehdit Kaynağının Risk Oluşturma Olasılığı Değeri)	BSGOS (Bilgi Sistemleri Güvenliği Önlem Seviyesi)	KGS (Kriptografik Önlem Seviyesi)
Tasnif Dışı	60 (4 x 5 x 3)	Yüksek (4)	Güvenlik Önlemleri Kısmen Alınmış Açık Ağ (5)	Elektronik İmza (3)
Hizmete Özel	32 (4 x 4 x 2)	Yüksek (4)	Tüm Güvenlik Önlemleri Alınmış Açık Ağ (4)	Elektronik İmza ve Şifreleme (2)

5 Güvenlik

Bu rehberde tarif edilen yöntemlerle **Hizmete Özel** ve daha alt gizlilik derecesindeki belgelerin işlenmesi önerilmektedir. Risk Değerlendirmesi ile ilgili bölümde bahsedilen risklerin en aza indirilmesi için Bölüm 5.1'de bahsedilen hizmetlerin kullanılması ve Bölüm 5.2'deki tedbirlerin alınması önerilir. Buna göre elektronik bir belge oluşturulduktan sonra sırasıyla:

- Oluşturan kişi ve onay silsilesindeki amirleri tarafından elektronik olarak imzalanmalıdır (CADES [R2] veya XADES [R3] standardında tarif edildiği şekilde).
- Belgenin oluşturulma tarihi önemliyse belgeye zaman damgası eklenmelidir (CADES [R2] veya XADES [R3] standardında tarif edildiği şekilde).
- Belgenin içeriği yetkisiz kişilerden korunmak isteniyorsa Bölüm 6'da anlatıldığı şekilde şifrelenmelidir.

5.1 Güvenlik Hizmetleri

Elektronik belgelerin güvenliğini sağlamak için çeşitli güvenlik hizmetleri mevcuttur. Bu güvenlik hizmetleri aşağıda görüldüğü gibi sınıflandırılabilir:

- **Veri Gizliliği:** Elektronik bir belgenin içeriğinin gizli kalmasını sağlayan ve yetkisiz kişilerce okunmasını engelleyen güvenlik hizmetleridir. Bu rehber kapsamında, veri gizliliğini sağlamak için şifreleme yöntemleri kullanılmalıdır.

- **Veri Bütünlüğü:** Elektronik bir belgenin hazırlandıktan sonra değiştirilmediğini ve orijinalliğini koruduğunu ispat etmeyi sağlayan güvenlik hizmetleridir. Bu rehber kapsamında, veri bütünlüğünü sağlamak için özet alma ve elektronik imza yöntemleri kullanılmalıdır.

- **İnkar Edilemezlik ve Kimlik Doğrulama:** Elektronik bir belgeyi kimin hazırladığı kesin olarak ispat etmeyi sağlayan güvenlik hizmetleridir. Bu rehber kapsamında, inkar edilemezlik ve kimlik doğrulamayı sağlamak için elektronik imza yöntemleri kullanılmalıdır.

- **Verinin Var Olduğu Tarihin İspatı:** Elektronik bir belgenin kesin olarak hangi tarihte var olduğunu ispat etmeyi sağlayan güvenlik hizmetleridir. Bu rehber kapsamında, verinin hangi tarihte var olduğunun ispatını sağlamak için zaman damgası kullanılmalıdır.

5.2 Zorunlu Önlemler

Bu rehberde belirtilen zayıflıkların ve tehditlerin olası etkilerini en aza indirmek için aşağıdaki önlemlerin alınması gerekmektedir:

Önlem 1: ZAY-BS-YGA, ZAY-BS-DGA ve ZAY-BS-AGA zayıflıklarına karşı bilgi sistemleri seviyesinde önlemler alınmalıdır ancak bu önlemlerin neler olduğu ve nasıl uygulanacakları elektronik belgeyi işleyen kurumun sorumluluğundadır. Bu nedenle rehberde ayrıntılı tanım yapılmamıştır.

Önlem 2: ZAY-KR-ALZ (zayıf ve yetersiz kriptografik algoritmaların kullanılması) zayıflığına karşı önerilen algoritma ve anahtar boyları **Tablo 8**'de verilmiştir. Algoritma ve anahtar boylarının önerilen son kullanım tarihine [R9]'dan erişmek mümkündür. Bu tabloda bahsedilen algoritmaların hatalı kullanılmasına engel olmak için ilgili standartların doğru gerçeklenmesi gereklidir.

Tablo 8: Önerilen Algoritma Listesi

Algoritma Tipi	Algoritma Adı	Anahtar Boyu	İlgili Standart
Asimetrik İmzalama	RSA	2048 bit	PKCS#1 sürüm 2.2 (RSASSA-PSS), ETSI TS 101733 (CADES), ETSI TS 101903 (XADES)
Asimetrik İmzalama	ECDSA	256 bit	FIPS 186-3, ETSI TS 101733 (CADES), ETSI TS 101903 (XADES)
Anahtar Taşıma	RSA	2048 bit	PKCS#1 sürüm 2.2 (RSAES-OAEP)
Anahtar Taşıma	ECDH	256 bit	NIST SP 800-56A
Simetrik Şifreleme	AES	128 bit	FIPS 197, Çalışma kipi: NIST SP-800-38A, CBC Mode
Özet alma	SHA256	-	FIPS 180-3

Önlem 3: ZAY-KR-AÜY (Kriptografik anahtar üretim yöntemlerinin güvenli olmaması) zayıflığına karşı önlem olarak Kamu SM tarafından üretilmiş asimetrik kripto anahtarlarının kullanılması tercih edilmelidir. Şifreleme ve elektronik imzalama işlemlerinde kullanılacak asimetrik anahtarlar milli kripto onaylı akıllı kartların içinde üretilmeli veya Kamu SM'nin milli kripto onaylı anahtar üretim sistemlerinde üretilerek akıllı kartlara yerleştirilmelidir.

Kripto anahtarlarının Kamu SM dışında oluşturulması istenmesi durumunda anahtarlar, milli kripto onaylı akıllı kartlarda üretilebilir. Anahtar üretilme sürecine Kamu SM yetkilileri nezaret etmelidir. Simetrik ve geçici asimetrik anahtarların üretiminde milli kripto onaylı akıllı kartta bulunan güvenli donanımsal rasgele sayı üreteci kullanılmalıdır. Kamu kurumları gerekli risk analizlerini yaparak simetrik ve asimetrik anahtarların oluşturulmasında ve işlenmesinde ticari güvenlik donanım modüllerini kullanabilirler.

Önlem 4: ZAY-KR-GOS ve ZAY-KR-YSÖ zayıflıklarına karşı önlem olarak kriptografik anahtarlar en az Ortak Kriterler (Common Criteria) CC EAL 4+ onaylı akıllı kartlarda veya donanım güvenlik modüllerinde saklanmalı ve kullanılmalıdır.

Önlem 5: ZAY-UY-DEĞ (Uygulama yazılımının elektronik belge, kriptografik anahtar ve sertifika kullanımıyla ilgili fonksiyonlarının değiştirildiğini kontrol etmemesi veya bu durumu fark etmemesi) zayıflığına karşı önlem olarak uygulama yazılımı çalışmaya başlarken aşağıdaki denetimleri yapmalıdır:

- **Kriptografik algoritma testleri**: Kullanılan her bir özet alma, şifreleme ve elektronik imzalama algoritması için FIPS Kriptografik Algoritma Geçerleme Testleri (Cryptographic Algorithm Validation Testing - CAVP) kapsamında yayınlanan test vektörleri ile testler yapılmalıdır.
- **Yazılım bütünlük testi**: Uygulama yazılım kütüphanesi üreticisi tarafından yazılımın orijinal hali üzerinde hesaplanmış bir imza değeri yazılımla beraber sunulmalıdır. Bu imza değeri açılışta yazılım paketinin özeti alınarak kontrol edilmelidir.

6 İşlevsel Özellikler

Elektronik belge güvenliğini sağlamak için elektronik imza ve şifreleme yöntemleri kullanılır. Bir belgenin kim tarafından hazırlandığını veya onaylandığını gösteren ve belgenin veri bütünlüğünü koruyan elektronik imzanın belgeye eklenmesi için ETSI TS 101 733 CAdES ve ETSI TS 101 903 XAdES standardına uygun işlem yapılmalıdır. Elektronik imzada kullanılacak algoritmalar ve anahtar boyları Bölüm 5'te belirtilenler arasından seçilmelidir.

Belge şifreleme işlemlerinde RFC 5652[R1]'de belirtilen CMS (Cryptographic Message Syntax) standardı uygulanır. Elektronik imzalı bir belgenin şifrelenmesi işlemi, elektronik imza taşımayan belgenin şifrelenmesi ile aynı şekilde yapılır.

Şifrelemede elektronik belge rastgele belirlenen simetrik bir anahtarla şifrelenir. Bu rastgele simetrik anahtar Bölüm 5.2 Önlem 3'te tarif edilen özelliklere sahip gerçek rastgele üreteçleri kullanılarak üretilmelidir. Rastgele belirlenen simetrik anahtar belgenin şifresini çözmesi istenen her bir alıcının açık anahtarıyla ayrı ayrı şifrelenir.

CMS standardına göre veri bir **`ContentInfo`** ASN.1 yapısı içerisinde şifreli olarak saklanır.

```
ContentInfo ::= SEQUENCE {
            contentType ContentType,
            content [0] EXPLICIT ANY DEFINED BY contentType }
ContentType ::= OBJECT IDENTIFIER
```

Şifreli belge (EnvelopedData) hazırlanırken **`ContentType`** değeri **`id-envelopedData`** (bkz. RFC 5652[R1] s.18) olarak belirtilir ve içerik **`EnvelopedData`** yapısı içerisinde kodlanarak **`ContentInfo`** yapısının **`content`** değerine kaydedilir.

```
EnvelopedData ::= SEQUENCE {
      version CMSVersion,
      originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
      recipientInfos RecipientInfos,
      encryptedContentInfo EncryptedContentInfo,
      unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL }

OriginatorInfo ::= SEQUENCE {
      certs [0] IMPLICIT CertificateSet OPTIONAL,
      crls [1] IMPLICIT RevocationInfoChoices OPTIONAL
}

RecipientInfos ::= SET SIZE (1..MAX) OF RecipientInfo

EncryptedContentInfo ::= SEQUENCE {
     contentType ContentType,
     contentEncryptionAlgorithm  ContentEncryptionAlgorithmIdentifier,
      encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }
```

```
EncryptedContent ::= OCTET STRING

UnprotectedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

EnvelopedData veri yapısındaki **version** değeri olarak RFC 5652[R1]'de belirtilen koşul ağacına uygun olarak **0** kullanılır. **OriginatorInfo** alanı kullanılmaz. **EnvelopedData** veri yapısında, şifreli belgeyi açması istenen alıcılar ile ilgili bilgiler **RecipientInfo** listesi şeklinde saklanır.

```
RecipientInfo ::= CHOICE {
      ktri KeyTransRecipientInfo,
      kari [1] KeyAgreeRecipientInfo,
      kekri [2] KEKRecipientInfo,
      pwri [3] PasswordRecipientinfo,
      ori [4] OtherRecipientInfo }
```

EnvelopedData oluşturulurken aşağıdaki adımlar takip edilir. Bu işlemler sırasında kullanılacak algoritmalar ve anahtar boyları Bölüm 5'te belirtilenler arasından seçilmelidir.

1. İçerik şifreleme algoritmasına uygun simetrik bir içerik şifreleme anahtarı (İŞA) rastgele şekilde üretilir.

2. Üretilen İŞA her bir alıcı için şifrelenir. Bu şifrelemenin detayları anahtar yönetim algoritmasına göre değişir. Bu anahtar yönetim şekilleri kullanılabilir:

   - **Anahtar Taşıma:** RSA algoritması kullanılıyorsa İŞA alıcının açık anahtarı ile şifrelenir.
   - **Anahtar Anlaşma:** ECDH algoritması kullanılıyorsa alıcının açık anahtarı ve gönderenin kapalı anahtarı birlikte bir simetrik anahtar üzerinde anlaşmak için kullanılır (ECDH algoritması yardımıyla) ve bu anahtarla İŞA şifrelenir.

3. Şifreli İŞA ve alıcıya özel diğer bilgiler RFC 5652[R1] Bölüm 6.2'de belirtildiği gibi **RecipientInfo** yapısının içerisine eklenir.

4. İçerik RFC 5652[R1] Bölüm 6.3'te belirtilen şekilde İŞA ile simetrik olarak şifrelenir.

5. **RecipientInfo**listesi ve şifreli içerik bir arada RFC 5652[R1] Bölüm 6.1'de belirtildiği gibi **EnvelopedData** yapısını oluşturur.

RSA anahtarlı alıcılar için **KeyTransRecipientInfo** yapısı kullanılır.

```
KeyTransRecipientInfo ::= SEQUENCE {
      version CMSVersion, -- always set to 0 or 2
      rid RecipientIdentifier,
      keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
      encryptedKey EncryptedKey }

EncryptedKey ::= OCTET STRING

RecipientIdentifier       ::=       CHOICE       {
```

```
        issuerAndSerialNumber   IssuerAndSerialNumber,
        subjectKeyIdentifier [0] SubjectKeyIdentifier
        }
```

Bu yapıda **version** değeri **0** olmalıdır. Dolayısıyla **RecipientIdentifier** olarak **issuerAndSerialNumber** tipi kullanılır (bkz. RFC 5652[R1] s.22).

EC anahtarlı alıcılar için RFC 3278[R4]'de belirtilen şekilde **KeyAgreeRecipientInfo** yapısı kullanılır. Bu durumda "**One-Pass Diffie-Hellman, C (1, 1, ECC CDH)**" (bkz. NIST SP800-56A Revision1[R5] Bölüm 6.2.2.2) algoritması kullanılır. Bu algoritmada kullanılan anahtar sarmalama (key-wrap) algoritması **AES-KEYWRAP,** anahtar türetme (key derivation) algoritması da **SHA1-KDF** olmalıdır.

Burada uygulanan **EC** bileşenlerinin detayları **[R6]** dökümanında belirtilmektedir.

```
KeyAgreeRecipientInfo ::= SEQUENCE {
      version CMSVersion, -- always set to 3
      originator [0] EXPLICIT OriginatorIdentifierOrKey,
      ukm [1] EXPLICIT UserKeyingMaterial OPTIONAL,
      keyEncryptionAlgorithm    KeyEncryptionAlgorithmIdentifier,
      recipientEncryptedKeys RecipientEncryptedKeys }

OriginatorIdentifierOrKey       ::=       CHOICE       {
      issuerAndSerialNumber       IssuerAndSerialNumber,
      subjectKeyIdentifier [0] SubjectKeyIdentifier,
      originatorKey [1] OriginatorPublicKey }

OriginatorPublicKey   ::=   SEQUENCE   {
      algorithm    AlgorithmIdentifier,
      publicKey BIT STRING }

RecipientEncryptedKeys ::= SEQUENCE OF RecipientEncryptedKey

RecipientEncryptedKey  ::=  SEQUENCE  {
      rid  KeyAgreeRecipientIdentifier,
      encryptedKey EncryptedKey }

KeyAgreeRecipientIdentifier    ::=    CHOICE    {
      issuerAndSerialNumber
      IssuerAndSerialNumber,
      rKeyId [0] IMPLICIT RecipientKeyIdentifier }

RecipientKeyIdentifier      ::=      SEQUENCE      {
      subjectKeyIdentifier SubjectKeyIdentifier,
      date GeneralizedTime OPTIONAL,
      other OtherKeyAttribute OPTIONAL }

SubjectKeyIdentifier ::= OCTET STRING
```

7 Örnek Belgeler

7.1 RSA Algoritması ile Şifreleme

RSA asimetrik şifreleme algoritmasını kullanarak (PKCS#1 sürüm 2.2'de anlatıldığı şekilde) Bölüm 6'da anlatılan yöntemlere göre oluşturulmuş bir şifreli dosyanın ASN.1 yapısı aşağıda gösterilmektedir.

```
0 NDEF: SEQUENCE { //ContentInfo
2 9: OBJECT IDENTIFIER envelopedData (1 2 840 113549 1 7 3) //ContentType
13 NDEF: [0] { //Content-Start
15 NDEF: SEQUENCE { // EnvelopedData
17 1: INTEGER 0 // Version
20 333: SET { // RecipientInfos
24 329: SEQUENCE { // RecipientInfo - KeyTransRecipientInfo
28 1: INTEGER 0 // Version
31 51: SEQUENCE { //RecipientIdentifier - IssuerAndSerialNumber
33 45: SEQUENCE { // Issuer Name
35 11: SET {
37 9: SEQUENCE {
39 3: OBJECT IDENTIFIER countryName (2 5 4 6)
44 2: PrintableString 'TR'
: }
: }
48 30: SET {
50 28: SEQUENCE {
52 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
57 21: UTF8String 'TÜBİTAK KURUMSAL SM'
: }
: }
: } // END-OF IssuerName
80 2: INTEGER 14030 // SerialNumber
: }
84 11: SEQUENCE { // Key Encryption Algorithm
86 9: OBJECT IDENTIFIER '1 2 840 113549 1 1 7'
: }
97 256: OCTET STRING // Encrypted Key
: 7A 50 AD 5F 6D 7C BD 4F 91 0A 0D DC 56 7B 2A 35
: 0F AA B8 8D 38 F0 16 01 88 BF 4B 89 FB 05 7E 30
: BB F5 FF 2C F7 9C D0 3D 13 97 F1 10 99 09 AE F4
: 5D 45 1E B3 62 E2 1C 00 9D 49 F2 9F 0E 9E 16 15
: E7 19 98 E6 AE A1 41 F3 FD 27 05 D8 24 C8 FC A1
: 7A C3 27 11 1D E5 DD D0 E1 8F 60 46 D4 64 0D C0
: 86 BD 56 92 74 7E 6A 85 4A 2F 2C 18 C4 FB 5F 27
: 10 9E 02 7D B9 A5 AD 17 70 7C 2E B6 52 7F 09 49
: [ Another 128 bytes skipped ]
: } // END-OF RecipientInfo-KeyTransRecipientInfo
: } // END-OF RecipientInfos
357 NDEF: SEQUENCE { // EncryptedContentInfo
359 9: OBJECT IDENTIFIER data (1 2 840 113549 1 7 1) // contentType
370 29: SEQUENCE { // contentEncryptionAlgorithm ContEnc Alg ID
372 9: OBJECT IDENTIFIER aes128-CBC (2 16 840 1 101 3 4 1 2)
383 16: OCTET STRING // ContEnc Alg Parameters
```

```
 : 0A 1A C9 E8 69 A7 CF 01 FC 46 57 C6 24 45 70 D7
 : }
401 NDEF: [0] { // EncryptedContent
403 1136: OCTET STRING
 : E3 A9 08 08 99 0F 5F FF 4D E4 33 2D 10 59 86 CC
 : 24 4D D8 45 59 60 E2 15 AD B0 BC 61 07 52 BC FE
 : 66 90 A9 0C 42 EB 8C 55 3E 51 AD 98 93 59 A5 6B
 : B8 31 BB EB 0C 14 CC 80 34 4F E1 C1 A2 E0 15 61
 : C5 25 52 98 1A BC 2C C0 85 4D 85 B4 03 B7 35 BE
 : 14 D6 99 52 16 BC C1 56 3D 80 6C 50 F2 1C CB 87
 : 93 5A 0A E1 15 C2 AA D4 63 2E F7 CA FA C9 B0 AE
 : D9 53 6D 4E 67 6A 02 79 D4 F4 EF F5 15 EA A9 F7
 : [ Another 1008 bytes skipped ]
1543 16: OCTET STRING
 : F5 41 A7 99 B0 89 51 E9 E5 36 69 2C BA A6 B6 86
 : }
 : } // END-OF EncryptedContentInfo
 : } // END-OF EnvelopedData
 : } // END-OF Content
 : } // END-OF ContentInfo
```

7.2 ECDH Algoritması ile Şifreleme

ECDH asimetrik anahtar değişim ve şifreleme algoritmasını kullanarak (NIST SP 800-56A'da anlatıldığı şekilde) Bölüm 6'da anlatılan yöntemlere göre oluşturulmuş bir şifreli dosyanın ASN.1 yapısı aşağıda gösterilmektedir.

```
 0 NDEF : SEQUENCE { // ContentInfo

2     9: OBJECT IDENTIFIER envelopedData (1 2 840 113549 1 7 3) // ContentType
13 NDEF: [0] { // Content-Start
15 NDEF: SEQUENCE { // EnvelopedData
17    1: INTEGER 0 // Version
20  434: SET { // RecipientInfos
24  430: [1] { // RecipientInfo - KeyAgreeRecipientInfo
28    1: INTEGER 3 // Version
31  305: [0] { // OriginatorIdentifierOrKey
35  301: [1] { // OriginatorPublicKey
39   11: SEQUENCE { // AlgorithmIdentifier
41    7: OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
50    0: NULL
       : }
52  284: BIT STRING, encapsulates { //publicKey
57  279: SEQUENCE {
61  212: SEQUENCE {
64    7: OBJECT IDENTIFIER
       : ecPublicKey (1 2 840 10045 2 1)
73  200: SEQUENCE {
76    1: INTEGER 1
79   41: SEQUENCE {
81    7: OBJECT IDENTIFIER
```

```
       : prime-field (1 2 840 10045 1 1)
90   30: INTEGER
       : 7F FF FF FF FF FF FF FF FF FF FF FF 7F FF FF FF
       : FF FF 80 00 00 00 00 00 7F FF FF FF FF FF
       : }
122  87: SEQUENCE {
124  30: OCTET STRING
       : 7F FF FF FF FF FF FF FF FF FF FF FF 7F FF FF FF
       : FF FF 80 00 00 00 00 00 7F FF FF FF FF FC
156  30: OCTET STRING
       : 6B 01 6C 3B DC F1 89 41 D0 D6 54 92 14 75 CA 71
       : A9 DB 2F B2 7D 1D 37 79 61 85 C2 94 2C 0A
188  21: BIT STRING
       : E4 3B B4 60 F0 B8 0C C0 C0 B0 75 79 8E 94 80 60
       : F8 32 1B 7D
       : }
211  31: OCTET STRING
       : 02 0F FA 96 3C DC A8 81 6C CC 33 B8 64 2B ED F9
       : 05 C3 D3 58 57 3D 3F 27 FB BD 3B 3C B9 AA AF
244  30: INTEGER
       : 7F FF FF FF FF FF FF FF FF FF FF FF 7F FF FF 9E
       : 5E 9A 9F 5D 90 71 FB D1 52 26 88 90 9D 0B
       : }
       : }
276  62: BIT STRING
       : 04 0F E1 69 58 41 79 AF 65 98 67 2D 16 86 37 AD
       : B8 8B E8 1E AF 15 EF A8 F1 2F DA 53 E6 7E 4C 57
       : 66 64 34 C8 EF 06 8C 76 30 A6 47 91 7A 17 4C AB
       : D4 A6 12 9C 47 64 25 86 10 67 4C 80 2B
       : }
       : }   // END-OF publicKey
       : }   // END-OF OriginatorPublicKey
       : }   // END-OF OriginatorIdentifierOrKey
340  26: SEQUENCE {       // KeyEncryptionAlgorithmIdentifier
342   9: OBJECT IDENTIFIER '1 3 133 16 840 63 0 2'
353  13: SEQUENCE {
355   9: OBJECT IDENTIFIER '2 16 840 1 101 3 4 1 5'
366   0: NULL
       : }
       : }
368  88: SEQUENCE {       // RecipientEncryptedKeys
370  86: SEQUENCE {       // RecipientEncryptedKey
372  42: SEQUENCE {       // KeyAgreeRecipientIdentifier-IssuerSerialNo
374  37: SEQUENCE { // Issuer
376  22: SET {
378  20: SEQUENCE {
380   3 : OBJECT IDENTIFIER organizationName (2 5 4 10)
385  13: UTF8String 'Test Yayinci1'
       : }
       : }
400  11: SET {
402   9: SEQUENCE {
404   3: OBJECT IDENTIFIER countryName (2 5 4 6)
409   2: PrintableString 'TR'
       : }
```

```
       :  }
       :  }
413    1: INTEGER 1          // SerialNumber
       :  }    // END-OF KeyAgreeRecipientIdentifier-IssuerSerialNo
416   40: OCTET STRING       // EncryptedKey
       :  7D BC 03 30 C7 CD 22 2D C8 1D 57 47 22 2C F3 44
       :  CA 06 2F A2 8C 83 CD B4 B1 B6 FD 67 05 1E C6 7B
       :  91 8A 86 1E 81 AD D5 92
       :  }    // END-OF RecipientEncryptedKey
       :  }    // END-OF RecipientEncryptedKeys
       :  }    // END-OF RecipientInfo-KeyTransRecipientInfo
       :  }    // END-OF RecipientInfos
458NDEF:  SEQUENCE {          // EncrptedContentInfo
460    9: OBJECT IDENTIFIER data (1 2 840 113549 1 7 1) // contentType
471   29: SEQUENCE {          // contentEncryptionAlgorithm
473    9: OBJECT IDENTIFIER aes256-CBC (2 16 840 1 101 3 4 1 42)
          // ContEnc Alg ID
484   16: OCTET STRING       // ContEnc Alg Parameters
       :  61 63 08 C5 4A 94 D0 AB 70 F4 9A A0 30 93 66 72
       :  }
502NDEF:  [0] {               // EncryptedContent
504   16: OCTET STRING
       :  79 94 81 0A 1C F7 C4 4C 73 0F 72 9D 30 0C EA 2A
522   16: OCTET STRING
       :  EE B5 48 5E D5 1D 47 59 46 12 FB 4F 38 E8 C6 11
       :  }
       :  }    // END-OF EncrptedContentInfo
       :  }    // END-OF EnvelopedData
       :  }   // END-OF content
       :  }    // END-OF ContentInfo
```