

**TASNİF DIŐI**



**TÜBİTAK BİLGEM  
KAMU SERTİFİKASYON MERKEZİ**

**NİTELİKLİ ELEKTRONİK SERTİFİKA İLKELERİ**

**Döküman Kodu**

POL.01.01

**Revizyon No**

11

**Revizyon Tarihi**

26.04.2018

**TASNİF DIŐI**

REVİZYON GEÇMİŐI		
Revizyon No	Revizyon Nedeni	Revizyon Tarihi
01	İlk yayın	28.03.2005
02	RFC 3647 tam uyumluluđu için yeniden düzenleme	06.06.2005
03	Sertifika yönetim süreçlerinde deđişiklik yapılması Kurum logosunda deđişikliği yapılması Nitelikli Elektronik Sertifika Taahhütnamesi'nin yönetim süreçlerine eklenmesi	13.02.2007
04	Planlı gözden geçirme sonrası küçük deđişiklikler yapıldı	07.05.2008
05	BTK denetimi sonrası, kapsamlı bir güncelleme yapılmıştır.	05.10.2009
06	Sertifikaların askıya alınması ve kullanıma açılması ile ilgili hususlar tekrar düzenlendi.	30.12.2010
07	Kayıtçı hizmeti eklendi. Sistem bileşenleri ve anahtar üretiminin kullanıcı tarafında yapılması ile ilgili eklemeler yapıldı.	02.11.2012
08	Şablon düzeltildi.	11.12.2012
09	Kayıtçı hizmeti politikalardan kaldırıldı.	28.08.2013
10	Gözetmen rolü çıkarıldı. Doküman genelinde düzenlemeler yapıldı. Adresler yeni sertifikalara göre düzenlendi.	20.10.2015
11	Atıf yapılan dokümanların isimleri deđiŐtiđi için güncelleme yapıldı. Doküman genelinde düzenlemeler yapıldı. Dokümanın eski revizyonları Doküman Yönetim Sistemi'nde POLT-001-013 kodu ile yer almaktadır.	26.04.2018

## İÇİNDEKİLER

1. GİRİŐ.....	11
1.1. Genel Bakıő .....	11
1.2. Doküman Adı ve Tanımı.....	12
1.3. Sistem Bileőenleri .....	12
1.3.1. Elektronik Sertifika Hizmet Saęlayıcısı.....	12
1.3.2. Kayıt Birimleri .....	14
1.3.3. Sertifika Sahipleri.....	14
1.3.4. Üçüncü Kiőiler .....	14
1.3.5. Dięer Bileőenler .....	14
1.4. Sertifika Kullanımı .....	14
1.4.1. Uygun Olan Sertifika Kullanımı .....	14
1.4.2. Sertifika Kullanımının Sınırları .....	14
1.5. İlkelerin Yönetimi .....	15
1.5.1. Doküman Yönetimi.....	15
1.5.2. İletişim Bilgileri .....	15
1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluęunu Belirleyen Kiő .....	15
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri .....	15
1.6. Tanımlar ve Kısaltmalar .....	15
1.6.1. Tanımlar.....	15
1.6.2. Kısaltmalar.....	17
2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ.....	19
2.1. Bilgi Depoları.....	19
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması .....	19
2.3. Yayım Sıklığı ve Zamanı.....	19
2.4. Eriőim Kontrolleri .....	19
3. KİMLİK BELİRLEME VE DOęRULAMA.....	20
3.1. İsimlendirme .....	20
3.1.1. İsim Alanı Tipleri .....	20
3.1.2. Kimlik Bilgilerinin Teőhise Elverişli Olması .....	20
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması .....	20
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması .....	20
3.1.5. Kimlik Bilgilerinin Tekillilięi .....	20
3.1.6. Markanın Tanınması, Doęrulanması ve Rolü.....	20
3.2. İlk Kimlik Belirleme.....	20
3.2.1. İmza Oluőturma Verisine Sahip Olmanın Kanıtlanması .....	20
3.2.2. Kiőisel Kimlięin Belirlenmesi .....	21
3.2.3. Doęrulanmayan Sertifika Sahibi Bilgileri .....	21
3.2.4. Yetkinin Doęrulanması .....	21
3.2.5. Uyum Kriterleri .....	21
3.3. Sertifika Yenileme İsteęinde Kimlik Doęrulama.....	21
3.3.1. Olaęan Sertifika Yenileme İsteęinde Kimlik Doęrulama .....	21
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doęrulama.....	21

<b>3.4. Sertifika İptal İsteğinde Kimlik Doğrulama</b> .....	<b>21</b>
<b>4. İŞLEMSEL GEREKLER</b> .....	<b>22</b>
<b>4.1. Sertifika Başvurusu</b> .....	<b>22</b>
4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği .....	22
4.1.2. Kayıt İşlemleri ve Sorumluluklar .....	22
<b>4.2. Sertifika Başvurusunun İşlenmesi</b> .....	<b>22</b>
4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi.....	22
4.2.2. Sertifika Başvurusunun Kabul veya Reddi .....	22
4.2.3. Sertifika Başvurusunun İşlenme Zamanı .....	23
<b>4.3. Sertifikanın Oluşturulması</b> .....	<b>23</b>
4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri .....	23
4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi .....	23
<b>4.4. Sertifikanın Kabulü</b> .....	<b>23</b>
4.4.1. Sertifikanın Kabul Koşulu.....	23
4.4.2. Sertifikanın ESHS Tarafından Yayımlanması .....	23
4.4.3. Sertifikanın Oluşturulmasının Diğer Tarafalara Duyurulması.....	23
<b>4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı</b> .....	<b>23</b>
4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı .....	23
4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı .....	24
<b>4.6. Sertifika Süresinin Uzatılması</b> .....	<b>24</b>
<b>4.7. Sertifika Yenileme</b> .....	<b>24</b>
4.7.1. Sertifika Yenileme Koşulları .....	24
4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği .....	24
4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi.....	24
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi .....	25
4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu .....	25
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması .....	25
4.7.7. Sertifika Yenilemenin Diğer Tarafalara Duyurulması .....	25
<b>4.8. Sertifikada Bilgi Değişikliği</b> .....	<b>25</b>
<b>4.9. Sertifikanın İptali ve Askıya Alınması</b> .....	<b>25</b>
4.9.1. Sertifikanın İptal Edildiği Durumlar .....	25
4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir .....	26
4.9.3. Sertifika İptal Başvurusunun İşlenmesi .....	26
4.9.4. İptal İsteği Ertelenme Süresi.....	26
4.9.5. İptal İsteğinin İşlenme Süresi.....	26
4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliği .....	26
4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı .....	27
4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi .....	27
4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti.....	27
4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi.....	27
4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri .....	27
4.9.12. İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu .....	27
4.9.13. Sertifikanın Askıya Alındığı Durumlar .....	27
4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği.....	28

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

5.5.3.	Arşivlerin Korunması .....	34
5.5.4.	Arşivlerin Yedeklenmesi .....	34
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri.....	35
5.5.6.	Arşivlerin Toplanması .....	35
5.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu.....	35
<b>5.6.</b>	<b>Anahtar Değişimi.....</b>	<b>35</b>
<b>5.7.</b>	<b>Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar .....</b>	<b>35</b>
5.7.1.	Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi .....	35
5.7.2.	Donanım, Yazılım veya Veri Bozulması.....	35
5.7.3.	İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi .....	35
5.7.4.	Arıza Sonrası Yeniden Çalışırılık.....	36
<b>5.8.</b>	<b>Sertifika Hizmetlerinin Sonlandırılması.....</b>	<b>36</b>
<b>6.</b>	<b>TEKNİK GÜVENLİK KONTROLLERİ .....</b>	<b>37</b>
<b>6.1.</b>	<b>Anahtar Çifti Üretimi ve Kurulumu .....</b>	<b>37</b>
6.1.1.	Anahtar Çifti Üretimi .....	37
6.1.2.	Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması .....	37
6.1.3.	Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması.....	37
6.1.4.	Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması.....	37
6.1.5.	Anahtar Uzunlukları.....	38
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü .....	38
6.1.7.	Anahtar Kullanım Amaçları.....	38
<b>6.2.</b>	<b>İmza Oluşturma Verisinin Korunması .....</b>	<b>38</b>
6.2.1.	Kriptografik Modül Standartları .....	38
6.2.2.	İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim .....	38
6.2.3.	İmza Oluşturma Verisinin Yeniden Elde Edilmesi .....	38
6.2.4.	İmza Oluşturma Verisinin Yedeklenmesi.....	39
6.2.5.	İmza Oluşturma Verisinin Arşivlenmesi.....	39
6.2.6.	İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi .....	39
6.2.7.	İmza Oluşturma Verisinin Kriptografik Modülde Saklanması.....	39
6.2.8.	İmza Oluşturma Verisine Erişim .....	39
6.2.9.	İmza Oluşturma Verisine Erişimin Kesilmesi .....	40
6.2.10.	İmza Oluşturma Verisinin Yok Edilmesi .....	40
6.2.11.	Kriptografik Modülün Değerlendirilmesi.....	40
<b>6.3.</b>	<b>Anahtar Çifti Yönetimiyle İlgili Diğer Konular .....</b>	<b>40</b>
6.3.1.	İmza Doğrulama Verisinin Arşivlenmesi .....	40
6.3.2.	İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri.....	40
<b>6.4.</b>	<b>Erişim Denetim Verileri.....</b>	<b>40</b>
6.4.1.	Erişim Denetim Verilerinin Oluşturulması .....	41
6.4.2.	Erişim Denetim Verilerinin Korunması .....	41
6.4.3.	Erişim Denetim Verileri İle İlgili Diğer Konular .....	41
<b>6.5.</b>	<b>Bilgisayar Güvenliği Denetimleri .....</b>	<b>41</b>
6.5.1.	Bilgisayar Güvenliği İle İlgili Teknik Gereklere.....	41
6.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi .....	41
<b>6.6.</b>	<b>Yaşam Döngüsü Teknik Denetimleri .....</b>	<b>41</b>

6.6.1.	Sistem Geliştirme Denetimleri .....	41
6.6.2.	Güvenlik Yönetimi Denetimleri .....	41
6.6.3.	Yaşam Döngüsü Güvenlik Denetimleri .....	41
<b>6.7.</b>	<b>Ağ Güvenliği Denetimleri .....</b>	<b>42</b>
<b>6.8.</b>	<b>Zaman Damgası .....</b>	<b>42</b>
<b>7.</b>	<b>SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ.....</b>	<b>43</b>
<b>7.1.</b>	<b>Sertifika Biçimi .....</b>	<b>43</b>
7.1.1.	Sürüm Numarası.....	43
7.1.2.	Sertifika Uzantıları .....	43
7.1.3.	Algoritma ve Nesne Tanımlayıcılar .....	44
7.1.4.	İsim Alanı Biçimleri .....	45
7.1.5.	İsim Kısıtları .....	45
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası .....	45
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	45
7.1.8.	İlke Niteleyiciler .....	46
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi .....	46
<b>7.2.</b>	<b>Sertifika İptal Listesi Biçimi .....</b>	<b>46</b>
7.2.1.	Sürüm Numarası.....	46
7.2.2.	Sertifika İptal Listesi Uzantıları .....	46
<b>7.3.</b>	<b>Çevrim İçi Sertifika Durum Protokolü Biçimi .....</b>	<b>46</b>
7.3.1.	Sürüm Numarası.....	46
7.3.2.	ÇİSDUP Uzantıları .....	47
<b>8.</b>	<b>UYGUNLUK DENETİMLERİ.....</b>	<b>48</b>
<b>8.1.</b>	<b>Uygunluk Denetiminin Sıklığı .....</b>	<b>48</b>
<b>8.2.</b>	<b>Denetçinin Nitelikleri.....</b>	<b>48</b>
<b>8.3.</b>	<b>Denetçinin Denetlenen Tarafla Olan İlişkisi .....</b>	<b>48</b>
<b>8.4.</b>	<b>Denetimin Kapsamı .....</b>	<b>48</b>
<b>8.5.</b>	<b>Yetersizliğin Tespiti Durumunda Yapılacaklar .....</b>	<b>48</b>
<b>8.6.</b>	<b>Sonucun Bildirilmesi .....</b>	<b>49</b>
<b>9.</b>	<b>DIĐER İŐLER VE HUKUKSAL MESELELER .....</b>	<b>50</b>
<b>9.1.</b>	<b>Ücretlendirme .....</b>	<b>50</b>
9.1.1.	Sertifika OluŐturma ve Yenileme Ücreti .....	50
9.1.2.	Sertifika EriŐim Ücreti .....	50
9.1.3.	İptal Durum Kaydına EriŐim Ücreti .....	50
9.1.4.	Diđer Servis Ücretleri.....	50
9.1.5.	İade Ücreti .....	50
<b>9.2.</b>	<b>Finansal Sorumluluk .....</b>	<b>50</b>
9.2.1.	Sigorta Kapsamı .....	50
9.2.2.	Diđer Varlıklar .....	50
9.2.3.	Sertifika Mali Sorumluluk Sigortası .....	50
<b>9.3.</b>	<b>Ticari Bilginin Korunması .....</b>	<b>51</b>
9.3.1.	Gizli Bilginin Kapsamı.....	51
9.3.2.	Gizlilik Kapsamında Olmayan Bilgiler .....	51

9.3.3.	Gizli Bilginin Korunma Sorumluluđu .....	51
<b>9.4.</b>	<b>Kişisel Bilginin Gizliliđi.....</b>	<b>51</b>
9.4.1.	Gizlilik Planı.....	51
9.4.2.	Gizli Olarak Tanımlanan Bilgiler .....	51
9.4.3.	Gizli Olarak Tanımlanmayan Bilgiler .....	51
9.4.4.	Gizli Bilginin Korunma Sorumluluđu .....	51
9.4.5.	Gizli Bilginin Kullanımına İzin Verilmesi .....	52
9.4.6.	Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması .....	52
9.4.7.	Diđer Bařlıklar .....	52
<b>9.5.</b>	<b>Telif Hakları.....</b>	<b>52</b>
<b>9.6.</b>	<b>Temsil Hakkı ve Yükümlölükler .....</b>	<b>52</b>
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yükümlölükleri.....	52
9.6.2.	Kayıt Birimi Yükümlölükleri .....	52
9.6.3.	Sertifika Sahibinin Yükümlölükleri .....	52
9.6.4.	Üçüncü Kişilerin Yükümlölükleri .....	53
9.6.5.	Diđer Bileşenlerin Yükümlölükleri .....	53
<b>9.7.</b>	<b>Yükümlölüklerden Feragat.....</b>	<b>53</b>
<b>9.8.</b>	<b>Sorumlulukla İlgili Sınırlamalar.....</b>	<b>53</b>
<b>9.9.</b>	<b>Tazminat Halleri .....</b>	<b>53</b>
<b>9.10.</b>	<b>Anlaşma Süresi ve Anlaşmanın Sona Ermesi .....</b>	<b>54</b>
9.10.1.	Anlaşma Süresi .....	54
9.10.2.	Anlaşmanın Sona Ermesi .....	54
9.10.3.	Anlaşmanın Sona Ermesinin Etkileri.....	54
<b>9.11.</b>	<b>Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme .....</b>	<b>54</b>
<b>9.12.</b>	<b>Deđişiklik Halleri .....</b>	<b>54</b>
9.12.1.	Deđişiklik Metodları.....	54
9.12.2.	Bilgilendirme Mekanizması ve Sıklığı.....	54
9.12.3.	Nesne Tanımlama Numarasının Deđişmesini Gerektiren Durumlar .....	54
<b>9.13.</b>	<b>Anlaşmazlık Halleri .....</b>	<b>55</b>
<b>9.14.</b>	<b>Uygulanacak Hukuk .....</b>	<b>55</b>
<b>9.15.</b>	<b>Uygulanabilir Yasalarla Uyum.....</b>	<b>55</b>
<b>9.16.</b>	<b>Diđer Hükümler .....</b>	<b>55</b>





**ŐEKİLLER**

Őekil 1 Kamu SM Aık Anahtar Altyapısı Mimarisi.....12



**TABLolar**

Tablo 1 NES Anahtar Kullanım Alanları .....	43
Tablo 2 Sertifika İsim Alanları .....	45

## 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) Nitelikli Elektronik Sertifika (NES) üreten Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) işlevleri sırasında uyulması gereken kuralları ve çalışma ilkelerini tanımlayan Sertifika İlkeleri (Sİ) dokümanıdır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu kapsamında ve Başbakanlığın 2004/21 sayılı "Kamu Sertifikasyon Merkezi Oluşturulması" konulu genelgesi uyarınca kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması amacıyla kurulmuştur. Kamu SM, kamu çalışanlarına kurum içi ve kurumlar arası işlemlerde kullanılmak üzere NES üretilir, sertifikaların yaşam döngüsü içinde gerekli iptal ve yenileme gibi işlemlerini yerine getirir. Kamu çalışanları Kamu SM tarafından kendilerine verilen NES'leri bireysel işlemlerinde de kullanabilirler.

Kamu SM Sİ dokümanı NES hizmeti verilirken ESHS'nin kendisine özel işlevsel ortamından bağımsız olarak sertifikaların başvuru, üretim, dağıtım, yenileme, iptal etme ile ilgili süreçler içindeki işlemlerinin hangi genel ilkeler doğrultusunda gerçekleştirildiğini, Açık Anahtar Altyapısı'nı (Public Key Infrastructure-PKI) oluşturan ve kullanan tüm bileşenlere uygulanan yönetim kurallarını tanımlayan üst düzey bir dokümandır. Bu doküman, 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 esas alınarak hazırlanmıştır.

Kamu SM, Sİ'de tanımlanan gerekleri nasıl karşıladığını anlatan Sertifika Uygulama Esasları (SUE) dokümanını hazırlar ve SUE dokümanına bağlı olarak çalışır. Sİ dokümanı sertifika yönetim işlemleri ile ilgili olarak "ne" yapılacağını tanımlarken, SUE dokümanı bunun "nasıl" yapılacağını tanımlar.

### 1.1. Genel Bakış

Bu doküman, NES'lerin üretim ve yönetim ilkelerinin, sertifika yönetimi ile ilgili tüm kural ve usullerin en üst düzeyde tanımlandığı bir dokümandır. Kamu SM'den sertifika talebinde bulunan kullanıcılar bu dokümanda belirtilen şartları kabul etmiş sayılırlar.

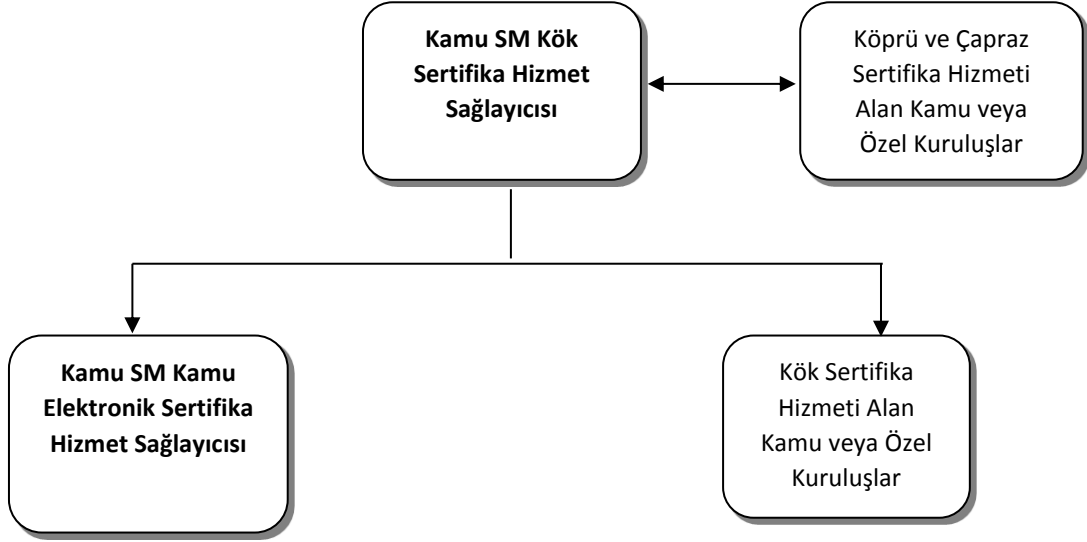
Kamu SM açık anahtar altyapısı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı (Kök SHS) ile buna bağlı olarak çalışan Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS) bulunur.

Kök SHS son kullanıcılar 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, köprü veya çapraz sertifika hizmeti verir.

Kamu ESHS ve Kamu SM'den kök sertifika hizmeti alan kamu kuruluşları veya özel kuruluşlar, Kök SHS'nin elektronik imzasını taşıyan sertifikaya sahiptir. Kamu SM açık anahtar altyapısı mimarisi Şekil 1'de verilmiştir.

Kamu ESHS, gerçek kişilere NES temini amacıyla hizmet verir.

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



Şekil 1 Kamu SM Açık Anahtar Altyapısı Mimarisi

## 1.2. Doküman Adı ve Tanımı

**Doküman Adı:** Nitelikli Elektronik Sertifika İlkeleri

**Doküman Sürüm Numarası:** 11

**Yayın Tarihi:** 26.04.2018

**Nesne Tanımlama Numarası:** 2.16.792.1.2.1.1.5.7.1.1

Kamu SM (Nitelikli Elektronik Sertifika) Sertifika İlkeleri { joint-iso-itu-t(2) ülke(16) tr(792) TÜBİTAK(1.2.1.1) UEKAE(5) KSM(7) ksm-sertifika-ilkeleri(1) ksm-nes-ilke-1 (1) }

## 1.3. Sistem Bileşenleri

Kamu SM açık anahtar altyapısını oluşturan sistem bileşenleri aşağıda tanımlanmıştır.

### 1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Kamu SM, BTK tarafından yetkilendirilmiş bir elektronik sertifika hizmet sağlayıcısıdır. Kamu SM



bünyesinde kurulan sertifika hizmet sağlayıcıları ve Kamu SM'den hizmet alan diğer ESHS'ler Kamu SM açık anahtar alt yapısını oluşturan sistem bileşenleridir. Bu bileşenler aşağıda belirtilmiştir.

#### Kök Sertifika Hizmet Sağlayıcısı (Kök SHS)

Kök SHS, alt kök sertifikası dağıtır. Kamu SM içinde en yetkili imza derecesine sahiptir ve sertifikası kendi imza oluşturma verisi ile imzalanmıştır.

Kamu SM, güvenlik gerekleri dolayısıyla özel statüye sahip kamu kuruluşlarına (Türk Silahlı Kuvvetleri, Dışişleri Bakanlığı, vb.) ait ESHS'ler, ülke içinde hizmet veren ulusal ESHS'ler ve ülke dışında kurulmuş olan diğer ESHS'lerle ortak çalışırılığı sağlayabilmek için alt kök, köprü ve çapraz sertifika hizmetleri verir. Üretilen alt kök, köprü ve çapraz sertifikalar Kök SHS'nin imzasını taşır.

Kök SHS imza oluşturma verisinin bulunduğu sistem çevrim dışı çalışır. İmza oluşturma verisi, en üst düzeyde fiziksel ve elektronik güvenlik sağlanarak korunur.

#### Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS)

Kamu ESHS, kamu çalışanı gerçek kişilere NES üretmekle yetkilidir. Kamu ESHS'nin sertifikası Kök SHS tarafından imzalanmıştır. Kişiler adına üretilen NES'ler Kamu ESHS'nin elektronik imzasını taşır. Kamu ESHS tarafından verilen NES'ler 5070 sayılı elektronik imza kanunu kapsamında verilir. Kamu ESHS, elektronik imza kanunu kapsamına girmeyen nitelikli olmayan sertifikalar da verebilir.

#### Alt Kök Sertifika Hizmeti Alan Kuruluşlar

Kamu SM'den alt kök sertifika hizmeti alan yurt içinde veya yurt dışında kurulmuş kamu veya özel kuruluşlara verilen alt kök sertifikalar Kök SHS tarafından imzalanmıştır. Alt kök sertifika hizmeti alan kuruluşlara verilen sertifikalar için başvuru, üretim, dağıtım, yenileme ve iptal etme ile ilgili süreçler içindeki işlemler bu dokümanın içeriğinde bulunmaz. Kamu SM'den alt kök sertifika hizmeti almak isteyen ESHS'ler konuyla ilgili olarak başvuru işlemlerini Kamu SM tarafından belirlenen şartlar doğrultusunda yerine getirirler. Üretilen alt kök sertifikaların üretim, dağıtım, iptal ve yenilenmeleri ile ilgili yönetim işlemleri de yine Kamu SM'nin belirlediği şartlara göre yerine getirilir. Alt kök sertifikasyon hizmeti alan ESHS'ler kullanıcılara verdikleri sertifika hizmetiyle ilgili süreçleri bu Sİ dokümanında belirtilen sertifika ilkelerine bağlı kalarak yerine getirirler.

#### Köprü veya Çapraz Sertifika Hizmeti Alan Kuruluşlar

Kamu SM'den köprü veya çapraz sertifika hizmeti alan yurt içinde veya yurt dışında kurulmuş kamu veya özel kuruluşlara verilen köprü veya çapraz sertifikalar Kök SHS tarafından imzalanmıştır. Köprü veya çapraz sertifika hizmeti alan tarafların başvuru işlemleri ile üretilen köprü ve çapraz sertifikaların yönetimi ile ilgili süreçler bu dokümanın içeriğinde bulunmaz. Kamu SM ile hizmeti alan taraf arasında karşılıklı güvenin temin edilmesi için gereken şartlar imzalanan sözleşmelerde belirtilir.

### 1.3.2. Kayıt Birimleri

Kayıt birimleri, son kullanıcıların sertifika başvuru kayıt işlemlerini ve sertifika teslimatlarını yapmakla yetkili birimlerdir. ESHS kendi bünyesi ve fiziksel ortamı içinde kayıt birimleri bulundurduğu gibi kayıt birimi hizmetini kendi fiziksel ortamından uzakta bir ortamda da kurabilir.

### 1.3.3. Sertifika Sahipleri

Sertifika sahipleri, elektronik sertifikanın içeriğinde adı bulunan ve sertifikasını Kamu SM sertifika ilkelerine ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek kişilerdir.

### 1.3.4. Üçüncü Kişiler

Üçüncü kişiler, sertifikaların içindeki kimlik ve imza doğrulama verisi arasındaki bağı doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir.

### 1.3.5. Diğer Bileşenler

Yukarıda yazılanlar dışındaki bileşenlerdir. Diğer bileşenler gerekirse bu Sİ dokümanına uygun oluşturulan SUE dokümanında detaylandırılır.

## 1.4. Sertifika Kullanımı

### 1.4.1. Uygun Olan Sertifika Kullanımı

Üretilen NES'lere ait imza oluşturma verileri, elektronik imzaya ilişkin mevzuatta tanımlanmış şekilde sertifika sahibi tarafından, güvenli elektronik imza oluşturma aracıyla birlikte, güvenli elektronik imza oluşturmak amacıyla kullanılır. Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur.

NES içeriğindeki imza doğrulama verisi, oluşturulan güvenli elektronik imzanın doğrulanması için kullanılır.

### 1.4.2. Sertifika Kullanımının Sınırları

NES'e ait imza oluşturma verisi, güvenli elektronik imza oluşturmak dışında başka amaçlar için kullanılmaz. NES içeriğindeki imza doğrulama verisi, oluşturulan güvenli elektronik imzanın doğrulanması dışında başka amaçlar için kullanılmaz.

Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez.

ESHS, dağıttığı sertifikaların hangi uygulamalarda ne amaçlar doğrultusunda kullanıldığını denetlemekle yükümlü değildir.

## 1.5. İlkelerin Yönetimi

### 1.5.1. Doküman Yönetimi

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

### 1.5.2. İletişim Bilgileri

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

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

**Tel.** : (262) 648 18 18

**Faks** : (262) 648 18 00

**E Posta** : [bilgi@kamusm.gov.tr](mailto:bilgi@kamusm.gov.tr)

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

Kamu SM, Sİ dokümanını herkesin erişimine açık bulunan aşağıdaki internet adreslerinden yayımlar:

- <http://depo.kamusm.gov.tr/ilke/>
- [http://www.kamusm.gov.tr/BilgiDeposu/KSM\\_NES\\_SI/KSM\\_NES\\_SI.pdf](http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SI/KSM_NES_SI.pdf)

### 1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluęunu Belirleyen Kiři

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

### 1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

Bu Sİ dokümanına uygun olarak oluşturulan SUE dokümanının uygunluęu, Kamu SM tarafından onaylanır.

## 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 dięer sertifika işlemleri ile ilgili bilgilerin yayımlandığı web sunucular, izin sunucular gibi veri saklama ortamları.

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

**Elektronik sertifika:** İmza sahibinin, imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt. Bu dokümanda bahsi geçen elektronik sertifika ve sertifika kelimeleri, NES'i ifade etmek amacıyla kullanılmıştır.

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

**Güvenli elektronik imza oluşturma aracı:** Sertifika sahibine ait imza oluşturma verisi ve sertifikanın içinde bulunduğu taşınabilir, akıllı kart ya da benzeri güvenli cihaz.

**Güvenli elektronik imza 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 gizli 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 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 Sertifika Hizmet Sağlayıcısı.

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

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

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

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

**Sertifika iptal 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.

**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

**BS (British Standards):** İngiliz Standartları

**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):** Değerlendirme Garanti Düzeyi

**ESHS:** Elektronik Sertifika Hizmet Sağlayıcısı

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

**ETSI TS (ETSI Technical Specification):** ETSI Teknik Özellikleri

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

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

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

**ITU (International Telecommunication Union):** Uluslararası Telekomünikasyon Birliği

**KPS:** Kimlik Paylaşım Sistemi

**Kamu SM:** Kamu Sertifikasyon Merkezi

**LDAP (Lightweight Directory Access Protocol):** Dizin Erişim Protokolü

**PKI (Public Key Infrastructure):** Açık Anahtar Altyapısı

**Si:** Sertifika İlkeleri

**SİL:** Sertifika İptal Listesi



**SUE:** Sertifika Uygulama Esasları

## 2. Yayınlama ve Bilgi Deposu Yükümlülükleri

### 2.1. Bilgi Depoları

ESHS, sistem bileşenleri ile paylaştığı bilgileri bilgi depoları üzerinden yayımlar. Bilgi deposu olarak web sunucular veya izin sunucuları kullanılır. Bilgi depolarına erişim internet üzerinden sağlanır.

### 2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması

ESHS, kendisine ait sertifikaları, iptal durum kayıtlarını, Sİ ve SUE dokümanlarını bilgi deposundan ücretsiz olarak erişime açık tutar; bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri alır; bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlar. ESHS, sertifika sahibinin izni olmadan sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz. ESHS, kendi sertifikasına ait sertifika özet değeri ile özet değerini hesaplamada kullandığı özetleme algoritması bilgisini internet sitesi üzerinden yayımlar.

### 2.3. Yayın Sıklığı ve Zamanı

ESHS'nin kendisine ait sertifikalar, ESHS'nin hizmet süresi boyunca kesintisiz olarak yayımlanır. ESHS'nin kendisine ait sertifikaların güncellenmesi durumunda, yenilenen sertifikalar en kısa zamanda yayımlanır.

Sİ/SUE dokümanları ve sertifika yönetim işlemleri ile ilgili bilgilendirmenin yapıldığı dokümanlar güncellendikten sonra en kısa zamanda yayımlanır.

İptal durum kayıtlarının yayımlanma sıklığı, ilgili SUE dokümanında belirtilir. NES iptal durum kayıtlarının yayımlanma sıklığı 1 (bir) günden fazla olamaz.

### 2.4. Erişim Kontrolleri

ESHS bilgi deposuna erişim herkese açıktır.

ESHS, bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak, bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamakla yükümlüdür.

### 3. Kimlik Belirleme ve Doğrulama

Sertifika başvurusu sırasında, sertifika içeriğinde adı bulunan kişilerin kimliklerinin belirlenmesi, daha sonra gerçekleştirilen yenileme, askıya alma ve iptal taleplerinin yerine getirilebilmesi için kimlik doğrulaması yapılması gerekir. Sertifika işlemlerinde gerekli olan, kimliklerinin belirlenmesi ve doğrulanması, bu bölümde anlatılan ilkelere uygun olarak gerçekleştirilir.

#### 3.1. İsimlendirme

##### 3.1.1. İsim Alanı Tipleri

Üretilen sertifikalarda kimlik bilgilerinin yazıldığı isim alanı "ITU X.500 Distinguished Name (Ayırt edici isim)" biçimine uygundur.

##### 3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Sertifika içeriğindeki kimlik bilgilerinin, anlamlı ve kişiyi tanımlayıcı nitelikte olması gerekmektedir. İsim alanlarının içinde sertifika sahibinin teşhis edilebileceği kimlik bilgisi bulunur.

##### 3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika sahibinin, sertifikasının içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

##### 3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Sertifikalar içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

##### 3.1.5. Kimlik Bilgilerinin Tekilliği

ESHS'nin ürettiği, farklı kişilere ait sertifikalarda aynı kimlik bilgilerinin kullanılması engellenir. Sertifika içeriğinde, sertifika sahibini tekil biçimde ifade edecek şekilde yeterli kimlik bilgisi kullanılır. Sertifikaların isim alanlarında, hangi bilgilerin benzersiz kimlik bilgisi oluşturma amacıyla kullanılacağı SUE dokümanında belirtilir.

##### 3.1.6. Markanın Tanınması, Doğrulaması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

#### 3.2. İlk Kimlik Belirleme

Kişi veya kuruluşların kimliklerinin ilk sertifika başvurusu sırasında belirlenmesi için aşağıdaki yöntemler uygulanır.

##### 3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

Sertifika sahibine ait imza oluşturma ve doğrulama verileri, ESHS tarafından üretilerek sertifika sahibine ulaştırılır. İmza oluşturma ve doğrulama verileri aynı anda sahibine teslim edildiğinden sertifika sahibinin imza oluşturma verisine sahip olduğu kabul edilir. Kurumsal Kimliğin Belirlenmesi

ESHS, sertifika başvurusunda bulunan kurumların kurum bilgilerini, resmi ve onaylı belgelere dayanarak belirler. Kamu kurum veya kuruluşlarının kimliklerinin belirlenmesi için resmi yazı ile yapılan bilgilendirmeler yeterlidir.

### 3.2.2. Kişisel Kimliğin Belirlenmesi

NES başvurusunda bulunan kurumlar, NES almak istediği çalışanlarına ait bilgileri ESHS'ye bildirir. Kişilere ait kimlik bilgileri, Kimlik Paylaşım Sistemi ve kurumsal başvuru belgesine dayanılarak belirlenir.

### 3.2.3. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibine ve kurumlara ait adres, faks numarası, telefon numarası ve elektronik posta gibi erişim bilgileri ile varsa SUE dokümanında işaret edilen diğer bilgiler ESHS tarafından doğrulanmayan bilgilerdir. Bu bilgilerle ilgili olarak sertifika sahibinin ve kurumun beyanı doğru kabul edilir.

### 3.2.4. Yetkinin Doğrulanması

Sertifika sahibinin yetkisi ile ilgili bilgiler sertifika içeriğine yazılacaksa resmi belgelere dayanılarak yetki tespit edilir.

### 3.2.5. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

## 3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

### 3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

### 3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

## 3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

ESHS'nin kullanım süresi dolmamış sertifikaları kullanımdan kaldırması işlemi, "sertifika iptali" olarak adlandırılır. İptal istekleri, sertifika sahibinin internet üzerinden veya telefonla kimliğini doğrulayarak ya da Kurum'un talebinin doğrulanması üzerine yapılır.

## 4. İşlemsel Gereklar

Bu bölümde, sertifika yaşam döngüsü içinde sertifika yönetimiyle ilgili gerçekleştirilen işlemler ile sertifika sahipleri, ESHS ve üçüncü kişilerin bu işlemlerdeki rol ve sorumlulukları anlatılmıştır.

### 4.1. Sertifika Başvurusu

#### 4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiđi

Sertifika başvurusu, kamu kurumları tarafından ESHS'ye kurumsal olarak yapılır. Kamu çalışanları bađlı buldukları kurumdan bađımsız olarak bireysel başvuruda bulunamazlar.

#### 4.1.2. Kayıt İşlemleri ve Sorumluluklar

Sertifika başvurusu ESHS'ye yapılır. Kayıt süreçleri ile ilgili detaylar SUE dokümanında anlatılır.

Sertifika başvurusu sırasında, başvuru sahibinin kimliđi tanımlanır ve dođrulandır. Bunun için kurum veya kuruluş, sertifika talebinde bulunduđu kişilerin bilgilerini ESHS'ye gönderir. Kurumsal başvuru sahibi, adına başvuruda bulunduđu kişilerin sertifika taleplerini resmi yazı ile; ıslak imzalı ya da elektronik imzalı olarak belgelendirir.

Sertifika başvurusunda bulunan çalışanlar, başvuru sırasında sertifika kullanımıyla ilgili sorumluluklarının belirtildiđi sertifika sözleşmesini veya taahhünamesini imzalarlar.

Başvuru sahibi kurum ve çalışanları, ESHS'nin tanımladıđı, detayları SUE dokümanında yer alan başvuru şartlarını yerine getirmekten sorumludur. ESHS, sertifika içinde yer alacak bilgilerin dođruluđunun sađlanmasıyla sorumludur.

### 4.2. Sertifika Başvurusunun İşlenmesi

#### 4.2.1. Kimlik Tanımlama ve Dođrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında ESHS'ye gönderilen belgeler incelenerek, işleme alınır. Belgelerin hatalı olması, eksik veya yanlışlıđının tespit edilmesi durumunda, kimlik tanımlama ve dođrulama yapılamaz.

#### 4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Başvuru sırasında alınan belgelerin incelenmesi sonucunda, başvuru kabul edilir veya geri çevrilir. Başvurunun kabul edilmesi veya geri çevrilmesi ile ilgili kriterler, SUE dokümanında yer alır. Geri çevrilen başvurular, reddediliş sebepleriyle birlikte kuruma bildirilir. Bilgilendirme süreci, elektronik ortam üzerinden veya yazı ile yapılabilir. Geçerli bulunan başvurular için sertifika üretim süreci başlatılır.

Sertifika başvurusunda bulunulmuş olması, sertifika üretimini zorunlu kılmaz. Usulüne uygun yapılmayan başvurular geri çevrilir ve sertifika üretimi yapılmaz.

#### 4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin ESHS'nin eline geçmesinin ardından en fazla 5 (beş) iş günü içinde sertifika başvurusu işleme alınır.

### 4.3. Sertifikanın Oluşturulması

#### 4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

ESHS tarafından değerlendirilen ve uygun bulunan sertifika başvuruları için, sertifika üretim aşamasına geçilir. Bu işlemin nasıl yapılacağı SUE'de anlatılır.

#### 4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Anahtar çiftlerinin ESHS tarafından üretilmesine müteakip sertifika, sahibine imza oluşturma verisiyle birlikte güvenli elektronik imza oluşturma aracı içinde teslim edilir. Sertifika sahibi kendisine gönderilen güvenli elektronik imza oluşturma aracını teslim aldığı anda, sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

### 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 hata olması ya da donanım sorunlarının olması durumunda ESHS'yi bilgilendirir.

#### 4.4.2. Sertifikanın ESHS Tarafından Yayınlanması

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

#### 4.4.3. Sertifikanın Oluşturulmasının Diğer Tarafalara Duyurulması

Sertifikanın oluşturulması, kurumun talep etmesi durumunda, ESHS tarafından, internetten erişimi sağlanan raporlar ya da e-posta ile kuruma bildirilir.

### 4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

#### 4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

Sertifika sahipleri, ilgili imza oluşturma verilerini elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza oluşturmak amacıyla kullanırlar. Sertifikalarla ilgili imza oluşturma verileri, güvenli elektronik imza oluşturma amacı dışında kullanılmaz. İmza oluşturma verisinin güvenli elektronik imza oluşturma amacı dışında kullanılması sonucu oluşabilecek zararlardan sertifika sahibi sorumludur.

Sertifika sahibi, geçerlilik süresi dolmuş veya iptal olmuş sertifikalara ait imza oluşturma verilerini kullanarak yasal geçerliliği olan işlem yapamaz.

#### 4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Üçüncü kişiler, oluşturulmuş güvenli elektronik imzayı doğrulama işlemini, sertifika içeriğinde bulunan imza doğrulama verisini kullanarak yapar. Sertifika içeriğindeki imza doğrulama verileri, üçüncü kişilerce imza doğrulaması dışında kullanılmaz.

İmza doğrulama verisinin veya sertifikanın, güvenli elektronik imza doğrulaması dışında kullanılması sonucu oluşabilecek zararlardan, üçüncü kişiler sorumludur.

#### 4.6. Sertifika Süresinin Uzatılması

Sertifika süresinin uzatılması, kullanım süresi dolan sertifikalarda, sertifikada yer alan bilgiler değişmeden aynı anahtar çifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. ESHS bu işlemi gerçekleştirmez.

#### 4.7. Sertifika Yenileme

ESHs, sertifika yenileme işlemini, yeni anahtar çifti üretmek sureti ile yerine getirir.

##### 4.7.1. Sertifika Yenileme Koşulları

Sertifika yenileme işlemi:

- Güvenli elektronik imza oluşturma aracının kayıp edilmesi, veya çalınması durumunda,
  - Güvenli elektronik imza oluşturma aracının arızalanması durumunda,
  - Güvenli elektronik imza oluşturma aracı erişim verisinin kayıp edilmesi, çalınması veya unutulması durumunda,
  - Elektronik sertifikanın iptal edilmesi ve yenisinin talep edilmesi durumunda,
  - Elektronik sertifikanın geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaşılması durumunda,
  - Elektronik sertifikada bilgi değişikliği gerekmesi durumunda,
- yapılmaktadır.

##### 4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

##### 4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

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 Koşulu

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 Diğer Taraplara Duyurulması

Bölüm 4.4.3’de tanımlanmaktadır.

### 4.8. Sertifikada Bilgi Değişikliği

Sertifikada bilgi değişikliği, anahtar çifti hariç sertifikada yer alan bilgilerin değişmesi olarak tanımlanır.

Sertifikada yer alan bilgilerde değişiklik olması, sertifikanın değiştirilmesini gerektirir. ESHS, sertifikada bilgi değişikliği gerçekleştirmez. Sertifikada bilgi değişikliği gerekli ise anahtar yenileme ile yeni bir sertifika üretilir.

### 4.9. Sertifikanın İptali ve Askıya Alınması

#### 4.9.1. Sertifikanın İptal Edildiği Durumlar

Sertifikanın, kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda, sertifika iptal edilir. İptal edilen sertifika ile ilgili imza oluşturma verisi ile bir daha işlem yapılmaz. Sertifika, aşağıda belirtilen;

- 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,
- 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 Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, kurum ile imzalanan sözleşmeler, Sİ veya SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,

- Kamu SM'nin NES'i imzalamak için kullandığı imza oluŐturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması,
- Kamu SM'nin işleyişine son verilmesi ve verilen NES'lerin yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması

durumlarında iptal edilir.

#### 4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir;

- Sertifika sahibinin kendisi,
- Kurum,
- Kamu SM, madde 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

#### 4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Bireysel sertifika iptal başvurusu internet üzerinden veya telefonla yapılabilir.

Kurumun iptal başvurularını ne şekilde yapacağı SUE dokümanında anlatılır.

Kamu SM tarafından gerçekleştirilen iptaller sonrası, sertifika sahibi ve bağılı bulunduğu kurum bilgilendirilir.

Geçerli iptal başvurusunun alınmasından sonra sertifika derhal iptal edilir.

#### 4.9.4. İptal İsteğı Ertelenme Süresi

Böyle bir süre öngörülmemiŐtir.

#### 4.9.5. İptal İsteğinin İşlenme Süresi

Geçerli bir sertifika iptal talebi geldikten sonra, ESHS, sertifika iptal talebini derhal işleme alır.

#### 4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliğı

Üçüncü kişilerin, sertifika sahiplerine ait sertifikaları işleme almadan önce, geçerlilik durumlarını ESHS'nin işaret ettiği internet ortamından edinebilecekleri SİL dosyasından veya tanımlanan diğere yöntemler aracılığıyla kontrol edip öğrenme sorumluluğı vardır.

Kamu SM, sertifikaların iptal edildiğı zamanın tam olarak tespit edilmesini sağlayan, üçüncü kişilerin herhangi bir kimlik doğrulamasına gerek olmaksızın kesintisiz ve ücretsiz olarak ulaşabileceğı şekilde iptal durum kaydını yayımlar. İptal edilen sertifika bilgisi, iptal durum kayıtlarında yer alır. Kayıtların bir sonraki güncelleme zamanı, söz konusu kayıtlarda açıkça gösterilir.

Sertifika iptal durum kaydının duyurulması için kullanılan yöntemlerden biri, "Sertifika İptal Listesi (SİL)" yayımlamaktır. İptal edilen sertifikalar, sertifikanın geçerlilik süresinin sonuna kadar SİL içinde tutulur. Sertifikanın iptal durum kaydına erişim, internet üzerinden çevrim içi yöntemlerle de

sağlanabilir. SİL veya çevrim içi iptal durum kaydına erişimin sağlanacağı internet adresleri SUE dokümanında belirtilir.

#### 4.9.7. Sertifika İptal Listesi Yayınlama Sıklığı

NES için SİL'ler internet ortamından en geç 1 (bir) günlük periyodik aralıklarla yayımlanır. Bir sonraki SİL yayınlama tarihi, duyurulan zamandan daha önce olabilir.

ESHS sertifikaları için SİL yayınlanma sıklığı 1 (bir) yıldan fazla olamaz.

SİL yenileme aralığı ESHS tarafından, sertifikaların kullanım amacının kritikliği doğrultusunda tespit edilir ve SUE'de belirtilir.

#### 4.9.8. Sertifika İptal Listesi Yayınlama Gecikme Süresi

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

#### 4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

ESHS, SİL yanında ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü) hizmeti de sağlar.

#### 4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

Çevrim içi sertifika iptal durum kayıtları, iptal bilgisinin daha hızlı ve sisteme daha az yük getirecek biçimde duyurulmasını sağlayabilir. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları gerekir.

#### 4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

ESHS, bu dokümanda belirtilmeyen ancak yaygınlıkla kullanılmaya başlanan diğer sertifika iptal durum kaydı bildirim yöntemlerini de destekleyebilir. Bu yöntemlerin neler olduğunu SUE dokümanında açıklar. Kullanılan yöntemler iptal durum kaydının bütünlüğünü ve ESHS tarafından yayımlandığını doğrulayacak şekilde tanımlanmış olmalıdır.

#### 4.9.12. İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunun, sertifikanın iptal nedeni olması dışında herhangi bir husus öngörülmemiştir.

#### 4.9.13. Sertifikanın Askıya Alındığı Durumlar

Askıya alma işlemi, sertifikanın geçici süre iptal edilmesi amacıyla tanımlanmıştır. Askıya alınmış bir sertifika iptal olmuş muamelesi görür. Ancak askıdan çıkartıldığında, yeniden geçerli bir sertifika olarak kullanılır.

Sertifikanın geçici olarak kullanım dışı olmasının istendiği durumlarda, sertifika sahibinin isteği doğrultusunda sertifika askıya alınır.

ESHS'lere ait sertifikalar askıya alınmaz.

#### 4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi

Askıya alma başvurusu sertifika sahibi tarafından yapılır.

#### 4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Askıya alma başvurusunun işlenme yöntemi, Bölüm 4.9.3’de belirtilen iptal başvurusu işlenme yöntemleri ile aynı biçimde yapılabilir.

#### 4.9.16. Askıda Kalma Süresi

Askıya alınan sertifika en az 1 (bir) kez SİL’de yayımlanmadan askıdan indirilemez.

### 4.10. Sertifika Durum Servisleri

Üçüncü kişiler sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılığıyla ulaşır.

#### 4.10.1. İşletimsel Özellikleri

SİL dosyası ESHS’ye ait bilgi deposunda güncel haliyle tutulur. SİL dosyasına erişmek isteyen üçüncü kişiler, SUE’de belirtilen erişim adreslerini kullanarak dosyayı kendi sistemlerine yüklerler. Bir sonraki SİL dosyasının yayımlanma tarihi bir öncekinde belirtilir. Güncel SİL dosyasına erişmek isteyen üçüncü kişilerin, her sertifika iptal durum kaydını öğrenmek istediklerinde, SİL dosyasını ESHS bilgi deposundan kendi sistemlerine indirerek, gerekli kontrolleri yapmaları önerilir.

ÇİSDUP servisinden sertifika iptal durumunun öğrenilebilmesi için, ilgili sertifika veya sertifikaları tanımlayan bilgiler ÇİSDUP İstemci tarafından ESHS ÇİSDUP Yanıtlayıcı’ya gönderilir. ÇİSDUP Yanıtlayıcı, sertifika veya sertifikaların iptal olup olmadığını anında istemciye bildirir.

#### 4.10.2. Servisin Erişilebilirliđi

SİL ve ÇİSDUP servislerinin verildiđi sistemlere erişim, ESHS tarafından kesintisiz olarak sağlanır. ESHS bu konuda gereken tüm tedbirleri alır, oluşan teknik problemleri en kısa zamanda giderir. Ancak, buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişilerin, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurması önerilir. Üçüncü kişilerin, erişimin kesilmesi sebebiyle iptal durum kaydını kontrol etmeden yaptıkları işlemlerden doğan zararlardan ESHS sorumlu tutulamaz.

#### 4.10.3. İsteđe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

### 4.11. Sertifika Sahipliđinin Sona Ermesi

Sertifika sahipliđi, sertifikanın kullanım süresinin sona ermesi, sertifikanın iptal edilmesi, ESHS’nin sertifika hizmetlerini sonlandırması ile sona erer.



#### 4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmaz.

## 5. Yönetim, İşlemsel ve Fiziksel Kontroller

Bu bölümde, ESHS tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan kontroller anlatılmıştır.

### 5.1. Fiziksel Güvenlik Denetimleri

ESHS sisteminin kurulu olduğu cihazlara, yetkisiz kişilerce erişim engellenir; hırsızlık, kaybolma gibi tehlikelere karşı gerekli önlemler alınır. Bunun için, sistemin kurulu olduğu binalar belirli güvenlik ihtiyaçlarını karşılar.

#### 5.1.1. Tesis Yeri ve İnşaatı

ESHS'ye ait yazılım ve donanım modüllerinin bulunduğu binalar, konum olarak güvenli yerlere inşa edilir. Bina, yüksek güvenlik gerektiren işlerin gerçekleştirilmesine imkan verecek ölçüde dışarıdan gelebilecek saldırılara karşı korumalıdır. Bina içinde, yazılım ve donanım modüllerinin yerleştirilmesi için kilitli ve giriş kontrollü odalar bulunur.

#### 5.1.2. Fiziksel Erişim

Binaya giriş, güvenlik görevlileri ve gerekli güvenlik donanımının sağladığı fiziksel kontrollerle yapılır. ESHS işlemlerinin gerçekleştirildiği yazılım ve donanım modülleri ile her türlü elektronik veya kağıt ortamda tutulan bilgilerin bulunduğu odalara, yetkisiz kişilerin erişiminin engellenmesi için gerekli önlemler alınır.

#### 5.1.3. Güç Kaynağı ve Havalandırma

ESHS işlemlerinin sürekliliği için sistem, kesintisiz güç kaynağı ile beslenir.

Bina gerekli havalandırma sistemi ile donatılır.

#### 5.1.4. Su Baskınları

ESHS'ye ait yazılım ve donanım modüllerinin bulunduğu ortamlarda, su baskınlarından en az zarar görecektir şekilde tedbirler alınır.

#### 5.1.5. Yangın Önleme ve Korunma

ESHS'ye ait yazılım ve donanım modüllerinin bulunduğu ortamlarda, yangını önleyen ve yangından korunmayı sağlayan tedbirler alınır.

#### 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

ESHS, 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

Sertifika ve bilgi sistemleri süreçlerinde kritik görevler üstlenen roller SUE dokümanında detaylandırılır.

#### 5.2.2. Her İşlem İçin Gereken Kişi Sayısı

ESHS, işlemin gereklerine bağlı olarak, bir işlemin gerçekleştirilebilmesi için birden fazla kişinin aynı anda hazır bulunmasını tanımlayabilir.

#### 5.2.3. Kimlik Doğrulama ve Yetkilendirme

ESHS çalışanlarının, sisteme erişimi ve işlemleri sırasında kimlikleri ve erişim yetkileri doğrulanır.

#### 5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

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

### 5.3. Personel Güvenlik Kontrolleri

#### 5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

ESHS bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam eder. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış kişilerdir.

#### 5.3.2. Geçmiş Araştırması

ESHS'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 ESHS gerekli güvenlik soruşturmasını yapar.

### 5.3.3. Eğitim Gereklere

Çalışanlar, gerekli öğrenim şartlarını sağlayan kişilerden seçilir ve ESHS işleyişinde yaptığı işle ilgili görev ve sorumluluklarının anlatıldığı eğitimden geçirilir. Tüm personele, ESHS tarafından uygulanan güvenlik ilkelerinin ve bu dokümanda belirtilen sertifika yönetimiyle ilgili ilkelerin neler olduğunun anlatıldığı temel farkındalık eğitimi verilir.

### 5.3.4. Sürekli Eğitim Gereklere ve Sıklığı

ESHS sisteminin işleyişinde yapılan her değişiklik personele, verilen eğitimlerle bildirilir. Yeni personelin işe başlamasında eğitimler tekrarlanır.

### 5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

### 5.3.6. Yetkisiz Eylemlerin Cezalandırılması

ESHS personelinin mevzuata aykırı işlem yapması halinde ilgili mevzuat gereğince işlem yapılır.

### 5.3.7. Anlaşmalı Personel Gereksinimleri

ESHS, kendi personeli olmayıp anlaşmalı olarak çalıştırdığı kişilerin gerekli güvenilirliği sağlaması için gereken kontrolleri yapar.

### 5.3.8. Sağlanan Dokümantasyon

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

## 5.4. Denetim Kayıtları

ESHS işleyişi sırasında gerçekleştirilen ve denetimi yapılmak istenen işlerin kayıtları tutulur. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

### 5.4.1. Kaydedilen İşlemler

Sistem güvenliğiyle ilgili işlemler ile sertifika yaşam döngüsü içinde gerçekleştirilen işlemler için, en azından aşağıdaki kayıtlar tutulmalıdır:

- Sertifika başvurusu ve başvuru onay kayıtları
- Sertifika yenileme başvurusu ve başvuru onay kayıtları
- Sertifika askıya alma ve iptal başvurusu ile başvuru onay kayıtları
- Sertifika üretim kayıtları
- Sertifika iptal kayıtları



- Sertifika askıya alma ve askıdan indirme kayıtları
- SİL üretim kayıtları
- Tutulan tüm kayıtların zamanı
- Süreçlerin işleyiői sırasında yapılan işlemler
- İşlemi yapan personelin kimlik bilgisi

#### 5.4.2. Kayıtların İncelenme Sıklığı

Tutulan kayıtlar, düzgün zaman aralıklarıyla incelenir. İncelemeler, güvenlik açıklarını uygun sürede yakalayabilecek sıklıkta yapılır.

#### 5.4.3. Kayıtların Saklanma Süresi

Kayıtlar, sistemin veri depolama kapasitesine göre, sistemde erişilebilir olarak tutulur. Ancak, yasalar gereğince daha uzun süre saklanması gereken kayıtlar arşivlenir. Arşivlenen kayıtlar ile ilgili bilgilendirme Bölüm 5.5’de yapılmıştır.

#### 5.4.4. Kayıtların Korunması

Kayıtlar, izinsiz izlenmeyi, değıştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur.

#### 5.4.5. Kayıtların Yedeklenmesi

Sistemin işleyiői ile ilgili elektronik kayıtlar, en azından her gün, sistemin yoğun olarak kullanılmadığı bir saatte yedeklenir. Sistem, geri kazanım işlevini yerine getirebilecek kapasitede olmalıdır. Herhangi bir arıza durumunda sistemin son durumuna dönebilmek için, alınan en son kayıt yedekleri sisteme yüklenir.

#### 5.4.6. Kayıtların Toplanması

Kayıtlar, elektronik olarak veya kağıt ortamda toplanır. Elektronik olarak toplanan kayıtlar, ESHS sisteminde tutulur; kağıt üzerindeki kayıtlar ise, ilgili ESHS çalışanı tarafından dosyalanır.

#### 5.4.7. Kayda Sebep Veren Tarafın Bilgilendirilmesi

Sistemde elektronik olarak yapılan sertifika başvurusunu onaylama, sertifikanın üretimi veya iptali gibi kritik işlemlerde kayda sebep olan taraf, kayıt hakkında bilgilendirilir.

#### 5.4.8. Saldırıya Açıklığın Değerlendirilmesi

Denetim kayıtlarının tahrifata, silinmeye ve kaçağına karşı korunması ve izinsiz erişimin engellenmesi için, kayıtlarının bulunduğu sistemler üzerinde elektronik ve fiziksel olarak gerekli güvenlik tedbirleri alınır.

## 5.5. Kayıt Arşivleme

Elektronik ya da kağıt üzerinde tutulan kayıtlar ESHS tarafından arşivlenir.

### 5.5.1. Arşivlenen Kayıt Bilgileri

Elektronik veya kağıt ortamda arşivlenmesi gereken kayıtlar şunlardır:

- Bölüm 5.4.1’de belirtilen, elektronik olarak kaydı yapılan tüm işlemler
- Üretilen tüm sertifikalar
- Yayınlanan tüm Sertifika İptal Listeleri
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Zaman Damgası İlkeleri
- Zaman Damgası Uygulama Esasları
- Sertifika taahhütnameleri
- Sözleşmeler
- Sertifika sahibinin sertifika başvurusu sırasında beyan ettiği kimlik bilgileri ve verdiği tüm belgeler
- Sertifika sahibinin çalıştığı kurum veya kuruluş tarafından beyan edilen bilgi ve belgeler
- İptal, askıya alma ve sertifika başvuru formları
- Verilen hizmetler sırasında yapılan önemli yazışmalar, alınan ve gönderilen faksler

### 5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler, Elektronik İmza Kanunu’nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik’te belirtilen süre boyunca saklanır.

### 5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler, izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Elektronik olarak tutulan arşivlerin, üzerinde kayıtlı bulunduğu elektronik ortamın bozulmasını önlemek için gerekli önlemler alınır. Kağıt üzerinde tutulan arşivler, her türlü yıpranma ve hasar görmeye karşı korunaklı ortamlarda tutulur.

### 5.5.4. Arşivlerin Yedeklenmesi

ESHS, ihtiyaç duyduğu durumlarda içeriğindeki bilginin güvenliğini bozmayacak şekilde arşivlerin yedeklerini alabilir. Yedeği alınan arşivler, orijinalleri ile aynı derecede güvenlik şartlarının sağlandığı ortamlarda tutulur.

#### 5.5.5. Kayıtların Zaman Damgası Gereksinimleri

ESHS gerekli gördüğü kayıtlara zaman damgası ekleyebilir.

#### 5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

#### 5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri, yetkili personelden edinilir. Aynı bilgiye ait birden fazla arşiv olması durumunda, arşivler kıyaslanarak doğruluğu kontrol edilir.

### 5.6. Anahtar Değişimi

ESHS'ye ait anahtarların ve sertifikaların, güvenlik sebeplerinden dolayı değiştirilmesi gerekebilir. Bu durumda eski anahtarlar, geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanır. ESHS'nin imza oluşturma verisinin değişiminden itibaren, yeni üretilen sertifikalar yeni imza oluşturma verisiyle imzalanır. Ancak, eskiden üretilmiş olan sertifikaların doğrulanabilmesi için, eski imza doğrulama verisinin içinde bulunduğu ESHS'ye ait eski sertifikaların erişilebilirliğinin sağlanması gerekir.

### 5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

#### 5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

ESHS, güvenliği tehlikeye düşürebilecek olayları en aza indiren ve herhangi bir felaket anında güvenliği en kısa zamanda yeniden sağlayan önlemleri alır.

#### 5.7.2. Donanım, Yazılım veya Veri Bozulması

ESHS, hizmeti kesintiye uğratan yazılım veya donanım arızalarında, iptal durum kaydını yayımladığı servislere öncelik vermek şartıyla en kısa zamanda gerekli düzeltmeleri yaparak sistemi yeniden işler hale getirir. ESHS'ye ait kayıtların yitirilmesi halinde yedekleme sistemleri aracılığıyla, ESHS sistemi tekrar işler hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün sertifika sahipleri ve kuruluşlar derhal bilgilendirilir. Gerekirse bazı sertifikalar iptal edilip, sertifika sahiplerine yeni sertifika üretilir.

#### 5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kullanıcı sertifikalarını imzalayan ESHS, imza oluşturma verisinin çalınması, bozulması, erişilememesi gibi durumlarda, kendisine ait sertifikasını iptal eder. Bu durumu, iptal sebebi ile birlikte en hızlı şekilde internet üzerinden duyurur ve ilgili tarafları bilgilendirir. Duyurunun yapılacağı internet adresi SUE dokümanında belirtilir. ESHS, sertifikasının iptal sebebine bağlı olarak sertifika sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı da yapar. ESHS kendi sertifikasını, imza oluşturma verisinin güvenliği veya gizliliğinin tehlikeye düşmesi durumunda iptal etmişse, ilgili taraflara eski sertifikalara güvenilmemesi konusunda ihtarda bulunur.

ESHS için, yeni anahtar çiftleri oluşturularak yeni bir sertifika üretilir. Üretilen yeni sertifika, mevzuta uygun olarak ilgili taraflara iletilir. Eski imza oluşturma verisi ile imzalanan son kullanıcı sertifikaları iptal edilir ve en kısa sürede yenilenen ESHS imza oluşturma verisi kullanılarak yeniden sertifikalar üretilir ve dağıtılır.

Sertifika sahibine ait güvenli elektronik imza oluşturma aracının ve imza oluşturma verisinin güvenliğinden şüphe edildiğinde, sertifika askıya alma/iptal işlemleri yapılır.

#### 5.7.4. Arıza Sonrası Yeniden Çalışırılık

ESHS, arıza sonrası çalışırılığın sağlanması için gerekli planları yapar ve önlemleri alır.

### 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 ilgili SUE'de tanımlanmıştır. ESHS sertifika hizmetlerine son verecek olursa, bu durumu 3 (üç) ay öncesinden tüm sistem bileşenlerine duyurur. ESHS sistemi ile ilgili tüm kayıtlar ve arşivler, uygun bir şekilde yönetmeliğe uygun süre boyunca korunur; kamuya açık bilgilere erişim, sistemin işlerliğine son verilmesinden sonra yönetmelikte belirtilen süre kadar devam eder. En son yayımlanan güncel SİL'ler, SUE'de belirtilen süre kadar erişime açık tutulur.

## 6. Teknik Güvenlik Kontrolleri

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

### 6.1. Anahtar Çifti Üretimi ve Kurulumu

#### 6.1.1. Anahtar Çifti Üretimi

##### 6.1.1.1. Elektronik Sertifika Hizmet Sağlayıcısı Anahtar Çiftinin Üretimi

ESHS'ye ait, sertifika imzalama amaçlı kullanılan anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, yazılım veya donanım aracı içinde üretilir. Anahtar üretiminde kullanılan algoritmalar ve anahtar uzunlukları, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde seçilir. Anahtar çiftlerinden imza oluşturma verisi, güvenli kriptografik donanım aracı içinde saklanır ve bu ortamdan yedekleme amacı dışında dışarıya çıkarılmaz. Üretilen anahtar çiftinin gerekli güvenlik şartlarını sağlaması için uygun üretim ve test yöntemleri kullanılır.

##### 6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Anahtar çiftleri, ESHS tarafından yetkisi olmayan personelin giremeyeceği gizli odada, yazılım veya donanım aracı içinde üretilir. Anahtar üretiminde kullanılan algoritmalar ve anahtar uzunlukları Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde seçilir. Anahtar çiftinin gerekli güvenlik şartlarını sağlaması için uygun üretim ve test yöntemleri kullanılır. Sertifika sahibine ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı içinde saklanır, kopyası veya anahtar çifti üretiminde kullanılan gizli değişkenler hiçbir şekilde sistemde tutulmaz.

##### 6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Üretilen imza oluşturma verisi, ilgili sertifika ile birlikte, güvenli elektronik imza oluşturma aracı içinde, sertifika sahibine kimlik kontrolü ve imza karşılığında teslim edilir.

Güvenli elektronik imza oluşturma aracı erişim verisi ise aşağıdaki yöntemlerle sertifika sahibine teslim edilir;

- Kapalı parola zarfı içinde imza karşılığı ve kimlik kontrolü yapılarak,
- Web üzerinden, güvenli bağlantı ve güçlü kimlik doğrulama gerçekleştirilerek.

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

Anahtar çiftleri ESHS tarafından üretildiği için imza doğrulama verisinin sertifika sahibi tarafından ESHS'ye ulaştırılmasına gerek yoktur.

##### 6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

ESHS'ye ait sertifikalar, internet ortamında ilgili tarafların erişimine hazır bulundurulur. Ayrıca, ESHS kendi sertifikasına ait sertifika özet değeri ile özetleme algoritmasını internet sitesi üzerinden

yayımlar ve faaliyete geçmesini müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur. Üçüncü kişiler, sertifika özet değerini, yayımlanan özet değeriyle kıyaslayarak sertifikanın güvenilirliğine karar verirler.

#### 6.1.5. Anahtar Uzunlukları

Belirlenen anahtar uzunlukları Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e uygundur.

#### 6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Anahtarların üretiminde, kriptografik açıdan gerekli güvenlik şartlarını sağlayan algoritma ve parametreler kullanılır. Anahtar üretme yöntemlerinin gerekli güvenlik şartlarını sağladığı, kriptografik testlerle ispatlanır.

#### 6.1.7. Anahtar Kullanım Amaçları

Üretilen sertifikalar ve ilgili imza oluşturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı üretmek ve doğrulamak amacıyla kullanılır.

ESHS'ye ait anahtar çiftleri sertifika imzalama, SİL imzalama, sertifika iptal durum kaydı imzalama ve ESHS'nin işleyişinde gerekli olduğu durumlarda elektronik imza, kimlik doğrulama, mesaj bütünlüğünün ve gizliliğinin sağlanması amacıyla kullanılır.

## 6.2. İmza Oluşturma Verisinin Korunması

### 6.2.1. Kriptografik Modül Standartları

ESHS'ye ait, sertifika imzalama amaçlı kullanılan imza oluşturma verisinin üretildiği veya saklandığı kriptografik modül ile sertifika sahibine ait güvenli elektronik imza oluşturma aracı, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen güvenlik standartlarını sağlar.

Kriptografik modül ve güvenli elektronik imza oluşturma aracı, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılmamasını ve gizli kalmasını sağlar; üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılmamasını ve elektronik imzanın sahteciliğe karşı korunmasını sağlayacak teknik özelliklere sahiptir.

### 6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

ESHS'ye ait imza oluşturma verisine erişim birden fazla kişinin kontrolünde sağlanır.

### 6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

#### 6.2.4. İmza OluŐturma Verisinin Yedeklenmesi

ESHS'ye ait imza oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı iinde yedeklenir. İmza oluŐturma verisinin yedeklenmesi iŐlemi, birden fazla yetkili alıŐanın ortak denetimi altındadır.

Sertifika sahiplerine ait imza oluŐturma verileri yedeklenmez.

#### 6.2.5. İmza OluŐturma Verisinin ArŐivlenmesi

ESHS'ye ve sertifika sahiplerine ait imza oluŐturma verileri arŐivlenmez. ESHS'ye ait imza oluŐturma verileri kullanım sureleri sonunda geri donuŐsz Őekilde silinir.

#### 6.2.6. İmza OluŐturma Verisinin Kriptografik Modle Yklenmesi

ESHS'ye ait imza oluŐturma verileri, gvenlik gereklerine uygun biimde kriptografik modl dıŐında retilbilir. Ancak, imza oluŐturma verisinin kriptografik modl iinde saklanması zorunludur. Kriptografik modl dıŐında retilen imza oluŐturma verisi, yetkili birden fazla personelin denetiminde modle yklenir.

Sertifika sahibinin imza oluŐturma verisinin, sertifika sahibine ait gvenli elektronik imza oluŐturma aracı dıŐında retilmesi durumunda, imza oluŐturma verisi gvenli elektronik imza oluŐturma aracı iine yetkili personelden baŐkasının giremediĐi gvenli odalarda ve Őifreli olarak yklenir. İmza oluŐturma verisinin gvenli elektronik imza oluŐturma aracı iinde retilmesi durumunda, aracın Elektronik İmza ile İlgili Srelere ve Teknik Kriterlere İliŐkin TebliĐ'de belirtilen gvenlik standartlarına uygunluĐu saĐlanır.

#### 6.2.7. İmza OluŐturma Verisinin Kriptografik Modlde Saklanması

ESHS'ye ait imza oluŐturma verileri yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik modl iinde Őifreli olarak tutulur. İmza oluŐturma verisinin kriptografik modl dıŐına ıkması engellenir.

Sertifika sahibine ait imza oluŐturma verisi sertifika sahibinin gvenli elektronik imza oluŐturma aracı iinde saklanır, gvenli elektronik imza oluŐturma aracı dıŐında baŐka bir ortamda bulunmaz. ESHS, sertifika sahiplerine ait imza oluŐturma verilerini kendi sistemi iinde saklamaz.

#### 6.2.8. İmza OluŐturma Verisine EriŐim

ESHS'ye ait imza oluŐturma verisi gvenli algoritma ve yntemlerle Őifreli olarak gvenli kriptografik modl iinde saklanır. İmza oluŐturma verisinin eriŐime aılması ve kullanılır duruma getirilmesi, yetkili birden fazla alıŐanın ortak denetimi altındadır.

Sertifika sahibine ait gvenli elektronik imza oluŐturma aracı iindeki imza oluŐturma verisine eriŐim, sadece sertifika sahibinin bildiĐi parola veya diĐer kriptografik yntemler ile saĐlanır.

#### 6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

İmza oluŐturma verisi imzalama iin kullanıldıktan sonra, 6.2.7’de tanımlanan Őekilde eriŐime yeniden aılıncaya kadar eriŐime kapalı tutulur.

#### 6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

ESHS’ye ait imza oluŐturma verilerinin aslı ve bütn yedekleri kullanım süresinin dolmasının ardından, bulunduĐu sistemden uygun yöntemlerle geri dnŐsz Őekilde silinir. İmza oluŐturma verisinin silinmesi, birden fazla yetkili alıŐanın ortak denetimi altındadır.

Sertifika sahiplerine ait imza oluŐturma verileri sadece sahibinde bulunduĐundan yok edilmesi sahibinin sorumluluĐundadır.

#### 6.2.11. Kriptografik Modln DeĐerlendirilmesi

ESHS, blm 6.2.1 de belirtilen standartlara uygun kriptografik modl kullanır.

### 6.3. Anahtar ifti Ynetimiyle İlgili DiĐer Konular

#### 6.3.1. İmza DoĐrulama Verisinin ArŐivlenmesi

ESHS’ye ve sertifika sahibine ait imza doĐrulama verilerinin iinde bulunduĐu sertifikalar yasa ve ilgili ynetmelikte belirtilen sre boyunca arŐivlenir. ArŐivde bulunduĐu sre boyunca, sertifikaların veri btnlĐnn saĐlanması iin gereken her trl nlem alınır.

#### 6.3.2. İmza OluŐturma ve DoĐrulama Verilerinin Kullanım Sreleri

İmza oluŐturma ve doĐrulama verilerinin kullanım sreleri, kullanım amalarına gre birbirlerinden farklı olabilir. İmza doĐrulama verisinin kullanım sresi, iinde bulunduĐu sertifikanın geerlilik sresidir.

ESHS’ye ait imza oluŐturma verisinin kullanım sresi ilgili mevzuatta tanımlanan sreden fazla olamaz ve sertifikanın kullanım sresi kadardır.

Sertifika sahiplerine ait imza oluŐturma verilerinin kullanım sresi sertifikanın kullanım sresi ile aynıdır. Kullanıcılara ait sertifikaların son kullanma tarihi, sertifikayı imzalayan ESHS’ye ait sertifikanın son kullanma tarihinden sonra olamaz.

### 6.4. EriŐim Denetim Verileri

EriŐim denetim verileri ESHS alıŐanlarının eriŐim parolalarını, gvenli donanım araları iindeki eriŐim denetimi saĐlayan diĐer verileri ve sertifika sahiplerinin gvenli donanım aralarına eriŐim parolalarını ierir.



#### 6.4.1. EriŐim Denetim Verilerinin OluŐturulması

ESHS sistemi iinde kullanılan eriŐim denetim verileri ile sertifika sahibine ait eriŐim parolaları yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda tahmin edilemez rastsallıkta üretilir.

#### 6.4.2. EriŐim Denetim Verilerinin Korunması

ESHS sistemi iinde kullanılan eriŐim denetim verileri yalnızca yetkili alıŐanlar tarafından bilinir, diĐer veriler ve bunları ieren güvenli donanım araları yetkisiz eriŐime karŐı güvenli saklanır.

Güvenli elektronik imza oluŐturma aracı eriŐim verisi ESHS’de bulunduĐu süre zarfında, güvenli bir ortamda Őifreli olarak saklanır.

#### 6.4.3. EriŐim Denetim Verileri İle İlgili DiĐer Konular

EriŐim denetimi verilerinin sahibine ulaŐtırılması güvenli yollarla yapılır. Sertifika sahibine ait eriŐim parolaları kapalı zarf iinde, kimlik kontrolü yapılarak imza karŐılıĐı ya da güvenli evrim ii yöntemlerle sahibine teslim edilir.

### 6.5. Bilgisayar GüvenliĐi Denetimleri

#### 6.5.1. Bilgisayar GüvenliĐi İle İlgili Teknik Gereker

ESHS sistemi iinde, son teknolojik geliŐmeler göz önünde bulundurularak bilgisayar güvenliĐi saĐlanır.

#### 6.5.2. Bilgisayar Sisteminin SaĐladıĐı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıŐtır.

### 6.6. YaŐam Döngüsü Teknik Denetimleri

#### 6.6.1. Sistem GeliŐtirme Denetimleri

Sistemin geliŐtirilmesi sırasında ortam ve personel güvenliĐi, kurulan yazılım ve donanım ürünlerinin güvenliĐi en güncel yöntemler göz önünde bulundurularak saĐlanır.

#### 6.6.2. Güvenlik Yönetimi Denetimleri

Sistem iindeki yazılım ve donanım ürünleri ile aĐ ortamının belirlenen güvenlik Őartlarını saĐlayıp saĐlamadıĐı, test cihazları ve test prosedürleri kullanılarak kontrol edilir.

#### 6.6.3. YaŐam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıŐtır.

### 6.7. Ađ Güvenliđi Denetimleri

ESHS sisteminde son teknolojik geliŐmeler göz önünde bulundurularak gerekli ađ güvenliđi denetimleri yapılır.

### 6.8. Zaman Damgası

ESHS sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'de belirtilen Őartlara 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

#### 7.1.1. Sürüm Numarası

ESHS "ITU-T X.509 V.3" sertifika standardını destekler.

#### 7.1.2. Sertifika Uzantıları

ESHS ve son kullanıcı sertifikaları içinde, ITU-T X.509 V.3 tarafından desteklenen bütün uzantılar kullanılabilir. NES profilleri oluşturulurken ETSI TS 101 862'de belirtilen yöntemler kullanılır. Kamu SM tarafından belirlenen ilkelere uygun sertifika üretim ve yönetimi yapıldığının belirtildiği uzantılarla ilgili açıklamalar aşağıda anlatılmıştır.

##### 7.1.2.1. Anahtar Kullanım Alanları Uzantısı

ESHS tarafından üretilen NES'lerin anahtar kullanım alanı uzantısında "inkar edilemezlik" tanımının tek başına veya "sayısal imza" tanımıyla birlikte kullanılması gerekir. Anahtar kullanımı ile ilgili diğer tanımlar sertifika içeriğinde bulunmaz.

Üretilen NES'ler içeriğinde tanımlanabilecek anahtar kullanım alanları kombinasyonları aşağıdaki tabloda verilmiştir:

**Tablo 1 NES Anahtar Kullanım Alanları**

Sertifikanın Tipi	İnkar Edilemezlik <sup>1</sup>	Sayısal İmza <sup>2</sup>	Anahtar Şifreleme <sup>3</sup> veya Anahtar Anlaşması <sup>4</sup>
NES	√		-
NES	√	√	-

<sup>1</sup> Non-Repudiation

<sup>2</sup> DigitalSignature

<sup>3</sup> KeyEncipherment

<sup>4</sup> KeyAgreement

ESHS'ye ait sertifikaların içindeki anahtar kullanım alanı uzantısında, "sertifika imzalama"<sup>5</sup> ve "SİL imzalama"<sup>6</sup> tanımları kullanılır.

#### 7.1.2.2. Nitelikli Sertifika İbaresini Uzantısı

ESHS tarafından üretilen NES'lerde "Nitelikli Sertifika İbaresini"<sup>7</sup> uzantısının bulunması zorunludur. Nitelikli olmayan sertifikalarda bu uzantı bulunmaz. "Nitelikli Sertifika İbaresini" uzantısının kullanımı ETSI TS 101 862'ye uygun olarak yapılır. Bu uzantı içerisinde aşağıdaki "ibare tanımlayıcılar"<sup>8</sup> mevcuttur:

- NES'in ETSI'ye uygunluğunun gösterilmesi amacıyla ETSI tarafından tanımlanan aşağıdaki "ibare tanımlayıcı" uzantısının içinde 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) }

- NES'in 5070 sayılı Elektronik İmza Kanunu'na uygunluğunun gösterilmesi amacıyla BTK tarafından tanımlanan aşağıdaki "ibare tanımlayıcı" ve ibarenin kendisi metin olarak uzantısının içinde bulunur. Bu ibare ve ibareye ait nesne tanımlama numarası aşağıda belirtilmiştir:

Nesne Tanımlama Numarası: 2.16.792.1.61.0.1.5070.1.1

{joint-iso-itu-t(2) ülke(16) tr(792) tk(61.0.1) nes-profili(5070) nes-ibaresini(1) nes-uygunlugu(1)}

"Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır."

Sertifikanın kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme de "Nitelikli Sertifika İbaresini Uzantısı" içinde ETSI TS 101 862'de belirtilen biçimde yapılır. Bu amaçla aşağıdaki "ibare 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

Kullanılan algoritmaların nesne tanımlayıcıları üretilen sertifikaların içeriğinde belirtilir.

<sup>5</sup> KeyCertSign

<sup>6</sup> CRLSign

<sup>7</sup> QcStatements

<sup>8</sup> StatementID

#### 7.1.4. İsim Alanı Biçimleri

Üretilen sertifikalardaki isim alanı, "ITU X.500 Distinguished Name (Ayırt edici isim)" biçimine uygundur.

#### 7.1.5. İsim Kısıtları

ESHS'nin ürettiği sertifikaların içinde kişiyi tekil olarak tanımlamayı sağlayacak nitelikte isim bilgileri kullanılır. Sertifika sahibinin ad ve soyadı bilgisi ile gerekiyorsa çalıştığı şirket veya kurumun bilgisi resmi kayıtlarda geçen isimlerden oluşmak zorundadır.

Kamu SM'ye ait ESHS sertifikalarında tanımlanan isim alanları ve bu isim alanlarına yazılan bilgiler aşağıdaki tabloda belirtilmiştir. Sürüm X ibaresi rakam olarak 1 den başlar ve yeni Kök SHS ve Kamu ESHS sertifikası üretildiğinde rakam olarak bir sonraki değeri alır.

**Tablo 2 Sertifika İsim Alanları**

Alan Adı <sup>9</sup>	Kök SHS Sertifikası	Kamu ESHS Sertifikası
<b>CN</b>	Kamu SM Kök Sertifika Hizmet Sağlayıcısı [Sürüm X]	Kamu Elektronik Sertifika Hizmet Sağlayıcısı [Sürüm X]
<b>OU</b>	BİLGEM	BİLGEM
<b>O</b>	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK
<b>L</b>	Gebze-Kocaeli	Gebze-Kocaeli
<b>C</b>	TR	TR

#### 7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bu Sİ dokümanına ait nesne tanımlama numarası bu dokümanın 1.2. Bölüm'ünde verilmiştir.

#### 7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

<sup>9</sup> CN: Common Name [Genel isim], O: Organization [Organizasyon adı], OU: Organization Unit [Organizasyon birimi], L: Locality [Şehir], C: Country [Ülke]

### 7.1.8. İlke Niteleyiciler

ESHS'lere ait elektronik sertifikaların Kamu SM Sİ dokümanına uygunluğu "Sertifika İlkeleri Uzantısı" içine Sİ dokümanına ait nesne tanımlama numarasının yazılmasıyla belirtilir. "Sertifika İlkeleri Uzantısı"<sup>10</sup> içindeki "İlke Niteleyici"<sup>11</sup> olarak belirtilen alana ESHS'ye ait SUE dokümanının erişilebileceği internet adresi tanımlanır.

ESHS'ler Kamu SM tarafından belirlenen ilke ve esasların yanında başka kurumlar tarafından belirlenen ilke ve esaslara da uygun olarak çalışabilir. Bu durumda ESHS veya son kullanıcı sertifikalarının içinde Kamu SM Sİ nesne tanımlama numarasının yanında başka Sİ dokümanlarına referans veren nesne tanımlama numaraları da bulunur.

Kullanıcı sertifikalarının "Sertifika İlkeleri Uzantısı" içine Sİ dokümanına ait nesne tanımlama numarası, "İlke Niteleyici" olarak belirtilen alana, Kamu SM'nin belirlediği ilkelere uygun olarak yazılmış SUE dokümanının bulunduğu internet adresi yazılır. Kamu SM tarafından tanımlanan nitelikli sertifika ibaresi "Kullanıcı Bildirim"<sup>12</sup> alanına yazılır. Kamu SM tarafından tanımlanan nitelikli sertifika ibaresi aşağıda verilmiştir:

"Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır."

### 7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

## 7.2. Sertifika İptal Listesi Biçimi

### 7.2.1. Sürüm Numarası

ESHS'nin ürettiği SİL'ler "ITU X.509 V.2" SİL formatına uygundur.

### 7.2.2. Sertifika İptal Listesi Uzantıları

SİL uzantıları ile ilgili detay SUE dokümanında yer almaktadır.

## 7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

### 7.3.1. Sürüm Numarası

Çevrim İçi Sertifika Durum Protokolü RFC 6960'da belirtilen versiyonları destekler.

---

<sup>10</sup> Certificate Policies

<sup>11</sup> Policy Identifier

<sup>12</sup> User Notice



7.3.2. ÇİSDUP Uzantıları

Çevrim İçi Sertifika Durum Protokolü RFC 6960'da tarif edilen "ÇİSDUP" formatını destekler.

## 8. Uygunluk Denetimleri

Bu bölüm, Kamu SM Sİ dokümanına baęlı olarak çalıştığını beyan eden ESHS'lerin denetlenmesi ile ilgili hususları kapsamaktadır.

ESHS, mevzuat gereęi BTK tarafından incelenir/denetlenir.

ESHS, ek olarak ISO/IEC 27001 bilgi güvenlięi yönetim standardına uygun olarak hizmet verir ve standart gereęi düzenli olarak iç ve dış denetimlere tabi tutulur.

ESHS iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

### 8.1. Uygunluk Denetiminin Sıklığı

Bu Sİ dokümanına uygun çalışan ESHS'ler, iki yılda en az bir defa BTK tarafından denetlenir.

ISO/IEC 27001 bilgi güvenlięi yönetim sistemi standardı gereęince yılda bir defa uygunluk denetimi gerçekleştirilir. Her üç yılda bir sertifika yenilenir.

İç denetim, yılda en az bir defa gerçekleştirilir. Gerekli hallerde denetim sayısı artırılabilir.

### 8.2. Denetçinin Nitelikleri

ESHS faaliyetlerinin denetimi, kanunla yetkilendirilmiş olan BTK tarafından gerçekleştirilir.

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir.

### 8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi

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

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir.

### 8.4. Denetimin Kapsamı

ESHS'lerin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek ESHS personeli tarafından belirlenir.

### 8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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



ISO/IEC 27001 standardına göre gerekleŐtirilen denetimlerde ortaya ıkan eksiklikler, ESHS tarafından planlı alıŐma ile giderilir. Eksiklikler, BGYS'nin temel iŐleyiŐini etkileyecek kadar byk ise, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

İ denetimlerde ortaya ıkan eksiklikler, ESHS ilgili personeli tarafından giderilir.

### 8.6. Sonucun Bildirilmesi

BTK ve ISO/IEC 27001 denetilerinin hazırladıĐı resmi raporlar ESHS'ye bildirilir.

İ denetim sonucu, ESHS st ynetimine raporlanır.

## 9. Diğer İşler ve Hukuksal Meseleler

### 9.1. Ücretlendirme

#### 9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

ESHS tarafından üretilen, güncellenen ve yenilenen her sertifika için ücret alınır. Ödenecek bedelin miktarı ile ilgili bilgilendirmenin ne şekilde yapıldığı SUE dokümanında belirtilir.

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

#### 9.1.2. Sertifika Erişim Ücreti

ESHS, kendisine ve sertifika sahiplerine ait sertifikaları ücretsiz olarak erişime açar.

#### 9.1.3. İptal Durum Kaydına Erişim Ücreti

ESHS, iptal durum kaydını duyurmak için sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

#### 9.1.4. Diğer Servis Ücretleri

ESHS, 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

ESHS kendi sorumluluklarını karşılamak amacıyla sigorta yaptırabilir.

#### 9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

#### 9.2.3. Sertifika Mali Sorumluluk Sigortası

ESHS'nin dağıttığı NES'ler, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalanır.

### 9.3. Ticari Bilginin Korunması

#### 9.3.1. Gizli Bilginin Kapsamı

Paylaşılan iş planları, satış bilgileri, ticari sırlar ve yapılan gizli anlaşmalarda verilen bilgiler, ticari bilgi olarak değerlendirilir.

#### 9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

ESHS'nin kendi güvenliğini sarsmayacak şekilde, yönetsel ve teknik bilgi ile güvenlik stratejisini gerçekleştirme yolu gizlilik kapsamında olmayan bilgilerdir.

#### 9.3.3. Gizli Bilginin Korunma Sorumluluđu

Sertifika hizmeti verilirken ESHS ve ilgili kuruluşların karşılıklı paylaştığı ticari bilgiler üçüncü taraflara açılmaz.

### 9.4. Kişisel Bilginin Gizliliđi

#### 9.4.1. Gizlilik Planı

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diđer paydaşların kişisel verilerinin gizliliđini 5070 ve 6698 sayılı kanunlar kapsamındaki mer'i mevzuata uygun olarak sağlar.

#### 9.4.2. Gizli Olarak Tanımlanan Bilgiler

Sertifika başvurusu sırasında ve sonrasında kimlik tanımlama ve doğrulama ile sertifika yönetim işlemleri içinde kullanılmak üzere toplanan, ancak sertifikanın içinde yer almayan sertifika sahiplerine ait bilgiler, kişisel gizli bilgi kapsamına girer.

#### 9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Sertifika içeriğinde bulunan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediđi sürece gizli bilgi kapsamında değerlendirilmez.

#### 9.4.4. Gizli Bilginin Korunma Sorumluluđu

ESHS, 5070 sayılı Elektronik İmza Kanunu uyarınca kişilere ait gizli bilgilerin korunması için aşağıda belirtilen şartları yerine getirir:

- Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler haricinde bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,
- Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceđi ortamlarda bulunduramaz,
- Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

#### 9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

ESHS, sertifika talep eden kişinin onayı ve yazılı rızası olması durumunda, kişisel verileri üçüncü kişilere verebilir.

#### 9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

#### 9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

### 9.5. Telif Hakları

Bu Sİ dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

### 9.6. Temsil Hakkı ve Yükümlülükler

ESHS'nin verdiği sertifika hizmetlerinde sistem bileşenleri olan ESHS'ler, sertifika sahipleri ve üçüncü kişiler 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 belirtilen şekilde üzerlerine düşen yükümlülükleri sağlarlar. ESHS'ler, sertifika sahipleri ve üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, karşılıklı imzaladıkları sözleşmelerde, taahhütnamelerde, Sİ, SUE, Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları dokümanlarında sözü geçen yükümlülükleri de yerine getirirler.

#### 9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

Elektronik imzaya ilişkin mevzuata uygun olarak elektronik sertifikaları üretmek, sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek, yenileme, askıya alma ve iptal gibi sertifika işlemlerinin gerçekleştirilmesini sağlamak, iptal olmuş sertifika bilgilerini zamanında ve doğru olarak duyurmak, sertifikanın veya sertifika işlemleriyle ilgili başvuruların durumu hakkında ilgili kişileri bilgilendirmekle yükümlüdür.

#### 9.6.2. Kayıt Birimi Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

#### 9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibi başvuru, yenileme, askıya alma ve iptal işlemlerini Kamu SM sertifika ilkelerinde belirtilen yöntemlere uygun olarak tanımlanmış usule göre yerine getirmek, sertifikasını ve ilgili imza oluşturma verisini, varsa taraflar arası sözleşme veya taahhütnameler ile Sİ ve SUE dokümanlarında belirtildiği şekilde kullanmak, imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kayıp ve üçüncü kişilerin yetkisiz kullanımı durumlarına karşı Bölüm 6.1, 6.2 ve

6.4'de belirtilen şekillerde gereken önlemleri almak, imza oluŐturma verisinin güvenliĐinin yitirildiĐinden ŐüphelendiĐi durumlarda sertifikasını iptal ettirmek, sertifika baŐvurusu sırasında doĐru bilgi beyan etmekle ykmldr.

Blm 1.4'te belirtilen sertifika kullanım amaları dıŐındaki kullanımlarda kendisinin ve nc kiŐilerin grebileceĐi zararlar, kendisine ait imza oluŐturma verisi kullanılarak yapılan iŐlemler, elektronik imza oluŐturma verisini kullandıĐı sırada sertifikasının geerli (kullanım sresinin dolmamıŐ olması ve iptal edilmemiŐ/askıya alınmamıŐ olması) durumda olması sertifika sahibinin ykmllkleri arasındadır.

Yukarıda beyan edilen ykmllklerin ihlali nedeniyle nc kiŐilerin zarara uĐraması halinde ESHS'nin demek zorunda olduĐu tazminatlarla ilgili sertifika sahibine rcu hakkı saklıdır.

#### 9.6.4. nc KiŐilerin Ykmllkleri

nc kiŐiler, sertifikaları kullanmadan nce gerekli geerlilik kontrollerini yapmakla ykmldr. nc kiŐiler, sertifikanın geerlilik kontroln yapıp yapmamaya veya geerlilik kontroln ne Őekilde yapacaklarına kendileri karar verirler. Sertifikaları uygun geerlilik denetimlerini yapmadan kullandıĐı takdirde doĐabilecek zararlardan sorumludur.

ESHS'nin yayımladıĐı SUE dokmanı nc kiŐilerin yapması gereken sertifika geerlilik kontrollerinin neler olması gerektiĐini belirtir.

#### 9.6.5. DiĐer BileŐenlerin Ykmllkleri

DiĐer bileŐenlerin ykmllkleri SUE dokmanında anlatılmaktadır.

### 9.7. Ykmllklerden Feragat

ESHS ile sertifika sahipleri ve kurumlar arasındaki ykmllk karŐılıklı imzalanan szleŐmelerde veya taahhnamelerde belirtildiĐi Őekilde sona erer.

### 9.8. Sorumlulukla İlgili Sınırlamalar

ESHS ve sertifika hizmeti alan tarafların sorumlulukları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomnikasyon Kurumu'nun yayımladıĐı Elektronik İmza Kanunu'nun Uygulanmasına İliŐkin Usul ve Esaslar Hakkında Ynetmelik, Elektronik İmza ile İlgili Srelere ve Teknik Kriterlere İliŐkin TebliĐ'de belirtilen Őartlar ile sınırlıdır.

### 9.9. Tazminat Halleri

ESHS ve sertifika hizmeti alan taraflar arasında yasa ve ynetmelikte belirtilen ykmllklerin yerine getirilmemesinden kaynaklanan zararlar, tarafların o ana kadar somut olarak gerekleŐmiŐ hak ve alacakları korunmak suretiyle tasfiye edilir.

## 9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

### 9.10.1. Anlaşma Süresi

Sertifika hizmetlerinin gerçekleştirilmesinde ESHS ile sertifika sahipleri ve ilgili kuruluşlar karşılıklı imzaladıkları sözleşmeler veya taahhütnameler süresince işbirliği içinde çalışır; süreçleri yerine getirirken gerekli desteği ve koordinasyonu Sİ ve SUE dokümanlarında belirtilen şartlar altında sağlar.

### 9.10.2. Anlaşmanın Sona Ermesi

ESHS ile sertifika hizmetlerini alan taraflar arasında imzalanan sözleşmeler veya taahhütnameler, sözleşme veya taahhütnameye uygun olarak yapılan taleple sonlandırılabilir. Anlaşmanın sonlandırıldığı durumlar SUE dokümanında anlatılır.

### 9.10.3. Anlaşmanın Sona Ermesinin Etkileri

ESHS ile sertifika hizmetlerini alan taraflar arasında imzalanan sözleşme veya taahhütnamenin sona ermesi ile sertifika hizmeti alan tarafların Sİ ve SUE dokümanları ile ilgili yükümlülükleri sona erer. Ancak ESHS, dağıttığı NES'lerle ilgili, elektronik imza mevzuatında belirtilen yükümlülüklerini yerine getirmeye devam eder.

## 9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Sertifika yönetim prosedürleri içindeki kritik her işlem sonrasında ESHS sertifika sahibini bilgilendirir. ESHS ile sertifika sahipleri arasındaki haberleşmeler posta yoluyla, telefonla veya elektronik ortam üzerinden yapılır.

## 9.12. Değişiklik Halleri

### 9.12.1. Değişiklik Metodları

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

### 9.12.2. Bilgilendirme Mekanizması ve Sıklığı

Sİ dokümanında yapılan değişiklikler dokümanın yenilenerek, bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer. Sİ'de yapılan değişiklikler 7 (yedi) gün içinde Telekomünikasyon Kurumu'na bildirilir.

### 9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Kamu SM'nin, Sİ dokümanında belirlediği ilkelerde yaptığı değişiklikler, sertifika kullanım amaç ve hedeflerini temel anlamda değiştirmedeği sürece yeni Sİ dokümanı için yeni bir nesne tanımlama

numarası almasına gerek yoktur. Kamu SM eski kullandığı nesne tanımlama numarasını yeni Sİ dokümanı için de kullanabilir. Ancak, sertifika ilkelerinde yaptığı değişiklikler sertifikanın kullanım amacını değiştiriyorsa Kamu SM'nin yeni belirlediği Sİ dokümanı için yeni bir nesne tanımlama numarası alması zorunludur.

### 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 veya taahhütnameler, Kamu SM Sertifika İlkeleri ve ilgili ESHS'ye ait Sertifika Uygulama Esasları dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

### 9.14. Uygulanacak Hukuk

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

### 9.15. Uygulanabilir Yasalarla Uyum

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

### 9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.