

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŞİFRELEME SERTİFİKA İLKELERİ

Doküman Kodu

POL.05.02

Revizyon No

03

Revizyon Tarihi

07.01.2022

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

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 Saęlayıcısı	10
1.3.2.	Kayıt Birimleri	10
1.3.3.	Sertifika Sahipleri	10
1.3.4.	Üçüncü Kiőiler	10
1.3.5.	Dięer 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.	İletiőim Bilgileri	11
1.5.3.	Sertifika Uygulama Esaslarının İlkelere Uygunluęunu 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 Yayımlanması	14
2.3.	Yayım Sıklıęı ve Zamanı	14
2.4.	Eriőim Kontrolleri	15
3.	KİMLİK BELİRLEME VE DOęRULAMA	15
3.1.	İsmlendirme	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 Tekillięi	15
3.1.6.	Markanın Tanınması, Doęrulanması ve Rolü	15
3.2.	İlk Kimlik Belirleme	15
3.2.1.	Özel Anahtar Sahiplięinin Kanıtlanması	15
3.2.2.	Kurumsal Kimlięin Belirlenmesi	16
3.2.3.	Kiőisel Kimlięin Belirlenmesi	16
3.2.4.	Doęrulanmayan Sertifika Sahibi Bilgileri	16
3.2.5.	Yetkinin Doęrulanması	16
3.2.6.	Uyum Kriterleri	16
3.3.	Sertifika Yenileme İsteęinde Kimlik Doęrulama	16
3.3.1.	Olaęan Sertifika Yenileme İsteęinde Kimlik Doęrulama	16

3.3.2.	İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama	16
3.4.	Sertifika İptal İsteğinde Kimlik Doğrulama	16
4.	İŐLEMSEL GEREKLER	16
4.1.	Sertifika Başvurusu	17
4.1.1.	Sertifika Başvurusunu Kimlerin Yapabildiđi	17
4.1.2.	Kayıt İşlemleri ve Sorumluluklar	17
4.2.	Sertifika Başvurusunun İşlenmesi	17
4.2.1.	Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi	17
4.2.2.	Sertifika Başvurusunun Kabul veya Reddi	17
4.2.3.	Sertifika Başvurusunun İşlenme Zamanı	17
4.3.	Sertifikanın OluŐturulması	17
4.3.1.	Sertifika OluŐturulmasında ESHS'nin İşlevleri	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 Yayınlanması	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 Anahtarı 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 İşlenmesi	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 Yayınlanması	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 Başvurusunu Kimler Yapabilir	19
4.9.3.	Sertifika İptal Başvurusunun İşlenmesi	19
4.9.4.	İptal İsteđi Ertelenme Süresi	19
4.9.5.	İptal İsteđinin İşlenme Süresi	19
4.9.6.	Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol Gerekliliđi	20
4.9.7.	Sertifika İptal Listesi Yayınlama Sıklıđı	20
4.9.8.	Sertifika İptal Listesi Yayınlama 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 Başvurusunu Kimlerin Yapabildiđi.....	20
4.9.15.	Sertifika Askıya Alma Başvurusunun İşlenmesi	20
4.9.16.	Askıda Kalma Süresi.....	21
4.10.	Sertifika Durum Servisleri.....	21
4.10.1.	İşletimsel Özellikleri.....	21
4.10.2.	Servisin Erişilebilirliđi	21
4.10.3.	İsteđe Bađlı Özellikler.....	21
4.11.	Sertifika Sahipliđinin Sona Ermesi.....	21
4.12.	Anahtar Yeniden Üretme	21
5.	YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER.....	21
5.1.	Fiziksel Güvenlik Denetimleri	21
5.1.1.	Tesis Yeri ve İnşaatı.....	22
5.1.2.	Fiziksel Erişim	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 İşlem için Gereken Kişi Sayısı.....	23
5.2.3.	Kimlik Doğrulama ve Yetkilendirme.....	23
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	23
5.3.	Personel Güvenlik Kontrolleri	23
5.3.1.	Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri	23
5.3.2.	Geçmiş Araştırması	23
5.3.3.	Eđitim Gerekleri	23
5.3.4.	Sürekli Eđitim Gerekleri ve Sıklıđı	23
5.3.5.	Görev Deđişim Sıklıđı ve Sırası.....	23
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	23
5.3.7.	Anlaşmalı Personel Gereksinimleri	24
5.3.8.	Sađlanan Dokümantasyon	24
5.4.	Denetim Kayıtları	24
5.4.1.	Kaydedilen İşlemler	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 Arşivleme	25
5.5.1.	Arşivlenen Kayıt Bilgileri.....	25

5.5.2.	Arşivlerin Tutulma Süresi	25
5.5.3.	Arşivlerin Korunması	25
5.5.4.	Arşivlerin Yedeklenmesi	25
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri	25
5.5.6.	Arşivlerin Toplanması	25
5.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu	25
5.6.	Anahtar Değişimi	25
5.7.	Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	25
5.7.1.	Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi	25
5.7.2.	Donanım, Yazılım veya Veri Bozulması	25
5.7.3.	İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi	26
5.7.4.	Arıza Sonrası Yeniden Çalışırılık	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 Ulaştırılması	27
6.1.3.	Elektronik Sertifika Hizmet Sağlayıcısına Açık Anahtarın Ulaştırılması	27
6.1.4.	Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması	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 Kişi Kontrolünde Erişim	28
6.2.3.	Özel Anahtarın Yeniden Elde Edilmesi	28
6.2.4.	Özel Anahtarın Yedeklenmesi	28
6.2.5.	Özel Anahtarın Arşivlenmesi	28
6.2.6.	Özel Anahtarın Kriptografik Modüle Yüklenmesi	28
6.2.7.	Özel Anahtarın Kriptografik Modülde Saklanması	28
6.2.8.	Özel Anahtara Erişim	28
6.2.9.	Özel Anahtara Erişimin Kesilmesi	28
6.2.10.	Özel Anahtarın Yok Edilmesi	29
6.2.11.	Kriptografik Modülün Değerlendirilmesi	29
6.3.	Anahtar Çifti Yönetimiyle İlgili Diğer Konular	29
6.3.1.	Açık Anahtarın Arşivlenmesi	29
6.3.2.	Özel ve Açık Anahtarların Kullanım Süreleri	29
6.4.	Erişim Denetim Verileri	29
6.4.1.	Erişim Denetim Verilerinin Oluşturulması	29
6.4.2.	Erişim Denetim Verilerinin Korunması	29
6.4.3.	Erişim Denetim Verileri ile İlgili Diğer Konular	30
6.5.	Bilgisayar Güvenliği Denetimleri	30
6.5.1.	Bilgisayar Güvenliği ile İlgili Teknik Gereklere	30
6.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi	30

6.6.	Yařam Döngüsü Teknik Kontrolleri.....	30
6.6.1.	Sistem Geliřtirme Kontrolleri	30
6.6.2.	Güvenlik Yönetimi Kontrolleri.....	30
6.6.3.	Yařam Döngüsü Güvenlik Denetimleri.....	30
6.7.	Ađ Güvenliđi 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.	DİĐER İŐLER VE HUKUKSAL MESELELER.....	33
9.1.	Ücretlendirme.....	33
9.1.1.	Sertifika Oluřturma ve Yenileme Ücreti.....	33
9.1.2.	Sertifika Eriřim Ücreti	33
9.1.3.	İptal Durum Kaydına Eriřim 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 Bařlıklar	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 Kişilerin Yüklümlülükleri	36
9.6.5.	Diđer Bileşenlerin Yüklümlülükleri.....	36
9.7.	Yüklümlülüklerden Feragat.....	36
9.8.	Sorumlulukla İlgili Sınırlamalar.....	36
9.9.	Tazminat Halleri	36
9.10.	Anlaşma Süresi ve Anlaşmanın Sona Ermesi	36
9.10.1.	Anlaşma Süresi.....	36
9.10.2.	Anlaşmanın Sona Ermesi	37
9.10.3.	Anlaşmanın Sona Ermesinin Etkileri	37
9.11.	Sistem Bileşenleri ile Haberleşme ve Kişisel Bilgilendirme	37
9.12.	Deđişiklik Halleri	37
9.12.1.	Deđişiklik Metotları	37
9.12.2.	Bilgilendirme Mekanizması ve Sıklığı.....	37
9.12.3.	Nesne Tanımlama Numarasının Deđişmesini Gerektiren Durumlar	37
9.13.	Anlaşmazlık 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 oluřturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti'ne baėlı kamu kurum ve kuruluşlara Kurumsal Őifreleme Sertifikası saėlayıcılıėı konusundaki iőlevleri sırasında uyulması gereken kuralları ve çalıőma 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 Süreçlere 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 gerçekteřtirildiėini, Açık Anahtar Altyapısı'nı (Public Key Infrastructure-PKI) oluřturan 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 tanımlandığı 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.

Kök SHS son kullanıcılar için sertifika üretmeyip, yürüttükleri görevler açısından özel niteliėi haiz kamu kurum ve kuruluşları ile dileyen gerçekte ve tüzel kiőilerin kuracakları Elektronik Sertifika Hizmet Saėlayıcıları'na kök, köprü veya çapraz sertifika hizmeti verir.

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

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 hazırlanmış olup, doküman içeriėinde belirtilen bir kısım alt baőlıkların altındaki "Düzenlenmesine gerek duyulmamıőtır" ibaresi, bu aőamada ihtiyaç duyulmadığından düzenleme yapılmadığıını 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. İletifim 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 kişilik.

Kurumsal Őifreleme SHS (Kurumsal Őifreleme 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 Sağlayıcısı.

Kurumsal Őifreleme Sertifikası Asıl Sorumlusu: Kamu kurumlarının başvuru formu ve taahhütname ile Kamu SM'ye bildirdiđi ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde kurumu temsile asıl yetkili kişi.

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

Kurumsal Őifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla kullanılan açık anahtar içeren elektronik sertifika.

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

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

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

Sertifika Sahibi: Kurumsal Őifreleme Sertifikası başvurusunda bulunan ve sertifikayı kullanma yetkisine sahip tüzel kişi.

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

Sİ ve SUE (Sertifika İlkeleri ve Uygulama Esasları): Kamu SM resmi 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 belgeler.

Üçüncü Kişiler: Sertifikalara güvenerek işlem yapan gerçek veya tüzel kişiler.

Zaman Damgası: Bir elektronik verinin, üretildiđi, deđiştirildiđi, gönderildiđi, alındıđı ve/veya kaydedildiđi zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doğrulanan kayıt.

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

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliđi

Kamu SM: Kamu Sertifikasyon Merkezi

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 yayınladığı 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 bileşenlerinin erişimine açacağı bilgi deposunda sistemin iç işleyişi ile ilgili olanlar hariç olmak üzere aşağıdaki bilgiler bulunur:

- Kamu SM'ye ait güncel Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait Kök SHS sertifikalarının özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi 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 içeriğinin deęiŐmesi 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 doęruluęunu ve güncellięini sağlamakla yükümlüdür.

3. Kimlik Belirleme ve Doęrulama

Kurumsal Őifreleme Sertifikası kurum kimlik tanımlama ve doęrulama yöntemleri ile Kurumsal Őifreleme Sertifikası içinde yazılan kurum bilgileri bu bölümde anlatılmıŐtır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

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

3.1.2. Kimlik Bilgilerinin TeŐhise ElveriŐli Olması

Kurumsal Őifreleme Sertifikaları içeriğindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimlięinin tespit edilmesini saęlayan niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

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

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

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

3.1.5. Kimlik Bilgilerinin Tekillięi

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

3.1.6. Markanın Tanınması, Doęrulanması ve Rolü

Düzenlenmesine gerek duyulmamıŐtır.

3.2. İlk Kimlik Belirleme

Kamu SM Kurumsal Őifreleme Sertifikası hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduęunda, ilgili kurumun doęrulanabilmesi için aŐaęıda 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 Őifreleme Sertifikası Asıl veya Yedek Sorumlusuna teslim edilir. Asıl veya Yedek Sorumlu tarafından Kurumsal Őifreleme Sertifikasının teslim alındığı teyit edilir. Ek olarak, HSM'ye yüklenmesi talep edilen sertifikalar için Kurum HSM Cihaz Sorumlusu tarafından imzalanan teslim tutanağı ile teyit işlemi yapılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Kurumsal Őifreleme Sertifikası başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini, kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazı ile Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhünamesi ile Kamu SM'ye bildirir. Kamu SM, başvuru formunda yer alan bilgilere istinaden kurum kimliğini belirler. Kurumların sertifika alma yetkisi DETSİS sorgusu aracılığıyla kontrol edilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Kurumsal Őifreleme Sertifikası, kurum adına verildiğinden yalnızca kurumsal başvuru kabul edilmektedir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika sorumluları tarafından başvuru sırasında ve daha sonra deęişiklik sebebiyle beyan edilen erişim bilgileri ve SUE dokümanında işaret edilen diđer bilgilerin doğruluęu Kamu SM tarafından kontrol edilmez.

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

SUE Bölüm 3.2'de anlatıldığı şekilde uygulanır.

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 yetkilendirdiğı sertifika sorumluları Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemi gerçekleştirebilir. Online İşlemler adresine ulaşamaması durumunda Kamu SM'ye Elektronik Mühür/Kurumsal Őifreleme Sertifikası İptal Başvuru Formu resmi yazısı ile birlikte gönderilerek iptal işlemi gerçekleştirilebilir. Kurum kimlik doğrulaması ve iptal işleminin teyidi SUE Bölüm 3.4'te anlatıldığı şekilde gerçekleştirilir.

4. İőlemsel Gereker

Bu bđlümde sertifika yđnetim sđreçlerinde yapılan iőlemler anlatılmaktadır. Sđreçlerle 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 TĐBİTAK BİLGEM ile karőılıklı imzalanan sđzleŐmeler ve/veya kurumun imzaladıđı Elektronik Mđhđr/Kurumsal Őifreleme Sertifikası Baővuru Formu ve Taahhđtnamesi, Kamu SM'nin internet üzerinden yayımladıđı ilgili yđnergeler, Sİ ve SUE dokđmanları dođrultusunda belirlenir.

Kurum baővuru sırasında Kamu SM'ye dođru bilgi beyan etmekle sorumludur. Kurum, Kamu SM'ye gđndermiŐ olduđu bilgilerin dođruluđunu takip etmekle ve bu bilgilerde deđiŐiklik olması halinde belirlenmiŐ araç ve yđntemler ile Kamu SM'yi bilgilendirmekle yđkđmlüdür. 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 Bđlüm 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 gđnderilen belgelerin dođrulanması için yapılan iőlemler SUE Bđlüm 4.2.1'de yer almaktadır.

4.2.2. Sertifika Baővurusunun Kabul veya Reddi

Bilgi Teknolojileri ve İletiŐim 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 Mđhđr Sertifikalarına iliŐkin Usul ve Esaslar" yayımlanmıŐtır. İlgili Karar ikinci bđlüm, 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 gđnđ içerisinde sertifika baővurusu iőleme alınır ve sonuçlandırılır.

4.3. Sertifikanın OluŐturulması

4.3.1. Sertifika OluŐturulmasında ESHS'nin İŐlevleri

SUE Bۆlüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika baŐvuruları Kamu SM tarafından iŐlenir. Kurum, iŐlem kapasitesini gۆz ۆnünde bulundurarak baŐvuru sırasında sertifikanın yۆkleneceėi 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 ۆzere 2 adet ۆretilir.

4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta y�klenen sertifika, sertifika sorumlusuna teslim edildiėinde Kurumsal Őifreleme Sertifikasının oluŐturulduėu konusunda bilgilendirilmiŐ olur.

HSM cihazına sertifika y�kleme iŐlemi, Kurum HSM Cihaz Sorumlusu gۆzetiminde gerekleŐtirilir. İŐlem sonrasında teslim tutanaėı imzalanır ve Kurumsal Őifreleme Sertifikasının oluŐturulduėu konusunda bilgilendirilmiŐ olur.

4.4. Sertifikanın Kabul ۆ

4.4.1. Sertifikanın Kabul KoŐulu

Kurumsal Őifreleme Sertifikası akıllı kart veya HSM cihazı ierisinde kullanılabilir. Sertifikanın kullanılacaėı cihaz seimine gۆre SUE Bۆlüm 4.4.1'de belirtilen kabul koŐulu uygulanmaktadır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM tarafından ۆretilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e y�klenmektedir.

4.4.3. Sertifikanın OluŐturulmasının Diėer Tarafalara Duyurulması

Kamu SM tarafından ۆretilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e y�klenmektedir.

4.5. Sertifikanın ve ۆzel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve ۆzel Anahtar Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait ۆzel anahtarını, tabi olunan standartlar, Sİ ve SUE dokümanında ve ilgili sertifika sahibi taahhۆnmesinde yer alan koŐullar ve belirlenmiŐ sınırlar iinde kullanmalıdır.

4.5.2. ۆüncü KiŐilerin Sertifika ve Aık Anahtar Kullanımı

Sertifika sahibine ait Kurumsal Őifreleme Sertifikasının iinde yer alan aık anahtar, ۆüncü kiŐilerce EYP 2.0 kapsamında verilerin Őifreli iletimi amacıyla kullanılır. Aık anahtarın veya sertifikanın, belirtilen ama dıŐında kullanılması sonucu oluŐabilecek zararlardan ۆüncü kiŐiler sorumludur.

4.6. Sertifika S ۆresinin Uzatılması

Sertifika s ۆresinin uzatılması, kullanım s ۆresi dolan sertifikalarda, sertifikada yer alan bilgiler deėiŐmeden aynı anahtar ifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar ۆretilmesini tanımlamaktadır. Kamu SM bu iŐlemi gerekleŐtirmez.

4.7. Sertifika Yenileme

Kamu SM, sertifika yenileme işlemini, yeni anahtar çifti üretmek suretiyle yerine getirir. Sertifika yenileme işlemleri SUE Bölüm 4.7'de anlatıldığı şekilde gerçekleştirilir.

4.7.1. Sertifikanın Yenileme Koşulları

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

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

SUE Bölüm 4.7.2'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

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 Koşulu

SUE Bölüm 4.7.5'te tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

SUE Bölüm 4.7.6'da tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Tarafra Duyurulması

SUE Bölüm 4.7.7'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

Sertifika içeriğinde yer alan bilgilerde değişiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi değişikliğinin gerekli olduğu durumlarda, kurum SUE Bölüm 4.7'de belirtilen sertifika yenileme sürecini işletmelidir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifikanın, kullanım süresi dolmadan geçerliliğini yitirdiği 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 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 İşlenmesi

Kurumsal Şifreleme Sertifikası iptal işlemi, kurum tarafından yetkilendirilen Kurumsal Şifreleme Sertifikası Asıl veya Yedek Sorumlusu tarafından Kamu SM resmi 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 belirtildiği 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 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 sağladığı 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 Őifreleme Sertifikası iptal edilir. Kurumsal Őifreleme Sertifikasının iptal edilmesi dıŐında herhangi bir iŐlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındıđı Durumlar

Kurumsal Őifreleme Sertifikası, üretim veya kullanım aŐamasında geđici iptal durumunu sađlamak amacıyla askıya alınabilir. Sertifikanın askıya alındıđı durumlar SUE Bölüm 4.9.13'te verilmiŐtir.

4.9.14. Sertifika Askıya Alma BaŐvurusunu Kimlerin Yapabildiđi

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

4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi

Kurumsal Őifreleme Sertifikası askı baŐvurusu, Kamu SM web sitesinde yer alan Online İŐlemler menüsünden veya Online İŐlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Askıya alma baŐvurusunun iŐlenmesi ile ilgili detaylar SUE Bölüm 4.9.15'te verilmiŐtir.

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

4.9.16. Askıda Kalma Süresi

İlk üretim sonrasında askıdan indirmeyle ilgili bir süre kısıtı bulunmamakla birlikte kurum tarafından askıya alınan sertifikalar en az 12 (on iki) saat süresince askıdan indirilemez.

4.10. Sertifika Durum Servisleri

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

4.10.1. İŐletimsel 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 erişimin kesintisiz olarak sađlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rađmen erişimin bir süreliđine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken iŐlemlerini durdurur. Üçüncü kişilerin iptal durum kaydını, erişimin kesilmesi sebebiyle kontrol etmeden yaptıkları iŐlemlerden 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 sũresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliđi sona erer. Kullanım sũresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda deđildir; sertifika sahibi sertifikanın kullanım sũresinin dolduđu zamanı kendisi takip etmekle yũkũmlũdũr.

4.12. Anahtar Yeniden Őretim

Sertifika sahiplerine ait anahtarların yeniden ũretilmesi veya yedeklenmesi iŐlemi uygulanmamaktadır.

5. Yönetim, İŐlemsel 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 kiŐilerin 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 yũrũtũlmektedir. Bina, yũksek güvenlik gerektiren iŐlerin yapılmasına imkan sađlayan yapıdadır. Alanlara ve binalara eriŐim, tek kiŐinin giriŐine veya çıkıŐına izin veren HI-SEC kilitleme kapıları dahil olmak ũzere fiziki güvenlik, video izleme ve kimlik dođrulama olmak ũzere çoklu güvenlik ile korunmaktadır. Bina içinde, yazılım ve donanım modũllerinin yerleŐtirilmesi için kilitli ve giriŐ kontrollũ odalar bulunur.

5.1.2. Fiziksel EriŐim

Kamu SM yazılım ve donanım modũlleri ile arŐivlere eriŐim denetim altındadır. Binaya giriŐler güvenlik görevlilerinin kontrolũ altında, geliŐmiŐ eriŐim kontrol cihazlarıyla sađlanmaktadır.

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduđu, elektronik veya kađıt ortamdaki bilgilerin tutulduđu, sistemin iŐletildiđi ve yönetildiđi odalara eriŐim geliŐmiŐ eriŐim kontrol cihazlarıyla yapılmaktadır.

5.1.3. Gũç Kaynađı ve Havalandırma

Kamu SM iŐlevlerinin yerine getirilmesi ve sũrekliliđin sađlanması için sistem, kesintisiz gũç kaynađı ile beslenir. Bina gerekli havalandırma sistemi ile donatılır.

5.1.4. Su Baskınları

Kamu SM iŐlevlerinin yerine getirildiđi ortamlarda su baskınlarından en az zarar gũrecek Őekilde önlemler alınmıŐtır.

5.1.5. Yangın Önleme ve Korunma

Kamu SM iŐlevlerinin 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, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve artık kullanılmayan elektronik veya kağıt 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 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 Kişi Sayısı

Kamu SM, Kök SHS ve Kurumsal Şifreleme SHS'ye ait sertifika üretilmesi, iptal edilmesi, imza oluşturma verilerinin başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar. Kurumsal Şifreleme Sertifikalarının üretimi iki kişinin kontrolünde gerçekleştirilir.

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. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

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

5.3.2. Geçmiş Araştırması

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

5.3.3. Eđitim Gerekleri

ÇalıŐanlar, Kamu SM'deki iŐlerine aktif olarak baŐlamadan önce gerekli eđitimden geçirilirler. ÇalıŐanlara verilen eđitimde Kamu SM'de uygulanan g¼venlik ilkeleri, sistemin teknik ve idari iŐleyiŐi, iŐleriyle ilgili s¼reçler, s¼reç içindeki g¼rev ve sorumluluklar anlatılır.

Kamu SM, çalıŐanlarına en az yılda bir defa, siber g¼venlik ve sosyal m¼hendislik saldırılarına karŐı farkındalık oluŐturmak amacıyla, bilgi g¼venliđi eđitimi vermektedir.

5.3.4. S¼rekli Eđitim Gerekleri ve Sıklıđı

Kamu SM sisteminde yapılan deđiŐikliklerin bildirilmesi amacıyla personele verilen eđitimler gerekli g¼r¼ld¼kçe tekrarlanır. Yeni g¼reve baŐlayanlar için eđitimler tekrarlanır.

5.3.5. G¼rev DeđiŐim Sıklıđı ve Sırası

D¼zenlenmesine gerek duyulmamıŐtır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin, tamamen veya kısmen sahte elektronik sertifika oluŐturması, geçerli olarak oluŐturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluŐturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diđer yetkisiz eylemlerde ilgili mevzuat geređince bilgi g¼venliđi politikaları ihlali ve ihlalin boyutuna g¼re hukuki soruŐturma ve disiplin s¼reci baŐlatılır.

5.3.7. AnlaŐmalı Personel Gereksinimleri

Kamu SM verdiđi hizmetler için dıŐ kaynak kullanmak durumunda kaldıđında, bu hizmeti sađlayacak firma personeli ile ilgili g¼venlik kontrollerini, firma ile yaptıđı s¼zleŐme ile belirler.

5.3.8. Sađlanan Dok¼mantasyon

ÇalıŐanlara iŐleriyle ve Kamu SM s¼reçleriyle ilgili gerekli kılavuz ve destek dok¼manlar ve bilgi g¼venliđi politikaları kapsamındaki ilgili dok¼manlar sađlanır.

5.4. Denetim Kayıtları

Kamu SM iŐleyiŐi sırasında gerçekteŐtirilen anahtar ve sertifika y¼netimi, sistemin g¼venliđi ile ilgili iŐlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diđer bir kısmı ise kađıt ¼zerindedir. Denetimler sırasında gerekli g¼r¼ld¼đ¼ takdirde bu kayıtlar g¼revliler tarafından incelenir.

5.4.1. Kaydedilen İŐlemler

Kamu SM sisteminde, SUE B¼l¼m 5.4.1'de belirtilen elektronik veya kađıt ortamda yapılan iŐlerin kayıtları tutulur.

5.4.2. Kayıtların İncelenme Sıklıđı

Sistemin iŐleyiŐiyle ilgili tutulan kayıtlar d¼zg¼n zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir g¼venlik açıđı oluŐup oluŐmadıđı 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 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.

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 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 Değişimi

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

5.7. Güvenliğin Yitilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitilmesi Durumunun Düzeltilmesi

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

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 Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin Kurumsal Şifreleme Sertifikalarını imzalamada kullandığı imza oluşturma verisinin gizliliğinin kaybedildiğinden 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 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 İlişkin 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 gerçekleştirdiği 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 Yayınlayıcı Anahtar Çifti Üretimi

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcıya 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 sađlayan 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 gerçekleştiren personel tarafından onaylanır.

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

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

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

6.1.2. Sertifika Sahibine Özel Anahtarın Ulařtırılması

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

6.1.3. Elektronik Sertifika Hizmet Sađlayıcısına Açık Anahtarın Ulařtırılması

Kurumsal Őifreleme Sertifikası HSM'ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteđi, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılıđıyla Kamu SM'ye ulařtırılır.

Kurumsal Őifreleme Sertifikası akıllı karta yüklenecekse, Kurumsal Őifreleme Sertifikaları anahtar çiftleri Kamu SM tarafından üretildiđi için açık anahtarın Kamu SM'ye ulařtırılması söz konusu deđildir.

6.1.4. Elektronik Sertifika Hizmet Sađlayıcısı Sertifikalarına Eriřim Sađlanması

Kamu SM'ye ait Kök SHS ve Kurumsal Őifreleme SHS sertifikaları internet ortamında tarafların eriřimine hazır bulundurulur. Sertifikanın yayımlandıđı ortamın izinsiz deđiřtirmeye ve silinmeye karřı güvenliđi sađlanır.

6.1.5. Anahtar Uzunlukları

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

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

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

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

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde kullanılan algoritmaların güvenliđi 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 kullanılabilceđi sertifikadaki "Anahtar Kullanımı" ve "Geniřletilmiş Anahtar Kullanımı" uzantısı içerisinde belirtilir.

Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Kurumsal Őifreleme Sertifikalarının imzalanmasında kullanılan sertifika zinciri 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 oluřturma verisi güvenli yazılım ve/veya donanım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduđu süre boyunca bu modül dıřına çıkmaz. Kriptografik modülün sahip olduđu güvenlik iřlevleri SUE Bölüm 6.2.1'de açıklanmaktadır.

6.2.2. Özel Anahtara Birden Fazla Kiři Kontrolünde Eriřim

Kamu SM'ye ait imza oluřturma verisinin bulunduđu odaya eriřim aynı anda 2 (iki) çalıřan tarafından sağlanmaktadır.

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıřtır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait imza oluřturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iřlemi hazırda kullanılmakta olan imza oluřturma verisi için sağlanan güvenlik ile eřdeđer güvenlik önlemleri altında yapılır. Sertifika sahiplerine ait özel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın Arřivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait özel anahtarlar arřivlenmez. Kullanım süreleri sonunda geri dönüşüz řekilde 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 içinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına çıkması engellenmiŐtir. İmza oluŐturma verisi kriptografik modül içinde güvenli algoritma ve yöntemlerle Őifreli olarak saklanır.

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

6.2.8. Özel Anahtara EriŐim

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

İmza oluŐturma verisi kriptografik modül içinde Őifreli durumdayken eriŐime kapalıdır. EriŐime açılması için eriŐimi saĐlayan verinin modüle sunulması gerekir.

Sertifika sahibine ait özel anahtar, akıllı kart veya HSM cihazı içinde 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 için kullanıldıktan sonra oturum kapandıĐında veriye eriŐim otomatik olarak kesilir ve bir dahaki kullanımına kadar Őifrelenerek eriŐime kapalı tutulur. EriŐimin yeniden saĐlanabilmesi için SUE Bölüm 6.2.8'de belirtilen yöntemin yeniden iŐletilmesi gerekir. Sertifika sahibinin kullandıĐı güvenli donanım araçları, özel anahtarı kullanan oturumun kapanmasından sonra veriye eriŐimi kesecek biçimde çalıŐır. EriŐimin yeniden saĐlanabilmesi için sertifika sahibinin eriŐim verisini yeniden girmesi gerekir. EriŐim verisinin art arda 3 (üç) defa yanlış girilmesi durumunda güvenli donanım aracı kilitletir ve araca eriŐim saĐlanamaz.

6.2.10. Özel Anahtarın Yok Edilmesi

Kamu SM'ye ait imza oluŐturma verileri kullanım süresinin dolmasının ardından, aslı ve bütün yedekleri buldukları ortamlardan uygun yöntemlerle geri dönüşsüz Őekilde silinir. Kamu SM'ye ait imza oluŐturma verisinin silinmesi iŐlemi için SUE Bölüm 6.2.8'de belirtilen Őekilde 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 iŐlemin yapılmasından sertifika sahibi sorumludur.

6.2.11. Kriptografik Modülün Deęerlendirilmesi

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 önlemlerin alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Kurumsal Şifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. 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 yükümlülüęü 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 Güvenlięi Denetimleri

6.5.1. Bilgisayar Güvenlięi ile İlgili Teknik Gereker

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

6.5.2. Bilgisayar Sisteminin Saęladıęı Gvenlik Seviyesi

Dzenlenmesine gerek duyulmamıŐtır.

6.6. YaŐam Dngs Teknik Kontrolleri

6.6.1. Sistem GeliŐtirme Kontrolleri

Sistem geliŐtirilirken genel anlamda yapılan denetimler SUE Blm 6.6.1’de aıklanmaktadır.

6.6.2. Gvenlik Ynetimi Kontrolleri

Sistem iindeki yazılım ve donanım rnleri ile aę ortamının belirlenen gvenlik Őartlarını saęlayıp saęlamadıęı, test cihazları ve test prosedrleri kullanılarak kontrol edilir. Gvenlik kontrolleri iin temel dayanak ISO 27001’in gncel srmdr.

6.6.3. YaŐam Dngs Gvenlik Denetimleri

Dzenlenmesine gerek duyulmamıŐtır.

6.7. Aę Gvenlięi Denetimleri

Kamu SM sisteminde son teknolojik geliŐmeler gz nnde bulundurularak gerekli aę gvenlięi denetimleri yapılır. Aę gvenlięi denetimlerine iliŐkin detaylar SUE Blm 6.7’de aıklanmaktadır.

6.8. Zaman Damgası

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

7. Sertifika ve Sertifika İptal Listesi Biimleri

7.1. Sertifika Biimi

Bu blmde Kamu SM tarafından daęıtılan Kurumsal Őifreleme Sertifikalarının ierięi ile ilgili bilgilendirme yapılmaktadır.

7.1.1. Srm Numarası

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

7.1.2. Sertifika Uzantıları

Kamu SM tarafından daęıtılan Kurumsal Őifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geerlilik tarihi, ilgili aık anahtar, sertifika sahibi kurumun adı ve DETSİS numarası, sertifikayı yayımlayan Kamu SM’ye ait isim bilgileri ve Kamu SM’nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını ierir. Kurumsal Őifreleme Sertifikasının ierięinde bulunan sertifika uzantıları sertifikanın kullanılacaęı uygulamanın gereklerine baęlı olarak belirlenir.

Kamu SM tarafından retilen Kurumsal Őifreleme Sertifikalarında asgari dzeyde bulunması gereken uzantılar SUE Blm 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 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

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

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Kurumsal Őifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Őifreleme Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikasının "Sertifika İlkeleri 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 ettiđinde Sİ ve SUE'de belirtilen ilke ve uygulama esasları çerçevesinde Kurumsal Őifreleme Sertifikalarını kullanarak işlem yapar.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

¹ Certificate Policies

² Policy Identifier

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 SUE Bölüm 7.3.2'de belirtilen bilgileri içerir.

8. Uygunluk Denetimleri

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

8.1. Uygunluk Denetiminin Sıklığı

Kamu SM, ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardı gereğince 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 edilmiş kuruluşlarca gerçekleştirilir.

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

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Dış denetçiler, herhangi bir çıkar çatışması olmaması ve bağımsızlığın zedelenmemesi için Kamu SM'den bağımsız 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 gerçekleştirecek Kamu SM personeli tarafından belirlenir.

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

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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, ISO/IEC 27001 denetçilerinin hazırladığı resmi raporlar ile Kamu SM'ye bildirilir.

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

9. Diđer İŐler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika OluŐturma ve Yenileme Ücreti

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

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

9.1.2. Sertifika EriŐim Ücreti

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

9.1.3. İptal Durum Kaydına EriŐim Ücreti

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

9.1.4. Diđer Servis Ücretleri

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

Kamu SM, 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. Diđer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, ürettiği Kurumsal Őifreleme 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 verdiđi taraflarca paylaŐılan iŐ planları, satıŐ bilgileri, ticari sırlar ve yapılan gizli anlaŐmalarda verilen bilgiler ticari bilgi olarak deđerlendirilir. Ayrıca gizli olmadıđı özel olarak bildirilmeyen tım 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 iđerisinde yer alan bilgiler gizli olarak deđerlendirilmez.

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. KiŐisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

Kamu SM verdiđi hizmetlerde sertifika sahiplerinin ve diđer paydaŐların kiŐisel verilerinin gizliliđini 2017/21 Sayılı BaŐbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurulu Kamu Kurum ve KuruluŐları Arasında Elektronik Ortamdaki Belge PaylaŐımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliŐkin Usul ve Esaslar'da ve 6698 sayılı kanunlar kapsamındaki mer'i mevzuata uygun olarak sađlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

KiŐisel bilgi, sertifika sahibi kurumun ve yetkilendirdiđi Kurumsal Őifreleme Sertifikası Asıl ve Yedek Sorumlusu ile Kurum HSM Cihaz Sorumlusunun, baŐvuru sırasında kimlik tanımlama ve dođrulama ile sertifika yönetim prosedürleri iđerinde 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 Őifreleme Sertifikası iđerisinde bulunan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediđi sürece gizli deđerdir.

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 iđerinde istenen bilgilere erişimin ve yetkisiz kullanımın engellenmesi ve mahremiyetinin korunması için, Kamu SM tarafından gerekli güvenlik tedbirleri alınır. Sadece yetkilendirilmiş çalıŐanlar sertifika sahibi kurumun bilgilerine erişirler.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yükümlülükler

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

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediğı halde imzalanmış olan Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi 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 9.6.1'de belirtilen ESHS yükümlülükleri ile aynıdır.

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 ve SUE dokümanlarında belirtilen şartları okuduğunu, başvuru süreci ve sertifika geçerliliğı boyunca Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhütnamesi, ilgili mevzuatlar ile Sİ ve 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. Diđer Bileőenlerin Yüklümlükleri

9.6.5.1. Kurumun Yüklümlükleri

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

9.6.5.2. Kurum Sertifika Sorumlularının Yüklümlükleri

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

9.7. Yüklümlüklerden Feragat

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

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 2017/21 Sayılı Başbakanlık 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 İlişkin Usul ve Esaslar'da belirtilen şartlar ile sınırlıdır.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

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

9.10.1. Anlaşma Süresi

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

9.10.2. Anlaşmanın Sona Ermesi

Kamu SM ile kurum arasında varsa imzalanan sözleşme SUE Bölüm 9.10.2'de belirtilen durumlarda sonlandırılabilir.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleşmenin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yüklümlükleri ortadan kalkar. Kamu SM kurumdan

sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmıő başvurular ile ilgili iőlemler, anlaşmanın 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 sonuları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılıėıyla saėlanır. Sertifika ynetimiyle ilgili kritik grlen iőlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

9.12. Deėiőiklik Halleri

9.12.1. Deėiőiklik Metotları

Sİ dokmanı Kamu SM tarafından yazılmıőtır. Bu Sİ dokmanında yapılabilecek deėiőiklikler ekleme ve deėiőtirme Őeklinde olabileceėi gibi Kamu SM dokmanının tamamen yenilenmesine de karar verebilir. Bu Sİ dokmanının herhangi bir kısmının yanlıő ya da geersiz olduėu ortaya ıksa bile Sİ dokmanının diėer kısımları, Sİ dokmanı gncellenene kadar geerliliėini srdrr.

9.12.2. Bilgilendirme Mekanizması ve Sıklıėı

Sİ dokmanında yapılan deėiőtiklikler dokmanın yenilenerek Kamu SM bilgi deposu zerinden eriőtme aılması ile duyurulur. Yenilenen dokman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandıėı tarihte yrrlėe girer.

9.12.3. Nesne Tanımlama Numarasının Deėiőtmesini Gerektiren Durumlar

Dzenlenmesine gerek duyulmamıőtır.

9.13. Anlaőtmazlık Halleri

Taraflar arasında ıkan tm anlaşmazlıkların sulhen zm esastır. İhtilafların zmnde 2017/21 Sayılı Baőbakanlık Genelgesi, Bilgi Teknolojileri ve İletiőt Kurulu Kararıyla yayımlanan Kamu Kurum ve Kuruluőları Arasında Elektronik Ortamdaki Belge Paylaőtımında Kullanılan Kurumsal Őifreleme ve Elektronik Mhr Sertifikalarına İliőtkin Usul ve Esaslara baőturulur. İhtilafların sulhen zmnn mmkn olmaması halinde, ihtilafların zmnde grevli ve yetkili mahkeme Trkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

Sİ dokmanındaki hkmler, 2017/21 Sayılı Baőbakanlık Genelgesi, Bilgi Teknolojileri ve İletiőt Kurulu kararıyla yayımlanan Kamu Kurum ve Kuruluőları Arasında Elektronik Ortamdaki Belge Paylaőtımında Kullanılan Kurumsal Őifreleme ve Elektronik Mhr Sertifikalarına İliőtkin Usul ve Esaslara uygun olarak yazılmıőtır.

9.15. Uygulanabilir Yasalarla Uyum

Sİ dokmanında geen hkmlerin daha sonra yrrlėe girecek ilgili mevzuata aykırı bulunması halinde dokmanda gerekli deėiőtiklikler yapılarak uygun hale getirilir.

9.16. Diėer Hkmler

Dzenlenmesine gerek duyulmamıőtır.