

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŞİFRELEME SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu

YON.05.02

Revizyon No

04

Revizyon Tarihi

17.02.2022

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 baŐvuru formlarının birleőtirilmesi dođrultusunda "Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi" dokümanının adı "Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taaahhütnamesi" olarak deđiőtirilmiőtir.	07.01.2022
04	Sertifika üretiminin iki kiőtinin kontrolünde yapılması gerektiđi ile ilgili ibare kaldırılmıőtir.	17.02.2022

İÇİNDEKİLER

1.	GİRİŐ	10
1.1.	Genel Bakıő	10
1.2.	Doküman Adı ve Tanımı	11
1.3.	Sistem Bileőenleri	11
1.3.1.	Elektronik Sertifika Hizmet Saėlayıcısı	11
1.3.2.	Kayıt Birimleri	11
1.3.3.	Sertifika Sahipleri	11
1.3.4.	Üçüncü Kiőiler	11
1.3.5.	Diėer Bileőenler	12
1.4.	Sertifika Kullanımı	12
1.4.1.	Uygun Olan Sertifika Kullanımı	12
1.4.2.	Sertifika Kullanımının Sınırları	12
1.5.	Uygulama Esaslarının Yönetimi	12
1.5.1.	Doküman Yönetimi	12
1.5.2.	İletiőim Bilgileri	12
1.5.3.	Sertifika Uygulama Esaslarının İkelere Uygunluėunu Belirleyen Kiő	13
1.5.4.	Sertifika Uygulama Esasları Onay Prosedürleri	13
1.6.	Tanımlar ve Kısaltmalar	13
1.6.1.	Tanımlar	13
1.6.2.	Kısaltmalar	15
2.	YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ	16
2.1.	Bilgi Depoları	16
2.2.	Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması	16
2.3.	Yayım Sıklıėı ve Zamanı	16
2.4.	Eriőim Kontrolleri	16
3.	KİMLİK BELİRLEME VE DOėRULAMA	17
3.1.	İsmlendirme	17
3.1.1.	İsim Alanı Tipleri	17
3.1.2.	Kimlik Bilgilerinin Teőhise Elveriőli Olması	17
3.1.3.	Sertifika Sahibinin Takma İsim veya Lakap Kullanması	17
3.1.4.	Farklı İsim Alanı Tiplerinin Yorumlanması	17
3.1.5.	Kimlik Bilgilerinin Tekilliėi	17
3.1.6.	Markanın Tanınması, Doėrulanması ve Rolü	17
3.2.	İlk Kimlik Belirleme	17
3.2.1.	Özel Anahtar Sahipliėinin Kanıtlanması	17
3.2.2.	Kurumsal Kimliėin Belirlenmesi	18
3.2.3.	Kiőisel Kimliėin Belirlenmesi	18
3.2.4.	Doėrulanmayan Sertifika Sahibi Bilgileri	18
3.2.5.	Yetkinin Doėrulanması	18
3.2.6.	Uyum Kriterleri	18
3.3.	Sertifika Yenileme İsteėinde Kimlik Doėrulama	18
3.3.1.	Olaėan Sertifika Yenileme İsteėinde Kimlik Doėrulama	18
3.3.2.	İptal Sonrası Yeni Sertifika Talebinde Kimlik Doėrulama	18
3.4.	Sertifika İptal İsteėinde Kimlik Doėrulama	19

4. İŐLEMSEL GEREKLER	19
4.1. Sertifika Başvurusu	19
4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiđi	19
4.1.2. Kayıt İŐlemleri ve Sorumluluklar	19
4.2. Sertifika Başvurusunun İŐlenmesi	20
4.2.1. Kimlik Tanımlama ve Doğrulama İŐlevlerinin Yerine Getirilmesi	20
4.2.2. Sertifika Başvurusunun Kabul veya Reddi	21
4.2.3. Sertifika Başvurusunun İŐlenme Zamanı	21
4.3. Sertifikanın OluŐturulması	21
4.3.1. Sertifika OluŐturulmasında ESHS'nin İŐlevleri	21
4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi	22
4.4. Sertifikanın Kabulü	22
4.4.1. Sertifikanın Kabul KoŐulu	22
4.4.2. Sertifikanın ESHS Tarafından Yayınlanması	22
4.4.3. Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması	22
4.5. Sertifikanın ve Özel Anahtarın Kullanımı	22
4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı	22
4.5.2. Üçüncü KiŐilerin Sertifika ve Açık Anahtar Kullanımı	23
4.6. Sertifika Süresinin Uzatılması	23
4.7. Sertifika Yenileme	23
4.7.1. Sertifikanın Yenileme KoŐulları	23
4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi	23
4.7.3. Sertifika Yenileme Başvurusunun İŐlenmesi	23
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi	24
4.7.5. Sertifika Yenileme Sonrası Kabul KoŐulu	24
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması	24
4.7.7. Sertifika Yenilemenin Diđer Tarafra Duyurulması	24
4.8. Sertifikada Bilgi DeđiŐikliđi	24
4.9. Sertifikanın İptali ve Askıya Alınması	24
4.9.1. Sertifikanın İptal Edildiđi Durumlar	24
4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir	25
4.9.3. Sertifika İptal Başvurusunun İŐlenmesi	25
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	26
4.9.7. Sertifika İptal Listesi Yayınlama Sıklıđı	26
4.9.8. Sertifika İptal Listesi Yayınlama Gecikme Süresi	26
4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti	26
4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi	26
4.9.11. Diđer Sertifika Durum Bildirim Yöntemleri	27
4.9.12. Özel Anahtarın Güvenliđini Yitirmesi Durumu	27
4.9.13. Sertifikanın Askıya Alındıđı Durumlar	27
4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi	27
4.9.15. Sertifika Askıya Alma Başvurusunun İŐlenmesi	28
4.9.16. Askıda Kalma Süresi	28
4.10. Sertifika Durum Servisleri	28

4.10.1.	İřletimsel Özellikleri.....	28
4.10.2.	Servisin Eriřilebilirliđi.....	28
4.10.3.	İsteđe Bađlı Özellikler.....	28
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.....	29
5.1.2.	Fiziksel Eriřim	29
5.1.3.	Güç Kaynađı ve Havalandırma	30
5.1.4.	Su Baskınları.....	30
5.1.5.	Yangın Önleme ve Korunma.....	30
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması	30
5.1.7.	Atıkların Yok Edilmesi	30
5.1.8.	Farklı Mekanlarda Yedekleme.....	30
5.2.	Prosedürel Kontroller.....	30
5.2.1.	Güvenilir Roller	30
5.2.2.	Her İřlem İin Gereken Kiři Sayısı.....	31
5.2.3.	Kimlik Doğrulama ve Yetkilendirme.....	31
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	31
5.3.	Personel Güvenlik Kontrolleri	31
5.3.1.	Kiřisel Geçmiş, Deneyim ve Nitelik Gerekleri	31
5.3.2.	Geçmiş Arařtırması	31
5.3.3.	Eđitim Gerekleri	32
5.3.4.	Sürekli Eđitim Gerekleri ve Sıklıđı.....	32
5.3.5.	Görev Deđişim Sıklıđı ve Sırası.....	32
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	32
5.3.7.	Anlařmalı Personel Gereksinimleri	32
5.3.8.	Sađlanan Dokümantasyon	32
5.4.	Denetim Kayıtları	32
5.4.1.	Kaydedilen İřlemler	32
5.4.2.	Kayıtların İncelenme Sıklıđı	33
5.4.3.	Kayıtların Saklanma Süresi	33
5.4.4.	Kayıtların Korunması	34
5.4.5.	Kayıtların Yedeklenmesi	34
5.4.6.	Kayıtların Toplanması	34
5.4.7.	Kayda Sebepiyet Veren Tarafın Bilgilendirilmesi.....	34
5.4.8.	Saldırıya Açıklıđın Deđerlendirilmesi.....	34
5.5.	Kayıt Arřivleme	34
5.5.1.	Arřivlenen Kayıt Bilgileri.....	34
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.....	35
5.5.6.	Arřivlerin Toplanması	35
5.5.7.	Arřiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu.....	35

5.6.	Anahtar DeęiŐimi.....	35
5.7.	Güvenlięin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	35
5.7.1.	Güvenilirlięin Yitirilmesi Durumunun Düzeltilmesi	35
5.7.2.	Donanım, Yazılım veya Veri Bozulması	36
5.7.3.	İmza OluŐturma Verisinin Gizlilięinin Kaybedilmesi	36
5.7.4.	Arıza Sonrası Yeniden ÇalıŐırlık	36
5.8.	Sertifika Hizmetlerinin Sonlandırılması.....	36
6.	TEKNİK GÜVENLİK KONTROLLERİ	37
6.1.	Anahtar Çifti Üretimi ve Kurulumu	37
6.1.1.	Anahtar Çifti Üretimi	37
6.1.2.	Sertifika Sahibine Özel Anahtarın UlaŐtırılması.....	38
6.1.3.	Elektronik Sertifika Hizmet Saęlayıcısı'na Açık Anahtarın UlaŐtırılması	38
6.1.4.	Elektronik Sertifika Hizmet Saęlayıcısı Sertifikalarına EriŐim Saęlanması	38
6.1.5.	Anahtar Uzunlukları.....	38
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü.....	39
6.1.7.	Anahtar Kullanım Amaçları	39
6.2.	Özel Anahtarın Korunması	39
6.2.1.	Kriptografik Modül Standartları	39
6.2.2.	Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim	39
6.2.3.	Özel Anahtarın Yeniden Elde Edilmesi	39
6.2.4.	Özel Anahtarın Yedeklenmesi	40
6.2.5.	Özel Anahtarın ArŐivlenmesi	40
6.2.6.	Özel Anahtarın Kriptografik Modüle Yüklmesi	40
6.2.7.	Özel Anahtarın Kriptografik Modülde Saklanması	40
6.2.8.	Özel Anahtara EriŐim	40
6.2.9.	Özel Anahtara EriŐimin Kesilmesi.....	40
6.2.10.	Özel Anahtarın Yok Edilmesi	41
6.2.11.	Kriptografik Modülün Deęerlendirilmesi	41
6.3.	Anahtar Çifti Yönetimiyle İlgili Dięer Konular	41
6.3.1.	Açık Anahtarın ArŐivlenmesi	41
6.3.2.	Özel ve Açık Anahtarların Kullanım Süreleri	41
6.4.	EriŐim Denetim Verileri.....	41
6.4.1.	EriŐim Denetim Verilerinin OluŐturulması	41
6.4.2.	EriŐim Denetim Verilerinin Korunması.....	42
6.4.3.	EriŐim Denetim Verileri ile İlgili Dięer Konular	42
6.5.	Bilgisayar Güvenlięi Denetimleri	42
6.5.1.	Bilgisayar Güvenlięi ile İlgili Teknik Gereker	42
6.5.2.	Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi.....	42
6.6.	YaŐam Döngüsü Teknik Kontrolleri.....	42
6.6.1.	Sistem GeliŐtirme Kontrolleri	42
6.6.2.	Güvenlik Yönetimi Kontrolleri.....	43
6.6.3.	YaŐam Döngüsü Güvenlik Denetimleri.....	43
6.7.	Aę Güvenlięi Denetimleri	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	44
7.1.3.	Algoritma ve Nesne Tanımlayıcılar	45
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	46
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	48
8.5.	Yetersizliğin Tespiti Durumunda Yapılacaklar	48
8.6.	Sonucun Bildirilmesi	48
9.	DIĞER 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.....	49
9.1.4.	Diđer Servis Ücretleri	49
9.1.5.	İade Ücreti.....	49
9.2.	Finansal Sorumluluk	49
9.2.1.	Sigorta Kapsamı	49
9.2.2.	Diđer Varlıklar	49
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	50
9.4.	Kişisel Bilginin Gizliliđi.....	50
9.4.1.	Gizlilik Planı	50
9.4.2.	Gizli Olarak Tanımlanan Bilgiler	50
9.4.3.	Gizli Olarak Tanımlanmayan Bilgiler	50
9.4.4.	Gizli Bilginin Korunma Sorumluluđu	50
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.....	51
9.6.	Temsil Hakkı ve Yüklümlüklükler	51
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yüklümlüklükleri	51
9.6.2.	Kayıt Birimi Yüklümlüklükleri	53
9.6.3.	Sertifika Sahibinin Yüklümlüklükleri	53
9.6.4.	Üçüncü KiŐilerin Yüklümlüklükleri	53
9.6.5.	Diđer BileŐenlerin Yüklümlüklükleri.....	54
9.7.	Yüklümlüklüklerden Feragat.....	54
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.....	55
9.10.2.	AnlaŐmanın Sona Ermesi	55
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri	56
9.11.	Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme	56
9.12.	DeđiŐiklik Halleri	57
9.12.1.	DeđiŐiklik Metotları	57
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.	Diđer Hükümler	57
10.	EK-A SERTİFİKA PROFİLLERİ.....	58
10.1.	KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI	58
10.2.	KAMU SM KURUMSAL ŐİFRELEME ALT KÖK SERTİFİKASI	59
10.3.	SON KULLANICI KURUMSAL ŐİFRELEME SERTİFİKA ŐABLONU	60

TABLolar

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

1. Giriő

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

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladıėı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik, 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 İletiőim Kurulu Kararı ile yayımlanan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliőkin Usul ve Esaslar'da belirtilen tanıma uygun olarak Kurumsal Őifreleme Sertifikası hizmeti saėlamaktadır.

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 etmiőt sayılır. Kurumsal Őifreleme Sertifikası talebinde bulunan kurumlar bununla ilgili olarak Kamu SM ile imzaladııkları sözleőme veya baővuru formu ve taahhütnemelerde SUE dokümanına atıfta bulunurlar. Kurumsal Őifreleme Sertifikası sahibi kurumlar ilgili sözleőme veya baővuru formu ve taahhütnemesini 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 oluşur. Kayıt iőlemleri sertifika verilecek kurumların baővurularını, kurum bilgileri ve ilgili resmi 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 Açık 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 hazırlanmıőt olup, doküman içeriėinde belirtilen bir kısım alt baőlıkların altındaki "Düzenlenmesine gerek duyulmamıőtır" ibaresi, bu aőamada ihtiyaç duyulmadıėından düzenleme yapılmadıėını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kurumsal Őifreleme Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 03

Yayın Tarihi: 07.01.2022

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. Kamu SM ESHS faaliyetlerinin tümü Kamu SM personeli tarafından yürütölmektedir.

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 yürütölmektedir. 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 tarafından üretilen sertifikanın üzerinde kurum adları bulunan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan tüzel kişilerdir.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kurum bilgileri ve açık anahtar arasındaki bağı 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. Kurum

Kamu SM'den Kurumsal Őifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Őifreleme Sertifikası almaya yetkisi olan tüzeli kiőiliktir. Kurum sözleşme veya başvuru formu ve taahhünamesine uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur.

1.3.5.2. Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusu

Sertifika başvurusunda bulunan kurum tarafından yetkilendirilen ve Kurumsal Őifreleme Sertifikası başvurusu sırasında kurumların bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan kiői/kiőilerdir. Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusu Kamu SM tarafından kendisine imzalatılan taahhünamedeki şartları yerine getirmekten sorumludur.

Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusu, Kurumsal Őifreleme Sertifikasını kullanmaya yetkili olmak zorunda değildir. Kurumsal Őifreleme Sertifikasını kullanmaya yetkili kiői/kiőilerin belirlenmesi kurum inisiyatifindedir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı Başbakanlık Genelgesi ile elektronik ortamda iletilen resmi yazıların Őifreli Őekilde gönderilebilmesine imkan sağlanmıştır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla e-Yazışma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

Kamu kurum ve kuruluşları adına üretilen Kurumsal Őifreleme Sertifikalarında bulunan açık anahtar, gönderici kurumların Őifreli paket oluşturabilmesi; sertifika sahibi kurumun himayesinde bulunan özel anahtar ise kendisine gönderilen Őifreli paketlerin açılabilmesi amacıyla kullanılır. Kurumsal Őifreleme Sertifikaları elektronik imzalama için kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Őifreleme Sertifikası Bölüm 1.4.1'de belirtilen amaçlar dışında kullanılamaz. Belirtilen kapsam dışında kullanımdan doğan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, ürettiđi sertifikaların hangi uygulamalarda ne amaçlar doğrultusunda kullanıldığının kontrolünü yapmakla yükümlü değildir.

1.5. Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

SUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüđü durumlarda SUE dokümanında deđişiklik yapabilir.

1.5.2. İletişim Bilgileri

Bu SUE dokümanının uygulanması ve ilgili yönetim ilkeleri hakkındaki sorular Kamu SM'nin aőađdaki erişim noktalarına yönlendirilebilir:

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

Tel. : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

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

Kamu SM, SUE dokŪmanını herkesin eriŐimine aŐık bulunan aŐaŐıdaki 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

1.5.3. Sertifika Uygulama Esaslarının İlkelere UygunluĐunu Belirleyen KiŐi

Bu SUE dokŪmanının uygunluĐu Kamu SM yoneti mi ve yoneti m tarafından yetki verilen kiŐiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay ProsedŪrleri

Bu SUE dokŪmanının yayımlanma onayı, Kamu SM yoneti mi ve yoneti m tarafından yetki verilen kiŐiler tarafından gerŐekleŐtirilen incelemelerden sonra verilir.

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

AŐık Anahtar: İlgili özel anahtarın sahibinin herkes ile paylaŐılabildiĐi, özel anahtarı ile oluŐturduĐu dijital imzaların doĐrulanmasında ve/veya kendisine Őifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileŐeni.

Akıllı Kart veya HSM EriŐim Verisi: Sertifika sahibine ait Özel Anahtara eriŐimin kontrolŪnŪ saĐlayan PIN ve PUK bilgisi.

Akıllı Kart: Sertifika ve sertifika ile iliŐkili özel anahtarın iŐinde bulunduĐu gŪvenli donanım.

Anahtar Çifti: Özel anahtar ve onunla iliŐkili olan aŐık anahtar.

Bilgi Deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve diĐer sertifika iŐlemleri ile ilgili bilgilerin yayımlandıĐı dizin sunucular gibi veri saklama ortamları.

ŐİSDUP (Çevrim İŐi Sertifika Durum ProtokolŪ): ŪçŪncŪ kiŐilerin sertifika iptal listesine alternatif olarak sertifika geŐerlilik kontrol talebini yapıp, sertifikanın iptal durumunu Ųğrenmelerine imkan tanıyan standart iletiŐim kuralı.

DETSİS (Devlet TeŐkilatı Merkezi Kayıt Sistemi): TŪrkiye Cumhuriyeti Devlet yapısındaki tŪm kurum ve kuruluŐların ve alt birimlerin tekil ve deĐiŐmez nitelikte numaralar ile elektronik ortamda kodlanarak tanımlandıĐı sistem.

EYP (e-YaŐıŐma Projesi): Kamu kurum ve kuruluŐları arasındaki resmi yaŐıŐmaların elektronik ortamda yŪrŪtŪlmesini amaŐlayan proje.

HSM (Hardware Security Module): Sertifikanın kriptografik anahtarlarının iŐinde bulunduĐu harici aĐıt; donanımsal gŪvenlik modŪlŪ.

İmza DoĐrulama Verisi: Elektronik imzayı doĐrulamak iŐin kullanılan Őifreler, kriptografik aŐık anahtarlar gibi veriler.

İmza OluŐturma Verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluŐturma amacıyla kullanılan ve bir eŐi daha olmayan Őifreler, kriptografik özel anahtarlar gibi veriler.

İptal Durum Kaydı: Kullanım süresi dolmamıŐ sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkan veren ve üçüncü kiŐilerin hızlı ve güvenli bir biçimde ulaŐabileceğı kayıt.

Kamu SM (Kamu Sertifikasyon Merkezi): Türkiye Bilimsel ve Teknolojik AraŐtırma Kurumu'na (TÜBİTAK) bağılı BiliŐim ve Bilgi Güvenliğı İleri Teknolojiler AraŐtırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sağılamak üzere oluŐturulan birim.

KAYSİS (Elektronik Kamu Bilgi Yönetim Sistemi): Kamu kurum ve kuruluşlarının teŐkilat yapısının tanımlanmasından, sunulan hizmetlere; hizmetlerde kullanılan belgelerden, kurumların iletiŐim ve yönetici bilgilerine kadar kamu yönetiminde yer alan unsurların mevzuat dayanaklarıyla birlikte tespit edilerek elektronik ortamda tanımlandığı, geliŐtirilen Dijital Türkiye (e-Devlet) uygulamalarının birbirine tek merkezden entegre edilmesini sağılayacak bilgi yönetim sistem.

KEP (Kayıtlı Elektronik Posta): E-postanın gönderim ve alımına dair kanıtların oluŐturulup saklandığı e-posta iletim hizmeti.

Kök Sertifika Hizmet Sağılayıcısı: Kamu Sertifikasyon Merkezi içinde oluŐturulmuŐ, en yetkili imza derecesi verilmiŐ ve sertifikasını kendisi imzalamıŐ olan Sertifika Hizmet Sağılayıcısı.

Kurum Doküman Dođrulama Sistemi: Elektronik ortamda hazırlanan belgelerin dođrulaması iŐleminde kullanılacak kuruma ait sistem veya e-Devlet belge dođrulama sistemidir.

Kurum HSM Cihaz Sorumlusu: Kamu SM ile kurum arasında HSM cihazına anahtar çifti ve sertifika yükleme ile ilgili süreci yürütecek kiŐidir.

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

Kurumsal Őifreleme SHS (Kurumsal Őifreleme Sertifika Hizmet Sağılayıcısı): Kamu Sertifikasyon Merkezi içinde oluŐturulmuŐ, Kök Sertifika Hizmet Sağılayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluŐturup imzalamakla yetkili kılınmıŐ Elektronik Sertifika Hizmet Sağılayıcısı.

Kurumsal Őifreleme Sertifikası Asıl Sorumlusu: Kamu kurumlarının baŐvuru formu ve taahhütname ile Kamu SM'ye bildirdiğı ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde kurumu temsile asıl yetkili kiŐi.

Kurumsal Őifreleme Sertifikası Yedek Sorumlusu: Kamu kurumlarının baŐvuru formu ve taahhütname ile Kamu SM'ye bildirdiğı ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde asıl yetkilinin bulunmaması durumunda kurumu temsile yetkili kiŐi.

Kurumsal Őifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla kullanılan ağık anahtarı iğeren elektronik sertifika.

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

Özel Anahtar: Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluŐturmak ve/veya ilgili Ağık Anahtarla ŐifrelenmiŐ elektronik kayıtların, dosyaların Őifresini çözmek için kullanılan anahtar.

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

Sertifika Sahibi: Kurumsal Őifreleme Sertifikası baŐurusunda bulunan ve sertifikayı kullanma yetkisine sahip tuzel kiŐi.

Sertifika Suresi: Uretim anında sertifikanın iŐine yazılan, sertifikanın geŐerlilik baŐlangiŐ ve bitiŐ tarihleri arasında kalan sure.

Si ve SUE (Sertifika İlkeleri ve Uygulama Esasları): Kamu SM resmi web sitesi Bilgi Deposu menusu altındaki ilke ve Uygulama Esasları'nda Elektronik Sertifika Hizmet SaĐlayıcısı'nın (ESHS) iŐleyiŐi ile ilgili genel kuralları ve bu kuralların nasıl uygulanacaĐını detaylı olarak anlatan belgeler.

UŐuncu KiŐiler: Sertifikalara guvenerek iŐlem yapan gercek veya tuzel kiŐiler.

Zaman Damgası: Bir elektronik verinin, uretildiĐi, deĐiŐtirildiĐi, gonderildiĐi, alindiĐi ve/veya kaydedildiĐi zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doĐrulan kayıt.

1.6.2. Kısaltmalar

BGYS: Bilgi GuvenliĐi Yonetim Sistemi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN ŐalıŐtay Kararı

ŐİSDUP (OCSP): Çevrim İŐi Sertifika Durum Protokolü (Online Certificate Status Protocol)

EAL (Evaluation Assurance Level): DeĐerlendirme Garanti Duzeyi

ECDSA (Elliptical Curve Digital Signature Algorithm): Eliptik EĐrisi Sayisal İmza Algoritması

ESHS: Elektronik Sertifika Hizmet SaĐlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Ozellikleri

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

IETF RFC (Internet Engineering Task Force Request for Comments): İnternet MühendisliĐi Gove Grubu Yorum Talebi

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon BirliĐi

Kamu SM: Kamu Sertifikasyon Merkezi

PKI (Public Key Infrastructure): AŐık Anahtar Altyapısı

RSA: Rivest Shamir Adleman (Algoritmayı bulan kiŐilerin baŐ harfleri)

SHA (Secure Hash Algorithm): Guvenli Ozet Algoritması

Si: Sertifika İlkeleri

SiL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayınlama ve Bilgi Deposu Yüklümlükleri

Bilgi deposu, Kamu SM'nin ürettiđi sertifikaları, iptal durum kayıtlarını, Sİ ve SUE gibi ilgili dokümanları sertifika sahibi kurumların ve üçüncü kişilerin ulaşabileceđi şekilde kesintisiz, güvenli ve ücretsiz olarak yayınladığı 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, Kamu SM Taahhütnamesi, Sİ ve SUE dokümanları, sertifika hizmetleri ile ilgili yönergeler, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması

Kamu SM'nin sistem bileşenlerinin erişimine açacağı bilgi deposunda sistemin iç işleyişi ile ilgili olanlar hariç olmak üzere aşağıdaki bilgiler bulunur:

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

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ ve SUE dokümanları içeriğinin deđişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip derhal yayımlanır.

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

2.4. Erişim 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 yükümlülükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve deđiştirilmeye 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 Şifreleme Sertifikası ile ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kurumun kimlik tanımlama veya doğrulanması yapılır. Bu bölümde Kurumsal Şifreleme Sertifikası yönetim prosedürleri içinde uygulanan kurum kimlik tanımlama ve doğrulama yöntemleri ile Kurumsal Şifreleme Sertifikası içinde yazılan kurum bilgileri anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kurumsal Şifreleme Sertifikalarında Kamu SM ve sertifika sahibi kurumlara ait bilgilerin belirtildiği DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Kurumsal Şifreleme Sertifikaları içeriğindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimliğinin tespit edilmesini sağlayan niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Kurumsal Şifreleme Sertifikası içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Kurumsal Şifreleme Sertifikası içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kurumsal Şifreleme Sertifikası içeriğindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum için ayırt edici niteliktedir. Aynı kuruma ait Kurumsal Şifreleme Sertifikaları içeriğindeki kurum bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kurumlara ait Kurumsal Şifreleme Sertifikaları içeriğindeki kurum bilgilerinin aynı olması engellenmektedir. Bunun sağlanabilmesi için Kurumsal Şifreleme Sertifikalarının isim alanı içinde benzersiz bir sayı olduğu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

3.1.6. Markanın Tanınması, Doğrulması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM Kurumsal Şifreleme Sertifikası hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kurumun doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

Sertifika sahibine ait açık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir ve Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusuna teslim edilir. Asıl veya Yedek Sorumlu tarafından Kurumsal Şifreleme Sertifikasının

teslim alındığı teyit edilir. Ek olarak, HSM'ye yüklenmesi talep edilen sertifikalar için Kurum HSM Cihaz Sorumlusu tarafından imzalanan teslim tutanağı ile teyit işlemi yapılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Kurumsal Őifreleme Sertifikası başvurusunda bulunan kurumlar, talep edilen kurum bilgilerini, Kamu SM tarafından sunulan başvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, kurum tarafından iletilen bilgilere istinaden kurum kimliğini belirler. Kurumların sertifika alma yetkisi DETSİS aracılığıyla kontrol edilir. Başvuru esnasında sertifika işlemlerini kurum adına yürütecek Kurumsal Őifreleme Sertifikası Sorumluları da belirlenerek Kamu SM'ye iletilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Kurumsal Őifreleme Sertifikası, kurum adına üretildiğinden yalnızca kurumsal başvuru kabul edilmektedir. Başvuru formu ve taahhütnamelerde yer alan kişisel bilgilerin doğruluğu kurumun sorumluluğundadır.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika sorumluları tarafından başvuru sırasında ve daha sonra değışiklik sebebiyle beyan edilen aŐağıdaki erişim bilgileri ve diđer bilgilerin doğruluğu Kamu SM tarafından kontrol edilmez:

- Telefon numaraları
- Kurumsal Őifreleme Sertifikası tesliminde kullanılacak adres bilgisi
- Elektronik posta adresleri
- Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun unvanı veya görevi ile ilgili bilgiler
- Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun çalıştığı kurum ile ilgili bilgiler
- Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun çalıştığı birim ile ilgili bilgiler

Bu bilgilerin doğruluğu kurumun beyanı üzerine kabul edilir.

Kurum bu bilgileri Kamu SM'ye doğru beyan etmekle yükümlüdür. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doğabilecek zararlardan, sertifikanın hatalı üretilmesinden ve sertifika yönetim sürecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin Doğrulanması

Sertifika içeriğine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.4. Sertifika İptal İsteęinde Kimlik Doğrulama

Sertifika sahibi kurumun yetkilendirdięi sertifika sorumluları Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. Online İşlemler adresine ulaşamaması durumunda Kamu SM'ye Elektronik Mühür/Kurumsal Şifreleme Sertifikası İptal Başvuru Formu resmi yazısı ile birlikte gönderilerek iptal işlemi gerçekleştirilebilir. Elektronik Mühür/Kurumsal Şifreleme Sertifikası İptal Başvuru Formu ile yapılan iptal başvurularında kurumdan gelen evraklar doğrulanır ve sertifika sorumlusu bilgileri kontrol edilir. Üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulaması gerçekleştirir. Ayrıca Elektronik Mühür/Kurumsal Şifreleme Sertifika Sorumlusu telefon ile aranarak kimlik doğrulama gerçekleştirilir ve iptal talebi teyit edilir.

4. İşlemsel Gereklere

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

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

Süreçler sertifika sahibi kurumlar ile kurum tarafından yetkilendirilen sertifika sorumluları ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildięi

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

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

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Şifreleme Sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacağı sertifika hizmetlerinin şartları TÜBİTAK BİLGEM ile karşılıklı imzalanan sözleşmeler ve/veya kurumun imzaladığı Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesi, Kamu SM'nin internet üzerinden yayımladığı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

Kurum, Kamu SM web sitesinde yayımlanan Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesini doldurur. Ardından üst yazısıyla birlikte Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesi eki de imzaya dahil olacak şekilde EYP dosyası oluşturularak e-posta veya KEP üzerinden Kamu SM'ye iletir. Kurum, Kurumsal Şifreleme Sertifikasını HSM içerisinde kullanmayı tercih ederse HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve

Taahhütnameyi 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 gereğince; kamu kurum ve kuruluşlarınca resmi yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu kapsamda, zorunlu haller veya olağanüstü durumlar dışında EYP dosyası ile başvuru dışında başvurular kabul edilmeyecektir. Zorunlu hallerde veya olağanüstü durumlarda resmi yazışmalar, KEP veya kurumsal e-posta yoluyla iletilen ilgili başvuru formu ve taahhünamelerin doğrulanmasının ardından ıslak imzalı ve mühürlü olacak şekilde üst yazısıyla birlikte Kamu SM'ye posta yoluyla iletilir. Kurumsal Şifreleme Sertifikası başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kurum başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kurum, Kamu SM'ye göndermiş olduğu bilgilerin doğruluğunu takip etmekle ve bu bilgilerde değişiklik olması halinde belirlenmiş araç ve yöntemler ile Kamu SM'yi bilgilendirmekle yükümlüdür. Kamu SM, Kurumsal Şifreleme Sertifikası içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Kamu SM, sertifika verilecek kurumların kimlik tanımlama ve doğrulama işlemlerini yaptıktan sonra başvurularını değerlendirir ve uygun görülen başvuruları onaylayarak işleme alır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve doğrulama işlevleri yerine getirilir. Kurumsal Şifreleme Sertifikası başvurusunda bulunan kurumların Kamu SM'ye gönderdiği bilgi ve belgeler aşağıda sıralanmıştır:

- Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnameyi
- Kurum tarafından yazılan resmi yazı
- HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnameyi

Kurumdan gönderilen belgelerin doğrulanması için aşağıdaki kontroller yapılır:

- Kurum tarafından gönderilen EYP dosyası kontrol edilerek üst yazı ve eklerinin e-imza doğrulanması yapılır.
- EYP dosyası içerisinde üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulanması gerçekleştirilir.
- Başvuru evraklarında yer alan kurum DETSİS numarası, DETSİS üzerinden sağlanan servis aracılığıyla kontrol edilerek kurumun Kurumsal Şifreleme Sertifikası almaya yetkili olup olmadığı sorgulanır.
- Kurum tarafından gönderilen Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnameyi yer alan kurumun adı, vergi kimlik numarası, yetkilendirilen Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusunun T.C. kimlik numarası, ad, soyad, kurumsal e-

posta adresi, kurum birimi ve sertifika üretim nedeni bilgilerinde eksiklik olup olmadığı kontrol edilir.

- Belgelerin elektronik ortamdan iletimi mümkün olmadığı durumda kurumdan evrak asılları talep edilir. Evrak asılları ulaşan kurumların başvurularını doğrulamak için, KEP ile gönderilen evraklar ile evrakların asılları karşılaştırılarak birbirinin aynı olduğu doğrulanır. KEP kullanmayan kurum başvurularını doğrulayabilmek için kuruma iki seçenek sunulur; resmi olarak sahibi oldukları web sitelerinin belirlenen dosya yoluna elektronik ortamda ilettikleri başvuru evraklarının özet değeri eklenmeli veya başvuru formunda kurum onayını veren üst düzey yetkili ses kaydı alabilen telefon ile aranarak doğrulama onayı alınmalıdır.

Bilgi ve belgeler hatasız ve tam ise kurum kimlik tanımlama ve doğrulama işlemi tamamlanır. Belgelere gözle görülen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kurum kimlik tanımlaması ve doğrulaması 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

Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 29.05.2019 tarihli ve 2019/DK-BTD/160 sayılı Kurul Kararı ile "Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar" yayımlanmıştır. İlgili Karar ikinci bölüm, 5'inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS'te bilgileri bulunmayan veya Kurumsal Şifreleme Sertifikası almaya yetkisi olmayan tarafların başvurusunu reddeder.

Buna ek olarak, Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, başvuru sırasında beyan edilen belgelere tahrifat, hata, eksik onay, eksik veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyen kurumlarla ilgili yazılı bilgilendirme, Kurumsal Şifreleme Sertifikası Sorumlularının başvuru sırasında beyan ettikleri e-posta adresleri aracılığı ile yapılır ve gerekli görülen 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 İşlenme Zamanı

Başvuru evraklarının eksiksiz bir şekilde Kamu SM'ye ulaşması ve doğrulanması ardından en fazla 15 (on beş) iş günü içerisinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

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

Kurumsal Şifreleme Sertifikası, kayıp veya arıza gibi durumlarda kurumun işlemlerinde aksaklık yaşanmaması amacıyla biri yedek olmak üzere 2 adet üretilir.

4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta yüklenen sertifika, sertifika sorumlusuna teslim edildiğinde Kurumsal Őifreleme Sertifikasının oluŐturulduđu konusunda bilgilendirilmiŐ olur.

HSM cihazına sertifika yükleme iŐlemi, Kurum HSM Cihaz Sorumlusu gözetiminde gerçekteŐirilir. İŐlem sonrasında teslim tutanađı imzalanır ve Kurumsal Őifreleme Sertifikasının oluŐturulduđu konusunda bilgilendirilmiŐ olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul KoŐulu

Akıllı karta basılan Kurumsal Őifreleme Sertifikası anlaşmalı kurye ile kurum adresine gönderilir ve Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilen Asıl Sorumluya teslim edilir. Teslimat, gerekli hallerde Asıl Sorumlunun bilgi vermesi durumunda Yedek Sorumluya yapılabilecektir. 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 yerleŐkesine gidip HSM cihazına anahtar üretimi ve sertifika yükleme iŐlemlerini yerinde gerçekteŐirdiđi süreçlerdir. Uzaktan yükleme, Kamu SM ve kurum arasında yapılan güvenli uzak bađlantı sonrası Kamu SM personelinin HSM cihazına anahtar üretimi ve sertifika yükleme iŐlemlerini uzaktan gerçekteŐirdiđi süreçlerdir. Her iki süreç de ilk başvuruda HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhütnamesinde belirtilen Kurum HSM Cihaz Sorumlusu gözetiminde gerçekteŐirilmektedir.

Asıl veya Yedek Sorumlu, sertifikanın içeriđini kontrol eder, herhangi bir eksiklik veya hata olması durumunda 5 (beŐ) iŐ günü içerisinde Kamu SM'yi bilgilendirir, aksi halde sertifikayı kabul etmiŐ sayılır.

4.4.2. Sertifikanın EŐHS Tarafından Yayımlanması

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

4.4.3. Sertifikanın OluŐturulmasının Diđer Taraplara Duyurulması

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

4.5. Sertifikanın ve Özel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait özel anahtarını, tabi olunan standartlar, Sİ ve SUE dokümanında ve ilgili sertifika sahibi taahhütnamesinde yer alan koŐullar ve belirlenmiŐ sınırlar içinde kullanmalıdır.

Sertifika sahibi, özel anahtarı yetkisiz kiŐilerin eriŐimine karŐı korumakla yükümlüdür. Kurumsal Őifreleme Sertifikasına karŐılık gelen özel anahtar yalnızca sertifikada "Anahtar Kullanımı" alanında belirtilen amaçlar dahilinde kullanılabilir.

4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifika sahibine ait Kurumsal Şifreleme Sertifikasının içinde yer alan açık anahtar, üçüncü kişilerce EYP 2.0 kapsamında verilerin şifreli iletimi amacıyla kullanılır. Açık anahtarın veya sertifikanın, belirtilen amaç dışında kullanılması sonucu oluşabilecek zararlardan üçüncü kişiler sorumludur.

4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, kullanım süresi dolan sertifikalarda, sertifikada yer alan bilgiler değişmeden 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 Sertifikasının 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 değişikliği gerekmesi

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

DETSİS'te bilgileri bulunan ve DETSİS tarafından Kurumsal Şifreleme Sertifikası alma yetkisi olduğu belirtilen 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 2 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 her iki sertifika sorumlusu tarafından elektronik imzalanmış bir şekilde (BES formatında ve .p7s uzantılı olarak), bilgi@kamusm.gov.tr veya kurumsal_bilgi@kamusm.gov.tr e-posta adresine iletilir. Kurum tarafından HSM kullanılacaksa başvuru listesi içerisindeki "HSM Bilgileri" de kurum tarafından doldurulmalı ve liste Kurum 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 dođrulama yapılamaz. Bařvuru evraklarının, tanımlanan yöntemler dıŐında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

Bařvurusu kabul edilen kurumların sertifika yenileme süreci bařlatılır.

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 Tarafra Duyurulması

Bölüm 4.4.3'te tanımlanmaktadır.

4.8. Sertifikada Bilgi DeđiŐikliđi

Sertifikada bilgi deđiŐikliđi, anahtar çifti hariç sertifikada yer alan bilgilerin deđiŐmesi olarak tanımlanmaktadır. Sertifika içeriđinde kurum KAYSİS unvanı ve DETSİS numarası yer alır. Sertifika içeriđinde yer alan bilgilerde deđiŐiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi deđiŐikliđinin gerekli olduđu durumlarda, kurum Bölüm 4.7'de belirtilen sertifika yenileme sürecini iŐletmelidir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiđi Durumlar

Sertifikanın kullanım süresi dolmadan geçerliliđini yitirdiđi durumlarda, sertifika iptal edilir. İptal edilen sertifikayla bir daha iŐlem yapılamaz. Sertifika, aŐađıda belirtilen durumlarda iptal edilir:

- Sertifika sahibi kurumun talebi
- Sertifika içeriđindeki bilgilerin sahteliđinin veya yanlışlıđının ortaya çıkması veya bilgilerin deđiŐmesi
- Sertifika sahibi kurumun kapanması
- Sertifika sahibi kurumun KAYSİS unvanının deđiŐmesi
- Sertifika sahibi kurumun DETSİS numarasının deđiŐmesi
- Özel anahtarın güvenliđinin kaybedildiđinden Őüphelenilmesi
- Özel anahtarın içinde bulunduđu aracın kaybolması, çalınması veya bozulması
- Akıllı kart veya HSM eriŐim verisinin unutulması veya kaybedilmesi
- Sertifikanın Elektronik Mühür/Kurumsal Őifreleme Sertifikası Bařvuru Formu ve Taahhütnamesi, kurum ile imzalanan sözleşmeler veya SUE dokümanında belirtilen Őartlara aykırı kullanımının tespit edilmesi
- Kamu SM'ye evrakları gönderen sertifika sorumlularının kurumun onayını almadıđının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM'ye bildirilmesi
- Kamu SM'nin Kurumsal Őifreleme Sertifikasını imzalamak için kullandıđı imza oluŐturma verisinin bütünlüđünün bozulması veya gizliliđinin ortadan kalkması

- Kamu SM'nin iŐleyiŐine son verilmesi ve verilen Kurumsal Őifreleme Sertifikalarının yonetim iŐlemlerinin baŐka bir ESHS tarafından devamlılıĐının saĐlanamaması

4.9.2. Sertifika İptal BaŐvurusunu Kimler Yapabilir

Sertifika iptal baŐvurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiŐ Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılabilir. Kamu SM, Bolum 4.9.1'de tanımlanan tum durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal BaŐvurusunun İŐlenmesi

Kurumsal Őifreleme Sertifikası iptal iŐlemi, kurum tarafından yetkilendirilen Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından Kamu SM resmi internet sitesinde yer alan Online İŐlemler menüsü aracılıĐı ile yapılır.

Kamu SM Online İŐlemler üzerinden yapılan iptal baŐvurusunda, Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu sisteme kimlik doĐrulamasıyla giriŐ yaparak iptal talebinde bulunur. İlgili talebin ardından, Kurumsal Őifreleme Sertifikası Kamu SM sisteminde otomatik olarak iptal edilir.

İptal iŐlemlerinin Kamu SM Online İŐlemler üzerinden yapılamadıĐı durumda Elektronik Mühür/Kurumsal Őifreleme Sertifikası İptal BaŐvuru Formu, Elektronik Mühür/Kurumsal Őifreleme Sertifikası Sorumlusu tarafından doldurularak iletilmelidir. Sorumluya ait bilgilerde deĐiŐiklik olması durumunda Kurum Sertifika Sorumlusu Yetkilendirme/Bilgi Guncelleme Formu ve Taahhütnamesi de eksiksiz bir Őekilde doldurulmalıdır. Formlar üst yazısıyla birlikte sorumluya ait kurumsal e-posta üzerinden Kamu SM'ye gönderilir. Formun ıslak imzalı ve mühürlü aslının da üst yazısıyla birlikte mutlaka Kamu SM'nin Gebze adresine posta yoluyla acil olarak iletilmesi gerekmektedir. Kurumdan e-posta ile gelen evraklarda yer alan bilgiler kontrol edilerek üst yazıda yer alan belge doĐrulama kodu ile Kurum Doküman DoĐrulama Sistemi üzerinden kurum doĐrulaması gerçekleştirilir. İptal sürecinin baŐlatılmasının ardından evrak asılları Kamu SM'ye ulaŐana kadar kurum yazıŐmalarında yaŐanabilecek aksaklıkların en aza indirgenmesi amacıyla Kurumsal Őifreleme Sertifikası Sorumlusu telefon ile aranarak iptal talebi teyit edilir ve iptali talep edilen sertifika askıya alınarak varsa yedek sertifika devreye alınır. Evrak asıllarının ulaŐmasının ardından Kamu SM'ye e-posta üzerinden gönderilen evraklar ile asılları karŐılaŐtırılır ve askıya alınan sertifika iptal edilir.

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

İptal süreci, Kamu SM resmi web sitesinde ayrıntılı olarak anlatılmaktadır. Kamu SM, internet sitesi üzerinden iptal iŐleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar.

Kamu SM iptal bilgilerini en kısa zamanda iŐler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en azından Kurumsal Őifreleme Sertifikasının seri numarası ile Kamu SM'nin elektronik imzasını taŐır. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da Kurumsal Őifreleme Sertifikasının durumunu iptal konumuna getirmek suretiyle duyurur. İptal edilen sertifika bilgisi Kamu SM tarafından DETSİS'ten kaldırılır.

SİL dosyası, Kamu SM'ye ait imza oluŐturma verisi ile imzalanır. İptal edilen Kurumsal Őifreleme Sertifikaları geŐerlilik süresinin sonuna kadar SİL içinde tutulur. GeŐerlilik süresi dolduktan sonra Kurumsal Őifreleme Sertifikası SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı'da geŐerlilik süresi dolan iptal edilmiŐ Kurumsal Őifreleme Sertifikalarının durumu iptal edilmiŐ olarak görünmeye devam eder.

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

4.9.4. İptal İsteęi Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteęinin 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 Gereklilięi

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 süreklilięini sağlar.

Üçüncü kişiler Kurumsal Őifreleme Sertifikasına dayanarak işlem yapmadan önce Kurumsal Őifreleme Sertifikasının geçerlilięini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

Üçüncü kişiler Kurumsal Őifreleme Sertifikası geçerlilik kontrolünü yaptığı SİL dosyasının veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının Kamu SM'ye ait imza oluřturma verisiyle imzalandıęını kontrol eder. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri Bölüm 9.6.4'te belirtilmiştir.

4.9.7. Sertifika İptal Listesi Yayımlama Sıklıęı

Sertifika sahiplerine ait iptal bilgisinin bulunduęu 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 Őifreleme Sertifikası iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerlilięini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduęu 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, belirtilen yayımlama zamanından en geç 5 (beş) dakika sonra yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, Kurumsal Őifreleme Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduęu duyurulan imza oluřturma verisiyle imzalanır.

ÇİSDUP desteęi olan uygulamalar Kurumsal Őifreleme Sertifikalarının geçerlilik durum kontrolünü ESHS Eriřim Bilgisi isimli sertifika uzantısında (Authority Information Access) 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 sağladıęı için, SİL yanında çevrim içi sertifika iptal durum kaydı desteęini de vermektedir.

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

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. Özel Anahtarın Güvenliğini Yitirmesi Durumu

Sertifika sahibi kuruma ait özel anahtarın güvenliğini yitirmesi durumunda Kurumsal Őifreleme Sertifikası iptal edilir. Kurum Őifreleme Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Kurumsal Őifreleme Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sağlamak amacıyla askıya alınabilir.

Kurumsal Őifreleme Sertifikaları biri yedek olmak üzere 2 adet üretilir. Sertifikalar akıllı kart içerisinde kullanılıyorsa askı durumunda kuruma gönderilir. Kullanılacak sertifika, kurumun sertifika sorumlusu tarafından Kamu SM Online İşlemler üzerinden askıdan indirilir. Aynı anda sertifikalardan sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

İlk başvuruda talep edilen sertifika HSM içerisinde kullanılıyorsa asıl sertifika geçerli; yedek sertifika askıda olacak şekilde yükleme gerçekleştirilir. Asıl sertifikanın yüklemesi geçerli yapıldığından, kurumun sertifika asıl veya yedek sorumlusu tarafından Kamu SM Online İşlemler üzerinden askıdan indirilmesine ihtiyaç bulunmamaktadır.

Kurum sertifika yenileme talebinde bulunduysa, yeni üretilen sertifikanın geçerlilik tarihi kurumun daha önce edinmiş olduğu sertifikanın bitiş tarihinde başlayacak şekilde üretilir. Bu sebeple, sertifikalar askıda üretilir (HSM cihazına askıda olmak üzere yüklenir) ve geçerlilik süreleri başladığında askıdan indirilerek kullanılabilir hale gelir.

Sertifika sahibi kurum veya kurumun yetkilendirdiği Asıl veya Yedek Sertifika Sorumlusu, aşağıda belirtilenlere benzer sebeplerden dolayı Kurumsal Őifreleme Sertifikasını askıya alabilir:

- Sertifika sahibi kurumun Kurumsal Őifreleme Sertifikasını kullanım dışı bırakmak istemesi
- Kurumsal Őifreleme Sertifikasının iptal sebebinin ortaya çıktığından şüphelenildiği durumlarda, yanlışlıkla iptalini engellemek amacıyla, Kurumsal Őifreleme Sertifikasının önce askıya alınmak istenmesi
- Aktif kullanılan geçerli sertifikanın kayıp/çalıntı/arıza durumunda yedek sertifikanın kullanıma açılabilmesi

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Kurumsal Őifreleme Sertifikasının askıya alma başvurusu, sadece sertifika sahibi kurum veya kurumun yetkilendirdiği Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılır.

4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi

Kurumsal Őifreleme Sertifikası askı baŐvurusu, Kamu SM web sitesinde yer alan Online İŐlemler menüsünden veya Online İŐlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Askı baŐvurusu alındığında öncelikle baŐvuruyu yapan sertifika sahibi kurumun ve yetkililerinin kimlik belirlemesi ve dođrulaması yapılır. Kimlik dođrulaması yapılamayan askı baŐvuruları işleme alınmaz.

Askıya alınan Kurumsal Őifreleme Sertifikası için, SİL'de geçici olarak iptal edildiđini belirten sebep kodu kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, Kurumsal Őifreleme Sertifikası askıya alındıktan sonra, gerekli gördüđü durumlarda sertifika sahibi kurumu ve bađlı bulunduđu kurum tarafından yetkilendirilen sorumluları sertifikanın askıya alındıđına dair bilgilendirir.

Sertifika sorumluları, Kamu SM Online İŐlemler üzerinden 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 Kök 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 12 (on iki) saat süresince askıdan indirilemez.

4.10. Sertifika Durum Servisleri

Üçüncü kişiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılıđıyla 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 desteđi 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 Őifreleme Sertifikalarının geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin Erişilebilirliđi

SİL ve ÇİSDUP servislerinin verildiđi sistemlere erişimin kesintisiz olarak sağlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rağmen erişimin bir süreliđine 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 dođan zararlardan Kamu SM sorumlu tutulamaz.

4.10.3. İsteđe Bađlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliđinin Sona Ermesi

Kurumsal Őifreleme Sertifikasının kullanım sũresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliđi sona erer. Kamu SM, Kurumsal Őifreleme Sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibi kurumu ve Kurumsal Őifreleme Sertifikası Asıl ve/veya Yedek Sorumlularını bilgilendirir. Kamu SM, Kurumsal Őifreleme Sertifikalarının sũresi dolmadan en az 15 (on beŐ) gũn nce sertifika sahibi kurumu bilgilendirir.

4.12. Anahtar Yeniden Őretim

Sertifika sahiplerine ait anahtarların yeniden retilmesi veya yedeklenmesi iŐlemi uygulanmamaktadır.

5. Ynetim, iŐlemsel ve Fiziksel Kontroller

Bu blmde Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan gũvenlik kontrolleri anlatılmıŐtır.

5.1. Fiziksel Gũvenlik Denetimleri

Kamu SM sisteminin alıŐtıđı cihazların bulunduđu binalar ve odalar, giriŐ ve ıkıŐların kontrol edildiđi yetkisiz kiŐilerin giriŐini engelleyen gũvenlik nlemleri ile donatılmıŐtır. Gũvenli alanlara eriŐimlerin kaydı tutulmaktadır.

5.1.1. Tesis Yeri ve İnaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yũrũtũlmektedir. Kamu SM sisteminin alıŐtıđı binanın bulunduđu Gebze tesisi, yerleŐim merkezinden uzak, yangın, su baskını, deprem, yıldıırım ve hava kirliliđinden en az etkilenecek, giriŐ ve ıkıŐların kontrol edildiđi bir blgedir. Alanlara ve binalara eriŐim, tek kiŐinin giriŐine veya ıkıŐına izin veren HI-SEC kilitleme kapıları dahil olmak ũzere fiziki gũvenlik, video izleme ve kimlik dođrulama olmak ũzere oklu gũvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrolũ bulunan bir alandır. Yetkisiz personel ve kayıtsız ziyaretiler bu hassas alanlara giremez.

Bina, yũksek gũvenlik gerektiren iŐlerin yapılmasına imkan 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 gũ birimleri, haberleŐme ũniteleri, yedekli iklimlendirme ũniteleri, havalandırıcılar, yangın sndũrũcũ sistemler mevcut olup, deprem, su ve afetlere karŐı gerekli tedbirler alınmıŐtır.

5.1.2. Fiziksel EriŐim

Kamu SM yazılım ve donanım modũlleri ile arŐivlere eriŐim denetim altındadır. Binaya giriŐler gũvenlik grevlilerinin kontrolũ altında, geliŐmiŐ eriŐim kontrol cihazlarıyla sađlanmaktadır.

Bina iinde Kamu SM sistemine ait yazılım ve donanım aralarının bulunduđu, elektronik veya kađıt ortamdaki bilgilerin tutulduđu, sistemin iŐletildiđi ve ynetildiđi odalara eriŐim geliŐmiŐ eriŐim kontrol cihazlarıyla yapılmaktadır. Gũvenli alanlarda tek kiŐi alıŐma yapamaz, en az biri yetkili olmak ũzere 2 (iki) kiŐi ile alıŐma yapılır. 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 dzenlenir.

5.1.3. Güç Kaynađı ve Havalandırma

AŐađıdaki güç kaynakları Kamu SM işlevlerinin yerine getirilmesi ve sürekliliđin sađlanması için kullanılmaktadır:

- Güç alma ve devşirme (transformatör) birimleri
- Dađıtım paneli
- Trafo
- UPS
- Kuru akü
- Acil jeneratör

Bina aşırı ısınmayı önleyebilecek kapasitede ve uygun nem seviyesini ayarlayabilecek özelliklerde kesintisiz/yedekli iklimlendirme sistemleri ile donatılmıştır.

5.1.4. Su Baskınları

Kamu SM işlevlerinin yerine getirildiđi ortamlarda su baskınlarından en az zarar göreceđ şekilde önlemler alınmıştır.

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kađıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur. Buna ek olarak gerekli görülen 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 kađıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir.

5.1.8. Farklı Mekanlarda Yedekleme

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

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

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Kamu SM'de çalışan personelin rolleri aŐađıda belirtildiđi şekilde sınıflandırılmıştır:

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 bileşenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

Sistem Denetçisi: Sertifika hizmetleriyle ilgili iş ve işlemlerin denetlenmesinden sorumludur.

Sertifika Kayıt Sorumlusu: Sertifika üretim/iptal başvurusunun alınması, başvuru evraklarının ve kurum kimliğinin doğrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleştiren personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Kurumsal Şifreleme SHS'ye ait sertifika üretilmesi ve iptal edilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, Kök SHS ve Kurumsal Şifreleme SHS'ye ait imza oluşturma verilerinin başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

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 ve Sistem Denetçisi 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 giymemiŐ olduĐu araŐtırılır. Adli sicil kayıtları incelenir. Gvenlik soruŐturması biten personel iŐe baŐlatılır. iŐe baŐlayan personelin bilgi gvenliĐi farkındalık eĐitimleri tamamlanmadan, sistemlere eriŐimine izin verilmez.

5.3.3. EĐitim Gerekleri

ÇalıŐanlar, Kamu SM'deki iŐlerine aktif olarak baŐlamadan nce gerekli eĐitimden geçirilirler. ÇalıŐanlara verilen eĐitimde Kamu SM'de uygulanan gvenlik ilkeleri, sistemin teknik ve idari iŐleyiŐi, iŐleriyle ilgili sreçler, sreç içindeki grev ve sorumluluklar anlatılır.

Kamu SM, çalıŐanlarına yılda en az bir defa, siber gvenlik ve sosyal mhendislik saldırılarına karŐı farkındalık oluŐturmak amacıyla, bilgi gvenliĐi eĐitimi vermektedir.

5.3.4. Srekli EĐitim Gerekleri ve SıklıĐı

Kamu SM sisteminde yapılan deĐiŐikliklerin bildirilmesi amacıyla personele verilen eĐitimler gerekli grldkçe tekrarlanır. Yeni greve baŐlayanlar için eĐitimler tekrarlanır.

5.3.5. Grev DeĐiŐim SıklıĐı ve Sırası

Dzenlenmesine gerek duyulmamıŐtır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluŐturması, geçerli olarak oluŐturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluŐturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diĐer yetkisiz eylemlerde ilgili mevzuat gereĐince bilgi gvenliĐi politikaları ihlali ve ihlalin boyutuna gre hukuki soruŐturma ve disiplin sreci baŐlatılır.

5.3.7. AnlaŐmalı Personel Gereksinimleri

Kamu SM verdiĐi hizmetler için dıŐ kaynak kullanmak durumunda kaldıĐında, bu hizmeti saĐlayacak firma personeli ile ilgili gvenlik kontrollerini, firma ile yaptıĐı szleŐme ile belirler.

5.3.8. SaĐlanan Dokmantasyon

ÇalıŐanlara iŐleriyle ve Kamu SM sreçleriyle ilgili gerekli kılavuz ve destek dokmanlar ve bilgi gvenliĐi politikaları kapsamındaki ilgili dokmanlar saĐlanır.

5.4. Denetim Kayıtları

Kamu SM iŐleyiŐi sırasında gerçekteŐtirilen anahtar ve sertifika ynetimi, sistemin gvenliĐi ile ilgili iŐlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diĐer bir kısmı ise kaĐıt zerindedir. Denetimler sırasında gerekli grldĐu takdirde bu kayıtlar grevliler tarafından incelenir.

5.4.1. Kaydedilen iŐlemler

Kamu SM sisteminde aŐaĐıda yapılan iŐlemler ile ilgili elektronik veya kaĐıt ortamda yapılan iŐlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaŐam dngs ynetimi iŐlemleri
 - Anahtar retimi
 - Anahtar yedekleme
 - Anahtar daĐıtımı

- 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 olduđu bilgisi
 - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
 - Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
 - Kağıt 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 işlemler
 - Sisteme başarılı veya başarısız tüm erişim denemeleri
 - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
 - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve deđiştirilmesi
 - Güvenlik profili deđişiklikleri
 - Sistemin çökmesi, donanım hataları ve diđer bozukluklar
 - Güvenlik cihaz/yazılım işlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
 - Kamu SM'ye ziyaretçi giriş ve çıkışı

Kayıtlarda genellikle kayıt zamanı ve kaydın oluşmasına sebep olan çalışanın ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyiőiyle ilgili tutulan kayıtlar düzgün zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluşup oluşmadığı kontrol edilir. Buna ek olarak, sistemde olađandışı hareketlerin görülmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görülen ve başlatılan işlemler de belgelenir.

Sertifika başvurusu sırasında sertifika sahiplerinden gelen bilgilerin elektronik veya kağıt ortamda tutulan kayıtları, sertifika yaşam döngüsü süresi içinde gerek görüldükçe veya yasal işlemler sebebiyle incelenebilir.

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelenmelerinden sonra, en az 2 (iki) ay sistemde tutulur. Ardından arşivlenir. 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 aŐağıdaki önlemler alınmıŐtır:

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

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliėi göz önüne alındıėında her gün düzenli olarak, sistemin yoğun olarak kullanılmadıėı bir saatte gerekli görülen kayıtların çevrim içi yedeėi alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme iŐlemlerini otomatikleŐtirmek için yedekleme yönetim yazılımı mevcuttur. Kritik kayıtlar ayrı bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, aė katmanında ve iŐletim seviyesi düzeyinde otomatik olarak toplanır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan iŐlemi baŐlatan Kamu SM sertifika yönetim sistemi kullanıcısı, kaydın yapıldıėına dair sistem tarafından bilgilendirilir.

5.4.8. Saldırıya Açıklıėın Deėerlendirilmesi

Denetim kayıtlarının tutulduėu sistemler için Bölüm 6.5, 6.6 ve 6.7'de sözü geėen teknik güvenlik kontrolleri uygulanır.

5.5. Kayıt ArŐivleme

5.5.1. ArŐivlenen Kayıt Bilgileri

Bölüm 5.4.1'de belirtilen kayıtlara ek olarak sertifika baŐvurusu ve sertifika yaŐam döngüsüyle ilgili, elektronik olarak ya da kağıt üzerinde tutulan aŐağıdaki belgeler arŐivlenir:

- Sertifika sahibi kurum tarafından, baŐvuru sırasında verilen tüm bilgi ve belgeler
- Sertifika üretimi, yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal baŐvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Sertifika iŐlemleriyle ilgili yapılan önemli yazıŐmalar
- Üretilen tüm sertifikalar
- Geėerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları
- Yayınlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı

- Sertifika yönetim prosedürleri
- Sertifika Sahibi Taahhütnameleri
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP senkronizasyon loglar

5.5.2. Arşivlerin Tutulma Süresi

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

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler izinsiz izlenmeyi, değiŐtirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduđu ortam Bölüm 5.5.2'de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş sürekliliđi politikası geređince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüđu kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kađıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir.

5.6. Anahtar DeđiŐimi

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 deđiŐimi işlemleri Őunları 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 oluŐturma verisiyle imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM imza oluŐturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluŐturma verisiyle oluŐturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluŐturma verisiyle imzalanmaya devam eder. Yeni üretilen sertifikalar için oluŐturulan yeni SİL dosyası yeni Kamu SM imza oluŐturma verisiyle imzalanır.
- Kamu SM, anahtarlarının yenilendiđi bilgisini Kamu SM resmi web sitesi üzerinden duyurur ve sertifika hizmeti verdiđi kurumları bilgilendirir.

5.7. Güvenliđin Yitilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliđin Yitilmesi Durumunun Düzeltilmesi

Güvenilirliđin 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.

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

İŐ sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar ve depolama alan ađı bileŐenleri yedekli yapıda çalışmaktadır ve kritik süreçler için felaket kurtarma merkezi oluşturulmuŐtur. 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 Gizliliğinin Kaybedilmesi

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

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde Kamu SM resmi web sitesi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, Kurumsal Őifreleme Sertifikası sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluşturulan Kurumsal Őifreleme Sertifikalarına güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikalarının gerekli görülen bir kısmı veya hepsi 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 işletir.
- 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 doğrultusunda sertifika yenileme süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalışırılık

Kamu SM, arıza ya da afet sonrası sistemin en kısa zamanda yeniden ve güvenli olarak çalışmaya başlaması için gerekli yöntemleri ve süreçleri Kamu SM iş sürekliliği planlarında tanımlar.

Kamu SM başka bir şehirde felaket kurtarma merkezine sahiptir. Kamu SM yedeklilik yönetim politikasına uygun olarak önemli veri ve uygulamaların yedeklerini almakta ve gerekli durumlarda yedekten geri dönme işlemlerini uygulamaktadır. İş sürekliliğinin devamı için Kamu SM merkez ofiste saklanan verilerin yedekleri felaket kurtarma merkezinde de saklanmaktadır.

Kamu SM, arıza sonrası yeniden çalışırılığı sağlayacak Kamu SM iş sürekliliği planlarını periyodik olarak gözden geçirir ve test eder. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, işleyişine Elektronik İmza Kanunu'nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verebilir. Bu durumda Kamu SM aŐađıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün kurumlara yazı, sertifika sahiplerine ise e-posta ile duyurur.

- Sertifika hizmetlerine son vereceđi bilgisini internet sitesi üzerinden ve ulusal yayın yapan en yüksek tirajlı 3 (u) gazetede ilan vermek suretiyle kamuoyuna duyurur.
- Sertifika hizmetlerine son vereceđini duyurmasından itibaren sertifika bařvurusu kabul etmez ve yeni sertifika oluřturmaz.
- Ürettiđi Kurumsal Őifreleme Sertifikalarını iptal eder, iptal bilgisini SİL ve İSDUP aracılıđıyla üçüncü kiřilere duyurur. İptal ettiđi Kurumsal Őifreleme Sertifikalarının bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.
- İptal ettiđi Kurumsal Őifreleme Sertifikalarının kullanım süreleri dolana kadar en son ürettiđi SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandıđı imza oluřturma verisine karřılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Kurumsal Őifreleme Sertifikalarını imzalamak için kullandıđı imza oluřturma verisini imha eder.
- İlgili tüm kayıtları ve arřivleri uygun bir řekilde 20 (yirmi) yıl boyunca korur.

6. Teknik Güvenlik Kontrolleri

Kamu SM'nin kendisi ve sertifika sahipleri adına, anahtar çiftleri ve erişim verilerini ürettiđi, sertifika yönetim işlemlerini gerçekleřtirdiđi 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, İSDUP Yayınlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde ařađıdaki anahtar çiftleri oluřturulur:

- Kök SHS'ye ait imza oluřturma ve dođrulama verisi
- Kurumsal Őifreleme SHS'ye ait imza oluřturma ve dođrulama verisi
- İSDUP Yayınlayıcı'ya ait imza oluřturma ve dođrulama verisi
- Kurumsal Őifreleme Sertifikası sahiplerine ait anahtar çifti

Kök SHS, Kurumsal Őifreleme SHS ve İSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceđi güvenli odada, birden fazla eğitimli personelin gözetiminde, ađ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden gemiş, FIPS-140-2 seviye 3 veya EAL4+ standartlarını sađlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen özel anahtar güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dıřarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemleri gerçekleřtiren personel tarafından onaylanır.

İmza oluřturma verisinin saklandıđı 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 giremediđi odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

Kurumsal Őifreleme Sertifikası HSM'ye yüklenecekse, Kurum HSM Cihaz Sorumlusu gözetiminde Kamu SM yetkili personeli tarafından, HSM yerli ve millî ise HSM içerisinde, deđilse HSM dıřında güvenli yazılım ve/veya donanım kullanılarak üretilir.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliği dünyaca kabul görmüş algoritmalar kullanılır. Sertifika sahibine ait özel anahtarın yedeđi alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandığı akıllı kart veya HSM Bölüm 6.2.1’de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine Özel Anahtarın Ulaőtırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip, özel anahtar, sertifikayla birlikte akıllı kart veya HSM’ye yüklenir. Akıllı kart, imza karşılığı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir. HSM’ye özel anahtar ve sertifika yükleme işlemi, Kurum HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Teslim Tutanađı doldurularak kurum tarafından imzalanır.

Akıllı karta erişim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bağlantı protokolleri (HTTPS) kullanılmaktadır. Asıl veya Yedek Sertifika Sorumlusunun kimlik kontrolü için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik doğrulaması sonrasında sertifika sahibi akıllı kart erişim verisine erişir. HSM’ye erişim verisinden Kamu SM sorumlu değildir, kurum inisiyatifindedir.

Kamu SM’nin yükümlülüklerinin belirtildiđi Kamu SM Taahhütnamesi, Kamu SM resmi web sitesi Bilgi Deposu sayfası üzerinden yayımlanır.

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı’na Açık Anahtarın Ulaőtırılması

Kurumsal Şifreleme Sertifikası HSM’ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteđi, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılığıyla Kamu SM’ye ulaőtırılır.

Kurumsal Şifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Şifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildiđi için açık anahtarın Kamu SM’ye ulaőtırılması söz konusu değildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

Kamu SM’ye ait Kök SHS ve Kurumsal Şifreleme SHS sertifikaları internet ortamında tarafların erişimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz deđiştirmeye ve silinmeye karşı güvenliği sağlanır.

Kök SHS ve Kurumsal Şifreleme SHS sertifikaları, sertifikaların özet deđeri ve özet algoritması Kamu SM resmi web sitesi Bilgi Deposu sayfası üzerinden yayımlanır.

6.1.5. Anahtar Uzunlukları

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

Kurumlara ait Kurumsal Şifreleme Sertifikalarını imzalayan Kurumsal Şifreleme 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 Şifreleme Sertifikaları, RSA anahtar boyu en az 2048-bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde kullanılan algoritmaların güvenliđi ispatlanmış ve dünyaca kabul görmüŐtür. Algoritmaların gerçekteŐirtiliminde kullanılan yöntemler gerekli güvenlik kriterlerini sađlar. Anahtarları üreten programlar gerekli güvenlik testlerinden geçirilirler.

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan anahtarların hangi amaçlar için kullanılabileređi sertifikadaki “Anahtar Kullanımı” ve “GeniŐletilmiş Anahtar Kullanımı” uzantısı içerisinde 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. Özel Anahtarın Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM’ye ait imza oluŐturma verisi güvenli yazılım ve/veya donanım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduđu süre boyunca bu modül dıŐına çikmaz.

Kriptografik modül aŐađıda belirlenen güvenlik iŐlevlerine sahiptir:

- İmza oluŐturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüđünü sađlar.
- Modüle erişimde kimlik belirleme ve dođrulama iŐlevlerini yerine getirir.
- EriŐim yetkisi birden fazla kiŐinin kontrolünde olacak şekilde tanımlanabilir.
- Sistem kullanıcılarına tanımlanan roller dođrultusunda, verdiđi hizmetlere erişimi sınırlar.
- Düzgün çalıŐtıđı test edilebilir, test sırasında hata oluŐtuđunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıŐtır.
- Yetkisiz erişime teŐebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeđinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin özel anahtarının içinde bulunduđu akıllı kart veya HSM cihazı, özel anahtarın donanım dıŐına çikmasını engelleyen ve donanıma erişimi parola ile sađlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibine ait akıllı kart veya HSM cihazı, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ’de belirtilen aŐađıdaki güvenlik standartlarından en azından birisini sađlar:
 - FIPS PUB 140-1 veya FIPS PUB 140-2’ye göre seviye 3 veya üzeri,
 - CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)’e veya ISO/IEC 15408 (-1,-2,-3)’e göre en az EAL4+.

6.2.2. Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim

Kamu SM’ye ait imza oluŐturma verisinin bulunduđu odaya erişim aynı anda 2 (iki) çalıŐan tarafından sađlanmaktadır.

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıŐtır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi iin sađlanan gvenlik ile eŐdeđer gvenlik nlemleri altında yapılır. Yedeklenen imza oluŐturma verisi yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak gvenli kriptografik donanım cihazı iinde tutulur. Gvenli donanım cihazı hazırda kullanılmakta olan imza oluŐturma verisinin bulunduđu ortam ile aynı gvenlik Őartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait zel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın ArŐivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait zel anahtarlar arŐivlenmez. Kullanım sreleri sonunda geri dnŐsz Őekilde silinir.

6.2.6. Özel Anahtarın Kriptografik Modle Yklenmesi

Kamu SM'ye ait imza oluŐturma verisi retildikten hemen sonra kriptografik modle yklenir. iŐlem, gvenilir yntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Sertifika sahiplerine ait zel anahtarlar, sadece yetkili personelin kontrolnde akıllı kart veya HSM cihazına Őifrelenerek yklenir. zel anahtar, akıllı kart veya HSM cihazına yklendikten sonra kopyası sistemden silinir.

6.2.7. Özel Anahtarın Kriptografik Modlde Saklanması

Kamu SM'ye ait imza oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak gvenli kriptografik donanım cihazı iinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına ıkması engellenmiŐtir. İmza oluŐturma verisi kriptografik modl iinde gvenli algoritma ve yntemlerle Őifreli olarak saklanır.

Sertifika sahibinin zel anahtarı, kendisine ait akıllı kart veya HSM cihazı iinde saklanır, baŐka bir ortamda bulunmaz. Kamu SM, sertifika sahiplerine ait zel anahtarları kendi sistemi iinde saklamaz.

6.2.8. Özel Anahtara EriŐim

Kamu SM'nin imza oluŐturma verisine eriŐim birden fazla yetkili alıŐanın ortak denetimi altındadır. İmza oluŐturma verisinin bulunduğu odaya giriŐ iin, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin dođrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin dođrulanamadığı durumlarda imza oluŐturma verisinin bulunduğu odaya eriŐim sađlanamaz.

İmza oluŐturma verisi kriptografik modl iinde Őifreli durumdayken eriŐime kapalıdır. EriŐime aılması iin eriŐimi sađlayan verinin modle sunulması gerekir. İmza oluŐturma verisinin eriŐime aılması ve kullanılabilir duruma getirilmesi birden fazla yetkili alıŐanın ortak denetimi altındadır.

Sertifika sahibine ait zel anahtar, akıllı kart veya HSM cihazı iinde sertifika sahibinin eriŐim verisi ile korunmuŐ olarak saklanır. EriŐim denetimi eriŐim denetim verisi ile sađlanır.

6.2.9. Özel Anahtara EriŐimin Kesilmesi

Kamu SM'nin imza oluŐturma verisi 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lm 6.2.8'de belirtilen yntemin yeniden iŐletilmesi gerekir.

Sertifika sahibinin kullandığı güvenli donanım araçları, özel anahtarı kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir. Erişim verisinin art arda 3 (üç) defa yanlış girilmesi durumunda güvenli donanım aracı kilitletir ve araca erişim sağlanamaz.

6.2.10. Özel Anahtarın Yok Edilmesi

Kamu SM'ye ait imza oluşturma verileri kullanım süresinin dolmasının ardından, aslı ve bütün yedekleri buldukları ortamlardan uygun yöntemlerle geri dönüşsüz şekilde silinir. Kamu SM'ye ait imza oluşturma verisinin silinmesi işlemi için Bölüm 6.2.8'de belirtilen şekilde yeterli sayıda yetkili personelin hazır bulunması gerekir.

Sertifika sahiplerine ait özel anahtarların kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından akıllı kart veya HSM cihazı üzerinden silinmelidir. Bu işlemin yapılmasından sertifika sahibi sorumludur.

6.2.11. Kriptografik Modülün Değerlendirilmesi

Kamu SM, Bölüm 6.2.1'de belirtilen standartlara uygun kriptografik modül kullanır.

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. Açık Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait açık anahtarlar, sertifikalar içinde tutulur ve Kurumsal Şifreleme Sertifikaları kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Kurumsal Şifreleme Sertifikalarının arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Kurumsal Şifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Kurumsal Şifreleme Sertifikasının kullanım süresinin dolmasıyla ya da Kurumsal Şifreleme Sertifikasının iptal edilmesiyle özel anahtarın kullanımı sona erer.

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

6.4. Erişim Denetim Verileri

Kamu SM çalışanlarının erişim denetim verileri erişim parolalarını, güvenli donanım araçları içindeki erişim denetimi sağlayan diğer verileri, biyometrik verileri içerir.

Sertifika sahibi kuruma ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, akıllı karta erişim verisi ile sertifika işlemlerinin yapıldığı internet şubesine erişim verileridir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

Kamu SM sistemi içinde kullanılan erişim denetim verileri ile sertifika sahibi kuruma ait erişim parolaları yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rasgele üretilir.

Kamu SM tarafından sertifika sahibi kurum adına oluşturulan erişim parolaları da yukarıdaki paragrafta belirtilen güvenlik şartlarını sağlar.

6.4.2. Erişim Denetim Verilerinin Korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir. Sertifika sahibi kuruma ait erişim parolaları sertifika sahibi kuruma güvenli yöntemlerle ulaştırılır. Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Erişim Denetim Verileri ile İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları, iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibine teslim edilir.

6.5. Bilgisayar Güvenliđi Denetimleri

6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereker

Kamu SM sistemi içinde kötü niyetli yazılımlara karşı gereken önlemler alınır. Sistemde ağ ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuştur, bunlar sürekli güncel tutulmaktadır. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerin tahrifata, silinmeye ve kaçađa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliđi konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır. Güvenlik yamaları değerlendirilip daha büyük bir riske sebebiyet vermesi durumunda yüklenmez ve risk süreç takip sistemi üzerinde kayıt altına alınır. Ağ bileşenleri ve konfigürasyonları dönemsel olarak ağ güvenliđi prosedürü yönergesine göre kontrol edilir.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda 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 ağa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmi 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 TS 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 ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için 2 (iki) yılda en az bir defa 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 Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

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

Sunucular üzerine ağ ve sistem yönetimi ve güvenliği ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı, dosya bütünlüğü, güvenlik kayıtları, harici depolama üniteleri takibi vb. bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi ve güvenliği altyapısı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır. Farklı güvenilir sistemlerle iletişim ihtiyacı olması durumunda, diğer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler (kök ve alt kök sunucuları gibi) için farklı ağ segmentleri oluşturulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıştır. 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 geliştiricileri gibi farklı çalışan gruplarına ait farklı amaca hizmet eden ağlar da birbirinden ayrılmıştır. Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler, güvenlik ekibince kontrollü olarak verilir ve kayıtlar üzerinden izlenir. Farklı bölgelere olan iletişim ve erişim engellendiği gibi gerekli olmayan bağlantı ve hizmetler de ağ güvenliği açısından devre dışı bırakılır.

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller sıkılaştırma prosedürlerine göre kaldırılır ya da devre dışı bırakılır. Ağ ve sistem güvenliğine dair tüm işlemler siber olaylara müdahale ekibi

tarafından izlenir ve gerektiğinde olay müdahale süreçleri doğrultusunda aksiyon alınır. Kamu SM çevrim içi açık anahtar altyapısı hizmetlerinin devamlılığı için Kamu SM ana merkez ve felaket kurtarma merkezinin dış ağ bağlantı hizmetlerini yedekli olarak kurgulamıştır.

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

6.8. Zaman Damgası

Kamu SM sistemi içinde kullanılan zaman damgası gerekli kesinlik ve bütünlük şartlarını sağlar. Kamu SM sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlara uyar.

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 dağıtılan Kurumsal Şifreleme Sertifikalarının içeriği 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 dağıtılan Kurumsal Şifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili açık anahtar, sertifika sahibi kurumun adı ve DETSİS 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 içerir. Kurumsal Şifreleme Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Tablo 1'de Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikalarında asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları

Sertifika Uzantısı	Kritik Uzantı	Açıklama
Temel Kısıtlar ¹	HAYIR	Sertifikanın son kullanıcı sertifikası olduđu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
Yetkili Anahtar Tanımlayıcısı ²	HAYIR	Kamu SM'ye ait Kurumsal Őifreleme SHS açık anahtarının SHA-1 özet çıktısından oluşur.
Sertifika Anahtar Tanımlayıcısı ³	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı ⁴	EVET	Anahtarların sadece Őifreleme amaçlı kullanıldığını ifade edilmesi için "keyEncipherment" [anahtar Őifreleme] alanı seçilmiştir.
SİL Dağıtım Noktaları ⁵	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl
Yetkili Bilgi Erişimi ⁶	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt http://ksifrelemeocspv1.kamusm.gov.tr/
Sertifika İlkeleri ⁷	HAYIR	Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.11) ile SUE dokümanının bulunduğu http://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan Kurumsal Őifreleme Sertifikası ibaresine ait metni içerir.
Genişletilmiş Anahtar Kullanımı ⁸	HAYIR	Kurumsal Őifreleme Sertifikası nesne tanımlama numarasını (2.16.792.1.2.1.1.5.7.51.1) içerir.

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiği Kurumsal Őifreleme Sertifikalarını imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

⁴ KeyUsage

⁵ CRLDistributionPoints

⁶ AuthorityInformationAccess

⁷ CertificatePolicies

⁸ ExtendedKeyUsage

Sertifika sahiplerine ait anahtar çiftleri RSA algoritması anahtar çiftleridir.

Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları içinde belirtilir.

7.1.4. İsim Alanı Biçimleri

Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikalarındaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici İsim]" biçimine uygundur.

7.1.5. İsim Kısıtları

Bölüm 3.1'de belirtilmiştir.

Tablo 2'de Kurumsal Őifreleme Sertifikası içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

Tablo 2 Kurumsal Őifreleme Sertifika İsim Alanı Bilgileri

Alan Adı	Kurumsal Őifreleme Sertifika İçeriđi
CN ⁹	Kurum DETSİS adı
Serial ¹⁰	Kurum DETSİS numarası
C ¹¹	TR

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bađlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.11

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Kurumsal Őifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Őifreleme Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikasının "Sertifika İlkeleri Uzantısı¹²"nın içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici¹³" olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler "Sertifika İlkeleri Uzantısı"nı kontrol ettiğinde Sİ ve 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.

⁹ CN: Common Name [Genel isim]

¹⁰ Serial: Serial Number [Seri Numarası]

¹¹ C: Country [Ülke]

¹² Certificate Policies

¹³ Policy Identifier

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

Kamu SM'nin ürettiđi 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 aŐađıdaki bilgileri içerir:

- SİL'i oluŐturan 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 açık anahtarlı imzalama algoritmasını kullanır.)
- SİL'in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen Kurumsal Őifreleme Sertifikaları ile ilgili aŐađıdaki bilgiler:
 - Sertifikanın seri numarası
 - Sertifikanın iptal tarihi
 - Sertifikanın neden iptal edildiđi bilgisi
- Kamu SM tarafından oluŐturulan elektronik imza
- SİL imzasını dođrulamak 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 aŐađıdaki bilgileri içermelidir:

- Protokol versiyonu
- Hedef sertifika belirteci (kullanılan özetleme algoritması, sertifikayı veren ESHS'nin DN özeti, sertifikayı veren ESHS'nin imza dođrulama verisi 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 aŐağıdaki Őekilde deęerlendirilir:

Good [iyi]: Sertifika geerli konumdadır.

Bad [kötü]: Sertifika askıdadır, iptal edilmiŐtir ya da henüz kullanıma aılmamıŐtır.

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

RFC 6960'ta belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

Kamu SM, ISO/IEC 27001 bilgi gvenlięi ynetim standardına uygun olarak hizmet verir ve standart gereęi dzenli olarak i ve dıŐ denetimlere tabi tutulur.

8.1. Uygunluk Denetiminin Sıklıęı

Kamu SM, ISO/IEC 27001 bilgi gvenlięi ynetim sistemi standardı gereęince yılda bir defa uygunluk denetimi geerir. Her  yılda bir sertifika yenilenir.

İ denetim, yılda bir defa gerekleŐtirilir.

8.2. Denetinin Nitelikleri

ISO/IEC 27001 BGYS'nin denetimi akredite edilmiŐ kuruluŐlarca gerekleŐtirilir.

İ denetim, Kamu SM sertifika srelerini bilen ve denetim konusunda tecrbeli Kamu SM personeli tarafından gerekleŐtirilir.

8.3. Denetinin Denetlenen Tarafla Olan İliŐkisi

DıŐ denetiler, herhangi bir ıkar atıŐması olmaması ve baęımsızlıęın zedelenmemesi iin Kamu SM'den baęımsız kiŐilerden oluŐur. İ denetim iin seilen denetiler ise denetlenecek birimden seilmez.

8.4. Denetimin Kapsamı

Kamu SM i denetimlerinde, Sİ ve SUE dokmanına uygunluk denetlenir. İ denetim kapsamı denetimi gerekleŐtirecek Kamu SM personeli tarafından belirlenir.

ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun Őekilde baęımsız kurum denetisi tarafından belirlenir.

8.5. Yetersizlięin Tespiti Durumunda Yapılacaklar

ISO/IEC 27001 standardına gre gerekleŐtirilen denetimlerde ortaya ıkan eksiklikler, Kamu SM tarafından planlı alıŐma ile giderilir. Eksiklikler, BGYS'nin temel iŐleyiŐini etkileyecek kadar byk ise Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İ denetimlerde ortaya ıkan eksiklikler, Kamu SM ilgili personeli tarafından giderilir. Tm denetimlerden elde edilen bulgular Uygunsuzluk veya Dzeltici/İyileŐtirici Faaliyetler aılarak takip edilir.

8.6. Sonucun Bildirilmesi

Denetim sonucu, ISO/IEC 27001 denetilerinin hazırladıęı resmi raporlar ile Kamu SM'ye bildirilir.

İ denetim sonucu, Kamu SM st ynetimine raporlanır.

9. Diđer İŐler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika OluŐturma ve Yenileme Ücreti

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

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

9.1.2. Sertifika EriŐim Ücreti

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

9.1.3. İptal Durum Kaydına EriŐim Ücreti

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

9.1.4. Diđer Servis Ücretleri

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

Kamu SM, kuruma ait özel anahtar 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.

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 tamamlanmamışsa kurumun talebi doğrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu değildir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Kamu SM, Bölüm 9.2.3'te belirtilen sertifika sahibi mali sorumluluk sigortası dışında, kendi sorumluluklarını karşılamak amacıyla sigortalanmamıştır.

9.2.2. Diđer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, ürettiği Kurumsal Şifreleme Sertifikaları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalar.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. Kişisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diğer paydaşların kişisel verilerinin gizliliğini 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar'da ve 6698 sayılı kanunlar kapsamındaki mer'i mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurumun ve yetkilendirdiği Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu ile Kurum HSM Cihaz Sorumlusunun, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi kurum tarafından atanan parolalar, numara, sembol gibi diğer tanımlayıcı bilgiler de kişisel bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kurumsal Şifreleme Sertifikası içeriğinde bulunan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluđu

Kamu SM, sertifika talep eden kurumdan Kurumsal Şifreleme Sertifikası vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiği kişisel bilgileri sertifika hizmeti vermek dışında başka amaçlar için kullanmaz, üçüncü kişilere vermez, sertifika sahibi kurumun izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulundurmaz.

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

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM, sertifika sorumlularının yazılı rızası ile kişisel bilgileri üçüncü kişilerle paylaşabilir.

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

Kamu SM tarafından üretilen tüm Kurumsal Şifreleme Sertifikaları ve dokümanlar ile bu SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM tarafından verilen sertifika hizmetlerinde sistem bileşenleri olarak tanımlanan Kamu SM, sertifika sahipleri ve üçüncü kişiler 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslarda belirtilen şekilde üzerlerine düşen yükümlülükleri sağlar.

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde imzalanmış olan Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi yükümlülüklerini de yerine getirirler.

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHs olarak Kamu SM'nin yükümlülükleri aşağıda belirtilmiştir:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak
- Kök SHS ve Kurumsal Şifreleme SHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak
- Kök SHS ve Kurumsal Şifreleme SHS sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak
- Kurumsal Şifreleme Sertifikası verdiği kurumların kimliğini DETSİS üzerinden güvenilir bir biçimde doğrulamak

- 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 içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine Kurumsal Őifreleme Sertifikası vermemek
- Kurumsal Őifreleme Sertifikası başvurularını değerlendirerek, 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 özel anahtarı oluşturduktan sonra özel anahtar ve üretiminde kullanılan gizli değişkenleri kendi sisteminden silmek, özel anahtarın kopyasını hiçbir şekilde tutmamak
- Sertifika sahibine akıllı kart temin etmesi durumunda, bu aracın güvenli olmasını sağlamak
- Üretilen Kurumsal Őifreleme Sertifikaları özel anahtarlarını Sİ ve SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek
- Sertifika sahiplerinin Kurumsal Őifreleme Sertifikalarını DETSİS'e yüklemek
- Kurumsal Őifreleme Sertifikalarının kullanım şartlarını belirleyen sertifika profillerini oluşturmak
- Kurumsal Őifreleme Sertifika başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli işlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıdan indirme işlemlerini Sİ ve SUE'de belirtilen şekilde yapmak
- Kurumsal Őifreleme Sertifikası iptal başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak
- Yayımlanan Sİ ve SUE dokümanları ile Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesine uygun olmayan Kurumsal Őifreleme Sertifikası kullanımlarının tespit edilmesi durumunda ilgili Kurumsal Őifreleme Sertifikasını iptal etmek
- İptal edilmiş Kurumsal Őifreleme Sertifikası bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak
- Kurumsal Őifreleme Sertifikalarının ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak
- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek
- Kurumsal Őifreleme Sertifikası üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak
- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen süreler boyunca güvenli olarak saklamak

9.6.2. Kayıt Birimi Yüklölölükleri

Kayıt birimlerinin yüklölölükleri Bölüm 9.6.1’de belirtilen ESHS yüklölölükleri ile aynıdır.

9.6.3. Sertifika Sahibinin Yüklölölükleri

Sertifika sahibinin yüklölölükleri aŐağıda belirtilmiŐtir:

- Kurumsal Őifreleme Sertifikası baŐvuru, askıya alma, iptal ve diđer iŐlemleri, ilgili Sİ ve SUE’de belirtildiđi Őekilde, detayları Kamu SM Kurumsal Őifreleme Sertifikası yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek
- Kurumsal Őifreleme Sertifikası baŐvurusu, yenileme ve iptal iŐlemleri sırasında dođru bilgi beyan etmek
- Kurum adına düzenlenen Kurumsal Őifreleme Sertifikası üretildiđinde sertifikadaki bilgilerin dođruluđunu kontrol etmek
- SUE Bölüm 6.2.1’de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- Özel anahtarın güvenliđini sađlamak, kendisine ait özel anahtarın içinde bulunduđu akıllı kart veya HSM’in ve eriŐim verisinin gizliliđini korumak, bunları baŐkasına kullanırmamak ve bu konuda gerekli tedbirleri almak
- İnternet veya çağrı merkezi üzerinden sertifika iŐlemlerini yapabilmesi için kullandıđı parolalarının gizliliđini ve güvenliđini sađlamak
- Özel anahtarın içinde bulunduđu akıllı kart veya HSM’in kaybolması, çalınması veya özel anahtarın gizliliđinin yitirildiđinden Őüphelenmesi durumunda Kurumsal Őifreleme Sertifikasının iptal edilmesi için Kamu SM’ye en kısa zamanda baŐvurmak
- Akıllı kart veya HSM eriŐim verisini ve sertifika iŐlemlerinde kullandıđı diđer parolaları düzenli olarak deđiŐtirmek
- Kurumsal Őifreleme Sertifikası içeriđinde bulunan bilgilerin deđiŐmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM’ye baŐvurmak
- Kurumsal Őifreleme Sertifikası baŐvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiđi bilgilerde meydana gelen deđiŐiklikleri derhal Kamu SM’ye bildirmek
- İptal olmuŐ, kullanıma aılmamıŐ, askıya alınmıŐ veya geçerlilik süresi dolmuŐ Kurumsal Őifreleme Sertifikası ile iŐlem yapmamak
- Özel anahtarını imzalama amacıyla kullanmamak

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

9.6.4. Üçüncü KiŐilerin Yüklölölükleri

Üçüncü kiŐiler, Kurumsal Őifreleme Sertifikasıyla iŐlem yapmadan önce sertifikanın aŐağıda belirtilen geçerlilik kontrollerini yapmakla yüklölölüdür:

- Kurumsal Őifreleme Sertifikasının tanımlanan veriliŐ amacına uygun olarak kullanıldıđını dođrulamak
- Kurumsal Őifreleme Sertifikasının kullanım süresinin dolup dolmadıđını kontrol etmek

- Kurumsal Őifreleme Sertifikasının geerliliđini SİL veya İSDUP Yanıtlayıcı aracılıđıyla kontrol etmek
- SİL veya İSDUP Yanıtlayıcı'dan aldıđı iptal durum kaydının bütünlüđünü 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 dođruluđunu sertifika özet deđerini kontrol etmek suretiyle dođrulamak
- Sertifika sahibinin Kurumsal Őifreleme Sertifikasının içindeki açık anahtarına karşılık gelen özel anahtara sahip olduđunu dođrulamak

9.6.5. Diđer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

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

- Sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olacak biri asıl biri yedek olmak üzere iki tane kurum sertifika sorumlusu görevlendirmek ve Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ile kurum sertifika sorumlularının bilgilerini Kamu SM'ye bildirmek
- Kurum sertifika sorumlusunun görevi sonlandırıldıđında bunu Kamu SM'ye resmi yazı ve Kurum Sertifika Sorumlusu Yetkilendirme/Bilgi Güncelleme Formu ve Taahhütnamesi ile bildirmek
- Yeni görevlendirdiđi kurum sertifika sorumlularının bilgilerini Kamu SM'ye resmi yazı ve Kurum Sertifika Sorumlusu Yetkilendirme/Bilgi Güncelleme Formu ve Taahhütnamesi ile bildirmek
- Sertifika yönetim süreçleri ile ilgili varsa Kamu SM ile imzalanan sözleşmeye uymak
- Sertifika yönetim süreçleri ile ilgili Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesindeki yükümlülükleri yerine getirmek
- Kamu SM'nin internet sitesi üzerinden yayımladıđı Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesini doldurarak sertifika başvurusu sırasında resmi yazı ile Kamu SM'ye iletmek

9.6.5.2. Kurum Sertifika Sorumlularının Yükümlülükleri

Kurum adına Kurumsal Őifreleme Sertifikası başvurusunda bulunan Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun yükümlülükleri aőađıda belirtilmiőtir:

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

Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun sertifika teslimatları ile ilgili yükümlülükleri Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilmiőtir.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yükümlülük, Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelerde belirtildiđi şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 2017/21 Sayılı BaŐbakanlık Genelgesi, Bilgi Teknolojileri ve İletifim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslar'da belirtilen Őartlar ile sınırlıdır.

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelerde 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 yükümlülüklerin yerine getirilmemesinden kaynaklanan zararlar, tarafların o ana kadar somut olarak gerçekteŐmiş hak ve alacakları korunmak suretiyle tasfiye edilir.

9.10. AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi

Sertifika sahibi kurum, Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile iŐ birliđi içinde çalıŐır.

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

Kamu SM sertifika hizmeti verdiđi süre boyunca Sİ ve SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine iletildiđi Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi ve varsa kurum ile imzaladıđı sözleşmelerdeki Őartları yerine getirir.

9.10.1. AnlaŐma Süresi

Sertifika sahibi kurumun imzaladıđı Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesinin veya imzalanan sözleşmenin süresi sertifikanın geçerlilik süresi veya taahhütname veya sözleşmede belirtilmiŐse hizmetin alınma süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda sözleşme veya taahhütnamenin süresi de sona erer. Kurumla imzalanan sözleşmenin geçerlilik süresi sözleşme içerisinde belirtilir.

9.10.2. AnlaŐmanın Sona Ermesi

Kamu SM ile kurum arasında varsa imzalanan sözleşme aŐađıdaki durumlarda sonlandırılabilir:

- Taraflardan birisinin sözleşmeye uygun olarak, sözleşmenin sonlandırılması için talepte bulunması
- Sözleşmenin süresinin sona ermesi
- Her iki tarafın da ortak karar olarak sözleşmeyi bitirmesi
- Taraflardan birisinin sözleşmeye aykırı davranması: Taraflardan biri sözleşme kapsamında üzerine düşen yükümlülükleri yerine getirmez ise diđer taraf sözleşmeye aykırı davranan tarafa bu yükümlülüđü yerine getirmesi için 20 (yirmi) günlük süre verir. Bu sürenin sonunda da sözleşmeye aykırılık ortadan kaldırılamaz veya dođacak zarar, ziyan talepleri saklı kalmak kaydıyla yükümlülük yerine getirilmez ise sözleşme tek taraflı olarak feshedilebilir.
- Bölüm 5.7.3'te belirtilen güvenlik açığıının ortaya çıkması sebebiyle Kamu SM sertifika sahiplerine ait Kurumsal Őifreleme Sertifikalarını iptal ederek sözleşmeyi sonlandırabilir.

- Kamu SM Bölüm 5.8’de belirtildiđi biçimde sertifika hizmetlerini sonlandırırđa, sertifika sahiplerine ait Kurumsal Őifreleme Sertifikalarını iptal ederek sözleşmeyi sonlandırabilir.

Kamu SM Taahhütnamesi ve Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi veya imzalanan sözleşme aŐađıdaki durumlarda sonlandırılabilir:

- Sertifika sahibi kurumun sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi
- Sertifika sahibi kurumun imzalanan sözleşme veya Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesine 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 sonlandırırđa, Kamu SM’nin sertifika sahibi kuruma ait sertifikayı iptal etmesi

9.10.3. AnlaŐmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleşmenin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Kamu SM kurumdan sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmıŐ başvurular ile ilgili işlemler, anlaşmanın sona erme sebebine bađlı olarak kurumun talep etmesi durumunda devam eder.

İmzalanan sözleşme veya Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Sertifika sahibi kurumun Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinden, Sİ ve 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.

Sözleşme ve 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, Bölüm 5.4 ve 5.5’te belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

9.11. Sistem BileŐenleri ile Haberleşme 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. Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde belirtilen sertifika sorumlusunun kurumsal e-posta adresine, deđişmesi halinde yeni bildirdiđi kurumsal e-posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

Sertifika yönetimiyle ilgili kritik görülen işlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

Sertifika yönetim işlemleri sırasında sertifika sorumluları veya kurumlarla yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacađı Kamu SM’nin Kurumsal Őifreleme Sertifikası yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. Deęişiklik Halleri

9.12.1. Deęişiklik Metotları

SUE dokümanı Kamu SM tarafından yazılmıştır. Bu SUE dokümanında yapılabilecek deęişiklikler ekleme ve deęiřtirme şeklinde olabileceęi gibi Kamu SM dokümanının tamamen yenilenmesine de karar verebilir. Bu SUE dokümanının herhangi bir kısmının yanlış ya da geçersiz olduęu ortaya çıksa bile SUE dokümanının dięer kısımları, SUE dokümanı güncellenene kadar geçerlilięini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklıęı

SUE dokümanında yapılan deęişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden eriřime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandıęı tarihte yürürlüęe girer.

9.12.3. Nesne Tanımlama Numarasının Deęişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlařmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilafların çözümünde 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslara başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

SUE dokümanındaki hükümler, 2017/21 Sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslara uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

SUE dokümanında geçen hükümlerin daha sonra yürürlüęe girecek ilgili mevzuata aykırı bulunması halinde dokümanda gerekli deęişiklikler yapılarak uygun hale getirilir.

9.16. Dięer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI

Alan	Deęer
Sürüm	V3
Seri Numarası	00ed1db82e01d6
İmza Algoritması	SHA-384 ile ECDSA { 1 2 840 10045 4 3 3 }
Sertifika Vereni	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	9 Ağustos 2019 Cuma 19:25:08
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Açık anahtar	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= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

10.2. KAMU SM KURUMSAL ŐİFRELEME ALT KÖK SERTİFİKASI

Alan	Deęer
Sürüm	V3
Seri Numarası	00f4dfbe9d0289
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifika Vereni	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	20 Kasım 2020 Cuma 15:56:15
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kurumsal Őifreleme Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR
Açık anahtar	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= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlar	Kritik=Evet ; 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 Niteleyicisi= http://depo.kamusm.gov.tr/ilke</p> <p>[1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=Kullanıcı Uyarısı Niteleyicisi= 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=http://depo.kamusm.gov.tr/nes/kokshs.v6.crl</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=http://depo.kamusm.gov.tr/nes/kokshs.v6.crt</p>

10.3. SON KULLANICI KURUMSAL ŐİFRELEME SERTİFİKA ŐABLONU

Alan	Deđer
Sürüm	V3
Seri Numarası	64 bit rastsal 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 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - 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
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Deęer
Yetkili Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimlięi= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimlięi= Sertifikanın ięerięindeki "subjectPublicKey" alanının "BIT STRING" olarak deęerinin SHA-1 özet çıkıtısından oluşur.
Anahtar Kullanımı	Kritik=Evet ; 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= http://depo.kamusm.gov.tr/ilke [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= http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl

Yetkili Bilgi EriŐimi	<p>[1]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diđer Ad: URL=http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt</p> <p>[2]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1) Diđer Ad: URL=http://ksifrelemeocspv1.kamusm.gov.tr/</p>
-----------------------	---