

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŐİFRELEME SERTİFİKA İLKELERİ

Doküman Kodu

POL.05.02

Revizyon No

04

Revizyon Tarihi

17.02.2022

TASNİF DIŐI

KURUMSAL ŐİFRELEME SERTİFİKA İLKELERİ

REVİZYON GEÇMİŐİ

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

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	11
1.4.1. Uygun Olan Sertifika Kullanımı	11
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	12
1.6.1. Tanımlar	12
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	15
3. KİMLİK BELİRLEME VE DOėRULAMA	15
3.1. İsimlendirme	15
3.1.1. İsim Alanı Tipleri	15
3.1.2. Kimlik Bilgilerinin Teőhise Elveriőli 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 Belirleme	15
3.2.1. Özel Anahtar Sahipliėinin Kanıtlanması	15
3.2.2. Kurumsal Kimliėin Belirlenmesi	16
3.2.3. Kiőisel Kimliėin Belirlenmesi	16
3.2.4. Doėrulanmayan Sertifika Sahibi Bilgileri	16
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. İŐLEMSEL GEREKLER	16
4.1. Sertifika BaŐvurusu	17
4.1.1. Sertifika BaŐvurusunu Kimlerin YapabildiĐi	17
4.1.2. Kayıt İŐlemleri ve Sorumluluklar	17
4.2. Sertifika BaŐvurusunun İŐlenmesi	17
4.2.1. Kimlik Tanımlama ve DoĐrulama İŐlevlerinin Yerine Getirilmesi	17
4.2.2. Sertifika BaŐvurusunun Kabul veya Reddi	17
4.2.3. Sertifika BaŐvurusunun 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	18
4.4. Sertifikanın Kabulü	18
4.4.1. Sertifikanın Kabul KoŐulu	18
4.4.2. Sertifikanın ESHS Tarafından Yayımlanması	18
4.4.3. Sertifikanın OluŐturulmasının DiĐer Tarafra Duyurulması	18
4.5. Sertifikanın ve Özel Anahtarın Kullanımı	18
4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı	18
4.5.2. Üçüncü KiŐilerin Sertifika ve Açık Anahtar 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 BaŐvurusunu Kimlerin YapabildiĐi	18
4.7.3. Sertifika Yenileme BaŐvurusunun İŐlenmesi	19
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi	19
4.7.5. Sertifika Yenileme Sonrası Kabul KoŐulu	19
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması	19
4.7.7. Sertifika Yenilemenin DiĐer Tarafra Duyurulması	19
4.8. Sertifikada Bilgi DeĐiŐikliĐi	19
4.9. Sertifikanın İptali ve Askıya Alınması	19
4.9.1. Sertifikanın İptal EdildiĐi Durumlar	19
4.9.2. Sertifika İptal BaŐvurusunu Kimler Yapabilir	19
4.9.3. Sertifika İptal BaŐvurusunun İŐlenmesi	19
4.9.4. İptal İŐteĐi Ertelenme Süresi	19
4.9.5. İptal İŐteĐinin İŐlenme Süresi	19
4.9.6. Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol GerekliliĐi	20
4.9.7. Sertifika İptal Listesi Yayımlama SıklıĐı	20
4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi	20
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. Özel Anahtarın GüvenliĐini Yitirmesi Durumu	20
4.9.13. Sertifikanın Askıya AlındıĐı Durumlar	20
4.9.14. Sertifika Askıya Alma BaŐvurusunu Kimlerin YapabildiĐi	20
4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi	20
4.9.16. Askıda Kalma Süresi	21
4.10. Sertifika Durum Servisleri	21

4.10.1.	İřletimsel Özellikleri.....	21
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.....	22
5.1.2.	Fiziksel Eriřim	22
5.1.3.	Güç Kaynađı ve Havalandırma	22
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.....	23
5.2.3.	Kimlik Dođrulama ve Yetkilendirme.....	23
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	23
5.3.	Personel Güvenlik Kontrolleri	23
5.3.1.	Kiřisel Geçmiř, Deneyim ve Nitelik Gerekleri	23
5.3.2.	Geçmiř Arařtırması	23
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	24
5.3.8.	Sađlanan Dokümantasyon	24
5.4.	Denetim Kayıtları	24
5.4.1.	Kaydedilen İřlemler	24
5.4.2.	Kayıtların İncelenme Sıklıđı	24
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 Sebepiyet Veren Tarafın Bilgilendirilmesi.....	24
5.4.8.	Saldırıya Açıklıđın Deđerlendirilmesi.....	24
5.5.	Kayıt Arřivleme	25
5.5.1.	Arřivlenen Kayıt Bilgileri.....	25
5.5.2.	Arřivlerin Tutulma Süresi	25
5.5.3.	Arřivlerin Korunması	25
5.5.4.	Arřivlerin Yedeklenmesi	25
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri.....	25
5.5.6.	Arřivlerin Toplanması	25
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 Kaybedilmesi	26
5.7.4.	Arıza Sonrası Yeniden ÇalıŐırlık	26
5.8.	Sertifika Hizmetlerinin Sonlandırılması.....	26
6.	TEKNİK GÜVENLİK KONTROLLERİ	26
6.1.	Anahtar Çifti Üretimi ve Kurulumu	26
6.1.1.	Anahtar Çifti Üretimi	26
6.1.2.	Sertifika Sahibine Özel Anahtarın UlaŐtırılması.....	27
6.1.3.	Elektronik Sertifika Hizmet Saęlayıcısına Açık Anahtarın UlaŐtırılması	27
6.1.4.	Elektronik Sertifika Hizmet Saęlayıcısı Sertifikalarına EriŐim Saęlanması	27
6.1.5.	Anahtar Uzunlukları.....	27
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü.....	27
6.1.7.	Anahtar Kullanım Amaçları	27
6.2.	Özel Anahtarın Korunması	27
6.2.1.	Kriptografik Modül Standartları	27
6.2.2.	Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim	28
6.2.3.	Özel Anahtarın Yeniden Elde Edilmesi	28
6.2.4.	Özel Anahtarın Yedeklenmesi	28
6.2.5.	Özel Anahtarın ArŐivlenmesi	28
6.2.6.	Özel Anahtarın Kriptografik Modüle Yüklenmesi	28
6.2.7.	Özel Anahtarın Kriptografik Modülde Saklanması	28
6.2.8.	Özel Anahtara EriŐim	28
6.2.9.	Özel Anahtara EriŐimin Kesilmesi.....	28
6.2.10.	Özel Anahtarın Yok Edilmesi	29
6.2.11.	Kriptografik Modülün Deęerlendirilmesi	29
6.3.	Anahtar Çifti Yönetimiyle İlgili Dięer Konular	29
6.3.1.	Açık Anahtarın ArŐivlenmesi	29
6.3.2.	Özel ve Açık Anahtarların Kullanım Süreleri	29
6.4.	EriŐim Denetim Verileri.....	29
6.4.1.	EriŐim Denetim Verilerinin OluŐturulması	29
6.4.2.	EriŐim Denetim Verilerinin Korunması.....	29
6.4.3.	EriŐim Denetim Verileri ile İlgili Dięer Konular	30
6.5.	Bilgisayar Güvenlięi Denetimleri	30
6.5.1.	Bilgisayar Güvenlięi ile İlgili Teknik Gereker	30
6.5.2.	Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi.....	30
6.6.	YaŐam Döngüsü Teknik Kontrolleri.....	30
6.6.1.	Sistem GeliŐtirme Kontrolleri	30
6.6.2.	Güvenlik Yönetimi Kontrolleri.....	30
6.6.3.	YaŐam Döngüsü Güvenlik Denetimleri.....	30
6.7.	Aę Güvenlięi Denetimleri	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	31
7.1.3.	Algoritma ve Nesne Tanımlayıcılar	31
7.1.4.	İsim Alanı Biçimleri	31
7.1.5.	İsim Kısıtları.....	31
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası	31
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	31
7.1.8.	İlke Niteleyiciler	31
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi	32
7.2.	Sertifika İptal Listesi Biçimi	32
7.2.1.	Sürüm Numarası	32
7.2.2.	Sertifika İptal Listesi Uzantıları.....	32
7.3.	Çevrim İçi Sertifika Durum Protokolü Biçimi	32
7.3.1.	Sürüm Numarası	32
7.3.2.	ÇİSDUP Uzantıları.....	32
8.	UYGUNLUK DENETİMLERİ.....	32
8.1.	Uygunluk Denetiminin Sıklığı	32
8.2.	Denetçinin Nitelikleri.....	32
8.3.	Denetçinin Denetlenen Tarafı Olan İlişkisi	32
8.4.	Denetimin Kapsamı	32
8.5.	Yetersizliğin Tespiti Durumunda Yapılacaklar	33
8.6.	Sonucun Bildirilmesi	33
9.	DIĞER İŐLER VE HUKUKSAL MESELELER.....	33
9.1.	Ücretlendirme	33
9.1.1.	Sertifika OluŐturma ve Yenileme Ücreti.....	33
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	34
9.2.1.	Sigorta Kapsamı	34
9.2.2.	Diđer Varlıklar	34
9.2.3.	Sertifika Mali Sorumluluk Sigortası.....	34
9.3.	Ticari Bilginin Korunması	34
9.3.1.	Gizli Bilginin Kapsamı.....	34
9.3.2.	Gizlilik Kapsamında Olmayan Bilgiler.....	34
9.3.3.	Gizli Bilginin Korunma Sorumluluđu	34
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	35
9.4.5.	Gizli Bilginin Kullanımına İzin Verilmesi	35
9.4.6.	Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması	35

9.4.7.	Diđer BaŐlıklar	35
9.5.	Telif Hakları.....	35
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	36
9.6.5.	Diđer BileŐenlerin Yüklümlülükleri.....	36
9.7.	Yüklümlülüklerden Feragat.....	36
9.8.	Sorumlulukla İlgili Sınırlamalar.....	36
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	37
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri	37
9.11.	Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme	37
9.12.	DeđiŐiklik Halleri	37
9.12.1.	DeđiŐiklik Metotları	37
9.12.2.	Bilgilendirme Mekanizması ve Sıklıđı.....	37
9.12.3.	Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar	37
9.13.	AnlaŐmazlık Halleri	37
9.14.	Uygulanacak Hukuk	37
9.15.	Uygulanabilir Yasalarla Uyum.....	38
9.16.	Diđer Hükümler	38

1. Giriő

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 iőlevleri sırasında uyulması gereken kuralları ve alıőma ilkelerini tanımlayan Sertifika İlkeleri (Sİ) dokümanıdır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Sürelere ve Teknik Kriterlere İliőkin Tebliė'de tanımlandığı 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 İletiliőim Kurulu Kararı ile yayımlanan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliőkin Usul ve Esaslar'da belirtilen tanıma uygun olarak Kurumsal Őifreleme Sertifikası hizmeti saėlamaktadır.

Kamu SM Sİ dokümanı Kurumsal Őifreleme Sertifikası hizmeti verilirken ESHS'nin kendisine özel iőlevsel ortamından baėımsız olarak sertifikaların baővuru, üretim, daėıtım, yenileme, iptal etme ile ilgili süreçler içindeki iőlemlerinin hangi genel ilkeler doėrultusunda gerekleőtirdiėini, Aık 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 karőtıladığını anlatan Sertifika Uygulama Esasları (SUE) dokümanını hazırlar ve SUE dokümanına baėlı kalarak alıőır. 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 tanımlandığı bir dokümandır. Kamu SM'den sertifika talebinde bulunan kurumlar bu dokümanda belirtilen Őartları kabul etmiőt sayılırlar.

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

Kök SHS son kullanıcılar için sertifika üretmeyip, yürüttükleri görevler aısından özel niteliėi haiz kamu kurum ve kuruluőları ile dileyen gerek ve tüzel kiőilerin kuracakları Elektronik Sertifika Hizmet Saėlayıcıları'na kök, köprü veya apraz sertifika hizmeti verir.

Kurumsal Őifreleme SHS ve Kamu SM'den kök sertifika hizmeti alan kamu kuruluőları veya özel kuruluőlar, Kök SHS'nin elektronik imzasını taşıyan sertifikaya sahiptir.

Sİ dokümanı, "İnternet Aık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları ereve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman ieriėinde belirtilen bir kısım alt baőtıkların altındaki "Düzenlenmesine gerek duyulmamıőtır" ibaresi, bu aőamada ihtiya duyulmadığından düzenleme yapılmadığını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kurumsal Őifreleme Sertifika İlkeleri

Doküman Sürüm Numarası: 03

Yayın Tarihi: 07.01.2022

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

1.3.4. Üçüncü Kişiler

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

1.3.5. Diđer Bileşenler

1.3.5.1. Kurum

Kamu SM'den Kurumsal Őifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Őifreleme Sertifikası almaya yetkisi olan tüzel kişiliktir.

1.3.5.2. Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusu

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

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı BaŐbakanlık Genelgesi ile elektronik ortamda iletilen resmi yazıların Őifreli Őekilde g3nderilebilmesine imkan saęlanmıŐtır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluŐları arasında elektronik ortamdaki belge paylaŐımında Őifreleme yapmak amacıyla e-YazıŐma Teknik Rehberi'ne uygun olarak kullanılmalıdır. Kurumsal Őifreleme Sertifikaları elektronik imzalama iin kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Őifreleme Sertifikası B3l3m 1.4.1'de belirtilen amalar dıŐında kullanılamaz. Belirtilen kapsam dıŐında kullanımdan doęan zararlardan Kamu SM sorumlu tutulamaz.

1.5. Uygulama Esaslarının Y3netimi

1.5.1. Dok3man Y3netimi

Sİ dok3manı Kamu SM tarafından yazılmıŐtır. Kamu SM, gerekli g3rd3ę3 durumlarda Sİ dok3manında deęiŐiklik yapabilir.

1.5.2. İletiŐim Bilgileri

Bu Sİ dok3manının uygulanması ve ilgili y3netim ilkeleri hakkındaki sorular Kamu SM'nin aŐaęıdaki eriŐim noktalarına y3nlendirilebilir:

Adres : Kamu Sertifikasyon Merkezi, T3BİTAK 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, Sİ dok3manını herkesin eriŐimine aık bulunan aŐaęıdaki internet adresinden yayımlar:

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

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluęunu Belirleyen KiŐi

Bu Sİ dok3manına uygun olarak yazılmıŐ olan SUE dok3manlarının uygunluęu, Kamu SM y3netimi ve y3netim tarafından yetki verilen kiŐiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosed3rleri

Bu Sİ dok3manına uygun olarak oluŐturulan SUE dok3manının uygunluęu, Kamu SM tarafından onaylanır.

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

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

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

Akıllı Kart: Sertifika ve sertifika ile iliŐkili özel anahtarın içinde bulunduđu güvenli donanım.

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

Bilgi Deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve diđer sertifika iŐlemleri ile ilgili bilgilerin yayımlandıđı izin sunucular gibi veri saklama ortamları.

ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü): Üçüncü kiŐilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öđrenmelerine imkan tanıyan standart iletiŐim kuralı.

DETSİS (Devlet TeŐkilatı Merkezi Kayıt Sistemi): Türkiye Cumhuriyeti Devlet yapısındaki tüm kurum ve kuruluşların ve alt birimlerin tekil ve deđiŐmez nitelikte numaralar ile elektronik ortamda kodlanarak tanımlandıđı sistem.

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

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

İmza Dođrulama Verisi: Elektronik imzayı dođrulamak için kullanılan Őifreler, kriptografik açık anahtarlar gibi veriler.

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

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

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 birim.

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

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

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

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

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

KURUMSAL ŐİFRELEME SERTİFİKA İLKELERİ

Kurumsal Őifreleme SHS (Kurumsal Őifreleme Sertifika Hizmet Saęlayıcısı): Kamu Sertifikasyon Merkezi iinde oluŐturulmuŐ, Kk Sertifika Hizmet Saęlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluŐturup imzalamakla yetkili kılınmıŐ Elektronik Sertifika Hizmet Saęlayıcısı.

Kurumsal Őifreleme Sertifikası Asıl Sorumlusu: Kamu kurumlarının baŐvuru formu ve taahhtname ile Kamu SM'ye bildirdięi ve Kurumsal Őifreleme Sertifikası ile ilgili srelerde kurumu temsile asıl yetkili kiŐi.

Kurumsal Őifreleme Sertifikası Yedek Sorumlusu: Kamu kurumlarının baŐvuru formu ve taahhtname ile Kamu SM'ye bildirdięi ve Kurumsal Őifreleme Sertifikası ile ilgili srelerde asıl yetkilinin bulunmaması durumunda kurumu temsile yetkili kiŐi.

Kurumsal Őifreleme Sertifikası: Elektronik ortamdaki belge paylaŐımında Őifreleme yapmak amacıyla kullanılan aık anahtar ieren elektronik sertifika.

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

zel Anahtar: Anahtar iftinin sahibi tarafından gizli tutulan ve dijital imza oluŐturmak ve/veya ilgili Aık Anahtarla ŐifrelenmiŐ elektronik kayıtların, dosyaların Őifresini zme iin kullanılan anahtar.

SİL (Sertifika İptal Listesi): İptal olmuŐ sertifika bilgilerinin iinde yer aldıęı, ESHS'nin imzasını taşıyan elektronik dosya.

Sertifika Sahibi: Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan ve sertifikayı kullanma yetkisine sahip tzel kiŐi.

Sertifika Sresi: retim anında sertifikanın iine yazılan, sertifikanın geerlilik baŐlangı ve bitiŐ tarihleri arasında kalan sre.

Sİ ve SUE (Sertifika İlkeleri ve Uygulama Esasları): Kamu SM resmi web sitesi Bilgi Deposu mens altındaki İlke ve Uygulama Esasları'nda Elektronik Sertifika Hizmet Saęlayıcısı'nın (ESHS) iŐleyiŐi ile ilgili genel kuralları ve bu kuralların nasıl uygulanacaęını detaylı olarak anlatan belgeler.

nc KiŐiler: Sertifikalara gvenerek iŐlem yapan gerek veya tzel kiŐiler.

Zaman Damgası: Bir elektronik verinin, retildięi, deęiŐtirildięi, gnderildięi, alındıęı ve/veya kaydedildięi zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doęrulan kayıt.

1.6.2. Kısaltmalar

BGYS: Bilgi Gvenlięi Ynetim Sistemi

BTK: Bilgi Teknolojileri ve İletifim Kurumu

CEN (Comit Europen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN alıŐtay Kararı

İSDUP (OCSP): evrim İi Sertifika Durum Protokol (Online Certificate Status Protocol)

EAL (Evaluation Assurance Level): Deęerlendirme Garanti Dzeyi

ECDSA (Elliptical Curve Digital Signature Algorithm): Eliptik Eęrisi Sayısal İmza Algoritması

ESHS: Elektronik Sertifika Hizmet Saęlayıcısı

ETSI (European Telecommunications Standards Institute): Avrupa Telekomnikasyon Standartları Enstits

ETSI TS (ETSI Technical Specification): ETSI Teknik zellikleri

FIPS PUB (Federal Information Processing Standards Publications): Federal Bilgi İŐleme 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 kişilerin baş harfleri)

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayınlama ve Bilgi Deposu Yükümlülükleri

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması

Kamu SM'nin sistem bileŐenlerinin erişimine açacağı bilgi deposunda sistemin iç işleyiŐi ile ilgili olanlar hariç olmak üzere aŐağıdaki 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 Kök SHS sertifikalarının özet deĐerleri ile özet deĐerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduĐu bilgisi
- Kamu SM Sİ ve SUE dokümanları
- Taahhütnameler
- Yönergeler
- Formlar
- Sertifika iptal durum kayıtları

2.3. Yayım Sıklığı ve Zamanı

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

Sertifika iptal durum kayıtlarının yayımlanma sıklığı ilgili SUE dokümanında 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 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 Teşhise Elverişli Olması

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

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

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

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

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

3.1.5. Kimlik Bilgilerinin Tekilliği

Kurumsal Şifreleme Sertifikası içeriğindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum için ayırt edici niteliktedir. Kurumsal Şifreleme Sertifikalarının isim alanı içinde benzersiz bir sayı olduğu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

3.1.6. Markanın Tanınması, Doğrulması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

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

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

Sertifika sahibine ait açık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir ve Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusuna teslim edilir. Asıl veya Yedek Sorumlu tarafından Kurumsal Şifreleme Sertifikasının teslim alındığı teyit edilir. Ek olarak, HSM'ye yüklenmesi talep edilen sertifikalar için Kurum HSM Cihaz Sorumlusu tarafından imzalanan teslim tutanağı ile teyit işlemi yapılır.

3.2.2. Kurumsal Kimliđin Belirlenmesi

Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini, kurumu temsile yetkili kiŐilerin imzaladıđı ve kurumun onayını taŐıyan resmi yazı ile Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi ile Kamu SM'ye bildirir. Kamu SM, baŐvuru formunda yer alan bilgilere istinaden kurum kimliđini belirler. Kurumların sertifika alma yetkisi DETSİS sorgusu aracılıđıyla kontrol edilir.

3.2.3. KiŐisel Kimliđin Belirlenmesi

Kurumsal Őifreleme Sertifikası, kurum adına verildiđinden yalnızca kurumsal baŐvuru kabul edilmektedir.

3.2.4. Dođrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika 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.

3.2.5. Yetkinin Dođrulanması

Sertifika içeriđine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıŐtır.

3.3. Sertifika Yenileme İsteđinde Kimlik Dođrulama

SUE Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.3.1. Olađan Sertifika Yenileme İsteđinde Kimlik Dođrulama

SUE Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Dođrulama

SUE Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.4. Sertifika İptal İsteđinde Kimlik Dođrulama

Sertifika sahibi kurumun yetkilendirdiđi sertifika sorumluları Kamu SM resmi web sitesinde yer alan Online İŐlemlere kimlik dođrulamasıyla giriŐ yaparak iptal iŐlemini gerŐekleŐtirebilir. Online İŐlemler adresine ulaŐılamaması durumunda Kamu SM'ye Elektronik Mühür/Kurumsal Őifreleme Sertifikası İptal BaŐvuru Formu resmi yazısı ile birlikte gönderilerek iptal iŐlemi gerŐekleŐtirilebilir. Kurum kimlik dođrulaması ve iptal iŐleminin teyidi SUE Bölüm 3.4'te anlatıldıđı Őekilde gerŐekleŐtirilir.

4. İŐlemsel Gereker

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

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 kuruluŐları Kurumsal Őifreleme Sertifikası baŐvurusunda bulunabilirler.

4.1.2. Kayıt İŐlemleri ve Sorumluluklar

Kurumsal Őifreleme Sertifikası baŐvurusu, kamu kurum veya kuruluŐu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacaĐı sertifika hizmetlerinin Őartları TŪBİTAK BİLGEM ile karŐılıklı imzalanan sŖzleŐmeler ve/veya kurumun imzaladıĐı Elektronik MŪhŪr/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve TaahhŪtnamesi, Kamu SM'nin internet ūzerinden yayımladıĐı ilgili yŖnergeler, Sİ ve SUE dokŪmanları doĐrultusunda belirlenir.

Kurum baŐvuru sırasında Kamu SM'ye doĐru bilgi beyan etmekle sorumludur. Kurum, Kamu SM'ye gŖndermiŐ olduĐu bilgilerin doĐruluĐunu takip etmekle ve bu bilgilerde deĐiŐiklik olması halinde belirlenmiŐ araç ve yŖntemler ile Kamu SM'yi bilgilendirmekle yūkŪmlŪdŪr. Kamu SM, Kurumsal Őifreleme Sertifikası içinde yer alacak bilgilerin doĐruluĐunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliĐini saĐlamak için gerekli tedbirleri alır.

Kayıt iŐlemleri ve sorumluluklar ile ilgili detaylı bilgi SUE BŖlŪm 4.1.2'de yer almaktadır.

4.2. Sertifika BaŐvurusunun İŐlenmesi

4.2.1. Kimlik Tanımlama ve DoĐrulama İŐlevlerinin Yerine Getirilmesi

BaŐvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve doĐrulama iŐlevleri yerine getirilir. Kurumdan gŖnderilen belgelerin doĐrulanması için yapılan iŐlemler SUE BŖlŪm 4.2.1'de yer almaktadır.

4.2.2. Sertifika BaŐvurusunun Kabul veya Reddi

Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 29.05.2019 tarihli ve 2019/DK-BTD/160 sayılı Kurul Kararı ile "Kamu Kurum ve KuruluŐları Arasında Elektronik Ortamdaki Belge PaylaŐımında Kullanılan Kurumsal Őifreleme ve Elektronik MŪhŪr Sertifikalarına iliŐkin Usul ve Esaslar" yayımlanmıŐtır. İlgili Karar ikinci bŖlŪm, 5'inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS'te bilgileri bulunmayan veya Kurumsal Őifreleme Sertifikası almaya yetkisi olmayan tarafların baŐvurusunu reddeder.

4.2.3. Sertifika BaŐvurusunun İŐlenme Zamanı

BaŐvuru evraklarının eksiksiz bir Őekilde Kamu SM'ye ulaŐması ve doĐrulanması ardından en fazla 15 (on beŐ) iŐ gūnŪ içerisinde sertifika baŐvurusu iŐleme alınır ve sonuçlandırılır.

4.3. Sertifikanın OluŐturulması

4.3.1. Sertifika OluŐturulmasında ESHS'nin İŐlevleri

SUE BŖlŪm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika baŐvuruları Kamu SM tarafından iŐlenir. Kurum, iŐlem kapasitesini gŖz Ŗnūnde bulundurarak baŐvuru sırasında sertifikanın yūkleneceĐi 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 ūzere 2 adet ūretilir.

4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

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

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

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul KoŐulu

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

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

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

4.4.3. Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması

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

4.5. Sertifikanın ve Özel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

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

4.5.2. Üçüncü KiŐilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifika sahibine ait Kurumsal Őifreleme Sertifikasının içinde yer alan açık anahtar, üçüncü kişilerce EYP 2.0 kapsamında verilerin Őifreli iletimi amacıyla kullanılır. Açık anahtarın veya sertifikanın, belirtilen amaç dıŐında kullanılması sonucu oluŐabilecek zararlardan üçüncü kişiler 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 bu iŐlemi gerçekteŐirmez.

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 gerçekteŐirilir.

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 Başvurusunun 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 Tarafıara Duyurulması

SUE Bölüm 4.7.7'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Deęiőiklięi

Sertifika ierięinde yer alan bilgilerde deęiőiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi deęiőiklięinin gerekli olduęu durumlarda, kurum SUE Bölüm 4.7'de belirtilen sertifika yenileme sürecini iőletmelidir.

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. Sertifikanın iptalini gerektiren durumlar SUE Bölüm 4.9.1'de verilmiőtir.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiőt Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından yapılabilir. Kamu SM, SUE Bölüm 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İőlenmesi

Kurumsal Őifreleme Sertifikası iptal iőlemi, kurum tarafından yetkilendirilen Kurumsal Őifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından Kamu SM resmi internet sitesinde yer alan Online İőlemler menüsü aracılıęı ile yapılır. İptal iőlemlerinin Kamu SM Online İőlemler üzerinden yapılamadıęı durumda süreç SUE Bölüm 4.9.3'te belirtildięi Őekilde iőletilir.

4.9.4. İptal İsteęi Ertelenme Süresi

Böyle bir süre öngörölmemiőtir.

4.9.5. İptal İsteęinin İőlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal iőleme alır ve Kurumsal Őifreleme Sertifikasını en geç 24 saat ierisinde iptal eder. İptal edilen Kurumsal Őifreleme Sertifikası bilgisini bir sonraki SİL iinde yayımlar, İSDUP Yanıtlayıcıdan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi iinde iőlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 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 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, belirtilen yayımlama zamanından en geç 5 (beş) dakika sonra yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

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

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. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiđi ölçüde ÇİSDUP kullanmaları gerekir.

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 Şifreleme Sertifikası iptal edilir. Kurumsal Şifreleme Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

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

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi

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

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Kurumsal Şifreleme Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden veya Online İşlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika

sorumları 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 12 (on iki) saat süresince 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. 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 Yanıtlayıcıdan öğrenebilirler. Üçüncü kişiler, Kurumsal Őifreleme 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 Őifreleme Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda değildir; sertifika sahibi sertifikanın kullanım süresinin dolduğu 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 anlatılmıştır.

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM sisteminin çalıştığı cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiği yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır. Güvenli alanlara erişimlerin kaydı tutulmaktadır.

5.1.1. Tesis Yeri ve İnŐaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütölmektedir. Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkan saęlayan yapıdadır. Alanlara ve binalara erişim, tek kişinin girişine veya çıkışına izin veren HI-SEC kilitleme kapıları dahil olmak üzere fiziki güvenlik, video izleme ve kimlik doğrulama olmak üzere çoklu güvenlik ile korunmaktadır. Bina içinde, yazılım ve donanım modüllerinin yerleŐtirilmesi için kilitli ve giriş kontrollü odalar bulunur.

5.1.2. Fiziksel EriŐim

Kamu SM yazılım ve donanım modülleri ile arŐivlere erişim denetim altındadır. Binaya girişler güvenlik görevlilerinin kontrolü altında, gelişmiş erişim kontrol cihazlarıyla saęlanmaktadır.

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kaęıt ortamdaki bilgilerin tutulduęu, sistemin işletildięi ve yönetildięi odalara erişim gelişmiş erişim kontrol cihazlarıyla yapılmaktadır.

5.1.3. Güç Kaynaęı ve Havalandırma

Kamu SM işlevlerinin yerine getirilmesi ve süreklilięin saęlanması için sistem, kesintisiz güç kaynaęı ile beslenir. Bina gerekli havalandırma sistemi ile donatılır.

5.1.4. Su Baskınları

Kamu SM işlevlerinin yerine getirildięi ortamlarda su baskınlarından en az zarar görecektir. Önlemler alınmıştır.

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kaęıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve artık kullanılmayan elektronik veya kaęıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir.

5.1.8. Farklı Mekanlarda Yedekleme

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

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Güvenilir roller, SUE Bölüm 5.2.1'de detaylandırılır.

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, imza oluŐturma verilerinin baŐka bir kriptografik modl ierisine yedeklenmesi iin birden fazla kiŐinin 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.

5.2.4. Grevlerin Ayrılmasını Gerektiren Roller

Kamu SM iinde, aynı kiŐinin birden fazla grevde bulunmasını engelleyecek sınırlamalar getirilebilir.

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.

5.3.2. GemiŐ AraŐtırması

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

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

5.3.4. Srekli Eėitim Gerekleri ve Sıklıėı

Kamu SM sisteminde yapılan deėiŐikliklerin bildirilmesi amacıyla personele verilen eėitimler gerekli grldkce tekrarlanır. Yeni greve baŐlayanlar iin eėitimler tekrarlanır.

5.3.5. Grev DeėiŐim Sıklıėı 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 diėer yetkisiz eylemlerde ilgili mevzuat gereėince bilgi gvenliėi 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 yaptığı 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 kaĐıt zerindedir. Denetimler sırasında gerekli grldĐi takdirde bu kayıtlar grevliler tarafından incelenir.

5.4.1. Kaydedilen İŐlemler

Kamu SM sisteminde, SUE Blm 5.4.1’de belirtilen elektronik veya kaĐıt ortamda yapılan iŐlerin kayıtları tutulur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin iŐleyiŐiyle ilgili tutulan kayıtlar dzgn zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir gvenlik aĐı olup olmadığı kontrol edilir.

5.4.3. Kayıtların Saklanma Sresi

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

5.4.4. Kayıtların Korunması

Kamu SM’ye ait kayıtlar, izinsiz izlenmeyi, deĐiŐtirmeyi ve silinmeyi engelleyecek Őekilde elektronik ve fiziksel olarak gvenli tutulur.

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliĐi gz nne alındıĐında her gn dzenli olarak, sistemin yoĐun olarak kullanılmadığı bir saatte gerekli grlen kayıtların evrim ii yedeĐi alınmaktadır. Kritik kayıtlar ayrı bir Őehirde bulunan gvenli felaket kurtarma merkezlerine yedeklenmektedir.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, aĐ katmanında ve iŐletim seviyesi dzeyinde otomatik olarak toplanır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

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

5.4.8. Saldırıya Aıklığın DeĐerlendirilmesi

Denetim kayıtlarının tutulduĐu sistemler iin SUE Blm 6.5, 6.6 ve 6.7’de sz geen teknik gvenlik 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 kağıt 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 kağıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir.

5.6. Anahtar Deęiřimi

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

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 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 OluŐturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin Kurumsal Őifreleme Sertifikalarını imzalamada kullandığı imza oluŐturma verisinin gizliliğinin kaybedildiğinden Őüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve SUE Bölüm 5.7.3'te belirtilen işlemler yerine getirilir.

5.7.4. Arıza Sonrası Yeniden ÇalıŐırlık

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

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, işleyişine Elektronik İmza Kanunu'nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verebilir. Bu durumda Kamu SM'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 ürettiği, sertifika yönetim işlemlerini gerçekleŐtirdiği 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 Yayımlayıcı Anahtar Çifti Üretimi

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcıya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği güvenli odada, birden fazla eğitimli personelin gözetiminde, ağ 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 özel anahtar 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 Őifreleme Sertifikası akıllı karta yüklenecekse, sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

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

Sertifika sahibine ait özel anahtarın yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandığı akıllı kart veya HSM SUE Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine Özel Anahtarın Ulaőtırılması

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

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısına Açık Anahtarın Ulaőtırılması

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

Kurumsal Şifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Şifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildięi için açık anahtarın Kamu SM'ye ulaőtırılması söz konusu deęildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

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 kullanılan algoritmaların güvenliği ispatlanmış ve dünyaca kabul görmüştür. Algoritmaların gerçekleştiriminde kullanılan yöntemler gerekli güvenlik kriterlerini sağlar. Anahtarları üreten programlar gerekli güvenlik testlerinden geçirilirler.

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan anahtarların hangi amaçlar için kullanılabilereceęi 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 dokümanında detaylı olarak bulunmaktadır. ÇİSDUP yanıtlarının imzalanmasında alt kök ve kök tarafından yetkilendirilmiş ÇİSDUP sertifikası kullanılır.

6.2. Özel Anahtarın Korunması

6.2.1. Kriptografik Modül Standartları

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

6.2.2. Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim

Kamu SM'ye ait imza oluŐturma verisinin bulunduĐu odaya eriŐim aynı anda 2 (iki) alıŐan tarafından saĐlanmaktadır.

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıŐtır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeĐinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi iin saĐlanan güvenlik ile eŐdeĐer güvenlik önlemleri altında yapılır. 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 süreleri sonunda geri dönüŐsüz Őekilde silinir.

6.2.6. Özel Anahtarın Kriptografik Modüle Yüklmesi

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

Sertifika sahiplerine ait özel anahtarlar, sadece yetkili personelin kontrolünde akıllı kart veya HSM cihazına Őifrelenerek yüklenir. Özel anahtar, akıllı kart veya HSM cihazına yüklendikten sonra kopyası sistemden silinir.

6.2.7. Özel Anahtarın Kriptografik Modülde Saklanması

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

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

6.2.8. Özel Anahtara EriŐim

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

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

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

6.2.9. Özel Anahtara EriŐimin Kesilmesi

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

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

6.2.10. Özel Anahtarın Yok Edilmesi

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

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

6.2.11. Kriptografik Modülün Değerlendirilmesi

Kamu SM, SUE 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 önlemler alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Kurumsal Şifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Üretilen Kurumsal Şifreleme Sertifikalarının son kullanma tarihi, Kurumsal Şifreleme SHS Sertifikasının son kullanma tarihini aşamaz.

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. Erişim Denetim Verileri

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

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

6.4.1. Erişim Denetim Verilerinin Oluşturulması

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

6.4.2. Erişim Denetim Verilerinin Korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir.

Sertifika sahibi kuruma ait erişim parolaları sertifika sahibi kuruma güvenli yöntemlerle ulaştırılır.

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

6.4.3. Erişim Denetim Verileri ile İlgili Diğer Konular

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

6.5. Bilgisayar Güvenliđi Denetimleri

6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereker

Kamu SM sistemi içinde, son teknolojik gelişmeler göz önünde bulundurularak bilgisayar güvenliđi sağlanır. Bilgisayar güvenliđiyle ilgili teknik gerekler SUE Bölüm 6.5.1’de açıklanmaktadır.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler SUE Bölüm 6.6.1’de açıklanmaktadır.

6.6.2. Güvenlik Yönetimi Kontrolleri

Sistem içindeki yazılım ve donanım ürünleri ile ağ ortamının belirlenen güvenlik şartlarını sağlayıp sağlamadığı, test cihazları ve test prosedürleri kullanılarak kontrol edilir. Güvenlik kontrolleri için temel dayanak ISO 27001’in güncel sürümüdür.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliđi Denetimleri

Kamu SM sisteminde son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliđi denetimleri yapılır. Ağ güvenliđi denetimlerine ilişkin 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 dağıtılan Kurumsal Şifreleme 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 dağıtılan Kurumsal Őifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili açık anahtar, sertifika sahibi kurumun adı ve DETSİS numarası, sertifikayı yayımlayan Kamu SM'ye ait isim bilgileri ve Kamu SM'nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını içerir. Kurumsal Őifreleme Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine baęlı olarak belirlenir.

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

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 algoritması anahtar çiftleridir.

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

7.1.4. İsim Alanı Biçimleri

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

7.1.5. İsim Kısıtları

SUE Bölüm 7.1.5'te belirtilmektedir.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

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

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Kurumsal Őifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Őifreleme Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikasının "Sertifika İlkeleri Uzantısı"¹nin içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici"² olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

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

¹ Certificate Policies

² Policy Identifier

7.1.9. Kritik BelirtilmiŐ Olan İlke Belirleyici Uzantılarının İŐlenmesi

Düzenlenmesine gerek duyulmamıŐtır.

7.2. Sertifika İptal Listesi BiŐimi

7.2.1. Sürüm Numarası

Kamu SM'nin ürettiĐi SİL'ler "ITU X.509 V.2" SİL formatına uygundur.

7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL'ler "ITU X.509" SİL formatına uygun olarak SUE Bölüm 7.2.2.'de belirtilen bilgileri içerir.

7.3. Çevrim İçi Sertifika Durum Protokolü BiŐimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları SUE Bölüm 7.3.2'de belirtilen bilgileri içerir.

8. Uygunluk Denetimleri

Kamu SM, ISO/IEC 27001 bilgi güvenliĐi yönetim standardına uygun olarak hizmet verir ve standart gereĐi düzenli olarak iç ve dış denetimlere tabi tutulur.

8.1. Uygunluk Denetiminin SıklıĐı

Kamu SM, ISO/IEC 27001 bilgi güvenliĐi yönetim sistemi standardı gereĐince yılda bir defa uygunluk denetimi geçirir. Her üç yılda bir sertifika yenilenir.

İç denetim, yılda bir defa gerçekleştirilir.

8.2. Denetçinin Nitelikleri

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

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

8.3. Denetçinin Denetlenen Tarafı Olan İliŐkisi

Dış denetçiler, herhangi bir çıkar çatıŐması olmaması ve baĐımsızlıĐın zedelenmemesi için Kamu SM'den baĐımsız kişilerden oluşur. İç denetim için seçilen denetçiler ise denetlenecek birimden seçilmez.

8.4. Denetimin Kapsamı

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

ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun şekilde baĐımsız kurum denetçisi tarafından belirlenir.

8.5. Yetersizliđin Tespiti Durumunda Yapılacaklar

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

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

8.6. Sonucun Bildirilmesi

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

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

9. Diđer İřler ve Hukuksal Meseleler

9.1. cretlendirme

9.1.1. Sertifika Oluřturma ve Yenileme creti

Kamu SM tarafından retilen, yenilenen ve gncellenen Kurumsal Őifreleme Sertifikası iin kurumlardan cret alınır. cretin miktarı ve deme řekli Kamu SM web sitesinde bildirilir.

Kamu SM'nin imza oluřturma verisinin alınması, kaybolması, gizliliđinin veya gvenilirliđinin ortadan kalkması, sertifika ilkelerinin deđiřmesi ya da Kurumsal Őifreleme Sertifikasının hatalı retilmesi gibi sertifika sahibi kurumun kusurunun bulunmadıđı durumların sonucunda Kurumsal Őifreleme Sertifikalarının Kamu SM tarafından iptal edilmesi ve gncellenmesi halinde, hibir cret talep edilmez.

9.1.2. Sertifika Eriřim creti

Kamu SM, kendisine ait sertifikaları resmi web sitesinde cretsiz olarak yayımlar. Kamu SM tarafından retilen Kurumsal Őifreleme Sertifikaları DETSİS'e yklenir.

9.1.3. İptal Durum Kaydına Eriřim creti

Kamu SM, iptal durum kaydını SİL veya İSDUP aracılıđıyla duyurma hizmeti iin, sertifika sahibi kurumdan veya nc kiřilerden cret talep etmez.

9.1.4. Diđer Servis cretleri

Sertifika ynetim prosedrleri iin elektronik ortamdan ve ađrı merkezi zerinden otomatik olarak gerekleřtirilen iřlemlerden cret talep edilmez.

Kamu SM, bilgi deposundan yayımladıđı bilgi ve dokmanlara eriřim iin sertifika sahibi kurumdan veya nc kiřilerden cret talep etmez.

9.1.5. İade creti

n demeli olarak talepte bulunulan sertifikanın/sertifikaların retimi tamamlanmamıřsa kurumun talebi dođrultusunda yatırılan miktar kadar cret iadesi yapılır. retilen sertifikalar iin cret iadesi sz konusu deđildir.

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

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. Kişisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

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

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurumun ve yetkilendirdiđi Kurumsal Şifreleme Sertifikası Asıl ve Yedek Sorumlusu ile Kurum HSM Cihaz Sorumlusunun, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiđi bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

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

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 kiŐisel bilgileri sertifika hizmeti vermek dıŐında 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 yetkilendirilmiş çalıŐanlar sertifika sahibi kurumun bilgilerine eriŐirler.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM sertifika sorumlularının yazılı rızası ile kiŐisel bilgileri üçüncü kiŐilerle paylaşabilir.

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM 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 SUE dokümanına bađlı olarak geliŐtirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlölükler

Kamu SM tarafından verilen sertifika hizmetlerinde sistem bileŐenleri olarak tanımlanan Kamu SM, sertifika sahipleri ve üçüncü kiŐiler 2017/21 Sayılı BaŐbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslarda belirtilen Őekilde üzerlerine düşen yükümlölükleri sađlar.

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kiŐiler yasa ve yönetmeliklerde belirtilmediđi halde imzalanmıŐ olan Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnameyi yükümlölüklerini de yerine getirirler.

9.6.1. Elektronik Sertifika Hizmet Sađlayıcısı Yükümlölükleri

Kamu SM'nin ESHS olarak iŐleyiŐinin güvenli olabilmesi için, sistem bileŐenlerinin yerine getirmesi gereken yükümlölükler SUE Bölüm 9.6.1'de açıklanmaktadır.

9.6.2. Kayıt Birimi Yükümlölükleri

Kayıt birimlerinin yükümlölükleri SUE Bölüm 9.6.1'de belirtilen ESHS yükümlölükleri ile aynıdır.

9.6.3. Sertifika Sahibinin Yükümlölükleri

Sertifika sahibinin yükümlölükleri SUE Bölüm 9.6.3'te açıklanmaktadır.

Sertifika sahibi kurum, Kamu SM Kurumsal Őifreleme Sertifikası Sİ ve SUE dokümanlarında belirtilen Őartları okuduđunu, baŐvuru süreci ve sertifika geçerliliđi boyunca Elektronik Mühür/Kurumsal

Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi, ilgili mevzuatlar ile Sİ ve SUE dokümanında belirtilen Őartlara uygun olarak hareket edeceđini kabul ve taahhüt eder. Yüklümlülüklerin ihlali nedeniyle üçüncü kiŐilerin/kurumun zarara uğraması halinde TÜBİTAK BİLGEM'in ödemek zorunda olduđu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü KiŐilerin Yüklümlülükleri

Üçüncü kiŐiler, Kurumsal Őifreleme Sertifikasıyla iŐlem yapmadan önce SUE Bölüm 9.6.4'te belirtilen sertifika geçerlilik kontrollerini yapmakla yüklümlüdür.

9.6.5. Diđer BileŐenlerin Yüklümlülükleri

9.6.5.1. Kurumun Yüklümlülükleri

Kamu SM'ye sertifika baŐvurusunda bulunan kurumun yüklümlülükleri SUE Bölüm 9.6.5.1'de belirtilmektedir.

9.6.5.2. Kurum Sertifika Sorumlularının Yüklümlülükleri

Kurum adına Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusunun yüklümlülükleri SUE Bölüm 9.6.5.2'de belirtilmektedir.

9.7. Yüklümlülüklerden Feragat

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

9.8. Sorumlulukla İlgili Sınırlamalar

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

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahibi kurum, Elektronik Mühür/Kurumsal Őifreleme Sertifikası BaŐvuru Formu ve Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile iŐ birliđi içinde çalıŐır; süreçleri yerine getirirken gerekli desteđi ve koordinasyonu Sİ ve SUE dokümanlarında belirtilen Őartlar altında sağlar.

9.10.1. Anlaşma Süresi

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

9.10.2. AnlaŐmanın Sona Ermesi

Kamu SM ile kurum arasında varsa imzalanan sözleŐme SUE Bölüm 9.10.2’de belirtilen durumlarda sonlandırılabilir.

9.10.3. AnlaŐmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleŐmenin sona ermesiyle hizmeti alan kurumun, sözleŐme ile Sİ ve SUE dokümanlarında belirtilen Őartları saėlamakla ilgili yükümlölükleri ortadan kalkar. Kamu SM kurumdan sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmıŐ başvurular ile ilgili iŐlemler, anlaŐmanın sona erme sebebine baėlı olarak kurumun talep etmesi durumunda devam eder.

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 aracılıėıyla saėlanır. Sertifika yönetimiyle ilgili kritik görölen iŐlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

9.12. DeėiŐiklik Halleri

9.12.1. DeėiŐiklik Metotları

Sİ dokümanı Kamu SM tarafından yazılmıŐtır. Bu Sİ dokümanında yapılabilecek deėiŐiklikler ekleme ve deėiŐtirme Őeklinde olabileceėi gibi Kamu SM dokümanın tamamen yenilenmesine de karar verebilir. Bu Sİ dokümanının herhangi bir kısmının yanlıŐ ya da gečeersiz olduėu ortaya çıksa bile Sİ dokümanının diėer kısımları, Sİ dokümanı güncellenene kadar gečeirliliėini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklıėı

Sİ dokümanında yapılan deėiŐiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden eriŐime aėılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandıėı tarihte yürürlüėe girer.

9.12.3. Nesne Tanımlama Numarasının DeėiŐmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıŐtır.

9.13. AnlaŐmazlık Halleri

Taraflar arasında çıkan tüm anlaŐmazlıkların sulhen çözümlü esastır. İhtilafların çözümlünde 2017/21 Sayılı BaŐbakanlık Genelgesi, Bilgi Teknolojileri ve İletifim Kurulu Kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge PaylaŐımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslara başvurulur. İhtilafların sulhen çözümlünün mümkün olmaması halinde, ihtilafların çözümlünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri’dir.

9.14. Uygulanacak Hukuk

Sİ dokümanındaki hükümler, 2017/21 Sayılı BaŐbakanlık Genelgesi, Bilgi Teknolojileri ve İletifim Kurulu kararıyla yayımlanan Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge PaylaŐımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslara uygun olarak yazılmıŐtır.

9.15. Uygulanabilir Yasalarla Uyum

Ői dokümanında geen hkmlerin daha sonra yrrlęe girecek ilgili mevzuata aykırı bulunması halinde dokmanda gerekli deęiŐiklikler yapılarak uygun hale getirilir.

9.16. Dięer Hkmler

Dzenlenmesine gerek duyulmamıŐtır.