

**KAMU SM
SERTİFİKA İLKELERİ
VE
SERTİFİKA UYGULAMA ESASLARI
(SSL VE S/MIME SERTİFİKASI İÇİNDİR)**

Doküman Kodu	Yayın Numarası	Yayın Tarihi
YONG-001-009	02	24.02.2009

**KAMU SM Sİ/SUE
(SSL VE S/MIME SERTİFİKASI İÇİNDİR)*****DEĞİŞİKLİK KAYITLARI***

Yayın No	Yayın Nedeni	Yayın Tarihi
01	İlk yayın	05.12.2007
02	RSA 1024-bit sertifikalar ile ilgili düzenleme yapıldı. Minimum anahtar uzunluğu RSA 2048-bit olarak düzenlendi.	24.02.2009

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

İÇİNDEKİLER

1. Giriş	10
1.1. Genel Bakış.....	10
1.2. Doküman Adı ve Tanımı.....	10
1.3. Sistem Bileşenleri.....	11
1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı	11
1.3.2. Kayıt Birimleri	11
1.3.3. Sertifika Sahipleri.....	11
1.3.4. Üçüncü Kişiler.....	11
1.3.5. Diğer Bileşenler	11
1.4. Sertifika Kullanımı	11
1.4.1. Uygun Olan Sertifika Kullanımı.....	11
1.4.2. Sertifika Kullanımının Sınırları	11
1.5. İlke ve Uygulama Esaslarının Yönetimi.....	11
1.5.1. Doküman Yönetimi	11
1.5.2. İletişim Bilgileri.....	11
1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi ..	12
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri.....	12
1.6. Tanımlar ve Kısaltmalar	12
1.6.1. Tanımlar	12
1.6.2. Kısaltmalar.....	13
2. Yayımlama ve Bilgi Deposu	15
2.1. Bilgi Depoları	15
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması	15
2.3. Yayın Sıklığı ve Zamanı	15
2.4. Erişim Kontrolleri	15
3. Kimlik Belirleme ve Doğrulama	17
3.1. İsimlendirme	17
3.1.1. İsim Alanı Tipleri	17
3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması	17
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması	17
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması	17
3.1.5. Kimlik Bilgilerinin Tekilliği.....	17
3.1.6. Markanın Tanınması, Doğrulaması ve Rolü	17
3.2. İlk Kimlik Belirleme	17
3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması.....	17
3.2.2. Kurumsal Kimliğin Belirlenmesi	18
3.2.3. Kişisel Kimliğin Belirlenmesi	18
3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri.....	18
3.2.5. Yetkinin Doğrulaması	18

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

3.2.6.	Uyum Kriterleri.....	18
3.3.	Sertifika Yenileme İsteğinde Kimlik Doğrulama.....	18
3.3.1.	Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama	18
3.3.2.	İptal Sonrası Sertifika Güncelleme İsteğinde Kimlik Doğrulama.....	18
3.4.	Sertifika İptal İsteğinde Kimlik Doğrulama.....	19
4.	İşlemsel Gerekler.....	20
4.1.	Sertifika Başvurusu	20
4.1.1.	Sertifika Başvurusunu Kimlerin Yapabildiği	20
4.1.2.	Kayıt İşlemleri ve Sorumluluklar	20
4.2.	Sertifika Başvurusunun İşlenmesi	21
4.2.1.	Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi	21
4.2.2.	Sertifika Başvurusunun Kabul veya Reddi	21
4.2.3.	Sertifika Başvurusunun İşlenme Zamanı.....	21
4.3.	Sertifikanın Oluşturulması	21
4.3.1.	Sertifika Oluşturulmasında ESHS'nin İşlevleri	21
4.3.2.	Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi	21
4.4.	Sertifikanın Kabul Edilmesi.....	22
4.4.1.	Sertifikanın Kullanıma Açılma Biçimi	22
4.4.2.	Sertifikanın ESHS Tarafından Yayımlanması.....	22
4.4.3.	Sertifikanın Oluşturulmasının Diğer Bileşenlere Duyurulması	22
4.5.	Sertifikanın ve İmza Oluşturma Verisinin Kullanımı	22
4.5.1.	Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı	22
4.5.2.	Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı	22
4.6.	Sertifikanın Yeniden Üretilmesi	23
4.7.	Sertifikanın Yenilenmesi.....	23
4.8.	Sertifikanın Güncellenmesi.....	23
4.9.	Sertifikanın İptali ve Askıya Alınması	23
4.9.1.	Sertifikanın İptal Edildiği Durumlar	23
4.9.2.	Sertifika İptal Başvurusunu Kimlerin Yapabildiği	24
4.9.3.	Sertifika İptal Başvurusunun İşlenmesi.....	24
4.9.4.	İptal İsteği Ertelenme Süresi.....	24
4.9.5.	İptal İsteğinin İşlenme Süresi.....	25
4.9.6.	Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği	25
4.9.7.	Sertifika İptal Listesi Yayımlama Sıklığı.....	25
4.9.8.	Sertifika İptal Listesi Yayımlama Gecikme Süresi	25
4.9.9.	Çevrim İçi Sertifika İptal Durum Kaydı Desteği.....	25
4.9.10.	Çevrim İçi Sertifika İptal Durum Kaydı Gereksinimi	25
4.9.11.	Diğer Sertifika Durum Bildirim Yöntemleri	26
4.9.12.	İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu	26
4.9.13.	Sertifikanın Askıya Alındığı Durumlar	26
4.9.14.	Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği	26
4.9.15.	Sertifika Askıya Alma Başvurusunun İşlenmesi.....	26

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.9.16.	Askıda Kalma Süresi	26
4.10.	Sertifika Durum Servisleri.....	26
4.10.1.	İşletimsel Özellikleri	26
4.10.2.	Servisin Erişilebilirliği	27
4.10.3.	İsteğe Bağlı Özellikler	27
4.11.	Sertifika Sahipliğinin Sona Ermesi	27
4.12.	Anahtar Yeniden Üretme	27
5.	Yönetim, İşlemsel ve Fiziksel Kontroller	28
5.1.	Fiziksel Güvenlik Denetimleri	28
5.1.1.	Tesis Yeri ve İnşaatı	28
5.1.2.	Fiziksel Erişim.....	28
5.1.3.	Güç Kaynağı ve Havalandırma.....	28
5.1.4.	Su Baskınları	29
5.1.5.	Yangın Önleme ve Korunma	29
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması.....	29
5.1.7.	Atıkların Yok Edilmesi.....	29
5.1.8.	Farklı Mekanlarda Yedekleme	29
5.2.	Prosedürel Kontroller	29
5.2.1.	Güvenilir Roller	29
5.2.2.	Her İşlem İçin Gereken Kişi Sayısı	30
5.2.3.	Kimlik Doğrulama ve Yetkilendirme	30
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	30
5.3.	Personel Güvenlik Kontrolleri	31
5.3.1.	Kişisel Geçmiş, Deneyim ve Nitelik Gereklere.....	31
5.3.2.	Geçmiş Araştırması	31
5.3.3.	Eğitim Gereklere	31
5.3.4.	Sürekli Eğitim Gereklere ve Sıklığı	31
5.3.5.	Görev Değişim Sıklığı ve Sırası.....	31
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	31
5.3.7.	Anlaşılabilir Personel Gereksinimleri.....	31
5.3.8.	Sağlanan Dokümantasyon	31
5.4.	Denetim Kayıtları.....	31
5.4.1.	Kaydedilen İşlemler	32
5.4.2.	Kayıtların İncelenme Sıklığı	32
5.4.3.	Kayıtların Saklanma Süresi	33
5.4.4.	Kayıtların Korunması	33
5.4.5.	Kayıtların Yedeklenmesi.....	33
5.4.6.	Kayıtların Toplanması.....	33
5.4.7.	Kayda Sebep Verilen Tarafın Bilgilendirilmesi.....	33
5.4.8.	Saldırıya Açıklığın Değerlendirilmesi	33
5.5.	Kayıt Arşivleme	34
5.5.1.	Arşivlenen Kayıt Bilgileri	34

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.5.2.	Arşivlerin Tutulma Süresi.....	34
5.5.3.	Arşivlerin Korunması	34
5.5.4.	Arşivlerin Yedeklenmesi	34
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri	34
5.5.6.	Arşivlerin Toplanması	34
5.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu.....	34
5.6.	Anahtar Değişimi	35
5.7.	Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	35
5.7.1.	Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi.....	35
5.7.2.	Donanım, Yazılım veya Veri Bozulması	35
5.7.3.	İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi.....	35
5.7.4.	Arıza Sonrası Yeniden Çalışırılık.....	36
5.8.	Sertifika Hizmetlerinin Sonlandırılması.....	36
6.	Teknik Güvenlik Kontrolleri.....	37
6.1.	Anahtar Çifti Üretimi ve Kurulumu	37
6.1.1.	Anahtar Çifti Üretimi	37
6.1.2.	Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması.....	37
6.1.3.	Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması.....	38
6.1.4.	Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması 38	
6.1.5.	Anahtar Uzunlukları	38
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü	38
6.1.7.	Anahtar Kullanım Amaçları	39
6.2.	İmza Oluşturma Verisinin Korunması	39
6.2.1.	Kriptografik Modül Standartları	39
6.2.2.	İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim	39
6.2.3.	İmza Oluşturma Verisinin Yeniden Elde Edilmesi.....	39
6.2.4.	İmza Oluşturma Verisinin Yedeklenmesi	39
6.2.5.	İmza Oluşturma Verisinin Arşivlenmesi	40
6.2.6.	İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi.....	40
6.2.7.	İmza Oluşturma Verisinin Kriptografik Modülde Saklanması.....	40
6.2.8.	İmza Oluşturma Verisine Erişim	40
6.2.9.	İmza Oluşturma Verisine Erişimin Kesilmesi	40
6.2.10.	İmza Oluşturma Verisinin Yok Edilmesi.....	41
6.2.11.	Kriptografik Modülün Değerlendirilmesi	41
6.3.	Anahtar Çifti Yönetimiyle İlgili Diğer Konular	41
6.3.1.	İmza Doğrulama Verisinin Arşivlenmesi	41
6.3.2.	İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri.....	41
6.4.	Erişim Denetim Verileri.....	41
6.4.1.	Erişim Denetim Verilerinin Oluşturulması	42
6.4.2.	Erişim Denetim Verilerinin Korunması	42

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

6.4.3.	Erişim Denetim Verileri İle İlgili Diğer Konular	42
6.5.	Bilgisayar Güvenliği Denetimleri.....	42
6.5.1.	Bilgisayar Güvenliği İle İlgili Teknik Gereklere	42
6.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi	42
6.6.	Yaşam Döngüsü Teknik Denetimleri	42
6.6.1.	Sistem Geliştirme Denetimleri	42
6.6.2.	Güvenlik Yönetimi Denetimleri	43
6.6.3.	Yaşam Döngüsü Güvenlik Denetimleri	43
6.7.	Ağ Güvenliği Denetimleri	43
6.8.	Zaman Damgası.....	43
7.	Sertifika ve Sertifika İptal Listesi Biçimleri	44
7.1.	Sertifika Biçimi.....	44
7.1.1.	Sürüm Numarası	44
7.1.2.	Sertifika Uzantıları	44
7.1.3.	Algoritma ve Nesne Tanımlayıcılar.....	44
7.1.4.	İsim Alanı Biçimleri	44
7.1.5.	İsim Kısıtları	44
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası	44
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	44
7.1.8.	İlke Niteleyiciler.....	44
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi	45
7.2.	Sertifika İptal Listesi Biçimi.....	45
7.2.1.	Sürüm Numarası	45
7.2.2.	Sertifika İptal Listesi Uzantıları	45
7.3.	Çevrim İçi Sertifika Durum Protokolü Biçimi.....	45
7.3.1.	Sürüm Numarası	45
7.3.2.	ÇİSDUP Uzantıları.....	45
8.	Uygunluk Denetimleri.....	47
8.1.	Uygunluk Denetiminin Sıklığı	47
8.2.	Denetçinin Nitelikleri.....	47
8.3.	Denetçinin Denetlenen Tarafı Olan İlişkisi.....	47
8.4.	Denetimin Kapsamı	47
8.5.	Yetersizliğin Tespiti Durumunda Yapılacaklar	47
8.6.	Sonucun Bildirilmesi	48
9.	Diğer İşler ve Hukuksal Meseleler.....	48
9.1.	Ücretlendirme	48
9.1.1.	Sertifika Oluşturma ve Yenileme Ücreti	48
9.1.2.	Sertifika Erişim Ücreti	48
9.1.3.	İptal Durum Kaydına Erişim Ücreti	48
9.1.4.	Diğer Servis Ücretleri.....	48

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

9.1.5. İade Ücreti	48
9.2. Finansal Sorumluluk.....	48
9.2.1. Sigorta Kapsamı	48
9.2.2. Diğer Varlıklar.....	48
9.2.3. Sertifika Mali Sorumluluk Sigortası.....	48
9.3. Ticari Bilginin Korunması.....	48
9.3.1. Gizli Bilginin Kapsamı	48
9.3.2. Gizlilik Kapsamında Olmayan Bilgiler.....	48
9.3.3. Gizli Bilginin Korunma Sorumluluğu	48
9.4. Kişisel Bilginin Gizliliği	48
9.4.1. Gizlilik Planı	48
9.4.2. Özel Olarak Tanımlanan Bilgiler.....	48
9.4.3. Özel Olarak Tanımlanmayan Bilgiler	48
9.4.4. Gizli Bilginin Korunma Sorumluluğu	48
9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi.....	48
9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması.....	48
9.4.7. Diğer Başlıklar	48
9.5. Telif Hakları	48
9.6. Temsil Hakkı ve Yükümlülükler	48
9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri.....	48
9.6.2. Kayıt Birimi Yükümlülükleri	48
9.6.3. Sertifika Sahibinin Yükümlülükleri	48
9.6.4. Üçüncü Kişilerin Yükümlülükleri	48
9.6.5. Diğer Bileşenlerin Yükümlülükleri	48
9.7. Yükümlülüklerden Feragat	48
9.8. Sorumlulukla İlgili Sınırlamalar	48
9.9. Tazminat Halleri	48
9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi.....	48
9.10.1. Anlaşma Süresi	48
9.10.2. Anlaşmanın Sona Ermesi	48
9.10.3. Anlaşmanın Sona Ermesinin Etkileri	48
9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme.....	48
9.12. Değişiklik Halleri	48
9.12.1. Değişiklik Metodları	48
9.12.2. Bilgilendirme Mekanizması ve Sıklığı	48
9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar..	48
9.13. Anlaşmazlık Halleri.....	48
9.14. Uygulanacak Hukuk	48
9.15. Uygulanabilir Yasalarla Uyum	48
9.16. Diğer Hükümler	48
EK-A Sertifika Biçimleri.....	48

**KAMU SM Sİ/SUE
(SSL VE S/MIME SERTİFİKASI İÇİNDİR)**

a)	TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı – Sürüm 3	48
b)	Kamu Elektronik Sertifika Hizmet Sağlayıcısı – Sürüm 3.....	48
c)	Cihaz Sertifikası Hizmet Sağlayıcısı – Sürüm 3.....	48
d)	SSL Sertifikası.....	48
e)	S/MIME Sertifikası.....	48

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) Müdürlüğü tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) SSL ve S/MIME sertifikası hizmeti verirken uyguladığı esasları tanımlayan Sertifika İlkeleri ve Sertifika Uygulama Esasları (Sİ/SUE) dokümanıdır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de tanımlandığı şekliyle Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) işlevlerini yerine getirir.

Kamu SM'den SSL ve S/MIME sertifikası talebinde bulunanlar bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Bu kapsamda oluşturulan sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmezler.

1.1. Genel Bakış

Sİ/SUE dokümanı, Kamu SM içinde yer alan sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini tanımlar; sertifika yönetim ve kayıt işlemlerinin gerçekleştirilme şeklini anlatır. Sertifika yönetimi, sertifika sahipleri için anahtar çifti ve sertifika üretmek, sertifikaları yayımlamak, yenilemek, güncellemek, iptal etmek, sertifika iptal bilgisini yayımlamak, sertifika işlemleri ile ilgili kişileri başvuru ve sertifikanın durumu hakkında bilgilendirmek, gerekli kayıtları tutmak ve kayıt işlemlerini gerçekleştirmek gibi işlerden oluşur. Kayıt işlemleri sertifika verilecek kişi yada kurumların başvurularını, kimlik bilgileri ve ilgili resmi belgeleri toplama, doğrulama, onaylama, iptal, yenileme ve güncelleme isteklerini alma, değerlendirme, onaylanan sertifika başvuru ve iptal istekleri doğrultusunda gerekli işlemleri başlatmayı içerir.

Sİ/SUE dokümanı, "İnternet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki "düzenlenmesine gerek duyulmamıştır" ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı:

Kamu SM

Sertifika İlkeleri ve Sertifika Uygulama Esasları
(SSL ve S/MIME Sertifikası içindir)

Doküman Sürüm Numarası: 02

Yayın Tarihi: 24.02.2009

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.2

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Kamu SM, Elektronik Sertifika Hizmet Sağlayıcısı olarak SSL ve S/MIME sertifikası hizmeti vermektedir. Bu amaçla aşağıdaki hizmetleri yerine getirir.

- Sertifikaların üretilmesi, imzalanması ve ilgili kişi yada kurumlara ulaştırılması
- Sertifikaların iptal edilmesi
- Sertifika durum bilgilerinin Sertifika İptal Listesi (SİL) şeklinde veya diğer yöntemlerle yayınlanması

1.3.2. Kayıt Birimleri

Düzenlenmesine gerek duyulmamıştır.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından kendileri için sertifika oluşturulan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek yada tüzel kişilerdir.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kimlik bilgileri ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir. Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

Düzenlenmesine gerek duyulmamıştır.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

SSL sertifikaları sunucu ve istemci sistemler arasında kimlik doğrulama faaliyetinin gerçekleştirilmesi ve iletişimin şifreli olarak sağlanması amacıyla kullanılırlar.

S/MIME sertifikaları e-posta mesajlarının imzalanması ve şifrelenmesi amacıyla kullanılırlar.

1.4.2. Sertifika Kullanımının Sınırları

Kamu SM tarafından oluşturulan SSL ve S/MIME sertifikaları Madde 1.4.1 de belirtilen amaçlar dışında kullanılamaz.

1.5. İlke ve Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

Bu Sİ/SUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda dokümanda değişiklik yapabilir.

1.5.2. İletişim Bilgileri

Bu Sİ/SUE dokümanının uygulanması ve ilgili yönetim ilkeleri hakkındaki sorular TÜBİTAK UEKAE'nin aşağıdaki erişim noktalarına yönlendirilebilir:

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Adres : TÜBİTAK UEKAE, PK. 74, 41470 Gebze-KOCAELİ

Tel : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

URL : <http://www.kamusm.gov.tr>

Kamu SM, Sİ/SUE dokümanını herkesin erişimine açık bulunan aşağıdaki internet adresinden yayımlar:

<http://www.kamusm.gov.tr/BilgiDeposu/>

1.5.3. Sertifika Uygulama Esaslarının İlgelere Uygunluğunu Belirleyen Kişi

Bu Sİ/SUE dokümanının uygunluğu Kamu SM yönetimi ve yönetim tarafından yetki verilen kişiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

Anahtar çifti: Elektronik imza oluşturmak amacıyla kullanılan özel anahtar ve ilgili açık anahtar. İmza oluşturma ve doğrulama verileri.

Bilgi deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve diğer sertifika işlemleri ile ilgili bilgilerin yayımlandığı dizin sunucular gibi veri saklama ortamları.

Cihaz Sertifikası Hizmet Sağlayıcısı: Kamu Sertifikasyon Merkezi içinde oluşturulmuş, Kök Sertifika Hizmet Sağlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve SSL sertifikalarını oluşturup imzalayan Elektronik Sertifika Hizmet Sağlayıcısı.

Çevrim içi sertifika durum protokolü : Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öğrenmelerine imkan tanıyan standart iletişim kuralı.

İptal durum kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkan veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıt.

Kamu Elektronik Sertifika Hizmet Sağlayıcısı: Kamu Sertifikasyon Merkezi içinde oluşturulmuş, Kök Sertifika Hizmet Sağlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve kullanıcıların sertifikalarını oluşturup imzalamakla yetkili kılınmış Elektronik Sertifika Hizmet Sağlayıcısı.

Kamu Sertifikasyon Merkezi: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

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

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Kullanıcı: Kamu SM sisteminde kimlik doğrulaması yapılmış ve sertifika almak üzere tanımlanmış kişiler.

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

Nitelikli elektronik sertifika: 5070 sayılı Elektronik İmza Kanunu'nun 9'uncu maddesinde sayılan nitelikleri haiz elektronik sertifika.

Sertifika güncelleme: Sertifika sahibi olarak sistemde geçerli kaydı olan ancak geçerli bir sertifikası bulunmayan kişilere yeni sertifika verilmesi süreci.

Sertifika iptal listesi: İptal olmuş sertifika bilgilerinin içinde yer aldığı ESHS'nin imzasını taşıyan elektronik dosya.

Sertifika sahibi: Kamu SM'den sertifika alan gerçek yada tüzel kişi.

Sertifika yenileme: Sertifika sahibi olarak sistemde geçerli kaydı ve geçerli bir sertifikası bulunan kişilere yeni sertifika verilmesi süreci.

Son kullanıcılar: Sertifika sahipleri ve sertifikaları kullanan üçüncü kişiler.

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

Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, ESHS tarafından elektronik imzayla doğrulanan kayıt.

1.6.2. Kısaltmalar

BS (British Standards): İngiliz Standartları

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]

DSA (Digital Signature Algorithm): Sayısal İmza Algoritması

DSA Eliptik Eğrisi (DSA Elliptical Curve): Sayısal İmza Algoritması Eliptik Eğrisi

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

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 Mühendisliği Görev Grubu Yorum Talebi

ISO/IEC (International Organisation for Standardisation / International Electrotechnical Committee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

PKI (Public Key Infrastructure): Açık Anahtarlı Altyapılar

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): RACE Bütünlük Asli Mesaj Değerlendirme Özeti

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SHS: Sertifika Hizmet Sağlayıcısı

SSL: Secure Sockets Layer

S/MIME: Secure Multipurpose Mail Extension

SUE: Sertifika Uygulama Esasları

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

2. Yayımlama ve Bilgi Deposu

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

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

2.1. Bilgi Depoları

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

<http://www.kamusm.gov.tr/BilgiDeposu> internet adresi üzerinden SUE ve Sİ dokümanları, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

<ldap://dizin.kamusm.gov.tr/> adresinden erişilebilen LDAP dizin sunucusu üzerinden SİL'lere erişim sağlanır.

<http://ocsp3.kamusm.gov.tr/> adresinden servis veren ÇİSDUP Yanıtlayıcısı üzerinden sertifika iptal listelerine alternatif olarak sertifikaların en güncel haliyle geçerlilik durumunun kontrolü yapılabilmektedir.

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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 Kök SHS ve ESHS sertifikaları,
- Kamu SM'ye ait Kök SHS sertifikasının özet değeri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi,
- Kamu SM Sİ ve SUE dokümanları,
- Taahhütnameler,
- Sözleşmeler,
- Formlar,
- Sertifika iptal durum kayıtları.

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, Sertifika Sözleşmeleri, sertifika yönetim prosedürleri, SUE ve Sİ dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip derhal yayımlanır.

Kamu SM'ye ait sertifikalar güncelleme yapılmasını müteakip derhal yayımlanır.

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

2.4. Erişim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM çalışanı kişiler tarafından yapılmaktadır.

Kamu SM bilgi deposu ile ilgili olarak aşağıdaki yükümlülükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve değiştirilmeye karşı bütünlüğünü korumak,
- Bilgi deposunda tutulan bilgilerin doğruluğu ve güncelliğini sağlamak,
- Bilgi deposunu sürekli olarak erişime açık tutmak,
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz sağlamak.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

3. Kimlik Belirleme ve Doğrulama

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kamu SM tarafından üretilen sertifikalarda, sertifika sahibine ait kimlik bilgilerinin 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

Sertifikalar üzerinde yer alan kimlik bilgileri gerçek yada tüzel kişileri tanımlayacak şekilde anlamlı olmalıdır (ad, soyad, kurum ismi, mail adresi).

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Sertifika içeriğinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kamu SM tarafından oluşturulan sertifikaların içeriğindeki kimlik bilgileri her gerçek yada tüzel kişiler için ayırt edici niteliktedir. Aynı gerçek yada tüzel kişiye ait sertifikaların içeriğindeki kimlik bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kişilere ait elektronik sertifikaların içeriğindeki kimlik bilgilerinin aynı olması engellenmektedir.

3.1.6. Markanın Tanınması, Doğrulaması ve Rolü

Sertifika başvuru sahipleri başvuru esnasında başkalarına ait fikri ve sınai mülkiyet haklarına zarar verecek isimleri kullanamazlar. Kamu SM sertifika başvurusu esnasında kullanılan isimlerin fikri ve sınai mülkiyet haklarının başvuru sahibine ait olup olmadığını doğrulamaz. Ortaya çıkabilecek herhangi bir fikri ve sınai mülkiyet hakkı problemi ile ilgili olarak Kamu SM sertifika başvurusunu reddetme veya ürettiği sertifikaları iptal etme hakkına sahiptir. Problemin giderilmesine yönelik olarak Kamu SM herhangi bir arabulucuk faaliyeti yürütmez.

3.2. İlk Kimlik Belirleme

Kamu SM, sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunduğu anda, ilgili kişi ve kurumun kimliklerinin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

SSL Sertifika başvurusu esnasında başvuru sahibi tarafından oluşturulan sertifika imzalama isteği imza oluşturma verisi ile imzalanır. Bu sayede imza oluşturma verisine sahiplik doğrulanır.

S/MIME sertifikası için imza oluşturma ve doğrulama verileri Kamu SM tarafından oluşturulup sertifika başvuru sahibine ulaştırılabilir. Bu durumda imza oluşturma verileri sertifika sahibine elektronik imza oluşturma aracında elden teslimat yapılarak ulaştırılır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

3.2.2. Kurumsal Kimliğin Belirlenmesi

Kamu SM'den SSL sertifikası talebinde bulunan kamu kurumlarının kimlik belirlenmesi Kamu SM ve ilgili kamu kurumu arasında yapılan resmi yazışmalar ve sertifika imzalama isteğinde belirtilen alan adının sahipliğinin ilgili kanallardan (nic.tr) doğrulanması yoluyla yapılır.

S/MIME sertifika başvurularında eğer başvuru sahibi tarafından sertifika içerisinde kurum bilgisi bulunması isteniyorsa ilgili kamu kurumlarının kimlik belirlenmesi Kamu SM ve ilgili kamu kurumu arasında yapılan resmi yazışmalar yoluyla yapılır.

3.2.3. Kişisel Kimliğin Belirlenmesi

Kamu SM'den SSL sertifikası talebinde bulunan kişilerin sertifika üzerinde yer alacak alan adı ile ilgili sertifika talep etmeye yetkili olup olmadığı madde 3.2.5 de anlatıldığı şekilde doğrulanır.

S/MIME sertifika başvurularında sertifika içeriğinde yer alacak olan e-posta adresinin başvuru sahibi tarafından kullanıldığını doğrulamak amacıyla e-posta adresi kullanılır. Bu amaçla ilgili e-posta adresi ile irtibata geçilerek doğrulama yapılır ve kişinin e-posta adresine erişiminin olduğu kanıtlanır. E-posta adresi olarak sadece kurum alan adına ait e-posta adresleri kabul edilir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Kamu SM tarafından oluşturulan SSL ve S/MIME sertifikaları doğrulanmayan bilgiler içermez.

3.2.5. Yetkinin Doğrulanması

Kamu SM'den SSL sertifikası talebinde bulunan kişilerin sertifika üzerinde yer alacak alan adı ile ilgili sertifika talep etmeye yetkili olup olmadığı ilgili kamu kurumları ile yapılan resmi yazışmalar ile doğrulanır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Geçerli bir sertifikası olan sertifika sahipleri, sertifikanın kullanım süresi dolmadan önce ve sertifikanın içeriğinde herhangi bir değişiklik olmaması durumunda, Kamu SM'ye olağan sertifika yenileme talebinde bulunabilirler. Olağan setifika yenileme isteğinde kimlik doğrulaması 3.2.2 ve 3.2.3 de belirtildiği şekilde yapılır.

3.3.2. İptal Sonrası Sertifika Güncelleme İsteğinde Kimlik Doğrulama

Sertifikanın içeriğindeki bilgilerin değişmesi, kullanım süresinin dolması ve iptal sonrası yeni sertifika isteğinde bulunulması durumunda, yeniden sertifika almak isteyen sertifika sahibi güncelleme talebinde bulunur. İptal sonrası sertifika güncelleme isteğinde kimlik doğrulaması 3.2.2 ve 3.2.3 de belirtildiği şekilde yapılır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi internet üzerinden işlem yaparak, çağrı merkezini arayarak veya Kamu SM'ye kağıt üzerinde ıslak imzalı form veya yazı göndererek sertifikasının iptal edilmesini isteyebilir.

İnternet üzerinden ve çağrı merkezinden iptal isteklerinin kabul edilebilmesi için sertifika sahibine ait parola veya kişisel bilgiler kullanılarak kimlik doğrulaması yapılır. Bunun için sertifika sahibinin iptal başvurusunda bulunduğu sırada bildirdiği parola ve diğer kişisel bilgileri, Kamu SM sisteminde kayıtlı bulunan bilgilerle kıyaslanarak doğruluğu kontrol edilir. Kağıt üzerinde ıslak imzalı form veya yazı ile yapılan iptal başvurularında kimlik doğrulaması sertifika sahibinin iletişim bilgileri kullanılarak irtibata geçilmesi yolu ile yapılır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4. İşlemsel Gereklere

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

- Sertifika başvurusu
- Sertifika yenileme
- Sertifika güncelleme
- Sertifika iptal etme

Süreçler sertifika sahipleri ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

SSL ve S/MIME sertifika başvurusu, kamu kurum veya kuruluşları tarafından Kamu SM'ye kurumsal olarak yapılır. Kurum, Kamu SM'den alacağı sertifika hizmetlerinin şartlarını belirleyen SSL veya S/MIME Sertifika Temini Sözleşmesini TÜBİTAK UEKAE ile karşılıklı imzalar. Kurum çalışanı kurumun talebi olmadan bireysel olarak sertifika başvurusunda bulunamaz.

Kurum, başvuru sırasında S/MIME sertifikası almak istediği çalışanlarının adını Kamu SM'ye bildirir. Kurum, çalışanın haberi olmadan çalışana adına sertifika başvurusunda bulunamaz. Kurum çalışanın durumdan haberdar olması ve S/MIME sertifikası almayı kendisinin talep etmesi gerekir. Bu talep, kurum çalışanı tarafından doldurulup imzalanan sertifika başvuru formunun Kamu SM'ye iletilmesi ile yapılır.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

SSL ve S/MIME sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurum, Kamu SM'den alacağı sertifika hizmetlerinin şartlarını belirleyen SSL veya S/MIME Sertifika Temini Sözleşmesini TÜBİTAK UEKAE ile karşılıklı imzalar.

Kurum SSL sertifikası için gerekli sertifika imzalama isteğini güvenli erişim kanalları kullanarak çevrimiçi olarak Kamu SM'ye iletir. S/MIME sertifikası için ise sertifika talebinde bulunduğu personelin listesini ilgili formlar ile birlikte resmi yazı ekinde Kamu SM'ye iletir. Bilgi ve belgelerin gizliliğinin sağlanması için belgelerin kapalı zarf içinde Kamu SM'ye iletilmesi gerekmektedir. Belgelerin Kamu SM'nin eline geçene kadarki zaman içerisinde gizliliğinin sağlanmasından kurum sorumludur.

S/MIME sertifikası başvurusunda bulunan kişi başvuru sırasında, sertifikasının herkesin erişimine açık izin sunuculardan yayımlanıp yayımlanmayacağı konusundaki talebini Kamu SM'ye yapar. S/MIME sertifikası başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama ve doğrulama işlevleri yerine getirilir.

SSL sertifikası başvurusunda bulunan kurumlar resmi yazı ve ekinde SSL sertifikası başvuru formunu Kamu SM'ye gönderir. İlgili form üzerindeki alan adı kaydının kurum tarafından kullanım hakkının olup olmadığı TR alan adları yönetiminden kontrol edilir.

S/MIME sertifikası başvurusunda bulunan kurumlar resmi yazı ve ekinde S/MIME sertifika başvuru formunu Kamu SM'ye gönderir. Başvuru formlarında bulunan e-posta adreslerine doğrulama mesajı gönderilerek başvuru sahibinin e-posta adresine sahipliği doğrulanır.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, sertifika başvurusu sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik bilgi veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyenlerle ilgili bilgilendirme kuruma ve/veya başvuru sahibi kişiye yazılı veya sözlü olarak yapılır. Yazılı bilgilendirme kuruma resmi yazı gönderme veya kurum ve/veya başvuru sahibine e-posta/sms gönderme yoluyla yapılır. Sözlü bilgilendirme kuruma ve/veya başvuru sahibine telefon açılarak yapılır. Kurum ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilenler Kamu SM sisteminde kullanıcı olarak tanımlanır ve sertifika üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin Kamu SM'nin eline geçmesinin ardından en fazla 10 (on) iş günü içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Sertifika başvurusu tamamlanarak sistemde kullanıcı olarak tanımlanan gerçek ve tüzel kişiler adına Kamu SM tarafından sertifika oluşturulur. SSL sertifikası oluşturulmadan önce başvuru sahibi tarafından Kamu SM'ye ulaştırılan sertifika imzalama isteğinin teknik kriterleri sağlayıp sağlamadığı da kontrol edilir.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Kamu SM oluşturulan SSL sertifikasını sahibine e-posta ve/veya güvenli çevrim içi yöntemler kullanarak ulaştırır, S/MIME sertifikası ise sertifika sahibine elektronik imza oluşturm aracında ulaştırılır. Hangi yöntemin kullanılacağı başvuru sahibi ile yapılan sözleşmelerde belirlenir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.4. Sertifikanın Kabul Edilmesi

4.4.1. Sertifikanın Kullanıma Açılma Biçimi

SSL sertifikaları sertifika sahibine ulaştırıldığı andan itibaren sertifika sahibi tarafından kabul edilmiş sayılır. Sertifika sahibi sertifika içerisindeki bilgilerin başvuru esnasında beyan ettiği bilgilerle aynı olup olmadığını kontrol eder ve herhangi bir uygunsuzluk durumunda derhal Kamu SM'yi bilgilendirir ve sertifikayı kullanmaz. Sertifika Kamu SM tarafından iptal edilir.

S/MIME sertifikaları ilk üretildiklerinde SİL içinde askıya alınmış konumda, ÇİSDUP yanıtlayıcı'da ise iptal konumunda bulunurlar. Askı ve iptal konumundaki sertifikalar ile işlem yapılamaz. S/MIME sertifikası sahibi aşağıdaki yöntemlerden birisi kullanılarak kullanıma açılabilir.

- <https://nesbireysel.kamusm.gov.tr> web adresi kullanılarak.

Sertifika sahibi, sertifikanın kullanıma açılması için <https://nesbireysel.kamusm.gov.tr> adresine bağlanarak, kendisine kapalı parola zarfı içinde gönderilen kullanıcı parolasını girer. İnternet üzerinden kimlik doğrulamasının yapılmasının ardından sertifikasının kullanıma açılması talimatını verir.

- Kamu SM Çağrı merkezi aranmak suretiyle.

Sertifika sahibi, Kamu SM çağrı merkezi vasıtasıyla kimlik doğrulamasının yapılmasının ardından sertifikasının kullanıma açılması talimatını verir.

- Kamu SM S/MIME Sertifikası Askıdan Çıkarma Başvuru Formu kullanılarak.

Sertifika sahibi, Kamu SM S/MIME Sertifikası Askıdan Çıkarma Başvuru Formu'nu doldurup imzalayarak Kamu SM'ye iletir.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM ürettiği S/MIME sertifikalarını, başvuru sırasında sertifika sahibinin onayını almak kaydıyla, herkesin erişimine açık LDAP dizin sunucusundan yayımlar.

4.4.3. Sertifikanın Oluşturulmasının Diğer Bileşenlere Duyurulması

Düzenlenmesine gerek duyulmamıştır.

4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

Sertifika sahipleri imza oluşturma verilerini yetkisiz kişilerin erişimine karşı korumakla yükümlüdür. SSL ve S/MIME sertifikalarına karşılık gelen imza oluşturma verileri yalnızca sertifikada “Anahtar Kullanımı” alanında belirtilen amaçlar dahilinde kullanılabilir.

4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Sertifika sahibine ait sertifikaların içinde yer alan imza doğrulama verileri, üçüncü kişilerce doğrulama amacıyla kullanılır. Üçüncü taraflar, güvencikleri sertifikanın ve sertifika yı oluşturan ESHS nin sertifikasının geçerliliğini kontrol etmekle, setifika “Anahtar kullanım” alanında belirtilen amaçlar doğrultusunda kullanıldığını doğrulamakla ve bu Sİ/SUE de belirtilen kullanım koşullarına uymakla yükümlüdürler.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.6. Sertifikanın Yeniden Üretilmesi

Sertifikanın yeniden üretilmesi, eski anahtar çifti kullanılarak sertifikanın yenilenmesi anlamına gelmektedir. Kamu SM sistemi içinde bu işlemin yapılmasına izin verilmemektedir.

4.7. Sertifikanın Yenilenmesi

Sertifikanın yenilenmesi, sistemde geçerli bir sertifikası bulunan sertifika sahibine, sertifikanın son geçerlilik tarihinden önce, yeni bir anahtar çifti üreterek ve sertifikanın içeriğinde bulunan bilgilerde değişiklik yapmadan, eskisinin yerine geçecek yeni bir sertifika verilmesi anlamına gelmektedir. SSL ve S/MIME sertifikaları için sertifika yenilemesi yapılmaz. Sertifika son geçerlilik tarihinden 60 gün önce sertifika sahibine e-posta gönderilerek sertifikasının geçerlilik süresi ve tekrar sertifika başvurusu yapması hususunda bilgilendirilir. Sertifika sahibi tekrar sertifika başvurusunda bulunmak isterse bölüm 4.1 de anlatıldığı şekilde başvurusunu gerçekleştirir.

4.8. Sertifikanın Güncellenmesi

Sertifikanın güncellenmesi, sertifika geçerlilik süresinin dolmuş olması veya sertifikanın içeriğindeki bilgilerde herhangi bir değişiklik olması durumlarında yeniden sertifika talep edilmesi ve üretilmesi anlamına gelmektedir. Sertifika güncellenmesi yeni sertifika başvurusu kapsamında değerlendirilir ve bölüm 4.1 de anlatılan süreç işletilir..

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifika iptali, sertifikanın kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda kullanımdan kaldırılması işlemidir. Sertifikanın kullanımdan kaldırılması iptal olduğu bilgisinin herkesin erişebileceği şekilde duyurulması anlamına gelmektedir.

Aşağıdaki sebeplerin ortaya çıkması durumunda sertifika sahibi Kamu SM'ye sertifikanın iptal edilmesi için başvuruda bulunur.

- İmza oluşturma verisinin güvenliğinin kaybedildiğinden şüphelenilmesi,
- Sertifikanın içeriğinde yer alan bilgilerin değişmesi.

Kamu SM, aşağıdaki sebeplerin ortaya çıkması durumunda sertifika sahibine ait sertifikayı iptal eder:

- Sertifika içeriğindeki sertifika sahibine ait bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması,
- Sertifika sahibinin fiil ehliyetinin sınırlandırıldığı, iflasının, gaipliğinin ya da ölümünün öğrenilmesi,
- Sertifikanın SSL ve S/MIME Sertifika Sahibi Taahhütnamesi, Kurum ile imzalanan SSLve S/MIME Sertifika Temini Sözleşmesi, Sİ/SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Kamu SM'nin sertifikayı imzalamak için kullandığı imza oluşturma verisinin güvenliğinin bozulması,
- Kamu SM'nin işleyişine son vermesi ve verilen sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.9.2. Sertifika İptal Başvurusunu Kimlerin Yapabildiği

Kamu SM tarafından verilen SSL sertifikalarını iptal etme yetkisi alan adı sahibi kurum yetkilisindedir. Kamu SM sertifika iptali yapmadan önce gerekli doğrulama işlemlerini yapar.

Kamu SM tarafından verilen S/MIME sertifikalarını iptal etme talebi, sözleşmede aksi belirtilmediği sürece, sadece sertifika sahibinin kendisi tarafından yapılabilir.

Kamu SM Bölüm 4.9.1’de belirtilen durumlarda sertifikayı iptal etme yetkisine sahiptir. Kamu SM, sertifikayı iptal ettiğinde sertifika sahibini ve gerekirse ilgili kişileri bilgilendirir, iptal sebebini açıklar.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

S/MIME sertifikası iptal başvurusu, sertifika sahibi tarafından telefonla çağrı merkezinden, internet sitesi üzerinden veya yazılı olarak Kamu SM’ye yapılır. İptal başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibinin kimlik belirlenmesi ve doğrulanması yapılır. Kimlik doğrulanması yapılamayan iptal başvuruları işleme alınmaz. İnternet üzerinden yapılan iptal başvurusunda, sertifika sahibi <https://nesbireysel.kamusm.gov.tr> internet adresi üzerinden, Kamu SM sisteminde kayıtlı bulunan kullanıcı parolasını girerek iptal talebinde bulunur. İnternet üzerinden kimlik doğrulama işleminin yapılmasıyla, sertifika Kamu SM sisteminde otomatik olarak iptal edilir. Çağrı merkezi aracılığıyla yapılan iptal başvurularında, sertifika sahibi Kamu SM çağrı merkezini arar. Çağrı merkezi üzerinden kimlik doğrulama işleminin yapılmasıyla, sertifika çağrı merkezinde çalışan sertifika işletmeni tarafından iptal edilir. Yazılı olarak yapılan taleplerde sertifika sahibi, imzasını taşıyan iptal başvuru formunu Kamu SM’ye iletir. Form üzerindeki bilgiler ve sertifika sahibine ait imza kontrol edilerek kimlik doğrulanması yapılır. Kimlik doğrulanmasının ardından sertifika Kamu SM sertifika işletmeni tarafından iptal edilir.

SSL sertifikası iptali başvuru alan adı sahibi kurum tarafından Kamu SM’ye kurum onaylı resmi yazı ile bildirimde bulunmak sureti ile yapılabilir.

Başvuruların nasıl yapılacağı Kamu SM’nin <http://www.kamusm.gov.tr> web adresinde ayrıntılı olarak anlatılır. Kamu SM iptal işleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar.

Kamu SM iptal bilgilerini en kısa zamanda işler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en azından sertifikanın seri numarası ile Kamu SM’nin elektronik imzasını taşır. Kamu SM, iptal durum kayıtlarını SSL ve S/MIME sertifikaları için SİL yayımlamak ve ek olarak S/MIME sertifikaları için ÇİSDUP Yanıtlayıcı’da sertifikanın durumunu iptal konumuna getirmek suretiyle duyurur.

SİL dosyası, Kamu SM’ye ait imza oluşturma verisi ile imzalanır. İptal edilen sertifikaların seri numarası sertifikanın geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra sertifika seri numarası SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı’da geçerlilik süresi dolan iptal edilmiş sertifikaların durumu iptal edilmiş konumda görünmeye devam eder.

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve gerekli doğrulamanın ardından sertifikayı iptal eder.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

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 sürekliliğini sağlar.

Üçüncü kişiler sertifikalara dayanarak işlem yapmadan önce sertifikaların geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

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

4.9.7. Sertifika İptal Listesi Yayınlama Sıklığı

Sertifika sahiplerine ait sertifika iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 36 (otuzaltı) saattir. Ancak bu sürenin dolması beklenmeden SİL yayım zamanından 24 (yirmidört) saat sonra güncellenir. Gün içinde yeni bir sertifika iptali olmasa dahi SİL güncellenir. Ancak geçerli bir iptal başvurusunun alınıp sertifika sahibine ait sertifikanın Kamu SM sistemi içinde iptal edilmesi durumunda, SİL dosyasının geçerlilik süresinin dolması beklenmeden en geç 5 (beş) dakika içinde yeni bir SİL dosyası yayımlanır. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait alt kök sertifikalarının iptal bilgilerinin duyurulduğu SİL dosyası 3 (üç) ayda bir yenilenir. Sertifikanın iptali durumunda SİL dosyası derhal yenilenir.

4.9.8. Sertifika İptal Listesi Yayınlama Gecikme Süresi

Sertifika İptal Listesi, belirtilen yayınlama zamanından en geç 5 (beş) dakika sonra yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Desteği

Kamu SM, S/MIME sertifikaların iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır. ÇİSDUP Yanıtlayıcı'daki iptal durum kayıtları geçerli iptal başvurusu alındığında 20 (yirmi) saniye sonra güncellenir.

ÇİSDUP desteği olan uygulamalar S/MIME sertifikasının geçerlilik durum kontrolünü <http://ocsp3.kamusm.gov.tr> adresi üzerinden sağlar.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Gereksinimi

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

SİL dosyası, iptal edilen her sertifika için iptal bilgisinin eklenmesiyle gittikçe büyüyen bir dosya niteliğindedir. Güncel iptal durum kaydına her ihtiyaç duyulduğunda dosyanın Kamu SM bilgi deposundan indirilmesi gerekir. Gittikçe büyüyen SİL dosyasının

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

sisteme getireceği yüke karşılık, ÇİSDUP ilgili sertifikanın iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır.

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. İmza Oluşturma Verisinin Güvenliğini Yitirmesi Durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunda sertifika iptal edilir. Sertifikanın iptal edilmesi dışında herhangi bir husus uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

SSL sertifikaları için askıya alma işlemi uygulanmamaktadır.

S/MIME sertifikaları sadece ilk üretildiklerinde Kamu SM tarafından askıya alınır ve sertifika sahibi tarafından Kamu SM'ye askıdan çıkarma talebi yapılmadığı sürece askıda kalmaya devam eder. S/MIME sertifikaları için sonraki aşamalarda askıya alma işlemi uygulanmaz.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Düzenlenmesine gerek duyulmamıştır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

4.9.16. Askıda Kalma Süresi

Kamu SM tarafından ilk üretildikleri sırada askıya alınan S/MIME sertifikaları aşağıdaki koşullar gerçekleşmediği sürece askıda kalmaya devam eder.

- Sertifika sahibi tarafından askıdan çıkarma talebinin Kamu SM'ye iletilmesi.
- Sertifikanın geçerlilik süresinin dolması.
- Sertifikanın herhangi bir sebepten dolayı iptal edilmesi.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. Kamu SM'ye ait SİL dosyalarına erişim bilgileri 2. Bölüm'de verilmiştir. SİL dosyaları her yeni iptal olduğunda güncellenir. Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi 2. Bölümde verilmiştir. Üçüncü kişiler sertifika veya sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

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

Sertifikanın kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM sertifikanın iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibini ve varsa sözleşmelerde belirtilen kişileri bilgilendirir. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmez; sertifika sahibi sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. Anahtar Yeniden Üretim

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

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.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM sisteminin çalıştığı binanın bulunduğu mekan, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgedir.

Bina, yüksek güvenlik gerektiren işlerin yapılmasına imkan sağlayan yapıdadır. Bina, esnek (çelik yapı) ve sert (çelik çatıyla desteklenmiş beton yapı veya desteklenmiş beton yapı) yapı şartlarını sağlamaktadır.

Kamu SM'nin kurulduğu yer ve binada güç birimleri, haberleşme birimleri, havalandırıcılar, yangın söndürücüler mevcut olup, deprem, su ve afetlere karşı gerekli tedbirler alınmıştır.

5.1.2. Fiziksel Erişim

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

Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kağıt ortamdaki bilgilerin tutulduğu, sistemin işletildiği ve yönetildiği odalara erişim gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Yetkisi olmayan kişiler sistemin kurulu olduğu odalara giriş yapamamaktadır. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

5.1.3. Güç Kaynağı ve Havalandırma

Aşağıdaki güç kaynakları Kamu SM işlevlerinin yerine getirilmesi ve sürekliliği için kullanılmaktadır:

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

Bina gerekli havalandırma sistemi ile donatılmıştır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.1.4. Su Baskınları

Kamu SM işlevlerinin yerine getirildiği ortamlarda su baskınlarından en az zarar görecektir şekilde önlemler alınmıştır.

5.1.5. Yangın Önleme ve Korunma

Kamu SM işlevlerinin yerine getirildiği 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, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve kullanılmayan elektronik veya kağıt ortamda tutulan bilgiler geri dönüşümsüz olarak yok edilir.

5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri , farklı bir fiziksel mekanda güvenli kasalarda saklar. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Kamu SM’de çalışan personelin rolleri aşağıda belirtildiği şekilde sınıflandırılmıştır:

Kamu SM Yöneticisi: Kamu SM iç işleyişinin yürütülmesini, Kamu SM’nin yasal yükümlülüklerinin yerine getirilmesini, talimat ve politikaların uygun olarak kullanılmasını, gerekli gördüğü durumlarda değişiklik ve düzenlemelerin yapılmasını sağlar.

Kamu SM Teknik Sorumlusu: Kamu SM birimleri arasında teknik uyumun gerçekleşmesini sağlar. Teknik faaliyetleri gözden geçirir. Bilgi sistemlerinin güvenliğini ve performansını izler.

Güvenlik Yöneticisi: Kamu SM güvenlik yöntemleri ve politikalarının uygulanmasını takip eder. Zaman içinde sistemin güvenlik ihtiyaçlarını belirler ve bu ihtiyaçların giderilmesini koordine eder.

Güvenlik İşletmeni: İşletmen sınır güvenliği ile ilgili varlıkların işlerliğinden sorumludur. Güvenlik duvarları, saldırı tespit sistemi, kayıt sistemi ve antivirüs sistemi idamesini sağlar.

Sistem Yöneticisi: Güvenlik bileşenleri hariç bütün sistemin işletiminden sorumludur. Sistemde zaman içerisinde yapılması gereken değişiklikleri koordine eder.

Sistem İşletmeni: Bütün sunucuların işletim sistemi ve donanım idamesinden sorumludur. Bileşenlerle ilgili gerekli güncellemeleri yapar.

Veri Sistemleri Yöneticisi: Dizin ve veritabanı yığınlarının (cluster) yönetimini yapar. Veritabanı yönetim faaliyetlerini gerçekleştirir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Sertifika Süreç Yöneticisi: Kamu SM internet sitesinde yayınlanan Sİ, SUE, ZDİ ve ZDUE dokümanlarını gerektiğinde güncellenmesini veya değiştirilmesini önerir, sertifika yönetim prosedürlerinde anlatılan prosedürlerin iyileştirilmesinden sorumludur.

Sertifika Üretim Ekip Lideri: Sertifikanın üretiminin planlanması, gerçekleştirilmesi ve sertifikaların teslimatı ile ilgili tüm çalışmaları yapar, sertifika üretim işletmenlerini koordine eder

Sertifika Üretim İşletmeni: Sertifika yaşam döngüsü işlemlerini Sertifika Yönetim Prosedürleri'nde belirtildiği şekilde yapar. Sertifika yaşam döngüsü süreçleri kapsamında gelen ve giden evrakı kontrol eder ve arşivler.

Sertifika Çağrı Destek İşletmeni: Kamu SM'ye gelen telefon çağrılara cevap verir. Prosedürler içinde belirtilen durumlarda sertifika sahibini bilgilendirir ve sertifika iptali isteklerini yerine getirir.

Elektronik Sertifika Yönetim Altyapısı (ESYA) ve Uygulama Destek Sorumlusu: Kamu SM'de kurulu olarak teslim aldığı ESYA sistemini yaşatmak için gerekli önlemleri alır.

Denetçi: Yönetim tarafından TÜBİTAK UEKAE içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından görevlendirilen bir kişi olan denetçi, sistem denetim profilinin kurulması, denetimlerin yönetimi ve gözden geçirilmesi ile sistemin teknik ve idari işleyişinin kontrolü ve raporlarının hazırlanmasından sorumludur.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök ve alt köklere ait sertifika üretilmesi ve iptal edilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, Kök ve alt köklere ait imza oluşturma verilerinin başka bir kriptografik modül içersine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilir.

Kamu SM sistemi içinde kimlik doğrulama güvenli donanım araçları, parolalar, gizli sorular ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Tanımlanan roller içinde sertifika işletmenleri dışındakiler için bir kişi birden fazla rolden sorumlu olabilir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

Çalışanlar sistemin işleyiş ve güvenlik gereklerini sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir. Kamu SM'nin istihdam ettirdiği personel sistem güvenliği, veri tabanı yönetimi, elektronik imza teknolojileri ve uygulamaları, sertifika yönetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kişilerden oluşur.

5.3.2. Geçmiş Araştırması

Çalışanların Kamu SM'nin işletilmesinde güvenlik ihtiyaçlarının gerektirdiği güvenilirliğe sahip olması gerekmektedir. Personelin güvenilirliği geçmişine yönelik yapılan araştırmalar ile belirlenir. İşe alınmadan önce geçmişe yönelik yapılan araştırmalarda personelin herhangi bir sebepten dolayı hüküm giyip giymemiş olduğu araştırılır.

5.3.3. Eğitim Gereklere

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

5.3.4. Sürekli Eğitim Gereklere ve Sıklığı

Kamu SM sisteminde yapılan değişikliklerin bildirilmesi amacıyla personele verilen eğitimler gerekli görüldükçe tekrarlanır. Yeni göreve başlayanlar için temel başlangıç eğitimi verilir.

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince işlem yapılır.

5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM kendi personeli dışındaki kişilerle çalışmak durumunda olduğunda, bu kişilerle ilgili olarak, kendi personeline uyguladığı güvenlik kontrollerini yapar.

5.3.8. Sağlanan Dokümantasyon

Çalışanlara işleriyle ve süreçlerle ilgili gerekli kılavuz ve destek dokümanları sağlanır.

5.4. Denetim Kayıtları

Kamu SM işleyişi sırasında gerçekleştirilen anahtar ve sertifika yönetimi, sistemin güvenliği ile ilgili işlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diğer bir kısmı ise kağıt üzerindedir. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde aşağıda yapılan işlemler ile ilgili elektronik veya kağıt ortamda yapılan işlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
 - Anahtar üretimi
 - Anahtar yedekleme
 - Anahtar yok etme
 - Kriptografik modül yaşam döngüsü işlemleri
- Sertifika üretim, yenileme, güncelleme , askıdan çıkarma ve iptal başvuruları
 - Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
 - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
 - Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
 - Kağıt belgelerin kopyalarının nerede saklandığı bilgisi
 - Geçerli ve geçersiz alınan tüm başvuru bilgileri
- Sertifika yaşam döngüsü yönetimi işlemleri
 - Sertifika kullanıma açma
 - Sertifika yenileme
 - Sertifika güncelleme
 - Sertifika askıdan çıkarma
 - Sertifika iptal etme
 - SİL yayımlanması
- Güvenlikle ilgili diğer işlemler
 - Sisteme başarılı veya başarısız tüm erişim denemeleri
 - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
 - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
 - Güvenlik profili değişiklikleri
 - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
 - Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
 - Kamu SM'ye ziyaretçi giriş ve çıkışı

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

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyişiyle ilgili tutulan kayıtlar düzgün zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluşup oluşmadığı kontrol edilir. Buna ek olarak, sistemde olağandışı hareketlerin görülmesi ya da alarm durumlarında

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görülen ve başlatılan işlemler de belgelenir.

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

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

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

- Kayıtlar yetkisi olan personel tarafından oluşturulur.
- Yetkisi olmayan kişiler elektronik kayıtların bulunduğu sistemlere erişemezler.
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunurlar.
- Kayıtların değiştirilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınmıştır.
- Elektronik olarak saklanan ve sistemin işleyişi açısından kritik olan kayıtlar, işlemi yapan personel tarafından gerektiğinde elektronik imza ile imzalanarak saklanır. Böylece kritik kayıtlarda oluşabilecek her değişiklik sistem tarafından fark edilir.
- Kritik bilgiler gerektiğinde Kamu SM'ye ait anahtarlarla şifreli olarak saklanır.

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim seviyesi düzeyinde otomatik olarak toplanır. Kamu SM çalışanları da sertifika işlemleri ile ilgili bilgi girişi yaptıklarında kayıt hazırlar.

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 Değerlendirilmesi

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

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sahibi veya bağlı bulunduğu kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Sertifika kullanıma açma yenileme, güncelleme, iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Sertifika işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM Kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Sertifika yönetim prosedürleri
- Kurumlarla yapılan Sözleşmeler
- Sertifika Sahibi Taahhütnameleri
- Kamu SM Taahhütnameleri
- Sertifika sahipleri ile yapılan Sertifika Sözleşmeleri

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, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduğu ortam 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 sürekliliği politikası gereğince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü 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. Aynı bilgiye ait birden fazla arşiv olması durumunda arşivler kıyaslanarak doğruluğu kontrol edilir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

5.6. Anahtar Değişimi

Kamu SM'ye ait anahtarlar ve sertifikalar geçerlilik süresinin dolması veya güvenlik gerekleriyle yenilenebilir. Kamu SM'ye ait sertifika nın kullanım süresinin dolmasından önce eski anahtar çiftinden yeni anahtar çiftine geçiş işlemleri yapılır. Anahtar değişimi işlemleri şunları gerektirir:

- Sertifika kullanım süresinin dolmasından en geç 6 (altı) ay önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyası aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalamaya devam eder. Yeni üretilen sertifikalar için oluşturulan SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.
- Kamu SM anahtarlarının yenilendiği bilgisini <http://www.kamusm.gov.tr> internet adresi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır. Depolama ünitesi fiziksel olarak farkı bir noktada bulunan veri depolama ünitesi ile veri senkronizasyonu yapabilecek niteliktedir. Arızanın giderilmesi süreci arıza sebebinin araştırılmasını, hatanın giderilmesini ve gerekli görüldüğünde Kamu SM hizmetlerini güvenilir yedek ortama aktarmayı içerir.

Gerekli görüldüğü takdirde imza oluşturma verisinin çalınması durumunda uygulanacak süreçler işletilir ve yeniden çalışırılık sağlanır.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin sertifika imzalamada kullandığı imza oluşturma verisinin gizliliğinin kaybedildiğinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aşağıdaki işlemler yerine getirilir:

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde <http://www.kamusm.gov.tr> internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Kamu SM, sertifika sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski gizli anahtarıyla oluşturulan sertifikalara güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM, tarafından üretilen sertifikaların gerekli görünen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM sertifika isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM imza oluşturma verisinin yok edilmesi sürecini işletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtar çiftinin yenilenmesiyle, iptal edilen sertifikaların kullanıcıdan gelen talep doğrultusunda güncellenmesi süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalışırılık

Kamu SM, arıza ya da afet sonrası sistemin en kısa zamanda yeniden ve güvenli olarak çalışmaya başlaması için gerekli yöntemleri ve süreçleri Kamu SM İş Sürekliliği Planı'nda tanımlar.

Kamu SM, arıza sonrası yeniden çalışırılığı sağlayacak Kamu SM İş Sürekliliği Planı'nı periyodik olarak gözden geçirir ve test eder.

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 aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün kurumlara yazı ile, sertifika sahiplerine e-posta ile duyurur.
- Sertifika hizmetlerine son vereceği bilgisini internet sitesi üzerinden ve ulusal yayın yapan en yüksek tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur.
- Sertifika hizmetlerine son vereceğini duyurmasından itibaren sertifika başvurusu kabul etmez ve yeni sertifika oluşturmaz.
- Dağıttığı sertifikaları iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği sertifikaların bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.
- İptal ettiği sertifikaların kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı imza oluşturma verisine karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Sertifikaları imzalamak için kullandığı imza oluşturma verisini imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde 20 (yirmi) yıl boyunca korur.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

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 ve ETSI TS 101 456 gereklilerini sağlar.

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1. Kök ve Alt Kök Anahtar Çifti Üretimi

Kök ve alt köklere ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, birden fazla eğitilmiş personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, güvenli yazılım kullanılarak üretilir. Üretilen imza oluşturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personeller tarafından onaylanır.

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

SSL sertifikaları için anahtar çifti üretimi sertifika sahibi tarafından gerçekleştirilir.

S/MIME sertifikaları için anahtar çifti Kamu SM tarafından üretilir. Sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım kullanılarak üretilir ve şifrelenerek elektronik imza oluşturma aracı içinde saklanır.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliği dünyaca kabul görmüş algoritmalar kullanılır. Anahtar çiftleri RSA, DSA, DSA Eliptik Eğrisi algoritmaları ile kullanılmak üzere üretilirler.

Sertifika sahibine ait imza oluşturma verisinin yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Elektronik imza oluşturma aracı sertifika sahibine teslim edilene kadar yetkisiz kişilerin erişemediği güvenli ve kilitli odalarda saklanır.

Sertifika sahibine ait imza oluşturma verisinin saklandığı elektronik imza oluşturma aracı Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip, imza oluşturma verisi, sertifika ile birlikte elektronik imza oluşturma aracı içinde imza karşılığı ve kimlik kontrolü yapılarak sahibine teslim edilir ve sertifika sahibi tarafından imzalanan elektronik imza oluşturma aracı teslim fişi teslim alınır.

Kamu SM, sertifika sahibine ait elektronik imza oluşturma aracı teslim fişinin kendisine ulaşmasına müteakip elektronik imza oluşturma aracı erişim verisini kapalı zarf içinde imza karşılığı ve kimlik kontrolü ile sahibine teslim eder, karşılığında sertifika sahibi tarafından imzalanmış parola teslim fişlerini teslim alır..

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Kamu SM, kurum ile yapılan sözleşmelerde belirtilmiş ise, kurum personeline ait, içerisinde imza oluşturma verisi ve sertifika olan elektronik imza oluşturma araçlarını ve elektronik imza oluşturma aracı erişim verilerini toplu olarak kurum yetkilisine imza karşılığında teslim eder. Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi <http://www.kamusm.gov.tr/BilgiDeposu> adresinden yayınlanır.

6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması

SSL sertifikası başvuru sahipleri başvurularının kabul edilmesi sonrasında imza doğrulama verisini PKCS#10 formatında sertifika imzalama isteği olarak güvenli kanallar üzerinden Kamu SM ye ulaştırırlar.

S/MIME sertifikası imza oluşturma ve doğrulama verileri Kamu SM tarafından oluşturulduğu için başvuru sahibi tarafından imza doğrulama verisinin Kamu SM ye ulaştırılması söz konusu değildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

Kamu SM'ye ait Kök ve alt kök sertifikaları internet ortamında tarafların erişimine hazır bulundurulur. Sertifikanın yayımlandığı ortamın izinsiz değiştirmeye ve silinmeye karşı güvenliği sağlanır.

Kamu SM'ye ait sertifikalar Kamu SM ye ait web sayfası üzerinden ve LDAP dizin sunucusundan yayımlanır.

Kök ve alt kök sertifikalarının özet değeri ve özet algoritması <http://www.kamusm.gov.tr> web adresi üzerinden yayımlanır ve Kamu SM'nin faaliyete geçmesini müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurulur.

6.1.5. Anahtar Uzunlukları

Kamu SM'ye ait Kök ve alt köklerin RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048-bittir.

ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarını imzalamak için kullanılan RSA imza oluşturma anahtar çiftlerinin boyu en az 2048-bittir.

Kamu SM tarafından üretilen S/MIME sertifika sahiplerine ait, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048-bittir.

Kamu SM tarafından üretilen SSL sertifika sahiplerine ait, RSA anahtar çiftlerinin 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.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan imza oluşturma verilerinin hangi amaçlar için kullanılabileceği ilgili imza oluşturma verisine karşılık gelen sertifikadaki “Anahtar Kullanımı” ve “Geliştirilmiş Anahtar Kullanımı” uzantısı içerisinde belirtilir.

6.2. İmza Oluşturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM’ye ait imza oluşturma verisi güvenli yazılım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduğu süre boyunca bu modül dışına çıkmaz.

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- İmza oluşturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- Erişim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.
- Kullanıcıya tanımlanan roller doğrultusunda verdiği hizmetlere erişimi sınırlar.
- Düzgün çalıştığı test edilebilir, test sırasında hata oluştuğunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluşturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluşturma verisinin içinde bulunduğu elektronik imza oluşturma aracı, imza oluşturma verisinin aracın dışına çıkmasını engelleyen ve araca erişimi parola ile sağlayan teknik özelliklere sahiptir.

Kriptografik modül aşağıdaki güvenlik standartlarından en azından birisini sağlar:

- FIPS PUB 140-1 veya FIPS PUB 140-2’ye göre seviye 3 veya üzeri,

Sertifika sahibinin elektronik imza oluşturma aracı aşağıdaki güvenlik standartlarından en azından birisini sağlar:

- CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-1,-2,-3)’e veya ISO/IEC 15408 (-1,-2,-3)’e göre en az EAL4+.

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

Kamu SM’ye ait imza oluşturma verisinin bulunduğu odaya erişim 2 (iki) çalışan tarafından sağlanmaktadır.

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

Kamu SM’ye ait imza oluşturma verisinin yedeğinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme işlemi hazırda kullanılmakta olan imza oluşturma

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

verisi için sağlanan güvenlik ile eşdeğer güvenlik önlemleri altında yapılır. Yedeklenen imza oluşturma verisi yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan imza oluşturma verisinin bulunduğu ortam ile aynı güvenlik şartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait imza oluşturma verileri Kamu SM tarafından yedeklenmez.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluşturma verileri arşivlenmez.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

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

S/MIME sertifika sahiplerine ait imza oluşturma verileri, sadece yetkili personelin giriş izninin bulunduğu odalarda elektronik imza oluşturma aracına, şifrelenerek yüklenir.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

Kamu SM'ye ait imza oluşturma verileri, yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. İmza oluşturma verisinin yedekleme amacı haricinde cihaz dışına çıkması engellenmiştir. İmza oluşturma verisi kriptografik modül içinde güvenli algoritma ve yöntemlerle şifreli olarak saklanır.

Sertifika sahibine ait imza oluşturma verisi sertifika sahibinin elektronik imza oluşturma aracı içinde saklanır, başka bir ortamda bulunmaz. Kamu SM sertifika sahiplerine ait imza oluşturma verilerini kendi sistemi içinde saklamaz.

6.2.8. İmza Oluşturma Verisine Erişim

Kamu SM'nin imza oluşturma verisine erişim birden fazla yetkili çalışanın ortak denetimi altındadır. İmza oluşturma verisinin bulunduğu odaya giriş için, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doğrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin doğrulanmadığı durumlarda imza oluşturma verisinin bulunduğu odaya erişim sağlanamaz.

İmza oluşturma verisi kriptografik modül içinde şifreli durumdayken erişime kapalıdır. Erişime açılması için erişimi sağlayan verinin modüle sunulması gerekir. İmza oluşturma verisinin erişime açılması ve kullanılabilir duruma getirilmesi birden fazla yetkili çalışanın ortak denetimi altındadır.

S/MIME sertifika sahibine ait imza oluşturma verisi elektronik imza oluşturma aracı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi

Kamu SM'nin imza oluşturma verisi imzalama için kullanıldıktan sonra oturum kapandığında veriye erişim otomatik olarak kesilir ve bir dahaki kullanımına kadar şifrelenerek erişime kapalı tutulur. Erişimin yeniden sağlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden işletilmesi gerekir.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Sertifika sahibinin kullandığı elektronik imza oluşturma araçları, imza oluşturma verisini kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir. Erişim verisinin ard arda 3 (üç) defa yanlış girilmesi durumunda elektronik imza oluşturma aracı kilitlenir ve araca erişim sağlanamaz.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

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

Sertifika sahiplerine ait imza oluşturma verileri kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından elektronik imza oluşturma aracı üzerinden silinmelidir. Bu işlemin yapılmasından sertifika sahibi sorumludur.

6.2.11. Kriptografik Modülün Değerlendirilmesi

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

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doğrulama verileri sertifikalar içinde tutulur ve sertifikalar kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Sertifikaların arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

İmza oluşturma verisinin kullanım süresi, sertifikanın içeriğinde belirtilen kullanım süresi kadardır. Sertifikanın kullanım süresinin dolmasıyla ya da sertifikanın iptal edilmesiyle imza oluşturma verisinin kullanımı sona erer. Ancak, kullanım süresi dolsa bile sertifikalar içindeki imza doğrulama verileri geçmişe yönelik imzaların doğrulanabilmesi için kullanılır.

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan imza algoritmasına göre belirlenir. Kamu SM'ye ait 2048 ve 4096 bitlik RSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. S/MIME sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 3 (üç) yıl için kullanılır.

Üretilen sertifikaların son kullanma tarihi kendisine sertifika veren Kamu SM'ye ait kök ve alt kök sertifikasının son kullanma tarihini aşamaz.

6.4. Erişim Denetim Verileri

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

S/MIME sertifika sahibine ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, elektronik imza oluşturma aracı erişim verisi ile internet ve çağrı merkezi üzerinden sertifika askıdan çıkarma ve iptal etme işlemlerinin yapılabilmesi için kullanılan kullanıcı parolasıdır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

6.4.1. Erişim Denetim Verilerinin Oluşturulması

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

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

6.4.2. Erişim Denetim Verilerinin Korunması

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

Sertifika sahibine ait erişim parolaları kapalı zarf içinde sertifika sahibine ulaştırılır ve kopyası Kamu SM tarafından tutulmaz.

Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı ikinci kişilerin erişiminden korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları kapalı zarf içinde, kimlik kontrolü yapılarak imza karşılığı sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gereklere

Kamu SM sistemi içinde kötü niyetli yazılımlara karşı gereken önlemler alınır. Sistemde ağ ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuştur. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerinin tahrifata, silinmeye ve kaçağa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliği konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Denetimleri

6.6.1. Sistem Geliştirme Denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda verilmiştir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileşenlerin yedekleri oluşturulur.
- Sistemin açık ağ bağlantısında gerekli güvenlik önlemleri alınır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs taramasından geçirilir ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileştirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan denetimler TS ISO/IEC 27001 gereklerini sağlar.

6.6.2. Güvenlik Yönetimi Denetimleri

Sistem içinde kurulu olan yazılım ve donanım ürünleri ile ağ ortamının işleyişinin planlanan şekilde güvenli olarak sürdürüldüğünü göstermek için iki (2) yılda en az bir defa güvenlik yönetimi denetimi yapılır. Kamu SM içinde güvenliğe uygun olmayan hareketler ve yetkilendirmeler denetleme sonucunda açıklanır ve düzeltici önlemler alınır.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği denetimleri yapılır. Sistem, dış açık ağa bağlantısında güvenlik duvarlarını kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi sunucuları mevcuttur.

Sunucular üzerine ağ ve sistem yönetimi ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı gibi bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi yazılımı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler için farklı ağlar kurulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir.

6.8. Zaman Damgası

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

Zaman damgasıyla ilgili ayrıntılı bilgi Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları'nda bulunur.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından oluşturulan Kök, Alt kök, SSL ve S/MIME sertifikaların içeriği ile ilgili bilgilendirme yapılmaktadır.

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

Kamu SM tarafından dağıtılan sertifikalar X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili imza doğrulama verisi, sertifika sahibine ve 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. Sertifikanın içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Kamu SM tarafından oluşturulan Kök, Alt kök, SSL ve S/MIME sertifikalarının içeriği EK-A da bulunmaktadır.

Uzantılardan bazıları kritik olarak tanımlanmıştır. Kritik olarak belirtilen uzantıların sertifikayı kullanan uygulama tarafından tanımlanamaması durumunda sertifikanın kullanılmaması gerekir.

7.1.3. Algoritma ve Nesne Tanımlayıcılar

EK-A da belirtilmiştir..

7.1.4. İsim Alanı Biçimleri

Kamu SM tarafından üretilen sertifikalardaki isim alanı “ITU X.500 Distinguished Name [Ayırt edici isim]” biçimine uygundur.

7.1.5. İsim Kısıtları

Bölüm 3.1 de belirtilmiştir.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Kamu SM tarafından oluşturulan her sertifika içeriğinde, o sertifikanın hangi sertifika ilkelerine göre kullanılacağını belirtmek amacıyla, ilgili sertifika ilkesine ait nesne tanımlayıcısı bulunmaktadır. SSL ve S/MIME sertifikalarında bu dökümana ait olan {2.16.792.1.2.1.1.5.7.1.2} nesne tanımlama numarası kullanılır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

“Sertifika İlkeleri Uzantısı” sertifikaların üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. SSL ve S/MIME sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ/SUE dokümanına

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen sertifikaların “Sertifika İlkeleri Uzantısı”nın içinde yer alır. “Sertifika İlkeleri Uzantısı”nın içinde “İlke Niteleyici” olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler “Sertifika İlkeleri Uzantısı”nı kontrol ettiğinde Sİ/SUE’de belirtilen ilke ve uygulama esasları çerçevesinde sertifikaları kullanarak işlem yapar.

Kamu SM tarafından oluşturulan SSL ve S/MIME sertifikalarda “Sertifika İlkeleri Uzantısı” içeriğinde nesne tanımlama numarası olarak {2.16.792.1.2.1.1.5.7.1.2} ve ilke niteleyici olarak http://www.kamusm.gov.tr/BilgiDeposu/KSM_CES_SUE yer alır.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

- SİL’i oluşturan Kamu SM’ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL’i imzalamak için SHA-1 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL’in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen sertifikalarla ilgili aşağıdaki bilgiler:
 - Sertifikanın seri numarası
 - Sertifikanın iptal tarihi
 - Sertifikanın neden iptal edildiği bilgisi
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM’ye ait sertifikanın “ESHS Anahtar Tanımlayıcı” bilgisi

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 2560 V.1’i destekler.

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir.

- Protokol versiyonu

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Hedef sertifika belirteci (kullanılan özetleme algoritması, sertifikayı veren ESHS'nin DN özeti, sertifikayı veren ESHS'nin imza doğrulama verisi özeti, sertifika seri numarası,)

ÇİSDUP cevapları aşağıdaki bilgileri içermektedir.

- Versiyon bilgisi
- Cevaplayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan İmza algoritmasının OID si.
- ÇİSDUP yanıtlayıcı imzası

Bütün geçerli ÇİSDUP cevapları ÇİSDUP yanıtlayıcı tarafından imzalanır. Geçersiz ÇİSDUP sorguları için dönen hata mesajları imzalanmaz.

Çevrim İçi Sertifika Durum Protokolü RFC 2560'da tarif edilen "ÇİSDUP" formatını destekler. ÇİSDUP Yanıtlayıcı'dan alınan cevaplar aşağıdaki şekilde değerlendirilir:

Good [iyi]: Sertifika geçerli konumdadır.

Bad [kötü]: Sertifika askıdadır, iptal edilmiştir ya da henüz kullanıma açılmamıştır.

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

RFC 2560'da belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

8. Uygunluk Denetimleri

Bu bölümde Kamu SM sertifika yönetim sisteminin Sİ/SUE dokümanına uygunluğunun denetlenmesi ile ilgili bilgilendirme yapılmaktadır.

8.1. Uygunluk Denetiminin Sıklığı

Kamu SM sertifika yönetim sisteminin bu Sİ/SUE dokümanında belirtilen şartları sağlayıp sağlamadığı 2 (iki) yılda en az bir kere denetlenir. Denetim Kamu SM'nin denetimle görevlendirdiği personel tarafından yerine getirilir.

8.2. Denetçinin Nitelikleri

Denetçinin Sİ/SUE dokümanında belirtilenleri iyi anlaması, açık anahtarlı altyapılar hakkında bilgi sahibi olması ve uygunluk denetimleri konusunda tecrübeli olması gerekir.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Denetçi TÜBİTAK UEKAE içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından seçilir.

8.4. Denetimin Kapsamı

Sertifika yönetim süreçlerini detaylandırarak anlatan sertifika yönetim prosedürlerinin, Kamu SM'nin iç işleyişindeki güvenlik ve işlevsel süreçlerin incelenerek işleyişin Sİ/SUE dokümanına uygunluğu denetlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

Denetim sırasında Kamu SM'nin, Sİ ve SUE dokümanlarının gereklerini yerine getirmediğinin tespit edilmesi durumunda, denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu yazdığı raporla ilgililere bildirir. Kamu SM yönetiminin önderliğinde yetersizliği tespit edilen durumların giderilmesi için yapılacak işlemler belirlenir ve yetersizliğin giderilmesi için çalışma başlatılır.

Denetimde sistemin kurulum, işletim veya bakım aşamaları sırasında, Sİ ve SUE dokümanlarının gereklerinin yerine getirilmediğinin tespit edilmesi durumunda aşağıdaki işlemler gerçekleştirilir:

- Denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu not eder ve ilgili tarafları 2 (iki) gün içinde bilgilendirir.
- Kamu SM denetim sonucu tespit edilen yetersizliklerini SUE dokümanında belirtilen uygulama esaslarına uygun olarak giderir.
- Sertifika yönetimiyle ilgili kritik bulunan işlemlerde yetersizliğin tespit edilmesi durumunda, Kamu SM ilgili işlemleri düzeltmeler yapılncaya kadar durdurur.

Ayrıca, Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluşturması, geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluşturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diğer yetkisiz eylemlerde ilgili mevzuat gereğince işlem yapılır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

8.6. Sonucun Bildirilmesi

Denetim sonucu rapor olarak Kamu SM yönetimine bildirilir. Kamu SM yönetimi raporda belirtilen, Sİ ve SUE'ye uygun olmadığı tespit edilen durumların en kısa zamanda düzeltilmesini sağlar.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen, yenilenen ve güncellenen sertifikalar için kurumlardan veya sertifika sahiplerinden ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında veya kurumlara yapılan sözleşmelerde bildirilir.

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

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ve kullanıcılara ait sertifikaları ücretsiz olarak yayımlar.

9.1.3. İptal Durum Kaydına Erişim Ücreti

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

9.1.4. Diğer Servis Ücretleri

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

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

9.1.5. İade Ücreti

Sertifika sahibi sertifikasını ilk teslim aldığı anda yaptığı kontrol neticesinde, sertifikasını kullanmadığını tespit ederse ve sorunun Kamu SM'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa, talebi halinde sertifika sahibinin sertifika için ödenen ücreti iade edilir. Elektronik imza oluşturma aracı erişim verisinin kaybolması, unutulması, aracın yanlış erişim verisi girilmesi dolayısıyla kilitlenmesi, sertifika sahibinin yanlış kullanımından dolayı aracın kullanılamaz duruma gelmesi, sertifikanın iptali ve benzeri durumlarda ücret iadesi yapılmaz..

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Kamu SM, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) Müdürlüğü tarafından işletilmektedir. TÜBİTAK – UEKAE SSL ve S/MIME sertifikaları ile ilgili olarak sertifika sahiplerine ve sertifikayı kullanan üçüncü taraflara yönelik şu an için herhangi bir sigorta uygulamamaktadır.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

9.2.3. Sertifika Mali Sorumluluk Sigortası

Düzenlenmesine gerek duyulmamıştır.

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 tarafından <http://www.kamusm.gov.tr/BilgiDeposu> adresinden yayımlanan her türlü döküman ve sertifikalar içerisinde yer alan bilgiler gizli olarak değerlendirilmezler.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Düzenlenmesine gerek duyulmamıştır.

9.4.2. Özel Olarak Tanımlanan Bilgiler

Kişisel bilgi sertifika sahibinin, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği doğum tarihi, doğum yeri gibi nüfus bilgileri ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi tarafından atanan parolalar, numara, sembol gibi diğer tanımlayıcıyı bilgiler de kişisel bilgi kapsamına girer.

9.4.3. Özel Olarak Tanımlanmayan Bilgiler

Kamu SM tarafında oluşturulan sertifikaların içeriğinde bulunan bilgiler aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiği kişisel bilgileri sertifika hizmeti vermek dışında başka amaçlar için kullanmaz, üçüncü kişilere vermez, sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulundurmaz.

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

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM sertifika sahiplerine ait gizli kişisel bilgileri, mahkeme kararı olması durumunda açıklayabilir.

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

Kamu SM tarafından üretilen tüm sertifikalar ve dokümanlar ile bu Sİ/SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM, sertifika sahipleri, sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları ile üçüncü kişiler sertifika sözleşmeleri ve taahhütnamelerde sözü geçen yükümlülükleri yerine getirirler.

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHS olarak Kamu SM'nin yükümlülükleri şunlardır:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek,
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek,
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak,
- Kök ve alt kök ler için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak,
- Kök ve alt kök sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak,
- Sertifika verdiği gerçek veya tüzel kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek,
- Kurumlardan gelen sertifika başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek suretiyle kimlik doğrulamalarını yapmak,
- Sertifikaların içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak,
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine sertifika vermemek,
- Sertifika başvurularını değerlendirerek, başvurunun sonucu hakkında ilgili kişileri bilgilendirmek,
- Sertifika başvurusu kabul edilmiş kişiler için sertifika üretmek,
- S/MIME sertifika sahibine ait imza oluşturma ve doğrulama verilerini oluşturmak,
- Üretilen S/MIME sertifikaları ile imza oluşturma verilerini veya SSL sertifikalarını Sİ/SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek,

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Sertifika sahiplerinin sertifikalarını aksi başvuru formu ve taraflar arası sözleşmelerde belirtilmedikçe son kullanıcıların erişebileceği ortamlarda yayımlamak,
- Sertifika yenileme/güncelleme başvurularını Sİ/SUE’de belirtilen şekilde kabul etmek ve değerlendirerek gerekli yenileme/güncelleme işlemlerini yapmak,
- S/MIME sertifikası askıdan çıkarma işlemlerini Sİ/SUE’de belirtilen şekilde yapmak,
- Sertifika iptal başvurularını Sİ/SUE’de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak,
- Yayımlanan Sİ/SUE dokümanı ile Sertifika Sahibi Taahhütnamesi’ne uygun olmayan sertifika kullanımlarının tespit edilmesi durumunda ilgili sertifikayı iptal etmek,
- İptal edilmiş sertifika bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak,
- Sertifikaların ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak,
- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek,
- Sertifika üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak,
- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları ilgili Sİ/SUE’de belirtilen süreler boyunca güvenli olarak saklamak,
- Kök SHS sertifikasının özet değerini Kamu SM’ye ait internet ortamından yayımlamak, ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurmak ve gazete ilanlarının bir örneğini Telekomünikasyon Kurumu’na iletmek.

9.6.2. Kayıt Birimi Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri şunlardır:

- Sertifika başvuru, yenileme, güncelleme, iptal ve diğer işlemleri ilgili Sİ/SUE’de belirtildiği şekilde, detayları Kamu SM sertifika yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- Sertifika başvurusu, yenileme, güncelleme ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- S/MIME sertifikaları için adına düzenlenen, imza oluşturma verisini içeren elektronik imza oluşturma aracı ve kapalı parola zarfını şahsen teslim almak,
- Adına düzenlenen sertifikadaki bilgilerin doğruluğunu kontrol etmek,
- Sİ/SUE Bölüm 6.2.1’de belirtilen standartlara uygun elektronik imza oluşturma aracı kullanmak,
- İmza oluşturma verisinin güvenliğini sağlamak, kendisine ait imza oluşturma verisinin içinde bulunduğu elektronik imza oluşturma aracının ve imza oluşturma verisi erişim

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

verisinin gizliliğini korumak, bunları başkasına kullanırmamak ve bu konuda gerekli tedbirleri almak,

- İnternet veya çağrı merkezi üzerinden sertifika işlemlerini yapabilmesi için kullandığı parolalarının gizliliğini ve güvenliğini sağlamak,
- İmza oluşturma verisinin içinde bulunduğu elektronik imza oluşturma aracının kaybolması, çalınması veya imza oluşturma verisinin gizliliğinin yitirildiğinden şüphelenmesi durumunda sertifikanın iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Elektronik imza oluşturma aracı erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları her ay düzenli olarak değiştirmek,
- Kamu SM tarafından kendisi için oluşturulmuş sertifikanın içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak,
- Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri derhal Kamu SM'ye bildirmek,
- İptal olmuş, kullanıma açılmamış, askıya alınmış veya geçerlilik süresi dolmuş sertifika ile işlem yapmamak,
- İmza oluşturma verisini SHS sertifikası imzalamak amacıyla kullanmamak,
- Kendisine verilen sertifikayı Sİ/SUE dokümanında belirtildiği biçimde, Sertifika Sözleşmesi'nde ve Sertifika Sahibi Taahhütnamesi'nde belirtilen şartlar dahilinde kullanmak.

Yukarıda beyan edilen yükümlülüklerin ihlali nedeniyle üçüncü kişilerin zarara uğraması halinde TÜBİTAK UEKAE'nin ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, sertifikalarla ilgili işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Sertifikanın, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek,
- Sertifikanın geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikalarının içinde mevcut olan imza doğrulama verilerini kullanarak doğrulamak,
- Sertifikanın doğruluğunu Kamu SM alt kök sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu SM alt kök sertifikasının doğruluğunu kök sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu SM kök sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Sertifika sahibinin sertifikasının içindeki imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğunu doğrulamak.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri veya sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları arasındaki yükümlülük, Sertifika Sözleşmesi, Sertifika Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve kurumla imzalanan SSL, S/MIME Temini Sözleşmesi'nde belirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ilgili sınırlamalar Sertifika Sözleşmesi, Sertifika Sahibi Taahhütnamesi ve kurumla imzalanan SSL, S/MIME Temini Sözleşmesi'nde de belirlenir.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahipleri Sertifika Sözleşmesi, Sertifika Sahibi Taahhütnamesi'ne uygun olarak Kamu SM ile işbirliği içinde çalışır. Kamu SM'den sertifika hizmeti alan kamu kurumları SSL, S/MIME Temini Sözleşmesi'ne uygun olarak Kamu SM ile işbirliği içinde çalışır.

Kurumlar ve sertifika sahipleri sertifika hizmetlerini aldıkları süre boyunca Sİ ve SUE dokümanları ile sertifika yönetim prosedürlerinde belirtilen şartları yerine getirmeyi kabul ederler.

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ/SUE dokümanı, sertifika yönetim prosedürleri, sertifika sahibine ilettiği Kamu SM Taahhütnamesi ve kurum ile imzaladığı SSL, S/MIME Temini Sözleşmesi'ndeki şartları yerine getirir.

9.10.1. Anlaşma Süresi

Sertifika sahibinin imzaladığı Sertifika Sözleşmesi veya Sertifika Sahibi Taahhütnamesi'nin süresi sertifikanın geçerlilik süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda Sertifika Sözleşmesi veya taahhütnamenin süresi de sona erer. Aynı şekilde Kamu SM Taahhütnamesi de sertifika sahibinin sertifikasının geçerlilik süresince geçerlidir.

Kurumla imzalanan SSL, S/MIME Temini Sözleşmesi'nin geçerlilik süresi sözleşme içerisinde belirtilir.

9.10.2. Anlaşmanın Sona Ermesi

Kamu SM ile kurum arasında imzalanan SSL, S/MIME Temini Sözleşmesi aşağıdaki durumlarda sonlandırılabilir:

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

- Taraflardan birisinin sözleşmeye uygun olarak, sözleşmenin sonlandırılması için talepte bulunması
- Sözleşmenin süresinin sona ermesi
- Her iki tarafın da ortak karar alarak sözleşmeyi bitirmesi
- Taraflardan birisinin sözleşmeye aykırı davranması: Taraflardan biri sözleşme kapsamında üzerine düşen yükümlülükleri yerine getirmez ise diğer taraf sözleşmeye aykırı davranan tarafa bu yükümlülüğü yerine getirmesi için 5 (beş) günlük süre verir. Bu sürenin sonunda da sözleşmeye aykırılık ortadan kaldırılamaz veya doğacak zarar, ziyan talepleri saklı kalmak kaydıyla yükümlülük yerine getirilmez ise sözleşme tek taraflı olarak fesh edilebilir.
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması durumunda Kamu SM sertifika sahiplerine ait sertifikaları iptal ederek SSL, S/MIME Temini Sözleşmesini sonlandırabilir.
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırır, sertifika sahiplerine ait sertifikaları iptal ederek SSL, S/MIME Temini Sözleşmesini sonlandırabilir.

Kamu SM Taahhütnamesi ve Sertifika Sahibi Taahhütnamesi veya Sertifika Sözleşmesi aşağıdaki durumlarda sonlandırılabilir:

- Sertifika sahibinin sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi
- Sertifika sahibinin Sertifika Sözleşmesi veya Sertifika Sahibi Taahhütnamesi'ne aykırı davranması durumunda Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi
- Bölüm 5.7.3'te belirtilen güvenlik açığının ortaya çıkması sebebiyle Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırır, Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

SSL, S/MIME Temini Sözleşmesi'nin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ/SUE dokümanında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Kamu SM kurumdan sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmış başvurular ile ilgili işlemler, anlaşmanın sona erme sebebine bağlı olarak kurumun talep etmesi durumunda devam eder.

Sertifika Sözleşmesi veya Sertifika Sahibi Taahhütnamesi'nin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ/SUE dokümanında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

Sözleşme ve taahhütnameler sona erse bile Kamu SM, dağıttığı sertifikalarla ilgili, yükümlülüklerini yerine getirmeye devam eder. Kamu SM, dağıttığı sertifikalara, iptal durum kayıtlarına taraflarca erişimin sağlanması, Bölüm 5.4 ve 5.5'de belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, sertifika yönetim prosedürlerinde sertifika başvurusunun sonucu, iptal, güncelleme ve yenileme taleplerinin sonuçları hakkında sertifika sahibini ve/veya ilgili kurumu bilgilendirir. Bilgilendirmeler telefon, faks veya e-posta aracılığıyla olur. Kişinin sertifika başvuru formunda belirtilen e-posta adresine, değişmesi halinde yeni bildirdiği e-posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

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

Sertifika yönetim işlemleri sırasında sertifika sahibi veya kurumlarla yapılan haberleşmenin hangi durumlarda, ne şekilde yapılacağı Kamu SM'nin sertifika yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metodları

Sİ/SUE dokümanı Kamu SM tarafından yazılmıştır. Bu Sİ/SUE dokümanında yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, Kamu SM dokümanının tamamen yenilenmesine de karar verebilir. Bu Sİ/SUE dokümanının herhangi bir kısmının yanlış ya da geçersiz olduğu ortaya çıksa bile, Kamu SM Sİ/SUE'nin diğer kısımları, Sİ/SUE dokümanı güncellenene kadar geçerliliğini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

Sİ/SUE dokümanında yapılan değişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer.

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilafların çözümünde karşılıklı imzalanan sözleşmeler, taahhütnameler, Kamu SM Sertifika İlkeleri ve Kamu SM Sertifika Uygulama Esasları dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

9.14. Uygulanacak Hukuk

İhtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

EK-A Sertifika Biçimleri

a) TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı – Sürüm 3

Alan	Değer
Sürüm	V3
Seri Numarası	11
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	24 Ağustos 2007 Cuma 13:37:07
Geçerlilik Sonu	21 Ağustos 2017 Pazartesi 13:37:07
Konu	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; bd 88 87 c9 8f f6 a4 0a 0b aa eb c5 fe 91 23 9d ab 4a 8a 32
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama , Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

b) Kamu Elektronik Sertifika Hizmet Sağlayıcısı – Sürüm 3

Alan	Değer
Sürüm	V3
Seri Numarası	14
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	24 Ağustos 2007 Cuma 16:25:29
Geçerlilik Sonu	21 Temmuz 2017 Cuma 16:25:29
Konu	CN = Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; bd 88 87 c9 8f f6 a4 0a 0b aa eb c5 fe 91 23 9d ab 4a 8a 32
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; e3 87 c3 ec 1d c4 25 b7 ed f7 92 1b 36 31 da ac d1 b9 cc f2
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama , Çevrimdışı Sil İmzalama, Sil İmzalama
Temel Kısıtlar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=1
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.1 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://www.kamusm.gov.tr/BilgiDeposu/KOKSIL.v3.crl [2]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=ldap://dizin.kamusm.gov.tr/CN=KOKSIL.v3,O=KSM,C=TR?certificateRevocationList?base?objectclass=cRLDistributionPoint
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://www.kamusm.gov.tr/BilgiDeposu/KOKSHS.v3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=ldap://dizin.kamusm.gov.tr/CN=KOKSHS.v3,O=KSM,C=TR?cACertificate?base?objectclass=certificationAuthority

c) Cihaz Sertifikası Hizmet Sağlayıcısı – Sürüm 3

Alan	Değer
Sürüm	V3
Seri Numarası	15
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	24 Ağustos 2007 Cuma 18:01:21
Geçerlilik Sonu	21 Temmuz 2017 Cuma 18:01:21

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Konu	CN = Cihaz Sertifikası Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; bd 88 87 c9 8f f6 a4 0a 0b aa eb c5 fe 91 23 9d ab 4a 8a 32
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 96 2a 85 76 7f b5 83 17 e0 e1 2e 34 86 0b 4b 3f d8 6e 29 4e
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama , Çevrimdışı Sil İmzalama, Sil İmzalama
Temel Kısıtlar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=1
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.2 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://www.kamusm.gov.tr/BilgiDeposu/KSM_CES_SUE [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://www.kamusm.gov.tr/BilgiDeposu/KOKSIL.v3.crl [2]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= ldap://dizin.kamusm.gov.tr/CN=KOKSIL.v3,O=KSM,C=TR?certificateRevocationList?base?objectclass=cRLDistributionPoint
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL= http://www.kamusm.gov.tr/BilgiDeposu/KOKSHS.v3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL= ldap://dizin.kamusm.gov.tr/CN=KOKSHS.v3,O=KSM,C=TR?cACertificate?base?objectclass=certificationAuthority

d) SSL Sertifikası

Alan	Değer
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

Sertifikayı Veren	CN = Cihaz Sertifikası Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Web sitesi DNS adı OU = Başvuru sahibinin ait olduğu bölüm adı O = Başvuru sahibi kurum adı L = Başvuru sahibinin bulunduğu ilçe S = Başvuru sahibinin bulunduğu il C = Başvuru sahibinin bulunduğu ülke
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 96 2a 85 76 7f b5 83 17 e0 e1 2e 34 86 0b 4b 3f d8 6e 29 4e
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	Kritik=Evet ; Dijital imza, Anahtar Şifreleme
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.2 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://www.kamusm.gov.tr/BilgiDeposu/KSM_CES_SUE [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika ilkelerini okumak için belirtilen web sitesini ziyaret ediniz.
Gelişmiş Anahtar Kullanımı	Sunucu Kimlik Doğrulaması (1.3.6.1.5.5.7.3.1) İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2)
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://www.kamusm.gov.tr/BilgiDeposu/CSHSIL.v3.crl [2]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=ldap://dizin.kamusm.gov.tr/CN=CSHSIL.v3,OU=KAMUSM,O=SM,O=KSM,C=TR?certificateRevocationList?base?objectclass=cRLDistributionPoint
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://www.kamusm.gov.tr/BilgiDeposu/CSHS.v3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=ldap://dizin.kamusm.gov.tr/CN=CSHS.v3,OU=KAMUSM,O=SM,O=KSM,C=TR?cACertificate?base?objectclass=certificationAuthority

KAMU SM Sİ/SUE (SSL VE S/MIME SERTİFİKASI İÇİNDİR)

e) S/MIME Sertifikası

Alan	Değer
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Başvuru sahibi adı soyadı Seri No = Başvuru sahibi Tckimlik numarası OU = Başvuru sahibi bölüm adı C = Başvuru sahibinin bulunduğu ülke
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; e3 87 c3 ec 1d c4 25 b7 ed f7 92 1b 36 31 da ac d1 b9 cc f2
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	Kritik=Evet ; Dijital imza, Red Olmayan (c0)
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.2 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://www.kamusm.gov.tr/BilgiDeposu/KSM_CES_SUE [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika yalnız bilgi güvenliği için kullanılır, 5070 sayılı Elektronik İmza Kanununda belirtilen nitelikli elektronik sertifika değildir.
Gelişmiş Anahtar Kullanımı	İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2) Güvenli E-posta (1.3.6.1.5.5.7.3.4)
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://www.kamusm.gov.tr/BilgiDeposu/NONES.v3.crl [2]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= ldap://dizin.kamusm.gov.tr/CN=NONES.v3,OU=KAMUSM,O=SM,O=KSM,C=TR?certificateRevocationList?base?objectclass=CRLDistributionPoint
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL= http://www.kamusm.gov.tr/BilgiDeposu/NESHS.v3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2)

**KAMU SM Sİ/SUE
(SSL VE S/MIME SERTİFİKASI İÇİNDİR)**

	<p>Diğer Ad: URL=ldap://dizin.kamusm.gov.tr/CN=NESHS.v3,OU=KAMUSM,O=SM,O=KSM, C=TR?cACertificate?base?objectclass=certificationAuthority [3]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durumu İletişim Kuralı(1.3.6.1.5.5.7.48.1) Diğer Ad: URL=http://ocsp3.kamusm.gov.tr/</p>
Konu Diğer Adı	RFC822 Adı=basvurusahibi e posta adresi