

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

**MOBİL İMZA KULLANIM AMAÇLI NİTELİKLİ ELEKTRONİK SERTİFİKA
UYGULAMA ESASLARI**

Doküman Kodu

YON.01.09

Revizyon No

03

Revizyon Tarihi

10.07.2024

TASNİF DIŐI

REVİZYON GEÇMİŐİ		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
00	İlk yayın [YONG-001-012 kodu ve “Kamu SM Sertifika İlkeleri ve Sertifika Uygulama Esasları (Mobil İmza Kullanım Amaçlı Nitelikli Elektronik Sertifikalar) ismi ile kabul edilmiştir.]	16.08.2011
01	Aynı doküman içerisinde yer alan; Mobil İmza Kullanım amaçlı Sertifika İlkeleri ve Uygulama Esasları iki ayrı doküman olacak şekilde düzenlenerek kodu ve şablonu güncellenmiştir. Doküman genelinde düzenlemeler yapılarak, web sitesi adresleri yeni atkık sertifikasına göre düzenlenmiştir.	28.09.2022
02	Yayın adresleri, SİL yayımlama gecikme süresi, sertifika kullanımının sınırları ve denetim sıklığı yeniden düzenlenmiştir.	14.10.2022
03	Sertifika başvurusunun işleme süresi belirtilmiştir. Sertifikanın askıda kalma süresi başlığındaki ifade güncellenmiştir. Doküman genelinde metinsel düzenlemeler yapılmıştır.	10.07.2024

İÇİNDEKİLER

1. GİRİŐ.....	10
1.1. Genel Bakış	10
1.2. Doküman Adı ve Tanımı	11
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	12
1.4. Sertifika Kullanımı	12
1.4.1. Uygun Olan Sertifika Kullanımı	12
1.4.2. Sertifika Kullanımının Sınırları	12
1.5. Uygulama Esaslarının Yönetimi.....	13
1.5.1. Doküman Yönetimi	13
1.5.2. İletişim Bilgileri	13
1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi.....	13
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri	13
1.6. Tanımlar ve Kısaltmalar	13
1.6.1. Tanımlar	13
1.6.2. Kısaltmalar	15
2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ.....	17
2.1. Bilgi Depoları	17
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması.....	17
2.3. Yayım Sıklığı ve Zamanı	17
2.4. Erişim Kontrolleri	17
3. KİMLİK BELİRLEME VE DOĞRULAMA.....	19
3.1. İsmiendirme.....	19
3.1.1. İsim Alanı Tipleri	19
3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması	19
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması	19
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması	19
3.1.5. Kimlik Bilgilerinin Tekilliği.....	19
3.1.6. Markanın Tanınması, Doğrulanması ve Rolü	19
3.2. İlk Kimlik Belirleme	19
3.2.1. İmza Oluşturma Verisi Sahipliğinin Kanıtlanması	20
3.2.2. Kurumsal Kimliğin Belirlenmesi.....	20
3.2.3. Kişisel Kimliğin Belirlenmesi	20
3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri.....	20
3.2.5. Yetkinin Doğrulanması	21
3.2.6. Uyum Kriterleri	21
3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama	21
3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama	21
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama	21
3.4. Sertifika İptal İsteğinde Kimlik Doğrulama.....	21

4. SERTİFİKA YAŐAM DÖNGÜŐÜ İŐLEVSEL GEREKLİLİLERİ	21
4.1. Sertifika Başvurusu.....	21
4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiđi	21
4.1.2. Kayıt İŐlemleri ve Sorumluluklar	22
4.2. Sertifika Başvurusunun İŐlenmesi	23
4.2.1. Kimlik Tanımlama ve Doğrulama İŐlevlerinin Yerine Getirilmesi	23
4.2.2. Sertifika Başvurusunun Kabul veya Reddi	23
4.2.3. Sertifika Başvurusunun İŐlenme Zamanı	24
4.3. Sertifikanın OluŐturulması	24
4.3.1. Sertifika OluŐturulmasında ESHS'nin İŐlevleri.....	24
4.3.2. Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi	24
4.4. Sertifikanın Kabulü.....	24
4.4.1. Sertifikanın Kabul KoŐulu.....	24
4.4.2. Sertifikanın ESHS Tarafından Yayınlanması	24
4.4.3. Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması	25
4.5. Sertifikanın ve İmza OluŐturma Verisinin Kullanımı	25
4.5.1. Sertifika Sahibinin Sertifika ve İmza OluŐturma Verisini Kullanımı	25
4.5.2. Üçüncü KiŐilerin Sertifika ve İmza Doğrulama Verisini Kullanımı	25
4.6. Sertifika Süresinin Uzatılması	25
4.7. Sertifika Yenileme	25
4.7.1. Sertifikanın Yenileme KoŐulları	25
4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi.....	26
4.7.3. Sertifika Yenileme Başvurusunun İŐlenmesi	26
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi	26
4.7.5. Sertifika Yenileme Sonrası Kabul KoŐulu	26
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması	26
4.7.7. Sertifika Yenilemenin Diđer Tarafra Duyurulması	26
4.8. Sertifikada Bilgi DeđiŐikliđi.....	26
4.9. Sertifikanın İptali ve Askıya Alınması	26
4.9.1. Sertifikanın İptal Edildiđi Durumlar	26
4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir	27
4.9.3. Sertifika İptal Başvurusunun İŐlenmesi	27
4.9.4. İptal İŐteđi Ertelenme Süresi.....	28
4.9.5. İptal İŐteđinin İŐlenme Süresi.....	28
4.9.6. Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol Gerekliliđi.....	28
4.9.7. Sertifika İptal Listesi Yayınlama Sıklıđı	28
4.9.8. Sertifika İptal Listesi Yayınlama Gecikme Süresi	28
4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti.....	29
4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi	29
4.9.11. Diđer Sertifika Durum Bildirim Yöntemleri	29
4.9.12. İmza oluŐturma Verisinin Güvenliđini Yitirmesi Durumu	29
4.9.13. Sertifikanın Askıya Alındıđı Durumlar	29
4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi.....	29
4.9.15. Sertifika Askıya Alma Başvurusunun İŐlenmesi	30
4.9.16. Askıda Kalma Süresi.....	30

4.10.	Sertifika Durum Servisleri.....	30
4.10.1.	İşletimsel Özellikleri.....	30
4.10.2.	Servisin Erişilebilirliği	30
4.10.3.	İsteğe Bağlı Özellikler.....	30
4.11.	Sertifika Sahipliğinin Sona Ermesi.....	31
4.12.	Anahtar Yeniden Üretme	31
5.	YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER.....	32
5.1.	Fiziksel Güvenlik Denetimleri.....	32
5.1.1.	Tesis Yeri ve İnşaatı.....	32
5.1.2.	Fiziksel Erişim	32
5.1.3.	Güç Kaynağı ve Havalandırma	32
5.1.4.	Su Baskınları	33
5.1.5.	Yangın Önleme ve Korunma	33
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması	33
5.1.7.	Atıkların Yok Edilmesi	33
5.1.8.	Farklı Mekanlarda Yedekleme.....	33
5.2.	Prosedürel Kontroller.....	33
5.2.1.	Güvenilir Roller	33
5.2.2.	Her İşlem İçin Gereken Kişi Sayısı	34
5.2.3.	Kimlik Doğrulama ve Yetkilendirme.....	34
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller.....	34
5.3.	Personel Güvenlik Kontrolleri	34
5.3.1.	Kişisel Geçmiş, Deneyim ve Nitelik Gereklere	34
5.3.2.	Geçmiş Araştırması	34
5.3.3.	Eğitim Gereklere	35
5.3.4.	Sürekli Eğitim Gereklere ve Sıklığı	35
5.3.5.	Görev Değişim Sıklığı ve Sırası.....	35
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	35
5.3.7.	Anlaşılabilir Personel Gereksinimleri	35
5.3.8.	Sağlanan Dokümantasyon	35
5.4.	Denetim Kayıtları	35
5.4.1.	Kaydedilen İşlemler	35
5.4.2.	Kayıtların İncelenme Sıklığı	37
5.4.3.	Kayıtların Saklanma Süresi	37
5.4.4.	Kayıtların Korunması	37
5.4.5.	Kayıtların Yedeklenmesi	37
5.4.6.	Kayıtların Toplanması	37
5.4.7.	Kayda Sebep Verilen Tarafın Bilgilendirilmesi.....	37
5.4.8.	Saldırıya Açıklığın Değerlendirilmesi.....	38
5.5.	Kayıt Arşivleme	38
5.5.1.	Arşivlenen Kayıt Bilgileri.....	38
5.5.2.	Arşivlerin Tutulma Süresi.....	38
5.5.3.	Arşivlerin Korunması	38
5.5.4.	Arşivlerin Yedeklenmesi	39
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri.....	39

5.5.6.	Arşivlerin Toplanması	39
5.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu	39
5.6.	Anahtar Değişimi	39
5.7.	Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	39
5.7.1.	Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi	39
5.7.2.	Donanım, Yazılım veya Veri Bozulması	39
5.7.3.	İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi	40
5.7.4.	Arıza Sonrası Yeniden Çalışırılık	40
5.8.	Sertifika Hizmetlerinin Sonlandırılması	40
6.	TEKNİK GÜVENLİK KONTROLLERİ	41
6.1.	Anahtar Çifti Üretimi ve Kurulumu	41
6.1.1.	Anahtar Çifti Üretimi	41
6.1.2.	Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması	41
6.1.3.	Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması	42
6.1.4.	Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması	42
6.1.5.	Anahtar Uzunlukları	42
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü	42
6.1.7.	Anahtar Kullanım Amaçları	42
6.2.	İmza Oluşturma Verisinin Korunması	43
6.2.1.	Kriptografik Modül Standartları	43
6.2.2.	İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim	43
6.2.3.	İmza Oluşturma Verisinin Yeniden Elde Edilmesi	43
6.2.4.	İmza Oluşturma Verisinin Yedeklenmesi	43
6.2.5.	İmza Oluşturma Verisinin Arşivlenmesi	44
6.2.6.	İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi	44
6.2.7.	İmza Oluşturma Verisinin Kriptografik Modülde Saklanması	44
6.2.8.	İmza Oluşturma Verisine Erişim	44
6.2.9.	İmza Oluşturma Verisine Erişimin Kesilmesi	44
6.2.10.	İmza Oluşturma Verisinin Yok Edilmesi	45
6.2.11.	Kriptografik Modülün Değerlendirilmesi	45
6.3.	Anahtar Çifti Yönetimiyle İlgili Diğer Konular	45
6.3.1.	İmza Doğrulama Verisinin Arşivlenmesi	45
6.3.2.	İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri	45
6.4.	Erişim Denetim Verileri	45
6.4.1.	Erişim Denetim Verilerinin Oluşturulması	45
6.4.2.	Erişim Denetim Verilerinin Korunması	46
6.4.3.	Erişim Denetim Verileri İle İlgili Diğer Konular	46
6.5.	Bilgisayar Güvenliği Denetimleri	46
6.5.1.	Bilgisayar Güvenliği İle İlgili Teknik Gereklere	46
6.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi	46
6.6.	Yaşam Döngüsü Teknik Denetimleri	46
6.6.1.	Sistem Geliştirme Denetimleri	46
6.6.2.	Güvenlik Yönetimi Denetimleri	47
6.6.3.	Yaşam Döngüsü Güvenlik Denetimleri	47
6.7.	Ağ Güvenliği Denetimleri	47

6.8. Zaman Damgası.....	47
7. SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ.....	48
7.1. Sertifika Biçimi	48
7.1.1. Sürüm Numarası	48
7.1.2. Sertifika Uzantıları	48
7.1.3. Algoritma ve Nesne Tanımlayıcılar	50
7.1.4. İsim Alanı Biçimleri	50
7.1.5. İsim Kısıtları.....	50
7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası	51
7.1.7. İlke Kısıtları Uzantısının Kullanımı.....	51
7.1.8. İlke Niteleyiciler	51
7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi	52
7.2. Sertifika İptal Listesi Biçimi	52
7.2.1. Sürüm Numarası	52
7.2.2. Sertifika İptal Listesi Uzantıları.....	52
7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi	52
7.3.1. Sürüm Numarası	52
7.3.2. ÇİSDUP Uzantıları.....	52
8. UYGUNLUK DENETİMLERİ.....	54
8.1. Uygunluk Denetiminin Sıklığı	54
8.2. Denetçinin Nitelikleri	54
8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi	54
8.4. Denetimin Kapsamı	54
8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar	54
8.6. Sonucun Bildirilmesi.....	55
9. DİĞER İŐLER VE HUKUKSAL MESELELER	56
9.1. Ücretlendirme.....	56
9.1.1. Sertifika OluŐturma ve Yenileme Ücreti.....	56
9.1.2. Sertifika EriŐim Ücreti	56
9.1.3. İptal Durum Kaydına EriŐim Ücreti	56
9.1.4. Diđer Servis Ücretleri	56
9.1.5. İade Ücreti.....	56
9.2. Finansal Sorumluluk	56
9.2.1. Sigorta Kapsamı	56
9.2.2. Diđer Varlıklar	56
9.2.3. Sertifika Mali Sorumluluk Sigortası.....	57
9.3. Ticari Bilginin Korunması	57
9.3.1. Gizli Bilginin Kapsamı.....	57
9.3.2. Gizlilik Kapsamında Olmayan Bilgiler.....	57
9.3.3. Gizli Bilginin Korunma Sorumluluđu.....	57
9.4. KiŐisel Bilginin Gizliliđi	57
9.4.1. Gizlilik Planı	57
9.4.2. Gizli Olarak Tanımlanan Bilgiler	57
9.4.3. Gizli Olarak Tanımlanmayan Bilgiler	57

9.4.4.	Gizli Bilginin Korunma Sorumluluđu.....	57
9.4.5.	Gizli Bilginin Kullanımına İzin Verilmesi	58
9.4.6.	Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması	58
9.4.7.	Diđer BaŐlıklar	58
9.5.	Telif Hakları.....	58
9.6.	Temsil Hakkı ve Yüklümlüklükler	58
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yüklümlüklükleri	58
9.6.2.	Kayıt Birimi Yüklümlüklükleri	59
9.6.3.	Sertifika Sahibinin Yüklümlüklükleri	60
9.6.4.	Üçüncü KiŐilerin Yüklümlüklükleri.....	61
9.6.5.	Diđer BileŐenlerin Yüklümlüklükleri	61
9.7.	Yüklümlüklüklerden Feragat.....	62
9.8.	Sorumlulukla İlgili Sınırlamalar	62
9.9.	Tazminat Halleri	62
9.10.	AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi.....	63
9.10.1.	AnlaŐma Süresi	63
9.10.2.	AnlaŐmanın Sona Ermesi	63
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri.....	64
9.11.	Sistem BileŐenleri İle HaberleŐme ve KiŐissel Bilgilendirme	64
9.12.	DeđiŐiklik Halleri	64
9.12.1.	DeđiŐiklik Metotları.....	64
9.12.2.	Bilgilendirme Mekanizması ve Sıklıđı	65
9.12.3.	Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar	65
9.13.	AnlaŐmazlık Halleri	65
9.14.	Uygulanacak Hukuk	65
9.15.	Uygulanabilir Yasalarla Uyum.....	65
9.16.	Diđer Hükümler	65
10.	EK-A SERTİFİKA PROFİLLERİ.....	66
10.1.	KAMU SM MOBİL NES KÖK SERTİFİKASI	66
10.2.	KAMU SM MOBİL NES ALT KÖK SERTİFİKASI	67
10.3.	SON KULLANICI MOBİL NES SERTİFİKA ŐABLONU	68

TABLolar

Tablo 1 Mobil NES Uzantıları	48
Tablo 2 Mobil NES İsim Alanı Bilgileri	51

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Mobil imza kullanım amaçlı nitelikli elektronik sertifika (Mobil NES) hizmeti verirken uyguladığı esasları tanımlayan Sertifika Uygulama Esasları (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.

Telekomünikasyon Kurumu tarafından 26 Haziran 2008 tarih ve 26918 sayısı Resmi Gazete'de yayımlanan Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ ile Mobil Elektronik İmza, madde 10/A içerisinde ilgili tebliğe eklenmiştir. Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ Madde 10/A gereğince ESHS'ler, mobil elektronik imza hizmetleri ve dolaşım ile ilgili ETSI TS 102 207 standardına ve nitelikli elektronik sertifika başvurusu, oluşturulması, yayımlanması, yenilenmesi süreçleri ile ilgili olarak ETSI TS 102 204 standardına uyar.

Kamu SM açık anahtar altyapısı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı (Kök SHS) ile buna bağlı olarak çalışan Mobil Elektronik Sertifika Hizmet Sağlayıcısı (Mobil ESHS) bulunur. Kök SHS, sertifika sahipleri için sertifika üretmeyip, yürüttükleri görevler açısından özel niteliği haiz kamu kurum ve kuruluşları ile dileyen gerçek ve tüzel kişilerin kuracakları Elektronik Sertifika Hizmet Sağlayıcılarına kök sertifika hizmeti verir. Mobil ESHS, Kök SHS'nin imzasını taşıyan Elektronik Sertifika Hizmet Sağlayıcısı sertifikasına sahiptir.

Kamu SM'den Mobil İmza Kullanım Amaçlı Nitelikli Elektronik Sertifika (Mobil NES) talebinde bulunan gerçek kişiler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Personeli için Mobil NES talebinde bulunan kurumlar bununla ilgili olarak Kamu SM ile imzaladıkları sözleşmelerde bu dokümana atıfta bulunmaktadır. Mobil NES sahibi kişiler ise Mobil Nitelikli Elektronik Sertifika Sahibi Taahhünamesi'ni imzalayarak bu dokümanda belirtilen esasları kabul ederler.

1.1. Genel Bakış

Bu SUE dokümanı, Mobil ESHS içinde yer alan sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini tanımlar; sertifika başvurusunun ve başvuruya ilişkin gerekli belgelerin alınması, başvuru sahipleri için sertifika oluşturulması, sertifikanın yenilenmesi, askıya alınması, iptal edilmesi, sertifikanın ve sertifika iptal bilgisinin yayımlanması sırasında uygulanan politika ve prosedürleri anlatır.

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.

SUE dokümanın bu versiyonu Kamu SM yönetimi tarafından onaylanmıştır. Kamu SM yönetimi gerekli gördüğü durumlarda doküman üzerinde deęişiklik yapabilir ve onaylanmış olan en güncel sürüm önceki sürümleri yürürlükten kaldırır.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Mobil İmza Kullanım Amaçlı Nitelikli Elektronik Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 03

Yayın Tarihi: 10.07.2024

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.8

Bu doküman, Kamu SM'nin Mobil NES hizmeti verirken uyguladığı esasları tanımlayan SUE dokümanıdır. SUE dokümanı <http://depo.kamasm.gov.tr/ilke/> adresinde kamuya açık olarak kesintisiz yayımlanmaktadır.

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluşturma verisiyle imzalamak olan ESHS'ler, sertifika başvurusunda bulunanların kayıt ve kimlik doğrulama işlemleri ile elektronik sertifika dağıtım, yenileme, iptal etme ve iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Mobil Elektronik Sertifika Hizmet Sağlayıcısı (Mobil ESHS) olarak kamu kurum ve kuruluşlarına Mobil NES hizmeti sağlar.

1.3.2. Kayıt Birimleri

Kayıt birimleri, Mobil NES başvurularını alan ve inceleyerek onaylayan ya da reddeden, sertifika yenileme taleplerini alan ve inceleyerek onaylayan ya da reddeden, bahsi geçen onay ve red kararlarını sertifika sahibine bildiren, yapmış olduğu işlemlere ilişkin düzenli olarak her türlü kayıt ve belgeyi tutarak en az 20 (yirmi) yıl süre ile arşivleyen yetkilendirilmiş birimlerdir. Kayıt birimleri kayıtçı olarak da anılmaktadır. Mobil ESHS'nin kendi bünyesinde ve fiziksel ortamında kayıtçılar bulunmaktadır. Buna ek olarak gerekli gördüğü durumlarda kendi fiziksel ortamı dışında da kayıtçı hizmeti verebilmektedir.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından dağıtılan sertifikanın üzerinde adları bulunan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek kişilerdir.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kimlik bilgileri ve imza doğrulama verisi arasındaki baęın doğruluęuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir.

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Çalışanları adına Kamu SM'ye sertifika başvurusunda bulunan kamu kurum veya kuruluşudur. Kurum ile Kamu SM arasında sertifika hizmetleri ile ilgili sözleşme imzalanır veya Kurumdan taahhütname/sipariş formu alınır. Kurum sözleşmeye/taahhütnameye/sipariş formuna uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur. Kurum ile Kamu SM bu dokümanda adı geçen yerlerdeki işlemleri Kurumsal Taahhütname'ye uygun olarak yerine getirmekten sorumludur.

1.3.5.2. Kurum Yetkilileri

Sertifika başvurusunda bulunan kurumların sertifika alınacak personeli ile ilgili bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan e-imza sorumlusudur. Kurum e-imza sorumlusu Kamu SM E-İmza Sorumlusu Taahhütnamesi'ndeki şartları yerine getirmekten sorumludur.

1.3.5.3. Mobil Hizmet Sağlayıcı

Mobil NES başvurusunda bulunan kişilerin bağlı oldukları GSM operatörüdür. Mobil Hizmet Sağlayıcı, sertifika yönetim sürecinde başvuru ve sertifika sahiplerinin kimlik doğrulamasını yapmaktan, mobil imza için gerekli olan anahtar çiftini başvuru sahibine ait SIM kart içerisinde güvenli bir şekilde üretmekten, başvuru sahibine ait imza doğrulama verisini içeren sertifika isteğini Kamu SM'ye iletmekten ve sertifika sahibinin yenileme, iptal ve askı taleplerine ilişkin kesintisiz hizmet sağlayarak ilgili talepleri anlık olarak Kamu SM'ye iletmekten sorumludur.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

Kamu SM'nin gerçek kişiler adına ürettiği Mobil NES güvenli elektronik imza uygulamalarında kullanılır. Mobil NES sahibi kamu çalışanı, ilgili imza oluşturma verisini kamu kurum ve kuruluşlarının elektronik ortamlarda yürütecekleri iş ve işlemlerinde veya kendi özel işlerinde güvenli elektronik imza oluşturmak amacıyla kullanır. İmza oluşturma verisi kullanılarak oluşturulan güvenli elektronik imzanın, elle atılan imza ile aynı hukuki sonucu doğurabilmesi için, imza oluşturma verisinin güvenli elektronik imza oluşturma aracı içinde saklanması, güvenli elektronik imzanın elektronik imza mevzuatında belirtildiği gibi güvenilir yöntemlerle, güvenli yazılım veya donanım araçları kullanılarak oluşturulması gerekmektedir. Mobil imzada kullanılan güvenli elektronik imza oluşturma aracı SIM karttır.

Mobil NES içeriğindeki imza doğrulama verisi güvenli elektronik imzayı doğrulamak için kullanılır.

1.4.2. Sertifika Kullanımının Sınırları

Mobil NES ve ilgili imza oluşturma verisi, güvenli elektronik imza oluşturma ve doğrulama dışında kullanılamaz. Mobil NES sahibi kişi, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile banka teminat mektupları ve Türkiye'de düzenlenen kefalet senetleri dışındaki teminat sözleşmelerini güvenli elektronik imza ile gerçekleştiremez. Mobil NES'lerin ve ilgili imza oluşturma

verilerinin tanımlı maddi sınırları üzerinde değerde işlem yapmak, elektronik imzalı e-posta göndermek, açık ağlar üzerinde kimlik doğrulaması yapmak, iletilen mesajların bütünlüğünü ve gizliliğini sağlamak gibi amaçlarla kullanımından doğan zararlardan Kamu SM sorumlu tutulamaz.

Kamu SM, vermiş olduğu sertifikaların hangi uygulamalar ve hangi amaçlar doğrultusunda kullanıldığının kontrolünü yapmakla yükümlü değildir.

1.5. Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

SUE dokümanı Kamu SM tarafından hazırlanmıştır. Kamu SM, gerekli gördüğü durumlarda doküman üzerinde değişiklik yapabilir.

1.5.2. İletişim Bilgileri

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

Adres : Kamu Sertifikasyon Merkezi, TÜBİTAK Yerleşkesi, PK. 74, 41470 Gebze-KOCAELİ

Tel. : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

URL : <https://kamusm.bilgem.tubitak.gov.tr/>

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

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

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

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

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

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 diđer sertifika işlemleri ile ilgili bilgilerin yayımlandığı dizin sunucular gibi veri saklama ortamları.

Çevrim İçi Sertifika Durum Protokolü: Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın iptal durumunu öğrenmelerine imkan tanıyan standart iletişim kuralı.

Elektronik Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt. Bu dokümanda bahsi geçen elektronik sertifika ya da sertifika ibaresi mobil nitelikli elektronik sertifikayı ifade etmek amacıyla kullanılmıştır.

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler.

Güvenli Elektronik İmza: Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir deęişiklik yapıp yapılmadığının tespitini sağlayan elektronik imza. Bu dokümanda bahsi geçen elektronik imza ibaresi güvenli elektronik imzayı ifade etmek amacıyla kullanılmıştır.

Güvenli Elektronik İmza Oluşturma Aracı: Sertifika sahibine ait imza oluşturma verisinin içinde bulunduğu akıllı kart ya da benzeri güvenli taşınabilir cihaz. Bu doküman kapsamında güvenli elektronik imza oluşturma aracı sertifika sahibi tarafından kullanılan SIM karttır.

Güvenli Elektronik İmza Oluşturma Aracı Erişim Verisi: Sertifika sahibine ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

İmza Doğrulama Verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler.

İmza Oluşturma Verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik özel anahtarlar gibi veriler.

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

Kimlik Paylaşım Sistemi: İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ile yapılan güvenli bağlantı ile tüm T.C. vatandaşlarına ait nüfus bilgilerinin paylaşıldığı sistem.

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

Kurum E-imza Sorumlusu: Kamu kurumlarının resmi yazı ile Kamu SM'ye bildirdiği ve Mobil nitelikli elektronik sertifika ile ilgili süreçlerde kurumu temsile yetkili kişi.

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

Mobil İmza: Mobil nitelikli elektronik sertifika sahibi tarafından, mobil iletişim cihazları ve ilgili iletişim/hizmet altyapısı kullanılarak oluşturulan güvenli elektronik imza.

Mobil Hizmet Sağlayıcı: Mobil nitelikli elektronik sertifika sahiplerine sahip olduğu GSM altyapısı üzerinden işlem yapma imkanı sağlayan taraf.

Nitelikli Elektronik Sertifika: 5070 sayılı Elektronik İmza Kanunu'nun 9'uncu maddesinde sayılan nitelikleri haiz elektronik sertifika. Bu dokümanda bahsi geçen nitelikli elektronik sertifika, mobil nitelikli elektronik sertifika (Mobil NES) olarak ifade edilmektedir.

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

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

Sertifika Sahibi: Güvenli elektronik imza oluşturmak amacıyla ESHS'den sertifika alan gerçek kişi. Bu dokümanda bahsi geçen sertifika sahibi, mobil nitelikli elektronik sertifika alan gerçek kişiyi ifade etmektedir.

SİM Kart: İlgili mevzuata uygun olan, mobil imza servisleriyle uyumlu çalışabilen güvenli elektronik imza oluşturma aracı niteliğindeki akıllı kart.

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

Son Kullanıcı: ESHS sisteminde kimlik doğrulaması yapılmış ve sertifika almak üzere tanımlanmış veya sertifika almış kişiler.

Telekomünikasyon Kurumu: Günümüzde faaliyetlerine Bilgi Teknolojileri ve İletişim Kurumu (BTK) ismi devam eden kurumdur.

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

BGYS: Bilgi Güvenliği Yönetim Sistemi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

EAL (Evaluation Assurance Level): Deęerlendirme Garanti Düzeyi

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

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

GSM (Global System for Mobile Communication): Mobil İletişim için Küresel Sistem

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

KPS: Kimlik Paylaşım Sistemi

Kamu SM: Kamu Sertifikasyon Merkezi

Mobil NES: Mobil Nitelikli Elektronik Sertifika

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

SIM (Subscriber Identity Module): Abone Kimlik Modülü

Si: Sertifika İlkeleri

SiL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayınlama ve Bilgi Deposu Yükümlülükleri

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 sayfası üzerinden Kamu SM hakkında bilgiler, sertifika yönetimiyle ilgili dokümanlar, teknik bilgilendirme dokümanları, başvuru formları ve duyurular yayımlanır.

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması

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

- Kamu SM'ye ait güncel Kök SHS ve Mobil ESHS sertifikaları,
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Mobil ESHS sertifikaları
- Sertifika sahibi kişilerin talep etmeleri durumunda sertifika sahiplerine ait Mobil NES'ler,
- Kamu SM'ye ait Kök SHS sertifikalarının özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi,
- Kamu SM Sİ ve SUE dokümanları,
- Taahhütnameler,
- Sertifika iptal durum kayıtları.

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ ve SUE dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, 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 deposu, bilgi edinme amaçlı olarak herkesin erişimine açıktır.

Bilgi deposunun güncellenmesi, yetkili personel tarafından yapılmaktadır.

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

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve deęiŐtirilmeye karŐı bütünlüğünü korumak,
- Bilgi deposunda tutulan bilgilerin doęruluęu ve güncellięini saęlamak,
- Bilgi deposunu sürekli olarak katılımcıların erişimine açık tutmak,
- Bilgi deposunun kesintisiz olarak erişilebilirliğini saęlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz saęlamak.

3. Kimlik Belirleme ve Doğrulama

Mobil NES'lerle ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kişi (Kurum e-imza sorumlusu) ve kurumun kimlik tanımlama veya doğrulaması yapılır. Bu bölümde Mobil NES yönetim prosedürleri içinde uygulanan kimlik tanımlama ve doğrulama yöntemleri ile Mobil NES'in içinde yazılan kimlik bilgileri anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Mobil NES'lerde Kamu SM ve 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

Mobil NES içeriğindeki isim alanına yazılan bilgiler kişiyi tanımlayan ve kişinin kimliğinin tespit edilmesini sağlayan niteliktedir; bu sebeple anlamlı olması gerekir. Mobil NES içeriğine konulacak bilgiler; kişiyi teşhis edebilecek kimlik bilgilerinden oluşur.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika sahibine ait Mobil NES içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Mobil NES içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Oluşturulan Mobil NES içeriğindeki kimlik bilgileri her kişi için ayırt edici niteliktedir. Aynı kişiye ait Mobil NES'lerin içeriğindeki kimlik bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kişilere ait Mobil NES'lerin içeriğindeki kimlik bilgilerinin aynı olması engellenmektedir. Bunun sağlanabilmesi için Mobil NES'lerin isim alanı içinde benzersiz bir sayı olduğu kabul edilen, sertifika sahibinin T.C. kimlik numarası yer alır. T.C. kimlik numarası bulunmayan yabancı uyruklu sertifika sahipleri için isim alanı içinde pasaport numarası veya yabancı kimlik numarası yer alır.

3.1.6. Markanın Tanınması, Doğrulaması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM'ye Mobil NES hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kişi ve kurumun kimliklerinin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. İmza OluŐturma Verisi SahipliĐinin Kanıtlanması

Sertifika sahibinin imza oluŐturma ve doĐrulama verileri, baŐvuru s¼recinin baŐarıyla sonuŐlanması halinde kendisine ait SIM kart iŐerisinde mobil hizmet saĐlayıcı tarafından oluŐturulur. Anahtar çiftinin oluŐturulmasının ardından Kamu SM'ye sertifika isteĐi g¼nderilir. Sertifika isteĐi, imza oluŐturma verisi ile imzalanmalıdır. Sertifika isteĐini alan Kamu SM, istek iŐerisinde yer alan imza doĐrulama verisini kullanarak imzayı matematiksel olarak doĐrular. Bu sayede, sertifika sahibinin imza oluŐturma ve doĐrulama verisine sahip olduĐu kanıtlanır.

3.2.2. Kurumsal KimliĐin Belirlenmesi

ÇalıŐanları adına Mobil NES baŐvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini kurumu temsile yetkili kiŐilerin imzaladıĐı ve kurumun onayını taŐıyan resmi yazıyla/taahh¼nameyle Kamu SM'ye bildirir. Kamu SM resmi yazıya istinaden kurum kimliĐini belirler. Resmi yazıda Kamu SM sertifika iŐlemlerini kurum adına y¼r¼tecek Kurum e-imza sorumlusu da belirlenerek Kamu SM'ye iletilir. Kurum e-imza sorumlusunun Kamu SM'ye g¼nderdiĐi elektronik imzalı belgeler de kurum kimliĐinin belirlenmesi iŐin kabul g¼r¼r. Belge ¼zerindeki Kurum e-imza sorumlusuna ait elektronik imzanın doĐrulanması yoluyla kurum e-imza sorumlusunun temsil ettiĐi kurum kimliĐi belirlenir.

3.2.3. KiŐisel KimliĐin Belirlenmesi

Mobil NES baŐvurusunda bulunan kurumlar, Mobil NES almak istediĐi çalıŐanlarına ait bilgileri, kurumun onayını taŐıyan resmi yazıyla ya da kurum e-imza sorumlusunun elektronik olarak imzaladıĐı form ile Kamu SM'ye bildirir. Resmi yazının ekinde Mobil NES alınacak kiŐilerin listesini Kamu SM'ye iletir. KiŐilere ait kimlik bilgileri Kimlik PaylaŐım Sistemi ile kurumsal baŐvuru belgesine dayanılarak belirlenir.

3.2.4. DoĐrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi veya kurum tarafından baŐvuru sırasında ve daha sonra deĐiŐiklik sebebiyle beyan edilen aŐaĐıdaki eriŐim bilgileri ve diĐer bilgilerin doĐruluĐu Kamu SM tarafından kontrol edilmez.

- Telefon numaraları
- Faks numaraları
- Sertifika sahibinin elektronik posta adresi
- Sertifika sahibinin unvanı veya g¼revi ile ilgili bilgiler
- Sertifika sahibinin çalıŐtıĐı kurum ile ilgili bilgiler
- Sertifika sahibinin çalıŐtıĐı birim ile ilgili bilgiler

Bu bilgilerin doĐruluĐu sertifika sahibinin veya kurumun beyanı ¼zerine kabul edilir.

Kurum ve sertifika sahibi bu bilgileri Kamu SM'ye doĐru beyan etmekle y¼k¼ml¼d¼r. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doĐabilecek zararlardan, sertifika y¼netim s¼recinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin Doğrulanması

Sertifika içeriğine sertifika sahibinin yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2’de belirtildiği gibi yapılır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2’de belirtildiği gibi yapılır.

Kamu SM olağan sertifika yenileme isteklerinde 3.2’de belirtildiği şekilde kimlik doğrulaması yapar.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2’de belirtildiği gibi yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sahibi, sertifika iptal talebini mobil hizmet sağlayıcıya ileterek gerçekleştirebilir. İptal isteğine ilişkin gerekli kontroller ve kimlik doğrulama adımları mobil hizmet sağlayıcı tarafından gerçekleştirilir.

Kamu SM, mobil hizmet sağlayıcı tarafından kendisine web servis aracılığıyla bildirilen iptalleri derhal işleme alır ve sertifika iptalini gerçekleştirir.

4. Sertifika Yaşam Döngüsü İşlevsel Gereklilikleri

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 askıya alma ve askıdan indirme
- Sertifika iptal etme

Süreçler mobil hizmet sağlayıcı, sertifika sahipleri, kamu kurumları ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

Mobil NES başvurusu, kamu kurum veya kuruluşları tarafından Kamu SM’ye kurumsal olarak yapılır. Kurum çalışanı kurumun talebi olmadan bireysel olarak Mobil NES başvurusunda bulunamaz.

Kurumsal başvuru süreci 3.2.2. Kurumsal Kimliğin Belirlenmesi başlığında anlatıldığı şekilde başlatılır. Kurumun, sertifika başvuru işlemlerini kurum adına yürütecek bir veya daha fazla sayıda kurum e-imza sorumlusu görevlendirmesi ve kurum yetkililerini Kamu SM'ye resmi yazı ile bildirmesi zorunludur.

Kurum veya kurum adına kurum yetkilileri, başvuru sırasında Mobil NES almak istediği çalışanlarının temel başvuru bilgilerini Kamu SM'ye bildirir. Bildirimler resmi yazı ile veya kurum e-imza sorumlusunun elektronik imzasını taşıyan formun Kamu SM'ye elektronik ortamdan gönderilmesi ile yapılır. Kurum, çalışanın haberi olmadan çalışana adına sertifika başvurusunda bulunamaz. Kurum çalışanın durumdan haberdar olması ve Mobil NES almayı kendisinin de talep etmesi gerekir. Başvurunun işleme alınması, kurum çalışana tarafından doldurulup imzalanan;

- Basılı formlar için ıslak imzalı
- Elektronik formlar için e-imzalı/e-onaylı

sertifika başvuru formunun Kamu SM'ye iletilmesi ile yapılır.

Mobil NES başvuru formu kurum çalışana tarafından internet üzerinden doldurulur. Başvuru formunun başvuru sahibi olan kurum çalışana tarafından ıslak imzalı veya elektronik imzalı/elektronik onaylı olması zorunludur.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Mobil NES başvurusu, sertifika sahipleri adına sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurum, Kamu SM'den alacağı sertifika hizmetlerinin şartlarını TÜBİTAK BİLGEM ile karşılıklı imzalanan sözleşmelerle veya Kurum tarafından onaylanan taahhütnamelerle ve Kamu SM'nin internet üzerinden yayımladığı ilgili yönergeler ile Sİ ve SUE dokümanları doğrultusunda belirler.

Kurum Mobil NES almak istediği personelinin listesini, personelin kimliklerinin belirlenmesi için istenen bilgilerle birlikte Kamu SM'ye gönderir. Başvurunun işleme alınabilmesi için sertifika alacak olan çalışanların kişisel bilgileri ile adres, GSM numarası, operatör adı gibi erişim bilgilerinin bulunduğu başvuru formunu doldurup imzalamaları gerekir. Başvuru formları kurum, kişi veya kurum e-imza sorumlusu tarafından Kamu SM'ye iletilir. Bilgi ve belgelerin gizliliğinin sağlanması için belgelerin kapalı zarf içinde Kamu SM'ye iletilmesi gerekmektedir. Belgeler Kamu SM'ye ulaşana kadar ilgili belgelerin gizliliğinin sağlanmasından kurum sorumludur.

Kurum veya kurum yetkilileri ve Mobil NES alacak olan kurum çalışana başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kamu SM, sertifika içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Sertifika başvurusunda bulunan kişi başvuru sırasında, Mobil NES'inin herkesin erişimine açık dizin sunuculardan yayımlanıp yayımlanmayacağı konusundaki talebini Kamu SM'ye iletir. Mobil NES başvurusunun nasıl yapılacağı ve hangi evrakların hazırlanacağına ilişkin ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kamu SM, Mobil NES verilecek kişilerin kimlik belirlemelerini yaptıktan sonra başvuruları değerlendirmeye alır ve uygun görülen başvuruları onaylayarak işleme koyar.

Mobil NES başvurusunda mobil hizmet sağlayıcının zorunlu kıldığı prosedürlere ilişkin gerekli bilgilendirmenin yapılması, prosedürlerin yerine getirilmesi ve takibi başvuru sahibi ve mobil hizmet sağlayıcının sorumluluğundadır.

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. Mobil NES başvurusunda bulunan kurumlar aşağıdaki bilgi ve belgeleri Kamu SM'ye gönderir:

- Mobil NES alacak çalışanların, T.C. kimlik no, (yabancı uyruklular için pasaport no veya yabancı kimlik no) ad, soyadı, kurumsal e-posta adresi, kurum birimi, sertifika üretim nedeni ve sertifika süresi bilgisinin bulunduğu liste,
- Pasaport numarası ile işlem yapılan yabancı uyruklu kişiler için pasaport sureti,

Kurumdan gönderilen belgeler üzerinde kimlik tanımlama işlemleri için aşağıdaki kontroller yapılır:

- Kurumdan gelen yazının ve formların e-imza sorumlusu/sorumluları tarafından gönderildiği kontrol edilir ve formların imzalı olup olmadığına bakılır.
- Kurum tarafından gönderilen Mobil NES alacak çalışanlar listesindeki T.C. kimlik no (yabancı uyruklular için pasaport no veya yabancı kimlik no), ad, soyadı, kurumsal e-posta adresi, kurum birimi, sertifika üretim nedeni ve sertifika süresi bilgisinin eksik olup olmadığına ve bu bilgilerin doğruluğuna bakılır.
- Mobil NES'te kullanılacak bilgilerin doğruluğu, KPS kullanılarak tespit edilir. Pasaportla işlem yapılacak yabancı uyruklu başvuru sahipleri için pasaport suretleri kontrol edilir.
- Bilgi ve belgeler hatasız ve tam ise kimlik tanımlama ve doğrulama işlevi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik onay ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kimlik tanımlama ve doğrulama yapılamaz.

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, kurum e-imza sorumlusu ve/veya başvuru sahibi kişiye yapılır ve gerekli görülen bilgi ve belgeler tekrar talep edilir. Yazılı bilgilendirme, kuruma resmi yazı gönderme veya Kurum e-imza sorumlusuna ve/veya başvuru sahibine e-posta gönderme yoluyla yapılır. Sözlü bilgilendirme kurum e-imza sorumlusuna ve/veya başvuru sahibine telefon açılarak yapılır. Sözlü bildirimler kayıt altına alınır. Kurum e-imza sorumlusu ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Geçerli bulunan başvurular için sertifikalandırma süreci başlar.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin Kamu SM'ye ulaşmasının ardından en fazla 5 (beş) iş günü içerisinde sertifika başvurusu işleme alınır. Başvurunun Kamu SM tarafından işleme alınmasını takiben mobil imza aboneliği ve sertifika üretim süreci mobil hizmet sağlayıcının süreçlerine bağlı olduğundan sertifikanın üretilmesi için gerekli süre değişkenlik göstermektedir.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Mobil NES, başvuru sahibinin SIM kartında oluşturularak Kamu SM'ye iletilmiş olan imza doğrulama verisi ve sistemde onayı verilmiş kimlik bilgilerinin Kamu SM'ye ait imza oluşturma verisi ile imzalanması suretiyle üretilir.

Nitelikli elektronik sertifikalar; ETSI TS 101 862, ITU-T X.509 v.3 standartlarına ve 5070 Sayılı Elektronik İmza Kanunu'nun 9'uncu maddesinde belirtilen niteliklere uygun olarak üretilir.

Kamu SM verdiği hizmetler kapsamında BTK tarafından 2007/DK-77/207 sayılı Kurul Kararı ile yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Profilleri" dokümanına uyar.

Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi https://kamusm.bilgem.tubitak.gov.tr/depo/yukumlulukler_tahhutnameler_sozlesmeler adresinden yayımlanır.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Anahtar çiftlerinin başvuru sahibinin akıllı SIM kartında mobil hizmet sağlayıcı tarafından üretilmesini müteakip Kamu SM'ye sertifika talebi gönderilir. Kamu SM, sertifika üretimini gerçekleştirir ve ürettiği sertifikayı mobil hizmet sağlayıcıya iletir. Mobil hizmet sağlayıcı, sertifika sahibine sertifika üretiminin tamamlandığına ilişkin gerekli bilgilendirmeyi SMS ya da e-posta yoluyla yapar.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Sertifika sahibi, kullanmaya başlamadan önce sertifikanın içeriğini kontrol eder ve doğrular. Sertifikanın kendisine ait olmaması, sertifika içerisindeki bilgilerde eksik veya hata olması durumunda Kamu SM'yi bilgilendirir.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM, sertifika sahibinin başvuru esnasında onay vermesi durumunda, ürettiği sertifikaları herkesin erişimine açık dizin ya da web servisi üzerinden yayımlar.

Sertifika sahibi başvuru sırasında Mobil NES'inin üçüncü kişilerin ulaşabileceği ortamlarda yayımlanması için Kamu SM'ye bildirimde bulunabilir. Kamu SM, sertifika sahibinin bu talebi doğrultusunda Mobil NES'i yayımlar.

4.4.3. Sertifikanın Oluřturulmasının Diđer Tarafllara Duyurulması

Sertifikanın oluřturulması; kurumun talep etmesi durumunda, ESHS tarafından internetten eriřimi sađlanan raporlar ya da e-posta yolu ile kurum e-imza sorumlusuna bildirilir.

4.5. Sertifikanın ve İmza Oluřturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluřturma Verisini Kullanımı

Mobil NES sahibi, imza oluřturma verisini elektronik imza mevzuatında belirtildiđi řekilde güvenli elektronik imza uygulamalarında kullanır. Güvenli elektronik imza oluřturma verisinin, güvenli elektronik imza oluřturma aracı iinde bulunması zorunludur. Güvenli elektronik imza oluřturma aracının Bölüm 6.2.1’de belirtilen güvenlik standartlarını sađlaması gerekmektedir.

Mobil NES’lerle ilgili imza oluřturma verilerinin güvenli elektronik imza oluřturma amacı dıřında kullanımlarından dođan zararlardan Kamu SM sorumlu tutulamaz.

İptal olmuř veya geerlilik süresi dolmuř Mobil NES’lere ait imza oluřturma verileri ile iřlem yapılamaz.

4.5.2. Üüncü Kiřilerin Sertifika ve İmza Dođrulama Verisini Kullanımı

Sertifika sahibine ait Mobil NES’lerin iinde yer alan imza dođrulama verileri, üüncü kiřilerce elektronik imzalı verilerin imzasının dođgulanması amacıyla kullanılır. İmza dođrulama verisinin veya sertifikanın, güvenli elektronik imza dođrulaması dıřında kullanılması sonucu oluřabilecek zararlardan, üüncü kiřiler sorumludur.

4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, kullanım süresi dolan sertifikalarda, sertifikada yer alan bilgiler deđiřmeden aynı anahtar çifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. Kamu SM bu iřlemi gerekleřtirmez.

4.7. Sertifika Yenileme

Sertifika yenileme, yeni bir anahtar çifti kullanılarak farklı bir seri numarasına sahip yeni bir sertifika oluřturulması anlamına gelmektedir.

Sertifika yenileme iřlemleri Bölüm 4.1’de anlatılan ilk sertifika bařvuru iřlemleri ile aynıdır. Ancak yenilemede kamu kurumunun Kamu SM’ye resmi yazı yazarak yeniden sertifika talebinde bulunmasına gerek yoktur. Yenilenecek sertifika bilgileri resmi yazıyla Kamu SM’ye bildirilebileceđi gibi, kurum e-imza sorumlusunun elektronik imzasını taşıyan yenileme yapılacak sertifika bilgilerinin bulunduđu formun Kamu SM’ye elektronik ortamdan gönderilmesi ile de yenileme bařvurusu yapılabilir.

4.7.1. Sertifikanın Yenileme Kořulları

Sertifika yenileme iřlemi:

- Güvenli elektronik imza oluřturma aracının kayıp edilmesi, veya alınması durumunda,
- Güvenli elektronik imza oluřturma aracının arızalanması durumunda,

- Güvenli elektronik imza oluŐturma aracı eriŐim verisinin kayıp edilmesi veya çalınması durumunda,
- Elektronik sertifikanın iptal edilmesi ve yenisinin talep edilmesi durumunda,
- Elektronik sertifikanın geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaŐılması durumunda,
- Elektronik sertifikada bilgi deęiŐiklięi gerekmesi durumunda yapılmaktadır.

4.7.2. Sertifika Yenileme BaŐvurusunu Kimlerin Yapabildięi

Bölüm 4.1.1’de tanımlanmaktadır.

4.7.3. Sertifika Yenileme BaŐvurusunun İŐlenmesi

Bölüm 4.2’de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2’de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul KoŐulu

Bölüm 4.4.1’de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması

Bölüm 4.4.2’de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Dięer Taraflara Duyurulması

Bölüm 4.4.3’te tanımlanmaktadır.

4.8. Sertifikada Bilgi DeęiŐiklięi

Sertifikada bilgi deęiŐiklięi, anahtar çifti hariç sertifikada yer alan bilgilerin deęiŐmesi olarak tanımlanmaktadır.

Sertifika içerięinde yer alan bilgiler; Ad, Soyadı, T.C. Kimlik No, varsa sertifikaya ait imza oluŐturma verisinin kullanılacaęı güvenli elektronik imza uygulamasına getirilen kısıt ile ilgili bilgiler ve sertifika içerięinde yazan dięer bilgilerdir.

Kamu SM, sertifikada bilgi deęiŐiklięi gerçekteŐtmez. Bilgi deęiŐiklięi gerekli olduęu durumlarda, anahtarlar yenilenerek sertifika yeni bilgilerle üretir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildięi Durumlar

Sertifikanın, kullanım süresi dolmadan geçerlilięini yitirdięi durumlarda sertifika iptal edilir. İptal edilen sertifikaya iliŐkin imza oluŐturma verisi ile bir daha iŐlem yapılmaz. Sertifika, aŐaęıda belirtilen durumlarda iptal edilir:

- Sertifika sahibinin talebi,
- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,
- Sertifika sahibinin fiil ehliyetinin sınırlandırıldığı, iflasının veya gaipliğinin ya da ölümünün öğrenilmesi,
- Sertifika sahibinin kurum ile ilişkisinin kesilmesinin bildirilmesi,
- İmza oluşturma verisinin güvenliğinin kaybedildiğinden şüphelenilmesi,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya bozulması,
- Güvenli elektronik imza oluşturma aracı erişim verisinin unutulması veya kayıp edilmesi,
- Sertifikanın Mobil Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, Kurum ile imzalanan sözleşmeler, Sİ veya SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Sertifikanın hatalı üretilmesi,
- Kamu SM'nin Mobil NES'i imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması,
- Kamu SM'nin işleyişine son verilmesi ve verilen Mobil NES'lerin yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir:

- Sertifika sahibinin kendisi,
- Kurum,
- Mobil Hizmet Sağlayıcı,
- Kamu SM, Bölüm 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Mobil NES iptal başvurusu, mobil hizmet sağlayıcının sunmuş olduğu yöntemler ile gerçekleştirilebilir. İptal başvurusunu alan mobil hizmet sağlayıcı, iptal başvurusu yapan sertifika sahibi için kimlik doğrulamasını yapar. Kimlik doğrulaması yapılamayan iptal başvuruları işleme alınmaz.

Doğrulama adımlarının başarılı bir şekilde tamamlanmasının ardından iptal başvurusu yapılan sertifika ile ilgili bilgiler mobil hizmet sağlayıcı tarafından güvenli bir şekilde Kamu SM'ye iletilir ve iptal işlemi Kamu SM tarafından gerçekleştirilir. Geçmişe yönelik olarak Mobil NES iptal edilmez.

Mobil NES iptal edildikten sonra, mobil hizmet sağlayıcı sertifika sahibini Mobil NES'in iptal edildiğine dair bilgilendirir.

Kurum, çalışanlarına ait sertifikaları gerekli gördüğünde iptal ettirebilir. Kurum iptal edilmesini istediği sertifika bilgilerini Kamu SM'ye resmi yazı ile bildirerek ya da kurumun yetkilendirdiği kurum e-imza sorumlusunun imzalı liste göndermesi ile iptal talebinde bulunabilir. İptal talebinin Kamu SM'ye

ulaşmasının ardından sertifika/sertifikalar iptal edilir. Sertifika sahibi ve kurum e-imza sorumlusu e-posta veya telefon ile sertifiakanın iptal edildiğine dair bilgilendirilir.

Kamu SM iptal bilgilerini en kısa zamanda işler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları asgari Mobil NES'in seri numarası ile Kamu SM'nin elektronik imzasını taşır. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da Mobil NES'in durumunu iptal konumuna getirmek suretiyle duyurur.

SİL dosyası, Kamu SM'ye ait imza oluşturma verisi ile imzalanır. İptal edilen Mobil NES'ler geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra Mobil NES SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı'da geçerlilik süresi dolan iptal edilmiş Mobil NES'lerin durumu iptal edilmiş konumda görünmeye devam eder.

Mobil NES iptal edildikten sonra yeniden Mobil NES talebinde bulunulabilir.

4.9.4. İptal İsteği Erteleme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Mobil hizmet sağlayıcı aracılığıyla gelen Mobil NES iptal talepleri Kamu SM'ye ulaştığı an işleme alınır. Kamu SM; iptal edilen Mobil NES bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan ise derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 4.9.7'de belirtilmiştir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, dileyen herkes kimlik doğrulaması yapılmaksızın erişebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

Üçüncü kişiler Mobil NES'lere dayanarak işlem yapmadan önce Mobil NES'lerin geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür. Üçüncü kişiler Mobil NES 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 Yayımlama Sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 72 (yetmiş iki) saattir. Ancak bu sürenin dolması beklenmeden her 4 (dört) saatte bir SİL tekrar yayımlanır. Gün içinde yeni bir Mobil NES iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

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

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, Mobil NES'lerin iptal durum bilgisini ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü) üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

ÇİSDUP desteği olan uygulamalar Mobil NES'in geçerlilik durum kontrolünü ESHS Erişim Bilgisi (Authority Information Access) isimli sertifika uzantısında yer alan adres üzerinden gerçekleştirir.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

SİL dosyası, iptal edilen her nitelikli elektronik 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 sisteme getireceği yüke karşılık ÇİSDUP, ilgili nitelikli elektronik sertifikanın iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle anlık olarak iletilmesine olanak tanımaktadır. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları önerilir.

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 Mobil NES iptal edilir. Mobil NES'in iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Mobil NES'in geçici bir süre için iptal durumunda olup sürenin sonunda yeniden kullanılabilir olmasını sağlamak amacıyla askıya alma işlemi tanımlanmıştır. Askıya alınmış bir sertifika askıda olduğu süre boyunca iptal olmuş bir sertifika olarak değerlendirilir. Ancak askıdan indirildiğinde, yeniden geçerli bir sertifika olarak kullanılır.

Sertifika sahibi, aşağıda belirtilenlere benzer sebeplerden dolayı Mobil NES'ini askıya almak isteyebilir:

- Sertifika sahibinin bir süreliğine görev başında olmaması ve Mobil NES'ini kullanım dışı bırakmak istemesi,
- Mobil NES'in iptal olmasını gerektirecek bir durumun ortaya çıktığından şüphelenmesi halinde yanlışlıkla iptalini engellemek amacıyla, Mobil NES'i önce askıya almak istemesi.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Mobil NES askıya alma başvurusu sadece sertifika sahibi tarafından yapılır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Sertifika sahibi, askı talebini mobil operatör çağrı merkezi üzerinden sesli olarak, kağıt üzerinde ıslak imzalı form ile yazılı olarak ya da mobil hizmet sağlayıcının sunmuş olduğu diğer yöntemler ile gerçekleştirebilir. Kimlik doğrulama adımlarının başarılı bir şekilde tamamlanmasından ardından askı başvurusu yapılan sertifika ile ilgili bilgiler mobil operatör tarafından Kamu SM'ye iletilir ve askı işlemi Kamu SM tarafından gerçekleştirilir. Kimlik doğrulaması yapılamayan askı başvuruları işleme alınmaz.

Askıya alınan Mobil NES için, SİL'de geçici olarak iptal edildiğini belirten tanımlı sebep kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Mobil hizmet sağlayıcı ve Kamu SM, Mobil NES askıya alındıktan sonra, gerekli gördüğü durumlarda sertifika sahibini ve bağlı bulunduğu kurum tarafından yetkilendirilen kişiyi sertifikanın askıya alındığına dair bilgilendirir.

4.9.16. Askıda Kalma Süresi

Böyle bir süre öngörülmemiştir.

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. Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi Bölüm 7.1.2'de verilmiştir. Üçüncü kişiler sertifika veya sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP İstemci tarafından ÇİSDUP Yanıtlayıcı'ya sertifika veya sertifikaları tanımlayan bilgileri gönderir ve ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin Erişilebilirliği

SİL ve ÇİSDUP servislerinin verildiği sistemlere erişim, Kamu SM tarafından kesintisiz olarak sağlanır ve hizmetin devamlılığının sağlanması için gereken tüm tedbirler alınır.

Ancak buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurmaları önerilir. 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

Mobil NES'in kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM Mobil NES'in 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 bilgilendirmek zorunda değildir; sertifika sahibi Mobil NES'inin kullanım süresinin dolduđu zamanı kendisi takip etmekle yükümlüdür.

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmaz.

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'ye ait sistemlerin kurulu olduğu cihazlara yetkisiz kişilerce erişim engellenir; hırsızlık, kaybolma gibi tehlikelere karşı gerekli önlemler alınır. 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'ye ait yazılım ve donanım modüllerinin bulunduğu binalar, konum olarak güvenli, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgededir.

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.

Bina içerisinde yazılım ve donanım modüllerinin yerleştirildiği odalar kilitli ve giriş kontrolü olan odalardır.

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.

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

Sistem Operatörleri: Tüm sistem bileşenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

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

Sertifika Kayıt Sorumlusu: Sertifika üretim başvurusunun alınması, başvuru evraklarının ve kurum kimliğinin doğrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimi ve iptalinden sorumlu personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Mobil ESHS'ye ait sertifika üretilmesi ve iptal edilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, Kök SHS ve Mobil ESHS'ye ait imza oluşturma verilerinin başka bir kriptografik modül içerisine 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 yapılabilmektedir.

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

- Sertifika Üretim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında,
- Sistem Denetçisi ile diğer roller arasında,
- Sistem Yöneticisi ile Güvenlik Personeli ve Sistem Denetçisi arasında,

görevler ayrılığı vardır.

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

Kamu SM'nin istihdam ettirdiği personel, taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya 6 (altı) aydan fazla hapis ya da basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş kişilerden oluşur. Bu şartların sağlanması için personeli işe almadan önce Kamu SM gerekli güvenlik soruşturmasını yapar. İşe başlayan personelin bilgi güvenliği farkındalık eğitimleri tamamlanmadan, sistemlere erişimine izin verilmez.

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 işleyiői, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır.

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

5.3.4. Sürekli Eğitim Gereklere ve Sıklıđı

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

5.3.5. Görev Deđişim Sıklıđı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

5.3.7. Anlaşmalı Personel Gereksinimleri

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

5.3.8. Sağlanan Dokümantasyon

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

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

Kamu SM sisteminde aőađıda yapılan işlemler ile ilgili elektronik veya kađıt ortamda yapılan işlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
- Anahtar üretimi
- Anahtar yedekleme

- Anahtar dağıtımı
- Anahtar saklama
- Anahtar arşivleme
- Anahtar yok etme
- Kriptografik modül yaşam döngüsü işlemleri
- Mobil NES üretim, yenileme, askıya alma 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
- Mobil nitelikli elektronik sertifika yaşam döngüsü yönetimi işlemleri
- Mobil nitelikli elektronik sertifika başvurusunun işlenmesi
- Mobil nitelikli elektronik sertifika üretimi
- Mobil nitelikli elektronik sertifika yenileme
- Mobil nitelikli elektronik sertifika askıya alma
- Mobil nitelikli elektronik sertifika askıdan indirme
- Mobil nitelikli elektronik sertifika iptal etme
- Mobil nitelikli elektronik sertifika yayımlanması
- SİL yayımlanması
- ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtları
- 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 işleyiŐiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı olup olmadığı kontrol edilir. Buna ek olarak, sistemde olağandışı hareketlerin görülmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görülen ve başlatılan işlemler de belgelenir.

Mobil NES 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, sistemin veri depolama kapasitesine göre, sistemde erişilebilir olarak tutulur. Kayıtlar incelenmelerinden sonra en az 2 (iki) ay sistemde tutulur. Ancak, yasalar gereğince daha uzun süre saklanması gereken kayıtlar bu süre sonunda arşivlenir. Arşivlenen kayıtlar ile ilgili bilgilendirme Bölüm 5.5'te yapılmıştır.

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 bulunur.
- Kayıtların değiştirilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınmıştır.
- Elektronik olarak saklanan ve sistemin işleyiŐi 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 kritikliğı göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeğı 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 giriŐi 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 Deęerlendirilmesi

Denetim kayıtlarının tutulduęu sistemler için Bölüm 6.5, 6.6 ve 6.7’de sözü geen teknik güvenlik kontrolleri uygulanır.

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sahibi veya baęlı bulunduęu kurum tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Mobil NES yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Mobil NES işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm Mobil NES’ler
- Geçerlilik süresi dolan tüm Kamu SM Kök SHS ve Mobil ESHS sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Zaman Damgası İlkeleri
- Zaman Damgası Uygulama Esasları
- Mobil NES yönetim prosedürleri
- Kurumlarla yapılan sözleşmeler
- Kurumsal Taahhütname
- Mobil NES Sahibi Taahhütnameleri
- Kamu SM Taahhütnameleri
- Sertifika sahipleri ile yapılan sözleşmeler

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler Elektronik İmza Kanunu’nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Yönetmelik uyarınca en az 20 (yirmi) yıl boyunca saklanır.

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler, izinsiz izlenmeyi, deęiŐtirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz alıŐanların erişimine kapalıdır. Arşivlerin tutulduęu ortam Bölüm 5.5.2’de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seęilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM İş 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. Yasal gereksinimlerin ortaya çıkması ya da BTK tarafından denetim amacıyla talep edilmesi durumunda yetkili personel eşliğinde arşiv bilgileri elde edilebilir.

5.6. Anahtar Değişimi

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

- Sertifika kullanım süresinin dolmasından en az 3 (üç) yıl önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış Mobil NES'lerin doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.

SİL dosyaları aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş Mobil NES'lerin kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalanmaya devam eder. Yeni üretilen Mobil NES'ler için oluşturulan yeni SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.

Kamu SM, anahtarlarının yenilendiği bilgisini <https://kamusm.bilgem.tubitak.gov.tr> internet adresi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

5.7. Güvenliğin Yitilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

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.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin Mobil NES 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 <https://kamusm.bilgem.tubitak.gov.tr> internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, Mobil NES sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluşturulan Mobil NES'lere güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Mobil NES'lerin gerekli görünen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Mobil NES 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 Mobil NES'lerin sertifika sahibinden gelen talep doğrultusunda sertifika yenileme süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalışırlık

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 çalışırlığı sağlayacak Kamu SM İş Sürekliliği Planı'nı periyodik olarak gözden geçirir ve test eder.

5.8. Sertifika Hizmetlerinin Sonlandırılması

ESHS'nin işleyişine, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verilebilir. Bu durumda yapılacaklar [Kamu SM Hizmetleri Sonlandırma Planı](#) dokümanında tanımlanmıştır.

6. Teknik Güvenlik Kontrolleri

Kamu SM'nin kendisi ve sertifika sahipleri adına, anahtar çiftleri ve erişim verilerini ürettiği, sertifika yönetim işlemlerini gerçekleştirdiği sistemler CWA 14167-1, ETSI TS 101 456 ve ISO/IEC 27001 gereklerini sağlar.

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1. Kök SHS, Mobil ESHS, ÇİSDUP Yanıtlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aşağıdaki imza oluşturma ve doğrulama verileri oluşturulur:

- Kök SHS'ye ait imza oluşturma ve doğrulama verisi
- Mobil ESHS'ye ait imza oluşturma ve doğrulama verisi
- ÇİSDUP Yanıtlayıcı'ya ait imza oluşturma ve doğrulama verisi

Kök SHS, Mobil ESHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, güvenli yazılım ve/veya donanım 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 Çifti Üretimi

Mobil NES için anahtar çifti üretimi başvuru sahibinin SIM kartında gerçekleştirilir. Anahtar çifti üretim süreci mobil hizmet sağlayıcı tarafından yürütülür. Kullanılan SIM kartların gerekli güvenlik seviyesine ve EAL 4+ sertifikasına sahip olması mobil hizmet sağlayıcının kontrolü ve sorumluluğundadır. Sertifika sahibine ait anahtar çiftlerinin üretiminde Kamu SM'nin herhangi bir dahli yoktur.

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Mobil NES için anahtar çifti üretimi başvuru sahibinin SIM kartında gerçekleştiği için sertifika sahibi imza oluşturma verisine anahtar üretimi gerçekleştiği anda sahip olur.

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

Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi https://kamusm.bilgem.tubitak.gov.tr/depo/yukumlulukler_taahtutnameler_sozlesmeler adresinden yayımlanır.

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

Başvuru sahibinin SIM kartı üzerinde üretilen imza doğrulama verisi sertifika üretimi için mobil hizmet sağlayıcı altyapısı üzerinden Kamu SM'ye ulaştırılır.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

Kök SHS ve Mobil ESHS sertifikasının özet değeri ve özet algoritması <http://kamusm.bilgem.tubitak.gov.tr> web adresi üzerinden yayımlanır ve Kamu SM'nin faaliyete geçmesini müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurulur.

6.1.5. Anahtar Uzunlukları

Kamu SM Kök SHS'ye ait ECDSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 384-bittir.

Sertifika sahiplerine ait Mobil NES'leri imzalayan Mobil ESHS'ye ait ECDSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 384-bittir.

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

Başvuru sahipleri için üretilen Mobil NES'lere 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.

6.1.7. Anahtar Kullanım Amaçları

Kök SHS'ye ait imza oluşturma verisi, kendi sertifikasını, Mobil ESHS'ye ait sertifikayı ve yayımladığı SİL dosyalarını imzalamak amacıyla kullanılır.

Mobil ESHS'ye ait imza oluşturma verisi, Mobil ESHS tarafından oluşturulan Mobil NES'lerin, yayımlanan SİL dosyalarının ve ÇİSDUP Yanıtlayıcı'ya ait sertifikanın imzalanması amacıyla kullanılır.

ÇİSDUP Yanıtlayıcı'ya ait imza oluşturma verisi, ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarının imzalanması amacıyla kullanılır.

Mobil NES sahiplerine ait imza oluşturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı oluşturmak için kullanılırlar. Sertifika sahibi, güvenli elektronik imza oluşturma aracı içinde bulunan imza oluşturma verisini imza oluşturma dışında kullanmaz. Üçüncü kişiler, nitelikli elektronik sertifikalar içindeki imza doğrulama verilerini, sertifika sahibi tarafından oluşturulmuş elektronik imzanın doğruluğunu kontrol etmek için kullanır. Anahtar çiftlerinin güvenli elektronik imza oluşturma ve doğrulama dışında kullanımlarından doğan sorumluluk sertifika sahibine ve üçüncü kişilere aittir; Kamu SM bu durumda sertifika sahibinin veya üçüncü kişilerin gördükleri zarardan sorumlu tutulamaz.

6.2. İmza OluŐturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluŐturma verisi güvenli yazılım ve/veya donanım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduđu süre boyunca bu modül dıŐına çıkmaz.

Kriptografik modül aŐađıda belirlenen güvenlik iŐlevlerine sahiptir:

- İmza oluŐturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüđünü sađlar.
- Modüle eriŐimde kimlik belirleme ve dođrulama iŐlevlerini yerine getirir.
- EriŐim yetkisi birden fazla kiŐinin kontrolünde olacak Őekilde tanımlanabilir.
- Sistem kullanıcılarına tanımlanan roller dođrultusunda, verdiđi hizmetlere eriŐimini sınırlar.
- Düzgün çalıŐtıđı test edilebilir, test sırasında hata oluŐtuđunda güvenli duruma geçer.
- Modüle izinsiz eriŐim ve kullanım ile tahrifata yol açaabilecek her türlü fiziksel önlem alınmıŐtır.
- Yetkisiz eriŐime teŐebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeđinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluŐturma verisinin içinde bulunduđu güvenli elektronik imza oluŐturma aracı, imza oluŐturma verisinin aracın dıŐına çıkmasını engelleyen ve araca eriŐimi parola ile sađlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluŐturma aracı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'de belirtilen aŐađıdaki güvenlik standartlarından en azından birisini sađlar:
 - FIPS PUB 140-2'ye göre seviye 3 veya üzeri,
 - 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 OluŐturma Verisine Birden Fazla KiŐi Kontrolünde EriŐim

Kamu SM'ye ait imza oluŐturma verisinin bulunduđu odaya eriŐim aynı anda 2 (iki) yetkili personel tarafından sađlanmaktadır.

6.2.3. İmza OluŐturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıŐtır.

6.2.4. İmza OluŐturma Verisinin Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi için sađlanan güvenlik ile eŐdeđer güvenlik önlemleri altında yapılır. Yedeklenen imza oluŐturma verisi yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan imza oluŐturma verisinin bulunduđu ortam ile aynı güvenlik Őartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait imza oluŐturma verileri yedeklenmez.

6.2.5. İmza OluŐturma Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluŐturma verileri arŐivlenmez. Kullanım sŸreleri sonunda geri dŸnŸsŸz Ÿekilde silinir.

6.2.6. İmza OluŐturma Verisinin Kriptografik ModŸle YŸklenmesi

Kamu SM'ye ait imza oluŐturma verisi Ÿretildikten hemen sonra kriptografik modŸle yŸklenir. İŐlem, gŸvenilir yŸntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Mobil NES'lere ait imza oluŐturma verisi gŸvenli imza oluŐturma aracı iŐerisinde oluŐturulur.

6.2.7. İmza OluŐturma Verisinin Kriptografik ModŸlde Saklanması

Kamu SM'ye ait imza oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak gŸvenli kriptografik donanım cihazı iŐinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına őkıması engellenmiŐtir. İmza oluŐturma verisi kriptografik modŸl iŐinde gŸvenli algoritma ve yŸntemlerle Ÿifreli olarak saklanır.

Sertifika sahibine ait imza oluŐturma verisi sertifika sahibinin gŸvenli elektronik imza oluŐturma aracı iŐinde saklanır, baŐka bir ortamda bulunmaz. Kamu SM sertifika sahiplerine ait imza oluŐturma verilerini kendi sistemi iŐinde saklamaz.

6.2.8. İmza OluŐturma Verisine EriŐim

Kamu SM'nin imza oluŐturma verisine eriŐim birden fazla yetkili personelin ortak denetimi altındadır. İmza oluŐturma verisinin bulunduĐu odaya giriŐ iŐin, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin doĐrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadıĐı ve kimliklerinin doĐrulanamadıĐı durumlarda imza oluŐturma verisinin bulunduĐu odaya eriŐim saĐlanamaz.

İmza oluŐturma verisi kriptografik modŸl iŐinde Ÿifreli durumdayken eriŐime kapalıdır. EriŐime aŐılması iŐin eriŐimi saĐlayan verinin modŸle sunulması gerekir. İmza oluŐturma verisinin eriŐime aŐılması ve kullanılabilir duruma getirilmesi birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahibine ait imza oluŐturma verisi gŸvenli elektronik imza oluŐturma aracı iŐinde sertifika sahibinin eriŐim verisi ile korunmuŐ olarak saklanır. EriŐim denetimi eriŐim denetim verisi ile saĐlanır.

6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

Kamu SM'nin imza oluŐturma verisi imzalama iŐin kullanıldıktan sonra oturum kapandıĐında veriye eriŐim otomatik olarak kesilir ve bir dahaki kullanımına kadar Ÿifrelenerek eriŐime kapalı tutulur. EriŐimin yeniden saĐlanabilmesi iŐin BŸlŸm 6.2.8'de belirtilen yŸntemin yeniden iŐletilmesi gerekir.

Sertifika sahibinin kullandıĐı gŸvenli elektronik imza oluŐturma araŐları, imza oluŐturma verisini kullanan oturumun kapanmasından sonra veriye eriŐimi kesecek biŐimde őkalıŐır. EriŐimin yeniden saĐlanabilmesi iŐin sertifika sahibinin eriŐim verisini yeniden girmesi gerekir. EriŐim verisinin ard arda 3 (Ÿç) defa yanlıŐ girilmesi durumunda gŸvenli elektronik imza oluŐturma aracı kilitlenir ve araca eriŐim saĐlanamaz.

6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

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

6.2.11. Kriptografik Modülün Deđerlendirilmesi

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

6.3. Anahtar Çifti Yönetimiyle İlgili Diđer Konular

6.3.1. İmza Doğrulama Verisinin ArŐivlenmesi

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

6.3.2. İmza OluŐturma ve Doğrulama Verilerinin Kullanım Süreleri

İmza oluŐturma verisinin kullanım süresi, Mobil NES'in içeriğinde belirtilen Mobil NES kullanım süresi kadardır. Mobil NES'in kullanım süresinin dolmasıyla ya da Mobil NES'in iptal edilmesiyle imza oluŐturma verisinin kullanımı sona erer. Ancak, kullanım süresi dolsa bile Mobil NES'ler 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 384 bitlik ECDSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 3 (üç) yıl için kullanılır.

Üretilen Mobil NES'lerin son kullanma tarihi kendisine Mobil NES veren Kamu SM'ye ait SHS sertifikasının son kullanma tarihini aşamaz.

6.4. EriŐim Denetim Verileri

Kamu SM çalışanlarının eriŐim denetim verileri; eriŐim parolalarını, güvenli donanım araçları içindeki eriŐim denetimi sađlayan diđer verileri ve biyometrik verileri içerir.

Sertifika sahibine ait eriŐim denetim verisi güvenli elektronik imza oluŐturma aracı eriŐim verisini içerir.

6.4.1. EriŐim Denetim Verilerinin OluŐturulması

Kamu SM sistemi içinde kullanılan eriŐim denetim verileri yetkisiz kişilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rastgele üretilir.

Sertifika sahibine ait güvenli elektronik imza oluŐturma aracı eriŐim denetim verisi sertifika sahibinin kontrolünde üretilir.

6.4.2. EriŐim Denetim Verilerinin Korunması

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

Sertifika sahibine ait güvenli elektronik imza oluŐturma aracı erişim denetim verisini yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. EriŐim Denetim Verileri İle İlgili Diğer Konular

Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar Güvenliđi Denetimleri

6.5.1. Bilgisayar Güvenliđi İle İlgili Teknik Gereklere

Kamu SM sistemi içinde kötü niyetli yazılımlara karşı gereken önlemler alınır. Sistemde ađ ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuŐtur. Kritik işlemlerin yapıldığı bilgisayarlar ađ ortamı dışında tutulur. Bilgilerin tahrifata, silinmeye ve kaçađa karşı korunması ve işlemin sürekliliđinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliđi konusunda bütün iyileŐtirme eylemleri gecikmesiz uygulanır.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. YaŐam Döngüsü Teknik Denetimleri

6.6.1. Sistem GeliŐtirme Denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler aŐađıda verilmiŐtir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliđini sağlamak için sistem bilgilerini tutan bileŐenlerin yedekleri oluŐturulur.
- Sistemin açık ađa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileŐtirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koŐullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- GeliŐtirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin dođrulanmasıyla 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 2 (iki) 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, dışa 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.

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan Mobil NES'lerin 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 Nitelikli Elektronik 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. Mobil NES'in içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Aşağıdaki tabloda Kamu SM tarafından üretilen Mobil NES'de asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Tablo 1 Mobil NES Uzantıları

Sertifika Uzantısı	Kritik Uzanti	Açıklama
Temel Kısıtlar ¹	HAYIR	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılmayacağı belirtilir.
ESHS Anahtar Tanımlayıcı ²	HAYIR	Kamu SM'ye ait Mobil ESHS açık anahtarının SHA-1 özet çıktısından oluşur.
Sertifika Anahtar Tanımlayıcı ³	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

Özne Dizin Nitelikleri ⁴	HAYIR	Mobil NES için gerekli olan doğum tarihi bilgisi bu alan içerisinde eklenmektedir.
Anahtar Kullanım ⁵	EVET	Anahtarların sadece elektronik imza amaçlı kullanıldığının ifade edilmesi için “nonRepudiation” [inkar edilemezlik] alanı ve “digitalSignature” [sayısal imza] alanı seçilmiştir.
SİL Yayımlama Adresi ⁶	HAYIR	http://depo.kamusm.gov.tr/mobil/mobil-s4.crl
ESHS Erişim Bilgisi ⁷	HAYIR	http://depo.kamusm.gov.tr/mobil/mobil-s4.crt http://ocspmobils4.kamusm.gov.tr/
Sertifika İlkeleri ⁸	HAYIR	Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için hazırlanmış olan SUE dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.8) ile SUE dokümanının bulunduğu http://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan Nitelikli Elektronik Sertifika ibaresine ait metni içerir.
Nitelikli Elektronik Sertifika İbaresini ⁹	HAYIR	ETSI 101 862’ye göre, id-etsi-qcs-QcCompliance=0.4.0.1862.1.1 nesne tanımlama numarasını ve varsa sertifikanın kullanımına ilişkin maddi sınır bilgisini içerir. BTK tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası bilgisini içerir.

Uzantılardan bazıları kritik olarak tanımlanmıştır. Kritik olarak belirtilen uzantıların sertifikayı kullanan uygulama tarafından tanımlanamaması durumunda sertifika kullanılamaz.

Kamu SM tarafından kişilere verilen Mobil NES’lerin kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme ETSI 101 862’ye göre “Nitelikli Elektronik Sertifika İbaresini” uzantısı içinde yapılır.

⁴ Subject Directory Attributes

⁵ KeyUsage

⁶ CRLDistributionPoints

⁷ AuthorityInformationAccess

⁸ CertificatePolicies

⁹ QcStatement

Sertifikanın nitelikli olduđu “Nitelikli Elektronik Sertifika İbaresini” uzantısı ierisindeki ETSI ve BTK’ya ait nitelikli elektronik sertifika ibareleri ile belirtilir.

BTK tarafından belirlenen ibare, “Nitelikli Elektronik Sertifika İbaresini” uzantısı iinde yer alan “İbare Bilgisi¹⁰” alanının iine yazılır. Bu ibareye ait nesne tanımlama numarası ise “İbare Tanımlayıcı¹¹” alanı iinde yer alır. Bu ibare ve ibareye ait nesne tanımlama numarası aŐađıda belirtilmiŐtir.

“Bu sertifika, 5070 sayılı Elektronik İmza Kanununa gore nitelikli elektronik sertifikadır.”

Nesne tanımlama numarası: 2.16.792.1.61.0.1.5070.1.1

{joint-iso-itu-t(2) lke(16) tr(792) tk(61.0.1) nes-profile(5070) nes-ibaresi (1) nes-uygunlugu (1)}

Mobil NES’in ETSI’ye uygunluđunun gsterilmesi amacıyla ETSI tarafından tanımlanan aŐađıdaki “İbare Tanımlayıcı” uzantısının iinde bulunur.

Nesne Tanımlama Numarası: 0.4.0.1862.1.1

{ itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) id-etsi-qcs(1) id-etsi-qcs-QcCompliance(1) }

Sertifikanın kullanımına iliŐkin, varsa maddi sınırlamalar ile ilgili bilgilendirme “Nitelikli Sertifika İbaresini” uzantısı iinde ETSI TS 101 862’de belirtilen biimde yapılır. Bu amala aŐađıdaki “İbare Tanımlayıcı” kullanılır:

Nesne Tanımlama Numarası: 0.4.0.1862.1.2

{ itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) id-etsi-qcs(1) id-etsi-qcs-QcLimitValue(2) }

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kiŐilere verdiđi nitelikli elektronik sertifikaları imzalamak iin SHA-384 zet algoritması ile ECDSA aık anahtarlı imzalama algoritmasını kullanır.

Sertifika sahiplerine ait anahtar iftleri RSA algoritması anahtar iftleridir.

Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları iinde belirtilir.

7.1.4. İsim Alanı Biimleri

Kamu SM tarafından retilen nitelikli elektronik sertifikalardaki isim alanı “ITU X.500 Distinguished Name [Ayrırt edici isim]” biimine uygundur.

7.1.5. İsim Kısıtları

retilen nitelikli elektronik sertifikalardaki isim bilgileri kiŐiyi tekil olarak tanımlamayı sađlayacak niteliktedir ve resmi kimlik belgelerinde geen ad ve soyad bilgisinden oluŐur.

¹⁰ StatementInfo

¹¹ StatementId

Kamu SM tarafından farklı kişiler için üretilen Mobil NES'lerin isim alanları aynı olamaz. İsim alanlarının benzersizliğinin sağlanması için T.C. Kimlik Numarası DN alanı içinde yer alır. Yabancı uyruklu Mobil NES sahiplerinin isim alanlarının benzersizliğinin sağlanması için pasaport numarası DN alanı içinde yer alır.

Aşağıdaki tabloda Mobil NES içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

Tablo 2 Mobil NES İsim Alanı Bilgileri

Alan Adı	Mobil NES İçeriği
CN ¹²	Sertifika sahibinin adı soyadı
Serial ¹³	T.C. kimlik numarası / Pasaport numarası
C ¹⁴	TR

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.8

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

“Sertifika İlkeleri” uzantısı Mobil NES'lerin üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Mobil NES'lerin üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Mobil NES'in “Sertifika İlkeleri¹⁵” uzantısının içinde yer alır. “Sertifika İlkeleri” uzantısının içinde “İlke Niteleyici¹⁶” olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler “Sertifika İlkeleri” uzantısını kontrol ettiğinde Sİ ve SUE'de belirtilen ilke ve uygulama esasları çerçevesinde Mobil NES'leri kullanarak işlem yapar.

¹² CN: Common Name [Genel isim]

¹³ Serial: Serial Number [Seri Numarası]

¹⁴ C: Country [Ülke]

¹⁵ Certificate Policies

¹⁶ Policy Identifier

Kamu SM tarafından kişilere verilen elektronik sertifikaların nitelikli olduğunu belirten ibare “Sertifika İlkeleri” uzantısı içindeki “Kullanıcı Bildirim¹⁷” alanında tanımlanır. Kamu SM tarafından tanımlanan Mobil NES ibaresi Kamu SM Sİ dokümanında verilmiştir.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

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

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

¹⁷ User Notice

- Protokol versiyonu
- 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
- Yanıtlayıcı adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritmasının Nesne Tanımlama Numarası.
- 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 6960'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 6960, ÇİSDUP sorguları ve yanıtları içerisinde bazı uzantıların kullanımına imkan verir. Tekrarlama (replay) saldırılarını önlemek için sorgu ve yanıt birbirine bağlayan "nonce" uzantısı bunlardan biridir. Kamu SM ÇİSDUP Yanıtlayıcı, "nonce" uzantısını desteklemektedir. RFC 6960'da belirtilen diğer uzantılar ÇİSDUP yanıt formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

Kamu SM, mevzuat geređi Bilgi Teknolojileri Kurumu tarafından incelenir/denetlenir.

Kamu SM, ek olarak ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) standardına uygun olarak hizmet verir ve standart geređi düzenli olarak iç ve dış denetimlere tabi tutulur.

Kamu SM iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

8.1. Uygunluk Denetiminin Sıklığı

BTK gerekli gördüđü durumlarda re'sen denetim yapılabilir.

Kamu SM, ISO/IEC 27001 BGYS standardı geređince yılda bir defa uygunluk denetimi geçirir. Her üç yılda bir sertifika yenilenir.

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

8.2. Denetçinin Nitelikleri

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

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

İç denetim, Kamu SM SUE'sine hakim, sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi

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

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

İç denetim, Kamu SM SUE'sine hakim, sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

8.4. Denetimin Kapsamı

Kamu SM'nin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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

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

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

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen, yenilenen ve güncellenen Mobil NES'ler için kurumlardan veya sertifika sahiplerinden ücret alınır. Ücretin bilgisi ve ödeme şekli Kamu SM resmi web sitesinde yayınlanır.

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

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ve izni dahilinde sertifika sahiplerine 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 tarafından üretilen Mobil NES'ler için ödenecek bedelin miktarı ile ilgili bilgilendirme e-posta ile yapılır. Ödemenin usulüne uygun biçimde yapılmaması durumunda Mobil NES üretimi yapılmayabilir.

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

9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi tamamlanmamışsa kurum/kişinin talebi doğrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu değildir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Kamu SM, Bölüm 9.2.3'de belirtilen sertifika sahibi mali sorumluluk sigortası dışında, kendi sorumluluklarını karşılamak amacıyla sigortalanmamıştır.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, ürettiği Mobil NES'leri 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalıdır.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

Kamu SM tarafından <http://depo.kamusm.gov.tr> adresinden yayımlanan her türlü doküman 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 alır.

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diğer paydaşların kişisel verilerinin gizliliğini 5070 ve 6698 sayılı kanunlar kapsamındaki mevzuata uygun olarak sağlar.

9.4.2. Gizli 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 tanımlayıcı bilgiler de kişisel bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Mobil NES'in 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.

Kamu SM Kişisel Verilerin Korunması Kanunu kapsamında <http://www.kamusm.gov.tr/kurumsal/kvkk> kurumsal web sayfasından bilgilendirme yapmaktadır.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

Kamu SM tarafından üretilen tüm Mobil NES'ler ve dokümanlar ile bu SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM'nin verdiği sertifika hizmetlerinde sistem bileşenleri olan ESHS'ler, sertifika sahipleri ve üçüncü kişiler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, 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 belirtilen şekilde üzerlerine düşen yükümlülükleri sağlar.

Kamu SM, sertifika sahipleri, sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, Mobil NES Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi, Kurumsal Taahhütname ve varsa taraflar arası yapılan sözleşmelerde 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 SHS ve Mobil ESHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak,

- K k SHS ve Mobil ESHS sertifikalarını son kullanıcıların erişebileceđi ortamlarda yayımlamak,
- Mobil NES verdiği kişiler kimliğini resmi belgelere g re g venilir bir biçimde tespit etmek,
- Kurumlardan gelen Mobil NES başvurularını usul ne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek,
- Mobil NES'in ieriğindeki bilgilerin dođruluđunu beyan edilen belgelere dayanarak sađlamak,
- Gerekli başvuru Őartlarını sađlamayan başvuru sahiplerine Mobil NES vermemek,
- Mobil NES başvurularını deđerlendirerek, başvurunun sonucu hakkında ilgili kişileri/kurum yetkililerini bilgilendirmek,
- Mobil NES başvurusu kabul edilmiŐ kişiler iin operat r tarafından SIM kart vasıtasıyla  retilen anahtar ifti iin Mobil NES  retmek,
- Sertifika sahiplerinin Mobil NES'lerini aksi sertifika sahibi tarafından başvuru formunda belirtilmedike son kullanıcıların erişebileceđi ortamlarda yayımlamak,
- Mobil NES'lerin kullanım Őartlarını belirleyen sertifika profillerini oluŐturmak,
- Mobil NES başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deđerlendirerek gerekli iŐlemlerini yapmak,
- Mobil NES askıya alma başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deđerlendirerek gerekli askıya alma iŐlemlerini yapmak,
- Mobil NES askıdan indirme iŐlemlerini Sİ ve SUE'de belirtilen Őekilde yapmak,
- Mobil NES iptal başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deđerlendirerek gerekli iptal iŐlemlerini zamanında yapmak,
- Yayımlanan Sİ ve SUE dok manları ile Mobil NES Sahibi Taahh namesi'ne uygun olmayan Mobil NES kullanımlarının tespit edilmesi durumunda ilgili Mobil NES'i iptal etmek,
- İptal edilmiŐ Mobil NES bilgilerini sertifika iptal listelerinde yayımlamak veya İSDUP Yanıtlayıcı aracılıđıyla duyurmak,
- Mobil NES'lerin ve iptal durum kayıtlarının b t nl đ n  ve erişilebilirliđini sađlamak iin her t rl  tedbiri almak,
- Sertifika sahiplerine ait elektronik veya kađıt ortamda tutulan bilgilerin gizliliđinin korunması iin gerekli  nlemleri almak, bu bilgileri   nc  kişilere mahkeme kararı olmaksızın vermemek,
- Mobil NES  retim, y netim ve iptali ile ilgili yapılan t m iŐlemlerin kaydını tutmak,
- İŐleyiŐ sırasında kullanılan t m kađıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen s reler boyunca g venli olarak saklamak,
- K k SHS sertifikasının  zet deđerini Kamu SM'ye ait internet ortamından yayımlamak, ulusal yayın yapan en y ksek trajlı 3 ( ) gazetede ilan vermek suretiyle kamuoyuna duyurmak ve gazete ilanlarının bir  rneđini BTK'ya iletmek.

9.6.2. Kayıt Birimi Y k ml l kleri

Kayıt birimlerinin sorumlulukları Őunlardır:

- Sertifika başvurularını almak,
- Sertifika başvuru sahibinin kimlik bilgilerini bu dokümanda belirtilen yöntemlerle gerekli belgelere dayanarak tespit etmek,
- Sertifika sahibinden gerekli belgeleri ve bilgileri almak,
- Mobil NES başvurularını değerlendirerek başvurunun sonucu hakkında ilgili kişileri/kurum yetkililerini bilgilendirmek,
- Doğrulanmış ve kişi tarafından tamamlanmış başvuruları operatöre iletmek,
- Sertifika iptal başvurularının almak,
- Doğrulan sertifika iptal başvurularını Kamu SM'nin ilgili birimlerine iletmek,
- İptal edilen sertifikalar hakkında sahiplerini bilgilendirmek.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri şunlardır:

- Mobil NES başvuru, askıya alma, iptal ve diğer işlemleri ilgili Sİ ve SUE'de belirtildiği şekilde, detayları Kamu SM Mobil NES yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- Mobil NES başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- İmza oluşturma verisini güvenli bir şekilde oluşturup saklayabilecek nitelikteki akıllı SIM kartı mobil hizmet sağlayıcıdan temin etmek,
- İmza oluşturma verisinin üretilmesi esnasında akıllı SIM karta erişim sahibi olmak ve sahipliği kanıtlamak,
- Adına düzenlenen Mobil NES yayımlandığında Mobil NES'deki bilgilerin doğruluğunu kontrol etmek,
- SUE Bölüm 6.2.1'de belirtilen standartlara uygun güvenli elektronik imza oluşturma aracı kullanmak,
- İmza oluşturma verisinin güvenliğini sağlamak, kendisine ait imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının ve imza oluşturma verisi erişim verisinin gizliliğini korumak, bunları başkasına kullandırmamak 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 güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya imza oluşturma verisinin gizliliğinin yitirildiğinden şüphelenmesi durumunda Mobil NES'in iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Güvenli elektronik imza oluşturma aracı erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları düzenli olarak değiştirmek,
- Mobil NES'in içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Operatör'e başvurmak,

- Mobil NES 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 Mobil NES ile işlem yapmamak,
- İmza oluşturma verisini SHS sertifikası imzalamak amacıyla kullanmamak,
- Kendisine verilen Mobil NES'i Sİ ve SUE dokümanlarında belirttiği biçimde varsa karşılıklı imzalanan sözleşmelere uygun ve NES Sahibi Taahhütnamesi'nde belirtilen şartlar dahilinde kullanmak,
- İmza oluşturma verisini, varsa Mobil NES içerisinde belirtilen maddi sınırları aşan finansal işlemlerde kullanmamak.

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

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, Mobil NES'lerle ilgili işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Mobil NES'lerin, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Mobil NES'in kullanım süresinin dolup dolmadığını kontrol etmek,
- Mobil NES'in geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,
- SİL veya ÇİSDUP Yanıtlayıcı'dan alınan iptal durum kaydının bütünlüğünü Kamu SM'ye ait ilgili sertifikaların içinde mevcut olan imza doğrulama verilerini kullanarak doğrulamak,
- Mobil NES'in doğruluğunu Mobil ESHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Mobil ESHS sertifikasının doğruluğunu Kök SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kök SHS sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,
- Sertifika sahibinin Mobil NES'inin içindeki imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğunu doğrulamak,
- Finansal işlemlerde sertifika içerisinde bulunan maddi sınır bilgisini kontrol etmek.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

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

- Sertifika alınacak kurum çalışanlarını belirlemek
- Sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olacak en az bir tane kurum e-imza sorumlusu görevlendirmek ve resmi yazı/ E-imza Sorumlusu Taahhütnamesi ile kurum e-imza sorumlusu nun bilgilerini Kamu SM'ye bildirmek

- Kurum e-imza sorumlusunun görevini sonlandırdığında bunu Kamu SM'ye resmi yazı/E-imza Sorumlusu Taahhütnamesi ile bildirmek
- Yeni görevlendirdiđi kurum yetkililerinin bilgilerini Kamu SM'ye resmi yazı/ E-imza Sorumlusu Taahhütnamesi ile bildirmek
- Sertifika yönetim süreçleri ile ilgili varsa Kamu SM ile imzalanan sözleşmeye uymak
- Sertifika yönetim süreçleri ile ilgili Kurumsal Taahhütname'deki yükümlülükleri yerine getirmek
- Kamu SM'nin internet sitesi üzerinden yayımladığı Kurumsal Taahhütname ve E-imza Sorumlusu Taahhütnamesi'ni doldurarak ilk sertifika başvurusu sırasında Kamu SM'ye iletmek

9.6.5.2. Kurum e-İmza Sorumlularının Yükümlülükleri

Kurum e-İmza Sorumluları sertifika alınacak kurum çalışanlarına ait bilgileri Kamu SM'ye göndermekle ilgili yükümlülükleri aşağıda belirtilmiştir:

- Sertifika alınacak kurum çalışanlarına ait bilgileri tam ve doğru bir şekilde Kamu SM'ye iletmek
- Kurum çalışanı olmayan veya kurum yetkili makamının bilgisi ve kabulü dışındaki kişiler adına sertifika başvurusunda bulunmamak
- Sertifika alınacak kurum personeli listesini Kamu SM'ye imzalı olarak göndermek
- Sertifika yönetim süreçleri ile ilgili işleri Kamu SM ile koordineli bir şekilde yürütmek
- Kamu SM'nin kendisine imzalattığı taahhütnamedeki yükümlülükleri yerine getirmek

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri veya sertifika sahiplerinin bađlı bulunduğu kamu kurum veya kuruluşları arasındaki yükümlülük, Mobil NES Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve varsa imzalanan sözleşmelerde belirtildiđi şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, 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 belirtilen şartlar ile sınırlıdır.

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar Mobil NES Sahibi Taahhütnamesi, Kurumsal Taahhütname, E-imza Sorumlusu Taahhütnamesi ve varsa imzalanan sözleşmelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diđer düzenlemeler dikkate alınır.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahipleri, Mobil NES Sahibi Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile işbirliği içinde çalışır. Kamu SM'den Mobil NES hizmeti alan kamu kurumları Kurumsal Taahhütname, E-imza Sorumlusu Taahhütnamesi ve varsa imzalanan sözleşmelere 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 dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği Kamu SM Taahhütnamesi, Kurumsal Taahhütname, E-imza Sorumlusu Taahhütnamesi ve varsa kurum ile imzaladığı sözleşmelerdeki şartları yerine getirir.

9.10.1. Anlaşma Süresi

Sertifika sahibinin imzaladığı Mobil NES Sahibi Taahhütnamesi'nin veya imzalanan sözleşmenin süresi Mobil NES'in geçerlilik süresi veya taahhütname veya sözleşmede belirtilmemişse hizmetin alınma süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda sözleşme veya taahhütnamenin süresi de sona erer. Aynı şekilde Kamu SM Taahhütnamesi de sertifika sahibinin Mobil NES'inin geçerlilik süresince veya hizmetin alınmaya devam ettiği sürece geçerlidir.

Kurumla imzalanan sözleşmenin geçerlilik süresi sözleşme içerisinde belirtilir.

9.10.2. Anlaşmanın Sona Ermesi

Kamu SM ile kurum arasında varsa imzalanan sözleşme aşağıdaki durumlarda sonlandırılabilir:

- 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 20 (yirmi) 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 sebebiyle Kamu SM sertifika sahiplerine ait Mobil NES'leri iptal ederek sözleşmeyi sonlandırabilir.
- Kamu SM Bölüm 5.8'de belirtildiği biçimde sertifika hizmetlerini sonlandırırca, sertifika sahiplerine ait Mobil NES'leri iptal ederek sözleşmeyi sonlandırabilir.

Kamu SM Taahhütnamesi ve Mobil NES Sahibi Taahhütnamesi veya imzalanan sözleşme aşağıdaki durumlarda sonlandırılabilir:

- Sertifika sahibinin sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi

- Sertifika sahibinin imzalanan sözleşme veya Mobil NES 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 sonlandırırca, Kamu SM'nin sertifika sahibine ait sertifikayı iptal etmesi

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleşmenin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili 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.

İmzalanan sözleşme veya Mobil NES Sahibi Taahhütnamesi'nin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Sertifika sahibinin Mobil NES Sahibi taahhütnamesinden, Sİ veya SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesi durumunda Kamu SM sertifikayı iptal eder. Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

Sözleşme ve taahhütnameler sona erse bile Kamu SM, dağıttığı Mobil NES'lerle ilgili, elektronik imza mevzuatında belirtilen yükümlülüklerini yerine getirmeye devam eder. Kamu SM, dağıttığı Mobil NES'lere, iptal durum kayıtlarına taraflarca erişimin sağlanması, Bölüm 5.4 ve 5.5'te belirtilen kayıtların ve arşivlerin saklanması ile ilgili hizmetleri sürdürür.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, Mobil NES yönetim prosedürlerinde Mobil NES başvurusunun sonucu, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibini ve/veya ilgili kurumu bilgilendirir. Bilgilendirmeler telefon, faks veya e-posta aracılığıyla sağlanır. Kişinin Mobil NES 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 Mobil NES yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan deęişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer. SUE'de yapılan deęişiklikler 7 (yedi) gün içinde Bilgi Teknolojileri ve İletişim Kurumu'na bildirilir.

9.12.3. Nesne Tanımlama Numarasının Deęişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

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

9.14. Uygulanacak Hukuk

SUE dokümanındaki hükümler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu'na uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM MOBİL NES KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	00ed1db82e01d6
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifika Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	9 Ağustos 2019 Cuma 19:25:08
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Açık anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	Değer
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

10.2. KAMU SM MOBİL NES ALT KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	00a05ec4d102af
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	19 Mart 2021 Cuma 09:50:42
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 4 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR
Açık anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	Değer
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 1f 76 a0 78 1a 95 61 fe 41 81 74 b9 79 25 86 7e 98 ab 93 16
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0

Sertifika İlkeleri	<p>[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.1.8 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyicisi= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyicisi= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.</p>
SİL Dağıtım Noktaları	<p>[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crl</p>
Yetkili Bilgi Erişimi	<p>[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crt</p>

10.3. SON KULLANICI MOBİL NES SERTİFİKA ŞABLONU

Alan	Değer
Sürüm	V3
Seri Numarası	64 bit rastsal sayı içeren tam sayı
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	<p>CN = Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 4 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR</p>
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu

Konu	CN = Sertifika Sahibinin Ad ve Soyadı Serial = Sertifika Sahibinin TC Kimlik Numarası C = TR
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Değer
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 1f 76 a0 78 1a 95 61 fe 41 81 74 b9 79 25 86 7e 98 ab 93 16
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	Kritik=Evet; Dijital İmzalama, İnkâr Edilemezlik
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.8 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni= Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/mobil/mobil-s4.crl

Yetkili Bilgi Eriőimi	<p>[1]Yetkili Bilgi Eriőimi</p> <p>Eriőim Yöntemi=Sertifika Yetkilisi Yayımcsısı (1.3.6.1.5.5.7.48.2)</p> <p>Diđer Ad:</p> <p>URL=http://depo.kamusm.gov.tr/mobil/mobil-s4.crt</p> <p>[2]Yetkili Bilgi Eriőimi</p> <p>Eriőim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1)</p> <p>Diđer Ad:</p> <p>URL=http://ocspmobils4.kamusm.gov.tr</p>
Özne Dizin Nitelikleri	<ul style="list-style-type: none">Kritik=Hayır; RFC 3739’da tanımlanmış “dateOfBirth” tipinde olacak şekilde kişinin doğum tarihi (1.3.6.1.5.5.7.9.1)”
Nitelikli Elektronik Sertifika İbaresini	<ul style="list-style-type: none">Telekomünikasyon Kurumu Nitelikli Elektronik Sertifika İbaresini (2.16.792.1.61.0.1.5070.1.1) “Bu sertifika, Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.”