

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŐİFRELEME SERTİFİKA İLKELERİ

Doküman Kodu

POL.05.02

Revizyon No

09

Revizyon Tarihi

13.04.2026

TASNİF DIŐI

REVİZYON GEÇMİŐI

Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk yayın	15.01.2021
01	Doküman formatı güncellenmiştir.	18.01.2021
02	Sertifika yenileme süreci güncellenmiştir.	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 Taahhütnamesi" olarak deđiŐtirilmiştir.	07.01.2022
04	Sertifika üretiminin iki kiŐinin kontrolünde yapılması gerektiđi ile ilgili ibare kaldırılmıştır.	17.02.2022
05	Sertifika İptal Listesi yayımlama gecikmesi süresi kısmında güncelleme yapılmıştır. Doküman genelinde ek düzeltmeler uygulanmıştır.	20.10.2022
06	Sertifika sorumluları arasındaki asıl/yedek ayrımı kaldırılmıştır. Sertifikanın askıda kalma süresi ile ilgili ifadeler düzenlenmiştir. Dokümanda referans verilen mevzuatlar için tanım eklenmiştir. Kullanılmayan "Kamu SM Taahhütnamesi" ve "Sözleşme" ibareleri kaldırılmıştır. HSM'li üretimlerde istek dosyalarının parola korumalı zip içerisinde iletimi ile ilgili ifade eklenmiştir. Doküman genelinde editöryal düzenlemeler yapılmıştır.	06.03.2023
07	Tanımlarda güncelleme yapılmıştır. KVKK linki güncellenmiştir. Genel gözden geçirme kapsamında metinsel düzenlemeler gerçekleştirilmiştir.	22.04.2024
08	e-Yazışma Teknik Rehberi'nin 2.1 versiyonunun yayımlanması dođrultusunda düzenlemeler yapılmıştır.	05.08.2024
09	Açık anahtar yerine imza dođrulama verisi; özel anahtar yerine imza oluŐturma verisi kavramları kullanılmıştır.	13.04.2026

İÇİNDEKİLER

1. GİRİŐ	9
1.1. Genel Bakıő	9
1.2. Doküman Adı ve Tanımı	10
1.3. Sistem Bileőenleri	10
1.3.1. Elektronik Sertifika Hizmet Saėlayıcısı	10
1.3.2. Kayıt Birimleri	10
1.3.3. Sertifika Sahipleri	10
1.3.4. Üçüncü Kiőiler	10
1.3.5. Diėer Bileőenler	10
1.4. Sertifika Kullanımı	10
1.4.1. Uygun Olan Sertifika Kullanımı	10
1.4.2. Sertifika Kullanımının Sınırları	11
1.5. Uygulama Esaslarının Yönetimi	11
1.5.1. Doküman Yönetimi	11
1.5.2. İletişim Bilgileri	11
1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluėunu Belirleyen Kiő	11
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri	11
1.6. Tanımlar ve Kısaltmalar	11
1.6.1. Tanımlar	11
1.6.2. Kısaltmalar	13
2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ	14
2.1. Bilgi Depoları	14
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması	14
2.3. Yayım Sıklığı ve Zamanı	14
2.4. Eriőim Kontrolleri	14
3. KİMLİK BELİRLEME VE DOėRULAMA	14
3.1. İsimlendirme	14
3.1.1. İsim Alanı Tipleri	14
3.1.2. Kimlik Bilgilerinin Teőhise Elverişli Olması	15
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması	15
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması	15
3.1.5. Kimlik Bilgilerinin Tekilliliėi	15
3.1.6. Markanın Tanınması, Doėrulanması ve Rolü	15
3.2. İlk Kimlik Doėrulama	15
3.2.1. İmza Oluőturma Verisi Sahipliliėinin Kanıtlanması	15
3.2.2. Kurumsal Kimliėin Belirlenmesi	15
3.2.3. Kiőisel Kimliėin Belirlenmesi	15
3.2.4. Doėrulanmayan Sertifika Sahibi Bilgileri	15
3.2.5. Yetkinin Doėrulanması	16
3.2.6. Uyum Kriterleri	16
3.3. Sertifika Yenileme İsteėinde Kimlik Doėrulama	16
3.3.1. Olaėan Sertifika Yenileme İsteėinde Kimlik Doėrulama	16
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doėrulama	16
3.4. Sertifika İptal İsteėinde Kimlik Doėrulama	16

4.	SERTİFİKA YAŐAM DÖNGÜSÜ İŐLEVSEL GEREKLİLİKLERİ	16
4.1.	Sertifika Başvurusu	16
4.1.1.	Sertifika Başvurusunu Kimlerin Yapabildiđi	16
4.1.2.	Kayıt İőlemleri ve Sorumluluklar	16
4.2.	Sertifika Başvurusunun İőlenmesi	17
4.2.1.	Kimlik Tanımlama ve Doğrulama İőlevlerinin Yerine Getirilmesi	17
4.2.2.	Sertifika Başvurusunun Kabul veya Reddi	17
4.2.3.	Sertifika Başvurusunun İőlenme Zamanı	17
4.3.	Sertifikanın OluŐturulması	17
4.3.1.	Sertifika OluŐturulmasında ESHS'nin İőlevleri	17
4.3.2.	Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi	17
4.4.	Sertifikanın Kabulü	17
4.4.1.	Sertifikanın Kabul KoŐulu	17
4.4.2.	Sertifikanın ESHS Tarafından Yayımlanması	17
4.4.3.	Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması	17
4.5.	Sertifikanın ve İmza OluŐturma Verisinin Kullanımı	18
4.5.1.	Sertifika Sahibinin Sertifika ve İmza OluŐturma Verisi Kullanımı	18
4.5.2.	Üçüncü KiŐilerin Sertifika İmza Doğrulama Verisi Kullanımı	18
4.6.	Sertifika Süresinin Uzatılması	18
4.7.	Sertifika Yenileme	18
4.7.1.	Sertifikanın Yenileme KoŐulları	18
4.7.2.	Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi	18
4.7.3.	Sertifika Yenileme Başvurusunun İőlenmesi	18
4.7.4.	Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi	18
4.7.5.	Sertifika Yenileme Sonrası Kabul KoŐulu	18
4.7.6.	Sertifika Yenileme Sonrası Sertifikanın Yayımlanması	18
4.7.7.	Sertifika Yenilemenin Diđer Tarafra Duyurulması	18
4.8.	Sertifikada Bilgi DeđiŐikliđi	18
4.9.	Sertifikanın İptali ve Askıya Alınması	19
4.9.1.	Sertifikanın İptal Edildiđi Durumlar	19
4.9.2.	Sertifika İptal Başvurusunu Kimler Yapabilir	19
4.9.3.	Sertifika İptal Başvurusunun İőlenmesi	19
4.9.4.	İptal İsteđi Ertelenme Süresi	19
4.9.5.	İptal İsteđinin İőlenme Süresi	19
4.9.6.	Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol Gerekliliđi	19
4.9.7.	Sertifika İptal Listesi Yayımlama Sıklıđı	19
4.9.8.	Sertifika İptal Listesi Yayımlama Gecikme Süresi	19
4.9.9.	Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti	20
4.9.10.	Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi	20
4.9.11.	Diđer Sertifika Durum Bildirim Yöntemleri	20
4.9.12.	İmza OluŐturma Verisinin Güvenliđini Yitirmesi Durumu	20
4.9.13.	Sertifikanın Askıya Alındıđı Durumlar	20
4.9.14.	Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi	20
4.9.15.	Sertifika Askıya Alma Başvurusunun İőlenmesi	20
4.9.16.	Askıda Kalma Süresi	20
4.10.	Sertifika Durum Servisleri	20

4.10.1.	İřletimsel Özellikleri.....	20
4.10.2.	Servisin Eriřilebilirliđi.....	21
4.10.3.	İsteđe Bađlı Özellikler.....	21
4.11.	Sertifika Sahipliđinin Sona Ermesi.....	21
4.12.	Anahtar Yeniden Üretme	21
5.	YÖNETİM, İŐLEMSEL VE FİZİKSEL KONTROLLER.....	21
5.1.	Fiziksel Güvenlik Denetimleri	21
5.1.1.	Tesis Yeri ve İnřaati.....	21
5.1.2.	Fiziksel Eriřim	21
5.1.3.	Güç Kaynađı ve Havalandırma.....	21
5.1.4.	Su Baskınları.....	22
5.1.5.	Yangın Önleme ve Korunma.....	22
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması	22
5.1.7.	Atıkların Yok Edilmesi.....	22
5.1.8.	Farklı Mekanlarda Yedekleme.....	22
5.2.	Prosedürel Kontroller	22
5.2.1.	Güvenilir Roller	22
5.2.2.	Her İřlem İin Gereken Kiři Sayısı.....	22
5.2.3.	Kimlik Dođrulama ve Yetkilendirme.....	22
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	22
5.3.	Personel Güvenlik Kontrolleri	22
5.3.1.	Kiřisel Geçmiř, Deneyim ve Nitelik Gerekleri	22
5.3.2.	Geçmiř Arařtırması.....	22
5.3.3.	Eđitim Gerekleri	23
5.3.4.	Sürekli Eđitim Gerekleri ve Sıklıđı.....	23
5.3.5.	Görev Deđiřim Sıklıđı ve Sırası.....	23
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	23
5.3.7.	Anlařmalı Personel Gereksinimleri	23
5.3.8.	Sađlanan Dokümantasyon.....	23
5.4.	Denetim Kayıtları	23
5.4.1.	Kaydedilen İřlemler	23
5.4.2.	Kayıtların İncelenme Sıklıđı	23
5.4.3.	Kayıtların Saklanma Süresi	24
5.4.4.	Kayıtların Korunması	24
5.4.5.	Kayıtların Yedeklenmesi	24
5.4.6.	Kayıtların Toplanması.....	24
5.4.7.	Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi.....	24
5.4.8.	Saldırıya Açıklıđın Deđerlendirilmesi.....	24
5.5.	Kayıt Arřivleme	24
5.5.1.	Arřivlenen Kayıt Bilgileri.....	24
5.5.2.	Arřivlerin Tutulma Süresi	24
5.5.3.	Arřivlerin Korunması	24
5.5.4.	Arřivlerin Yedeklenmesi	24
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri.....	24
5.5.6.	Arřivlerin Toplanması.....	24
5.5.7.	Arřiv Bilgilerinin Elde Edilme ve Dođerulanma Metodu.....	25

5.6.	Anahtar DeęiŐimi.....	25
5.7.	Güvenlięin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	25
5.7.1.	Güvenilirlięin Yitirilmesi Durumunun Düzeltilmesi	25
5.7.2.	Donanım, Yazılım veya Veri Bozulması	25
5.7.3.	İmza OluŐturma Verisinin Gizlilięinin Kaybetmesi Durumunda İzlenecek Prosedürler	25
5.7.4.	Arıza Sonrası Yeniden ÇalıŐırlık	25
5.8.	Sertifika Hizmetlerinin Sonlandırılması.....	25
6.	TEKNİK GÜVENLİK KONTROLLERİ.....	25
6.1.	Anahtar Çifti Üretimi ve Kurulumu	25
6.1.1.	Anahtar Çifti Üretimi	25
6.1.2.	Sertifika Sahibine İmza OluŐturma Verisinin UlaŐtırılması.....	26
6.1.3.	İmza Doğrulama Verisinin ESHS'ye UlaŐtırılması.....	26
6.1.4.	ESHS Sertifikalarına EriŐim Saęlanması	26
6.1.5.	Anahtar Uzunlukları.....	26
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü.....	27
6.1.7.	Anahtar Kullanım Amaçları	27
6.2.	İmza OluŐturma Verisinin Korunması	27
6.2.1.	Kriptografik Modül Standartları	27
6.2.2.	İmza OluŐturma Verisine Birden Fazla KiŐi Kontrolünde EriŐim.....	27
6.2.3.	İmza OluŐturma Verisinin Yeniden Elde Edilmesi	27
6.2.4.	İmza OluŐturma Verisinin Yedeklenmesi	27
6.2.5.	İmza OluŐturma Verisinin ArŐivlenmesi	27
6.2.6.	İmza OluŐturma Verisinin Kriptografik Modüle Yüklenmesi.....	27
6.2.7.	İmza OluŐturma Verisinin Kriptografik Modülde Saklanması	27
6.2.8.	İmza OluŐturma Verisine EriŐim	28
6.2.9.	İmza OluŐturma Verisine EriŐimin Kesilmesi.....	28
6.2.10.	İmza OluŐturma Verisinin Yok Edilmesi	28
6.2.11.	Kriptografik Modülün Deęerlendirilmesi	28
6.3.	Anahtar Çifti Yönetimiyle İlgili Dięer Konular.....	28
6.3.1.	İmza Doğrulama Verisinin ArŐivlenmesi	28
6.3.2.	İmza OluŐturma ve Doğrulama Verilerinin Kullanım Süreleri	29
6.4.	Aktivasyon Verileri	29
6.4.1.	Aktivasyon Verilerinin OluŐturulması	29
6.4.2.	Aktivasyon Verilerinin Korunması.....	29
6.4.3.	Aktivasyon Verileri ile İlgili Dięer Konular	29
6.5.	Bilgisayar Güvenlięi Kontrolleri	29
6.5.1.	Bilgisayar Güvenlięi ile İlgili Teknik Gereker	29
6.5.2.	Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi.....	29
6.6.	YaŐam Döngüsü Teknik Kontrolleri.....	29
6.6.1.	Sistem GeliŐtirme Kontrolleri	29
6.6.2.	Güvenlik Yönetimi Kontrolleri.....	29
6.6.3.	YaŐam Döngüsü Güvenlik Kontrolleri	30
6.7.	Aę Güvenlięi Kontrolleri.....	30
6.8.	Zaman Damgası.....	30
7.	SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ.....	30

7.1.	Sertifika Biçimi	30
7.1.1.	Sürüm Numarası	30
7.1.2.	Sertifika Uzantıları	30
7.1.3.	Algoritma ve Nesne Tanımlayıcılar	30
7.1.4.	İsim Alanı Biçimleri	30
7.1.5.	İsim Kısıtları.....	30
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası	30
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	31
7.1.8.	İlke Niteleyiciler	31
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi	31
7.2.	Sertifika İptal Listesi Biçimi	31
7.2.1.	Sürüm Numarası	31
7.2.2.	Sertifika İptal Listesi Uzantıları.....	31
7.3.	Çevrim İçi Sertifika Durum Protokolü Biçimi	31
7.3.1.	Sürüm Numarası	31
7.3.2.	ÇİSDUP Uzantıları.....	31
8.	UYGUNLUK DENETİMLERİ	31
8.1.	Uygunluk Denetiminin Sıklığı	31
8.2.	Denetçinin Nitelikleri.....	32
8.3.	Denetçinin Denetlenen Tarafı Olan İlişkisi	32
8.4.	Denetimin Kapsamı	32
8.5.	Yetersizliğin Tespiti Durumunda Yapılacaklar	32
8.6.	Sonucun Bildirilmesi	32
9.	DIŐER İŐLER VE HUKUKSAL MESELELER	32
9.1.	Ücretlendirme	32
9.1.1.	Sertifika OluŐturma ve Yenileme Ücreti.....	32
9.1.2.	Sertifika EriŐim Ücreti	33
9.1.3.	İptal Durum Kaydına EriŐim Ücreti.....	33
9.1.4.	Diđer Servis Ücretleri	33
9.1.5.	İade Ücreti.....	33
9.2.	Finansal Sorumluluk	33
9.2.1.	Sigorta Kapsamı	33
9.2.2.	Diđer Varlıklar	33
9.2.3.	Sertifika Mali Sorumluluk Sigortası.....	33
9.3.	Ticari Bilginin Korunması	33
9.3.1.	Gizli Bilginin Kapsamı.....	33
9.3.2.	Gizlilik Kapsamında Olmayan Bilgiler.....	33
9.3.3.	Gizli Bilginin Korunma Sorumluluđu	33
9.4.	Kişisel Bilginin Gizliliđi.....	34
9.4.1.	Gizlilik Planı	34
9.4.2.	Gizli Olarak Tanımlanan Bilgiler	34
9.4.3.	Gizli Olarak Tanımlanmayan Bilgiler	34
9.4.4.	Gizli Bilginin Korunma Sorumluluđu	34
9.4.5.	Gizli Bilginin Kullanımına İzin Verilmesi.....	34
9.4.6.	Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması	34

9.4.7.	Diđer BaŐlıklar	34
9.5.	Telif Hakları.....	34
9.6.	Temsil Hakkı ve Yüklümlülükler	35
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yüklümlülükleri	35
9.6.2.	Kayıt Birimi Yüklümlülükleri.....	35
9.6.3.	Sertifika Sahibinin Yüklümlülükleri.....	35
9.6.4.	Üçüncü KiŐilerin Yüklümlülükleri	35
9.6.5.	Diđer BileŐenlerin Yüklümlülükleri.....	35
9.7.	Yüklümlülüklerden Feragat.....	35
9.8.	Sorumlulukla İlgili Sınırlamalar.....	35
9.9.	Tazminat Halleri	36
9.10.	AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi	36
9.10.1.	AnlaŐma Süresi.....	36
9.10.2.	AnlaŐmanın Sona Ermesi	36
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri	36
9.11.	Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme	36
9.12.	DeđiŐiklik Halleri	36
9.12.1.	DeđiŐiklik Metotları	36
9.12.2.	Bilgilendirme Mekanizması ve Sıklıđı.....	36
9.12.3.	Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar	36
9.13.	AnlaŐmazlık Halleri	37
9.14.	Uygulanacak Hukuk	37
9.15.	Uygulanabilir Yasalarla Uyum.....	37
9.16.	ÇeŐitli Hükümler	37
9.16.1.	Tüm SözleŐmeler.....	37
9.16.2.	Atama	37
9.16.3.	Bölünebilirlik.....	37
9.16.4.	İcra (Avukatlık Ücretleri ve Haklardan Feragat)	37
9.16.5.	Mücbir Sebepler.....	37
9.17.	Diđer Hükümler	37

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

Bu doküman, Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) tarafından oluőturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti'ne baėlı kamu kurum ve kuruluőlarına Kurumsal Őifreleme Sertifikası saėlayıcılıėı konusundaki iőlevleri sırasında uyulması gereken kuralları ve çalıőma ilkelerini tanımlayan Sertifika İlkeleri (Sİ) dokümanıdır.

Kamu SM Sİ dokümanı Kurumsal Őifreleme Sertifikası hizmeti verilirken ESHS'nin kendisine özel iőlevsel ortamından baėımsız olarak sertifikaların baėvuru, üretim, daėıtım, yenileme, iptal etme ile ilgili süreçler içindeki iőlemlerinin hangi genel ilkeler doėrultusunda gerçekteřtirildiėini, Açık Anahtar Altyapısı'nı (Public Key Infrastructure-PKI) oluőturan ve kullanan tüm bileőenlere uygulanan yönetim kurallarını tanımlayan üst düzey bir dokümandır.

Kamu SM, Sİ'de tanımlanan gerekleri nasıl karőıladıėını anlatan Sertifika Uygulama Esasları (SUE) dokümanını hazırlar ve SUE dokümanına baėlı kalarak çalıőır. Sİ dokümanı sertifika yönetim iőlemleri ile ilgili olarak "ne" yapılacaėını tanımlarken, SUE dokümanı bunun "nasıl" yapılacaėını tanımlar.

1.1. Genel Bakıő

Bu doküman, Kurumsal Őifreleme Sertifikalarının üretim ve yönetim ilkelerinin, sertifika yönetimi ile ilgili tüm kural ve usullerin en üst düzeyde tanımlandıėı bir dokümandır. Kamu SM'den sertifika talebinde bulunan kurumlar bu dokümanda belirtilen Őartları kabul etmiőt sayılırlar.

Kamu SM açık anahtar altyapısı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Saėlayıcısı (Kök SHS) ile buna baėlı olarak çalıőan Sertifika Hizmet Saėlayıcısı (Kurumsal Őifreleme SHS) bulunur.

Sİ dokümanı, "İnternet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmıőt olup, doküman içeriėinde belirtilen bir kısım alt baőlıkların altındaki "Düzenlenmesine gerek duyulmamıőtır" ibaresi, bu aőamada ihtiyaç duyulmadıėından düzenleme yapılmadıėını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kurumsal Őifreleme Sertifika İlkeleri

Doküman Sürüm Numarası: 09

Yayın Tarihi: 13.04.2026

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.11

1.3. Sistem Bileşenleri

Kamu SM açık anahtar altyapısını oluŐturan sistem bileşenleri aŐađıda tanımlanmıŐtır.

1.3.1. Elektronik Sertifika Hizmet Sađlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluŐturma verisi ile imzalamak olan ESHS'ler, sertifika başvurusunda bulunan kurumların kayıt ve kimlik dođrulama işlemleri ile Kurumsal Őifreleme Sertifikası üretim, dađıtım, yenileme, askı, iptal etme ve iptal olmuŐ sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen Őartlara uygun olarak yerine getirmekle yükümlüdür.

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

1.3.2. Kayıt Birimleri

Kayıt birimleri, Kamu SM'nin sertifika ve iptal başvurusu gibi dođrudan son kullanıcılara yönelik hizmetlerini yürüten birimdir. Bu birim, ilk müşteri kayıtlarını oluŐturur, gerekli kurum kimlik tanımlama ve dođrulama 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, sertifika almaya yetkili, üretilen sertifikanın üzerinde kurum adları ve DETSİS numarası yer alan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan tüzel kişilerdir.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluŐturulan sertifikaların içindeki kurum bilgileri ve imza dođrulama verisi arasındaki bađın dođruluđuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir/kurumlardır.

1.3.5. Diđer Bileşenler

1.3.5.1. Kurumsal Őifreleme Sertifikası Sorumlusu

Sertifika başvurusunda bulunan kurum tarafından yetkilendirilen ve Kurumsal Őifreleme Sertifikası başvurusu sırasında kurumların bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan kişi/kişilerdir. Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları Kamu SM tarafından kendisine imzalatılan taahhütnamedeki Őartları yerine getirmekten sorumludur.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı BaŐbakanlık Genelgesi ile elektronik ortamda iletilen resmî yazıların Őifreli Őekilde gönderilebilmesine imkân sađlanmıŐtır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla güncel e-YazıŐma Teknik

Rehberi'ne uygun olarak kullanılmalıdır. Kurumsal Őifreleme Sertifikaları, bilgi ve belgelerin Őifrelenerek uzun süreli saklanması ve elektronik imzalama için kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

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

1.5. Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

Sİ dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda Sİ dokümanında deęişiklik yapabilir.

1.5.2. İletişim Bilgileri

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

Adres : Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi, 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, Sİ 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 Uygunluęunu Belirleyen Kiři

Bu Sİ dokümanına uygun olarak yazılmış olan SUE dokümanlarının uygunluęu, Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

Akıllı Kart veya HSM Erişim Verisi: Sertifika sahibine ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisidir.

Akıllı Kart: Sertifika ve sertifika ile ilişkili imza oluşturma verisinin içinde bulunduğu güvenli donanımdır.

Anahtar Çifti: İmza oluşturma ve onunla ilişkili olan imza doğrulama verisi çiftidir.

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

ŐİSDUP (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 Teşkilatı Merkezi Kayıt Sistemi): Türkiye Cumhuriyeti devlet teşkilatı içerisinde yer alan kurum ve kuruluşların merkez, taşra ve yurt dışı teşkilatlarında bulunan her düzeydeki birimleri ile birlikte hiyerarşik yapıya uygun olarak kayıt altına alındığı sistemdir.

EYP (e-Yazışma Projesi): Kamu kurum ve kuruluşları arasındaki resmî yazışmaların elektronik ortamda yürütülmesini amaçlayan projedir.

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

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 Başbakanlık Genelgesi", Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan "Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar" ve "Elektronik Mühre İlişkin Usul ve Esaslar Hakkında Yönetmeliği" ifade eder.

İmza Doğrulama Verisi: İlgili imza oluşturma verisi sahibinin herkes ile paylaşılabilirdiği, imza oluşturma verisi ile oluşturduğu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşenidir.

İmza Oluşturma Verisi: Anahtar çiftinin sahibi tarafından gizli tutulan ve dijital imza oluşturmak ve/veya ilgili imza doğrulama verisi ile şifrelenmiş elektronik kayıtların, dosyaların şifresini çözmek için kullanılan anahtardır.

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

Kamu SM (Kamu Sertifikasyon Merkezi): Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birimdir.

Kök Sertifika Hizmet Sağlayıcısı: Kamu Sertifikasyon Merkezi içinde oluşturulmuş, en yetkili imza derecesi verilmiş ve sertifikasını kendisi imzalamış olan Sertifika Hizmet Sağlayıcısıdır.

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

Kurum Doküman Doğrulama Sistemi: Elektronik ortamda hazırlanan belgelerin doğrulanması işleminde kullanılacak kuruma ait sistem veya e-Devlet belge doğrulama sistemidir.

Kurumsal Şifreleme SHS (Kurumsal Şifreleme Sertifika Hizmet Sağlayıcısı): Kamu Sertifikasyon Merkezi içinde oluşturulmuş, Kök Sertifika Hizmet Sağlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluşturup imzalamakla yetkili kılınmış Elektronik Sertifika Hizmet Sağlayıcısıdır.

Kurumsal Şifreleme Sertifikası Sorumlusu/Sorumluları: Kamu kurumlarının başvuru formu ve taahhütname ile Kamu SM'ye bildirdiği ve Kurumsal Şifreleme Sertifikası ile ilgili süreçlerde kurumu temsile yetkili kişi/kişilerdir.

Kurumsal Şifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılan imza doğrulama verisini içeren elektronik sertifikadır.

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

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

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

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

Üçüncü KiŐiler: Sertifikalara güvenerek işlem yapan gerçek veya tüzel kiŐilerdir.

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

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

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ/SUE: Sertifika İlkeleri/Sertifika Uygulama Esasları

SİL: Sertifika İptal Listesi

2. Yayınlama ve Bilgi Deposu Yüklümlükleri

2.1. Bilgi Depoları

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

<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 Yayınlanması

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

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

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ/SUE dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip mümkün olan en kısa sürede yayımlanır. Sertifika iptal durum kayıtlarının yayımlanma sıklığı ilgili SUE dokümanında belirtilmektedir.

2.4. Erişim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır. Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM personeli tarafından yapılmaktadır. Kamu SM, bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak, bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamakla yükümlüdür.

3. Kimlik Belirleme ve Doğrulama

Kurumsal Şifreleme Sertifikası kurum kimlik tanımlama ve doğrulama yöntemleri ile Kurumsal Şifreleme Sertifikası içinde yazılan kurum bilgileri bu bölümde anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

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

3.1.2. Kimlik Bilgilerinin 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 biĐimi 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. Kurumsal Őifreleme Sertifikalarının isim alanı iinde benzersiz bir sayı olduĐu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

3.1.6. Markanın Tanınması, DoĐrulanması ve Rolü

Düzenlenmesine gerek duyulmamıŐtır.

3.2. İlk Kimlik DoĐrulama

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

3.2.1. İmza OluŐturma Verisi SahipliĐinin Kanıtlanması

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

Kurumsal Őifreleme Sertifikası, baŐvuru sırasında belirlenen sorumlu/sorumlulara teslim edilir. Akıllı kart ierisinde teslim edilen kurumsal Őifreleme sertifikasının teslim teyidi Online İŐlemler üzerinden alınır. HSM'ye yüklenmesi talep edilen sertifikaların teslim teyidi iin 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.

3.2.3. KiŐisel KimliĐin Belirlenmesi

Kurumsal Őifreleme Sertifikaları, yalnızca SUE Bölüm 1.3.3'te belirtilen sertifika sahibi kurumlar adına üretildiĐinden bireysel baŐvurular kabul edilmemektedir.

3.2.4. DoĐrulanmayan Sertifika Sahibi Bilgileri

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

Kurum bu bilgileri Kamu SM'ye doĐru beyan etmekle yükümlüdür.

3.2.5. Yetkinin Doğrulanması

Sertifika içeriğine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Kamu SM yenileme talebinde bulunan sertifika sahibi kurumun bilgilerini güncelliğini doğrular.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

SUE Bölüm 3.2’de anlatıldığı şekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

SUE Bölüm 3.2’de anlatıldığı şekilde uygulanır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi kurumun yetkilendirdiği sertifika sorumlusu/sorumluları Kamu SM resmî web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. Online İşlemler adresine ulaşılamaması durumunda Kamu SM web sitesinde belirtilen yöntemlerle iptal işlemi gerçekleştirilebilir. Kurum kimlik doğrulaması ve iptal işleminin teyidi SUE Bölüm 3.4’te anlatıldığı şekilde gerçekleştirilir.

4. Sertifika Yaşam Döngüsü İşlevsel Gereklilikleri

Bu bölümde sertifika yönetim süreçlerinde yapılan işlemler anlatılmaktadır. Süreçlerle ilgili ayrıntılar Kamu SM’nin internet sitesinde belirtilmektedir.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

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

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Şifreleme Sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM’ye yapılır. Kurumun Kamu SM’den alacağı sertifika hizmetlerinin şartları kurumun imzaladığı başvuru formu ve taahhütnameler, Kamu SM’nin internet üzerinden yayımladığı ilgili yönergeler, Si/SUE dokümanları doğrultusunda belirlenir.

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

Kayıt işlemleri ve sorumluluklar ile ilgili detaylı bilgi SUE Bölüm 4.1.2’de yer almaktadır.

4.2. Sertifika Başvurusunun İőlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İőlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve doğrulama iőlevleri yerine getirilir. Kurumdan gönderilen belgelerin doğrulanması için yapılan iőlemler SUE Bölüm 4.2.1’de yer almaktadır.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

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

4.2.3. Sertifika Başvurusunun İőlenme Zamanı

SUE Bölüm 4.2.3’te belirtilen başvuru iőlenme süreleri uygulanır.

4.3. Sertifikanın Oluőturulması

4.3.1. Sertifika Oluőturulmasında ESHS’nin İőlevleri

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

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

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

4.3.2. Sertifika Oluőturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

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

HSM cihazına sertifika yükleme iőlemi, HSM Cihaz Sorumlusu gözetiminde gerçekteőirilir. İőlem sonrasında kurulum tutanađı imzalanır ve Kurumsal Őifreleme Sertifikasının oluşturulduđu konusunda HSM sorumlusu bilgilendirilmiő olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koőulu

Kurumsal Őifreleme Sertifikası akıllı kart veya HSM cihazı içerisinde kullanılabilir. Sertifikanın kullanılacađı cihaz seđimine göre SUE Bölüm 4.4.1’de belirtilen kabul koőulu uygulanmaktadır.

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 Tarafra Duyurulması

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

4.5. Sertifikanın ve İmza OluŐturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza OluŐturma Verisi Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait imza oluŐturma verisini; tabi olunan standartlar, ilgili mevzuat, Sİ/SUE dokümanı ve ilgili baŐvuru formu ve taahhütnamesinde yer alan koŐullar ve belirlenmiŐ sınırlar içinde kullanmalıdır.

4.5.2. Üçüncü KiŐilerin Sertifika İmza Doğrulama Verisi Kullanımı

Sertifika sahibine ait Kurumsal Őifreleme Sertifikasının içinde yer alan imza doğrulama verisi, üçüncü kiŐilerce e-YazıŐma Projesi kapsamında verilerin Őifreli iletimi amacıyla kullanılır. İmza doğrulama verisinin veya sertifikanın, belirtilen amaç dıŐında kullanılması sonucu oluŐabilecek zararlardan üçüncü kiŐiler sorumludur.

4.6. Sertifika Süresinin Uzatılması

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

4.7. Sertifika Yenileme

Kamu SM, sertifika yenileme iŐlemini, yeni anahtar çifti üretmek suretiyle yerine getirir. Sertifika yenileme iŐlemleri SUE Bölüm 4.7'de anlatıldıđı Őekilde gerçekteŐtirilir.

4.7.1. Sertifikanın Yenileme KoŐulları

Sertifika yenileme iŐlemi SUE Bölüm 4.7.1'de belirtilen durumlarda yapılmaktadır.

4.7.2. Sertifika Yenileme BaŐvurusunu Kimlerin Yapabildiđi

SUE Bölüm 4.7.2'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme BaŐvurusunun İŐlenmesi

SUE Bölüm 4.7.3'te tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

SUE Bölüm 4.7.4'te tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul KoŐulu

SUE Bölüm 4.7.5'te tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması

SUE Bölüm 4.7.6'da tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diđer Tarafra Duyurulması

SUE Bölüm 4.7.7'de tanımlanmaktadır.

4.8. Sertifikada Bilgi DeđiŐikliđi

Sertifika içeriđinde yer alan bilgilerde deđiŐiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi deđiŐikliđinin gerekli olduđu durumlarda, kurum SUE Bölüm 4.7'de belirtilen sertifika yenileme sürecini iŐletmelidir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiđi Durumlar

Sertifikanın, kullanım süresi dolmadan geçerliliđini yitirdiđi durumlarda, sertifika iptal edilir. İptal edilen sertifikayla bir daha işlem yapılamaz. Sertifikanın iptalini gerektiren durumlar SUE Bölüm 4.9.1’de verilmiştir.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

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

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Kurumsal Şifreleme Sertifikası iptal işlemi, kurum tarafından yetkilendirilen Kurumsal Şifreleme Sertifikası Sorumlusu/Sorumluları tarafından Kamu SM resmî internet sitesinde yer alan Online İşlemler menüsü aracılığı ile yapılır. İptal işlemlerinin Kamu SM Online İşlemler üzerinden yapılamadığı durumda süreç SUE Bölüm 4.9.3’te belirtildiđi şekilde işletilir.

4.9.4. İptal İsteđi Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteđinin İşlenme Süresi

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

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliđi

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, sorgulama yapacak kişinin kimlik doğrulamasına gerek kalmadan dileyen herkes tarafından erişilebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliđini sağlar. Üçüncü kişilerin yapması gereken geçerlilik kontrolleri SUE 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, üretildiđini andan itibaren mümkün olan en kısa sürede yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

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

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Kamu SM, sertifika iptal bilgisinin sisteme daha az yük getirecek biçimde yayımlanmasını sađladığı için, SİL yanında çevrim içi sertifika iptal durum kaydı desteđini de vermektedir. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiđi ölçüde ÇİSDUP kullanmaları önerilir.

4.9.11. Diđer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. İmza OluŐturma Verisinin Güvenliđini Yitirmesi Durumu

Sertifika sahibi kuruma ait imza oluŐturma verisinin güvenliđini yitirmesi durumunda Kurumsal Őifreleme Sertifikası iptal edilir. Kurumsal Őifreleme Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Kurumsal Őifreleme Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sađlamak amacıyla askıya alınabilir. Sertifikanın askıya alındığı durumlar SUE Bölüm 4.9.13'te verilmiştir.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi

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

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Kurumsal Őifreleme Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden veya Online İşlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Askıya alma başvurusunun işlenmesi ile ilgili detaylar SUE Bölüm 4.9.15'te verilmiştir.

Kamu SM'ye ait Kök SHS ve Kurumsal Őifreleme SHS sertifikaları askıya alınmaz.

4.9.16. Askıda Kalma Süresi

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

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteđi olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcıdan öğrenebilirler. Üçüncü kişiler, Kurumsal Őifreleme Sertifikalarının geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin Eriőilebilirliđi

SİL ve ÇİSDUP servislerinin verildiđi sistemlere eriőimin kesintisiz olarak sađlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rađmen eriőimin bir süreliđine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurur. Üçüncü kişilerin iptal durum kaydını, eriőimin kesilmesi sebebiyle kontrol etmeden yaptıkları işlemlerden dođan zararlardan Kamu SM sorumlu tutulamaz.

4.10.3. İsteđe Bađlı Özellikler

Düzenlenmesine gerek duyulmamıőtır.

4.11. Sertifika Sahipliđinin Sona Ermesi

Kurumsal Őifreleme Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliđi sona erer. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda deđildir; sertifika sahibi sertifikanın kullanım süresinin dolduđu zamanı kendisi takip etmekle yükümlüdür.

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 anlatılmıőtır.

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM sisteminin çalıőtıđı cihazların bulunduđu binalar ve odalar, giriő ve çıkıőların kontrol edildiđi yetkisiz kişilerin giriőini engelleyen güvenlik önlemleri ile donatılmıőtır. Güvenli alanlara eriőimlerin kaydı tutulmaktadır.

5.1.1. Tesis Yeri ve İnőaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütölmektedir. Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkân sađlayan yapıdadır. Alanlara ve binalara eriőim fiziki güvenlik, video izleme ve kimlik dođrulama olmak üzere çoklu güvenlik ile korunmaktadır.

5.1.2. Fiziksel Eriőim

Kamu SM yazılım ve donanım modöleri ile arşivlere eriőim denetim altındadır. Binaya giriőler güvenlik görevlilerinin kontrolü altında, gelişmiş eriőim kontrol cihazlarıyla sađlanmaktadır.

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduđu, elektronik veya kâđit ortamdaki bilgilerin tutulduđu, sistemin işletildiđi ve yönetildiđi odalara eriőim gelişmiş eriőim kontrol cihazlarıyla yapılmaktadır.

5.1.3. Güç Kaynađı ve Havalandırma

Kamu SM işlevlerinin yerine getirilmesi ve sürekliliđin sađlanması için sistem, kesintisiz güç kaynađı ile beslenir. Bina gerekli havalandırma sistemi ile donatılır.

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.

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.

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 sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Güvenilir roller, SUE Bölüm 5.2.1’de detaylandırılır.

5.2.2. Her İşlem İçin Gereken KiŐi Sayısı

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

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Kamu SM içinde, aynı kişinin birden fazla görevde bulunmasını engelleyecek sınırlamalar getirilebilir.

5.3. Personel Güvenlik Kontrolleri

5.3.1. KiŐisel Geçmiş, Deneyim ve Nitelik Gereklere

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir.

5.3.2. Geçmiş AraŐtırması

Çalışanların Kamu SM’nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiđi güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan araŐtırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araŐtırmalarda personelin herhangi bir sebepten dolayı

hüküm giyip giymemiş olduđu araştırılır. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. İşe başlayan personelin bilgi güvenliđi farkındalık eğitimleri tamamlanmadan, sistemlere erişim izni verilmez.

5.3.3. Eğitim Gerekleri

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

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

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

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

5.3.5. Görev Deđişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

5.3.7. Anlaşmalı Personel Gereksinimleri

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

5.3.8. Sağlanan Dokümantasyon

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

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde, SUE Bölüm 5.4.1'de belirtilen elektronik veya kâğıt ortamda yapılan işlerin kayıtları tutulur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyiőisiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluşup oluşmadığı kontrol edilir.

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

Kamu SM'ye ait kayıtlar, izinsiz izlenmeyi, deęiřtirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur.

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritiklięi göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı 1 (bir) saatte gerekli görülen kayıtların çevrim içi yedeęi alınmaktadır. Kritik kayıtlar ayrı bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, aę 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 Deęerlendirilmesi

Denetim kayıtlarının tutulduęu sistemler için SUE Bölüm 6.5, 6.6 ve 6.7'de sözü geçen teknik güvenlik kontrolleri uygulanır.

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

SUE Bölüm 5.4.1'de belirtilen kayıtlara ek olarak SUE Bölüm 5.5.1'de belirtilen sertifika başvurusu ve sertifika yaşam döngüsüyle ilgili elektronik ortamda ya da kâğıt üzerinde tutulan belgeler arşivlenir.

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, deęiřtirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduęu ortam SUE Bölüm 5.5.2'de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş 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 doğruluđu kontrol edilir.

5.6. Anahtar Deđiřimi

Kamu SM'ye ait anahtarlar ve sertifikalar geđerlilik süresinin dolması veya güvenlik gerekleriyle yenilenebilir. Kamu SM'ye ait sertifikanın kullanım süresinin dolmasından önce eski anahtar çiftinden yeni anahtar çiftine geđiş işlemleri yapılır. Anahtar deđişimine ilişkin detaylar SUE Bölüm 5.6'da açıklanmaktadır.

5.7. Güvenliđin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliđin Yitirilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

5.7.3. İmza Oluřturma Verisinin Gizliliđinin Kaybetmesi Durumunda İzlenecek Prosedürler

Kamu SM'nin Kurumsal Őifreleme Sertifikalarını imzalamada kullandıđı imza oluřturma verisinin gizliliđinin kaybedildiđinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve SUE Bölüm 5.7.3'te belirtilen işlemler yerine getirilir.

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 sürekliliđi planlarında tanımlar. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, işleyişine Elektronik İmza Kanunu'nun Uygulanmasına İliřkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verebilir. Bu durumda Kamu SM'nin yerine getirmesi gereken işlemler SUE Bölüm 5.8'de açıklanmaktadır.

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 sağlar.

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

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceđi güvenli odada, birden fazla eğitimli personelin gözetiminde, ađ ortamına

kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS-140-2 seviye 3 veya EAL4+ standartlarını sağlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen imza oluŐturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleŐtiren personel tarafından onaylanır.

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

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

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

Sertifika sahibine ait imza oluŐturma verisinin yedeđi alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait imza oluŐturma verisinin saklandığı akıllı kart veya HSM SUE Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine İmza OluŐturma Verisinin UlaŐtırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluŐturulmasına müteakip, imza oluŐturma verisi, sertifikayla birlikte akıllı kart veya HSM'ye yüklenerek teslim edilir. Akıllı kart, imza karŐılıđı ve resmî kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye imza oluŐturma verisi ve sertifika yükleme işlemi, HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Kurulum Tutanađı doldurularak kurum tarafından imzalanır.

6.1.3. İmza Doğrulama Verisinin ESHS'ye UlaŐtırılması

Kurumsal Şifreleme Sertifikası HSM'ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteđi, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılıđıyla Kamu SM'ye parola korumalı ZIP dosyası içerisinde ulaŐtırılır.

Kurumsal Şifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Şifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildiđi için imza doğrulama verisinin Kamu SM'ye ulaŐtırılması söz konusu deđildir.

6.1.4. ESHS Sertifikalarına EriŐim Sađlanması

Kamu SM'ye ait Kök SHS ve Kurumsal Şifreleme SHS sertifikaları internet ortamında tarafların eriŐimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz deđiŐtirmeye ve silinmeye karŐı güvenliđi sađlanır.

6.1.5. Anahtar Uzunlukları

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

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

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

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

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde Tebliğ'de belirtilen kriterlere uygun algoritmalar kullanılmaktadır. Algoritmaların gerçekleştiriminde kullanılan yöntemler gerekli güvenlik kriterlerini sağlar.

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan anahtarların hangi amaçlar için kullanılabilceği sertifikadaki "Anahtar Kullanımı" ve "Genişletilmiş Anahtar Kullanımı" uzantısı içerisinde belirtilir.

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

6.2. İmza Oluşturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluşturma verileri güvenli yazılım ve/veya donanım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduğu süre boyunca bu modül dışına çıkmaz. Kriptografik modülün sahip olduğu güvenlik işlevleri SUE Bölüm 6.2.1'de açıklanmaktadır.

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

Kamu SM'ye ait imza oluşturma verisinin bulunduğu odaya erişim aynı anda 2 (iki) yetkili personel tarafından sağlanmaktadır.

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

Kamu SM'ye ait imza oluşturma verisinin yedeğinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme işlemi hazırda kullanılmakta olan imza oluşturma verisi için sağlanan güvenlik ile eşdeğer güvenlik önlemleri altında yapılır. Sertifika sahiplerine ait imza oluşturma verileri Kamu SM tarafından yedeklenmez.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluşturma verileri arşivlenmez. Kullanım süreleri sonunda geri dönüşsüz şekilde silinir.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

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

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

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

Kamu SM'ye ait imza oluşturma verileri, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. İmza oluşturma verisinin yedekleme amacı haricinde

cihaz dıŐına ıkması engellenmiŐtir. İmza oluŐturma verileri kriptografik modl iinde gvenli algoritma ve yntemlerle Őifreli olarak saklanır.

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

6.2.8. İmza OluŐturma Verisine EriŐim

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

İmza oluŐturma verisi kriptografik modl iinde Őifreli durumdayken eriŐime kapalıdır. EriŐime aılması iin eriŐimi saĐlayan verinin modle sunulması gerekir.

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

6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

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

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

6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

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

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

6.2.11. Kriptografik Modln DeĐerlendirilmesi

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

6.3. Anahtar ifti Ynetimiyle İlgili DiĐer Konular

6.3.1. İmza DoĐrulama Verisinin ArŐivlenmesi

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

6.3.2. İmza OluŐturma ve Dođrulama Verilerinin Kullanım Süreleri

İmza oluŐturma verisinin kullanım süresi, Kurumsal Őifreleme Sertifikasının ieriđinde belirtilen kullanım süresi kadardır. Üretilen Kurumsal Őifreleme Sertifikalarının son kullanma tarihi, Kurumsal Őifreleme SHS Sertifikasının son kullanma tarihini aŐamaz.

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.

6.4. Aktivasyon Verileri

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

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

6.4.1. Aktivasyon Verilerinin OluŐturulması

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

6.4.2. Aktivasyon Verilerinin Korunması

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

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

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

6.4.3. Aktivasyon Verileri ile İlgili Diđer Konular

Düzenlenmesine gerek duyulmamıŐtır.

6.5. Bilgisayar Güvenliđi Kontrolleri

6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereker

Kamu SM sistemi içinde, son teknolojik geliŐmeler göz önünde bulundurularak bilgisayar güvenliđi sađlanır. Bilgisayar güvenliđiyle ilgili teknik gerekler SUE Bölüm 6.5.1'de açıklanmaktadır.

6.5.2. Bilgisayar Sisteminin Sađladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıŐtır.

6.6. YaŐam Döngüsü Teknik Kontrolleri

6.6.1. Sistem GeliŐtirme Kontrolleri

Sistem geliŐtirilirken genel anlamda yapılan denetimler SUE Bölüm 6.6.1'de açıklanmaktadır.

6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içindeki yazılım ve donanım ürünleri ile ađ ortamının belirlenen güvenlik Őartlarını sađlayıp sađlamadıđı, test cihazları ve test prosedürleri kullanılarak kontrol edilir. Güvenlik kontrolleri için temel dayanak ISO 27001'in güncel sürümüdür.

6.6.3. YaŐam Döngüsü Güvenlik Kontrolleri

Düzenlenmesine gerek duyulmamıŐtır.

6.7. Ađ Güvenliđi Kontrolleri

Kamu SM sisteminde son teknolojik geliŐmeler göz önünde bulundurularak gerekli ađ güvenliđi denetimleri yapılır. Ađ güvenliđi denetimlerine iliŐkin detaylar SUE Bölüm 6.7’de açıklanmaktadır.

6.8. Zaman Damgası

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, geçerlilik tarihi, ilgili imza dođrulama verisi, sertifika sahibi kurumun adı ve DETSİS numarası, sertifikayı yayımlayan Kamu SM’ye ait isim bilgileri ve Kamu SM’nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını içerir. Kurumsal Őifreleme Sertifikasının içeriđinde bulunan sertifika uzantıları sertifikanın kullanılacađı uygulamanın gereklerine bađlı olarak belirlenir.

Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikalarında asgari düzeyde bulunması gereken uzantılar SUE Bölüm 7.1.2’de tanımlanmıŐtır.

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiđi Kurumsal Őifreleme Sertifikalarını imzalamak için SHA-384 özet algoritması ile ECDSA imza dođrulama verisi 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

SUE Bölüm 7.1.5’te belirtilmektedir.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

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

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

“Sertifika İlkeleri Uzantısı” Kurumsal Şifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Şifreleme 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 Şifreleme Sertifikasının “Sertifika İlkeleri Uzantısı¹”nın içinde yer alır. “Sertifika İlkeleri Uzantısı”nın içinde “İlke Niteleyici²” 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 Şifreleme 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 SUE Bölüm 7.2.2.’de belirtilen bilgileri içerir.

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları ve yanıtları SUE Bölüm 7.3.2’de belirtilen bilgileri içerir.

8. Uygunluk Denetimleri

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

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

8.1. Uygunluk Denetiminin Sıklığı

BTK, gerekli gördüğü durumlarda resen denetim yapabilir.

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

¹ Certificate Policies

² Policy Identifier

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

8.2. Denetçinin Nitelikleri

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

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

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

8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi

BTK, kanun gereği tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kurumdur.

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

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

8.4. Denetimin Kapsamı

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

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

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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

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

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

8.6. Sonucun Bildirilmesi

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

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

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

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

9.1.2. Sertifika 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 aracılığıyla 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, 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, SUE 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, ürettiği Kurumsal Őifreleme Sertifikalarını 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalıdır.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.4. Kişisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

Kamu SM verdiđi hizmetlerde sertifika sahiplerinin ve diđer paydaşların kişisel verilerinin gizliliđini ilgili mevzuat ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki mer'i mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurumun ve yetkilendirdiđi Kurumsal Őifreleme Sertifika Sorumlusu/Sorumluları ile HSM Cihaz Sorumlusunun, başvuru sırasında kimlik tanımlama ve dođrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiđi bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi kurum tarafından atanan parolalar, numara, sembol gibi diđer tanımlayıcı bilgiler de kişisel 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 kurumdan Kurumsal Őifreleme Sertifikası vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiđi kişisel bilgileri sertifika hizmeti vermek dışında başka amaçlar için kullanmaz, üçüncü kişilere vermez, sertifika sahibi kurumun izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceđi ortamlarda bulundurmaz.

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

Kamu SM Kişisel 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 kişisel bilgileri kişilerin yazılı rızası ile izin almak şartıyla yapılacak iş geređi üçüncü kişilerle paylaşabilir.

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diđer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yüklümlülükler

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

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

Kamu SM'nin ESHS olarak işleyişinin güvenli olabilmesi için, sistem bileşenlerinin yerine getirmesi gereken yükümlülükler SUE Bölüm 9.6.1'de açıklanmaktadır.

9.6.2. Kayıt Birimi Yükümlülükleri

Kayıt birimlerinin yükümlülükleri SUE Bölüm 9.6.2'de açıklanmaktadır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri SUE Bölüm 9.6.3'te açıklanmaktadır.

Sertifika sahibi kurum, Kamu SM Kurumsal Şifreleme Sertifikası Sİ/SUE dokümanlarında belirtilen şartları okuduğunu, başvuru süreci ve sertifika geçerliliği boyunca taahhütname, ilgili mevzuatlar ile Sİ/SUE dokümanında belirtilen şartlara uygun olarak hareket edeceğini kabul ve taahhüt eder. Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin/kurumun zarara uğraması halinde TÜBİTAK BİLGEM'in ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, Kurumsal Şifreleme Sertifikasıyla işlem yapmadan önce SUE Bölüm 9.6.4'te belirtilen sertifika geçerlilik kontrollerini yapmakla yükümlüdür.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

Kamu SM'ye sertifika başvurusunda bulunan kurumun yükümlülükleri SUE Bölüm 9.6.5.1'de belirtilmektedir.

9.6.5.2. Sertifika Sorumlularının Yükümlülükleri

Kurum adına Kurumsal Şifreleme Sertifikası başvurusunda bulunan Kurumsal Şifreleme Sertifikası Sorumlusunun/Sorumlularının yükümlülükleri SUE Bölüm 9.6.5.2'de belirtilmektedir.

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.

9.9. Tazminat Halleri

Kamu SM ve sertifika hizmeti alan taraflar arasında yükümlölüklerin yerine getirilmemesinden kaynaklanan zararlar, tarafların o ana kadar somut olarak gerçekteşmiş 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 birliđi içinde çalışır; süreçleri yerine getirirken gerekli desteđi ve koordinasyonu Sİ/SUE dokümanlarında belirtilen şartlar altında sağlar.

9.10.1. Anlaşma Süresi

Sertifika sahibi kurumun imzaladığı taahhütnamelerin süresi sertifikanın geçerlilik süresi veya taahhütnamede belirtilmişse hizmetin alınma süresi kadardır.

9.10.2. Anlaşmanın Sona Ermesi

Kamu SM imzalanan taahhütnameleri SUE Bölüm 9.10.2’de belirtilen durumlarda sonlandırılabilir.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

İmzalanan taahhütnamelerin sona ermesiyle hizmeti alan kurumun, taahhütname ile Sİ/SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlölükleri ortadan kalkar.

9.11. Sistem Bileşenleri ile Haberleşme ve Kişisel Bilgilendirme

Kamu SM, Kurumsal Şifreleme Sertifikaları başvuru, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılığıyla sağlanır. Sertifika yönetim işlemleri sırasında sertifika sorumlusu/sorumluları veya sertifika sahibi kurum ile yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacağı Kamu SM’nin Kurumsal Şifreleme Sertifikası yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. Deđişiklik Halleri

9.12.1. Deđişiklik Metotları

Sİ dokümanı Kamu SM tarafından yazılmıştır. Bu Sİ dokümanında yapılabilecek deđişiklikler ekleme ve deđiştirme şeklinde olabileceđi gibi Kamu SM dokümanının tamamen yenilenmesine de karar verebilir. Bu Sİ dokümanının herhangi bir kısmının yanlış ya da geçersiz olduđu ortaya çıksa bile Sİ dokümanının diđer kısımları, Sİ dokümanı güncellenene kadar geçerliliđini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

Sİ dokümanında yapılan deđişiklikler 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 Deđişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. AnlaŐmazlık Halleri

Taraflar arasında çıkan tüm anlaŐmazlıkların 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

Sİ dokümanındaki hükümler, ilgili mevzuata uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. ÇeŐitli Hükümler

9.16.1. Tüm SözleŐmeler

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 olduęu 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 verdięi ölçüde bu Sİ/SUE kapsamındaki bir yükümlülüęün yerine getirilmesinde kendi makul kontrolü dışındaki bir olaydan kaynaklanan gecikme veya başarısızlıklardan sorumlu deęildir.

9.17. Dięer Hükümler

Düzenlenmesine gerek duyulmamıştır.