

**TASNİF DIŐI**



**TÜBİTAK BİLGEM  
KAMU SERTİFİKASYON MERKEZİ**

**KURUMSAL ŞİFRELEME SERTİFİKA UYGULAMA ESASLARI**

**Doküman Kodu**

YON.05.02

**Revizyon No**

13

**Revizyon Tarihi**

13.04.2026

**TASNİF DIŐI**

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk Çıkıő.	15.01.2021
01	Doküman formatı güncellenmiőtir.	18.01.2021
02	Sertifika yenileme süreci güncellenmiőtir.	29.11.2021
03	Elektronik mühür ve kurumsal Őifreleme sertifikaları başvuru formlarının birleőtirilme dođrultusunda "Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi" dokümanının adı "Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi" olarak deđiőtirilmiőtir.	07.01.2022
04	Sertifika üretiminin iki kiőtinin kontrolünde yapılması gerektiđi ile ilgili ibare kaldırılmıőtir.	17.02.2022
05	Yenileme sürecinde üretimi gerçekleştirilen sertifikaların baőtlangıç tarihleri ile ilgili bilgilendirme kaldırılmıőtir.	16.03.2022
06	Yenileme sürecinde her iki sertifika sorumlusunun başvuru listesini imzalama koőtulu kaldırılarak yalnızca bir sorumlunun imzasıyla iőtlem yapılması sađlanmıőtir.	31.03.2022
07	Güvenli elektronik imza oluőturma araçlarının güvenlik seviyelerinde düzenleme yapılmıőtir. Sertifika hizmetlerinin sonlandırılması baőtlığında Kamu SM Hizmetleri Sonlandırma Planına referans eklenmiőtir.	28.04.2022
08	Sertifika İptal Listesi yayımlama gecikmesi süresi kısmında güncelleme yapılmıőtir. Doküman genelinde ek düzeltmeler uygunlanmıőtir.	20.10.2022
09	Sertifika sorumluları arasındaki asıl/yedek ayrımı kaldırılmıőtir. Sertifikanın askıda kalma süresi ile ilgili ifadeler düzenlenmiőtir. Dokümanda referans verilen mevzuatlar için tanım eklenmiőtir. Kullanılmayan "Kamu SM Taahhütnamesi" ve "Sözleőtme" ibareleri kaldırılmıőtir.	06.03.2023

	HSM'li üretimlerde istek dosyalarının parola korumalı zip içerisinde iletimi ile ilgili ifade eklenmiştir. MERNİS tanımı eklenmiştir. Doküman genelinde editöryal düzenlemeler yapılmıştır.	
10	Yenileme sürecinde üretim 3 ay öncesinde başlayacak şekilde düzenleme yapılmıştır.	21.12.2023
11	Yenilemelerde DETSİS web servisi üzerinden sertifika alma yetki sorgusu yapılamadığı durumlarda uygulanacak süreç ile ilgili bilgilendirmeler eklenmiştir. Genel gözden geçirme kapsamında metinsel düzenlemeler gerçekleştirilmiştir.	22.04.2024
12	e-Yazışma Teknik Rehberi'nin 2.1 versiyonunun yayımlanması doğrultusunda düzenlemeler yapılmıştır.	05.08.2024
13	Anahtar değişimi sonrası yeni sertifika makamlarına ait kök ve altkök sertifika bilgileri eklenmiştir. Açık anahtar yerine imza doğrulama verisi; özel anahtar yerine imza oluşturma verisi kavramları kullanılmıştır.	13.04.2026

## İÇİNDEKİLER

1. GİRİŐ	11
1.1. Genel Bakıő	11
1.2. Doküman Adı ve Tanımı	12
1.3. Sistem Bileőenleri	12
1.3.1. Elektronik Sertifika Hizmet Saęlayıcısı	12
1.3.2. Kayıt Birimleri	12
1.3.3. Sertifika Sahipleri	12
1.3.4. Üçüncü Kiőiler	12
1.3.5. Dięer Bileőenler	13
1.4. Sertifika Kullanımı	13
1.4.1. Uygun Olan Sertifika Kullanımı	13
1.4.2. Sertifika Kullanımının Sınırları	13
1.5. Uygulama Esaslarının Yönetimi	13
1.5.1. Doküman Yönetimi	13
1.5.2. İletişim Bilgileri	13
1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluęunu Belirleyen Kiő	14
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri	14
1.6. Tanımlar ve Kısaltmalar	14
1.6.1. Tanımlar	14
1.6.2. Kısaltmalar	16
2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ	16
2.1. Bilgi Depoları	17
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması	17
2.3. Yayım Sıklığı ve Zamanı	17
2.4. Eriőim Kontrolleri	17
3. KİMLİK BELİRLEME VE DOęRULAMA	17
3.1. İsimlendirme	18
3.1.1. İsim Alanı Tipleri	18
3.1.2. Kimlik Bilgilerinin Teőhise Elverişli Olması	18
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması	18
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması	18
3.1.5. Kimlik Bilgilerinin Tekillięi	18
3.1.6. Markanın Tanınması, Doęrulanması ve Rolü	18
3.2. İlk Kimlik Doęrulama	18
3.2.1. İmza Oluőturma Verisi Sahiplięinin Kanıtlanması	18
3.2.2. Kurumsal Kimlięin Belirlenmesi	18
3.2.3. Kiőisel Kimlięin Belirlenmesi	19
3.2.4. Doęrulanmayan Sertifika Sahibi Bilgileri	19
3.2.5. Yetkinin Doęrulanması	19
3.2.6. Uyum Kriterleri	19
3.3. Sertifika Yenileme İsteęinde Kimlik Doęrulama	19
3.3.1. Olaęan Sertifika Yenileme İsteęinde Kimlik Doęrulama	19
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doęrulama	19
3.4. Sertifika İptal İsteęinde Kimlik Doęrulama	19

4.	SERTİFİKA YAŐAM DÖNGÜSÜ İŐLEVSEL GEREKLİLİKLERİ .....	20
4.1.	Sertifika Başvurusu .....	20
4.1.1.	Sertifika Başvurusunu Kimlerin Yapabildiđi .....	20
4.1.2.	Kayıt İŐlemleri ve Sorumluluklar .....	20
4.2.	Sertifika Başvurusunun İŐlenmesi .....	21
4.2.1.	Kimlik Tanımlama ve Doğrulama İŐlevlerinin Yerine Getirilmesi .....	21
4.2.2.	Sertifika Başvurusunun Kabul veya Reddi .....	22
4.2.3.	Sertifika Başvurusunun İŐlenme Zamanı .....	22
4.3.	Sertifikanın OluŐturulması .....	22
4.3.1.	Sertifika OluŐturulmasında ESHS'nin İŐlevleri .....	22
4.3.2.	Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi .....	22
4.4.	Sertifikanın Kabulü .....	23
4.4.1.	Sertifikanın Kabul KoŐulu .....	23
4.4.2.	Sertifikanın ESHS Tarafından Yayımlanması .....	23
4.4.3.	Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması .....	23
4.5.	Sertifikanın ve İmza OluŐturma Verisinin Kullanımı .....	23
4.5.1.	Sertifika Sahibinin Sertifika ve İmza OluŐturma Verisi Kullanımı .....	23
4.5.2.	Üçüncü KiŐilerin Sertifika ve İmza Doğrulama Verisi Kullanımı .....	23
4.6.	Sertifika Süresinin Uzatılması .....	24
4.7.	Sertifika Yenileme .....	24
4.7.1.	Sertifikanın Yenileme KoŐulları .....	24
4.7.2.	Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi .....	24
4.7.3.	Sertifika Yenileme Başvurusunun İŐlenmesi .....	24
4.7.4.	Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi .....	24
4.7.5.	Sertifika Yenileme Sonrası Kabul KoŐulu .....	25
4.7.6.	Sertifika Yenileme Sonrası Sertifikanın Yayımlanması .....	25
4.7.7.	Sertifika Yenilemenin Diđer Tarafra Duyurulması .....	25
4.8.	Sertifikada Bilgi DeđiŐikliđi .....	25
4.9.	Sertifikanın İptali ve Askıya Alınması .....	25
4.9.1.	Sertifikanın İptal Edildiđi Durumlar .....	25
4.9.2.	Sertifika İptal Başvurusunu Kimler Yapabilir .....	26
4.9.3.	Sertifika İptal Başvurusunun İŐlenmesi .....	26
4.9.4.	İptal İŐteđi Ertelenme Süresi .....	26
4.9.5.	İptal İŐteđinin İŐlenme Süresi .....	26
4.9.6.	Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol Gerekliliđi .....	27
4.9.7.	Sertifika İptal Listesi Yayımlama Sıklıđı .....	27
4.9.8.	Sertifika İptal Listesi Yayımlama Gecikme Süresi .....	27
4.9.9.	Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti .....	27
4.9.10.	Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi .....	27
4.9.11.	Diđer Sertifika Durum Bildirim Yöntemleri .....	27
4.9.12.	İmza OluŐturma Verisinin Güvenliđini Yitirmesi Durumu .....	28
4.9.13.	Sertifikanın Askıya Alındıđı Durumlar .....	28
4.9.14.	Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi .....	28
4.9.15.	Sertifika Askıya Alma Başvurusunun İŐlenmesi .....	28
4.9.16.	Askıda Kalma Süresi .....	29
4.10.	Sertifika Durum Servisleri .....	29

4.10.1.	İřletimsel Özellikleri.....	29
4.10.2.	Servisin Eriřilebilirliđi.....	29
4.10.3.	İsteđe Bađlı Özellikler.....	29
4.11.	Sertifika Sahipliđinin Sona Ermesi.....	29
4.12.	Anahtar Yeniden Üretme .....	29
5.	YÖNETİM, İŐLEMSEL VE FİZİKSEL KONTROLLER.....	29
5.1.	Fiziksel Güvenlik Denetimleri .....	29
5.1.1.	Tesis Yeri ve İnřaati.....	30
5.1.2.	Fiziksel Eriřim .....	30
5.1.3.	Güç Kaynađı ve Havalandırma.....	30
5.1.4.	Su Baskınları.....	30
5.1.5.	Yangın Önleme ve Korunma.....	31
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması .....	31
5.1.7.	Atıkların Yok Edilmesi.....	31
5.1.8.	Farklı Mekanlarda Yedekleme.....	31
5.2.	Prosedürel Kontroller.....	31
5.2.1.	Güvenilir Roller .....	31
5.2.2.	Her İřlem İin Gereken Kiři Sayısı.....	31
5.2.3.	Kimlik Dođrulama ve Yetkilendirme.....	32
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller .....	32
5.3.	Personel Güvenlik Kontrolleri .....	32
5.3.1.	Kiřisel Geçmiř, Deneyim ve Nitelik Gerekleri .....	32
5.3.2.	Geçmiř Arařtırması.....	32
5.3.3.	Eđitim Gerekleri .....	32
5.3.4.	Sürekli Eđitim Gerekleri ve Sıklıđı.....	32
5.3.5.	Görev Deđiřim Sıklıđı ve Sırası.....	33
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması .....	33
5.3.7.	Anlařmalı Personel Gereksinimleri .....	33
5.3.8.	Sađlanan Dokümantasyon.....	33
5.4.	Denetim Kayıtları .....	33
5.4.1.	Kaydedilen İřlemler .....	33
5.4.2.	Kayıtların İncelenme Sıklıđı .....	34
5.4.3.	Kayıtların Saklanma Süresi .....	34
5.4.4.	Kayıtların Korunması .....	34
5.4.5.	Kayıtların Yedeklenmesi .....	34
5.4.6.	Kayıtların Toplanması.....	35
5.4.7.	Kayda Sebepiyet Veren Tarafın Bilgilendirilmesi.....	35
5.4.8.	Saldırıya Açıklıđın Deđerlendirilmesi.....	35
5.5.	Kayıt Arřivleme .....	35
5.5.1.	Arřivlenen Kayıt Bilgileri.....	35
5.5.2.	Arřivlerin Tutulma Süresi .....	35
5.5.3.	Arřivlerin Korunması .....	35
5.5.4.	Arřivlerin Yedeklenmesi .....	35
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri.....	36
5.5.6.	Arřivlerin Toplanması.....	36
5.5.7.	Arřiv Bilgilerinin Elde Edilme ve Dođerulanma Metodu.....	36

5.6.	Anahtar DeęiŐimi.....	36
5.7.	Güvenlięin Yitirilmesi ve Arıza Durumlarında Yapılacaklar .....	36
5.7.1.	Güvenilirlięin Yitirilmesi Durumunun Düzeltilmesi .....	36
5.7.2.	Donanım, Yazılım veya Veri Bozulması .....	36
5.7.3.	İmza OluŐturma Verisinin Gizlilięini Kaybetmesi Durumunda İzlenecek Prosedürler.....	37
5.7.4.	Arıza Sonrası Yeniden ÇalıŐırlık .....	37
5.8.	Sertifika Hizmetlerinin Sonlandırılması.....	37
6.	TEKNİK GÜVENLİK KONTROLLERİ.....	37
6.1.	Anahtar Çifti Üretimi ve Kurulumu .....	38
6.1.1.	Anahtar Çifti Üretimi .....	38
6.1.2.	Sertifika Sahibine İmza OluŐturma Verisinin UlaŐtırılması.....	38
6.1.3.	İmza Doğrulama Verisinin ESHS'ye UlaŐtırılması.....	39
6.1.4.	ESHS Sertifikalarına EriŐim Saęlanması .....	39
6.1.5.	Anahtar Uzunlukları.....	39
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü.....	39
6.1.7.	Anahtar Kullanım Amaçları .....	39
6.2.	İmza OluŐturma Verisinin Korunması .....	39
6.2.1.	Kriptografik Modül Standartları .....	39
6.2.2.	İmza OluŐturma Verisine Birden Fazla KiŐi Kontrolünde EriŐim.....	40
6.2.3.	İmza OluŐturma Verisinin Yeniden Elde Edilmesi .....	40
6.2.4.	İmza OluŐturma Verisinin Yedeklenmesi .....	40
6.2.5.	İmza OluŐturma Verisinin ArŐivlenmesi .....	40
6.2.6.	İmza OluŐturma Verisinin Kriptografik Modüle Yüklenmesi.....	40
6.2.7.	İmza OluŐturma Verisinin Kriptografik Modülde Saklanması .....	40
6.2.8.	İmza OluŐturma Verisine EriŐim .....	41
6.2.9.	İmza OluŐturma Verisine EriŐimin Kesilmesi.....	41
6.2.10.	İmza OluŐturma Verisinin Yok Edilmesi .....	41
6.2.11.	Kriptografik Modülün Deęerlendirilmesi .....	41
6.3.	Anahtar Çifti Yönetimiyle İlgili Dięer Konular.....	41
6.3.1.	İmza Doğrulama Verisinin ArŐivlenmesi .....	41
6.3.2.	İmza OluŐturma ve Doğrulama Verilerinin Kullanım Süreleri .....	42
6.4.	Aktivasyon Verileri .....	42
6.4.1.	Aktivasyon Verilerinin OluŐturulması .....	42
6.4.2.	Aktivasyon Verilerinin Korunması.....	42
6.4.3.	Aktivasyon Verileri ile İlgili Dięer Konular .....	42
6.5.	Bilgisayar Güvenlięi Kontrolleri .....	42
6.5.1.	Bilgisayar Güvenlięi ile İlgili Teknik Gereker .....	42
6.5.2.	Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi.....	43
6.6.	YaŐam Döngüsü Teknik Kontrolleri.....	43
6.6.1.	Sistem GeliŐtirme Kontrolleri .....	43
6.6.2.	Güvenlik Yönetimi Kontrolleri.....	43
6.6.3.	YaŐam Döngüsü Güvenlik Kontrolleri .....	43
6.7.	Aę Güvenlięi Kontrolleri.....	43
6.8.	Zaman Damgası.....	44
7.	SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ.....	44

7.1.	Sertifika Biçimi .....	44
7.1.1.	Sürüm Numarası .....	44
7.1.2.	Sertifika Uzantıları .....	45
7.1.3.	Algoritma ve Nesne Tanımlayıcılar .....	46
7.1.4.	İsim Alanı Biçimleri .....	46
7.1.5.	İsim Kısıtları.....	46
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası .....	46
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	46
7.1.8.	İlke Niteleyiciler .....	46
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi .....	47
7.2.	Sertifika İptal Listesi Biçimi .....	47
7.2.1.	Sürüm Numarası .....	47
7.2.2.	Sertifika İptal Listesi Uzantıları.....	47
7.3.	Çevrim İçi Sertifika Durum Protokolü Biçimi .....	47
7.3.1.	Sürüm Numarası .....	47
7.3.2.	ÇİSDUP Uzantıları.....	47
8.	UYGUNLUK DENETİMLERİ .....	48
8.1.	Uygunluk Denetiminin Sıklığı .....	48
8.2.	Denetçinin Nitelikleri.....	48
8.3.	Denetçinin Denetlenen Tarafı Olan İlişkisi .....	48
8.4.	Denetimin Kapsamı .....	49
8.5.	Yetersizliğin Tespiti Durumunda Yapılacaklar .....	49
8.6.	Sonucun Bildirilmesi .....	49
9.	DIŐER İŐLER VE HUKUKSAL MESELELER .....	49
9.1.	Ücretlendirme .....	49
9.1.1.	Sertifika OluŐturma ve Yenileme Ücreti.....	49
9.1.2.	Sertifika EriŐim Ücreti .....	49
9.1.3.	İptal Durum Kaydına EriŐim Ücreti.....	50
9.1.4.	Diđer Servis Ücretleri .....	50
9.1.5.	İade Ücreti.....	50
9.2.	Finansal Sorumluluk .....	50
9.2.1.	Sigorta Kapsamı .....	50
9.2.2.	Diđer Varlıklar .....	50
9.2.3.	Sertifika Mali Sorumluluk Sigortası.....	50
9.3.	Ticari Bilginin Korunması .....	50
9.3.1.	Gizli Bilginin Kapsamı.....	50
9.3.2.	Gizlilik Kapsamında Olmayan Bilgiler.....	50
9.3.3.	Gizli Bilginin Korunma Sorumluluđu .....	51
9.4.	Kişisel Bilginin Gizliliđi.....	51
9.4.1.	Gizlilik Planı .....	51
9.4.2.	Gizli Olarak Tanımlanan Bilgiler .....	51
9.4.3.	Gizli Olarak Tanımlanmayan Bilgiler .....	51
9.4.4.	Gizli Bilginin Korunma Sorumluluđu .....	51
9.4.5.	Gizli Bilginin Kullanımına İzin Verilmesi.....	51
9.4.6.	Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması .....	51

9.4.7.	Diđer BaŐlıklar .....	51
9.5.	Telif Hakları.....	52
9.6.	Temsil Hakkı ve Yüklümlüklükler .....	52
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yüklümlüklükleri .....	52
9.6.2.	Kayıt Birimi Yüklümlüklükleri.....	53
9.6.3.	Sertifika Sahibinin Yüklümlüklükleri.....	53
9.6.4.	Üçüncü KiŐilerin Yüklümlüklükleri .....	54
9.6.5.	Diđer BileŐenlerin Yüklümlüklükleri.....	55
9.7.	Yüklümlüklüklerden Feragat.....	55
9.8.	Sorumlulukla İlgili Sınırlamalar.....	55
9.9.	Tazminat Halleri .....	55
9.10.	AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi .....	55
9.10.1.	AnlaŐma Süresi.....	56
9.10.2.	AnlaŐmanın Sona Ermesi .....	56
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri .....	56
9.11.	Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme .....	56
9.12.	DeđiŐiklik Halleri .....	56
9.12.1.	DeđiŐiklik Metotları .....	56
9.12.2.	Bilgilendirme Mekanizması ve Sıklıđı.....	57
9.12.3.	Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar .....	57
9.13.	AnlaŐmazlık Halleri .....	57
9.14.	Uygulanacak Hukuk .....	57
9.15.	Uygulanabilir Yasalarla Uyum.....	57
9.16.	ÇeŐitli Hükümler .....	57
9.16.1.	Tüm SözleŐmeler.....	57
9.16.2.	Atama .....	57
9.16.3.	Bölünebilirlik.....	57
9.16.4.	İcra (Avukatlık Ücretleri ve Haklardan Feragat) .....	57
9.16.5.	Mücbir Sebepler.....	57
9.17.	Diđer Hükümler .....	57
10.	EK-A SERTİFİKA PROFİLLERİ .....	58
10.1.	KAMU SM KURUMSAL ŐFRELEME KÖK SERTİFİKASI .....	58
10.2.	KAMU SM KURUMSAL ŐFRELEME ALT KÖK SERTİFİKASI .....	59
10.3.	SON KULLANICI KURUMSAL ŐFRELEME SERTİFİKA ŐABLONU .....	60

**TABLolar**

Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları.....	45
Tablo 2 Kurumsal Őifreleme Sertifika İsim Alanı Bilgileri.....	46

## 1. Giriő

Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) tarafından oluőturulan Kamu Sertifikasyon Merkezi (Kamu SM), 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Bilgi Teknolojileri ve İletifim Kurumu'nun (BTK) yayımladıėı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliőkin Tebliė'de tanımlandıėı Őekliyle Elektronik Sertifika Hizmet Saėlayıcısı (ESHS) iőlevlerini yerine getirir.

2017/21 sayılı Baőbakanlık Genelgesi ile Kurumsal Őifreleme Sertifikalarının üretilmesi için TÜBİTAK bünyesindeki Kamu Sertifikasyon Merkezi (Kamu SM) yetkilendirilmiőtir. Kamu SM; 2019/DK-BTD/160 Sayılı Bilgi Teknolojileri ve İletifim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluőları Arasında Elektronik Ortamdaki Belge Paylaőımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliőkin Usul ve Esaslar'da belirtilen tanıma uygun olarak Kurumsal Őifreleme Sertifikası hizmeti saėlamaktadır.

Bu doküman, Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) tarafından oluőturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti'ne baėlı kamu kurum ve kuruluőlarına Kurumsal Őifreleme Sertifikası saėlayıcılıėı konusundaki faaliyetlerini nasıl yürüttüėünü anlatmak amacıyla yazmıő olduėu Sertifika Uygulama Esasları (SUE) dokümanıdır.

Kamu SM, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalıőır. SUE dokümanı, Kurumsal Őifreleme Sertifikalarının yönetimi ve kayıt iőlemleri sırasında yapılan iőlerin hangi ortamlarda ve nasıl yürütüldüėünü Sİ dokümanına baėlı olarak detaylandırarak anlatır. Bu SUE dokümanı, sertifika baővurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal iőlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; Kamu SM'nin, sertifika sahibinin ve üçüncü kiőilerin uygulama sorumluluklarını belirler.

Kamu SM'den Kurumsal Őifreleme Sertifikası talebinde bulunan tüzel kiőiler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiőtir sayılır. Kurumsal Őifreleme Sertifikası talebinde bulunan kurumlar bununla ilgili olarak taahhütnamelerde SUE dokümanına atıfta bulunurlar. Kurumsal Őifreleme Sertifikası sahibi kurumlar baővuru formu ve taahhütnamesini imzalayarak SUE dokümanında belirtilen esasları kabul ederler.

### 1.1. Genel Bakıő

SUE dokümanı, Kamu SM içinde yer alan sistem bileőenlerinin rollerini, sorumluluklarını ve iliőkilerini tanımlar; sertifika yönetim ve kayıt iőlemlerinin gerçekteőirilmesi Őeklini anlatır. Sertifika yönetimi, sertifika sahipleri için anahtar çifti ve sertifika üretmek, sertifikaları yayımlamak, yenilemek, askıya almak, askıdan indirmek, iptal etmek, sertifika iptal bilgisini yayımlamak, sertifika iőlemleri ile ilgili kiőileri baővuru ve sertifikanın durumu hakkında bilgilendirmek, gerekli kayıtları tutmak ve kayıt iőlemlerini gerçekteőirmek gibi iőlerden oluőur. Kayıt iőlemleri sertifika verilecek kurumların baővurularını, kurum bilgileri ve ilgili resmî belgeleri toplama, kurum kimliėi doėrulama, onaylama, iptal, yenileme isteklerini alma, deėerlendirme, onaylanan sertifika baővuru ve iptal istekleri doėrultusunda gerekli iőlemleri baőlatmayı içerir.

SUE dokümanı, "İnternet Açıık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices

Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki “Düzenlenmesine gerek duyulmamıştır” ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

## 1.2. Doküman Adı ve Tanımı

**Doküman Adı:** Kurumsal Őifreleme Sertifika Uygulama Esasları

**Doküman Sürüm Numarası:** 13

**Yayın Tarihi:** 13.04.2026

**Nesne Tanımlama Numarası:** 2.16.792.1.2.1.1.5.7.1.11

Bu doküman, Kamu SM'nin Kurumsal Őifreleme Sertifikası hizmeti verirken uyguladığı esasları tanımlayan SUE dokümanıdır ve kamu kurum ve kuruluşlarına verilen Kurumsal Őifreleme Sertifikalarını kapsar. SUE dokümanı <http://depo.kamusm.gov.tr/ilke/> adresinde kamuya açık olarak kesintisiz yayımlanmaktadır.

## 1.3. Sistem Bileşenleri

Bu doküman kapsamında tanımlanan sistem bileşenleri, Kamu SM'nin ESHS faaliyetlerinde rol alan ve sertifika hizmetleriyle ilgili hak ve yükümlülükleri bulunan taraflardır. Bu taraflar, ESHS, kayıt birimleri, sertifika sahipleri ve üçüncü kişiler olarak tanımlanır.

### 1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluşturma verisiyle imzalamak olan ESHS'ler, sertifika başvurusunda bulunan kurumların kayıt ve kimlik doğrulama işlemlerini yapmak, sertifikaların üretim, dağıtım, yenileme, askı, iptal, iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Kurumsal Őifreleme Sertifika Hizmet Sağlayıcısı (Kurumsal Őifreleme SHS) olarak kamu kurum ve kuruluşlarına Kurumsal Őifreleme Sertifikası hizmeti sağlamaktadır.

### 1.3.2. Kayıt Birimleri

Tüm kayıt işlemleri doğrudan Kamu SM personeli tarafından yürütülmektedir. Kayıt birimleri, Kamu SM'nin sertifika ve iptal başvurusu gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimdir. Bu birim, ilk müşteri kayıtlarını oluşturur, gerekli kurum kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim birimine yönlendirir.

### 1.3.3. Sertifika Sahipleri

Kamu SM'den kurumsal şifreleme sertifikası talep eden, DETSİS'te bilgileri bulunan, üretilen sertifikanın üzerinde kurum adları yer alan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan tüzel kişilerdir.

Sertifika sahibi kurum, taahhütnamelere uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda belirtilen işlemleri yapmaktan sorumludur.

### 1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kurum bilgileri ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir/kurumlardır. Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

### 1.3.5. Diđer BileŐenler

#### 1.3.5.1. Kurumsal Őifreleme Sertifikası Sorumlusu

Sertifika baŐvurusunda bulunan kurum tarafından yetkilendirilen ve sertifika y6netim s6re6lerinde Kamu SM ile iletiŐim i6inde olan kiŐi/kiŐilerdir.

Kurumsal Őifreleme sertifikaları i6in sertifika sahibi kurum tarafından onaylanan taahh6tname ile Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları belirlenmektedir.

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları Kamu SM tarafından kendisine imzalatılan taahh6tnamedeki Őartları yerine getirmekten sorumludur. Sertifika sorumluları, Kurumsal Őifreleme Sertifikasını kullanmaya yetkili olmak zorunda deđildir. Kurumsal Őifreleme Sertifikasını kullanmaya yetkili kiŐi/kiŐilerin belirlenmesi kurum inisiyatifindedir.

### 1.4. Sertifika Kullanımı

#### 1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı BaŐbakanlık Genelgesi ile elektronik ortamda iletilen resm6 yazıların Őifreli Őekilde g6nderilebilmesine imk6n sađlanmıŐtır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluŐları arasında elektronik ortamdaki belge paylaŐımında Őifreleme yapmak amacıyla g6ncel e-YazıŐma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

Kamu kurum ve kuruluŐları adına 6retilen Kurumsal Őifreleme Sertifikalarında bulunan imza dođrulama verisi, g6nderici kurumların Őifreli paket oluŐturabilmesi; sertifika sahibi kurumun himayesinde bulunan imza oluŐturma verisi ise kendisine g6nderilen Őifreli paketlerin a6ılabilmesi amacıyla kullanılır. Kurumsal Őifreleme Sertifikaları, bilgi ve belgelerin Őifrelenerek uzun s6reli saklanması ve elektronik imzalama amacıyla kullanılmaz.

#### 1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Őifreleme Sertifikası B6l6m 1.4.1'de belirtilen ama6lar dıŐında kullanılamaz. Belirtilen kapsam dıŐında kullanımdan dođan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, 6rettiđi sertifikaların hangi uygulamalarda ne ama6lar dođrultusunda kullanıldıđının kontrol6n6 yapmakla y6k6ml6 deđildir.

### 1.5. Uygulama Esaslarının Y6netimi

#### 1.5.1. Dok6man Y6netimi

SUE dok6manı Kamu SM tarafından yazılmıŐtır. Kamu SM, gerekli g6rd6đ6 durumlarda SUE dok6manında deđiŐiklik yapabilir.

#### 1.5.2. İletiŐim Bilgileri

Bu SUE dok6manının uygulanması ve ilgili y6netim ilkeleri hakkındaki sorular Kamu SM'nin aŐađıdaki eriŐim noktalarına y6nlendirilebilir:

**Adres** : Kamu Sertifikasyon Merkezi, T6BİTAK YerleŐkesi, PK. 74, 41470 Gebze-KOCAELİ

**Tel.** : (262) 648 18 18

**Faks** : (262) 648 18 00

**E Posta** : [bilgi@kamusm.gov.tr](mailto:bilgi@kamusm.gov.tr)

**URL** : <https://kamusm.bilgem.tubitak.gov.tr>

Kamu SM, SUE dokümanını herkesin erişimine açık bulunan aşağıdaki internet adresinden yayımlar:

- <http://depo.kamusm.gov.tr/ilke/>
- [https://kamusm.bilgem.tubitak.gov.tr/depo/ilke\\_ve\\_uygulama\\_esaslari/guncel\\_ilke\\_ve\\_uygulama\\_esaslari.jsp](https://kamusm.bilgem.tubitak.gov.tr/depo/ilke_ve_uygulama_esaslari/guncel_ilke_ve_uygulama_esaslari.jsp)

### 1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluęunu Belirleyen KiŐi

Bu SUE dokümanının uygunluęu Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

### 1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

Bu SUE dokümanının yayımlanma onayı, Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından gerçekleştirilen incelemelerden sonra verilir.

## 1.6. Tanımlar ve Kısaltmalar

### 1.6.1. Tanımlar

**Akıllı Kart veya HSM EriŐim Verisi:** Sertifika sahibine ait imza oluŐturma verisine erişimin kontrolünü saęlayan PIN ve PUK bilgisidir.

**Akıllı Kart:** Sertifika ve sertifika ile iliŐkili imza oluŐturma verisinin içinde bulunduęu güvenli donanımdır.

**Anahtar Çifti:** İmza oluŐturma ve onunla iliŐkili olan imza doęrulama verisi çiftidir.

**Bilgi Deposu:** Sertifikaların, sertifika iptal durum kayıtlarının ve dięer sertifika işlemleri ile ilgili bilgilerin yayımlandıęı dizin sunucular gibi veri saklama ortamlarıdır.

**ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü):** Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öğrenmelerine imkân tanıyan standart iletişim kuralıdır.

**DETSİS (Devlet TeŐkilatı Merkezi Kayıt Sistemi):** Türkiye Cumhuriyeti devlet teŐkilatı içerisinde yer alan kurum ve kuruluşların merkez, taŐra ve yurt dıŐı teŐkilatlarında bulunan her düzeydeki birimleri ile birlikte hiyerarŐik yapıya uygun olarak kayıt altına alındıęı sistemdir.

**EYP (e-YazıŐma Projesi):** Kamu kurum ve kuruluşları arasındaki resmî yazıŐmaların elektronik ortamda yürütölmesini amaçlayan projesidir.

**HSM (Hardware Security Module):** Sertifikanın kriptografik anahtarlarının içinde bulunduęu harici aygıt; donanımsal güvenlik modölüdür.

**HSM Cihaz Sorumlusu:** HSM sahibi kurum tarafından yetkilendirilen, Kamu SM ile kurum arasında HSM cihazına anahtar çifti ve sertifika yükleme ile ilgili süreci yürütecek kişidir.

**İlgili Mevzuat:** “5070 Sayılı Elektronik İmza Kanunu”, “2017/21 Sayılı BaŐbakanlık Genelgesi”, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan “Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslar” ve “Elektronik Mühre İliŐkin Usul ve Esaslar Hakkında Yönetmelięi” ifade eder.

**İmza Doęrulama Verisi:** İlgili imza oluŐturma verisi sahibinin herkes ile paylaşılabilirdięi, imza oluŐturma verisi ile oluŐturduęu dijital imzaların doęrulanmasında ve/veya kendisine Őifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileŐenidir.

**İmza OluŐturma Verisi:** Anahtar çiftinin sahibi tarafından gizli tutulan ve dijital imza oluşturmak ve/veya ilgili imza dođrulama verisi ile ŐifrelenmiŐ elektronik kayıtların, dosyaların Őifresini çözmek için kullanılan anahtardır.

**İptal Durum Kaydı:** Kullanım süresi dolmamıŐ sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceđi kayıtlardır.

**Kamu SM (Kamu Sertifikasyon Merkezi):** Türkiye Bilimsel ve Teknolojik AraŐtırma Kurumu'na (TÜBİTAK) bađlı BiliŐim ve Bilgi Güvenliđi İleri Teknolojiler AraŐtırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sađlamak üzere oluşturulan birimdir.

**KEP (Kayıtlı Elektronik Posta):** E-postanın gönderim ve alımına dair kanıtların oluşturulup saklandıđı e-posta iletim hizmetidir.

**Kök Sertifika Hizmet Sađlayıcısı:** Kamu Sertifikasyon Merkezi içinde oluşturulmuŐ, en yetkili imza derecesi verilmiŐ ve sertifikasını kendisi imzalamıŐ olan Sertifika Hizmet Sađlayıcısıdır.

**Kurum:** TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi'nden Kurumsal Őifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Őifreleme Sertifikası almaya yetkisi olan tüzel kişiliktir.

**Kurum Doküman Dođrulama Sistemi:** Elektronik ortamda hazırlanan belgelerin dođrulanması iŐleminde kullanılacak kuruma ait sistem veya e-Devlet belge dođrulama sistemidir. **Kurumsal Őifreleme SHS (Kurumsal Őifreleme Sertifika Hizmet Sađlayıcısı):** Kamu Sertifikasyon Merkezi içinde oluşturulmuŐ, Kök Sertifika Hizmet Sađlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluşturup imzalamakla yetkili kılınmıŐ Elektronik Sertifika Hizmet Sađlayıcısıdır.

**Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları:** Kamu kurumlarının baŐvuru formu ve taahhütname ile Kamu SM'ye bildirdiđi ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde kurumu temsile yetkili kiŐi/kiŐilerdir.

**Kurumsal Őifreleme Sertifikası:** Elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla kullanılan imza dođrulama verisini içeren elektronik sertifikadır.

**MERNİS (Merkezi Nüfus İdare Sistemi):** Kâğıt ortamında bulunan nüfus kayıtlarının elektronik ortama aktarılarak merkezi bir yapıda tutulmasını sađlayan projedir.

**Nesne Tanımlama Numarası:** Herhangi bir nesneyi eşsiz olarak tanımlayan, uluslararası standart belirleyen bir kuruluŐtan alınan numaradır.

**SİL (Sertifika İptal Listesi):** İptal olmuŐ sertifika bilgilerinin içinde yer aldığı, ESHS'nin imzasını taşıyan elektronik dosyadır.

**Sertifika Süresi:** Üretim anında sertifikanın içine yazılan, sertifikanın geçerlilik baŐlangıç ve bitiŐ tarihleri arasında kalan süredir.

**Sİ/SUE (Sertifika İlkeleri ve Uygulama Esasları):** Kamu SM resmî web sitesi Bilgi Deposu menüsü altındaki İlke ve Uygulama Esasları'nda Elektronik Sertifika Hizmet Sađlayıcısı'nın (ESHS) iŐleyiŐi ile ilgili genel kuralları ve bu kuralların nasıl uygulanacağını detaylı olarak anlatan belgelerdir.

**Tebliđ:** 6/1/2005 tarihli ve 25692 sayılı Resmî Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'dir.

**Üçüncü KiŐiler:** Sertifikalara güvenerek iŐlem yapan gerçek veya tüzel kişilerdir.

**Zaman Damgası:** Bir elektronik verinin, üretildiđi, deđiŐtirildiđi, gönderildiđi, alındıđı ve/veya kaydedildiđi zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla dođrulanan kaydı ifade eder.

### 1.6.2. Kısaltmalar

**BGYS:** Bilgi Güvenliđi Yönetim Sistemi

**BTK:** Bilgi Teknolojileri ve İletişim Kurumu

**CEN (Comité Européen de Normalisation):** Avrupa Standardizasyon Komitesi

**CWA (CEN Workshop Agreement):** CEN Çalıştay Kararı

**ÇİSDUP (OCSP):** Çevrim İçi Sertifika Durum Protokolü (Online Certificate Status Protocol)

**EAL (Evaluation Assurance Level):** Deđerlendirme Garanti Düzeyi

**ECDSA (Elliptic Curve Digital Signature Algorithm):** Eliptik Eğrisi Sayısal İmza Algoritması

**ESHS:** Elektronik Sertifika Hizmet Sağlayıcısı

**ETSI (European Telecommunications Standards Institute):** Avrupa Telekomünikasyon Standartları Enstitüsü

**ETSI TS (ETSI Technical Specification):** ETSI Teknik Özellikleri

**FIPS PUB (Federal Information Processing Standards Publications):** Federal Bilgi İşleme Standartları Yayınları

**IETF RFC (Internet Engineering Task Force Request for Comments):** İnternet Mühendisliđi Görev Grubu Yorum Talebi

**ISO/IEC (International Organization for Standardization/International Electrotechnical Commission):** Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komisyonu

**ITU (International Telecommunication Union):** Uluslararası Telekomünikasyon Birliđi

**Kamu SM:** Kamu Sertifikasyon Merkezi

**MERNİS:** Merkezi Nüfus İdare Sistemi

**PKI (Public Key Infrastructure):** Açık Anahtar Altyapısı

**RSA:** Rivest Shamir Adleman (Algoritmayı bulan kişilerin baş harfleri)

**SHA (Secure Hash Algorithm):** Güvenli Özet Algoritması

**Si/SUE:** Sertifika İlkeleri/ Sertifika Uygulama Esasları

**SiL:** Sertifika İptal Listesi

## 2. Yayınlama ve Bilgi Deposu Yükümlülükleri

Bilgi deposu, Kamu SM'nin kendisine ait sertifikaları, iptal durum kayıtlarını, Si/SUE gibi ilgili dokümanları sertifika sahibi kurumların ve üçüncü kişilerin ulaşabileceđi şekilde kesintisiz, güvenli ve ücretsiz olarak yayınladıđı ortamdır.

Kamu SM'nin bilgi deposuna internet üzerinden erişilir. İnternet üzerinden Kamu SM hakkında bilgiler, sertifika yönetimiyle ilgili dokümanlar, teknik bilgilendirme dokümanları, başvuru formları ve duyurular yayımlanır.

## 2.1. Bilgi Depoları

Kamu SM, bilgi deposu olarak internet üzerinden hizmet veren servisleri kullanmaktadır. Bilgi depolarına erişim adresleri ve erişilebilen bilgiler aşağıda verilmektedir.

<https://kamusm.bilgem.tubitak.gov.tr> internet adresi üzerinden yayımlanan Bilgi Deposu'nda sertifika sahibi kurumlara imzalatılan başvuru formu ve taahhütnameler, Sİ/SUE dokümanları, sertifika hizmetleri ile ilgili yönergeler, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

## 2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

Kamu SM'nin bilgi deposunda sistemin iç işleyiŐi ile ilgili olanlar hariç olmak üzere aşağıdaki bilgiler bulunur:

- Kamu SM'ye ait güncel Kök SHS ve Kurumsal Őifreleme SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Kurumsal Őifreleme SHS sertifikaları
- Kamu SM'ye ait sertifikaların özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduđu bilgisi
- Kamu SM Sİ/SUE dokümanları
- Taahhütnameler
- Yönergeler
- Formlar
- Sertifika iptal durum kayıtları

## 2.3. Yayım Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ/SUE dokümanları içeriğinin deđişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip mümkün olan en kısa sürede yayımlanır.

Sertifika iptal durum kayıtlarının yayımlanma sıklığı bu dokümanda Bölüm 4.9.7 ve 4.9.9'da belirtilmektedir.

## 2.4. EriŐim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır. Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM personeli tarafından yapılmaktadır. Kamu SM, bilgi deposu ile ilgili olarak aşağıdaki yükümlölükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve deđiŐtirilmeye karşı bütünlüğünü korumak
- Bilgi deposunda tutulan bilgilerin doğruluđu ve güncelliğini sağlamak
- Bilgi deposunu sürekli olarak katılımcıların erişimine açık tutmak
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak
- Bilgi deposuna erişimi ücretsiz sağlamak

## 3. Kimlik Belirleme ve Doğrulama

Kurumsal Őifreleme Sertifikası ile ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kurumun kimlik tanımlama ve doğrulaması yapılır. Bu bölümde Kurumsal Őifreleme Sertifikası yönetim prosedürleri içinde uygulanan kurum kimlik tanımlama ve doğrulama yöntemleri ile Kurumsal Őifreleme Sertifikası içinde yazılan kurum bilgileri anlatılmıştır.

### 3.1. İsimlendirme

#### 3.1.1. İsim Alanı Tipleri

Kurumsal Őifreleme Sertifikalarında Kamu SM ve sertifika sahibi kurumlara ait bilgilerin belirtildiĐi DN [Distinguished Name (Ayırt edici isim)] alanı iinde "ITU X.500" biiminin desteklediĐi isim tipleri kullanılır.

#### 3.1.2. Kimlik Bilgilerinin TeŐhise ElveriŐli Olması

Kurumsal Őifreleme Sertifikaları ieriĐindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimliĐinin tespit edilmesini saĐlayan niteliktedir.

#### 3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Kurumsal Őifreleme Sertifikası ieriĐinde takma isim veya lakap kullanılmasına izin verilmez.

#### 3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Kurumsal Őifreleme Sertifikası iinde ITU X.500 biimi dıŐında isim alanı tipi kullanılmaz.

#### 3.1.5. Kimlik Bilgilerinin TekilliĐi

Kurumsal Őifreleme Sertifikası ieriĐindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum iin ayırt edici niteliktedir. Aynı kuruma ait Kurumsal Őifreleme Sertifikaları ieriĐindeki kurum bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kurumlara ait Kurumsal Őifreleme Sertifikaları ieriĐindeki kurum bilgilerinin aynı olması engellenmektedir. Bunun saĐlanabilmesi iin Kurumsal Őifreleme Sertifikalarının isim alanı iinde benzersiz bir sayı olduĐu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

#### 3.1.6. Markanın Tanınması, DoĐrulanması ve Rolü

Düzenlenmesine gerek duyulmamıŐtır.

### 3.2. İlk Kimlik DoĐrulama

Kamu SM Kurumsal Őifreleme Sertifikası hizmetlerinden faydalanmak iin baŐvuruda bulunulduĐunda, ilgili kurumun doĐrulanabilmesi iin aŐaĐıda tanımlanan yöntemler uygulanır.

#### 3.2.1. İmza OluŐturma Verisi SahipliĐinin Kanıtlanması

Sertifika sahibine ait imza doĐrulama ve imza oluŐturma verisi, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir.

Kurumsal Őifreleme Sertifikası, baŐvuru sırasında belirlenen sertifika sorumlusu/sorumlularına imza karŐılıĐında teslim edilir. Akıllı kart ierisinde teslim edilen kurumsal Őifreleme sertifikasının teslim teyidi Online İŐlemler üzerinden alınır. HSM'ye yüklenmesi talep edilen sertifikaların teslim teyidi iin Kurum HSM Cihaz Sorumlusuna kurulum tutanaĐı imzalatılır.

#### 3.2.2. Kurumsal KimliĐin Belirlenmesi

Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan kurumlar, talep edilen kurum bilgilerini, Kamu SM tarafından sunulan baŐvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, kurum tarafından iletilen bilgilere istinaden kurum kimliĐini doĐrular. Kurumların sertifika alma yetkisi DETSİS aracılıĐıyla kontrol edilir. BaŐvuru esnasında sertifika iŐlemlerini kurum adına yürütecek Kurumsal Őifreleme Sertifikası Sorumluları da belirlenerek Kamu SM'ye iletilir.



Mühür/Kurumsal Őifreleme Sertifika Sorumlusu telefon ile aranarak kimlik doęrulama gerekleřtirilir ve iptal talebi teyit edilir.

#### 4. Sertifika Yařam Döngüsü İřlevsel Gereklilikleri

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Süreçlerle ilgili ayrıntılar Kamu SM'nin internet sitesinde belirtilmektedir. Sertifika yönetimi ařaęıdaki süreçlerden oluşmaktadır:

- Sertifika başvurusu
- Sertifika yenileme
- Sertifika askıya alma ve askıdan indirme
- Sertifika iptal etme

Süreçler sertifika sahibi kurumlar ile kurum tarafından yetkilendirilen sertifika sorumlusu/sorumluları ve Kamu SM arasında gerekleřtirilen işlemlerden oluşmaktadır.

##### 4.1. Sertifika Başvurusu

###### 4.1.1. Sertifika Başvurusunu Kimlerin Yapabildięi

DETSİS'te bilgileri bulunan ve DETSİS tarafından Kurumsal Őifreleme Sertifikası alma yetkisi olduęu belirtilen kamu kurum ve kuruluşları Kurumsal Őifreleme Sertifikası başvurusunda bulunabilirler.

Başvuru süreci, kamu kurumunun resmî yazısı ekinde Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ile HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesini Kamu SM'ye göndermesiyle başlar. Belgelerin iletim yöntemi Kamu SM resmî internet sitesinden yayımlanır. Kurumun sertifika başvuru işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumlusu/sorumluları tarafından yürütülür.

###### 4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Őifreleme Sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacaęı sertifika hizmetlerinin şartları sertifika sahibi kurumun imzaladıęı başvuru formu ve taahhütnameler, Kamu SM'nin internet üzerinden yayımladıęı ilgili yönergeler, Sİ/SUE dokümanları doęrultusunda belirlenir.

Kurum, Kamu SM web sitesinde yayımlanan Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesini doldurur. Ardından üst yazısıyla birlikte Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi eki de imzaya dahil olacak şekilde E-Yazışma Teknik Rehberin'nin güncel haline uygun EYP dosyası oluşturularak e-posta veya KEP üzerinden Kamu SM'ye iletir. Kurum, Kurumsal Őifreleme Sertifikasını HSM içerisinde kullanmayı tercih ederse HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesi dosyasını da EYP formatı imzalı eklerine dahil etmelidir. EYP dosyası, başvuru formunda yetkili olarak belirtilen sertifika sorumlularından birine ait kurumsal e-posta veya KEP adresi üzerinden iletilmelidir. Bunun mümkün olmadığı durumlarda başvuru evrakları Kamu SM ile görüşülerek alınan onaya istinaden harici depolama aygıtı ile gönderilebilir.

Cumhurbaşkanlığı tarafından 10.06.2020 tarihli ve 2646 sayılı Resmî Gazetede yayımlanan "Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" in, 4. Maddesi gereęince; kamu kurum ve kuruluşlarınca resmî yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu kapsamda, zorunlu haller veya

olađanüstü durumlar dıŐında EYP dosyası ile baŐvuru dıŐında baŐvurular kabul edilmeyecektir. Zorunlu hallerde veya olađanüstü durumlarda resmî yazıŐmalar, KEP veya kurumsal e-posta yoluyla iletilen ilgili baŐvuru formu ve taahhütnamelerin dođrulanmasının ardından ıslak imzalı ve mühürlü olacak Őekilde üst yazısıyla birlikte Kamu SM'ye posta yoluyla iletilir. Kurumsal Őifreleme Sertifikası baŐvurusunun nasıl yapılacađı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kurum baŐvuru sırasında Kamu SM'ye dođru bilgi beyan etmekle sorumludur. Kurum, Kamu SM'ye göndermiŐ olduđu bilgilerin dođruluđunu takip etmekle ve bu bilgilerde deđiŐiklik olması halinde belirlenmiŐ araç ve yöntemler ile Kamu SM'yi bilgilendirmekle yükümlüdür. Kamu SM, Kurumsal Őifreleme Sertifikası içinde yer alacak bilgilerin dođruluđunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliđini sađlamak için gerekli tedbirleri alır.

Kamu SM, sertifika verilecek kurumların kimlik tanımlama ve dođrulama iŐlemlerini yaptıktan sonra baŐvurularını deđerlendirir ve uygun görülen baŐvuruları onaylayarak iŐleme alır.

## 4.2. Sertifika BaŐvurusunun İŐlenmesi

### 4.2.1. Kimlik Tanımlama ve Dođrulama İŐlevlerinin Yerine Getirilmesi

BaŐvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve dođrulama iŐlevleri yerine getirilir. Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan kurumların Kamu SM'ye gönderdiđi bilgi ve belgeler aŐađıda sıralanmıŐtır:

- Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi
- Kurum tarafından yazılan resmî yazı
- HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesi

Kurum tarafından gönderilen belgelerin dođrulanması için aŐađıdaki kontroller yapılır:

- Kurum tarafından gönderilen EYP dosyası kontrol edilerek üst yazı ve eklerinin e-imza dođrulaması yapılır.
- EYP dosyası içerisinde üst yazıda yer alan belge dođrulama kodu ile Kurum Doküman Dođrulama Sistemi üzerinden kurum dođrulaması gerçekteŐtirilir.
- BaŐvuru evraklarında yer alan kurum DETSİS numarası, DETSİS üzerinden sađlanan servis aracılıđıyla kontrol edilerek kurumun Kurumsal Őifreleme Sertifikası almaya yetkili olup olmadıđı sorgulanır.
- Kurum tarafından gönderilen Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesinde yer alan kurumun adı, vergi kimlik numarası, yetkilendirilen Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının T.C. kimlik numarası, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgilerinde eksiklik olup olmadıđı kontrol edilir.
- Belgelerin elektronik ortamdan iletimi mümkün olmadıđı durumda kurumdan evrak asılları talep edilir. Evrak asılları ulaŐan kurumların baŐvurularını dođrulamak için, KEP ile gönderilen evraklar ile evrakların asılları karŐılaŐtırılarak birbirinin aynı olduđu dođrulandır. KEP kullanmayan kurum baŐvurularını dođrulayabilmek için kuruma iki seçenek sunulur; resmî olarak sahibi oldukları web sitelerinin belirlenen dosya yoluna elektronik ortamda ilettikleri baŐvuru evraklarının özet deđeri eklenmeli veya baŐvuru formunda kurum onayını veren üst düzey yetkili ses kaydı alabilen telefon ile aranarak dođrulama onayı alınmalıdır.

Bilgi ve belgeler hatasız ve tam ise kurum kimlik tanımlama ve dođrulama iŐlemi tamamlanır. Belgelerde gözle görölen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kurum kimlik tanımlaması ve dođrulaması yapılamaz. Başvuru evraklarının, tanımlanan yöntemler dışında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

#### 4.2.2. Sertifika Başvurusunun Kabul veya Reddi

“Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslar”ın ikinci bölüm, 5’inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS’te bilgileri bulunmayan veya Kurumsal Őifreleme Sertifikası almaya yetkisi olmayan tarafların başvurusunu reddeder.

Buna ek olarak, Bölüm 4.2.1’deki kontrollerin yapılması sonucunda, başvuru sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyen kurumlarla ilgili yazılı bilgilendirme, Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının başvuru sırasında beyan ettikleri e-posta adresleri aracılığı ile yapılır ve gerekli görölen bilgi ve belgeler tekrar talep edilir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilen kurumlar, Kamu SM sisteminde tanımlanır ve sertifika üretim süreci başlatılır.

#### 4.2.3. Sertifika Başvurusunun İŐlenme Zamanı

Başvuru evraklarının eksiksiz bir şekilde Kamu SM’ye ulaşması ve dođrulanmasının ardından en fazla 15 (on beŐ) iŐ günü içerisinde sertifika başvurusu iŐleme alınır ve sonuçlandırılır.

### 4.3. Sertifikanın OluŐturulması

#### 4.3.1. Sertifika OluŐturulmasında ESHS’nin İŐlevleri

Bölüm 4.2.2’de yer alan esaslar uyarınca kabul edilen sertifika başvuruları Kamu SM tarafından iŐlenir. Kurum, iŐlem kapasitesini göz önünde bulundurarak başvuru sırasında sertifikanın yükleneceđi donanım olarak akıllı kart ya da HSM tercih eder.

Kurumsal Őifreleme Sertifikası, kayıp veya arıza gibi durumlarda kurumun iŐlemlerinde aksaklık yaŐanmaması amacıyla biri yedek olmak üzere 2 adet üretilir.

Kamu SM tarafından üretilen kurumsal Őifreleme sertifikaları; BTK tarafından yayımlanan 2019/DK-BTD/160 sayılı Kurul Kararı Madde 5’de belirtilen hüküm ve niteliklere uygun olarak üretilir.

#### 4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta yüklenen sertifika, sertifika sorumlusuna teslim edildiđinde Kurumsal Őifreleme Sertifikasının oluşturulduđu konusunda bilgilendirilmiŐ olur.

HSM cihazına sertifika yükleme iŐlemi, HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir. İŐlem sonrasında kurulum tutanađı imzalanır ve Kurumsal Őifreleme Sertifikasının oluşturulduđu konusunda HSM sorumlusu bilgilendirilmiŐ olur.

#### 4.4. Sertifikanın Kabulü

##### 4.4.1. Sertifikanın Kabul Koőulu

Akıllı karta yüklenen Kurumsal Őifreleme Sertifikası anlaşmalı kurye ile kurum adresine gönderilir. Kurumsal Őifreleme Sertifikası, başvuruda belirtilen sertifika sorumlusu/sorumlularına teslim edilir. Sertifika sorumlusu kendisine teslim edilen zarf içerisinde sertifika bulunmuyorsa zarfı teslim almadan iade eder.

Kurumsal Őifreleme Sertifikasının HSM'ye yüklenmesi talebi durumunda kuruma yerinde ve uzaktan olmak üzere iki farklı yükleme seçeneđi sunulmaktadır. Yerinde yükleme, kurum tarafından belirtilen zorunlu hallerde Kamu SM personelinin kurum yerleşkesine gidip HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini yerinde gerçekleőtirdiđi süreçtir. Uzaktan yükleme, Kamu SM ve kurum arasında yapılan güvenli uzak bağlantı sonrası Kamu SM personelinin HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini uzaktan gerçekleőtirdiđi süreçtir. Her iki süreç de başvuruda HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesinde belirtilen Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilmektedir.

Sertifika sorumlusu/sorumluları, sertifikanın içeriđini kontrol eder, herhangi bir eksiklik veya hata olması durumunda 5 (beő) iş günü içerisinde Kamu SM'yi bilgilendirir, aksi halde sertifikayı kabul etmiő sayılır.

##### 4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM tarafından üretilen ve askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e yüklenmektedir.

##### 4.4.3. Sertifikanın Oluőturulmasının Diđer Tarafalara Duyurulması

Kamu SM tarafından üretilen ve askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e yüklenmektedir.

#### 4.5. Sertifikanın ve İmza Oluőturma Verisinin Kullanımı

##### 4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluőturma Verisi Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait imza oluőturma verisi; tabi olunan standartlar, ilgili mevzuat, Sİ/SUE dokümanı ve ilgili başvuru formu ve taahhütnamesinde yer alan koőullar ve belirlenmiő sınırlar içinde kullanılmalıdır.

Sertifika sahibi, imza oluőturma verisini yetkisiz kiőilerin erişimine karşı korumakla yükümlüdür. Kurumsal Őifreleme Sertifikasına karşılık gelen imza oluőturma verisi yalnızca sertifikada "Anahtar Kullanımı" alanında belirtilen amaçlar dahilinde kullanılabilir.

##### 4.5.2. Üçüncü Kiőilerin Sertifika ve İmza Doğrulama Verisi Kullanımı

Sertifika sahibine ait Kurumsal Őifreleme Sertifikasının içinde yer alan imza doğrulama verisi, üçüncü kiőilerce e-Yazışma Projesi kapsamında verilerin şifreli iletimi amacıyla kullanılır. İmza doğrulama verisinin veya sertifikanın, belirtilen amaç dışında kullanılması sonucu oluőabilecek zararlardan üçüncü kiőiler sorumludur.

#### 4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, kullanım süresi dolan sertifikalarda, sertifikada yer alan bilgiler deęişmeden aynı anahtar çifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. Kamu SM bu işlemi gerçekleştirmez.

#### 4.7. Sertifika Yenileme

Kamu SM, sertifika yenileme işlemi, yeni anahtar çifti üretmek suretiyle yerine getirir.

##### 4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi aşağıdaki durumlarda yapılmaktadır:

- Kurumsal Şifreleme Sertifikasının kaybedilmesi veya çalınması
- Kurumsal Şifreleme Sertifikasını içeren donanımın arızalanması
- Akıllı karta veya HSM'ye erişim verisinin kaybedilmesi, çalınması veya unutulması
- Kurumsal Şifreleme Sertifikasının iptal edilmesi ve yenisinin talep edilmesi
- Kurumsal Şifreleme Sertifikasının geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaşılması
- Kurumsal Şifreleme Sertifikasında bilgi deęişikliği gerekmesi

##### 4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildięi

Daha önce Kamu SM'den Kurumsal Şifreleme Sertifikası temin eden ve sertifika alma yetkisi olan kamu kurum ve kuruluşları Kurumsal Şifreleme Sertifikası yenileme başvurusunda bulunabilirler.

Yenileme süreci, Elektronik Mühür/Kurumsal Şifreleme Başvuru Listesinin eksiksiz bir şekilde doldurularak Kamu SM'ye iletilmesiyle başlar. Kurumun sertifika yenileme işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumluları tarafından yürütülür.

##### 4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Yenileme süreci, sertifikanın bitimine 3 ay kala başlatılabilir. Kamu SM, yenileme sürecinde kurumların sorun yaşamaması amacıyla kurum sertifika sorumlularının kayıtlı kurumsal e-posta adresleri üzerinden sertifika bitiş tarihine 3 ay, 2 ay, 1 ay, 15 gün ve 1 hafta kala kuruma hatırlatma maili göndermektedir.

Elektronik Mühür/Kurumsal Şifreleme Başvuru Listesi eksiksiz şekilde doldurularak sertifika sorumlularından biri tarafından elektronik imzalanmış bir şekilde (BES formatında ve .p7s uzantılı olarak), [bilgi@kamusm.gov.tr](mailto:bilgi@kamusm.gov.tr) veya [kurumsal\\_bilgi@kamusm.gov.tr](mailto:kurumsal_bilgi@kamusm.gov.tr) e-posta adresine iletilir. Sertifika HSM içerisinde kullanılacaksa başvuru listesinde yer alan "HSM Bilgileri" de kurum tarafından doldurulmalı ve liste HSM Cihaz Sorumlusu tarafından da seri olarak imzalanmalıdır.

Bilgi ve belgeler hatasız ve tam ise gerekli doğrulamalar yapılır. Belgelerde gözle görülen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda doğrulama yapılamaz. Başvuru evraklarının, tanımlanan yöntemler dışında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir. Başvurusu kabul edilen kurumların sertifika yenileme süreci başlatılır.

##### 4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

#### 4.7.5. Sertifika Yenileme Sonrası Kabul Koőulu

Bölüm 4.4.1'de tanımlanmaktadır.

#### 4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması

Bölüm 4.4.2'de tanımlanmaktadır.

#### 4.7.7. Sertifika Yenilemenin Diđer Tarafllara Duyurulması

Bölüm 4.4.3'te tanımlanmaktadır.

### 4.8. Sertifikada Bilgi DeęiŐiklięi

Sertifikada bilgi deęiŐiklięi, anahtar çifti hariç sertifikada yer alan bilgilerin deęiŐmesi olarak tanımlanmaktadır. Sertifika içerisinde yer alan bilgilerin deęiŐmesi durumunda, Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi dokümanında BaŐvuru Nedeni "Kurum Ad/Ünvan/DETSİS ID DeęiŐiklięi" sečilerek yeniden baŐvuru yapılması gerekmektedir.

### 4.9. Sertifikanın İptali ve Askıya Alınması

#### 4.9.1. Sertifikanın İptal Edildięi Durumlar

Sertifikanın kullanım süresi dolmadan geçerlilięini yitirdięi durumlarda, sertifika iptal edilir. İptal edilen sertifikayla bir daha işlem yapılamaz. Sertifika, aŐaęıda belirtilen durumlarda iptal edilir:

- Sertifika sahibi kurumun talebi
- Sertifika içerięindeki bilgilerin sahtelięinin veya yanlışlıęının ortaya çıkması veya bilgilerin deęiŐmesi
- Kurumun sertifika alma yetkisinin olmadıęının anlaşılması
- Sertifika sahibi kurumun kapanması
- Sertifika sahibi kurumun adının deęiŐmesi
- Sertifika sahibi kurumun DETSİS numarasının deęiŐmesi
- İmza oluŐturma verisinin güvenlięinin kaybedildięinden Őüphelenilmesi
- İmza oluŐturma verisinin içinde bulunduęu aracın kaybolması, çalınması veya bozulması
- Akıllı kart veya HSM eriŐim verisinin unutulması veya kaybedilmesi
- Sertifikanın taahhütnameler veya Sİ/SUE dokümanında belirtilen Őartlara aykırı kullanımının tespit edilmesi
- Kamu SM'ye evrakları gönderen sertifika sorumlusu/sorumlularının kurumun onayını almadıęının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM'ye bildirilmesi
- Sertifikanın hatalı üretilmesi
- Kamu SM'nin Kurumsal Őifreleme Sertifikasını imzalamak için kullandıęı imza oluŐturma verisinin bütünlüęünün bozulması veya gizlilięinin ortadan kalkması
- Kamu SM'nin işleyiŐine son verilmesi ve verilen Kurumsal Őifreleme Sertifikalarının yönetim işlemlerinin baŐka bir ESHS tarafından devamlılıęının sağlanamaması

#### 4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiş Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından yapılabilir. Kamu SM, Bölüm 4.9.1’de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

#### 4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Kurumsal Őifreleme Sertifikası iptal işlemi, kurum tarafından yetkilendirilen Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından Kamu SM resmî internet sitesinde yer alan Online İşlemler menüsü aracılığı ile yapılır.

Kamu SM Online İşlemler üzerinden yapılan iptal başvurusunda, Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları sisteme kimlik doğrulamasıyla giriş yaparak iptal talebinde bulunur. İlgili talebin ardından, Kurumsal Őifreleme Sertifikası Kamu SM sisteminde otomatik olarak iptal edilir ve DETSİS sisteminden silinir.

İptal işlemlerinin Kamu SM Online İşlemler üzerinden yapılamadığı durumda Kamu SM web sitesinde belirtilen yöntemlerle iptal işlemi gerçekleştirilebilir.

İptal sürecinin web sitesinde belirtilen yöntemle fiziksel olarak yürütülmesi durumunda sürecin başlatılmasının ardından evrak asılları Kamu SM’ye ulaşana kadar kurum yazışmalarında yaşanabilecek aksaklıkların en aza indirgenmesi amacıyla Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları telefon ile aranarak iptal talebi teyit edilir ve iptali talep edilen sertifika askıya alınır. Evrak asıllarının ulaşmasının ardından Kamu SM’ye e-posta üzerinden gönderilen evraklar ile asılları karşılaştırılır ve askıya alınan sertifika iptal edilir.

Kurumsal Őifreleme Sertifikası iptal edildikten sonra, Kamu SM sertifika sahibi kurumu ve gerekirse sertifika sorumlularını iptal işlemine dair bilgilendirir. Kurumsal Őifreleme Sertifikaları geçmişe yönelik olarak iptal edilmez.

Kamu SM iptal bilgilerini en kısa zamanda işleyerek SİL yayımlamak ve ÇİSDUP Yanıtlayıcı’da Kurumsal Őifreleme sertifikasının durumunu iptal konumuna getirmek suretiyle kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en az Kurumsal Őifreleme sertifikasının seri numarası ile Kamu SM’nin elektronik imzasını taşır. SİL dosyası, Kamu SM’ye ait imza oluşturma verisiyle imzalanır. İptal edilen Kurumsal Őifreleme Sertifikaları geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra Kurumsal Őifreleme Sertifikası SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı’da geçerlilik süresi dolan iptal edilmiş Kurumsal Őifreleme Sertifikalarının durumu iptal edilmiş olarak görünmeye devam eder.

Kurum, Kurumsal Őifreleme Sertifikası iptal edildikten sonra yeniden Kurumsal Őifreleme Sertifikası talebinde bulunulabilir.

#### 4.9.4. İptal İsteđi Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

#### 4.9.5. İptal İsteđinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve Kurumsal Őifreleme Sertifikasını en geç 24 saat içerisinde iptal eder. İptal edilen Kurumsal Őifreleme Sertifikası bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı’dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL’in yayımlanma süresi Bölüm 4.9.7’de belirtilmiştir.

#### 4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliđi

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, sorgulama yapacak kişinin kimlik doğrulamasına gerek kalmadan dileyen herkes tarafından erişilebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliđini sağlar.

Üçüncü kişiler Kurumsal Şifreleme Sertifikasına dayanarak işlem yapmadan önce Kurumsal Şifreleme Sertifikasının geçerliliđini SİL ya da ÇİSDUP üzerinden kontrol etmekle yükümlüdür.

Üçüncü kişiler Kurumsal Şifreleme Sertifikası geçerlilik kontrolünü yaptıđı SİL dosyasının veya ÇİSDUP Yanıtlayıcı'dan aldıđı iptal durum kaydının Kamu SM'ye ait imza oluŐturma verisiyle imzalandıđını kontrol eder. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri Bölüm 9.6.4'te belirtilmiŐtir.

#### 4.9.7. Sertifika İptal Listesi Yayımlama Sıklıđı

Sertifika sahiplerine ait iptal bilgisinin bulunduđu SİL'lerin geçerlilik süresi 36 (otuz altı) saattir. Ancak bu sürenin dolması beklenmeden her 4 (dört) saatte bir SİL tekrar yayımlanır. Gün içinde yeni bir Kurumsal Şifreleme Sertifikası iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliđini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduđu SİL dosyası, en geç 12 (on iki) ayda bir yenilenir. Kamu SM'ye ait bu sertifikalardan birinin iptali durumunda SİL dosyası derhal yenilenir.

#### 4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

Sertifika İptal Listesi, üretildiđi andan itibaren mümkün olan en kısa sürede yayımlanır.

#### 4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, Kurumsal Şifreleme Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduđu duyurulan imza oluŐturma verisiyle imzalanır.

ÇİSDUP desteđi olan uygulamalar Kurumsal Şifreleme Sertifikalarının geçerlilik durum kontrolünü ESHS EriŐim Bilgisi (Authority Information Access) isimli sertifika uzantısında yer alan adres üzerinden gerçekleştirir.

#### 4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Kamu SM, sertifika iptal bilgisinin sisteme daha az yük getirecek biçimde yayımlanmasını sağladıđı için, SİL yanında çevrim içi sertifika iptal durum kaydı desteđini de vermektedir.

SİL dosyası, iptal edilen her Kurumsal Şifreleme Sertifikası için iptal bilgisinin eklenmesiyle gittikçe büyüyen bir dosya niteliğindedir. Güncel iptal durum kaydına her ihtiyaç duyulduđunda dosyanın Kamu SM bilgi deposundan indirilmesi gerekir. Gittikçe büyüyen SİL dosyasının sisteme getireceđi yüke karşılık, ÇİSDUP ilgili Kurumsal Şifreleme Sertifikasının iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiđi ölçüde ÇİSDUP kullanmaları önerilir.

#### 4.9.11. Diđer Sertifika Durum Bildirim Yöntemleri

Kamu SM, SİL ve ÇİSDUP dışında iptal durum kaydı bildirim yöntemlerini uygulamamaktadır.

#### 4.9.12. İmza OluŐturma Verisinin Gvenliđini Yitirmesi Durumu

Sertifika sahibi kuruma ait imza oluŐturma verisinin gvenliđini yitirmesi durumunda Kurumsal Őifreleme Sertifikası iptal edilir. Kurumsal Őifreleme Sertifikasının iptal edilmesi dıŐında herhangi bir iŐlem uygulanmamaktadır.

#### 4.9.13. Sertifikanın Askıya Alındıđı Durumlar

Kurumsal Őifreleme Sertifikası, retim veya kullanım aŐamasında geđici iptal durumunu sađlamak amacıyla askıya alınabilir.

Kurumsal Őifreleme Sertifikaları biri yedek olmak zere 2 adet retilir. Sertifikalar askı durumunda retilir. Kullanılacak sertifika, kurumun sertifika sorumlusu/sorumluları tarafından Kamu SM Online İŐlemler zerinden askıdan indirilir. Aynı anda sertifikalardan sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

Kurum sertifika yenileme talebinde bulunduysa, yeni retilen sertifikalar askıda retilir ve geđerlilik sreleri baŐladıđında askıdan indirilerek kullanılabilir hale getirilir.

Sertifika sahibi kurum veya kurumun yetkilendirdiđi sertifika sorumlusu/sorumluları, aŐađıda belirtilenlere benzer sebeplerden dolayı Kurumsal Őifreleme Sertifikasını askıya alabilir:

- Sertifika sahibi kurumun Kurumsal Őifreleme Sertifikasını kullanım dıŐı bırakmak istemesi
- Kurumsal Őifreleme Sertifikasının iptalini gerektirebilecek bir durumun ortaya çıktıđından Őphelenildiđi durumlarda, yanlıŐlıkla iptalini engellemek amacıyla, Kurumsal Őifreleme Sertifikasının nce askıya alınmak istenmesi
- Aktif kullanılan geđerli sertifikanın kayıp/çalıntı/arıza durumunda iptal kadar geđer srede yedek sertifikanın kullanıma ađılabilmesi

#### 4.9.14. Sertifika Askıya Alma BaŐvurusunu Kimlerin Yapabildiđi

Kurumsal Őifreleme Sertifikasının askıya alma baŐvurusu, sadece sertifika sahibi kurum veya kurumun yetkilendirdiđi Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından yapılır.

#### 4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi

Kurumsal Őifreleme Sertifikası askı baŐvurusu, Kamu SM web sitesinde yer alan Online İŐlemler mensnden veya Online İŐlemlerin Kamu SM kaynaklı eriŐilemez olması durumunda sertifika sorumlusu/sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Telefonla yapılan grŐme kayıt altına alınır. Askı baŐvurusu alındıđında ncelikle baŐvuruyu yapan sertifika sahibi kurumun ve yetkililerinin kimlik belirlemesi ve dođrulaması yapılır. Kimlik dođrulaması yapılamayan askı baŐvuruları iŐleme alınmaz.

Askıya alınan Kurumsal Őifreleme Sertifikası iđin, SİL'de geđici olarak iptal edildiđini belirten sebep kodu kullanılır, İSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, Kurumsal Őifreleme Sertifikası askıya alındıktan sonra, gerekli grdđ durumlarda sertifika sahibi kurumu ve sertifika sorumlusu/sorumlularını sertifikanın askıya alındıđına dair bilgilendirir.

Kurumsal Őifreleme Sertifika Sorumlusu/Sorumluları, Kamu SM Online İŐlemler zerinden kuruma ait sertifikayı askıdan indirebilir. Askıya alınan sertifika en az bir defa SİL'e girmeden askıdan indirilemez.

Kuruma ait Kurumsal Őifreleme Sertifikalarından aynı anda sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

Kamu SM'ye ait Kk SHS ve Kurumsal Őifreleme SHS sertifikaları askıya alınmaz.

#### 4.9.16. Askıda Kalma Süresi

İlk üretim sonrasında askıdan indirmeye ilgili bir süre kısıtı bulunmamakla birlikte kurum tarafından askıya alınan sertifikalar en az bir defa SİL'e girmeden askıdan indirilemez.

#### 4.10. Sertifika Durum Servisleri

Üçüncü kişiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılığıyla ulaşır.

##### 4.10.1. İşletimsel Özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. Kamu SM'ye ait SİL dosyalarına erişim bilgileri Bölüm 7.1.2 Tablo 1'de verilmiştir. Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi Bölüm 7.1.2 Tablo 1'de verilmiştir. Üçüncü kişiler, Kurumsal Şifreleme Sertifikalarının geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

##### 4.10.2. Servisin Erişilebilirliği

SİL ve ÇİSDUP servislerinin verildiği sistemlere erişimin kesintisiz olarak sağlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurur. Üçüncü kişilerin iptal durum kaydını, erişimin kesilmesi sebebiyle kontrol etmeden yaptıkları işlemlerden doğan zararlardan Kamu SM sorumlu tutulamaz.

##### 4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

#### 4.11. Sertifika Sahipliğinin Sona Ermesi

Kurumsal Şifreleme Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM, Kurumsal Şifreleme Sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibi kurumu ve Kurumsal Şifreleme Sertifikası Sorumlusunu/Sorumlularını bilgilendirir. Kamu SM, Kurumsal Şifreleme Sertifikalarının süresi dolmadan en az 15 (on beş) gün önce sertifika sahibi kurumu bilgilendirir.

#### 4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

### 5. Yönetim, İşlemsel ve Fiziksel Kontroller

Bu bölümde Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan güvenlik kontrolleri anlatılmıştır.

#### 5.1. Fiziksel Güvenlik Denetimleri

Kamu SM, sertifika üretim ve yönetim süreçlerinde kullanılan sistemler için fiziksel ve çevresel güvenlik politikaları uygular.

Kamu SM sisteminin alıŐtıĐı cihazların bulunduĐu binalar ve odalar, giriŐ ve ıkıŐların kontrol edildiĐi yetkisiz kiŐilerin giriŐini engelleyen gvenlik nlemleri ile donatılmıŐtır. Gvenli alanlara eriŐimlerin kaydı tutulmaktadır.

#### 5.1.1. Tesis Yeri ve İnaŐatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yrtlmektedir. Kamu SM sisteminin alıŐtıĐı binanın bulunduĐu Gebze tesisi, yerleŐim merkezinden uzak, yangın, su baskını, deprem, yıldırim ve hava kirliliĐinden en az etkilenecek, giriŐ ve ıkıŐların kontrol edildiĐi bir blgedir. Alanlara ve binalara eriŐim, fiziki gvenlik, video izleme ve kimlik doĐrulama olmak zere oklu gvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrol bulunan bir alandır.

Bina, yksek gvenlik gerektiren iŐlerin yapılmasına imkn saĐlayan yapıdadır. Bina, esnek (elik yapı) ve sert (elik atıyla desteklenmiŐ beton yapı veya desteklenmiŐ beton yapı) yapı Őartlarını saĐlamaktadır.

Kamu SM'nin kurulduĐu yer ve binada g birimleri, haberleŐme niteleri, yedekli iklimlendirme niteleri, havalandırıcılar, yangın sndrc sistemler mevcut olup, deprem, su ve afetlere karŐı gerekli tedbirler alınmıŐtır. Yetkisiz personel ve kayıtsız ziyaretler bu hassas alanlara giremez.

#### 5.1.2. Fiziksel EriŐim

Kamu SM yazılım ve donanım modlleri ile arŐivlere eriŐim denetim altındadır. Binaya giriŐler gvenlik grevlilerinin kontrol altında, geliŐmiŐ eriŐim kontrol cihazlarıyla saĐlanmaktadır.

Bina iinde Kamu SM sistemine ait yazılım ve donanım aralarının bulunduĐu, elektronik veya kĐıt ortamdaki bilgilerin tutulduĐu, sistemin iŐletildiĐi ve ynetildiĐi odalara eriŐim geliŐmiŐ eriŐim kontrol cihazlarıyla yapılmaktadır. Gvenli alanlarda yetkisiz kiŐilerin alıŐması gereken durumlarda en az bir yetkili personel eŐlik eder. Yetkisi olmayan kiŐiler sistemin kurulu olduĐu odalara giriŐ yapamamaktadır. Yetkisiz kiŐilerin donanım bakımı veya bunun gibi sıra dıŐı bir amala sistemin kurulu olduĐu odalara giriŐleri zel eriŐim talimatları uyarınca dzenlenir.

#### 5.1.3. G KaynaĐı ve Havalandırma

AŐaĐıdaki g kaynakları Kamu SM iŐlevlerinin yerine getirilmesi ve srekliiliĐin saĐlanması iin kullanılmaktadır:

- G alma ve devŐirme (transformatr) birimleri
- DaĐıtım paneli
- Trafo
- UPS
- Kuru ak
- Acil jeneratr

Bina aŐırı ısınmayı nleyebilecek kapasitede ve uygun nem seviyesini ayarlayabilecek zelliklerde kesintisiz/yedekli iklimlendirme sistemleri ile donatılmıŐtır.

#### 5.1.4. Su Baskınları

Kamu SM iŐlevlerinin yerine getirildiĐi ortamlarda su baskınlarından en az zarar grecek Őekilde nlemler alınmıŐtır.

### 5.1.5. Yangın Önleme ve Korunma

Kamu SM işlevlerinin yerine getirildiđi ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıŐtır.

### 5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kâğıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur. Buna ek olarak gerekli görölen ortamların yerinde yedeđi alındıđı gibi gerekli güvenlik kriterlerini sađlayan ayrı bir lokasyonda da yedekler alınmaktadır.

### 5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduđu ve artık kullanılmayan elektronik veya kâğıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir. İmza oluŐturma verisi içeren kriptografik cihazlar endüstrideki en iyi uygulamalara göre imha edilir ve sıfırlanır. Diđer atıklar standart atık imha prosedürlerine uygun olarak imha edilir.

### 5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, farklı mekânda yedekleme işi için konum olarak tamamen ayrı, uzak bir felaket kurtarma merkezine sahiptir. Yedek sistemin bulunduđu mekân, asıl sistemin sađladığı tüm güvenlik ve işlevsellik şartlarını sađlar.

Kamu SM, sisteminin sürekliliđini sađlayabilmek amacıyla gerekli gördüđu bileŐenleri, farklı bir fiziksel mekânda güvenli kasalarda saklar.

## 5.2. Prosedürel Kontroller

### 5.2.1. Güvenilir Roller

Kamu SM'de çalıŐan personelin rolleri aŐađıda belirtildiđi şekilde sınıflandırılmıŐtır:

**Kamu SM Yönetimi:** Kamu SM'nin stratejik hedeflerinin gerçekleştirilmesi için gerekli tüm idari ve teknik faaliyetlerin yönetilmesinden sorumludur.

**Güvenlik Personeli:** Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

**Sistem Yöneticileri:** Sertifika hizmetlerinin yürütülmesi için gereken bilgi teknolojileri altyapısının yönetilmesinden sorumludur.

**Sistem Operatörleri:** Tüm sistem bileŐenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

**Sistem Denetçisi:** Sertifika hizmetleriyle ilgili arŐiv ve denetim kayıtlarının denetlenmesinden sorumludur.

**Sertifika Kayıt Sorumlusu:** Sertifika üretim/iptal başvurusunun alınması, başvuru evraklarının ve kurum kimliđinin dođrulanmasından sorumlu personeldir.

**Sertifika Üretim Sorumlusu:** Sertifika üretimini gerçekleŐtiren personeldir.

### 5.2.2. Her İşlem İçin Gereken KiŐi Sayısı

Kamu SM, Kök SHS ve Kurumsal Şifreleme SHS'ye ait sertifika üretilmesi, iptal edilmesi ve imza oluŐturma verilerinin başka bir kriptografik modöl içerisine yedeklenmesi için birden fazla yetkili personelin aynı anda hazır bulunmasını sađlar.

### 5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilir.

Kamu SM sistemi içinde kimlik doğrulama güvenli donanım araçları, parolalar, gizli sorular ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır.

Kullanıcı hesapları yetkilendirme ve yönetiminde, Kamu SM Erişim Yönetimi Politikası temel alınmaktadır.

### 5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Aşağıda verilen roller arasında görevler ayrılığı vardır:

- Sertifika Üretim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında
- Sistem Denetçisi ile diğer roller arasında
- Sistem Yöneticisi ile Güvenlik Personeli arasında

## 5.3. Personel Güvenlik Kontrolleri

### 5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir. Kamu SM'nin istihdam ettirdiği personel sistem güvenliği, veri tabanı yönetimi, elektronik imza teknolojileri ve uygulamaları, sertifika yönetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kişilerden oluşur.

### 5.3.2. Geçmiş Araştırması

Çalışanların Kamu SM'nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiği güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan araştırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araştırmalarda personelin herhangi bir sebepten dolayı hüküm giyip giymemiş olduğu araştırılır. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. İşe başlayan personelin bilgi güvenliği farkındalık eğitimleri tamamlanmadan, sistemlere erişimine izin verilmez.

### 5.3.3. Eğitim Gereklere

Çalışanlar, Kamu SM'deki işlerine aktif olarak başlamadan önce gerekli eğitimden geçirilirler. Çalışanlara verilen eğitimde Kamu SM'de uygulanan güvenlik ilkeleri, sistemin teknik ve idari işleyişi, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır.

### 5.3.4. Sürekli Eğitim Gereklere ve Sıklığı

Kamu SM sisteminde yapılan değişikliklerin bildirilmesi amacıyla personele verilen eğitimler gerekli görüldükçe tekrarlanır. Yeni göreve başlayanlar için eğitimler tekrarlanır.

Kamu SM, çalışanlarına yılda en az bir defa, siber güvenlik ve sosyal mühendislik saldırılarına karşı farkındalık oluşturmak amacıyla, bilgi güvenliği eğitimi vermektedir.

### 5.3.5. Görev Deęişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

### 5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince bilgi güvenliği politikaları ihlali ve ihlalin boyutuna göre hukuki soruşturma ve disiplin süreci başlatılır.

### 5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM verdiği hizmetler için dış kaynak kullanmak durumunda kaldığında, bu hizmeti sağlayacak firma personeli ile ilgili güvenlik kontrollerini, firma ile yaptığı sözleşme ile belirler.

### 5.3.8. Sağlanan Dokümantasyon

Çalışanlara işleriyle ve Kamu SM süreçleriyle ilgili gerekli kılavuz ve destek dokümanlar ve bilgi güvenliği politikaları kapsamındaki ilgili dokümanlar sağlanır.

## 5.4. Denetim Kayıtları

Kamu SM işleyişi sırasında gerçekleştirilen anahtar ve sertifika yönetimi, sistemin güvenliği ile ilgili işlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diğer bir kısmı ise kâğıt üzerindedir. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

### 5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde aşağıda yapılan işlemler ile ilgili elektronik veya kâğıt ortamda yapılan işlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
  - Anahtar üretimi
  - Anahtar yedekleme
  - Anahtar dağıtımı
  - Anahtar saklama
  - Anahtar arşivleme
  - Anahtar yok etme
  - Kriptografik modül yaşam döngüsü işlemleri
- Sertifika üretim, yenileme, askıya alma ve iptal başvuruları
  - Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
  - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
  - Başvuru sırasında elektronik veya kâğıt ortamda alınan form veya belgeler
  - Kâğıt belgelerin kopyalarının nerede saklandığı bilgisi
  - Geçerli ve geçersiz alınan tüm başvuru bilgileri
- Sertifika yaşam döngüsü yönetimi işlemleri
  - Sertifika başvurusunun işlenmesi
  - Sertifika üretimi

- Sertifika yenileme
- Sertifika iptal etme
- SİL yayımlanması
- Güvenlikle ilgili diđer iŐlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi iŐlemleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve deđiŐtirilmesi
  - Güvenlik profili deđiŐiklikleri
  - Sistemin çökmesi, donanım hataları ve diđer bozukluklar
  - Güvenlik cihaz/yazılım iŐlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

Kayıtlarda genellikle kayıt zamanı ve kaydı oluŐturan personelin ismi bulunur.

#### 5.4.2. Kayıtların İncelenme Sıklığı

Sistemin iŐleyiŐiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluŐup oluŐmadığı kontrol edilir. Buna ek olarak, sistemde olađandışı hareketlerin görölmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görölün ve başlatılan iŐlemler de belgelenir.

Sertifika başvurusu sırasında sertifika sahiplerinden gelen bilgilerin elektronik veya kâğıt ortamda tutulan kayıtları, sertifika yaşam döngüsü süresi içinde gerek göröldükçe veya yasal iŐlemler sebebiyle incelenebilir.

#### 5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelenmelerinden sonra, en az 2 (iki) ay sistemde tutulur. Ardından arŐivlenir. Talep edilmesi halinde kayıtlar yetkili denetçilere sunulur.

#### 5.4.4. Kayıtların Korunması

Kamu SM'ye ait kayıtların elektronik ve fiziksel olarak güvenlik altında tutulması için aŐađıdaki önlemler alınmıŐtır:

- Yetkisi olmayan kişiler, elektronik kayıtların bulunduđu sistemlere erişemezler.
- Kâğıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunur.
- Kayıtların deđiŐtirilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınmıŐtır.
- Elektronik olarak saklanan ve sistemin iŐleyiŐi açısından kritik olan kayıtlar, iŐlemi yapan personel tarafından gerektiğinde elektronik imza ile imzalanarak saklanır. Böylece kritik kayıtlarda oluŐabilecek her deđiŐiklik sistem tarafından fark edilir.
- Kritik bilgiler gerektiğinde Kamu SM'ye ait anahtarlarla Őifreli olarak saklanır.

#### 5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliđi göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görölün kayıtların çevrim içi yedeđi alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme iŐlemlerini otomatikleŐtirmek için yedekleme yönetim yazılımı mevcuttur. Kritik kayıtlar ayrı bir Őehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

#### 5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ađ katmanında ve iŐletim seviyesi dűzeyinde otomatik olarak toplanır. Otomatik kayıt toplama iŐlemi sistemin baŐlatılmasından kapanmasına kadar alıŐır.

#### 5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluŐmasına sebep olan iŐlemi baŐlatan Kamu SM sertifika yűnetim sistemi kullanıcısı, kaydın yapıldığına dair sistem tarafından bilgilendirilir.

#### 5.4.8. Saldırıya Aıklığın Deđerlendirilmesi

Denetim kayıtlarının tutulduđu sistemler iin Bűlűm 6.5, 6.6 ve 6.7’de sűzű geen teknik gűvenlik kontrolleri uygulanır.

Zafiyetlerin deđerlendirilmesiyle ilgili detaylar Kamu SM Teknik Aıklık Yűnetim Politikasında belirtilmektedir. Kamu SM bu politikaya uygun Őekilde periyodik olarak zafiyet taraması ve sızma testi yapar.

### 5.5. Kayıt ArŐivleme

#### 5.5.1. ArŐivlenen Kayıt Bilgileri

Bűlűm 5.4.1’de belirtilen kayıtlara ek olarak sertifika baŐvurusu ve sertifika yaŐam dűngűsűyle ilgili, elektronik olarak ya da kâđıt üzerinde tutulan aŐađıdaki belgeler arŐivlenir:

- Sertifika sahibi kurum tarafından, baŐvuru sırasında verilen tűm bilgi ve belgeler
- Sertifika űretimi, yenileme, askıya alma, askıdaki sertifikayı kullanıma ama ve iptal baŐvuruları sırasında elektronik veya kâđıt ortamda alınan formlar
- űretilen tűm sertifikalar
- Geerlilik sűresi dolan tűm Kamu SM kűk ve alt kűk sertifikaları
- Yayınlanan tűm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokűmanı
- Sertifika Uygulama Esasları dokűmanı
- Zaman Damgası Sİ/SUE dokűmanları
- Sertifika yűnetim prosedűrleri
- BaŐvuru Formu ve Taahhűnameler
- Sertifikasyon sűrelerinde kullanılan sistemlerin NTP senkronizasyon logları

#### 5.5.2. ArŐivlerin Tutulma Sűresi

ArŐivlenen bilgiler ve belgeler en az 20 (yirmi) yıl boyunca saklanır.

#### 5.5.3. ArŐivlerin Korunması

ArŐivlenen bilgi ve belgeler izinsiz izlenmeyi, deđer değiŐtirmeyi ve silinmeyi engelleyecek Őekilde elektronik ve fiziksel olarak gűvenli tutulur. ArŐivler yetkisiz alıŐanların eriŐimine kapalıdır. ArŐivlerin tutulduđu ortam Bűlűm 5.5.2’de belirtilen sűre boyunca arŐivlerin zarar gűrmesini engelleyecek Őekilde seilir.

#### 5.5.4. ArŐivlerin Yedeklenmesi

Kritik bilgi ieren elektronik arŐivler Kamu SM iŐ sűrekliliđi politikası geređince yedeklenir.

### 5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

### 5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kâğıt ortamda ilgili Kamu SM prosedürlerine göre toplanır.

### 5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Aynı bilgiye ait birden fazla arşiv olması durumunda arşivler kıyaslanarak doğruluğu kontrol edilir.

## 5.6. Anahtar Değişimi

Kamu SM'ye ait anahtarlar ve sertifikalar geçerlilik süresinin dolması veya güvenlik gerekleriyle yenilenebilir. Kamu SM'ye ait sertifikanın kullanım süresinin dolmasından önce eski anahtar çiftinden yeni anahtar çiftine geçiş işlemleri yapılır. Anahtar değişimi işlemleri şunları gerektirir:

- Kök sertifikası kullanım süresinin dolmasından en geç 3 (üç) yıl önce; alt kök sertifikası kullanım süresinin dolmasından en geç 1 (bir) yıl önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisi ile imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisi ile imzalanmaya devam eder. Yeni üretilen sertifikalar için oluşturulan yeni SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.
- Kamu SM, yenilediği anahtarları Kamu SM resmî web sitesi üzerinden üçüncü taraflarla paylaşır.

## 5.7. Güvenliğin Yitilmesi ve Arıza Durumlarında Yapılacaklar

### 5.7.1. Güvenilirliğin Yitilmesi Durumunun Düzeltilmesi

Güvenilirliğin yitilmesi durumlarında, sertifika yönetim sisteminin en kısa zamanda yeniden güvenli olarak çalışmaya başlaması, durumdan etkilenen tarafların haberdar edilmesi, zararlarının en aza indirgenmesi için belirlenen süreçler işletilir.

Kamu SM bünyesinde olası bir kriz, felaket veya güvenlik ihlali durumlarının gerçekleşmesi halinde operasyonları kesintiye uğratabilecek olaylara müdahale ve yönetim çerçevesi çizmek amacıyla İş Sürekliliği Planları hazırlanmıştır. İş Sürekliliği Planlarının test edilmesi, gözden geçirilmesi ve güncellenmesi yılda en az bir defa gerçekleştirilir.

### 5.7.2. Donanım, Yazılım veya Veri Bozulması

Donanım, yazılım veya veri bozulması durumları raporlanır ve arızanın/hatanın giderilmesi için gerekli süreç başlatılır.

İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır ve kritik süreçler için felaket kurtarma merkezi oluşturulmuştur. Depolama ünitesi fiziksel olarak farkı bir noktada bulunan veri depolama ünitesi ile veri senkronizasyonu yapabilecek niteliktedir. Arızanın giderilmesi süreci arıza sebebinin araştırılmasını, hatanın giderilmesini ve gerekli görüldüğünde Kamu SM hizmetlerini güvenilir yedek ortama aktarmayı içerir.

### 5.7.3. İmza OluŐturma Verisinin Gizliliđini Kaybetmesi Durumunda İzlenecek Prosedürler

Kamu SM'nin Kurumsal Őifreleme Sertifikalarını imzalamada kullandığı imza oluŐturma verisinin gizliliđinin kaybedildiđinden Őüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aŐađıdaki iŐlemler yerine getirilir:

- Kamu SM kendisine ait sertifikanın iptal edildiđini, iptal sebebi ile birlikte en hızlı Őekilde Kamu SM resmî web sitesi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, Kurumsal Őifreleme Sertifikası sahiplerinin durumdan ne Őekilde etkileneceđini belirten aŐıklamayı yapar, eski imza oluŐturma verisiyle oluŐturulan Kurumsal Őifreleme Sertifikalarına gúvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiđi bilgisini yayımladıđı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikaları iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Kurumsal Őifreleme Sertifikası isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM imza oluŐturma verisinin yok edilmesi sürecini iŐletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtar çiftinin yenilenmesiyle, iptal edilen Kurumsal Őifreleme Sertifikalarının sertifika sahibinden gelen talep dođrultusunda sertifika yenileme süreci baŐlatılır.

### 5.7.4. Arıza Sonrası Yeniden ÇalıŐırlık

Kamu SM, arıza ya da afet sonrası sistemin en kısa zamanda yeniden ve güvenli olarak çalıŐmaya baŐlaması için gerekli yöntemleri ve süreçleri Kamu SM iŐ sürekliliđi planlarında tanımlar.

Kamu SM baŐka bir Őehirde felaket kurtarma merkezine sahiptir. Kamu SM Yedekleme Yönetim Politikasına uygun olarak önemli veri ve uygulamaların yedeklerini almakta ve gerekli durumlarda yedekten geri dönme iŐlemlerini uygulamaktadır. İŐ sürekliliđinin devamı için Kamu SM merkez ofiste saklanan verilerin yedekleri felaket kurtarma merkezinde de saklanmaktadır.

Kamu SM, arıza sonrası yeniden çalıŐırlığı sađlayacak Kamu SM İŐ Sürekliliđi Planlarını periyodik olarak gözden geçirir ve test eder. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

### 5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, Elektronik İmza Kanunu'nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen Őekilde faaliyetlerine son verebilir. Bu durumda gerçekteŐirilecek iŐlemler [Kamu SM Hizmetleri Sonlandırma Planı](#) dokümanında tanımlanmıŐtır.

## 6. Teknik Güvenlik Kontrolleri

Kamu SM'nin kendisi ve sertifika sahipleri adına, anahtar çiftleri ve eriŐim verilerini ürettiđi, sertifika yönetim iŐlemlerini gerçekteŐirdiđi sistemler CWA 14167-1, ETSI TS 101 456 ve TS ISO/IEC 27001 veya ISO/IEC 27001 gereklerini sađlar.

## 6.1. Anahtar Çifti Üretimi ve Kurulumu

### 6.1.1. Anahtar Çifti Üretimi

#### 6.1.1.1. Kök SHS, Kurumsal Őifreleme SHS, ÇİSDUP Yanıtlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aŐağıdaki anahtar çiftleri oluşturulur:

- Kök SHS'ye ait imza oluŐturma ve imza doęrulama verisi
- Kurumsal Őifreleme SHS'ye ait imza oluŐturma ve imza doęrulama verisi
- ÇİSDUP Yanıtlayıcı'ya ait imza oluŐturma ve imza doęrulama verisi

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceęi güvenli odada, birden fazla eęitimli personelin gözetiminde, aę ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiŐ, FIPS PUB 140-2 seviye 3 veya EAL4+ standartlarını saęlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen imza oluŐturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dıŐarıya çıkarılmaz. Yapılan bütün iŐlemler kayıt altına alınır ve iŐlemi gerçekteŐiren personel tarafından onaylanır.

İmza oluŐturma verisinin saklandığı kriptografik modül Bölüm 6.2.1'de belirtilen standartlara uyar.

#### 6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Kurumsal Őifreleme Sertifikası akıllı karta yüklenecekse, sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremedięi odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

Kurumsal Őifreleme Sertifikası HSM'ye yüklenecekse, HSM Cihaz Sorumlusu gözetiminde Kamu SM yetkili personeli tarafından, HSM Yükleme Bilgi Formu dokümanında belirtilen Őekilde güvenli yazılım kullanılarak üretilir.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiŐ, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirlięi dünyaca kabul görmüŐ algoritmalar kullanılır. Sertifika sahibine ait imza oluŐturma verisinin yedeęi alınmaz, bir kopyası hiçbir Őekilde sistemde tutulmaz. Sertifika sahibine ait imza oluŐturma verisinin saklandığı akıllı kart veya HSM Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

#### 6.1.2. Sertifika Sahibine İmza OluŐturma Verisinin UlaŐtırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluŐturulmasına müteakip, imza oluŐturma verisi, sertifikayla birlikte akıllı kart içerisinde veya HSM'ye yüklenerek teslim edilir. Akıllı kart, imza karŐılıęı ve resmî kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye imza oluŐturma verisi ve sertifika yükleme iŐlemi, HSM Cihaz Sorumlusu gözetiminde gerçekteŐirilir ve iŐlem sonrası Kurulum Tutanaęı doldurularak imzalanır.

Akıllı karta eriŐim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli baęlantı protokolleri (HTTPS) kullanılmaktadır. Sertifika sorumlusunun/sorumlularının kimlik kontrolü için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu Őekilde gerçekteŐirilen kimlik doęrulaması sonrasında sertifika sahibi akıllı kart eriŐim verisine eriŐir. HSM'ye eriŐim verisinden Kamu SM sorumlu deęildir, eriŐim verisi kurum sahiplięindedir.

### 6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaőtırılması

Kurumsal Őifreleme Sertifikası HSM'ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteęi, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılıęıyla Kamu SM'ye parola korumalı ZIP dosyası ierisinde ulaőtırılır.

Kurumsal Őifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Őifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildięi için imza doğrulama verisinin Kamu SM'ye ulaőtırılması söz konusu deęildir.

### 6.1.4. ESHS Sertifikalarına Eriřim Saęlanması

Kamu SM'ye ait Kök SHS ve Kurumsal Őifreleme SHS sertifikaları internet ortamında tarafların eriřimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz deęiřtirmeye ve silinmeye karřı güvenlięi saęlanır.

Kök SHS ve Kurumsal Őifreleme SHS sertifikaları, sertifikaların özet deęeri ve özet algoritması <https://kamusm.bilgem.tubitak.gov.tr> web adresi üzerinden yayımlanır.

### 6.1.5. Anahtar Uzunlukları

Kamu SM Kök SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

Kurumlara ait Kurumsal Őifreleme Sertifikalarını imzalayan Kurumsal Őifreleme SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarını imzalamak için kullanılan RSA anahtar boyu en az 2048-bittir.

Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikaları, RSA anahtar boyu en az 2048-bittir.

### 6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde Teblię'de belirtilen kriterlere uygun algoritmalar kullanılmaktadır. Algoritmaların gerekleřtiriminde kullanılan yöntemler gerekli güvenlik kriterlerini saęlar.

### 6.1.7. Anahtar Kullanım Amaları

Kamu SM tarafından oluşturulan anahtarların hangi amalar için kullanılabilereceęi sertifikadaki "Anahtar Kullanımı" ve "Geniřletilmiş Anahtar Kullanımı" uzantısı ierisinde belirtilir.

Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Kurumsal Őifreleme Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. ÇİSDUP yanıtlarının imzalanmasında alt kök ve kök tarafından yetkilendirilmiş ÇİSDUP sertifikası kullanılır.

## 6.2. İmza Oluřturma Verisinin Korunması

### 6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluřturma verileri güvenli yazılım ve/veya donanım kullanılarak üretilir, güvenli kriptografik modül iinde saklanır ve geerli olduęu süre boyunca bu modül dıřına ıkmaz.

Kriptografik modül ařaęıda belirlenen güvenlik iřlevlerine sahiptir:

- İmza oluřturma verisinin geerlilik süresi boyunca gizlilik ve bütünlüęünü saęlar.
- Modüle eriřimde kimlik belirleme ve doğrulama iřlevlerini yerine getirir.

- EriŐim yetkisi birden fazla kiŐinin kontrolünde olacak Őekilde tanımlanabilir.
- Sistem kullanıcılarına tanımlanan roller dođrultusunda, verdiđi hizmetlere eriŐimi sınırlar.
- Düzgün çalıŐtıđı test edilebilir, test sırasında hata oluŐtuđunda güvenli duruma geçer.
- Modüle izinsiz eriŐim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıŐtır.
- Yetkisiz eriŐime teŐebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeđinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluŐturma verisinin içinde bulunduđu akıllı kart veya HSM cihazı, imza oluŐturma verisinin donanım dıŐına çıkmasını engelleyen ve donanıma eriŐimi parola ile sađlayan teknik özelliklere sahiptir. Sertifika sahibine ait HSM cihazının yurt içinde ve fiziksel olarak konumlandırılmıŐ olması gerekmektedir.
- Kriptografik modül ve sertifika sahibine ait akıllı kart veya HSM cihazı, Tebliđ'de belirtilen güvenlik standartlarını sađlar.

### 6.2.2. İmza OluŐturma Verisine Birden Fazla KiŐi Kontrolünde EriŐim

Kamu SM'ye ait imza oluŐturma verisinin bulunduđu odaya eriŐim aynı anda 2 (iki) yetkili personel tarafından sađlanmaktadır. Yetkili kiŐiler dıŐında eriŐim gerekli kontroller vasıtasıyla engellenir.

### 6.2.3. İmza OluŐturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıŐtır.

### 6.2.4. İmza OluŐturma Verisinin Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi için sađlanan güvenlik ile eŐdeđer güvenlik önlemleri altında yapılır. Yedeklenen imza oluŐturma verisi yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan imza oluŐturma verisinin bulunduđu ortam ile aynı güvenlik Őartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait imza oluŐturma verileri Kamu SM tarafından yedeklenmez.

### 6.2.5. İmza OluŐturma Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluŐturma verileri arŐivlenmez. Kullanım süreleri sonunda geri dönüŐsüz Őekilde silinir.

### 6.2.6. İmza OluŐturma Verisinin Kriptografik Modüle Yüklenmesi

Kamu SM'ye ait imza oluŐturma verisi üretildikten hemen sonra kriptografik modüle yüklenir. İŐlem, güvenilir yöntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Sertifika sahiplerine ait imza oluŐturma verileri, sadece yetkili personelin kontrolünde akıllı kart veya HSM cihazına Őifrelenerek yüklenir. İmza oluŐturma verilerinin varsa kopyaları yüklemelerinin tamamlanmasının ardından sistemden silinir.

### 6.2.7. İmza OluŐturma Verisinin Kriptografik Modülde Saklanması

Kamu SM'ye ait imza oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına çıkması engellenmiŐtir. İmza oluŐturma verileri kriptografik modül içinde güvenli algoritma ve yöntemlerle Őifreli olarak saklanır.

Sertifika sahibinin imza oluŐturma verisi, kendisine ait akıllı kart veya HSM cihazı iinde saklanır, baŐka bir ortamda bulunmaz. Kamu SM, sertifika sahiplerine ait imza oluŐturma verileri kendi sistemi iinde saklamaz.

#### 6.2.8. İmza OluŐturma Verisine EriŐim

Kamu SM'nin imza oluŐturma verisine eriŐim birden fazla yetkili personelin ortak denetimi altındadır. İmza oluŐturma verisinin bulunduĐu odaya giriŐ iin, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doĐrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadıĐı ve kimliklerinin doĐrulanamadıĐı durumlarda imza oluŐturma verisinin bulunduĐu odaya eriŐim saĐlanamaz.

İmza oluŐturma verisi kriptografik modül iinde Őifreli durumdayken eriŐime kapalıdır. EriŐime aılması iin eriŐimi saĐlayan verinin modüle sunulması gerekir. İmza oluŐturma verisinin eriŐime aılması ve kullanılır duruma getirilmesi birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahibine ait imza oluŐturma verisi, akıllı kart veya HSM cihazı iinde sertifika sahibinin eriŐim verisi ile korunmuŐ olarak saklanır. Aktivasyon, eriŐim verisi ile saĐlanır.

#### 6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

Kamu SM'nin imza oluŐturma verileri imzalama iin kullanıldıktan sonra oturum kapandıĐında veriye eriŐim otomatik olarak kesilir ve bir dahaki kullanımına kadar Őifrelenerek eriŐime kapalı tutulur. EriŐimin yeniden saĐlanabilmesi iin Blüm 6.2.8'de belirtilen yntemin yeniden iŐletilmesi gerekir.

Sertifika sahibinin kullandıĐı güvenli donanım araları, imza oluŐturma verisini kullanan oturumun kapanmasından sonra veriye eriŐimi kesecek biimde alıŐır. EriŐimin yeniden saĐlanabilmesi iin sertifika sahibinin eriŐim verisini yeniden girmesi gerekir. EriŐim verisinin art arda 3 () defa yanlıŐ girilmesi durumunda güvenli donanım aracı kilitletir ve araca eriŐim saĐlanamaz.

#### 6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

Kamu SM'ye ait imza oluŐturma verileri kullanım sresinin dolmasının ardından, aslı ve btn yedekleri buldukları ortamlardan uygun yntemlerle geri dnŐsz Őekilde silinir. Kamu SM'ye ait imza oluŐturma verisinin silinmesi iŐlemi iin Blüm 6.2.8'de belirtilen Őekilde yeterli sayıda yetkili personelin hazır bulunması gerekir.

Sertifika sahiplerine ait imza oluŐturma verileri, kullanım sresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından akıllı kart veya HSM cihazı zerinden silinmelidir. Bu iŐlemin yapılmasından sertifika sahibi sorumludur.

#### 6.2.11. Kriptografik Modln DeĐerlendirilmesi

Kamu SM, Blüm 6.2.1'de belirtilen standartlara uygun kriptografik modl kullanır.

### 6.3. Anahtar ifti Ynetimiyle İlgili DiĐer Konular

#### 6.3.1. İmza DoĐrulama Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doĐrulama verisi, sertifikalar iinde tutulur ve Kurumsal Őifreleme Sertifikaları kullanım srelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arŐivlenir. Kurumsal Őifreleme Sertifikalarının arŐivleri yetkisiz kiŐilerce tahrifatına ve silinmesine karŐı gerekli nlemlerin alındıĐı ortamlarda tutulur.

### 6.3.2. İmza OluŐturma ve Dođrulama Verilerinin Kullanım Süreleri

İmza oluŐturma verisinin kullanım süresi, Kurumsal Őifreleme Sertifikasının ieriđinde belirtilen kullanım süresi kadardır. Kurumsal Őifreleme Sertifikasının kullanım süresinin dolmasıyla ya da Kurumsal Őifreleme Sertifikasının iptal edilmesiyle imza oluŐturma verisinin kullanımı sona erer.

Kamu SM'ye ve sertifika sahibine ait anahtar iftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan algoritmaya göre belirlenir. Kamu SM'ye ait 384 bitlik ECDSA anahtar iftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar iftleri en fazla 1 (bir) yıl için kullanılır. Üretilen Kurumsal Őifreleme Sertifikalarının son kullanma tarihi, Kurumsal Őifreleme SHS Sertifikasının son kullanma tarihini aşamaz.

### 6.4. Aktivasyon Verileri

Kamu SM alıŐanlarının aktivasyon verileri; eriŐim parolalarını, güvenli donanım araçları içindeki eriŐim denetimi sađlayan diđer verileri, biyometrik verileri ierir.

Sertifika sahibi kuruma ait iki farklı aktivasyon verisi tanımlanmıŐtır. Bunlar, akıllı karta eriŐim verisi ile sertifika iŐlemlerinin yapıldıđı internet Őubesine eriŐim verileridir.

#### 6.4.1. Aktivasyon Verilerinin OluŐturulması

Kamu SM sistemi içinde kullanılan aktivasyon verileri ile sertifika sahibi kuruma ait eriŐim parolaları yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rastgele üretilir.

#### 6.4.2. Aktivasyon Verilerinin Korunması

Kamu SM sistemi içinde kullanılan aktivasyon verileri yalnızca yetkili personeller tarafından bilinir.

Sertifika sahibi kuruma ait eriŐim parolaları, iki kademeli kimlik dođrulama ile eriŐilen web sayfası üzerinden sahibi tarafından belirlenir.

EriŐim parolaları ilk kullanımda sertifika sahibi tarafından deđiŐtirilir. Parolayı yetkisiz kiŐilerin eriŐimine karŐı korumak sertifika sahibinin yükümlölüđü altındadır.

#### 6.4.3. Aktivasyon Verileri ile İlgili Diđer Konular

Düzenlenmesine gerek duyulmamıŐtır.

### 6.5. Bilgisayar Güvenliđi Kontrolleri

#### 6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereker

Kamu SM sistemi içinde kötü niyetli yazılımlara karŐı gereken önlemler alınır. Sistemde ađ ve sunucu bazlı sensörler ieren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuŐtur, bunlar sürekli güncel tutulmaktadır. Kritik iŐlemlerin yapıldıđı bilgisayarlar ađ ortamı dışında tutulur. Bilgilerin tahrifata, silinmeye ve kaađa karŐı korunması ve iŐletimin sürekliliđinin sađlanması için gerekli güvenlik sađlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliđi konusunda bütün iyileŐtirme eylemleri gecikmesiz uygulanır. Güvenlik yamaları deđerlendirilip daha büyük bir riske sebebiyet vermesi durumunda yüklenmez ve risk süreç takip sistemi üzerinde kayıt altına alınır. Ađ bileŐenleri ve konfigürasyonları dönemsel olarak Ađ Güvenliđi Prosedürüne göre kontrol edilir.

### 6.5.2. Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

## 6.6. Yaşam Döngüsü Teknik Kontrolleri

### 6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler aŐağıda verilmiştir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileşenlerin yedekleri oluşturulur.
- Sistemin açık aęa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmî olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileştirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan işler ISO/IEC 27001 gereklerini sağlar.
- Geliştirme faaliyetleri sırasında geliştirme, test ve canlı sistemler ayrılır. Canlıya alınma işlemi onay mekanizmalarından sonra gerçekleştirilir.
- Sistem bileşenlerine dair periyodik risk değerlendirmeleri yapılır ve yönetime sunulur.
- Sistemlerde gerçekleştirilen değişiklikler kayıt altına alınır ve izlenir.
- Uzaktan erişim dahil üçüncü tarafların sistemlere erişimine izin verilmez.

### 6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile aę ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için periyodik olarak güvenlik yönetimi denetimi yapılır. Kamu SM içinde güvenliğe uygun olmayan hareketler ve yetkilendirmeler denetleme sonucunda açıklanır ve düzeltici önlemler alınır. Güvenlik kontrolleri için temel dayanak ISO 27001'in güncel sürümüdür.

### 6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

Düzenlenmesine gerek duyulmamıştır.

## 6.7. Aę Güvenliği Kontrolleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli aę güvenliği kontrolleri yapılır. Sertifikasyon işlemlerinde aęlar arası gereksinim duyulmayan protokoller güvenlik duvarları ile engellenmiştir. Sistem, dışa açık aęa bağlantısında saldırı engelleme özellikli yeni nesil güvenlik duvarları kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceęe yönelik performans eğilimlerini saptamak amacı ile aę ve sistem yönetimi altyapıları mevcuttur.

Sunucular üzerine ađ ve sistem yönetimi ve güvenliđi ajanları kurulmuŐtur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı, dosya bütünlüđü, güvenlik kayıtları, harici depolama üniteleri takibi vb. bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalıŐması için önem arz eden kaynaklar için eşik deđerler belirlenir ve bu eşik deđerlerin aŐılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ađ ve sistem yönetimi ve güvenliđi altyapısı çektiđi bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmiŐe dönük rapor üretilmesine imkân tanınır. Farklı güvenilir sistemlerle iletişim ihtiyacı olması durumunda, diđer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldıđı sistemler (kök ve alt kök sunucuları gibi) için farklı ađ segmentleri oluşturulmuŐtur. Kritik işlemlerin yapıldıđı sistemler ađa bađlı deđildir. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıŐtır. Güvenli ve yüksek güvenli bölgelere erişimler erişim kontrol protokolüne göre belirlenir. Yüksek güvenlik gerektiren sistemlerde kullanılan donanımlar farklı yerlerde tekrar tekrar kullanılmaz, imha edilirler.

Bilgi işlem yöneticileri, uygulama geliŐtiricileri gibi farklı çalıŐan gruplarına ait farklı amaca hizmet eden ađlar da birbirinden ayrılmıŐtır. Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler, güvenlik ekibince kontrollü olarak verilir ve kayıtlar üzerinden izlenir. Farklı bölgelere olan iletişim ve erişim engellendiđi gibi gerekli olmayan bađlantı ve hizmetler de ađ güvenliđi açısından devre dıŐı bırakılır.

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller Kamu SM SıkılaŐtırma Prosedürüne göre kaldırılır ya da devre dıŐı bırakılır. Ađ ve sistem güvenliđine dair tüm işlemler siber olaylara müdahale ekibi tarafından izlenir ve gerektiđinde olay müdahale süreçleri dođrultusunda aksiyon alınır. Kamu SM çevrim içi açık anahtar altyapısı hizmetlerinin devamlılıđı için Kamu SM ana merkez ve felaket kurtarma merkezinin dıŐ ađ bađlantı hizmetlerini yedekli olarak kurgulamıŐtır.

Sistemler üzerinde periyodik olarak zafiyet taramaları ve yılda en az bir kez penetrasyon testi yapılır. Penetrasyon testini yapan kiŐi veya kurum; test metot ve araçlarını, testleri yapan kiŐilerin yetkinliklerini içeren raporlar hazırlar. Bu raporlar Kamu SM tarafından saklanır. Sistemlerin belirlenen kural setlerine uygunluđu düzenli olarak gözden geçirilir.

## 6.8. Zaman Damgası

Kamu SM sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'de belirtilen Őartlara uyararak gerekli kesinlik ve bütünlük Őartlarını sađlar.

Zaman damgasıyla ilgili ayrıntılı bilgi Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esaslarında bulunur.

## 7. Sertifika ve Sertifika İptal Listesi Biçimleri

### 7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından verilen Kurumsal Őifreleme Sertifikalarının içeriđi ile ilgili bilgilendirme yapılmaktadır.

#### 7.1.1. Sürüm Numarası

Kamu SM "ITU-T X.509 V.3" sertifika standardını destekler.

### 7.1.2. Sertifika Uzantıları

Kamu SM tarafından verilen Kurumsal Őifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geerlilik tarihi, ilgili imza dođrulama verisi, sertifika sahibi kurumun adı ve DETSIS numarası, sertifikayı yayımlayan Kamu SM'ye ait isim bilgileri ve Kamu SM'nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını ierir. Kurumsal Őifreleme Sertifikasının ieriđinde bulunan sertifika uzantıları sertifikanın kullanılacađı uygulamanın gereklerine bađlı olarak belirlenir.

Tablo 1'de Kamu SM tarafından retilen Kurumsal Őifreleme Sertifikalarında asgari dzeyde bulunması gereken uzantılar tanımlanmıŐtır.

**Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları**

Sertifika Uzantısı	Kritik Uzantı	Aıklama
Temel Kısıtlar <sup>1</sup>	HAYIR	Sertifikanın son kullanıcı sertifikası olduđu, ESHS sertifikası amacıyla kullanılmayacađı belirtilir.
Yetkili Anahtar Tanımlayıcısı <sup>2</sup>	HAYIR	Kamu SM'ye ait Kurumsal Őifreleme SHS imza dođrulama verisinin SHA-1 zet ıktısından oluŐur.
Sertifika Anahtar Tanımlayıcısı <sup>3</sup>	HAYIR	Sertifikanın ieriđindeki "subjectPublicKey" alanının "BIT STRING" olarak deđerinin SHA-1 zet ıktısından oluŐur.
Anahtar Kullanımı <sup>4</sup>	EVET	Anahtarların sadece Őifreleme amalı kullanıldıđının ifade edilmesi iin "keyEncipherment" [anahtar Őifreleme] alanı seilmiŐtir.
SİL Dađıtım Noktaları <sup>5</sup>	HAYIR	<a href="http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl">http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl</a>
Yetkili Bilgi EriŐimi <sup>6</sup>	HAYIR	<a href="http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt">http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt</a> <a href="http://ksifrelemeocspv1.kamusm.gov.tr/">http://ksifrelemeocspv1.kamusm.gov.tr/</a>
Sertifika ilkeleri <sup>7</sup>	HAYIR	Kamu SM Sİ dokmanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.11) ile SUE dokmanının bulunduđu <a href="http://depo.kamusm.gov.tr/ilke">http://depo.kamusm.gov.tr/ilke</a> internet adresini ve BTK tarafından oluŐturulan Kurumsal Őifreleme Sertifikası ibaresine ait metni ierir.

<sup>1</sup> BasicConstraints

<sup>2</sup> AuthorityKeyIdentifier

<sup>3</sup> SubjectKeyIdentifier

<sup>4</sup> KeyUsage

<sup>5</sup> CRLDistributionPoints

<sup>6</sup> AuthorityInformationAccess

<sup>7</sup> CertificatePolicies

Geniřletilmiř Anahtar Kullanımı <sup>8</sup>	HAYIR	Kurumsal Őifreleme Sertifikası nesne tanımlama numarasını (2.16.792.1.2.1.1.5.7.51.1) ierir.
----------------------------------------------	-------	-----------------------------------------------------------------------------------------------

Uzantılardan bazıları kritik olarak tanımlanmıřtır. Kritik olarak belirtilen uzantıların sertifikayı kullanan uygulama tarafından tanımlanamaması durumunda sertifika kullanılamaz.

### 7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiđi Kurumsal Őifreleme Sertifikalarını imzalamak iin SHA-384 zet algoritması ile ECDSA imza dođrulama verisi imzalama algoritmasını kullanır.

Sertifika sahiplerine ait anahtar iftleri RSA algoritmasına sahiptir.

Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları iinde belirtilir.

### 7.1.4. İsim Alanı Biimleri

Kamu SM tarafından retilen Kurumsal Őifreleme Sertifikalarındaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici İsim]" biimine uygundur.

### 7.1.5. İsim Kısıtları

Blm 3.1'de belirtilmiřtir.

Tablo 2'de Kurumsal Őifreleme Sertifikası iinde yer alan isim alanları ve bu alanlar iine yazılacak bilgiler belirtilmiřtir.

Tablo 2 Kurumsal Őifreleme Sertifika İsim Alanı Bilgileri

Alan Adı	Kurumsal Őifreleme Sertifika İeriđi
CN <sup>9</sup>	Kurum DETSİS adı
Serial <sup>10</sup>	Kurum DETSİS numarası
C <sup>11</sup>	TR

### 7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bađlı olunan Kamu SM Sİ dokmanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.11

### 7.1.7. İlke Kısıtları Uzantısının Kullanımı

Dzenlenmesine gerek duyulmamıřtır.

### 7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Kurumsal Őifreleme Sertifikalarının retim ve ynetim iřlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduđuna iřaret eder. Kurumsal Őifreleme Sertifikalarının retim ve ynetiminde takip edilen kurallara iřaret eden Sİ dokmanına ait nesne tanımlama numarası

<sup>8</sup> ExtendedKeyUsage

<sup>9</sup> CN: Common Name [Genel isim]

<sup>10</sup> Serial: Serial Number [Seri Numarası]

<sup>11</sup> C: Country [lke]

[Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikasının “Sertifika İlkeleri Uzantısı<sup>12</sup>”nın içinde yer alır. “Sertifika İlkeleri Uzantısı”nın içinde “İlke Niteleyici<sup>13</sup>” olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler “Sertifika İlkeleri Uzantısı”nı kontrol ettiğinde Sİ/SUE’de belirtilen ilke ve uygulama esasları çerçevesinde Kurumsal Őifreleme Sertifikalarını kullanarak işlem yapar.

### 7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

## 7.2. Sertifika İptal Listesi Biçimi

### 7.2.1. Sürüm Numarası

Kamu SM’nin ürettiği SİL’ler “ITU X.509 V.2” SİL formatına uygundur.

### 7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL’ler “ITU X.509” SİL formatına uygun olarak aşağıdaki bilgileri içerir:

- SİL’i oluşturan Kamu SM’ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL’i imzalamak için SHA-384 özet algoritması ile ECDSA imza doğrulama verisi imzalama algoritmasını kullanır.)
- SİL’in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanması için son tarih
- İptal edilen Kurumsal Őifreleme Sertifikaları ile ilgili aşağıdaki bilgiler:
  - Sertifikanın seri numarası
  - Sertifikanın iptal tarihi
  - Sertifikanın neden iptal edildiği bilgisi (opsiyonel)
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM’ye ait sertifikanın “Yetkili Anahtar Tanımlayıcı” numarası

## 7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

### 7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 6960 V.1’i destekler.

### 7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

- Protokol versiyonu

<sup>12</sup> Certificate Policies

<sup>13</sup> Policy Identifier

- Hedef sertifika belirteci (kullanılan özetleme algoritması, sertifikayı veren ESHS'nin DN özeti, sertifikayı veren ESHS'nin imza dođrulama verisinin özeti, sertifika seri numarası)

ÇİSDUP yanıtları aŐađıdaki bilgileri içermektedir:

- Versiyon bilgisi
- Yanıtlayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritmasının nesne tanımlama numarası
- ÇİSDUP Yanıtlayıcı imzası

Bütün geçerli ÇİSDUP cevapları ÇİSDUP Yanıtlayıcı tarafından imzalanır. Geçersiz ÇİSDUP sorguları için dönen hata mesajları imzalanmaz.

Çevrim İçi Sertifika Durum Protokolü RFC 6960'ta tarif edilen "ÇİSDUP" formatını destekler. ÇİSDUP Yanıtlayıcı'dan alınan cevaplar aŐađıdaki Őekilde deđerlendirilir:

*Good [iyi]:* Sertifika geçerli konumdadır.

*Bad [kötü]:* Sertifika iptal edilmiŐtir (askı durumu da dahil).

*Unknown [bilinmiyor]:* Sorgusu yapılan sertifika hakkında herhangi bir bilgi bulunmamaktadır.

RFC 6960, ÇİSDUP sorguları ve yanıtları içerisinde bazı uzantıların kullanımına imkân verir. Tekrarlama (replay) saldırılarını önlemek için sorgu ve yanıtı birbirine bađlayan "nonce" uzantısı bunlardan biridir. Kamu SM ÇİSDUP Yanıtlayıcı, "nonce" uzantısını desteklemektedir. RFC 6960'da belirtilen diđer uzantılar ÇİSDUP yanıt formatında kullanılmamaktadır.

## 8. Uygunluk Denetimleri

Kamu SM, mevzuat geređi Bilgi Teknolojileri Kurumu (BTK) tarafından incelenir/denetlenir.

Kamu SM ek olarak, ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) standardına uygun olarak hizmet verir ve standart geređi düzenli olarak iç ve diŐ denetimlere tabi tutulur. Kamu SM iç iŐleyiŐini denetlemek için ayrıca iç denetimler gerçekleştirilir.

### 8.1. Uygunluk Denetiminin Sıklıđı

BTK, gerekli gördüđü durumlarda re'sen denetim yapabilir.

Kamu SM, ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) standardı geređince yılda bir defa uygunluk denetimi geçirir. Her üç yılda bir sertifika yenilenir.

İç denetim, yılda en az 1 (bir) defa olmak üzere gerçekleştirilir.

### 8.2. Denetçinin Nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiŐ olan BTK tarafından gerçekleştirilir.

ISO/IEC 27001 BGYS'nin denetimi akredite edilmiŐ kuruluşlarca gerçekleştirilir.

İç denetim, Kamu SM sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

### 8.3. Denetçinin Denetlenen Tarafı Olan İliŐkisi

BTK, kanun geređi tüm ESHS'leri denetlemekle yetkili kılınmiŐ düzenleyici kurumdur.

ISO/IEC 27001 BGYS'nin denetimi bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirilir.

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir. İç denetim için seçilen denetçiler denetlenecek birimden seçilmez.

#### 8.4. Denetimin Kapsamı

ESHS'lerin denetim kapsamı BTK tarafından belirlenir. ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun şekilde bağımsız kurum denetçisi tarafından belirlenir.

Kamu SM iç denetimlerinde, Sİ/SUE dokümanına uygunluk denetlenir. İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

#### 8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

BTK tarafından gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, ESHS tarafından planlı çalışma ile giderilir. Eksiklikler ESHS'nin işleyişini etkileyecek kadar büyük ise, ilgili mevzuata göre yaptırım ve cezalar uygulanır.

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'nin temel işleyişini etkileyecek kadar büyük ise Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İç denetimlerde ortaya çıkan eksiklikler, Kamu SM ilgili personeli tarafından giderilir. Tüm denetimlerden elde edilen bulgular Uygunsuzluk veya Düzeltici/İyileştirici Faaliyetler açılarak takip edilir.

#### 8.6. Sonucun Bildirilmesi

Denetim sonucu, BTK ve ISO/IEC 27001 denetçilerinin hazırladığı resmî raporlar ile Kamu SM'ye bildirilir.

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

### 9. Diğer İşler ve Hukuksal Meseleler

#### 9.1. Ücretlendirme

##### 9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen, yenilenen ve güncellenen Kurumsal Şifreleme Sertifikası için kurumlardan ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM web sitesinde bildirilir.

Kamu SM'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi ya da Kurumsal Şifreleme Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Kurumsal Şifreleme Sertifikalarının Kamu SM tarafından iptal edilmesi ve güncellenmesi halinde, hiçbir ücret talep edilmez.

##### 9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ait sertifikaları resmî web sitesinde ücretsiz olarak yayımlar. Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikaları DETSİS'e yüklenir.

### 9.1.3. İptal Durum Kaydına EriŐim Ücreti

Kamu SM, iptal durum kaydını SİL veya ÇİSDUP aracılıđıyla duyurma hizmeti için, sertifika sahibi kurumdan veya üçüncü kişilerden ücret talep etmez.

### 9.1.4. Diğer Servis Ücretleri

Sertifika yönetim prosedürleri için elektronik ortamdan ve çağrı merkezi üzerinden otomatik olarak gerçekleştirilen işlemlerden ücret talep edilmez.

Kamu SM, kuruma ait imza oluŐturma verisi ve sertifikanın saklandığı akıllı kartın teminini kendi imkanlarıyla sağlayabilir. Kurumsal Őifreleme Sertifikaları ve güvenli donanım araçları için ödenecek bedelin miktarı ile ilgili bilgilendirme Kamu SM tarafından gönderilen teklif mektuplarında veya Kamu SM web sitesinde bildirilir. Ödemenin usulüne uygun biçimde yapılmaması durumunda Kurumsal Őifreleme Sertifikası üretimi yapılmayabilir veya mevcut sertifika kullanım dıŐı bırakılabilir.

Kamu SM, bilgi deposundan yayımladığı bilgi ve dokümanlara erişim için sertifika sahibi kurumdan veya üçüncü kişilerden ücret talep etmez.

### 9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi tamamlanmamıŐsa kurumun talebi doğrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu deđildir.

## 9.2. Finansal Sorumluluk

### 9.2.1. Sigorta Kapsamı

Kamu SM, Bölüm 9.2.3'te belirtilen sertifika sahibi mali sorumluluk sigortası dıŐında, kendi sorumluluklarını karŐılamak amacıyla sigortalanmamıŐtır.

### 9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıŐtır.

### 9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu dođan zararların karŐılanması amacıyla, ürettiđi Kurumsal Őifreleme Sertifikalarını 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu geređince mali sorumluluk sigortası ile sigortalıdır.

## 9.3. Ticari Bilginin Korunması

### 9.3.1. Gizli Bilginin Kapsamı

Kamu SM ve sertifika hizmeti verdiđi taraflarca paylaşılan iş planları, satış bilgileri, ticari sırlar ve yapılan gizli anlaşmalarda verilen bilgiler ticari bilgi olarak deđerlendirilir. Ayrıca gizli olmadığı özel olarak bildirilmeyen tüm belge ve dokümanlar gizli olarak kabul edilir.

### 9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

Kamu SM resmî web sitesi bilgi deposu üzerinden yayımlanan doküman ve sertifikalar içerisinde yer alan bilgiler gizli olarak deđerlendirilmez.

### 9.3.3. Gizli Bilginin Korunma Sorumluluęu

Kamu SM ve ilgili taraflar karŐılıklı ticari bilgilerini üçüncü taraflarla paylaşmaz. Bu amaçla gerekli olan önlemleri alırlar.

## 9.4. KiŐisel Bilginin Gizlilięi

### 9.4.1. Gizlilik Planı

Kamu SM verdięi hizmetlerde sertifika sahiplerinin ve dięer paydaŐların kiŐisel verilerinin gizlilięini ilgili mevzuat ve 6698 sayılı KiŐisel Verilerin Korunması Kanunu (KVKK) kapsamındaki mer'i mevzuata uygun olarak saęlar.

### 9.4.2. Gizli Olarak Tanımlanan Bilgiler

KiŐisel bilgi, sertifika sahibi kurumun ve yetkilendirdięi Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları ile HSM Cihaz Sorumlusunun, baŐvuru sırasında kimlik tanımlama ve doęrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettięi bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi kurum tarafından atanan parolalar, numara, sembol gibi dięer tanımlayıcıyı bilgiler de kiŐisel bilgi kapsamına girer.

### 9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kurumsal Őifreleme Sertifikası içerięinde bulunan bilgiler, taraflar arası sözleşmelerde aksi belirtilmedięi sürece gizli deęildir.

### 9.4.4. Gizli Bilginin Korunma Sorumluluęu

Kamu SM, sertifika talep eden kurumdan Kurumsal Őifreleme Sertifikası vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettięi kiŐisel bilgileri sertifika hizmeti vermek dışında baŐka amaçlar için kullanmaz, üçüncü kiŐilere vermez, sertifika sahibi kurumun izni olmaksızın sertifikayı üçüncü kiŐilerin ulaŐabileceęi ortamlarda bulundurmaz.

Sertifika sahiplerinden baŐvuru sırasında ve daha sonra sertifika yaŐam döngüsü içinde istenen bilgilere erişimin ve yetkisiz kullanımın engellenmesi ve mahremiyetinin korunması için, Kamu SM tarafından gerekli güvenlik tedbirleri alınır. Sadece yetkilendirilmiş çalıŐanlar sertifika sahibi kurumun bilgilerine erişirler.

Kamu SM KiŐisel Verilerin Korunması Kanunu kapsamında <https://kamusm.bilgem.tubitak.gov.tr/kurumsal/kvkk> kurumsal web sayfasından bilgilendirme yapmaktadır.

### 9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM elde ettięi kiŐisel bilgileri kiŐilerin yazılı rızası ile izin almak Őartıyla yapılacak iŐ gereęi üçüncü kiŐilerle paylaşabilir.

### 9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM tarafından sertifika sorumlularına ait gizli kiŐisel bilgiler, mahkeme kararı olması durumunda açıklanabilir.

### 9.4.7. Dięer BaŐlıklar

Düzenlenmesine gerek duyulmamıŐtır.

## 9.5. Telif Hakları

Kamu SM tarafından üretilen tüm Kurumsal Őifreleme Sertifikaları ve dokümanlar ile bu Sİ/SUE dokümanları ile diđer ilişkili dokümanlara bađlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

## 9.6. Temsil Hakkı ve Yükümlölükler

Kamu SM tarafından verilen sertifika hizmetlerinde sistem bileşenleri olarak tanımlanan Kamu SM, sertifika sahipleri ve üçüncü kişiler ilgili mevzuatlarda belirtilen şekilde üzerlerine düşen yükümlölükleri yerine getirir.

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kişiler, yasa ve yönetmeliklerde belirtilmediđi halde imzalanmış olan başvuru formu ve taahhütnamelerde yer alan yükümlölüklerini de yerine getirirler.

Kamu SM'nin ESHS olarak işleyişinin güvenli olabilmesi için, sistem bileşenlerinin yerine getirmesi gereken yükümlölükler aşağıda belirtilmiştir.

### 9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlölükleri

ESHS olarak Kamu SM'nin yükümlölükleri aşağıda belirtilmiştir:

- Hizmetin gerektirdiđi nitelikte personel istihdam etmek
- Belirlediđi ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek
- Sİ/SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak
- Kök SHS ve Kurumsal Őifreleme SHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak
- Kök SHS ve Kurumsal Őifreleme SHS sertifikalarını son kullanıcıların erişebileceđi ortamlarda yayımlamak
- Kurumsal Őifreleme Sertifikası verdiđi kurumların kimliđini DETSİS üzerinden güvenilir bir biçimde dođrulamak
- Kurumlardan gelen Kurumsal Őifreleme Sertifikası başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kurumların belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek
- Kurumsal Őifreleme Sertifikasının içeriđindeki bilgilerin dođruluđunu beyan edilen belgelere dayanarak sağlamak
- Gereklili başvuru şartlarını sağlamayan başvuru sahiplerine Kurumsal Őifreleme Sertifikası vermemek
- Kurumsal Őifreleme Sertifikası başvurularını deđerlendirerek, başvurunun sonucu hakkında kurumları ya da kurumların yetkilendirdikleri sorumlu kişileri bilgilendirmek
- Kurumsal Őifreleme Sertifikası başvurusu kabul edilmiş kurumlar için anahtar çifti ve Kurumsal Őifreleme Sertifikası üretmek
- Sertifika sahibi kuruma ait imza oluşturma verisini oluşturduktan sonra imza oluşturma verisi ve üretiminde kullanılan gizli deđerkenleri kendi sisteminden silmek, imza oluşturma verisinin kopyasını hiçbir şekilde tutmamak
- Sertifika sahibine akıllı kart temin etmesi durumunda, bu aracın güvenli olmasını sağlamak
- Üretilen Kurumsal Őifreleme Sertifikaları imza oluşturma verilerini Sİ/SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek

- Sertifika sahiplerinin Kurumsal Őifreleme Sertifikalarını DETSİS'e yklemek
- Kurumsal Őifreleme Sertifikalarının kullanım Őartlarını belirleyen sertifika profillerini oluŐturmak
- Kurumsal Őifreleme Sertifika baŐvurularını Sİ/SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli iŐlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıya alma baŐvurularını Sİ/SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli askıya alma iŐlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıdan indirme iŐlemlerini Sİ/SUE'de belirtilen Őekilde yapmak
- Kurumsal Őifreleme Sertifikası iptal baŐvurularını Sİ/SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli iptal iŐlemlerini zamanında yapmak
- Yayımlanan Sİ/SUE dokmanları ile taahhnamelere uygun olmayan Kurumsal Őifreleme Sertifikası kullanımlarının tespit edilmesi durumunda ilgili Kurumsal Őifreleme Sertifikasını iptal etmek
- İptal edilmiŐ Kurumsal Őifreleme Sertifikası bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılıęıyla duyurmak
- Kurumsal Őifreleme Sertifikalarının ve iptal durum kayıtlarının btnlęn ve eriŐilebilirlięini saęlamak iin her trl tedbiri almak
- Sertifika sahiplerine ait elektronik veya kâęit ortamda tutulan bilgilerin gizlilięinin korunması iin gerekli nlemleri almak, bu bilgileri nc kiŐilere mahkeme kararı olmaksızın vermemek
- Kurumsal Őifreleme Sertifikası retim, ynetim ve iptali ile ilgili yapılan tm iŐlemlerin kaydını tutmak
- İŐleyiŐ sırasında kullanılan tm kâęit ve elektronik kayıtları ilgili Sİ/SUE'de belirtilen sreler boyunca gvenli olarak saklamak

### 9.6.2. Kayıt Birimi Ykmllkleri

Kayıt biriminin sorumlulukları Őunlardır:

- Kurumsal Őifreleme Sertifika baŐvurularını almak,
- Kurum kimlięini ve kurum adına iŐlem yapan yetkili kimlięini Sİ/SUE'de ve ilgili prosedrlerde belirtilen yntemlerle gerekli belgelere dayanarak doęrulamak,
- BaŐvuruları deęerlendirerek, baŐvurunun sonucu hakkında ilgili kiŐileri bilgilendirmek,
- Sertifika iptal baŐvurularını almak,
- Doęrulan sertifika iptal baŐvurularını Kamu SM'nin ilgili birimlerine iletmek,
- İptal edilen sertifikalar hakkında sahiplerini bilgilendirmek.

### 9.6.3. Sertifika Sahibinin Ykmllkleri

Sertifika sahibinin ykmllkleri aŐaęıda belirtilmiŐtir:

- Kurumsal Őifreleme Sertifikası baŐvuru, askıya alma, iptal ve dięer iŐlemleri, Sİ/SUE'de belirtildięi Őekilde, detayları Kamu SM Kurumsal Őifreleme Sertifikası ynetim prosedrlerinde anlatılan usule uygun biimde yerine getirmek
- Kurumsal Őifreleme Sertifikası baŐvurusu, yenileme ve iptal iŐlemleri sırasında doęru bilgi beyan etmek
- Kurum adına dzenlenen Kurumsal Őifreleme Sertifikası retildięinde sertifikadaki bilgilerin doęruluęunu kontrol etmek

- SUE Bölüm 6.2.1’de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- İmza oluŐturma verisinin güvenliğini sađlamak, kendisine ait imza oluŐturma verisinin içinde bulunduđu akıllı kart veya HSM cihazının ve eriŐim verisinin gizliliğini korumak, bunları başkasına kullandırmamak ve bu konuda gerekli tedbirleri almak
- İnternet veya çağrı merkezi üzerinden sertifika işlemlerini yapabilmesi için kullandıđı parolalarının gizliliğini ve güvenliğini sađlamak
- İmza oluŐturma verisinin içinde bulunduđu akıllı kart veya HSM’nin kaybolması, çalınması veya imza oluŐturma verisinin gizliliğinin yitirildiğinden Őüphelenmesi durumunda Kurumsal Őifreleme Sertifikasının iptal edilmesi için Bölüm 3.4’te belirtilen kanallar üzerinden Kamu SM’ye en kısa zamanda başvurmak
- Akıllı kart veya HSM eriŐim verisini ve sertifika işlemlerinde kullandıđı diđer parolaları düzenli olarak deđiŐtirmek
- Kurumsal Őifreleme Sertifikası içeriğinde bulunan bilgilerin deđiŐmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM’ye başvurmak
- Kurumsal Őifreleme Sertifikası başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiđi bilgilerde meydana gelen deđiŐiklikleri derhal Kamu SM’ye bildirmek
- İptal olmuŐ, kullanıma açılmamıŐ, askıya alınmıŐ veya geçerlilik süresi dolmuŐ Kurumsal Őifreleme Sertifikası ile işlem yapmamak
- Kurumsal Őifreleme Sertifikası ile iliŐkili imza oluŐturma verilerini imzalama amacıyla kullanmamak.

Sertifika sahibi kurum, Kamu SM Kurumsal Őifreleme Sertifikası Sİ/SUE dokümanlarında belirtilen Őartları okuduđunu, başvuru süreci ve sertifika geçerliliđi boyunca taahhütname, ilgili mevzuatlar ile Sİ/SUE dokümanında belirtilen Őartlara uygun olarak hareket edeceđini kabul ve taahhüt eder. Yükümlölüklerin ihlali nedeniyle üçüncü kiŐilerin/kurumun zarara uđraması halinde TÜBİTAK BİLGEM’in ödemek zorunda olduđu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

#### 9.6.4. Üçüncü KiŐilerin Yükümlölükleri

Üçüncü kiŐiler, Kurumsal Őifreleme Sertifikasıyla işlem yapmadan önce sertifikanın aŐađıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Kurumsal Őifreleme Sertifikasının tanımlanan veriliŐ amacına uygun olarak kullanıldıđını dođrulamak
- Kurumsal Őifreleme Sertifikasının kullanım süresinin dolup dolmadıđını kontrol etmek
- Kurumsal Őifreleme Sertifikasının geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılıđıyla kontrol etmek
- SİL veya ÇİSDUP Yanıtlayıcı’dan aldıđı iptal durum kaydının bütünlüğünü Kamu SM’nin ilgili sertifikası içinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kurumsal Őifreleme Sertifikasının dođruluđunu Kurumsal Őifreleme SHS sertifikasının içinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kurumsal Őifreleme SHS sertifikasının dođruluđunu Kök SHS sertifikasının içinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kök SHS sertifikasının bütünlüğünü sertifika özet deđerini kontrol etmek suretiyle dođrulamak
- Sertifika sahibinin Kurumsal Őifreleme Sertifikasının içindeki imza dođrulama verisine karŐılık gelen imza oluŐturma verisine sahip olduđunu dođrulamak

### 9.6.5. Diđer Bileőenlerin Yüklümlükleri

#### 9.6.5.1. Kurumun Yüklümlükleri

Kamu SM'ye sertifika başvurusunda bulunan kurumun yüklümlükleri aőađıda belirtilmiőtir:

- Sertifika başvurusunu Kamu SM web sitesinde belirtilen yöntemleri kullanarak Kamu SM'ye iletmek ve Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularını görevlendirerek belirlenen sorumluları Kamu SM'ye bildirmek
- Sertifika sorumlusunun/sorumlularının görevi sonlandırıldıđında ya da yeni bir sorumlu görevlendirildiđinde Kamu SM'ye Kamu SM web sitesinde yer alan sorumlu deđiŐikliđi yönergesi kapsamında bildirmek
- Sertifika yönetim süreçleri ile ilgili taahhütnamelerdeki yüklümlükleri yerine getirmek

#### 9.6.5.2. Kurum Sertifika Sorumlularının Yüklümlükleri

Kurum adına Kurumsal Őifreleme Sertifikası başvurusunda bulunan Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının yüklümlükleri aőađıda belirtilmiőtir:

- Sertifika alınacak kuruma ait bilgileri tam ve dođru bir Őekilde Kamu SM'ye iletmek
- Sertifika yönetim süreçleri ile ilgili iŐleri Kamu SM ile koordineli bir Őekilde yürütmek
- Kamu SM'nin kendisine imzalattıđı taahhütnamedeki yüklümlükleri yerine getirmek

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının sertifika teslimatları ile ilgili yüklümlükleri taahhütnamelerde belirtilmiőtir.

### 9.7. Yüklümlüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yüklümlük, taahhütnamelerde belirtildiđi Őekilde sona erer.

### 9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları ilgili mevzuatta belirtilen Őartlar ile sınırlıdır. Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar taahhütnamelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel Őartları ile diđer düzenlemeler dikkate alınır.

### 9.9. Tazminat Halleri

Kamu SM ve sertifika hizmeti alan taraflar arasında yüklümlüklerin yerine getirilmemesinden kaynaklanan zararlar, tarafların o ana kadar somut olarak gerçekleŐmiŐ hak ve alacakları korunmak suretiyle tasfiye edilir.

### 9.10. AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi

Sertifika sahibi kurum, taahhütnamelere uygun olarak Kamu SM ile iŐ birliđi içinde çalıŐır.

Sertifika sahibi kurumlar sertifika hizmetlerini aldıkları süre boyunca Sİ/SUE dokümanları ile sertifika yönetim prosedürlerinde belirtilen Őartları yerine getirmeyi kabul ederler.

Kamu SM sertifika hizmeti verdiđi süre boyunca Sİ/SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine iletildiđi taahhütnamelerdeki Őartları yerine getirir.

### 9.10.1. AnlaŐma Suresi

Sertifika sahibi kurumun imzaladıđı taahhütnamelerin süresi sertifikanın geçerlilik süresi veya taahhütnamede belirtilmiŐse hizmetin alınma süresi kadardır.

### 9.10.2. AnlaŐmanın Sona Ermesi

Kamu SM, imzalanan taahhütnameleri aŐađıdaki durumlarda sonlandırılabilir:

- Sertifika sahibi kurumun sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi
- Sertifika sahibi kurumun imzalanan taahhütnamelere aykırı davranması durumunda Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Bölüm 5.7.3'te belirtilen güvenlik açığına ortaya çıkması sebebiyle Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Kamu SM Bölüm 5.8'de belirtildiđi biçimde sertifika hizmetlerini sonlandırırorsa, Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi

### 9.10.3. AnlaŐmanın Sona Ermesinin Etkileri

İmzalanan taahhütnamelerin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ/SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Sertifika sahibi kurumun taahhütnamelerden, Sİ/SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesi durumunda, Kamu SM sertifikayı iptal eder. Sertifika sahibi kurumun taahhütnameye uygun hareket etmemesinden dolayı uğrayacađı zararlardan Kamu SM sorumlu tutulamaz.

Taahhütnameler sona erse bile Kamu SM, ürettiđi Kurumsal Őifreleme Sertifikaları ile ilgili mevzuatta belirtilen yükümlülükleri yerine getirmeye devam eder. Kamu SM, ürettiđi Kurumsal Őifreleme Sertifikalarının iptal durum kayıtlarına taraflarca erişimin sağlanması ile Bölüm 5.4 ve 5.5'te belirtilen kayıtların ve arŐivlerin saklanması ile ilgili hizmetleri sürdürür.

## 9.11. Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme

Kamu SM, Kurumsal Őifreleme Sertifikaları başvuru, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılıđıyla sağlanır. Başvuru Formu ve Taahhütnamede belirtilen sertifika sorumlularının kurumsal e-posta adresine, deđiŐmesi halinde yeni bildirdiđi kurumsal e-posta adresine yapılan bilgilendirmeler resmî bildirim olarak kabul edilir.

Sertifika yönetim iŐlemleri sırasında sertifika sorumluları veya sertifika sahibi kurumlarla yapılan haberleŐmenin hangi durumlarda, ne Őekilde yapılacađı Kamu SM'nin Kurumsal Őifreleme Sertifikası yönetim prosedürlerinde detaylı olarak belirtilir.

## 9.12. DeđiŐiklik Halleri

### 9.12.1. DeđiŐiklik Metotları

SUE dokümanı Kamu SM tarafından yazılmıŐtır. Bu SUE dokümanında yapılabilecek deđiŐiklikler ekleme ve deđiŐtirme Őeklinde olabileceđi gibi Kamu SM dokümanının tamamen yenilenmesine de karar verebilir. Bu SUE dokümanının herhangi bir kısmının yanlış ya da geçersiz olduđu ortaya çıksa bile SUE dokümanının diđer kısımları, SUE dokümanı güncellenene kadar geçerliliđini sürdürür.

### 9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan deęişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman makul bir süre içerisinde bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer.

### 9.12.3. Nesne Tanımlama Numarasının Deęişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

### 9.13. Anlaşmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilaf durumlarında ilgili mevzuata başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

### 9.14. Uygulanacak Hukuk

Bu SUE dokümanı, Türkiye Cumhuriyeti'nin yürürlükteki tüm uygulanabilir yasa ve yönetmeliklerine tabidir. SUE'nin uygulanmasında ve yorumlanmasında Türkiye Cumhuriyeti Hukuku geçerlidir.

### 9.15. Uygulanabilir Yasalarla Uyum

Kamu SM, sertifika sahibi ve ilgili tüm taraflar Türkiye Cumhuriyeti'nde yürürlükte olan tüm uygulanabilir yasa ve yönetmeliklere uymayı kabul eder. Sİ/SUE dokümanında geçen hükümlerin daha sonra yürürlüğe girecek ilgili mevzuata aykırı bulunması halinde dokümanda gerekli deęişiklikler yapılarak uygun hale getirilir.

### 9.16. Çeşitli Hükümler

#### 9.16.1. Tüm Sözleşmeler

Kamu SM ürün ve hizmetlerini kullanan her bir tarafın, ürün veya hizmete ilişkin şartları tanımlayan bir sözleşme yapmasını gerektirir.

#### 9.16.2. Atama

Düzenlenmesine gerek duyulmamıştır.

#### 9.16.3. Bölünebilirlik

Bu Sİ/SUE'nin herhangi bir hükmünün geçersiz veya uygulanamaz olduğu tespit edilirse, Sİ/SUE'nin geri kalanı geçerli ve uygulanabilir olmaya devam eder.

#### 9.16.4. İcra (Avukatlık Ücretleri ve Haklardan Feragat)

Düzenlenmesine gerek duyulmamıştır.

#### 9.16.5. Mücbir Sebepler

Kamu SM, yürürlükteki yasaların izin verdiği ölçüde bu Sİ/SUE kapsamındaki bir yükümlülüğün yerine getirilmesinde kendi makul kontrolü dışındaki bir olaydan kaynaklanan gecikme veya başarısızlıklardan sorumlu değildir.

### 9.17. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

## 10. EK-A SERTİFİKA PROFİLLERİ

## 10.1. KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI

Alan	Deęer
Sürüm	V3
Seri Numarası	00e1ce95c004aa
İmza Algoritması	SHA-384 ile ECDSA { 1 2 840 10045 4 3 3 }
Sertifikayı Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 7 O = TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi S = Kocaeli C = TR
Geçerlilik Başlangıcı	24 Eylül 2025 Çarşamba 14:53:39
Geçerlilik Sonu	22 Eylül 2035 Cumartesi 14:53:39
Konu	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 7 O = TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi S = Kocaeli C = TR
İmza Doğrulama Verisi	384 bit ECC { 1 2 840 10045 2 1 } ECDSA_P384 { 1 3 132 0 34 }
Uzantılar	Deęer
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 11 4e 71 d3 e3 3b b6 c0 68 2f 9e 84 65 9e 93 23 4b 98 a6 9d
Anahtar Kullanımı	<b>Kritik=Evet</b> ; Sertifika İmzalama, SİL İmzalama
Temel Kısıtlamalar	<b>Kritik=Evet</b> ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

## 10.2. KAMU SM KURUMSAL ŐİFRELEME ALT KÖK SERTİFİKASI

Alan	Deęer
Sürüm	V3
Seri Numarası	32d34cef04f8
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifika Vereni	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 7 O = TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi S = Kocaeli C = TR
Geçerlilik Başlangıcı	10 Nisan 2026 Cuma 11:54:16
Geçerlilik Sonu	22 Eylül 2035 Cumartesi 14:53:39
Konu	CN = Kurumsal Őifreleme Sertifika Hizmet Sağlayıcısı - Sürüm 2 O = TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi S = Kocaeli C = TR
İmza Doğrulama Verisi	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	Deęer
Yetkili Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 11 4e 71 d3 e3 3b b6 c0 68 2f 9e 84 65 9e 93 23 4b 98 a6 9d
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 0d d5 f0 8d 71 76 f2 71 dd a7 fd c9 2f d3 dd 3f 7d 51 29 9b
Anahtar Kullanımı	<b>Kritik=Evet</b> ; Sertifika İmzalama, SİL İmzalama
Temel Kısıtlar	<b>Kritik=Evet</b> ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0

Sertifika İlkeleri	<p>[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=CPS Niteleyici= <a href="http://depo.kamusm.gov.tr/ilke">http://depo.kamusm.gov.tr/ilke</a></p> <p>[1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.</p>
SİL Dađıtım Noktaları	<p>[1]SİL Dađıtım Noktası Dađıtım Noktası Adı: Tam Ad: URL=<a href="http://depo.kamusm.gov.tr/nes/kokshs.v7.crl">http://depo.kamusm.gov.tr/nes/kokshs.v7.crl</a></p>
Yetkili Bilgi EriŐimi	<p>[1]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Sertifika Yetkilisi Yayımıcısı (1.3.6.1.5.5.7.48.2) Diđer Ad: URL=<a href="http://depo.kamusm.gov.tr/nes/kokshs.v7.crt">http://depo.kamusm.gov.tr/nes/kokshs.v7.crt</a></p>

### 10.3. SON KULLANICI KURUMSAL ŐİFRELEME SERTİFİKA ŐABLONU

Alan	Deđer
Sürüm	V3
Seri Numarası	En fazla 64 bit rassal sayı içeren tam sayı
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	<p>CN = Kurumsal Őifreleme Sertifika Hizmet Sađlayıcısı - Sürüm 2 O = TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi S = Kocaeli C = TR</p>
Geçerlilik BaŐlangıcı	Sertifika geçerlilik baŐlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu

Konu	CN = Kurum DETSİS adı Serial = Kurum DETSİS numarası C = TR
İmza Doğrulama Verisi	2048 bit RSA {1 2 840 113549 1 1 1}
<b>Uzantılar</b>	<b>Deęer</b>
Yetkili Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimlięi= 0d d5 f0 8d 71 76 f2 71 dd a7 fd c9 2f d3 dd 3f 7d 51 29 9b
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimlięi= Sertifikanın içerięindeki "subjectPublicKey" alanının "BIT STRING" olarak deęerinin SHA-1 özet çiktısından oluşur.
Anahtar Kullanımı	<b>Kritik=Evet</b> ; Anahtar Őifreleme
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluęu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimlięi=CPS Niteleyicisi= <a href="http://depo.kamusm.gov.tr/ilke">http://depo.kamusm.gov.tr/ilke</a> [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimlięi=Kullanıcı Uyarısı Niteleyicisi= Uyarı Metni=Bu sertifika, 2017/21 sayılı Başbakanlık Genelgesi kapsamında belirtilen kurumsal Őifreleme sertifikasıdır.
Geniřletilmiş Anahtar Kullanımı	Kurumsal Őifreleme Sertifikası (2.16.792.1.2.1.1.5.7.51.1)
SİL Daęıtım Noktaları	[1]SİL Daęıtım Noktası Daęıtım Noktası Adı: Tam Ad: URL= <a href="http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v2.crl">http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v2.crl</a>

Yetkili Bilgi EriŐimi	<p>[1]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Sertifika Yetkilisi Yayımcsısı (1.3.6.1.5.5.7.48.2) Diđer Ad: URL=<a href="http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v2.crt">http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v2.crt</a></p> <p>[2]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1) Diđer Ad: URL=<a href="http://ksifrelemeocspv2.kamusm.gov.tr/">http://ksifrelemeocspv2.kamusm.gov.tr/</a></p>
-----------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------