

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŞİFRELEME SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu

YON.05.02

Revizyon No

12

Revizyon Tarihi

05.08.2024

TASNİF DIŐI

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk Çıkıő.	15.01.2021
01	Doküman formatı güncellenmiőtir.	18.01.2021
02	Sertifika yenileme süreci güncellenmiőtir.	29.11.2021
03	Elektronik mühür ve kurumsal Őifreleme sertifikaları başvuru formlarının birleőtirilmesi dođrultusunda "Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi" dokümanının adı "Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taaahhütnamesi" olarak deđiőtirilmiőtir.	07.01.2022
04	Sertifika üretiminin iki kiőtinin kontrolünde yapılması gerektiđi ile ilgili ibare kaldırılmıőtir.	17.02.2022
05	Yenileme sürecinde üretimi gerçekleőtirilen sertifikaların baőtlangıç tarihleri ile ilgili bilgilendirme kaldırılmıőtir.	16.03.2022
06	Yenileme sürecinde her iki sertifika sorumlusunun başvuru listesini imzalama koőtulu kaldırılarak yalnızca bir sorumlunun imzasıyla iőtlem yapılması sađlanmıőtir.	31.03.2022
07	Güvenli elektronik imza oluőturma araçlarının güvenlik seviyelerinde düzenleme yapılmıőtir. Sertifika hizmetlerinin sonlandırılması baőtliđında Kamu SM Hizmetleri Sonlandırma Planına referans eklenmiőtir.	28.04.2022
08	Sertifika İptal Listesi yayımlama gecikmesi süresi kısmında güncelleme yapılmıőtir. Doküman genelinde ek düzeltmeler uygunlanmıőtir.	20.10.2022
09	Sertifika sorumluları arasındaki asıl/yedek ayrımı kaldırılmıőtir. Sertifikanın askıda kalma süresi ile ilgili ifadeler düzenlenmiőtir. Dokümanda referans verilen mevzuatlar için tanım eklenmiőtir. Kullanılmayan "Kamu SM Taahhütnamesi" ve "Sözleőtme" ibareleri kaldırılmıőtir. HSM'li üretimlerde istek dosyalarının parola korumalı zip içerisinde iletimi ile ilgili ifade eklenmiőtir. MERNİS tanımı eklenmiőtir. Doküman genelinde editöryal düzenlemeler yapılmıőtir.	06.03.2023
10	Yenileme sürecinde üretim 3 ay öncesinde baőtlayacak Őekilde düzenleme yapılmıőtir.	21.12.2023

KURUMSAL ŐİFRELEME SERTİFİKA UYGULAMA ESASLARI

11	Yenilemelerde DETSİS web servisi üzerinden sertifika alma yetki sorgusu yapılamadığı durumlarda uygulanacak süreç ile ilgili bilgilendirmeler eklenmiştir. Genel gözden geçirme kapsamında metinsel düzenlemeler gerçekleştirilmiştir.	22.04.2024
12	e-Yazışma Teknik Rehberi'nin 2.1 versiyonunun yayımlanması doğrultusunda düzenlemeler yapılmıştır.	05.08.2024

İÇİNDEKİLER

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

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

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

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

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

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

TABLolar

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

1. Giriő

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

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

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

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

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

1.1. Genel Bakıő

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

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

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

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kurumsal Őifreleme Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 12

Yayın Tarihi: 05.08.2024

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.11

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

1.3. Sistem Bileşenleri

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

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

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

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

1.3.2. Kayıt Birimleri

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

1.3.3. Sertifika Sahipleri

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

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

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kurum bilgileri ve açık anahtar arasındaki bağıın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir/kurumlardır.

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diđer Bileőenler

1.3.5.1. Kurumsal Őifreleme Sertifikası Sorumlusu

Sertifika bařvurusunda bulunan kurum tarafından yetkilendirilen ve sertifika ynetim srelerinde Kamu SM ile iletiőim iinde olan kiői/kiőilerdir.

Kurumsal Őifreleme sertifikaları iin sertifika sahibi kurum tarafından onaylanan taahhtname ile Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları belirlenmektedir.

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları Kamu SM tarafından kendisine imzalatılan taahhtnamedeki Őartları yerine getirmekten sorumludur. Sertifika sorumluları, Kurumsal Őifreleme Sertifikasını kullanmaya yetkili olmak zorunda deđildir. Kurumsal Őifreleme Sertifikasını kullanmaya yetkili kiői/kiőilerin belirlenmesi kurum inisiyatifindedir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı Bařbakanlık Genelgesi ile elektronik ortamda iletilen resm yazıların Őifreli Őekilde gnderilebilmesine imkn sađlanmıŐtır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluŐları arasında elektronik ortamdaki belge paylaŐımında Őifreleme yapmak amacıyla gncel e-YazıŐma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

Kamu kurum ve kuruluŐları adına retilen Kurumsal Őifreleme Sertifikalarında bulunan aık anahtar, gnderici kurumların Őifreli paket oluŐturabilmesi; sertifika sahibi kurumun himayesinde bulunan zel anahtar ise kendisine gnderilen Őifreli paketlerin aılabilmesi amacıyla kullanılır. Kurumsal Őifreleme Sertifikaları, bilgi ve belgelerin Őifrelenerek uzun sreli saklanması ve elektronik imzalama amacıyla kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Őifreleme Sertifikası Blm 1.4.1'de belirtilen amalar dıŐında kullanılamaz. Belirtilen kapsam dıŐında kullanımdan dođan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, rettiđi sertifikaların hangi uygulamalarda ne amalar dođrultusunda kullanıldıđının kontroln yapmakla ykml deđildir.

1.5. Uygulama Esaslarının Ynetimi

1.5.1. Dokman Ynetimi

SUE dokmanı Kamu SM tarafından yazılmıŐtır. Kamu SM, gerekli grdđ durumlarda SUE dokmanında deđiŐiklik yapabilir.

1.5.2. İletiŐim Bilgileri

Bu SUE dokmanının uygulanması ve ilgili ynetim ilkeleri hakkındaki sorular Kamu SM'nin aŐađıdaki eriŐim noktalarına ynlendirilebilir:

Adres : Kamu Sertifikasyon Merkezi, TBİTAK 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 dokümanını herkesin erişimine açık bulunan aşağıdaki internet adresinden yayımlar:

- <http://depo.kamusm.gov.tr/ilke/>
- https://kamusm.bilgem.tubitak.gov.tr/depo/ilke_ve_uygulama_esaslari/guncel_ilke_ve_uygulama_esaslari.jsp

1.5.3. Sertifika Uygulama Esaslarının İlgelere Uygunluğunu Belirleyen KiŐi

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

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

Açık Anahtar: İlgili özel anahtarın sahibinin herkes ile paylaşılabilirdiđi, özel anahtarı ile oluşturduđu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşenidir.

Akıllı Kart veya HSM EriŐim Verisi: Sertifika sahibine ait Özel Anahtara erişimin kontrolünü sađlayan PIN ve PUK bilgisidir.

Akıllı Kart: Sertifika ve sertifika ile ilişkili özel anahtarın içinde bulunduđu güvenli donanımdır.

Anahtar Çifti: Özel anahtar ve onunla ilişkili olan açık anahtar çiftidir.

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

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

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

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

HSM (Hardware Security Module): Sertifikanın kriptografik anahtarlarının içinde bulunduđu harici aygıt; donanımsal güvenlik modüldür.

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

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

İptal Durum Kaydı: Kullanım süresi dolmamıő sertifikaların iptal bilgisinin yer aldıđı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kiőilerin hızlı ve güvenli bir biçimde ulaşabileceđi kayıtlardır.

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

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

Kök Sertifika Hizmet Sađlayıcısı: Kamu Sertifikasyon Merkezi içinde oluőturulmuő, en yetkili imza derecesi verilmiő ve sertifikasını kendisi imzalamıő olan Sertifika Hizmet Sađlayıcısıdır.

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

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

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları: Kamu kurumlarının baővuru formu ve taahhütname ile Kamu SM'ye bildirdiđi ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde kurumu temsile yetkili kiői/kiőilerdir.

Kurumsal Őifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifikadır.

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

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

Özel Anahtar: Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluőturmak ve/veya ilgili Açık Anahtarla Őifrelenmiő elektronik kayıtların, dosyaların Őifresini çözmek için kullanılan anahtardır.

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

Sertifika Süresi: Üretim anında sertifikanın içine yazılan, sertifikanın geçerlilik baőlangıç ve bitiő tarihleri arasında kalan süredir.

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

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

Üçüncü Kiőiler: Sertifikalara güvenerek iőlem yapan gerçek veya tüzel kiőilerdir.

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliđi Yönetim Sistemi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

EAL (Evaluation Assurance Level): Deđerlendirme Garanti Düzeyi

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

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliđi

Kamu SM: Kamu Sertifikasyon Merkezi

MERNİS: Merkezi Nüfus İdare Sistemi

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Śİ/SUE: Sertifika İlkeleri/ Sertifika Uygulama Esasları

ŚİL: Sertifika İptal Listesi

2. Yayınlama ve Bilgi Deposu Yükümlölükleri

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

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

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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

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

2.3. Yayımlık Sıklık ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ/SUE dokümanları içeriğinin deėiŐmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip mümkün olan en kısa sürede yayımlanır. Sertifika iptal durum kayıtlarının yayımlanma sıklık bu dokümanda Bölüm 4.9.7 ve 4.9.9'da belirtilmektedir.

2.4. EriŐim Kontrolleri

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

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

3. Kimlik Belirleme ve Doğrulama

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

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

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

3.1.2. Kimlik Bilgilerinin TeŐhise ElveriŐli Olması

Kurumsal Őifreleme Sertifikaları ieriđindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimliđinin tespit edilmesini sađlayan niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

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

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

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

3.1.5. Kimlik Bilgilerinin Tekilliđi

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

3.1.6. Markanın Tanınması, Dođrulması ve Rolü

Düzenlenmesine gerek duyulmamıŐtır.

3.2. İlk Kimlik Dođrulama

Kamu SM Kurumsal Őifreleme Sertifikası hizmetlerinden faydalanmak iin baŐvuruda bulunulduđunda, ilgili kurumun dođrulanabilmesi iin aŐađıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliđinin Kanıtlanması

Sertifika sahibine ait aık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir.

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

3.2.2. Kurumsal Kimliđin Belirlenmesi

Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan kurumlar, talep edilen kurum bilgilerini, Kamu SM tarafından sunulan baŐvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, kurum tarafından iletilen bilgilere istinaden kurum kimliđini dođrular. Kurumların sertifika alma yetkisi DETSİS aracılıđıyla kontrol

edilir. BaŐvuru esnasında sertifika iŐlemlerini kurum adına yűrűtecek Kurumsal Őifreleme Sertifikası Sorumluları da belirlenerek Kamu SM'ye iletilir.

3.2.3. KiŐisel KimliĐin Belirlenmesi

Kurumsal Őifreleme Sertifikaları, yalnızca Bűlűm 1.3.3'te belirtilen kurumlar adına űretildiĐinden bireysel baŐvurular kabul edilmemektedir. BaŐvuru formu ve taahhűnamelerde yer alan kiŐisel bilgiler MERNİS űzerinden kontrol edilmektedir. Kontrol edilemeyen bilgilerin doĐruluĐu kurumun sorumluluĐundadır.

3.2.4. DoĐrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika sorumlusu/sorumluları tarafından baŐvuru sırasında ve daha sonra deĐiŐiklik sebebiyle beyan edilen aŐaĐıdaki eriŐim bilgileri ve diĐer bilgilerin doĐruluĐu Kamu SM tarafından kontrol edilmez:

- Telefon numaraları
- Kurumsal Őifreleme Sertifikası tesliminde kullanılacak adres bilgisi
- Elektronik posta adresleri
- Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının űvanı veya gűrevi ile ilgili bilgiler
- Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının alıŐtıĐı birim ile ilgili bilgiler

Bu bilgilerin doĐruluĐu kurumun beyanı űzerine kabul edilir.

Kurum bu bilgileri Kamu SM'ye doĐru beyan etmekle yűkűmlűdűr. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doĐabilecek zararlardan, sertifikanın hatalı űretilmesinden ve sertifika yűnetim sűrecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin DoĐrulanması

Sertifika ieriĐine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Dűzenlenmesine gerek duyulmamıŐtır.

3.3. Sertifika Yenileme İŐteĐinde Kimlik DoĐrulama

Kamu SM yenileme talebinde bulunan sertifika sahibi kurumun bilgilerini gűncelliĐini doĐrular.

3.3.1. OlaĐan Sertifika Yenileme İŐteĐinde Kimlik DoĐrulama

Bűlűm 3.2'de anlatıldıĐı Őekilde uygulanır. Bu bűlűmde belirtilen doĐrulamaların gerekleŐtirilememesi durumunda Kamu SM'nin ilgili prosedűrlerinde belirlenen sűreler iŐletilir.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik DoĐrulama

Bűlűm 3.2'de anlatıldıĐı Őekilde uygulanır. Bu bűlűmde belirtilen doĐrulamaların gerekleŐtirilememesi durumunda Kamu SM'nin ilgili prosedűrlerinde belirlenen sűreler iŐletilir.

3.4. Sertifika İptal İŐteĐinde Kimlik DoĐrulama

Sertifika sahibi kurumun yetkilendirdiĐi sertifika sorumlusu/sorumluları Kamu SM resmű web sitesinde yer alan Online İŐlemlere kimlik doĐrulamasıyla giriŐ yaparak iptal iŐlemini gerekleŐtirebilir. Online İŐlemler adresine ulaŐılamaması durumunda Kamu SM web sitesinde belirtilen yűntemlerle iptal iŐlemi

gerçekleŐtirilebilir. Web sitesinde yer alan yöntemlerle yapılan iptal baŐvurularında baŐvuru sahibinden gelen evraklar dođrulanır ve sertifika sorumlusu bilgileri kontrol edilir. Ayrıca Elektronik Mühür/Kurumsal Őifreleme Sertifika Sorumlusu telefon ile aranarak kimlik dođrulama gerçekleştirilir ve iptal talebi teyit edilir.

4. Sertifika YaŐam Döngüsü Őİşlevsel Gereklilikleri

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

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

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

4.1. Sertifika BaŐvurusu

4.1.1. Sertifika BaŐvurusunu Kimlerin Yapabildiđi

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

BaŐvuru süreci, kamu kurumunun resmî yazısı ekinde Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru 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 resmî internet sitesinden yayımlanır. Kurumun sertifika baŐvuru işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumlusu/sorumluları tarafından yürütülür.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Őifreleme Sertifikası baŐvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacađı sertifika hizmetlerinin şartları sertifika sahibi kurumun imzaladıđı baŐvuru formu ve taahhünamesi, Kamu SM'nin internet üzerinden yayımladıđı ilgili yönergeler, Sİ/SUE dokümanları dođrultusunda belirlenir.

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

Cumhurbaşkanlıđı tarafından 10.06.2020 tarihli ve 2646 sayılı Resmî Gazetede yayımlanan "Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" in, 4. Maddesi geređince; kamu kurum

ve kuruluşlarınca resmî yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu kapsamda, zorunlu haller veya olağanüstü durumlar dışında EYP dosyası ile başvuru dışında başvurular kabul edilmeyecektir. Zorunlu hallerde veya olağanüstü durumlarda resmî yazışmalar, KEP veya kurumsal e-posta yoluyla iletilen ilgili başvuru formu ve taahhütnamelerin doğrulanmasının ardından ıslak imzalı ve mühürlü olacak şekilde üst yazısıyla birlikte Kamu SM'ye posta yoluyla iletilir. Kurumsal Őifreleme 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 olduđu bilgilerin doğruluđunu takip etmekle ve bu bilgilerde deđişiklik olması halinde belirlenmiş araç ve yöntemler ile Kamu SM'yi bilgilendirmekle yükümlüdür. Kamu SM, Kurumsal Őifreleme Sertifikası içinde yer alacak bilgilerin doğruluđunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliđini sağlamak için gerekli tedbirleri alır.

Kamu SM, sertifika verilecek kurumların kimlik tanımlama ve doğrulama işlemlerini yaptıktan sonra başvurularını deđerlendirir 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 Őifreleme Sertifikası başvurusunda bulunan kurumların Kamu SM'ye gönderdiği bilgi ve belgeler aşağıda sıralanmıştır:

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

Kurum tarafından 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 Őifreleme Sertifikası almaya yetkili olup olmadığı sorgulanır.
- Kurum tarafından gönderilen Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesinde yer alan kurumun adı, vergi kimlik numarası, yetkilendirilen Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının T.C. kimlik numarası, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgilerinde eksiklik olup 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; resmî olarak sahibi oldukları web sitelerinin belirlenen dosya yoluna elektronik ortamda ilettikleri

baŐuru evraklarının 3zet deęeri eklenmeli veya baŐuru formunda kurum onayını veren 3st d3zey yetkili ses kaydı alabilen telefon ile aranarak doęrulama onayı alınmalıdır.

Bilgi ve belgeler hatasız ve tam ise kurum kimlik tanımlama ve doęrulama iŐlemi tamamlanır. Belgelere g3zle g3r3len tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlıęının tespit edilmesi durumunda kurum kimlik tanımlaması ve doęrulaması yapılamaz. BaŐuru evraklarının, tanımlanan y3ntemler dıŐında bir y3ntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

4.2.2. Sertifika BaŐurusunun Kabul veya Reddi

“Kamu Kurum ve KuruluŐları Arasında Elektronik Ortamdaki Belge PaylaŐımında Kullanılan Kurumsal Őifreleme ve Elektronik M3h3r Sertifikalarına iliŐkin Usul ve Esaslar”ın ikinci b3l3m, 5’inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS’te bilgileri bulunmayan veya Kurumsal Őifreleme Sertifikası almaya yetkisi olmayan tarafların baŐurusunu reddeder.

Buna ek olarak, B3l3m 4.2.1’deki kontrollerin yapılması sonucunda, baŐuru sırasında beyan edilen belgelere tahrifat, hata, eksik onay, eksik veya yanlış bilgi olması durumlarında baŐuru geri 3evrilir. BaŐurusu kabul edilmeyen kurumlarla ilgili yazılı bilgilendirme, Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının baŐuru sırasında beyan ettikleri e-posta adresleri aracılıęı ile yapılır ve gerekli g3r3len bilgi ve belgeler tekrar talep edilir. Gereken d3zeltmeler yapıp eksiklikler tamamladıktan sonra baŐuru tekrarlanabilir.

BaŐurusu kabul edilen kurumlar, Kamu SM sisteminde tanımlanır ve sertifika 3retim s3reci baŐlatılır.

4.2.3. Sertifika BaŐurusunun İŐlenme Zamanı

BaŐuru evraklarının eksiksiz bir şekilde Kamu SM’ye ulaŐması ve doęrulanmasının ardından en fazla 15 (on beŐ) iŐ g3n3 3erisinde sertifika baŐurusu iŐleme alınır ve sonu3landırılır.

4.3. Sertifikanın OluŐturulması

4.3.1. Sertifika OluŐturulmasında ESHS’nin İŐlevleri

B3l3m 4.2.2’de yer alan esaslar uyarınca kabul edilen sertifika baŐuruları Kamu SM tarafından iŐlenir. Kurum, iŐlem kapasitesini g3z 3n3nde bulundurarak baŐuru sırasında sertifikanın y3kleneceęi donanım olarak akıllı kart ya da HSM tercih eder.

Kurumsal Őifreleme Sertifikası, kayıp veya arıza gibi durumlarda kurumun iŐlemlerinde aksaklık yaŐanmaması amacıyla biri yedek olmak 3zere 2 adet 3retilir.

Kamu SM tarafından 3retilen kurumsal Őifreleme sertifikaları; BTK tarafından yayımlanan 2019/DK-BTD/160 sayılı Kurul Kararı Madde 5’de belirtilen h3k3m ve niteliklere uygun olarak 3retilir.

4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta y3klenen sertifika, sertifika sorumlusuna teslim edildięinde Kurumsal Őifreleme Sertifikasının oluŐturulduęu konusunda bilgilendirilmiŐ olur.

HSM cihazına sertifika y3kleme iŐlemi, HSM Cihaz Sorumlusu g3zetiminde ger3ekleŐtirilir. İŐlem sonrasında kurulum tutanaęı imzalanır ve Kurumsal Őifreleme Sertifikasının oluŐturulduęu konusunda HSM sorumlusu bilgilendirilmiŐ olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koőulu

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

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

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

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

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

4.4.3. Sertifikanın Oluőturulmasının Diđer Tarafalara Duyurulması

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

4.5. Sertifikanın ve Özel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait özel anahtarını; tabi olunan standartlar, ilgili mevzuat, Sİ/SUE dokümanı ve ilgili başvuru formu ve taahhütnamesinde yer alan koőullar ve belirlenmiş sınırlar içinde kullanmalıdır.

Sertifika sahibi, özel anahtarı yetkisiz kişilerin erişimine karşı korumakla yükümlüdür. Kurumsal Őifreleme Sertifikasına karşılık 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 Őifreleme Sertifikasının içinde yer alan açık anahtar, üçüncü kişilerce e-Yazışma Projesi 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 deęişmeden aynı anahtar çifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. Kamu SM bu işlemi gerçekleştirmez.

4.7. Sertifika Yenileme

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

4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi aşağıdaki durumlarda yapılmaktadır:

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

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildięi

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

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

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

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

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

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

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koőulu

Bölüm 4.4.1’de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2’de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diđer Tarafllara Duyurulması

Bölüm 4.4.3’te tanımlanmaktadır.

4.8. Sertifikada Bilgi Deęiőiklięi

Sertifikada bilgi deęiőiklięi, anahtar çifti hariç sertifikada yer alan bilgilerin deęiőmesi olarak tanımlanmaktadır. Sertifika ierisinde yer alan bilgilerin deęiőmesi durumda, Elektronik Mühür/Kurumsal Őifreleme Sertifikası Baővuru Formu ve Taahhütnamesi dokümanında Baővuru Nedeni "Kurum Ad/Ünvan/DETSİS ID Deęiőiklięi" seilerek yeniden baővuru yapılması gerekmektedir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildięi Durumlar

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

- Sertifika sahibi kurumun talebi
- Sertifika ierięindeki bilgilerin sahtelięinin veya yanlıőlıęının ortaya çıkması veya bilgilerin deęiőmesi
- Kurumun sertifika alma yetkisinin olmadıęının anlaşılması
- Sertifika sahibi kurumun kapanması
- Sertifika sahibi kurumun adının deęiőmesi
- Sertifika sahibi kurumun DETSİS numarasının deęiőmesi
- Özel anahtarın güvenlięinin kaybedildięinden Őüphelenilmesi
- Özel anahtarın iinde bulunduęu aracın kaybolması, alınması veya bozulması
- Akıllı kart veya HSM eriőim verisinin unutulması veya kaybedilmesi
- Sertifikanın taahhütnameler veya Sİ/SUE dokümanında belirtilen Őartlara aykırı kullanımının tespit edilmesi
- Kamu SM'ye evrakları gönderen sertifika sorumlusu/sorumlularının kurumun onayını almadıęının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM'ye bildirilmesi
- Sertifikanın hatalı üretilmesi
- Kamu SM'nin Kurumsal Őifreleme Sertifikasını imzalamak iin kullandıęı özel anahtarın bütünlüęünün bozulması veya gizlilięinin ortadan kalkması
- Kamu SM'nin iőleyiőine son verilmesi ve verilen Kurumsal Őifreleme Sertifikalarının yönetim iőlemlerinin baőka bir ESHS tarafından devamlılıęının saęlanamaması

4.9.2. Sertifika İptal BaŐvurusunu Kimler Yapabilir

Sertifika iptal baŐvurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiŐ Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından yapılabilir. Kamu SM, Bۆlüm 4.9.1’de tanımlanan tۆm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal BaŐvurusunun İŐlenmesi

Kurumsal Őifreleme Sertifikası iptal iŐlemi, kurum tarafından yetkilendirilen Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından Kamu SM resmī internet sitesinde yer alan Online İŐlemler menۆsۆ aracılıėı ile yapılır.

Kamu SM Online İŐlemler ۆzerinden yapılan iptal baŐvurusunda, Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları sisteme kimlik doėrulamasıyla giriŐ yaparak iptal talebinde bulunur. İlgili talebin ardından, Kurumsal Őifreleme Sertifikası Kamu SM sisteminde otomatik olarak iptal edilir ve DETSİS sisteminden silinir.

İptal iŐlemlerinin Kamu SM Online İŐlemler ۆzerinden yapılamadıėı durumda Kamu SM web sitesinde belirtilen yۆntemlerle iptal iŐlemi gerekleŐtirilebilir.

İptal sۆrecinin web sitesinde belirtilen yۆntemle fiziksel olarak yۆrۆtۆlmesi durumunda sۆrecin baŐlatılmasının ardından evrak asılları Kamu SM’ye ulaŐana kadar kurum yazıŐmalarında yaŐanabilecek aksaklıkların en aza indirgenmesi amacıyla Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları telefon ile aranarak iptal talebi teyit edilir ve iptali talep edilen sertifika askıya alınır. Evrak asıllarının ulaŐmasının ardından Kamu SM’ye e-posta ۆzerinden gۆnderilen 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 gemiŐe yۆnelik olarak iptal edilmez.

Kamu SM iptal bilgilerinin en kısa zamanda iŐleyerek SİL yayımlamak ve İSDUP Yanıtlayıcı’da Kurumsal Őifreleme sertifikasının durumunu iptal konumuna getirmek suretiyle kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en az Kurumsal Őifreleme sertifikasının seri numarası ile Kamu SM’nin elektronik imzasını taŐır. SİL dosyası, Kamu SM’ye ait ۆzel anahtarla imzalanır. İptal edilen Kurumsal Őifreleme Sertifikaları geerlilik sۆresinin sonuna kadar SİL iinde tutulur. Geerlilik sۆresi dolduktan sonra Kurumsal Őifreleme Sertifikası SİL iinden ıkarılır. İSDUP Yanıtlayıcı’da geerlilik sۆresi dolan iptal edilmiŐ Kurumsal Őifreleme Sertifikalarının durumu iptal edilmiŐ olarak gۆrۆnmeye devam eder.

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

4.9.4. İptal İsteėi Ertelenme Sۆresi

Bۆyle bir sۆre ۆngۆrۆlmemiŐtir.

4.9.5. İptal İsteėinin İŐlenme Sۆresi

Kamu SM, kendisine gelen geerli iptal baŐvurularını derhal iŐleme alır ve Kurumsal Őifreleme Sertifikasını en ge 24 saat ierisinde iptal eder. İptal edilen Kurumsal Őifreleme Sertifikası bilgisini bir sonraki SİL iinde yayımlar, İSDUP Yanıtlayıcı’dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi iinde iŐlenmesinin ardından bir sonraki SİL’in yayımlanma sۆresi Bۆlüm 4.9.7’de belirtilmiŐtir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliđi

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

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

Üçüncü kişiler Kurumsal Şifreleme Sertifikası geçerlilik kontrolünü yaptığı SİL dosyasının veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının Kamu SM'ye ait özel anahtarla imzalandığını kontrol eder. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri Bölüm 9.6.4'te belirtilmiştir.

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

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

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

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

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

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

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

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

4.9.11. Diđer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. Özel Anahtarın Güvenliđini Yitirmesi Durumu

Sertifika sahibi kuruma ait özel anahtarın güvenliđini yitirmesi durumunda Kurumsal Őifreleme Sertifikası iptal edilir. Kurumsal Őifreleme Sertifikasının iptal edilmesi dıŐında herhangi bir iŐlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındıđı Durumlar

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

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

Kurum sertifika yenileme talebinde bulunduysa, yeni üretilen sertifikalar askıda üretilir ve geđerlilik süreleri baŐladığında askıdan indirilerek kullanılabilir hale getirilir.

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

- Sertifika sahibi kurumun Kurumsal Őifreleme Sertifikasını kullanım dıŐı bırakmak istemesi
- Kurumsal Őifreleme Sertifikasının iptalini gerektirebilecek bir durumun ortaya çıktıđından Őüphelenildiđi durumlarda, yanlışlıkla iptalini engellemek amacıyla, Kurumsal Őifreleme Sertifikasının önce askıya alınmak istenmesi
- Aktif kullanılan geđerli sertifiakanın kayıp/çalıntı/arıza durumunda iptal kadar geđen sürede yedek sertifiakanın kullanıma ađılabilmesi

4.9.14. Sertifika Askıya Alma BaŐvurusunu Kimlerin Yapabildiđi

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

4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi

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

Askıya alınan Kurumsal Őifreleme Sertifikası için, SİL'de geđici 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 sertifika sorumlusu/sorumlularını sertifiakanın askıya alındığına dair bilgilendirir.

Kurumsal Őifreleme Sertifika Sorumlusu/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 indirmeyle ilgili bir süre kısıtı bulunmamakla birlikte kurum tarafından askıya alınan sertifikalar en az bir defa SİL'e girmeden askıdan indirilemez.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

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

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

4.10.2. Servisin Erişilebilirliği

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

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

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

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Gvenlik Denetimleri

Kamu SM, sertifika retim ve ynetim srelerinde kullanılan sistemler iin fiziksel ve evresel gvenlik politikaları uygular.

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

5.1.1. Tesis Yeri ve İnŐaatı

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

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

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

5.1.2. Fiziksel EriŐim

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

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

5.1.3. G KaynaĐı ve Havalandırma

AŐaĐıdaki g kaynakları Kamu SM iŐlevlerinin yerine getirilmesi ve srekliliĐin saĐlanması iin kullanılmaktadır:

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

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

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kâğıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur. Buna ek olarak gerekli 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 kâğıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir. Özel anahtar içeren kriptografik cihazlar endüstrideki en iyi uygulamalara göre imha edilir ve sıfırlanır. Diđer atıklar standart atık imha prosedürlerine uygun olarak imha edilir.

5.1.8. Farklı Mekanlarda Yedekleme

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

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

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

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

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

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

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

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

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleŐtiren personeldir.

5.2.2. Her İŐlem İin Gereken KiŐi Sayısı

Kamu SM, Kk SHS ve Kurumsal Őifreleme SHS'ye ait sertifika retilmesi, iptal edilmesi ve zel anahtarların baŐka bir kriptografik modl ierisine yedeklenmesi iin birden fazla yetkili personelin aynı anda hazır bulunmasını saėlar.

5.2.3. Kimlik Doėrulama ve Yetkilendirme

Kamu SM iŐleyiŐinin her adımında, iŐlemleri yerine getirecek kiŐilerin kimlik tanımlaması ve doėrulaması yapılır. Bylece her sistem birimine sadece yetkili kiŐilerin eriŐimi saėlanır. Sistemdeki bazı birimlere eriŐim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere eriŐimin saėlanabilmesi iin kimlik doėrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler erevesinde sistemde iŐlem yapılabilir.

Kamu SM sistemi iinde kimlik doėrulama gvenli donanım araları, parolalar, gizli sorular ve biyometrik veri kullanılarak gncel kriptografik yntemlerle yapılır.

Kullanıcı hesapları yetkilendirme ve ynetiminde, Kamu SM EriŐim Ynetimi Politikası temel alınmaktadır.

5.2.4. Grevlerin Ayrılmasını Gerektiren Roller

AŐaėıda verilen roller arasında grevler ayrılıėı vardır:

- Sertifika retim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında
- Sistem Denetisi ile diėer roller arasında
- Sistem Yneticisi ile Gvenlik Personeli arasında

5.3. Personel Gvenlik Kontrolleri

5.3.1. KiŐisel GemiŐ, Deneyim ve Nitelik Gerekleri

alıŐanlar sistemin iŐleyiŐ ve gvenlik gereklerini saėlayabilecek nitelikte, bilgili ve deneyimli kiŐilerden seilir. Kamu SM'nin istihdam ettirdiėi personel sistem gvenliėi, veri tabanı ynetimi, elektronik imza teknolojileri ve uygulamaları, sertifika ynetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kiŐilerden oluŐur.

5.3.2. GemiŐ AraŐırtması

alıŐanların Kamu SM'nin iŐletilmesinde gvenlik ihtiyalarının gerektirdiėi gvenilirliėe sahip olması gerekmektedir. Personelin gvenilirliėi gemiŐine ynelik yapılan araŐırtmalar ile belirlenir. İŐe alınmadan nce gemiŐe ynelik yapılan araŐırtmalarda personelin herhangi bir sebepten dolayı hkm giyip giymemiŐ olduėu araŐırtılır. Adli sicil kayıtları incelenir. Gvenlik soruŐturması biten personel iŐe baŐlatılır. İŐe baŐlayan personelin bilgi gvenliėi farkındalık eėitimleri tamamlanmadan, sistemlere eriŐimine izin verilmez.

5.3.3. Eėitim Gerekleri

alıŐanlar, Kamu SM'deki iŐlerine aktif olarak baŐlamadan nce gerekli eėitimden geirilirler. alıŐanlara verilen eėitimde Kamu SM'de uygulanan gvenlik ilkeleri, sistemin teknik ve idari iŐleyiŐi, iŐleriyle ilgili sreler, sre iindeki grev ve sorumluluklar anlatılır.

5.3.4. Srekli Eđitim Gerekleri ve Sıklıđı

Kamu SM sisteminde yapılan deđiŐikliklerin bildirilmesi amacıyla personele verilen eđitimler gerekli grldke tekrarlanır. Yeni greve baŐlayanlar iin eđitimler tekrarlanır.

Kamu SM, alıŐanlarına yılda en az bir defa, siber gvenlik ve sosyal mhendislik saldırılarına karŐı farkındalık oluŐturmak amacıyla, bilgi gvenliđi eđitimi vermektedir.

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, geerli 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 iin 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

alıŐanlara iŐleriyle ve Kamu SM sreleriyle 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 gerekleŐtirilen anahtar ve sertifika ynetimi, sistemin gvenliđi ile ilgili iŐlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diđer bir kısmı ise kâđıt zerindedir. Denetimler sırasında gerekli grldđ takdirde bu kayıtlar grevliler tarafından incelenir.

5.4.1. Kaydedilen iŐlemler

Kamu SM sisteminde aŐađıda yapılan iŐlemler ile ilgili elektronik veya kâđıt ortamda yapılan iŐlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaŐam dngs ynetimi iŐlemleri
 - Anahtar retimi
 - Anahtar yedekleme
 - Anahtar dađıtımı
 - Anahtar saklama
 - Anahtar arŐivleme
 - Anahtar yok etme
 - Kriptografik modl yaŐam dngs iŐlemleri
- Sertifika retim, yenileme, askıya alma ve iptal baŐvuruları
 - BaŐvuru sahibi tarafından sunulan belgelerin neler olduđu bilgisi
 - BaŐvuru sırasında alınan kimlik tanımlamaya yarayan belgeler

- Başvuru sırasında elektronik veya kâğıt ortamda alınan form veya belgeler
- Kâğıt belgelerin kopyalarının nerede saklandığı bilgisi
- Geçerli ve geçersiz alınan tüm başvuru bilgileri
- Sertifika yaşam döngüsü yönetimi işlemleri
 - Sertifika başvurusunun işlenmesi
 - Sertifika üretimi
 - Sertifika yenileme
 - Sertifika iptal etme
 - SİL yayımlanması
- Güvenlikle ilgili diğer işlemler
 - Sisteme başarılı veya başarısız tüm erişim denemeleri
 - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
 - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
 - Güvenlik profili değişiklikleri
 - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
 - Güvenlik cihaz/yazılım işlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
 - Kamu SM'ye ziyaretçi giriş ve çıkışı

Kayıtlarda genellikle kayıt zamanı ve kaydı oluşturan personelin ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyiŐiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı olup olmadığı kontrol edilir. Buna ek olarak, sistemde olağandışı 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 kâğıt 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 arŐivlenir. Talep edilmesi halinde kayıtlar yetkili denetŐilere sunulur.

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

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

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim seviyesi düzeyinde otomatik olarak toplanır. Otomatik kayıt toplama işlemi sistemin başlatılmasından kapanmasına kadar çalışır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan işlemi başlatan Kamu SM sertifika yönetim sistemi kullanıcısı, kaydın yapıldığına dair sistem tarafından bilgilendirilir.

5.4.8. Saldırıya Açıklığın Deđerlendirilmesi

Denetim kayıtlarının tutulduđu sistemler için Bölüm 6.5, 6.6 ve 6.7’de sözü geçen teknik güvenlik kontrolleri uygulanır.

Zafiyetlerin deđerlendirilmesiyle ilgili detaylar Kamu SM Teknik Açıklık Yönetim Politikasında belirtilmektedir. Kamu SM bu politikaya uygun şekilde periyodik olarak zafiyet taraması ve sızma testi yapar.

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

Bölüm 5.4.1’de belirtilen kayıtlara ek olarak sertifika başvurusu ve sertifika yaşam döngüsüyle ilgili, elektronik olarak ya da kâğıt üzerinde tutulan aşağıdaki belgeler arşivlenir:

- Sertifika sahibi kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Sertifika üretimi, yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kâğıt ortamda alınan formlar
- Üretilen tüm sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Zaman Damgası Sİ/SUE dokümanları
- Sertifika yönetim prosedürleri
- Başvuru Formu ve Taahhütnameler
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP senkronizasyon logları

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, deęiőtirmeyi ve silinmeyi engelleyecek Őekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalıŐanların eriŐimine kapalıdır. Arşivlerin tutulduęu ortam Bölüm 5.5.2’de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek Őekilde sečilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iŐ süreklilięi politikası gereęince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüęü kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

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

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

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

5.6. Anahtar DeęiŐimi

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 geçiŐ iŐlemleri yapılır. Anahtar deęiŐimi iŐlemleri 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 iŐlemler baŐlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM’nin eski özel anahtarla imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM özel anahtarla imzalanıyorsa, Kamu SM’nin eski özel anahtarla oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL’leri eski özel anahtarla imzalanmaya devam eder. Yeni üretilen sertifikalar için oluşturulan yeni SİL dosyası yeni Kamu SM özel anahtarıyla imzalanır.
- Kamu SM, yeniledięi anahtarları Kamu SM resmî web sitesi üzerinden üçüncü taraflarla paylaşır.

5.7. Güvenlięin Yitilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirlięin Yitilmesi Durumunun Düzeltilmesi

Güvenilirlięin yitilmesi durumlarında, sertifika yönetim sisteminin en kısa zamanda yeniden güvenli olarak çalıŐmaya baŐlaması, durumdan etkilenen tarafların haberdar edilmesi, zararlarının en aza indirgenmesi için belirlenen süreçler iŐletilir.

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

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. Özel Anahtarın Gizliliğini Kaybetmesi Durumunda İzlenecek Prosedürler

Kamu SM'nin Kurumsal Şifreleme Sertifikalarını imzalamada kullandığı özel anahtarın 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 resmî web sitesi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, Kurumsal Şifreleme Sertifikası sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluşturulan Kurumsal Şifreleme Sertifikalarına güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Kurumsal Şifreleme Sertifikaları iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Kurumsal Şifreleme Sertifikası isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM özel anahtarın 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 Şifreleme 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 Yedekleme 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 İş 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, Elektronik İmza Kanunu'nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde faaliyetlerine son verebilir. Bu durumda gerçekleştirilecek işlemler [Kamu SM Hizmetleri Sonlandırma Planı](#) dokümanında tanımlanmıştır.

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, ÇİSDUP Yanıtlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aŐađıdaki anahtar çiftleri oluşturulur:

- Kök SHS'ye ait özel ve açık anahtar
- Kurumsal Őifreleme SHS'ye ait özel ve açık anahtar
- ÇİSDUP Yanıtlayıcı'ya ait özel ve açık anahtar

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceđi güvenli odada, birden fazla eđitilmiş personelin gözetiminde, ađ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS PUB 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 dıŐarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemleri gerçekleřtiren personel tarafından onaylanır.

Özel anahtarın saklandığı kriptografik modül Bölüm 6.2.1'de belirtilen standartlara uyar.

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

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

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

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliđi 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 içerisinde veya HSM'ye yüklenerek teslim edilir. Akıllı kart, imza karŐılıđı ve resmî kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye özel anahtar ve sertifika yükleme işlemi, HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Kurulum Tutanađı doldurularak imzalanır.

Akıllı karta erişim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bađlantı protokolleri (HTTPS) kullanılmaktadır. Sertifika sorumlusunun/sorumlularının kimlik kontrolü için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde

gerçekleřtirilen kimlik doęrulaması sonrasında sertifika sahibi akıllı kart eriřim verisine eriřir. HSM'ye eriřim verisinden Kamu SM sorumlu deęildir, eriřim verisi kurum sahiplięindedir.

6.1.3. Aık Anahtarın ESHS'ye Ulařtırılması

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

Kurumsal Őifreleme Sertifikası akıllı karta yklenecekse, Kurumsal Őifreleme Sertifikaları anahtar iftleri Kamu SM tarafından retildięi iin aık anahtarın Kamu SM'ye ulařtırılması sz konusu deęildir.

6.1.4. ESHS Sertifikalarına Eriřim Saęlanması

Kamu SM'ye ait Kk SHS ve Kurumsal Őifreleme SHS sertifikaları internet ortamında tarafların eriřimine hazır bulundurulur. Sertifikanın yayımlandıęı ortamın izinsiz deęiřtirmeye ve silinmeye karřı gvenlięi saęlanır.

Kk SHS ve Kurumsal Őifreleme SHS sertifikaları, sertifikaların zet deęeri ve zet algoritması <https://kamusm.bilgem.tubitak.gov.tr> web adresi zerinden yayımlanır.

6.1.5. Anahtar Uzunlukları

Kamu SM Kk SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

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

İSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarını imzalamak iin kullanılan RSA anahtar boyu en az 2048-bittir.

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

6.1.6. Anahtar retim Parametreleri ve Kalitesinin Kontrol

Kamu SM tarafından anahtar retiminde Teblię'de belirtilen kriterlere uygun algoritmalar kullanılmaktadır. Algoritmaların gerekleřtiriminde kullanılan yntemler gerekli gvenlik kriterlerini saęlar.

6.1.7. Anahtar Kullanım Amaları

Kamu SM tarafından oluřturulan anahtarların hangi amalar iin kullanılabileceęi sertifikadaki "Anahtar Kullanımı" ve "Geniřletilmiř Anahtar Kullanımı" uzantısı ierisinde belirtilir.

Kamu SM kk anahtarı, alt kk sertifikasını ve SİL'i imzalamak iin kullanılır. Kamu SM Kurumsal Őifreleme Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. İSDUP yanıtlarının imzalanmasında alt kk ve kk tarafından yetkilendirilmiř İSDUP sertifikası kullanılır.

6.2. zel Anahtarın Korunması

6.2.1. Kriptografik Modl Standartları

Kamu SM'ye ait zel anahtarlar gvenli yazılım ve/veya donanım kullanılarak retilir, gvenli kriptografik modl iinde saklanır ve geerli olduęu sre boyunca bu modl dıřına ıkmaz.

Kriptografik modl ařaęıda belirlenen gvenlik iřlevlerine sahiptir:

- Özel anahtarın geerlilik sűresi boyunca gizlilik ve bűtűnlűğűnű saėlar.
- Modűle eriŐimde kimlik belirleme ve doėrulama iŐlevlerini yerine getirir.
- EriŐim yetkisi birden fazla kiŐinin kontrolűnde olacak Őekilde tanımlanabilir.
- Sistem kullanıcısına tanımlanan roller doėrultusunda, verdiėi hizmetlere eriŐimi sınırlar.
- Dűzgűn alıŐtıėı test edilebilir, test sırasında hata oluŐtuėunda güvenli duruma geer.
- Modűle izinsiz eriŐim ve kullanım ile tahrifata yol aabilecek her tűrlű fiziksel űnlem alınmıŐtır.
- Yetkisiz eriŐime teŐebbűs edilmesi durumunda, modűl iindeki veriyi siler.
- Özel anahtarın yedeėinin güvenli biimde alınmasına olanak verir.
- Sertifika sahibinin özel anahtarının iinde bulunduėu akıllı kart veya HSM cihazı, özel anahtarın donanım dıŐına ıkmasını engelleyen ve donanıma eriŐimi parola ile saėlayan teknik űzelliklere sahiptir.
- Kriptografik modűl ve sertifika sahibine ait akıllı kart veya HSM cihazı, Tebliė'de belirtilen güvenlik standartlarını saėlar.

6.2.2. Özel Anahtara Birden Fazla KiŐi Kontrolűnde EriŐim

Kamu SM'ye ait özel anahtarın bulunduėu odaya eriŐim aynı anda 2 (iki) yetkili personel tarafından saėlanmaktadır. Yetkili kiŐiler dıŐında eriŐim gerekli kontroller vasıtasıyla engellenir.

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Dűzenlenmesine gerek duyulmamıŐtır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait özel anahtarın yedeėinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan özel anahtar iin saėlanan güvenlik ile eŐdeėer güvenlik űnlemleri altında yapılır. Yedeklenen özel anahtar yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı iinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan özel anahtarın bulunduėu ortam ile aynı güvenlik Őartlarına sahip ortamda saklanır. Sertifika sahiplerine ait özel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın ArŐivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait özel anahtarlar arŐivlenmez. Kullanım sűreleri sonunda geri dűnűŐsűz Őekilde silinir.

6.2.6. Özel Anahtarın Kriptografik Modűle Yűklenmesi

Kamu SM'ye ait özel anahtar űretilikten hemen sonra kriptografik modűle yűklenir. İŐlem, güvenilir yűntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Sertifika sahiplerine ait özel anahtarlar, sadece yetkili personelin kontrolűnde akıllı kart veya HSM cihazına Őifrelenerek yűklenir. Özel anahtarların varsa kopyaları yűklemelerinin tamamlanmasının ardından sistemden silinir.

6.2.7. Özel Anahtarın Kriptografik Modűlde Saklanması

Kamu SM'ye ait özel anahtarlar, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı iinde tutulur. Özel anahtarın yedekleme amacı haricinde cihaz dıŐına

çıkması engellenmiştir. Özel anahtarlar kriptografik modül içinde güvenli algoritma ve yöntemlerle şifreli olarak saklanır.

Sertifika sahibinin özel anahtarı, kendisine ait akıllı kart veya HSM cihazı içinde saklanır, başka bir ortamda bulunmaz. Kamu SM, sertifika sahiplerine ait özel anahtarları kendi sistemi içinde saklamaz.

6.2.8. Özel Anahtara Erişim

Kamu SM'nin özel anahtarlarına erişim birden fazla yetkili personelin ortak denetimi altındadır. Özel anahtarın bulunduğu odaya giriş için, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin doğrulanamadığı durumlarda özel anahtarın bulunduğu odaya erişim sağlanamaz.

Özel anahtar kriptografik modül içinde şifreli durumdayken erişime kapalıdır. Erişime açılması için erişimi sağlayan verinin modüle sunulması gerekir. Özel anahtarın erişime açılması ve kullanılabilir duruma getirilmesi birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahibine ait özel anahtar, akıllı kart veya HSM cihazı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Aktivasyon, erişim verisi ile sağlanır.

6.2.9. Özel Anahtara Erişimin Kesilmesi

Kamu SM'nin özel anahtarları imzalama için kullanıldıktan sonra oturum kapandığında veriye erişim otomatik olarak kesilir ve bir dahaki kullanımına kadar şifrelenerek erişime kapalı tutulur. Erişimin yeniden sağlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden işletilmesi 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 kilitletlenir ve araca erişim sağlanamaz.

6.2.10. Özel Anahtarın Yok Edilmesi

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

Sertifika sahiplerine ait özel anahtarlar, 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 Őifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Kurumsal Őifreleme Sertifikasının kullanım süresinin dolmasıyla ya da Kurumsal Őifreleme 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 Őifreleme Sertifikalarının son kullanma tarihi, Kurumsal Őifreleme SHS Sertifikasının son kullanma tarihini aşamaz.

6.4. Aktivasyon Verileri

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

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

6.4.1. Aktivasyon Verilerinin Oluşturulması

Kamu SM sistemi içinde kullanılan aktivasyon 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 rastgele üretilir.

6.4.2. Aktivasyon Verilerinin Korunması

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

Sertifika sahibi kuruma ait erişim parolaları, iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibi tarafından belirlenir.

Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Aktivasyon Verileri ile İlgili Diğer Konular

Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar Güvenliđi Kontrolleri

6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereklere

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 sürekliliđinin 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 Prosedürüne göre kontrol edilir.

6.5.2. Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler aŐağıda verilmiştir:

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

6.6.2. Güvenlik Yönetimi Kontrolleri

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

6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Aę Güvenlięi Kontrolleri

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

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

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

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

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

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

6.8. Zaman Damgası

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

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

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

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

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

Kamu SM tarafından verilen Kurumsal Őifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geerlilik tarihi, ilgili aık 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 ierir. Kurumsal Őifreleme Sertifikasının ieriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine baėlı olarak belirlenir.

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

Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları

Sertifika Uzantısı	Kritik Uzantı	Aıklama
Temel Kısıtlar ¹	HAYIR	Sertifikanın son kullanıcı sertifikası olduėu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
Yetkili Anahtar Tanımlayıcısı ²	HAYIR	Kamu SM'ye ait Kurumsal Őifreleme SHS aık anahtarının SHA-1 zet ıktısından oluşur.
Sertifika Anahtar Tanımlayıcısı ³	HAYIR	Sertifikanın ieriğindeki "subjectPublicKey" alanının "BIT STRING" olarak deėerinin SHA-1 zet ıktısından oluşur.
Anahtar Kullanımı ⁴	EVET	Anahtarların sadece Őifreleme amalı kullanıldığına ifade edilmesi iin "keyEncipherment" [anahtar Őifreleme] alanı seilmiştir.
SİL Daėıtım Noktaları ⁵	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl
Yetkili Bilgi EriŐimi ⁶	HAYIR	http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt http://ksifrelemeocspv1.kamusm.gov.tr/
Sertifika İlkeleri ⁷	HAYIR	Kamu SM Sİ dokmanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.11) ile SUE dokmanının bulunduėu

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

⁴ KeyUsage

⁵ CRLDistributionPoints

⁶ AuthorityInformationAccess

⁷ CertificatePolicies

		http://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan Kurumsal Őifreleme Sertifikası ibaresine ait metni içerir.
Geniřletilmiş 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.

Sertifika sahiplerine ait anahtar çiftleri RSA algoritmasına sahiptir.

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.

⁸ ExtendedKeyUsage

⁹ CN: Common Name [Genel isim]

¹⁰ Serial: Serial Number [Seri Numarası]

¹¹ C: Country [Ülke]

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/SUE’de belirtilen ilke ve uygulama esasları çerçevesinde Kurumsal Őifreleme Sertifikalarını kullanarak işlem yapar.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

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

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

¹² Certificate Policies

¹³ Policy Identifier

7.3.2. ŐİSDUP Uzantıları

ŐİSDUP sorguları aŐağıdaki bilgileri iermelidir:

- Protokol versiyonu
- Hedef sertifika belirteci (kullanılan zetleme algoritması, sertifikayı veren ESHS'nin DN zeti, sertifikayı veren ESHS'nin aık anahtarının zeti, sertifika seri numarası)

ŐİSDUP yanıtları aŐağıdaki bilgileri iermektedir:

- Versiyon bilgisi
- Yanıtlayıcının adı
- Her bir sertifika iin cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geerlilik suresi)
- Kullanılan imza algoritmasının nesne tanımlama numarası
- ŐİSDUP Yanıtlayıcı imzası

Btn geerli ŐİSDUP cevapları ŐİSDUP Yanıtlayıcı tarafından imzalanır. Geersiz ŐİSDUP sorguları iin dnen hata mesajları imzalanmaz.

evrim İi Sertifika Durum Protokol RFC 6960'ta tarif edilen "ŐİSDUP" formatını destekler. ŐİSDUP Yanıtlayıcı'dan alınan cevaplar aŐağıdaki Őekilde deęerlendirilir:

Good [iyi]: Sertifika geerli konumdadır.

Bad [kt]: Sertifika iptal edilmiŐtir (askı durumu da dahil).

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

RFC 6960, ŐİSDUP sorguları ve yanıtları ierisinde bazı uzantıların kullanımına imkn verir. Tekrarlama (replay) saldırılarını nlemek iin sorgu ve yanıtı birbirine baęlayan "nonce" uzantısı bunlardan biridir. Kamu SM ŐİSDUP Yanıtlayıcı, "nonce" uzantısını desteklemektedir. RFC 6960'da belirtilen dięer uzantılar ŐİSDUP yanıt formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

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

Kamu SM ek olarak, ISO/IEC 27001 Bilgi Gvenlięi Ynetim Sistemi (BGYS) standardına uygun olarak hizmet verir ve standart gereęi dzenli olarak i ve dıŐ denetimlere tabi tutulur. Kamu SM i iŐleyiŐini denetlemek iin ayrıca i denetimler geerleŐtirilir.

8.1. Uygunluk Denetiminin Sıklıęı

BTK, gerekli grdę durumlarda re'sen denetim yapabilir.

Kamu SM, ISO/IEC 27001 Bilgi Gvenlięi Ynetim Sistemi (BGYS) standardı gereęince yılda bir defa uygunluk denetimi geirir. Her  yılda bir sertifika yenilenir.

İ denetim, yılda en az 1 (bir) defa olmak zere geerleŐtirilir.

8.2. Denetinin Nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiŐ olan BTK tarafından geerleŐtirilir.

ISO/IEC 27001 BGYS'nin denetimi akredite edilmiŐ kuruluşlarca geerleŐtirilir.

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

8.3. Denetçinin Denetlenen Tarafla Olan İliŐkisi

BTK, kanun geređi tđm ESHS'leri denetlemekle yetkili kılınmıŐ dđzenleyici kurumdur.

ISO/IEC 27001 BGYS'nin denetimi bađımsız ve akredite edilmiŐ kuruluşlarca gerçekteŐirilir.

İç denetim, Sİ dokđmanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrđbeli ESHS personeli tarafından gerçekteŐirilir. İç denetim için seçilen denetçiler denetlenecek birimden seçilmez.

8.4. Denetimin Kapsamı

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

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

8.5. Yetersizliđin Tespiti Durumunda Yapılacaklar

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

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

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

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, Kamu SM üst yđnetimine 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 şekli Kamu SM web sitesinde bildirilir.

Kamu SM'nin özel anahtarının çalınması, kaybolması, gizliliđinin veya güvenilirliđinin ortadan kalkması, sertifika ilkelerinin deđiŐmesi ya da Kurumsal Őifreleme Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadıđı 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 resmî 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 aracılıđıyla duyurma hizmeti için, sertifika sahibi kurumdan veya üçüncü kişilerden ücret talep etmez.

9.1.4. Diğer Servis Ücretleri

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

Kamu SM, kuruma ait özel anahtar ve sertifikanın saklandığı akıllı kartın teminini kendi imkanlarıyla sağlayabilir. Kurumsal Şifreleme 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 Şifreleme Sertifikası üretimi yapılmayabilir veya mevcut sertifika kullanım dışı bırakılabilir.

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

9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi 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. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

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

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. KiŐisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

Kamu SM verdiđi hizmetlerde sertifika sahiplerinin ve diđer paydaŐların kiŐisel verilerinin gizliliđini ilgili mevzuat ve 6698 sayılı KiŐisel Verilerin Korunması Kanunu (KVKK) kapsamındaki mer'i mevzuata uygun olarak sađlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

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

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kurumsal Őifreleme Sertifikası içeriđinde bulunan bilgiler, taraflar arası sözleşmelerde aksi belirtilmediđi sürece gizli deđildir.

9.4.4. Gizli Bilginin Korunma Sorumluluđu

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

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

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

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diđer BaŐlıklar

Düzenlenmesine gerek duyulmamıŐtır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yükümlölükler

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

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

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlölükleri

ESHS olarak Kamu SM'nin yükümlölükleri aşağıda belirtilmiştir:

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

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

9.6.2. Kayıt Birimi Ykmllkleri

Kayıt biriminin sorumlulukları Őunlardır:

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

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

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

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

- Kurum adına dzenlenen Kurumsal Őifreleme Sertifikası retildiđinde sertifikadaki bilgilerin dođruluđunu kontrol etmek
- SUE Blm 6.2.1’de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- zel anahtarın gvenliđini sađlamak, kendisine ait zel anahtarın iinde bulunduđu akıllı kart veya HSM cihazının ve eriŐim verisinin gizliliđini korumak, bunları baŐkasına kullandırmamak ve bu konuda gerekli tedbirleri almak
- İnternet veya ađrı merkezi zerinden sertifika iŐlemlerini yapabilmesi iin kullandıđı parolalarının gizliliđini ve gvenliđini sađlamak
- zel anahtarın iinde bulunduđu akıllı kart veya HSM’nin kaybolması, alınması veya zel anahtarın gizliliđinin yitirildiđinden Őphelenmesi durumunda Kurumsal Őifreleme Sertifikasının iptal edilmesi iin Blm 3.4’te belirtilen kanallar zerinden Kamu SM’ye en kısa zamanda baŐvurmak
- Akıllı kart veya HSM eriŐim verisini ve sertifika iŐlemlerinde kullandıđı diđer parolaları dzenli olarak deđiŐtirmek
- Kurumsal Őifreleme Sertifikası ieriđinde bulunan bilgilerin deđiŐmesi durumunda derhal sertifikanın iptal edilmesi iin Kamu SM’ye baŐvurmak
- Kurumsal Őifreleme Sertifikası baŐvurusu sırasında ve sertifikanın geerlilik sresi boyunca beyan ettiđi bilgilerde meydana gelen deđiŐiklikleri derhal Kamu SM’ye bildirmek
- İptal olmuŐ, kullanıma aılmamıŐ, askıya alınmıŐ veya geerlilik sresi dolmuŐ Kurumsal Őifreleme Sertifikası ile iŐlem yapmamak
- Kurumsal Őifreleme Sertifikası ile iliŐkili zel anahtarını imzalama amacıyla kullanmamak.

Sertifika sahibi kurum, Kamu SM Kurumsal Őifreleme Sertifikası Sİ/SUE dokmanlarında belirtilen Őartları okuduđunu, baŐvuru sreci ve sertifika geerliliđi boyunca taahhtname, ilgili mevzuatlar ile Sİ/SUE dokmanında belirtilen Őartlara uygun olarak hareket edeceđini kabul ve taahht eder. Ykmllklerin ihlali nedeniyle nc kiŐilerin/kurumun zarara uđraması halinde TBİTAK BİLGEM’in demek zorunda olduđu tazminatlarla ilgili sertifika sahibine rcu hakkı saklıdır.

9.6.4. nc KiŐilerin Ykmllkleri

nc kiŐiler, Kurumsal Őifreleme Sertifikasıyla iŐlem yapmadan nce sertifikanın aŐađıda belirtilen geerlilik kontrollerini yapmakla ykmldr:

- Kurumsal Őifreleme Sertifikasının tanımlanan veriliŐ amacına uygun olarak kullanıldıđını dođrulamak
- Kurumsal Őifreleme Sertifikasının kullanım sresinin 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 btnlđn Kamu SM’nin ilgili sertifikası iinde mevcut olan aık anahtarını kullanarak dođrulamak
- Kurumsal Őifreleme Sertifikasının dođruluđunu Kurumsal Őifreleme SHS sertifikasının iinde mevcut olan aık anahtarını kullanarak dođrulamak
- Kurumsal Őifreleme SHS sertifikasının dođruluđunu Kk SHS sertifikasının iinde mevcut olan aık anahtarını kullanarak dođrulamak
- Kk SHS sertifikasının btnlđn sertifika zet deđerini kontrol etmek suretiyle dođrulamak

- Sertifika sahibinin Kurumsal Őifreleme Sertifikasının içindeki açık anahtarına karşılık gelen özel anahtara sahip olduğunu doğrulamak

9.6.5. Diđer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

Kamu SM'ye sertifika başvurusunda bulunan kurumun yükümlülükleri aşağıda belirtilmiştir:

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

9.6.5.2. Kurum Sertifika Sorumlularının Yükümlülükleri

Kurum adına Kurumsal Őifreleme Sertifikası başvurusunda bulunan Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının yükümlülükleri aşağıda belirtilmiştir:

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

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının sertifika teslimatları ile ilgili yükümlülükleri taahhütnamelerde belirtilmiştir.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yükümlülük, taahhütnamelerde belirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları ilgili mevzuatta belirtilen şartlar ile sınırlıdır. Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar taahhütnamelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları 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 gerçekleşmiş hak ve alacakları korunmak suretiyle tasfiye edilir.

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahibi kurum, taahhütnamelere uygun olarak Kamu SM ile iş birliği içinde çalışır.

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

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ/SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği taahhütnamelerdeki şartları yerine getirir.

9.10.1. AnlaŐma Suresi

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

9.10.2. AnlaŐmanın Sona Ermesi

Kamu SM, imzalanan taahhütnameleri aŐađıdaki durumlarda sonlandırılabilir:

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

9.10.3. AnlaŐmanın Sona Ermesinin Etkileri

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

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

9.11. Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme

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

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

9.12. DeđiŐiklik Halleri

9.12.1. DeđiŐiklik Metotları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

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

9.12.3. Nesne Tanımlama Numarasının Deęişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

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

9.14. Uygulanacak Hukuk

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

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Çeşitli Hükümler

9.16.1. Tüm Sözleşmeler

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

9.16.2. Atama

Düzenlenmesine gerek duyulmamıştır.

9.16.3. Bölünebilirlik

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

9.16.4. İcra (Avukatlık Ücretleri ve Haklardan Feragat)

Düzenlenmesine gerek duyulmamıştır.

9.16.5. Mücbir Sebepler

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

9.17. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI

Alan	Deęer
Sürüm	V3
Seri Numarası	00ed1db82e01d6
İmza Algoritması	SHA-384 ile ECDSA { 1 2 840 10045 4 3 3 }
Sertifikayı Veren	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, 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, 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 Niteleyici= http://depo.kamusm.gov.tr/ilke</p> <p>[1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.</p>
SİL Dađıtım Noktaları	<p>[1]SİL Dađıtım Noktası Dađıtım Noktası Adı: Tam Ad: URL=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	En fazla 64 bit rassal sayı içeren tam sayı
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	<p>CN = Kurumsal Őifreleme Sertifika Hizmet Sađlayıcısı - Sürüm 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 içerięindeki "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>
-----------------------	---