



# SERTİFİKA İLKELERİ (Sİ)

**SÜRÜM** : 02

**TARİH** : 20.08.2007



<b>1. GİRİŞ .....</b>	<b>10</b>
<b>1.1. Genel Bakış .....</b>	<b>10</b>
<b>1.2. Kitapçık Adı ve Tanımlama .....</b>	<b>10</b>
<b>1.3. Taraflar.....</b>	<b>11</b>
1.3.1. Sertifika Üretim Merkezleri .....	11
1.3.2. Sertifika Kayıt Merkezleri.....	11
1.3.3. Sertifika Sahipleri .....	11
1.3.4. Üçüncü Kişiler .....	11
1.3.5. Diğer Taraflar.....	11
<b>1.4. Sertifika Kullanımı .....</b>	<b>12</b>
1.4.1. Geçerli Sertifika Kullanım Şekilleri .....	12
1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri .....	12
<b>1.5. Sertifika İlkeleri Yönetimi.....</b>	<b>12</b>
1.5.1. Sİ Kitapçığından Sorumlu Organizasyon .....	12
1.5.2. İletişim Noktası .....	12
1.5.3. SUE'nin İlkelere Uygunluğunun Belirlenmesi .....	13
1.5.4. SUE Onaylama Prosedürleri.....	13
<b>1.6. Kısaltmalar ve Tanımlar .....</b>	<b>13</b>
1.6.1. Kısaltmalar.....	13
1.6.2. Tanımlar .....	13
<b>2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI .....</b>	<b>16</b>
<b>2.1. Bilgi Deposu .....</b>	<b>16</b>
<b>2.2. Sertifikasyon Bilgisinin Yayımlanması.....</b>	<b>16</b>
<b>2.3. Yayımin Zamanı veya Sıklığı .....</b>	<b>16</b>
<b>2.4. Bilgi Deposuna Erişim Kontrolleri .....</b>	<b>16</b>
<b>3. KİMLİĞİN DOĞRULANMASI .....</b>	<b>17</b>
<b>3.1. İsimlendirme.....</b>	<b>17</b>
3.1.1. İsim Tipleri.....	17
3.1.2. İsimlerin Anlamlı Olması Gerekliliği .....	17
3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği.....	17
3.1.4. İsim Biçimlerinin Değerlendirilmesi .....	17
3.1.5. İsimlerin Benzersizliği .....	17
3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü .....	17
<b>3.2. İlk Kimlik Doğrulama .....</b>	<b>17</b>
3.2.1. İmza Oluşturma Verisine Sahip Olunduğunun Kanıtlanma Metodu .....	17
3.2.2. Ticari Unvanın Doğrulanması.....	17
3.2.3. Kimliğin Doğrulanması .....	17

3.2.4.	Doğrulanmamış Sertifika Sahibi Bilgisi .....	18
3.2.5.	Yetkinin Doğrulanması .....	18
3.2.6.	Uyumlu Çalışabilirlik Kriterleri .....	18
<b>3.3.</b>	<b>Anahtar Yenileme Taleplerinin Doğrulanması .....</b>	<b>18</b>
3.3.1.	Rutin Anahtar Yenileme için Kimlik Doğrulama .....	18
3.3.2.	İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama .....	18
<b>3.4.</b>	<b>İptal Talebi için Kimlik Doğrulama .....</b>	<b>18</b>
<b>4.</b>	<b>SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ .....</b>	<b>19</b>
<b>4.1.</b>	<b>Sertifika Başvurusu .....</b>	<b>19</b>
4.1.1.	Kimler Sertifika Başvurusunda Bulunabilir? .....	19
4.1.2.	Sertifika Başvuru Kayıtları ve Sorumluluklar .....	19
<b>4.2.</b>	<b>Sertifika Başvurusunun İşlenmesi .....</b>	<b>19</b>
4.2.1.	Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi .....	19
4.2.2.	Sertifika Başvurularının Kabulü veya Reddedilmesi .....	20
4.2.3.	Sertifika Başvurularının İşlenme Süresi .....	20
<b>4.3.</b>	<b>Sertifika Üretimi .....</b>	<b>20</b>
4.3.1.	Sertifika Üretimi Sırasındaki ESHS Faaliyetleri .....	20
4.3.2.	Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi .....	20
<b>4.4.</b>	<b>Sertifikanın Kabulü .....</b>	<b>21</b>
4.4.1.	Kabulün Şekli .....	21
4.4.2.	ESHS Tarafından Sertifikanın Yayınlanması .....	21
4.4.3.	Diğer Tarafların Sertifika Üretimiyle İlgili Bilgilendirilmesi .....	21
<b>4.5.</b>	<b>Anahtar Çifti ve Sertifika Kullanımı .....</b>	<b>21</b>
4.5.1.	Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı .....	21
4.5.2.	Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı .....	22
<b>4.6.</b>	<b>Sertifika Yenileme .....</b>	<b>23</b>
4.6.1.	Sertifika Yenilemeyi Gerektiren Durumlar .....	23
4.6.2.	Yenileme Talebinde Bulunabilecek Kişiler .....	23
4.6.3.	Sertifika Yenileme Talebinin İşlenmesi .....	23
4.6.4.	Yenilenmiş Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi .....	23
4.6.5.	Yenilenen Sertifikanın Kabulü .....	23
4.6.6.	ESHS Tarafından Yenilenen Sertifikanın Yayınlanması .....	23
4.6.7.	Diğer Tarafların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi .....	24
<b>4.7.</b>	<b>Anahtar Yenileme .....</b>	<b>24</b>
4.7.1.	Anahtar Yenilemeyi Gerektiren Durumlar .....	24
4.7.2.	Anahtar Yenileme Talebinde Bulunabilecek Kişiler .....	24
4.7.3.	Anahtar Yenileme Talebinin İşlenmesi .....	24
4.7.4.	Yeni Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi .....	24
4.7.5.	Anahtar Yenilenen Sertifikanın Kabulü .....	24
4.7.6.	ESHS Tarafından Anahtar Yenilenen Sertifikanın Yayınlanması .....	24
4.7.7.	Diğer Tarafların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi .....	24
<b>4.8.</b>	<b>Sertifika Değişikliği .....</b>	<b>24</b>
4.8.1.	Sertifika Değişikliğini Gerektiren Durumlar .....	25

4.8.2.	Sertifika Değişiklik Talebinde Bulunabilecek Kişiler .....	25
4.8.3.	Sertifika Değişiklik Talebinin İşlenmesi .....	25
4.8.4.	Yeni Sertifika Üretimine İlgili Sertifika Sahibinin Bilgilendirilmesi.....	25
4.8.5.	Değişiklik Yapılmış Sertifikanın Kabul Şekli.....	25
4.8.6.	ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması.....	25
4.8.7.	Diğer Tarafların Yeni Sertifika Üretimine İlgili Bilgilendirilmesi .....	25
<b>4.9.</b>	<b>Sertifika İptali ve Askıya Alma .....</b>	<b>25</b>
4.9.1.	Sertifika İptalini Gerektiren Durumlar .....	25
4.9.2.	Sertifika İptal Talebinde Bulunabilecek Kişiler .....	25
4.9.3.	Sertifika İptal Talebi Prosedürleri .....	26
4.9.4.	Sertifika İptal Talebi Gecikme Periyodu .....	26
4.9.5.	TÜRKTRUST'ın Sertifika İptal Talebini İşleme Zamanı.....	26
4.9.6.	Üçüncü Kişilerin İptal Kontrol Gerekliliği .....	26
4.9.7.	Sertifika İptal Listesi (SİL) Yayımlama Sıklığı .....	27
4.9.8.	SİL'lerin En Geç Yayımlanma Zamanı .....	27
4.9.9.	Çevrim İçi Sertifika İptal/Durum Kontrol İmkani (OCSP).....	27
4.9.10.	Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri.....	27
4.9.11.	Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı .....	27
4.9.12.	Anahtar Güvenliğinin Yitirilmesi Durumlarına Özel Gereklilikler.....	27
4.9.13.	Sertifika Askıya Almayı Gerektiren Durumlar .....	27
4.9.14.	Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler .....	27
4.9.15.	Sertifika Askıya Alma Talebi Prosedürü.....	28
4.9.16.	Sertifikanın Askıda Kalma Süresinin Sınırları .....	28
<b>4.10.</b>	<b>Sertifika Durum Servisleri.....</b>	<b>28</b>
4.10.1.	İşlevsel Özellikler .....	28
4.10.2.	Hizmetin Sürekliliği .....	29
4.10.3.	İsteğe Bağlı Özellikler .....	29
<b>4.11.</b>	<b>Sertifika Sahipliğinin Sona Ermesi.....</b>	<b>29</b>
<b>4.12.</b>	<b>İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma.....</b>	<b>29</b>
4.12.1.	Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları.....	29
4.12.2.	Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları.....	29
<b>5.</b>	<b>TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER .....</b>	<b>30</b>
<b>5.1.</b>	<b>Fiziksel Kontroller .....</b>	<b>30</b>
5.1.1.	Tesis Yeri ve İnşaatı .....	30
5.1.2.	Fiziksel Erişim.....	30
5.1.3.	Güç Kaynakları ve Havalandırma .....	30
5.1.4.	Su Baskınları .....	30
5.1.5.	Yangın Önleme ve Yangından Korunma .....	30
5.1.6.	Saklama Ortamları .....	30
5.1.7.	Atıkların Atılması.....	30
5.1.8.	Tesis Dışı Yedekleme .....	30
<b>5.2.</b>	<b>Prosedürel Kontroller.....</b>	<b>31</b>
5.2.1.	Güvenilir Roller.....	31
5.2.2.	Her Görev İçin Gereken En Az Kişi Sayısı.....	31
5.2.3.	Her Görev için Kimlik Doğrulama .....	31
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller .....	32

<b>5.3. Personel Kontrolleri .....</b>	<b>32</b>
5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri .....	32
5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri .....	32
5.3.3. Eğitim Gereklilikleri .....	32
5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri .....	32
5.3.5. İş Rotasyonu Sıklığı ve Sırası .....	32
5.3.6. Yetkisiz İşlemler için Yaptırımlar .....	32
5.3.7. Bağımsız Alt Yüklenici Gereklilikleri .....	32
5.3.8. Personele Sağlanan Dokümantasyon.....	33
<b>5.4. Denetim Kayıtları Alma Prosedürleri .....</b>	<b>33</b>
5.4.1. Kaydedilen Olay Tipleri .....	33
5.4.2. Kayıtları İşleme Sıklığı .....	33
5.4.3. Denetim Kayıtlarının Saklanma Süresi .....	33
5.4.4. Denetim Kayıtlarının Korunması .....	33
5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri .....	33
5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış).....	33
5.4.7. Olayı Yaratan Kişiyi Bilgilendirme .....	33
5.4.8. Zarar Görebilirlik Değerlendirmesi.....	33
<b>5.5. Kayıtların Arşivlenmesi .....</b>	<b>34</b>
5.5.1. Arşivlenen Kayıt Tipleri .....	34
5.5.2. Arşivlerin Saklanma Süresi .....	34
5.5.3. Arşivlerin Korunması .....	34
5.5.4. Arşivlerin Yedeklenme Prosedürleri .....	34
5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri .....	34
5.5.6. Arşiv Toplama Sistemi.....	34
5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri .....	34
<b>5.6. Anahtar Değişimi .....</b>	<b>34</b>
<b>5.7. Güvenliğin Yitirilmesi ve Afet Durumlarında Yapılacaklar .....</b>	<b>34</b>
5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar .....	34
5.7.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması.....	34
5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi.....	35
5.7.4. Afet Sonrası İş Sürekliliği Yetenekleri .....	35
<b>5.8. TÜRKTRUST veya Kayıt Merkezi İşletmesine Son Verilmesi ...</b>	<b>35</b>
<b>6. TEKNİK GÜVENLİK KONTROLLERİ .....</b>	<b>36</b>
<b>6.1. Anahtar Çifti Üretimi ve Kurulumu .....</b>	<b>36</b>
6.1.1. Anahtar Çifti Üretimi .....	36
6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması .....	36
6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması .....	36
6.1.4. TÜRKTRUST İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması.....	37
6.1.5. Anahtar Uzunlukları .....	37
6.1.6. Anahtar Üretimi ve Kalite Kontrolü .....	37
6.1.7. Anahtar Kullanım Amaçları .....	37
<b>6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri.....</b>	<b>37</b>
6.2.1. Kriptografik Modül Standartları ve Kontroller .....	37
6.2.2. İmza Oluşturma Verisinin Çok Kullanımlı Kontrolü .....	37

6.2.3.	İmza Oluşturma Verisinin Saklanması .....	38
6.2.4.	İmza Oluşturma Verisinin Yedeklenmesi .....	38
6.2.5.	İmza Oluşturma Verisinin Arşivlenmesi .....	38
6.2.6.	İmza Oluşturma Verisinin Kriptografik Modül Transferi .....	38
6.2.7.	İmza Oluşturma Verisinin Kriptografik Modülde Saklanması .....	38
6.2.8.	İmza Oluşturma Verisinin Aktive Edilme Yöntemi .....	39
6.2.9.	İmza Oluşturma Verisinin Deaktive Edilme Yöntemi .....	39
6.2.10.	İmza Oluşturma Verisi Yok Etme Metodu .....	39
6.2.11.	Kriptografik Modül Değerlendirmesi .....	40
<b>6.3.</b>	<b>Anahtar Çifti Yönetimiyle İlgili Diğer Konular .....</b>	<b>40</b>
6.3.1.	İmza Doğrulama Verilerinin Arşivlenmesi .....	40
6.3.2.	Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri .....	40
<b>6.4.</b>	<b>Erişim Şifreleri .....</b>	<b>40</b>
6.4.1.	Erişim Şifrelerinin Oluşturulması ve Kurulumu .....	40
6.4.2.	Erişim Şifrelerinin Korunması .....	40
6.4.3.	Erişim Şifreleriyle İlgili Diğer Konular .....	41
<b>6.5.</b>	<b>Bilgisayar Güvenlik Kontrolleri .....</b>	<b>41</b>
6.5.1.	Bilgisayar Güvenliği Teknik Gereklilikleri .....	41
6.5.2.	Bilgisayar Güvenliği Sıralaması .....	41
<b>6.6.</b>	<b>Yaşam Döngüsü Teknik Kontrolleri .....</b>	<b>41</b>
6.6.1.	Sistem Geliştirme Kontrolleri .....	41
6.6.2.	Güvenlik Yönetimi Kontrolleri .....	41
6.6.3.	Yaşam Döngüsü Güvenlik Kontrolleri .....	41
<b>6.7.</b>	<b>Ağ Güvenlik Kontrolleri .....</b>	<b>42</b>
<b>6.8.</b>	<b>Zaman Damgası .....</b>	<b>42</b>
<b>7.</b>	<b>SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (SİL) VE OCSP PROFİLLERİ ....</b>	<b>43</b>
<b>7.1.</b>	<b>Sertifika Profili .....</b>	<b>43</b>
7.1.1.	Sürüm Numaraları .....	43
7.1.2.	Sertifika Uzantıları .....	43
7.1.3.	Algoritma Nesne Tanımlayıcıları .....	44
7.1.4.	İsim Biçimleri .....	44
7.1.5.	İsim Kısıtları .....	44
7.1.6.	Sertifika İlkeleri Nesne Tanımlayıcısı .....	44
7.1.7.	İlke Kısıtları Uzantısının Kullanımı .....	44
7.1.8.	İlke Niteleyicilerinin Yazımı .....	44
7.1.9.	Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği .....	44
<b>7.2.</b>	<b>SİL Profili .....</b>	<b>44</b>
7.2.1.	Sürüm Numarası .....	44
7.2.2.	SİL ve SİL Giriş Uzantıları .....	44
<b>7.3.</b>	<b>OCSP Profili .....</b>	<b>44</b>
7.3.1.	Sürüm Numarası .....	45
7.3.2.	OCSP Uzantıları .....	45

<b>8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER .....</b>	<b>46</b>
<b>8.1. Denetim Sıklığı ve Durumları .....</b>	<b>46</b>
<b>8.2. Denetçinin Kimliği ve Özellikleri .....</b>	<b>46</b>
<b>8.3. Denetçinin ESHS'yle İlişkisi .....</b>	<b>46</b>
<b>8.4. Denetimde Kapsanan Başlıklar .....</b>	<b>46</b>
<b>8.5. Eksiklik Durumunda Yapılacaklar .....</b>	<b>47</b>
<b>8.6. Sonuçların Bildirilmesi .....</b>	<b>47</b>
<b>9. DİĞER İŞ KONULARI VE YASAL KONULAR .....</b>	<b>48</b>
<b>9.1. Ücretler .....</b>	<b>48</b>
9.1.1. Sertifika Üretim ve Yenileme Ücretleri .....	48
9.1.2. Sertifika Erişim Ücretleri .....	48
9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri .....	48
9.1.4. Diğer Hizmetlerin Ücretleri .....	48
9.1.5. Bedel İadesi .....	48
<b>9.2. Finansal Sorumluluk .....</b>	<b>49</b>
9.2.1. Sigorta Kapsamı .....	49
9.2.2. Diğer Varlıklar .....	49
9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı .....	49
<b>9.3. İş Bilgisinin Gizliliği .....</b>	<b>49</b>
9.3.1. Gizli Bilginin Kapsamı .....	49
9.3.2. Gizlilik Kapsamı Dışındaki Bilgi .....	49
9.3.3. Gizli Bilginin Korunması Sorumluluğu .....	49
<b>9.4. Kişisel Bilgilerin Gizliliği/Özelliği .....</b>	<b>49</b>
9.4.1. Gizlilik Planı .....	49
9.4.2. Özel Olarak Değerlendirilecek Bilgi .....	50
9.4.3. Özel Sayılmayacak Bilgi .....	50
9.4.4. Özel Bilgiyi Koruma Sorumluluğu .....	50
9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı .....	50
9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması .....	50
9.4.7. Bilginin Açıklandığı Diğer Durumlar .....	50
<b>9.5. Fikri Mülkiyet Hakları .....</b>	<b>50</b>
<b>9.6. Sorumluluklar .....</b>	<b>50</b>
9.6.1. ESHS Sorumlulukları .....	50
9.6.2. Kayıt Merkezi Sorumlulukları .....	51
9.6.3. Sertifika Sahibi Sorumlulukları .....	51
9.6.4. Üçüncü Kişilerin Sorumlulukları .....	51
9.6.5. Diğer Tarafların Sorumlulukları .....	51
<b>9.7. Sorumlulukların Geçersiz Olduğu Durumlar .....</b>	<b>51</b>



<b>9.8. Sorumluluk Sınırları .....</b>	<b>51</b>
<b>9.9. Tazminatlar .....</b>	<b>51</b>
<b>9.10. Sİ Kitapçığının Geçerliliği .....</b>	<b>51</b>
9.10.1. Sİ Kitapçığının Geçerlilik Dönemi .....	51
9.10.2. Sİ Kitapçığının Geçerliliğinin Sona Ermesi .....	52
9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi .....	52
<b>9.11. Taraplara Özel Duyurular ve İletişim .....</b>	<b>52</b>
<b>9.12. Değişiklikler .....</b>	<b>52</b>
9.12.1. Değişiklik Prosedürü .....	52
9.12.2. Duyuru Mekanizması ve Süresi .....	53
9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar .....	53
<b>9.13. Anlaşmazlıkların Çözümü.....</b>	<b>53</b>
<b>9.14. Yasal Düzenleme.....</b>	<b>53</b>
<b>9.15. İlgili Yasalara Uygunluk.....</b>	<b>53</b>
<b>9.16. Çeşitli Hükümler.....</b>	<b>53</b>
9.16.1. Bütün Anlaşma .....	53
9.16.2. Görevlendirme.....	54
9.16.3. Kitapçık Kısımlarının Ayrılabilirliği .....	54
9.16.4. Yasal Haklardan Vazgeçme .....	54
9.16.5. Mücbir Sebepler .....	54
<b>9.17. Diğer Hükümler.....</b>	<b>54</b>

## 1. GİRİŞ

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (kitapçıkta bundan sonra kısaca "TÜRKTRUST" olarak anılacaktır), 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiş olan 15 Ocak 2004 tarihli ve 5070 sayılı "Elektronik İmza Kanunu (kitapçıkta bundan sonra kısaca "Kanun" olarak anılacaktır)" ve Telekomünikasyon Kurumu tarafından yayımlanmış olan ikincil mevzuat uyarınca, elektronik sertifika hizmet sağlayıcılığı alanında faaliyet göstermektedir.

Sertifika İlkeleri (Sİ) olarak adlandırılan bu kitapçık, TÜRKTRUST'ın sertifika hizmet sağlayıcılığı alanındaki faaliyetleri sırasında uyulması gereken ilke ve kuralları belirlemek amacıyla, Telekomünikasyon Kurumu'nun kanun kapsamında yayımlanmış olduğu "Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ"ın 7. Maddesi uyarınca "IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" rehber kitapçığına uygun olarak TÜRKTRUST tarafından hazırlanmıştır.

Sİ kitapçığı, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal işlemleriyle ilgili tüm idari, teknik ve yasal gereklilikleri ortaya koyar; elektronik sertifika hizmet sağlayıcısı (ESHS) olarak TÜRKTRUST'ın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler.

### 1.1. Genel Bakış

Sİ kitapçığı, TÜRKTRUST'ın verdiği tüm elektronik sertifika hizmetlerini kapsar. Yasa gereği elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikalar ile yasal düzenleme dışında kalan güvenli sunucu sertifikaları, nesne imzalama sertifikaları ve deneme sertifikaları, bu Sİ kitapçığı tarafından belirlenen ilkeler uyarınca yönetilir.

Sİ'de belirtilen ilke ve kurallar, TÜRKTRUST'ın tüm müşteri hizmetleri birimlerini, kayıt merkezlerini ve sertifika üretim merkezi birimlerini kapsar.

TÜRKTRUST sertifika hizmet sağlayıcısı, bu Sİ kitapçığı hükümlerine bağlı bir uygulama kitapçığı olan Sertifika Uygulama Esasları (SUE) uyarınca işletme faaliyetlerini yürütür.

### 1.2. Kitapçık Adı ve Tanımlama

Bu Sİ kitapçığının açık adı "TÜRKTRUST Sertifika İlkeleri (Sİ)"dir. Kitapçık sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

TÜRKTRUST, bu Sİ kitapçığı uyarınca sertifika hizmetlerine yönelik ilkeleri tanımlayan kuruluş olarak, Türk Standartları Enstitüsü'nden (TSE) "2.16.792.3.0.3" benzersiz kurumsal nesne tanımlayıcı numarasını (OID) almıştır. TÜRKTRUST, Sİ kitapçığında yer alan aşağıdaki sertifika tipleri için, TÜRKTRUST kurumsal nesne tanımlayıcı numarasına bağlı aşağıdaki sertifika ilkeleri nesne tanımlayıcı numaralarını atamıştır:

- TÜRKTRUST Nitelikli Elektronik Sertifika İlkeleri (2.16.792.3.0.3.1.1.1): Kanun, yönetmelik ve tebliğ uyarınca, bireylerin elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikaları kapsar.
- TÜRKTRUST Sunucu Sertifikası İlkeleri (2.16.792.3.0.3.1.1.2): Sunuculara yönelik SSL sertifikalarını kapsar.

**Sürüm 02**

- TÜRKTRUST Deneme Sertifikası İlkeleri (2.16.792.3.0.3.1.1.3): Deneme amaçlı bireysel sertifikaları kapsar.
- TÜRKTRUST Nesne İmzalama Sertifikası İlkeleri (2.16.792.3.0.3.1.1.4): Nesne imzalama işlemlerine yönelik sertifikaları kapsar.

Sİ kitapçığı "<http://www.turktrust.com.tr>" web adresinde kamuya açık olarak yayımlanmaktadır.

**1.3. Taraflar**

Bu ilke kitapçığında hak ve yükümlülükleri tanımlanan TÜRKTRUST sertifika hizmetleriyle ilgili taraflar, sertifika hizmetlerini veren ESHS birimleri ve hizmeti alan müşteri ve kullanıcılar olarak tanımlanır.

**1.3.1. Sertifika Üretim Merkezleri**

Sertifika üretim merkezleri, ESHS'lerin sertifika üretim, dağıtım ve yayımlamasından sorumlu birimleridir. TÜRKTRUST sertifika üretim merkezleri bir hiyerarşi içinde çalışır. Ana sertifika üretim merkezi TÜRKTRUST'ın kök sertifikasına sahiptir. Bu merkez tarafından üretilmiş olan alt kök sertifikalara sahip olan diğer sertifika üretim merkezleri tarafından son kullanıcı sertifikaları üretilir.

**1.3.2. Sertifika Kayıt Merkezleri**

Sertifika kayıt merkezleri, ESHS'lerin sertifika başvuru, yenileme ve iptal gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimleridir. Bu birimler, prosedürler uyarınca müşteri kayıtlarını oluşturur, gerekli kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim merkezlerine yönlendirir.

Kayıt merkezleriyle ilgili işlemler, TÜRKTRUST satış temsilcilerinden gelen sertifika başvuruları doğrultusunda TÜRKTRUST merkezinde yer alan kayıt birimlerince yürütüldüğü gibi, doğrudan TÜRKTRUST'a bağlı kayıt merkezleri tarafından da yürütülür. Her iki durumda da, sertifika talepleri TÜRKTRUST sertifika üretim merkezine iletilir ve sertifika üretimi gerçekleştirilir.

**1.3.3. Sertifika Sahipleri**

Sertifika sahipleri, TÜRKTRUST kayıt merkezleri üzerinden sertifika başvuruları alınırken kimlik tanımlaması ve doğrulaması yapılarak adına sertifika üretilen ve kendisine gönderilen kişilerdir.

Kanun kapsamında sertifika sahibi olan gerçek kişiler, bu sertifikalarını elle atılan imza ile aynı hukuki sonucu doğuran güvenli elektronik imza oluşturmak için kullanabilirler.

Kanun kapsamına girmemekle birlikte, bir gerçek veya tüzel kişi tarafından başvurusu yapılarak adına sertifika verilen sunucular da sertifika kullanıcılarıdır.

**1.3.4. Üçüncü Kişiler**

Üçüncü kişiler, TÜRKTRUST sertifika hizmetleri kapsamında, TÜRKTRUST tarafından verilmiş olan sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikaları doğrulayan taraflardır.

**1.3.5. Diğer Taraflar**

TÜRKTRUST sertifika hizmetleri kapsamında sertifika üretimi, bilgi deposu yayımlama ve benzeri sertifika hizmetlerinin tümü TÜRKTRUST tarafından verildiği için, yukarıda belirtilen tarafların dışında başka bir taraf tanımlanmamıştır.

TÜRKTRUST'ın sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer taraflar, verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini ve TÜRKTRUST iş süreçleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. TÜRKTRUST ile hizmet aldığı kuruluşlar arasında bu garantilerin açıkça belirtildiği hizmet sözleşmeleri imzalanır.

#### **1.4. Sertifika Kullanımı**

##### **1.4.1. Geçerli Sertifika Kullanım Şekilleri**

TÜRKTRUST kök ve alt kök sertifikaları sadece kullanım amaçları doğrultusunda sertifika imzalamak için kullanılır.

TÜRKTRUST nitelikli sertifikaları, elle atılan imzayla aynı hukuki sonucu doğuran güvenli elektronik imza oluşturmak amacıyla kullanılır. Elektronik devlet, elektronik ticaret ve benzeri uygulamalarda belge ve form imzalamak, elektronik ortamdaki her türlü sözleşme ve kontrat gibi ticari ve/veya resmi belgeleri imzalamak, e-posta mesaj metinlerini imzalamak, web üzerindeki işlem talimatlarını imzalamak, kimlik tanımlama ve doğrulama gerektiren ağ ortamlarında istemci kimlik doğrulama özelliğiyle kimliği ispat etmek geçerli sertifika kullanım şekilleridir.

Sunucu sertifikaları, güvenli iletişimi sağlamak amacıyla sunucular üzerinde sunucu kimlik doğrulaması yapmak ve güvenli iletişim kanalı oluşturmak amacıyla kullanılır.

Nesne imzalama sertifikaları, yazılım kodlarını ya da kurulum öncesi sıkıştırılarak paketlenmiş yazılım parçalarını elektronik olarak imzalamak için kullanılır.

Deneme sertifikaları ise sadece deneme amaçlı e-posta mesaj metni imzalamak için kullanılır.

##### **1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri**

TÜRKTRUST nitelikli sertifikaları, Kanuna göre, "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinde" kullanılamaz.

Bu yasal şartın yanında, TÜRKTRUST sertifikaları çeşitlerine göre Madde 1.4.1'de belirtilen kullanım amaçları dışında da kullanılamaz.

#### **1.5. Sertifika İlkeleri Yönetimi**

TÜRKTRUST, sertifika ilkelerini oluşturan otorite olarak, bu Sİ kitapçığının yönetimi ve kayıt altına alınmasından sorumludur.

##### **1.5.1. Sİ Kitapçığından Sorumlu Organizasyon**

Bu Sİ kitapçığının tüm hakları ve sorumluluğu TÜRKTRUST'a aittir.

##### **1.5.2. İletişim Noktası**

Sİ kitapçığıyla ilgili iletişim bilgileri aşağıdadır:

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Adres : Hollanda Caddesi 62.Sokak No:7 Yıldız, Çankaya 06550 ANKARA

Telefon : (90-312) 439 10 00

Faks : (90-312) 439 10 01

Çağrı Merkezi : 444 0 263

E-posta : [sertifika@turktrust.com.tr](mailto:sertifika@turktrust.com.tr)

Web : <http://www.turktrust.com.tr>

**1.5.3. SUE'nin İlgelere Uygunluğunun Belirlenmesi**

TÜRKTRUST SUE kitapçığının bu Sİ kitapçığına uygunluğu TÜRKTRUST ilke yönetimi yetkilileri tarafından belirlenir.

**1.5.4. SUE Onaylama Prosedürleri**

TÜRKTRUST SUE içeriğinde, kitapçığın bu Sİ kitapçığına uygun olarak hazırlandığı açık olarak belirtilir. TÜRKTRUST yetkilileri, SUE'de yer alan faaliyetlerin Sİ'ye uygunluğunu gerekli incelemelerin ardından onaylar. Gerekli onayı alan SUE, ESHS faaliyetlerini düzenlemek ve işletmek için kullanılır.

**1.6. Kısaltmalar ve Tanımlar****1.6.1. Kısaltmalar**

- ESHS** : Elektronik Sertifika Hizmet Sağlayıcısı  
**IETF** : Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu  
**OID** : Object Identifier – Nesne Tanımlayıcı Numarası  
**OCSP** : On-line Certificate Status Protokol – Çevrim İçi Sertifika Durum Protokolü  
**PKI** : Public Key Infrastructure – Açık Anahtarlı Altyapı  
**RFC** : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları  
**Sİ** : Sertifika İlkeleri  
**SİL** : Sertifika İptal Listesi  
**SSL** : Secure Sockets Layer  
**SUE** : Sertifika Uygulama Esasları  
**TSE** : Türk Standartları Enstitüsü

**1.6.2. Tanımlar**

**Açık Anahtar:** bkz. İmza Doğrulama Verisi.

**Açık Anahtarlı Altyapı (PKI):** Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan, mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünüdür.

**Alt Kök Sertifikası:** ESHS'nin PKI hiyerarşisi uyarınca sertifika üretim merkezi tarafından oluşturulmuş, ESHS kök sertifikasının imzasını taşıyan ve son kullanıcı sertifikalarını imzalama amaçlı kullanılan sertifikadır.

**Anahtar:** İmza oluşturma verisi veya imza doğrulama verisinden herhangi biri.

**Anahtar Yenileme:** İmza doğrulama verisi ve geçerlilik süresi dışında, bir sertifika içinde yer alan tüm bilgi alanlarının aynı şekilde kullanılmasıyla yeni bir sertifikanın üretilmesidir. Anahtar yenileme için, sertifikanın geçerli olması zorunludur.

**Arşiv:** ESHS'nin saklamakla yükümlü olduğu bilgi, belge ve elektronik verilerdir.

**Çevrim İçi Sertifika Durum Protokolü (OCSP):** Sertifikaların geçerlilik durumunun kamuya duyurulması için oluşturulmuş, sertifika durum bilgisinin çevrim içi yöntemlerle anında ve kesintisiz alınmasını sağlayan standart protokol.

**Denetim:** ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin

**Sürüm 02**

tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan çalışmalar bütünüdür.

**Dizin:** Geçerli sertifikaları içinde bulunduran elektronik depodur.

**Elektronik İmza:** Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.

**Elektronik Sertifika:** İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır.

**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.

**Elektronik Veri:** Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlardır.

**Erişim Verisi:** Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verilerdir.

**Gizli Anahtar:** bkz. İmza Oluşturma Verisi.

**Güvenli Elektronik İmza:** Kanunun 4 üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran elektronik imzadır.

**Güvenli Elektronik İmza Doğrulama Aracı:** Kanunun 7 nci maddesinde sayılan niteliklere sahip imza doğrulama aracıdır.

**Güvenli Elektronik İmza Oluşturma Aracı:** Kanunun 6 ncı maddesinde sayılan niteliklere sahip imza oluşturma aracıdır.

**İmza Doğrulama Aracı:** Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır.

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

**İmza Oluşturma Aracı:** Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır.

**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 verilerdir.

**İmza Sahibi:** Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir.

**İnceleme:** Kuruma yapılan bildirim gerekliliği şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalar bütünüdür,

**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 kayıttır.

**Kanun:** 15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'dur.

**Kök Sertifika:** ESHS kurumsal kimlik bilgilerini ESHS imza doğrulama verisine bağlayan, sertifika üretim merkezi tarafından üretilmiş olan ve kendi imzasını taşıyan, ESHS'nin ürettiği tüm sertifikaların doğrulanabilmesi için ESHS tarafından yayımlanan sertifikadır.

**Kurum:** Telekomünikasyon Kurumu'dur.

**Kurumsal Başvuru:** Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusudur.

**Nitelikli Elektronik Sertifika:** Kanununun 9 uncu maddesinde sayılan niteliklere sahip elektronik sertifikadır.

**Özetleme Algoritması:** İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritmadır.

**Sertifika İlkeleri:** ESHS'nin işleyişi ile ilgili genel kuralları içeren belgedir.

**Sertifika İptal Listesi:** İptal edilmiş sertifikaların kamuya duyurulması amacıyla ESHS tarafından oluşturulan, imzalanan ve yayımlanan elektronik dosyadır.

**Sertifika Mali Sorumluluk Sigortası:** ESHS'nin, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortadır.

**Sertifika Özet Değeri:** Sertifikanın, özetleme algoritması ile elde edilen çıktısıdır.

**Sertifika Uygulama Esasları:** Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi,

**Sertifika Kayıt Merkezi:** ESHS yapısında yer alan, sertifika başvuruları ile sertifika yenileme başvurularını alan, ilgili kimlik tanımlama ve doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak sertifika üretim merkezine yönelten, ESHS faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip olan birimdir.

**Sertifika Üretim Merkezi:** ESHS yapısında yer alan, onaylı sertifika talepleri doğrultusunda sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştiren, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birimdir.

**Sertifika Yenileme:** İmza doğrulama verisi de dahil olmak üzere, geçerlilik süresi dışında bir sertifika içinde yer alan tüm bilgi alanlarının aynı şekilde kullanılmasıyla yeni bir sertifikanın üretilmesidir. Sertifika yenileme için, sertifikanın geçerli olması zorunludur.

**Tebliğ:** Telekomünikasyon Kurumu tarafından yayımlanan Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ'dir.

**Yönetmelik:** Telekomünikasyon Kurumu tarafından yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'tir.

**Zaman Damgası:** Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıttır.

**Zaman Damgası İlkeleri:** Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgedir.

**Zaman Damgası Uygulama Esasları:** Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgedir.



## **2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI**

TÜRKTRUST, elektronik sertifika hizmet sağlayıcılığı kapsamında sertifika hizmetleriyle ilgili gereken doküman ve kayıtları hazırlamak ve saklamakla yükümlüdür. Bu doküman ve kayıtların bazıları, sertifika hizmetlerinin etkin bir şekilde müşterilere ulaştırılabilmesi ve sertifika kullanımının güvenilirliğinin ve sürekliliğinin sağlanması amacıyla kamuya açık olarak yayımlanır.

### **2.1. Bilgi Deposu**

TÜRKTRUST, bilgi deposunda tutulan tüm bilgilerin doğruluğunu ve güncelliğini sağlar. TÜRKTRUST, bilgi deposunu işletmek ve ilgili doküman ve kayıtları yayımlamak için üçüncü bir güvenilir kişi ya da kuruluş kullanmaz.

### **2.2. Sertifikasyon Bilgisinin Yayınlanması**

TÜRKTRUST bilgi deposunda, ESHS iç işleyişine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler dışında kalan, sertifika hizmetlerinin yürütülmesine ilişkin bilgiler herkesin erişimine açık tutulur. ESHS'nin temel çalışma ilkelerini içeren Sİ kitapçığı, bu ilkelerin nasıl uygulandığını gösteren SUE kitapçığı, sertifika sahibi ve sertifika hizmetleri taahhünameleri, sertifika süreçleriyle ilgili müşteri kılavuzları, herkesin erişimine açık olarak bilgi deposunda yer alır. Ayrıca, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetlerine ilişkin tüm kök ve alt kök sertifikaları herkesin erişimine açık olarak dizin sunucularında ve bilgi deposunda yayımlanır. Güncel iptal durum kayıtları, hem OCSP desteğiyle hem de SİL'ler aracılığıyla erişime açık tutulur.

TÜRKTRUST tarafından üretilen sertifikalar da, ancak sertifika sahibinin yazılı rızası olması kaydıyla herkesin erişimine açık tutulur.

### **2.3. Yayımların Zamanı veya Sıklığı**

Madde 2.2'de bahsedilen dokümanların yeni sürümleri çıktıkça, eski sürümlerle birlikte bilgi deposunda yayımlanır. Sertifika ve çevrim içi sertifika durum sorgulama kayıtları sürekli, sertifika iptal listeleri günde en az bir kez yayımlanır.

### **2.4. Bilgi Deposuna Erişim Kontrolleri**

Bilgi deposu herkesin erişimine açıktır. TÜRKTRUST bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere gerekli her türlü güvenlik önlemini alır.



### **3. KİMLİĞİN DOĞRULANMASI**

TÜRKTRUST, ilk kez sertifika başvurusunda bulunan, sertifikasını yenilemek isteyen veya yeni bir sertifika edinmek isteyen kişilerin kimliklerini veya adına sertifika alınacak olan web, elektronik posta ve benzeri sunucuların elektronik adres bilgilerini, yasal ve teknik gereklilikler uyarınca gerekli tüm bilgilere ve resmi kaynaklara dayandırarak doğrular.

#### **3.1. İsimlendirme**

##### **3.1.1. İsim Tipleri**

TÜRKTRUST'ın ürettiği tüm sertifikalarda X.500 ayırt edici isimleri kullanılır.

##### **3.1.2. İsimlerin Anamlı Olması Gerekliliği**

Üretilen sertifikalardaki isimler belirsizlikten uzak ve anlamlıdır.

##### **3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği**

TÜRKTRUST, anonim veya takma ad içeren nitelikli elektronik sertifika üretmez.

##### **3.1.4. İsim Biçimlerinin Değerlendirilmesi**

Sertifikalarda yer alan isimler X.500 ayırt edici isim biçimine uygun olarak değerlendirilmelidir.

##### **3.1.5. İsimlerin Benzersizliği**

TÜRKTRUST nitelikli elektronik sertifikalarında kullanılan isimler, kendi aralarında benzersizdir.

##### **3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü**

TÜRKTRUST tarafından şirket veya kurumlara ait sunuculara verilen SSL sertifikaları ile nesne imzalama sertifikaları, şirket ticari unvanı veya kurum resmi adı doğrulanarak üretilir. Bunun dışında ticari marka kontrolü yapılmaz.

#### **3.2. İlk Kimlik Doğrulama**

##### **3.2.1. İmza Oluşturma Verisine Sahip Olunduğunun Kanıtlanma Metodu**

İmza oluşturma ve doğrulama veri çiftlerinin ESHS tarafından oluşturulmadığı durumlarda, sertifika başvuru sahibinin imza oluşturma verisine sahip olduğunun doğrulanması gerekir.

##### **3.2.2. Ticari Unvanın Doğrulanması**

Şirket veya kurumlara ait sunucular ile şirket veya kurum adına sertifika alacak olan kişisel başvuru sahipleri için sertifika üretilirken, şirket ticari unvanı veya kurum resmi adının resmi belgelere dayandırılarak doğrulanması gerekir.

##### **3.2.3. Kimliğin Doğrulanması**

Nitelikli elektronik sertifika başvurusunda bulunan kişilerin, sertifikada yer alacak kişisel bilgilerinin yasal düzenlemelerle belirlendiği şekilde ve resmi belgelere dayandırılarak doğrulanması gerekir. Nitelikli elektronik sertifika başvuruları alınırken, yasa gereği ilk başvuru sırasında yüz yüze kimlik doğrulanması yapılır.

Deneme sertifikalarının başvurularında geçerli bir e-posta adresi ve kişisel beyan yeterlidir.

Kurum çalışanları için yapılan kurumsal başvurularda da, sertifikada yer alacak kişisel bilgiler, yasal düzenlemelerle belirlendiği şekilde ve resmi belgelere dayandırılarak doğrulanır. Nitelikli elektronik sertifika başvuruları alınırken, yasa gereği ilk başvuru sırasında yüz yüze kimlik doğrulaması yapılır. Kurumsal başvurularda ayrıca, kurumun tüzel kişiliğinin tespiti amacıyla ticari sicil kaydı ve ilgili diğer belgeler de alınır.

### **3.2.4. Doğrulanmamış Sertifika Sahibi Bilgisi**

Başvuru sahiplerinin, kimlik belgelerinde veya diğer resmi belgelerde yer alan kişisel bilgileri ile kurumsal bağ ve yetkilerini gösteren kurumsal bilgilerinin dışında kalan bilgileri beyan üzerine kabul edilir ve üçüncü bir kaynaktan doğrulanmaz. Adres, telefon, e-posta gibi iletişim bilgileri ve kurumsal birim, kurumsal unvan gibi bilgiler, imzalı beyan ile alınan bilgiler arasındadır.

### **3.2.5. Yetkinin Doğrulanması**

Sertifika başvuru sahibinin talebi varsa, sertifikasına eklenecek olan mesleki unvanı, bağlı bulunduğu şirket, şirketteki unvanı ve kullanım yetkisi gibi bilgilerin kaynaklarının resmi belgelerle doğrulanması gerekir.

### **3.2.6. Uyumlu Çalışabilirlik Kriterleri**

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalar, diğer tüm nitelikli elektronik sertifikalarla uyumludur. Sertifikalar uygun müşteri yazılımları üzerinden karşılıklı olarak doğrulanabilir.

## **3.3. Anahtar Yenileme Taleplerinin Doğrulanması**

### **3.3.1. Rutin Anahtar Yenileme için Kimlik Doğrulama**

Anahtar çiftinin güvenli kullanım süresinin sonunda yeni anahtar çifti üretimi, kullanıcının yeni bir nitelikli elektronik sertifika başvurusunda bulunmasıyla gerçekleştirilir. Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalı olarak yapılabilir. Bu durumda eğer anahtar çifti sertifika sahibi tarafından üretiliyorsa sertifika talebiyle birlikte imza doğrulama verisi de ESHS'ye gönderilir.

Mevcut sertifika kullanıcılarının yeni sertifika başvurularında, başvuru sahibinin imzalı beyan formu ve taahhünamesi dışında, kimlik doğrulama için ilk başvuruda istenilen resmi belgelerden halen geçerli olanlar yeniden istenmez, özel gereklilik durumları dışında kimlik doğrulama için bizzat hazır bulunma şartı aranmaz.

### **3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama**

Sertifika iptali sonrası yeni sertifika başvurusu sırasında, başvuru sahibinin imzalı beyan formu ve taahhünamesi dışında, kimlik doğrulama için ilk başvuruda istenilen resmi belgelerden halen geçerli olanlar yeniden istenmez, özel gereklilik durumları dışında kimlik doğrulama için bizzat hazır bulunma şartı aranmaz.

## **3.4. İptal Talebi için Kimlik Doğrulama**

TÜRKTRUST, sertifika iptal taleplerini güvenilir yollarla alır; sertifika iptali yapmadan önce sertifika iptal talebinde bulunan kişinin kimliğini şüpheye yer bırakmayacak şekilde, web üzerinden veya telefonla bilgilerini kontrol ederek ya da imzalı iptal talep yazısı üzerinden doğrular.

## **4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ**

TÜRKTRUST, kendi sertifika üretim merkezlerinin kök ve alt kök sertifikaları ile son kullanıcı sertifikalarını bu Sİ uyarınca üretir ve yönetir. Kişisel ve sunucu sertifikalarının, nitelikli ve deneme amaçlı kişisel sertifikaların yaşam döngüsü uygulamaları birbirinden farklıdır. İzleyen bölümlerde bu farklı sertifika çeşitleri için ortak ve ayrı olan işlemlerin hangi ilkelere göre yürütüleceği açıklanacaktır.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikaları, kendi güvenli elektronik imza oluşturma araçlarında üretilen imza oluşturma verilerine bağlı imza doğrulama verilerinin alınmasıyla TÜRKTRUST sertifika üretim merkezinde üretilir.

### **4.1. Sertifika Başvurusu**

#### **4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?**

Nitelikli elektronik sertifika veya deneme sertifikası almak isteyen gerçek kişiler; kişisel başvuru belgeleri olmak kaydıyla çalışanları adına sertifika almak isteyen şirket ve kurumlar; sunucu sertifikası veya nesne imzalama sertifikası almak isteyen gerçek kişiler veya tüzel kişiler adına sunucu sorumluları veya teknik sorumlular TÜRKTRUST'a sertifika başvurusunda bulunabilir.

TÜRKTRUST kayıt merkezlerinde ve TÜRKTRUST iç hizmetlerinde çalışan yetkililerin başvuruları diğer nitelikli elektronik sertifika başvurularıyla aynı ilkeler uyarınca işlenir.

#### **4.1.2. Sertifika Başvuru Kayıtları ve Sorumluluklar**

Nitelikli elektronik sertifika başvurusu sırasında, başvuru sahibi, sertifika başvuru formunu eksiksiz doldurmalı ve elle atılan imza ile imzalamalı, istenilen kimlik doğrulama belgelerini ve imzalı sertifika sahibi taahhünamesini başvuru formuyla birlikte TÜRKTRUST kayıt merkezlerine iletmelidir. Kayıt merkezlerinde başvuru doğrudan başvuru sahibi tarafından yapılabilirken, kurumsal başvurularda ilgili form ve belgeler TÜRKTRUST kayıt yetkilileri aracılığıyla yerinde de hazırlanabilir.

Nitelikli elektronik sertifika başvurusu için gerekli olan imza doğrulama verisi, imza oluşturma verisiyle eş zamanlı üretilir. TÜRKTRUST sertifika başvuru sürecine bağlı olarak, imza oluşturma ve doğrulama veri çifti TÜRKTRUST merkezinde üretilir. TÜRKTRUST'ın sağlayacağı imkanlar dahilinde, imza oluşturma ve doğrulama veri çiftinin talep sahibinin kendisi tarafından kayıt merkezlerinde veya başka bir mekanda üretilmesi de mümkündür.

Sunucu sertifikası başvurusu sırasında sunucu sorumlusu, nesne imzalama sertifikası başvurusu sırasında teknik sorumlu ilgili formu doldurmalı ve gerekli belgeleri temin ederek sunucu sertifikası taahhünamesiyle birlikte TÜRKTRUST'a iletmelidir.

Deneme sertifikası başvurusu kimlik doğrulaması yapılmadan web üzerinden yapılır.

### **4.2. Sertifika Başvurusunun İşlenmesi**

#### **4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi**

Nitelikli elektronik sertifika başvurusu sırasında, başvuru sahibinin kimliği yasal düzenlemeler uyarınca resmi belgelere dayandırılarak doğrulanır. Kişi sertifikasını bir şirketteki temsilcilik, acentelik ve benzeri temsil veya vekalet ilişkisine dayanarak alıyorsa, şirket ile başvuru sahibinin arasındaki temsil ilişkisi resmi olarak doğrulanır. İlk başvuru sırasında kimlik doğrulama işlemi TÜRKTRUST kayıt merkezleri veya satış temsilcileri tarafından yüz yüze yapılır. Sonraki başvurularda bu şart aranmayabilir.

Sunucu sertifikası başvurusu sırasında, sunucu adı, sunucuya ait alan adı sahipliği ve sunucu sorumlusuna ait kişisel bilgiler TÜRKTRUST kayıt merkezleri tarafından doğrulanır.

Nesne imzalama sertifikası başvurularında, başvuru sahibinin sertifika bilgileri, belgelerle sağlanan kişisel ve/veya kurumsal bilgilere göre doğrulanır.

Deneme sertifikalarının başvuruları sırasında kimlik doğrulama yapılmaz.

#### **4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi**

TÜRKTRUST kayıt merkezleri tarafından yapılan kimlik doğrulama ve belge kontrolü sonrasında, sertifika başvurusu sertifika çeşidine göre, bu Sİ hükümlerine ve sertifika başvuru prosedürlerine uygunsa kabul edilir. Aksi halde başvuru reddedilir ve sertifika alınabilmesi için aynı başvuru adımlarının tekrarlanması gerekir.

#### **4.2.3. Sertifika Başvurularının İşlenme Süresi**

TÜRKTRUST kayıt merkezlerine ulaşan nitelikli elektronik sertifika başvurularının işlenerek üretilen sertifikaların yayımlanma süresi en çok 10 (on) iş günüdür.

Sunucu ve nesne imzalama sertifika başvurularının işlenmesi ve sertifikaların yayımlanma süresi, elektronik ortamda sertifika talebinin TÜRKTRUST merkezine ulaşmasının ardından 5 (beş) iş günüdür.

Deneme sertifikaları için kimlik doğrulama gerekmediğinden işlem süresi en çok 1 (bir) iş günüdür.

### **4.3. Sertifika Üretimi**

#### **4.3.1. Sertifika Üretimi Sırasındaki ESHS Faaliyetleri**

Kayıt yetkilisi tarafından TÜRKTRUST kayıt merkezine gönderilen kurumsal nitelikli elektronik sertifika başvuruları ile bireysel olarak hazırlanarak TÜRKTRUST'a gönderilen nitelikli elektronik sertifikalar prosedürler uyarınca kontrol edilir. Uygun bulunan başvurular kayıt altına alınarak TÜRKTRUST sertifika üretim merkezinde işlenir ve sertifikalar üretilir.

TÜRKTRUST'a ulaşan nitelikli elektronik sertifika başvurularının kayıt işlemleri web üzerinden online olarak veya TÜRKTRUST kayıt merkezlerindeki operatörler tarafından tamamlanabilir. Her iki durumda da başvuruya ait form ve belgeler TÜRKTRUST'a ulaştırılır ve sertifika üretimi gerçekleştirilir.

Sunucu sertifikası ve nesne imzalama sertifikası üretim işlemleri de prosedürler uyarınca yürütülür.

Deneme sertifikalarının başvuruları otomatik olarak sistem üzerinde işlenir ve sertifikalar üretilerek yayımlanır.

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikaların, sunucu sertifikalarının ve nesne imzalama sertifikalarının geçerlilik süresi 1 (bir), 2 (iki) veya 3 (üç) yıl, deneme sertifikalarının geçerlilik süresi 3 (üç) aydır.

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalar ITU-TRec. X.509V.3'e ve Tebliğ'le belirlenmiş diğer standartlarla uyumludur.

#### **4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi**

Sertifika üretimi tamamlandıktan sonra sertifika sahipleri, sunucu ve nesne imzalama sertifikaları için sunucu sorumluları ve teknik sorumlular prosedürler uyarınca bilgilendirilir.

#### **4.4. Sertifikanın Kabulü**

##### **4.4.1. Kabulün Şekli**

Nitelikli elektronik sertifikalarda sertifika içeriğinin kabulü aranmaz. Sertifika sahibi, sertifika içeriğinde başvurudan farklı veya gerçek olmayan verilerin varlığını tespit eder ise, TÜRKTRUST'ı derhal bilgilendirerek sertifikanın iptalini talep etmekle yükümlüdür.

Sunucu ve nesne imzalama sertifikalarında da sertifika içeriğinin kabulü aranmaz. Sunucu sertifikası sorumlusu veya teknik sorumlu, sunucu sertifikası veya nesne imzalama sertifikası içeriğinde başvurudan farklı veya gerçek olmayan verilerin varlığını tespit eder ise, TÜRKTRUST'ı derhal bilgilendirerek sertifikanın iptalini talep etmekle yükümlüdür.

Deneme sertifikaları için kabul işlemi yoktur.

##### **4.4.2. ESHS Tarafından Sertifikanın Yayınlanması**

Nitelikli elektronik sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla web üzerinde ve/veya izin sunucularında yayımlanır.

Sunucu ve nesne imzalama sertifikaları ile deneme sertifikaları da ilgili prosedürler uyarınca erişime açık tutulur.

##### **4.4.3. Diğer Tarafların Sertifika Üretimiyle İlgili Bilgilendirilmesi**

Uygulama dışıdır.

#### **4.5. Anahtar Çifti ve Sertifika Kullanımı**

##### **4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı**

Sertifika sahipleri, imza oluşturma verileri ve sertifikalarını, Kanun, Yönetmelik ve diğer düzenleyici işlemler ile, Sİ ve SUE kitapçıklarında ve ilgili sertifika sahibi taahhünamesinde yer alan koşullar uyarınca kullanılmalıdır. Sertifika sahibi taahhünamesi, ilgili sertifikanın çeşidine göre sertifikanın hangi amaçlarla ve nasıl kullanılacağını, sertifika sahibinin imza oluşturma verisinin güvenliğini sağlamak ve güvenli elektronik imza oluşturma aracı kullanmakla ilgili sorumluluklarını içerir.

Sertifikanın çeşidine göre, aşağıda sayılan genel koşullar sağlanmalıdır.

Nitelikli elektronik sertifikalar için sertifika sahibi,

- Adına düzenlenen güvenli elektronik imza oluşturma aracını ve bu araca ait erişim şifrelerini şahsen teslim almalıdır.
- Sertifika başvurusu sırasında, imza oluşturma ve doğrulama verilerini kendi ürettiği durumlarda, ilgili yasal düzenlemelere uygun ve güvenli bir şekilde işlemi yapmalıdır. ESHS'ye doğru imza doğrulama verisini bu SUE'de geçen koşullar dahilinde ulaştırmalıdır.
- İmza oluşturma verisini, güvenli elektronik imza oluşturma aracını ve ilgili şifreleri, kayıp, açığa çıkma, değişime uğrama ve üçüncü kişilerin erişimine ve kullanımına karşı korumalıdır.
- Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği tüm kişisel bilgiler tam ve doğru olmalıdır. Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri gecikmeksizin ESHS'ye bildirmelidir.
- İmza oluşturma verisinin ve/veya imza oluşturma aracının, kayıp, açığa çıkma, değişime uğrama ve diğer kişilerce kullanımı durumlarında veya bu durumların

oluşmasına neden olabilecek şartların ortaya çıkması halinde sertifikanın iptalini sağlamak üzere derhal ESHS'ye bilgi vermelidir.

- Sİ ve SUE kitapçıklarında yer alan ilke ve esaslar ile kılavuzlarda yer alan yükümlülüklerini yerine getirmelidir.
- Elektronik sertifikasını, imza oluşturma aracı ve imza oluşturma verisini Sİ ve SUE kitapçıkları ve sertifika sahibi taahhütnamesinde belirtilen amaçlar dışında kullanmamalıdır.

Sunucu sertifikaları ve nesne imzalama sertifikaları için:

- Sertifika başvurusu sırasında imza oluşturma ve doğrulama verileri, sunucu sorumlusu veya teknik sorumlu tarafından güvenli bir şekilde üretilmeli, ESHS'ye imza doğrulama verisi bu Sİ'de geçen koşullar dahilinde ulaştırılmalıdır.
- Sertifika alınan sunucu ile sunucu sertifikası veya nesne imzalama sertifikasına bağlı her türlü şifre ve anahtarların, diğer kişilerce yetkisiz ve izinsiz bir biçimde yerinin değiştirilmesine karşı gerekli önlemler alınmalıdır.
- Sunucu sertifikasını veya nesne imzalama sertifikasını, sertifika alınan sunucu ve sunucuda kurulu bulunan ilgili yazılımların bütünü ve sertifikaya bağlı her türlü şifre ve anahtarları, kayıp, açığa çıkma, değişime uğrama ve diğer kişilerce kullanımı durumlarına karşı korumak için gerekli önlemler alınmalıdır.
- Sunucu sertifikası sadece bir cihaz için kullanılmalı ve bu cihazın fiziksel güvenliği sağlanmalıdır.
- Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan edilen tüm bilgiler tam ve doğru olmalı, beyan edilen bilgilerde oluşabilecek değişiklikler derhal TÜRKTRUST'a bildirilmelidir.
- Sunucu sertifikasının veya nesne imzalama sertifikasının, sertifika alınan sunucu ve sunucuda kurulu bulunan ilgili yazılımların bütünü ve sertifikaya bağlı her türlü şifre ve anahtarların, kayıp, açığa çıkma, değişime uğrama ve yetkisiz kullanımı durumlarında, sertifikanın iptalini sağlamak üzere derhal TÜRKTRUST bilgilendirilmelidir.
- Sertifikanın süresinin dolması ya da iptali durumunda, sertifika kurulmuş olduğu sunucudan silinmeli ve daha sonra hiçbir amaçla yeniden kullanılmamalıdır.
- Sİ ve SUE kitapçıklarında yer alan ilke ve esaslar ile kılavuzlarda yer alan yükümlülükler yerine getirilmelidir.
- Sunucu sertifikası veya nesne imzalama sertifikası ile imza oluşturma verisi, Sİ ve SUE kitapçıkları ile sertifika sahibi taahhütnamesinde belirtilen amaçlar dışında kullanılmamalıdır.

Deneme sertifikalarının sahipleri, deneme dışında hiçbir amaçla sertifikalarını kullanmamalıdır.

#### **4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı**

Üçüncü kişiler, güvencikleri sertifikaların geçerliliğini kontrol etmekle ve sertifikaları Kanun, Yönetmelik ve diğer düzenleyici işlemler ile, Sİ ve SUE kitapçıklarında belirlenmiş kullanım amaçları dahilinde kullanmakla yükümlüdürler.

**4.6. Sertifika Yenileme**

TÜRKTRUST tarafından üretilen 1 (bir) yıllık nitelikli elektronik sertifikaların, geçerlilik sürelerinin sonunda aynı koşullarla kullanımına devam edilebilmesi için yenilenmesi gerekir.

Sertifika yenileme, sertifikanın süresinin sonunda sertifika bilgilerinde bir değişiklik olmadığı durumlarda yapılır. Bu durumda yeni bir anahtar çifti üretilmez, aynı imza doğrulama verisine bağlı, tarihi yenilenmiş yeni bir sertifika üretilir ve sertifika sahibine ulaştırılır.

Süresi dolmuş sertifikalar için yenileme yapılamaz; Madde 4.1.-4.5.'te belirtilen uygulama esasları uyarınca yeniden sertifika başvurusu ve üretimi yapılması gerekir. Aynı şekilde, 2 (iki) ve 3 (yıllık) TÜRKTRUST nitelikli elektronik sertifikaları için yeni bir anahtar çifti üretilmeden sertifika yenileme imkanı yoktur. Bu sertifikaların sürelerinin sonunda sertifika kullanımının devam edebilmesi için, Madde 4.1.-4.5.'te belirtilen uygulama esasları uyarınca yeniden sertifika başvurusu ve üretimi yapılması gerekir.

Kök ve alt kök sertifikaları için anahtar çifti yenilenmeden standart yenileme işlemi yapılmaz.

Sunucu sertifikaları ve nesne imzalama sertifikaları için sertifika yenileme işlemi yapılmaz, yeni sertifika başvurusu ile yeni bir sertifika üretilir.

Deneme sertifikaları için yenileme işlemi uygulanmaz.

**4.6.1. Sertifika Yenilemeyi Gerektiren Durumlar**

Sertifikanın kullanım süresinin dolmasına belirli bir süre kalmış olması ve sertifika içeriğindeki bilgilerde bir değişiklik olmaması durumunda, sertifika sahibinin talebi üzerine sertifika yenilenir.

**4.6.2. Yenileme Talebinde Bulunabilecek Kişiler**

1 (bir) yıllık nitelikli elektronik sertifikalar için, sertifika sahipleri sertifika yenileme talebinde bulunabilir.

**4.6.3. Sertifika Yenileme Talebinin İşlenmesi**

1 (bir) yıllık nitelikli elektronik sertifikalar için, sertifika yenileme başvurusu elektronik ortamda mevcut imza oluşturma verisiyle elektronik imzalı olarak web üzerinden yapılır.

**4.6.4. Yenilenmiş Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi**

Yenilenmiş nitelikli elektronik sertifikalar üretildiğinde, sertifika sahipleri e-posta ile bilgilendirilir. Yenileme süreci boyunca, eski sertifika da geçerlilik süresinin sonuna kadar kullanılabilir.

**4.6.5. Yenilenen Sertifikanın Kabulü**

Nitelikli elektronik sertifikalarda yenilenen sertifika içeriğinin kabulü aranmaz. Sertifika sahibi, sertifika içeriğinde başvurudan farklı veya gerçek olmayan verilerin varlığını tespit eder ise, TÜRKTRUST'ı derhal bilgilendirerek sertifikanın iptalini talep etmekle yükümlüdür.

Deneme sertifikaları için kabul işlemi yoktur.

**4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması**

Yenilenen nitelikli elektronik sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla web üzerinde ve/veya dizin sunucularında yayımlanır.



**4.6.7. Diğer Tarafların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi**

Uygulama dışıdır.

**4.7. Anahtar Yenileme**

Son kullanıcı sertifikalarında, aynı imza oluşturma ve doğrulama verisi çifti en çok 3 (üç) yıl süreyle kullanılabilir. Bu sürenin sonunda anahtar yenileme işlemi yerine, ilk başvuru adımları uyarınca yeni anahtar çiftiyle birlikte yeni bir sertifika üretilerek sertifika kullanımına devam edilebilir.

1 (bir) yıllık nitelikli elektronik sertifikalar için, standart sertifika yenileme işlemleriyle aynı imza oluşturma ve doğrulama verisi çiftinin 3 (üç) yıllık güvenli kullanım süresinin dolması durumunda, 2 (iki) ve 3 (yıllık) nitelikli elektronik sertifikalar için geçerlilik süresinin sonunda, tüm sunucu ve nesne imzalama sertifikalarının geçerlilik sürelerinin sonuna gelindiğinde, deneme sertifikalarının süresi dolduğunda sertifika kullanımına devam edilebilmesi için Madde 4.1.-4.5.'te belirtilen uygulama esasları uyarınca yeniden sertifika başvurusu ve yeni bir anahtar çiftiyle birlikte yeni sertifikanın üretiminin yapılması gerekir.

Kök sertifikaların süresi sonuna yaklaştığında, üretilecek son kullanıcı sertifikalarının geçerlilik süresi, bağlı bulunduğu kök sertifikaların her hangi birinin son kullanma tarihini geçmeyecek biçimde verilir. Eski kök sertifika ile yenilenen kök sertifikanın geçerlilik sürelerinin çakıştığı dönem için, TÜRKTRUST tarafından her iki kök ile üretilen sertifikaların sorunsuz olarak kullanılabilmesi için, bu iki kök sertifika arasında çapraz sertifikasyon yapılır ve bu çapraz sertifikasyon uygun biçimde sertifika sahipleri ile üçüncü kişilere duyurulur.

**4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar**

Uygulama dışıdır.

**4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler**

Uygulama dışıdır.

**4.7.3. Anahtar Yenileme Talebinin İşlenmesi**

Uygulama dışıdır.

**4.7.4. Yeni Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi**

Uygulama dışıdır.

**4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü**

Uygulama dışıdır.

**4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayınlanması**

Uygulama dışıdır.

**4.7.7. Diğer Tarafların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi**

Uygulama dışıdır.

**4.8. Sertifika Değişikliği**

TÜRKTRUST tarafından üretilmiş olan sertifikaların içeriğindeki bilgilerde bir değişiklik olması durumunda, sertifika iptal edilir ve yeni bilgilerle birlikte yeni bir sertifika başvurusunda bulunulur. Başka bir yöntemle mevcut sertifika üzerinde değişiklik yapılamaz.

Yeni sertifika başvurusu ve üretimi Madde 4.1.-4.5.'de belirtilen ilkeler uyarınca yürütülür.



**4.8.1. Sertifika Değişikliğini Gerektiren Durumlar**

Uygulama dışıdır.

**4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler**

Uygulama dışıdır.

**4.8.3. Sertifika Değişiklik Talebinin İşlenmesi**

Uygulama dışıdır.

**4.8.4. Yeni Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi**

Uygulama dışıdır.

**4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli**

Uygulama dışıdır.

**4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayınlanması**

Uygulama dışıdır.

**4.8.7. Diğer Tarafların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi**

Uygulama dışıdır.

**4.9. Sertifika İptali ve Askıya Alma****4.9.1. Sertifika İptalini Gerektiren Durumlar**

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifika sahibinin talebi,
- Nitelikli elektronik sertifikaya ilişkin TÜRKTRUST'ta bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması,
- Sertifika içeriğinde yer alan sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandırıldığı, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,
- İmza oluşturma verisinin kaybedilmesi, çalınması, ortaya çıkması veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
- Sertifikanın, Sİ ve SUE kitapçıkları ile TÜRKTRUST sertifika sahibi taahhütnamesi hükümlerine aykırı olarak kullanıldığı anlaşıldığı,
- TÜRKTRUST'ın sertifika hizmetleri vermeyi durdurması.

İptal edilen sertifikalar, sertifika geçerlilik süresinin sonuna kadar SİL ve OCSP servisi aracılığıyla duyurulur.

**4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler**

Aşağıda belirtilen kişiler sertifika iptal talebinde bulunabilir:

- Kişisel sertifikalar için sertifika sahibinin kendisi,
- Sunucu sertifikaları için sunucu sorumlusu,

- Nesne imzalama sertifikaları için teknik sorumlu,
- Kurumsal kullanımdaki sertifikalarda, sertifika sahibinin ya da sunucunun bağlı bulunduğu şirketin veya kurumun yetkilisi,
- Güvenlik gereği doğduğunda, son kullanıcı sertifikaları ile kök ve alt kök sertifikaları için TÜRKTRUST yetkilileri (TÜRKTRUST merkezi ve kayıt merkezleri yetkilileri).

#### **4.9.3. Sertifika İptal Talebi Prosedürleri**

Nitelikli elektronik sertifika iptal talepleri, sertifika sahibinden TÜRKTRUST web sitesi aracılığıyla, telefonla ve yazıyla olmak üzere farklı yollarla alınabilir. İşlem sonrası iptal durumu sertifika sahibine e-posta ile bildirilir.

Kurumsal sertifikaların iptal talepleri, sertifika sahiplerinin yanı sıra onaylı iptal başvuruları ile şirket yetkililerinden de alınabilir. İşlem sonrası iptal durumu şirket veya kurum yetkilisi ile sertifika sahibine e-posta ile bildirilir.

Deneme sertifikaları için iptal işlemi uygulanmaz.

Sunucu sertifikaları veya nesne imzalama sertifikaları için sertifika iptal talepleri sadece yazılı olarak alınır. İşlem sonrası iptal durumu şirket veya kurum yetkilisi ile sertifika sahibine e-posta ile bildirilir.

TÜRKTRUST'a ait bir güvenlik sorunu oluşması, mevcut sertifikalarla ilgili ihbar alınması ya da TÜRKTRUST'ın iç işleyişinde oluşan bir hatanın fark edilmesi durumlarından birinin gerçekleşmesi halinde, TÜRKTRUST sertifika iptalini başlatabilir. TÜRKTRUST tarafından başlatılan iptal süreci, kayıt merkezi ya da sertifika üretim merkezi kaynaklı olabilir.

TÜRKTRUST kaynaklı tüm sertifika iptal işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur. İptal sonrası eğer gerekiyorsa yeni sertifika üretim işlemleri ivedilikle başlatılır.

TÜRKTRUST, sertifika iptal hizmetini, web üzerinden kesintisiz olarak haftada 7 gün 24 saat ilkesine göre verir. Çağrı Merkezine telefonla gelen ya da TÜRKTRUST merkezine yazıyla gelen sertifika iptal talepleri, mesai saatleri içinde işleme alınır.

TÜRKTRUST'a ait kök ve alt kök sertifikaların iptal edilmesi durumunda, mümkün olan en kısa sürede durum tüm ilgili taraflara elektronik ortamda ivedilikle duyurulur. İptal edilen kök veya alt kök sertifikasının imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar e-posta ile bilgilendirilir.

#### **4.9.4. Sertifika İptal Talebi Gecikme Periyodu**

Uygulama dışıdır.

#### **4.9.5. TÜRKTRUST'ın Sertifika İptal Talebini İşleme Zamanı**

TÜRKTRUST, kendisine web üzerinden kesintisiz olarak haftada 7 gün 24 saat ulaşan tüm sertifika iptal taleplerini, talebin uygun bulunması ve kimlik doğrulamanın çevrim içi olarak tamamlanmasının ardından anında sonuçlandırır. Çağrı Merkezi üzerinden telefonla gelen veya yazıyla kağıt ortamında alınan sertifika iptal talepleri ise, mesai saatleri içinde derhal değerlendirmeye alınır ve gerekli işlemler ivedilikle tamamlanır.

#### **4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği**

Üçüncü kişiler, kendilerine gönderilen bir elektronik imzaya güvenmeden önce, ilgili sertifikayı doğrulamakla yükümlüdür. Sertifika durumunun doğrulanması için TÜRKTRUST

tarafından yayımlanan güncel SİL ya da çevrim içi sertifika durum sorgulama servisi olan OCSP kullanılmalıdır. TÜRKTRUST üçüncü kişilere, elektronik imza doğrulamada Tebliğ ile belirlenen güvenli elektronik imza doğrulama araçlarını kullanmalarını tavsiye eder.

#### **4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı**

TÜRKTRUST son kullanıcı sertifikaları için, sertifika durumlarında hiçbir değişiklik olmasa bile, günde en az bir kez yeni bir SİL yayımlar.

TÜRKTRUST alt kök sertifikalarına ait SİL'ler, bir alt kök sertifika iptali durumunda veya sertifika iptali olmasa bile yılda en az bir kez yayımlanır.

#### **4.9.8. SİL'lerin En Geç Yayımlanma Zamanı**

SİL'ler üretildikleri andan itibaren en geç 10 (on) dakika içinde yayımlanır.

#### **4.9.9. Çevrim İçi Sertifika İptal/Durum Kontrol İmkkanı (OCSP)**

TÜRKTRUST, kesintisiz çevrim içi sertifika durum protokolü OCSP desteği verir. SİL'lere göre daha güvenilir ve gerçek zamanlı bir sertifika durum sorgusu olan OCSP hizmetiyle, müşteri tarafındaki uygun yazılımlar aracılığıyla çevrimiçi olarak sertifika durum sorgusu yapılabilir. Bu sorguyla, belirli bir zamanda bir sertifikanın durumu (geçerli, askıda, iptal, süresi dolmuş/bilinmiyor) hakkında bilgi edinmek mümkündür.

#### **4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri**

Üçüncü kişilerin sertifika durum sorgusu yaparken, eğer teknik imkanları yeterliyse OCSP'yi tercih etmeleri, SİL'i ikinci alternatif olarak seçmeleri önerilir.

#### **4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı**

TÜRKTRUST, OCSP ve SİL dışında iptal durumu yayımlama yöntemi kullanmaz.

#### **4.9.12. Anahtar Güvenliğinin Yitirilmesi Durumlarına Özel Gereklilikler**

TÜRKTRUST'a ait bir güvenlik sorunu oluşması durumunda, durumdan etkilenen son kullanıcı sertifikaları TÜRKTRUST tarafından iptal edilir. TÜRKTRUST'a ait kök veya alt kök sertifikalarının iptal edilmesi gerekirse, bu sertifikaların imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar bilgilendirilir.

Güvenlik sorunu ve sonuçları, TÜRKTRUST tarafından ivedilikle kamuya açık bir şekilde web sitesi üzerinden ve gerekli durumlarda basın ve yayın organları aracılığıyla sertifika sahiplerine ve üçüncü kişilere duyurulur.

TÜRKTRUST kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim işlemlerinin ivedilikle başlatılmasından TÜRKTRUST sorumludur.

#### **4.9.13. Sertifika Askıya Almayı Gerektiren Durumlar**

TÜRKTRUST, bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda doğrulama işlemi sonuçlanıncaya kadar, ya da son kullanıcı tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığı zamanlarda gelen talep üzerine, iptal işlemi yapmak yerine ilgili sertifikaları askıya alır.

#### **4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler**

Sertifika iptal talebinde bulunabilen aşağıda belirtilen tüm taraflar, sertifika askıya alma talebinde de bulunabilir:

- Kişisel sertifikalar için sertifika sahibinin kendisi,
- Sunucu sertifikaları için sunucu sorumlusu,

**Sürüm 02**

- Nesne imzalama sertifikaları için teknik sorumlu,
- Kurumsal kullanımdaki sertifikalarda, sertifika sahibinin ya da sunucunun bağlı bulunduğu şirketin veya kurumun yetkilisi,
- Güvenlik gereği doğduğunda, son kullanıcı sertifikaları ile kök ve alt kök sertifikaları için TÜRKTRUST yetkilileri (TÜRKTRUST merkezi ve kayıt merkezleri yetkilileri).

**4.9.15. Sertifika Askıya Alma Talebi Prosedürü**

Sertifika askıya alma talepleri, sertifika sahibi veya sunucu sorumlusu veya teknik sorumlu tarafından, web üzerinden, telefonla veya yazıyla, Madde 4.9.3.'te belirtilen sertifika iptal talebi prosedürleriyle aynı adımlar üzerinden TÜRKTRUST'a iletilir. İlgili adımların tamamlanmasının ardından, sertifika TÜRKTRUST tarafından askıya alınır. Askıya alma durumu sertifika sahibine, sunucu sorumlusuna veya teknik sorumluya bildirilir.

Kurumsal sertifikaların askıya alma talepleri, sertifika sahiplerinin yanı sıra onaylı askıya alma başvuruları ile şirket yetkililerinden de alınabilir. İşlem sonrası askıya alma durumu şirket yetkilisi ile sertifika sahibine, sunucu sorumlusuna veya teknik sorumluya bildirilir.

Deneme sertifikaları için askıya alma işlemi uygulanmaz.

TÜRKTRUST'a ait bir güvenlik sorunu oluşması ya da mevcut sertifikalarla ilgili ihbar alınması durumunda, iptal gerekliliği kesinleşene kadar TÜRKTRUST ilgili sertifikaları askıya alabilir. TÜRKTRUST tarafından başlatılan askı süreci, kayıt merkezi ya da sertifika üretim merkezi kaynaklı olabilir. TÜRKTRUST kaynaklı tüm sertifika askıya alma işlemlerinde, sonuç ilgili sertifika kullanıcılarına duyurulur.

TÜRKTRUST'a ait kök ve alt kök sertifikaları için askıya alma işlemi uygulanmaz.

**4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları**

TÜRKTRUST'ın, bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikalar, doğrulama işlemi sonuçlanıncaya veya süre sınırı aşılanaya kadar askıda bırakılır. Sertifika sahipleri tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığında askıya alınan sertifikalar, sertifika sahibinden iptal gerekliliği onaylandığında iptal edilir.

Her iki durumda da, askıya alma süresi 30 (otuz) günü aşamaz. Bu sürenin sonunda hala askıda bulunan sertifikalar, güvenlik nedeniyle otomatik olarak iptal edilir.

Sertifikaların askıda bulunduğu süre içinde, iptali gerektiren bir durumun olmadığı anlaşılırsa, sertifika askıdan çıkarılarak tekrar geçerli duruma alınabilir.

**4.10. Sertifika Durum Servisleri**

TÜRKTRUST tarafından üretilmiş olan sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla, tüm sertifika sahiplerinin ve üçüncü kişilerin erişimine açık olarak web ve/veya LDAP dizin sunucusu üzerinden yayımlanır.

Sertifika durum sorgulaması ise iki ayrı yöntemle yapılır. Sertifika İptal Listesi (SİL-CRL) ve Çevrimiçi Sertifika Durum Protokolü (OCSP).

**4.10.1. İşlevsel Özellikler**

TÜRKTRUST günde en az bir kez, sertifika durumlarında hiçbir değişiklik olmasa bile yeni bir SİL yayımlar.

**Sürüm 02**

TÜRKTRUST, çevrim içi sertifika durum protokolü OCSP desteği verir. Bu sorguyla, gerçek zamanlı sertifika durum (geçerli, askıda, iptal, süresi dolmuş/bilinmiyor) bilgisi alınabilir.

**4.10.2. Hizmetin Sürekliliği**

TÜRKTRUST, Madde 4.10.1.'de belirtilen koşullarda SİL ve OCSP hizmetini, kesintisiz olarak haftada 7 gün 24 saat ilkesine göre verir.

**4.10.3. İsteğe Bağlı Özellikler**

Uygulama dışıdır.

**4.11. Sertifika Sahipliğinin Sona Ermesi**

Sertifika sahipliğinin sona ermesi, sertifikanın süresinin dolması ya da iptal edilmesiyle gerçekleşir.

**4.12. İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma**

TÜRKTRUST, elektronik imza amaçlı kullanılmak üzere ürettiği son kullanıcı sertifikalarının imza oluşturma verilerini kesinlikle saklamaz veya yeniden oluşturmaz; yeniden oluşturulabileceği bilgileri elinde tutmaz.

**4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları**

Uygulama dışıdır.

**4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları**

Uygulama dışıdır.

## **5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER**

Sİ kitapçığının bu kısmında, TÜRKTRUST'ın sertifika hizmetlerini yürütürken tesis ve işletme güvenliğini sağlamaya yönelik olarak uyguladığı, teknik olmayan çeşitli güvenlik kontrolleri yer almaktadır.

### **5.1. Fiziksel Kontroller**

#### **5.1.1. Tesis Yeri ve İnşaatı**

TÜRKTRUST merkezi, dış tehditlere karşı korunaklı ve güvenli bir alanda kurulmuş, tesis içinde yüksek güvenli bölgeler ve çeşitli güvenlik alanları oluşturulmuştur.

#### **5.1.2. Fiziksel Erişim**

TÜRKTRUST merkezindeki alanlara fiziksel erişim sürekli kontrol altında tutulmaktadır.

#### **5.1.3. Güç Kaynakları ve Havalandırma**

TÜRKTRUST merkezinde kullanılan tüm donanım ve teçhizat için kesintisiz çalışacak güç kaynakları oluşturulmuştur.

Özellikle bilgisayar donanımlarının yoğun bulunduğu bölgelerde, bu bölgelerin dışında kalan alanlarda ise ihtiyaca göre yeterli havalandırma kesintisiz olarak sağlanır.

#### **5.1.4. Su Baskınları**

TÜRKTRUST merkezi, sel ve su baskınlarına karşı korunmuştur.

#### **5.1.5. Yangın Önleme ve Yangından Korunma**

TÜRKTRUST merkezinde, yangın ihbar sistemleri ile olası yangın durumlarına anında müdahale edilmesini sağlayacak söndürme sistemleri kurulmuştur.

#### **5.1.6. Saklama Ortamları**

TÜRKTRUST faaliyetleri sırasında oluşturulan tüm kayıtların yedekleri uygun saklama ortamlarında tutulur.

#### **5.1.7. Atıkların Atılması**

Temel sertifika hizmetlerine bağlı, elektronik veya kağıt ortamda saklanan tüm bilgi ve belgeler, saklanmaları gerekmiyorsa ilgili prosedürler uyarınca tamamen imha edilerek atılır. Kriptografik modüller atılmaları gerektiğinde ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.

Binanın ve TÜRKTRUST birimlerinin diğer tüm atıkları uygun biçimde tesis dışına çıkarılır.

#### **5.1.8. Tesis Dışı Yedekleme**

TÜRKTRUST, sertifika hizmetleri iş sürekliliğini sağlayabilmek amacıyla, mevcut tesis ve binada oluşabilecek herhangi bir afet durumunda sistemlerini yeniden işletilebilir duruma getirebilmek için elektronik işlem kayıtlarının yedeklerini tesis dışında güvenli kasalarda saklar.

## 5.2. Prosedürel Kontroller

### 5.2.1. Güvenilir Roller

TÜRKTRUST elektronik sertifika hizmetlerinde görev alan personelin organizasyonunun sağlanması amacıyla, tüm sertifika iş süreçlerinin yürütülmesinde görev alacak güvenilir roller belirlenmiştir.

- **Üst Düzey Yöneticiler:** TÜRKTRUST sertifika hizmetlerinin planlandığı gibi yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Birim Yöneticileri:** Müşteri hizmetleri ile temel sertifika süreçleri yanında, arşiv, tesis güvenlik gibi tüm destek hizmetlerinin yürütüldüğü ilgili birimlerin teknik ve idari işleyişinin planlanması, yönetimi ve kontrolünden sorumlu yöneticilerdir.
- **Kayıt Yetkilileri ve Müşteri Hizmetleri Yetkilileri:** Sertifika başvuru kaydı, evrak kontrolü, sertifika yenileme, sertifika iptali ve müşteri hizmetleriyle ilgili işlemleri içeren tüm sertifika hizmetlerinden sorumlu birim çalışanlarıdır.
- **Bilgi Güvenliği Yönetim Sistemi Sorumlusu:** TÜRKTRUST sertifika hizmetleri kapsamındaki iş süreçlerinde bilgi güvenliğinin sağlanmasından, güvenlik politikalarının ve bağlı prosedürlerin uygulanmasından, belgelendirilmiş ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin devamlılığından sorumludur.
- **Sistem ve Ağ Yöneticileri:** Sertifika süreçlerinin yürütülmesinde kullanılan tüm yazılım ve donanım bileşenlerinin kurulumu, konfigürasyonu ve devamlılığının sağlanmasından sorumlu çalışanlardır.
- **Sertifika Üretim Merkezi İşletmecileri:** Günlük sertifika üretim işlemlerinden sorumlu, özel erişim yetkilerine sahip sistem görevlileridir. Sertifika Üretim Merkezi İşletmecileri, aynı zamanda sistem yedekleme ve geri yükleme işlemlerinden de sorumludur.
- **Sistem Denetçileri:** Sertifika üretim işlemlerinin ve ilgili tüm kayıtların denetiminden sorumlu çalışanlardır.
- **Güvenlik Görevlileri:** TÜRKTRUST binasının ve tesisin tümünün fiziksel güvenliğini sağlayan, bina girişleri ve kritik birimlerde görev yapan güvenlik personelidir.

### 5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

TÜRKTRUST'ta sertifika süreçleri dahilindeki kritik işlemlerin yapılabilmesi için çok kişi kontrollü bir sistem kurulmuştur. Kriptografik modül kullanımı gerektiren sertifika ve SİL üretimi işlemleri, en az iki yetkilinin hazır bulunmasıyla sonuçlandırılabilir.

Yukarıda belirtilen rutin sertifika üretim adımları dışında, TÜRKTRUST kök ve alt kök sertifikalarıyla ilgili her türlü üretim, yenileme ve iptal işlemi en az iki yetkilinin hazır bulunması ve onaylı görev talimatının ilgili yetkililere verilmiş olmasıyla yapılabilir.

### 5.2.3. Her Görev için Kimlik Doğrulama

TÜRKTRUST içinde güvenilir rollere atanan çalışanlar, öncelikle atanmış yetkileriyle birlikte güvenlik sistemine tanıtılır. Böylelikle her kritik işlem öncesi bu rollerdeki kişilerin kimlik doğrulaması yapılır. Doğrulama tamamlandıktan sonra işleme izin verilir ve işlem tamamlandıktan sonra kaydedilir.



#### **5.2.4. Görevlerin Ayrılmasını Gerektiren Roller**

Sertifika süreçleri işletilirken, aynı sertifikayla yapılan ardışık işlemlerin tümü farklı işlem noktalarında farklı kişiler tarafından yapılır. Görevlerin dağıtımı farklı rollere atanarak süreç içinde aynı kişinin işin bütününe ya da büyük bir kısmını yapması engellenmiştir. Yapılan her işlem, rol bazlı olarak ayrıntılı yer ve zaman bilgisi içerecek şekilde kayıt altına alınmaktadır.

### **5.3. Personel Kontrolleri**

#### **5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri**

TÜRKTRUST'ta çalışan personel, sertifika süreçlerinin işleyişini doğru ve güvenilir bir şekilde yürütebilecek nitelikte, göreve uygun eğitim düzeyine sahip (lise, üniversite, yüksek lisans vb.), konusunda bilgili ve eğitilmiş, benzer çalışma alanlarında deneyimli ve güvenlik kontrollerinden geçmiştir.

#### **5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri**

TÜRKTRUST'ta çalışan personelin özgeçmiş ve referansları ayrıntılı bir şekilde değerlendirilmekte, işe teknik ve idari açıdan uygunluğundan emin olunmaktadır. Uygun nitelikte olduğu belirlenen kişiler için adli sicil belgesi istenir ve gerekiyorsa güvenlik soruşturması yapılır.

#### **5.3.3. Eğitim Gereklilikleri**

TÜRKTRUST personeli göreve başlamadan önce sorumlulukları kapsamında eğitimden geçirilir. Eğitim süresince, çalışanlar temel sertifika iş süreçleri; müşteri hizmetleri, kayıt merkezleri ve sertifika üretim merkezi işleyişiyle ilgili prosedürler ve talimatlar; bilgi güvenliği ilkeleri ve mevcut bilgi güvenliği yönetim sistemi; kullanılacak yazılım ve donanım birimleri hakkında ayrıntılı olarak bilgilendirilir.

Kayıt merkezlerindeki çalışanlar da görevlerinin gerektirdiği ölçüde eğitime tabi tutulurlar.

#### **5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri**

Çalışanlara yönelik eğitim, göreve başlanırken verilen ilk eğitimin ardından periyodik olarak ve diğer gerekli görülen durumlarda tekrarlanır.

#### **5.3.5. İş Rotasyonu Sıklığı ve Sırası**

TÜRKTRUST'a bağlı güvenlik görevlileri ve operatörler kendi çalışma alanları içindeki alt görevler üzerinde rotasyona tabi tutulurlar. Ancak çalışma alanları arasında görev değişikliği yapılmaz.

#### **5.3.6. Yetkisiz İşlemler için Yaptırımlar**

TÜRKTRUST personelinin teşebbüs edeceği yetkisiz işlemler için, TÜRKTRUST insan kaynakları yönergesi uyarınca gerekli disiplin cezaları uygulanır. Eğer bu yetkisiz işlem sonucunda TÜRKTRUST ya da TÜRKTRUST müşterileri zarar görürse, bu zararın ilgili çalışandan tazmini yoluna gidilir.

TÜRKTRUST yetkisiz işlem yapanlar hakkında, Kanun, Yönetmelik ve Tebliğ gereğince işlem yapılmasını temin etmek üzere, adli mercilere başvuruda bulunur.

#### **5.3.7. Bağımsız Alt Yüklenici Gereklilikleri**

Sertifika süreçleri dahilinde alt yükleniciler aracılığıyla yürütülen işlemler için, TÜRKTRUST ile alt yüklenici firma arasında bir hizmet sözleşmesi imzalanır. Bu hizmet sözleşmesi TÜRKTRUST'ın gerektirdiği güvenlik koşullarını ve hizmet esaslarını ortaya koyar.



**5.3.8. Personele Sağlanan Dokümantasyon**

TÜRKTRUST personeline, Sİ ve SUE kitapçıkları, sertifika süreçleriyle ilgili uygulama ve güvenlik prosedürleri, çalışanların rollerine göre düzenlenmiş iş talimatları, kullanılan yazılım ve donanıma ait kullanım kılavuzları sağlanır.

**5.4. Denetim Kayıtları Alma Prosedürleri****5.4.1. Kaydedilen Olay Tipleri**

Sertifika yaşam döngüsü içinde yürütülen tüm sertifika hizmetlerine ait kayıtlar TÜRKTRUST tarafından tutulur. Bu kayıtların arasında sertifika başvuru kayıtları; üretilen, yenilenen, askıya alınan ve iptal edilen sertifikalarla ilgili her türlü müşteri talebinin kayıtları; üretilip yayımlanan sertifikalar ile SİL'ler hakkındaki kayıtlar; TÜRKTRUST birimlerindeki güvenilir rollere sahip çalışanların işlem kayıtları; çalışanların TÜRKTRUST birimlerine giriş ve çıkış kayıtları ile sistem modüllerine erişim kayıtları; doküman takibiyle ilgili kayıtlar; yazılım ve donanım kurulum, güncelleme ve onarım kayıtları sayılabilir.

İşlem kayıtları tutulurken temel olarak işlemin tanımı, işlemi yapan kişi, işlemin tarih ve zaman bilgisi kaydedilir.

**5.4.2. Kayıtları İşleme Sıklığı**

Denetim kayıtları sürekli olarak tutulur ve periyodik olarak bu kayıtların yedekleri alınarak arşivlenir.

**5.4.3. Denetim Kayıtlarının Saklanma Süresi**

TÜRKTRUST işleyişine ait denetim kayıtları, bir yıl süreyle sistemde tutulur. Bu sürenin sonunda yasal düzenlemeler uyarınca saklanmak üzere arşivlenir.

**5.4.4. Denetim Kayıtlarının Korunması**

Denetim kayıtları fiziksel ve elektronik güvenlik önlemleriyle korunur, sadece yetkili kişilerin erişimine açık tutulur. Denetim kayıtlarının veri bütünlüğü anahtarlanmış özet yöntemiyle sağlanmaktadır.

**5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri**

Yedekleme prosedürleri uyarınca, kayıtların periyodik olarak tesis içi ve tesis dışı yedekleri alınır.

**5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış)**

Denetim kayıtları, ESHS iş süreçlerinin yürütülmesinde kullanılan ESHS yönetim yazılımı tarafından tutulur.

**5.4.7. Olayı Yaratan Kişiyi Bilgilendirme**

Rutin işlemlerin dışında kalan denetim kayıtlarının oluştuğu durumlarda, olayı yaratan kişi sistem tarafından uyarılır. Olayın çeşidine ve önemine göre, sistem üzerinde olayı yaratan kişinin yönetiminden sorumlu üst yetki seviyesindeki kişi veya kişiler de bilgilendirilebilir.

**5.4.8. Zarar Görebilirlik Değerlendirmesi**

Denetim kayıtları sistem üzerinde raporlanır. Bu raporların analiz edilmesiyle sistemdeki güvenlik açıkları ve sertifika süreçlerindeki hata noktaları belirlenerek önlem alınmaktadır.

## **5.5. Kayıtların Arşivlenmesi**

### **5.5.1. Arşivlenen Kayıt Tipleri**

TÜRKTRUST işleyişi uyarınca, Madde 5.4.'te belirtilen tüm denetim kayıtları, sertifika süreçlerine yönelik başvuru, talep ve talimatlar, kağıt üzerinde alınan tüm destekleyici belgeler ile sertifika sahibi sözleşmesi, müşterilerle yapılan tüm yazışmalar, üretilen tüm sertifikalar ve SİL'ler, Sİ ve SUE kitapçıklarının tüm sürümleri, uygulama prosedürlerinin, talimatların ve formların bütünü, TÜRKTRUST arşiv prosedürleri uyarınca arşivlenir. Arşivlerin büyük bir kısmı elektronik ortamda tutulurken, kağıt üzerindeki yazışmalar, formlar, belgeler, müşteri dosyaları, şirket belgeleri gibi kayıtlar da kağıt ortamında arşivlenir.

### **5.5.2. Arşivlerin Saklanma Süresi**

Nitelikli elektronik sertifikalarla ilgili TÜRKTRUST işleyişine ait arşivler, yasal düzenlemeler uyarınca en az 20 (yirmi) yıl süreyle saklanır. Sunucu ve nesne imzalama sertifikalarına ilişkin arşivler de TÜRKTRUST tarafından 20 (yirmi) yıl süreyle korunur. Deneme sertifikalarına ait işlemlerin kayıtları saklanmaz.

### **5.5.3. Arşivlerin Korunması**

Arşivler fiziksel ve elektronik güvenlik önlemleriyle korunur ve sadece yetkili kişilerin erişimine açık tutulur.

### **5.5.4. Arşivlerin Yedeklenme Prosedürleri**

Yedekleme prosedürleri uyarınca, elektronik ortamdaki arşivlerin yedekleri tesis içinde ve dışında tutulur. Kağıt ortamdaki arşivlerin ise yedekleri alınmaz.

### **5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri**

TÜRKTRUST elektronik arşiv kayıtları zaman damgasıyla saklanır.

### **5.5.6. Arşiv Toplama Sistemi**

Arşiv kayıtları, TÜRKTRUST arşiv yönetim sistemi kullanılarak derlenir.

### **5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri**

TÜRKTRUST arşiv bilgilerine, Kurum talebi veya yasal süreçlerin bir gereği olarak kontrollü erişim sağlanır.

## **5.6. Anahtar Değişimi**

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin kök ve alt kök sertifikalarının anahtar yenileme işlemleri, TÜRKTRUST merkezi tarafından yönetilir.

## **5.7. Güvenliğin Yitilmesi ve Afet Durumlarında Yapılacaklar**

### **5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar**

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST afet yönetim prosedürleri ve iş sürekliliği planları uyarınca duruma müdahale edilir.

### **5.7.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması**

Bilgisayar kaynaklarının zarar görmesi, yazılım birimlerinde veya işleyişe dair verilerde bozulma oluşması durumunda, öncelikle tesisteki hasarlı donanım yeniden işler hale getirilir. Daha sonra, kaybolan kayıtlar yedekleme sistemleri aracılığıyla yeniden oluşturulur ve sertifika hizmetleri tekrar etkin hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün sertifika

sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir. Gerekli durumlarda bazı sertifikalar iptal edilip yeni sertifika üretimine geçilir.

### **5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi**

TÜRKTRUST imza oluşturma verilerinin güvenliğinin ve güvenilirliğinin yitilmesi durumunda, TÜRKTRUST afet yönetim prosedürleri ve iş sürekliliği planları uyarınca, ilgili sertifikalar iptal edilir ve Madde 5.6. uyarınca yeni imza oluşturma verisi oluşturularak devreye alınır. İptal edilen sertifikaların yerine prosedürler gereği yeni sertifikalar üretilir ve bu durumdan etkilenebilecek olan bütün sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

### **5.7.4. Afet Sonrası İş Sürekliliği Yetenekleri**

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST afet yönetim prosedürleri ve iş sürekliliği planları uyarınca duruma müdahale edilir.

## **5.8. TÜRKTRUST veya Kayıt Merkezi İşletmesine Son Verilmesi**

Kayıt merkezlerinin yaptıkları tüm sertifika başvuru ve kayıt işlemlerine ait elektronik ve kağıt ortamdaki kayıtlar, sertifika başvurusu ve işlem taleplerinin sonuçlandırılabilmesi için TÜRKTRUST merkezinde tutulmaktadır. Bu nedenle, bir kayıt merkezinin işletmesine son verilmesi durumunda, kayıt merkezinde tutulan kayıtlar ve kayıt merkezinin ESHS ile iletişimde kullandığı imza oluşturma verisi imha edilir.

TÜRKTRUST, sertifika üretim hizmetlerine son vermesi durumunda, Kanun ve Yönetmelik gereği bu durumu en az 3 ay önce Kuruma bildirir ve kamuoyuna duyurur. TÜRKTRUST, işletmenin durdurulması prosedürü uyarınca, mevcut sertifikalarla ilgili tüm bilgi, belge ve kayıtları, Kanun gereği bir ay içinde başka bir ESHS'ye devreder. Kurum, uygun görmesi halinde, bir ayı geçmemek üzere ek süre verebilir. Eğer devir işlemi belirtilen süreler içinde tamamlanamazsa, TÜRKTRUST ilgili sertifikaları iptal eder ve tüm ilgili tarafları bu durumdan haberdar eder. Bu durumda, TÜRKTRUST son SİL kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

## **6. TEKNİK GÜVENLİK KONTROLLERİ**

Sİ kitapçığının bu kısmında, TÜRKTRUST'ın sertifika hizmetleriyle ilgili iş süreçlerinde kullanılan imza oluşturma verilerinin ve erişim verilerinin yönetimi ile teknik altyapıya ve sertifika hizmetlerinin işleyişine yönelik güvenlik kontrolleri yer almaktadır.

### **6.1. Anahtar Çifti Üretimi ve Kurulumu**

#### **6.1.1. Anahtar Çifti Üretimi**

Nitelikli elektronik sertifika sahiplerinin imza oluşturma ve doğrulama verileri TÜRKTRUST tarafında veya müşteri tarafında üretilebilir. Üretim TÜRKTRUST tarafında gerçekleştirildiğinde, sertifika üretim merkezinde uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde işlem gerçekleştirilir. Bu durumda müşterilere ait imza oluşturma verileri TÜRKTRUST'ta saklanmaz, hiçbir kopyası alınmaz. Buna alternatif olarak, güvenli elektronik imza oluşturma aracı edinen bir başvuru sahibi, ilgili TÜRKTRUST sertifika başvuru yöntemleri uyarınca imza oluşturma ve doğrulama verilerini kendisi de üretebilir.

Sunucu ve nesne imzalama sertifikalarının imza oluşturma ve doğrulama veri çiftleri başvuru sahiplerinin kontrolü altındaki sunucularda üretilir.

Deneme sertifikalarına ait anahtar çiftleri, otomatik sertifika üretimi sırasında başvuru sahibinin istemci yazılımı veya sahip olduğu imza oluşturma aracı tarafından üretilir. Deneme sertifikalarında imza oluşturma verisinin güvenli elektronik imza oluşturma aracında üretilmesi veya saklanması şartı aranmaz.

TÜRKTRUST kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, teknik ve idari güvenlik önlemleri alınmış ortamlarda, TÜRKTRUST kök sertifikaları anahtar üretim prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur.

Anahtar üretiminin TÜRKTRUST'ta olduğu tüm durumlarda, anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde üretilir.

Anahtar çiftini kendi tarafında üreten nitelikli elektronik sertifika başvurusu sahipleri, güvenli elektronik imza oluşturma aracı kullanmaktan kendileri sorumludur.

Sunucu sertifikası başvurusunda bulunacak sunucu sorumluları ile nesne imzalama sertifikası başvurusunda bulunacak teknik sorumlular, sertifika başvurusu sırasında anahtar üretiminin güvenli yapılmasından sorumludur.

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

Anahtar çifti TÜRKTRUST tarafından oluşturulan nitelikli elektronik sertifikalar için, imza oluşturma verisi güvenli elektronik imza oluşturma aracının içinde kurye ile kimlik kontrolü ve imza karşılığında teslim edilmek üzere sertifika sahibine gönderilir. Güvenli elektronik imza oluşturma aracının erişim verisi de ayrıca kurye ile kimlik kontrolü ve imza karşılığında sertifika sahibine teslim edilir.

Sunucu sertifikaları, nesne imzalama sertifikaları ve deneme sertifikalarının imza oluşturma verileri müşteri tarafında üretildiği için başvuru sahibinin sorumluluğu altındadır.

#### **6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması**

Anahtar üretiminin müşteri tarafında gerçekleştirildiği durumlarda, sertifika talebinin imza doğrulama verisine karşılık gelen imza oluşturma verisiyle imzalanmış olması şarttır. Böylelikle talep, içeriğindeki olası bir değişikliğin tespiti mümkün olur. Talep bilgisine üçüncü

kişilerin erişimini engellemek için, talebin güvenli elektronik haberleşme yoluyla TÜRKTRUST'a gönderilmesi sağlanır.

#### **6.1.4. TÜRKTRUST İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması**

TÜRKTRUST kök ve alt kök sertifikaları üçüncü kişilerin erişebileceği şekilde yayımlanır. Böylelikle, TÜRKTRUST'a ait imza doğrulama verileri üçüncü kişilerce kullanılabilir.

#### **6.1.5. Anahtar Uzunlukları**

TÜRKTRUST sertifikaları, Tebliğ'le belirlenen minimum anahtar uzunluklarına uygundur.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikaları üretilirken en az 2048 bit RSA anahtar çiftleri kullanılır.

TÜRKTRUST tarafından üretilen tüm son kullanıcı sertifikaları için en az 1024 bit RSA anahtar çifti kullanılır.

#### **6.1.6. Anahtar Üretimi ve Kalite Kontrolü**

Anahtar üretiminin TÜRKTRUST merkezinde olması durumunda, anahtar çifti uygun güvenlik düzeyine sahip donanım güvenlik modüllerinde, Tebliğ'de belirlenen parametrelere uygun olarak üretilir.

Anahtar üretiminin müşteri tarafında olduğu durumlarda, imza oluşturma verisinin uygun araçlarda ve nitelikte üretiminden müşteri sorumludur.

#### **6.1.7. Anahtar Kullanım Amaçları**

TÜRKTRUST sertifika hizmetleri kapsamında üretilen son kullanıcı anahtarları, kimlik doğrulama ve elektronik imza amaçlı kullanılır.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına ait anahtarlar, sertifika ve SİL imzalamak için kullanılır.

Anahtarların kullanım amacı, X.509 v3 sertifikaların anahtar kullanım alanlarında belirtilir.

### **6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri**

#### **6.2.1. Kriptografik Modül Standartları ve Kontroller**

TÜRKTRUST'ta anahtar çifti üretimi ile sertifika ve SİL imzalama işlemleri, Tebliğ'le belirlenen standartlarla uyumlu, güvenli kriptografik donanım modüllerinde gerçekleştirilir.

Nitelikli elektronik sertifika sahiplerinin imza oluşturma verileri TÜRKTRUST tarafında üretildiğinde, Tebliğ'le belirlenen standartlarda güvenlik düzeyine sahip akıllı kartlara, akıllı çubuklara ve benzeri güvenli elektronik imza oluşturma araçlarına yüklenir. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verilerinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir. Sertifika başvuru sahibinin kendi tarafında anahtar üretimi yapması durumunda, yine Tebliğ'de tanımlı güvenlik düzeyine sahip bir araç kullanılmalıdır.

#### **6.2.2. İmza Oluşturma Verisinin Çok Kullanımcılı Kontrolü**

TÜRKTRUST'a bağlı sertifika üretim merkezlerinin kök ve alt kök sertifikalarına erişim yetkili kişiler dışında yasaklanmıştır. Fiziksel ve teknik erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, ilgili modüle aynı anda iki ayrı yetkilinin bağlanması ve sistem

tarafından onaylanmasıyla mümkündür. Sistem içindeki hiçbir yetkilinin tek başına TÜRKTRUST imza oluşturma verilerini kullanabilmesine izin verilmez.

Nitelikli elektronik sertifikaların imza oluşturma verileri sadece sertifika sahiplerinin kendi sorumluluğu altındaki, şifre kontrollü güvenli elektronik imza oluşturma araçlarında saklanır. Aracın şifresi bilinmediği sürece imza oluşturma verisine kullanılamaz. Şifre güvenliği araç donanımı tarafından sağlanır.

Sunucu sertifikalarının ve nesne imzalama sertifikalarının imza oluşturma verilerinin güvenliğinin sağlanmasından sunucu sorumluları ile teknik sorumlular sorumludur.

Deneme sertifikaları için donanım kontrolü uygulanmaz.

### **6.2.3. İmza Oluşturma Verisinin Saklanması**

TÜRKTRUST tarafından üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri TÜRKTRUST tarafından kesinlikle saklanmaz, bu verilerin bir kopyası alınmaz.

### **6.2.4. İmza Oluşturma Verisinin Yedeklenmesi**

TÜRKTRUST tarafından üretilen son kullanıcı sertifikalarına bağlı imza oluşturma verileri yedeklenmez, bu verilerin kopyası alınmaz. Nitelikli elektronik sertifikalar, sunucu sertifikaları, nesne imzalama sertifikaları ve deneme sertifikalarına bağlı imza oluşturma verileri, sertifika sahiplerinin, sunucu ve teknik sorumluların sorumluluğundadır.

Herhangi bir afet durumu veya sorun anında hizmetlerin kesintiye uğramaması amacıyla, TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri TÜRKTRUST kök sertifikaları anahtar üretim prosedürü uyarınca yedeklenir ve fiziksel ve teknik güvenlik kontrolleri altında saklanır.

### **6.2.5. İmza Oluşturma Verisinin Arşivlenmesi**

Uygulama dışıdır.

### **6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi**

ESHS kök ve alt kök sertifikalarına ait imza oluşturma verileri güvenli kriptografik donanım modüllerinde üretilir. Bu veriler yedekleme amacıyla kullanılan güvenli modüllere transferi dışında hiçbir biçimde modül dışına çıkarılamaz. Yedekleme işlemi, kriptografik donanım modülü üzerinde şifreli bir biçimde gerçekleştirilir.

Anahtar üretiminin TÜRKTRUST'ta olduğu durumlarda, anahtar çifti uygun güvenlik düzeyine sahip güvenli kriptografik donanım modüllerinde üretilir ve nitelikli elektronik sertifika sahiplerinin güvenli elektronik imza oluşturma araçlarına güvenli yollarla taşınır.

Anahtar üretiminin müşteri tarafında olduğu durumlarda, imza oluşturma verisinin kontrolü ve olası transferi sırasında güvenliğinin sağlanması müşterinin sorumluluğundadır.

### **6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde saklanır.

Nitelikli elektronik sertifika sahiplerinin imza oluşturma verileri TÜRKTRUST tarafında üretildiğinde, üretildikleri Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır. Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verisinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmiştir.

Sertifika başvuru sahibinin kendi tarafında anahtar üretimi yapması durumunda, yine Tebliğ'de tanımlı güvenlik düzeyine sahip bir güvenli elektronik imza oluşturma aracı kullanılmalıdır.

Sunucu sertifikalarına ve nesne imzalama sertifikalarına bağlı imza oluşturma verilerinin üretildikleri sunucularda güvenli bir biçimde saklanmasından sunucu ve teknik sorumlular sorumludur.

Deneme sertifikalarının imza oluşturma verilerinin saklanması sertifika sahibinin sorumluluğundadır.

### **6.2.8. İmza Oluşturma Verisinin Aktive Edilme Yöntemi**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde buldukları donanım güvenlik modülü üzerinde, iki yetkilinin hazır bulunmasıyla aktive edilir.

Nitelikli elektronik sertifikalara bağlı imza oluşturma verileri, güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle aktive edilir.

Sunucu sertifikaları ve nesne imzalama sertifikaları için imza oluşturma verisinin aktivasyonu müşteri yazılımı üzerinden yapılır.

Deneme sertifikalarına bağlı imza oluşturma verilerinin aktivasyon şekli müşteri kontrolü altındadır.

### **6.2.9. İmza Oluşturma Verisinin Deaktive Edilme Yöntemi**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde buldukları donanım güvenlik modülü üzerinde sadece belirli bir süreyle ve işlem bazlı aktive edilir; işlem tamamlandıktan ya da süre bittikten sonra deaktive olur. İmza oluşturma verisinin yeniden kullanılabilmesi için, yetkililerin tekrar sisteme tanıtılarak imza oluşturma verisinin aktive edilmesi gerekir.

Nitelikli elektronik sertifikalara bağlı imza oluşturma verileri güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle belirli bir süre için aktive edilir ve süre sonunda deaktive olur. Ayrıca, sertifika sahibi kendi isteğiyle de imza oluşturma verisini deaktive edebilir. İmza oluşturma verisinin yeniden kullanılabilmesi için, sertifika sahibinin güvenli elektronik imza oluşturma aracı şifresini tekrar girmesi gerekir.

Sunucu sertifikaları, nesne imzalama sertifikaları ve deneme sertifikaları için imza oluşturma verisinin deaktive edilmesi müşteri yazılımı üzerinden yapılır.

### **6.2.10. İmza Oluşturma Verisi Yok Etme Metodu**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, içinde buldukları donanım güvenlik modüllerinin sıfırlama özelliği kullanılarak sadece yetkili kişiler tarafından yok edilebilir. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

Nitelikli elektronik sertifikalara bağlı olan ve güvenli elektronik imza oluşturma aracı içinde saklanan imza oluşturma verileri, aracın yönetim yazılımı kullanılarak veya donanımsal olarak yok edilebilir.

Son kullanıcı sertifikalarına ait imza oluşturma verilerinin sertifika iptali ya da sertifika süresinin dolmasından sonra yok edilmesiyle ilgili bir koşul yoktur. Sertifika sahibi, sunucu sorumlusu ya da teknik sorumlu, isteği halinde imza oluşturma verisini yok edebilir.



### **6.2.11. Kriptografik Modül Değerlendirmesi**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verileri, Tebliğ'de tanımlı güvenlik düzeyine sahip kriptografik donanım modüllerinde üretilir ve saklanır.

Nitelikli elektronik sertifika sahiplerinin imza oluşturma verileri de, Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır.

## **6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular**

### **6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza doğrulama verileri, ESHS tarafından 20 yıl süreyle saklanır.

### **6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri**

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikaların, sunucu sertifikalarının ve nesne imzalama sertifikalarının geçerlilik süresi 1 (bir), 2 (iki) veya 3 (üç) yıl, deneme sertifikalarının geçerlilik süresi 3 (üç) aydır. 1 (bir) yıllık nitelikli elektronik sertifikalar için kullanılan anahtar çiftlerinin güvenli geçerlilik süresi ise toplam 3 (üç) yılı aşamaz.

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının geçerlilik süreleri 10 (on) yılı aşmaz. Bu sürenin sonunda sertifikalar yenilenirken mutlaka anahtar çiftleri de yenilenir.

## **6.4. Erişim Şifreleri**

### **6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının imza oluşturma verilerine ya da bu verilerin bulunduğu kriptografik modüllere erişim, iki ayrı yetkilinin hazır bulunmasıyla ve erişim şifreleriyle gerçekleşir.

TÜRKTRUST yetkilileri ile nitelikli elektronik sertifika sahiplerinin imza oluşturma verilerine ait erişim şifreleri, sertifika üretimi sırasında oluşturulur ve kapalı zarfa basılarak kendilerine iletilir. Bu kişiler, sadece kendi kontrolleri altında olan bu şifreleri istedikleri zaman değiştirebilir.

Sunucu sertifikalarının ve nesne imzalama sertifikalarının imza oluşturma verilerinin erişim şifreleri sunucu sorumlusunda ve teknik sorumluda bulunur. Deneme sertifikalarının imza oluşturma verileri için erişim şifreleri müşteri tarafında oluşturulur.

### **6.4.2. Erişim Şifrelerinin Korunması**

TÜRKTRUST yetkilileri ile nitelikli elektronik sertifika sahiplerinin imza oluşturma verilerine ait erişim şifreleri, kapalı zarfa basılarak kendilerine iletiildiği için sadece kendi kontrolleri altındadır. Bu erişim şifrelerinin hiçbir kopyası bulunmaz ve TÜRKTRUST tarafından saklanmaz. Sertifika sahipleri erişim şifrelerini istedikleri zaman değiştirebilir ve periyodik olarak değiştirilmesi önerilir. Şifrelerin sertifika sahibine tesliminden sonra gizliliğinin ve güvenliğinin sağlanması sertifika sahibinin sorumluluğundadır.

TÜRKTRUST yetkilileri de güvenlik prosedürleri gereği kendi imza oluşturma verilerine ait erişim şifrelerini belirtilen sıklıkta değiştirmek ve kendileri dışında kimse tarafından bilinmemesini sağlamakla yükümlüdür.

Sunucu sertifikalarının, nesne imzalama sertifikalarının ve deneme sertifikalarının imza oluşturma verilerinin erişim şifrelerinin gizliliği ve güvenliği sunucu sorumluları, teknik sorumlular ve sertifika sahipleri tarafından sağlanmalıdır.



**6.4.3. Erişim Şifreleriyle İlgili Diğer Konular**

Erişim şifrelerinin TÜRKTRUST tarafından üretilip sertifika sahibine iletildiği nitelikli elektronik sertifika üretim ve dağıtım süreci uyarınca, bu şifreler kapalı zarflara basılır ve güvenli elektronik imza oluşturma aracından ayrı olarak kurye ile sertifika sahiplerine iletilir. İmza oluşturma aracı ile erişim şifresinin ayrı gönderilmesi, kayıp, açığa çıkma veya yanlış kişiler tarafından ele geçirilme durumlarına karşı güvenlik önlemidir. Kurye gönderiminin güvenilir biçimde sağlanabilmesi için TÜRKTRUST ile kurye firması arasında güvenlik koşulları ve sorumlulukların açık olarak belirtildiği bir hizmet sözleşmesi imzalanır.

**6.5. Bilgisayar Güvenlik Kontrolleri****6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri**

TÜRKTRUST tarafından yürütülen sertifika iş süreçleri kapsamında, tüm bilgi sistemlerine erişim ve bu sistemlerin işletilmesi için aşağıda yer alan güvenlik kontrolleri uygulanmaktadır:

- Bilgisayar sistemlerinde güvenilir ve sertifikalı donanım ve yazılım ürünleri kullanılmaktadır.
- Bilgisayar sistemleri yetkisiz erişime ve güvenlik açıklarına karşı korunmuştur. Penetrasyon ve istemsiz erişim kontrolleri kurulmuş ve ilgili testlerle kontrollerin güncelliği ve sürekliliği sağlanmıştır.
- Bilgisayar sistemleri ağ güvenliği saldırılarına karşı korunmuştur.
- Bilgisayar sistemlerine erişim hakları ve kimlik doğrulama, TÜRKTRUST personeline verilen şifrelerle sağlanmaktadır.
- Bilgisayarlara erişim hakları, yetkili personele tanımlanan rollerle sınırlanmıştır.
- Bilgisayar sistemini oluşturan birimler arasındaki veri iletişimi güvenli olarak yapılmaktadır.
- İşlem kayıtları sürekli olarak tutulduğu için bilgisayar sistemlerinde oluşabilecek sorunlar kısa zamanda ve doğru biçimde belirlenebilmektedir.

**6.5.2. Bilgisayar Güvenliği Sıralaması**

Uygulama dışıdır.

**6.6. Yaşam Döngüsü Teknik Kontrolleri****6.6.1. Sistem Geliştirme Kontrolleri**

Uygulama dışıdır.

**6.6.2. Güvenlik Yönetimi Kontrolleri**

İşlevsel sistemler ve TÜRKTRUST içinde kullanılan bilgisayar ağının güvenliğinin sağlanması için uygun araçlar kullanılmakta ve güvenlik prosedürleri işletilmektedir.

TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı sertifikası sahibidir.

**6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri**

Uygulama dışıdır.

**6.7. Ağ Güvenlik Kontrolleri**

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının imza oluşturma verileri, ağ güvenliği sağlanmış ortamlarda kullanılmaktadır. Bu sistemler fiziksel ve teknik olarak korunurlar.

TÜRKTRUST içindeki diğer tüm sistemler de uygun ağ güvenliği yöntemleriyle korunmaktadır. Güvenlik duvarları, anahtarlama cihazları ve yönlendiriciler gibi tüm ağ elemanları, doğru ve güvenli bir biçimde ağ konfigürasyonu prosedürleri uyarınca kurulmuştur. Bu ağ elemanlarının güvenlik kontrolleri prosedürler uyarınca sürekli olarak yapılmaktadır.

TÜRKTRUST'a bağlı kayıt merkezleri, yürüttükleri sertifika işlemleriyle ilgili kayıtları TÜRKTRUST merkezine internet üzerinden güvenli ağ bağlantısıyla iletir.

**6.8. Zaman Damgası**

TÜRKTRUST tarafından sertifika hizmetlerinin yürütülmesi sırasında ilgili işlemlere ait elektronik kayıtlar, zaman damgası hizmetlerinde kullanılan zaman kaynağı ile senkronize edilmiş zaman bilgisini içerir. Kayıt bütünlüğü anahtarlanmış özet yöntemi kullanılarak korunur ve arşivleme aşamasında zaman damgası kullanılır.

## 7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (SİL) VE OCSP PROFİLLERİ

Sİ kitapçığının bu kısmında, TÜRKTRUST tarafından üretilen sertifikalar ile SİL'lerin profilleri ve verilen OCSP hizmetinin yapısı yer almaktadır.

### 7.1. Sertifika Profili

TÜRKTRUST sertifikalarında temel olarak aşağıdaki alanlar bulunur:

- Sertifika sahibi bilgileri (isim, şirket, çalışılan birim, yer, ülke, e-posta vb.)
- Sunucu sertifikalarında sunucu bilgileri (alan adı, sunucu adı, şirket adı vb.)
- Nesne imzalama sertifikalarında sertifika sahibine ait bilgiler (şirket, çalışılan birim vb.)
- Ülke adı TR (Türkiye) olmak üzere TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı bilgileri
- Sertifika geçerlilik süresinin başlangıç ve bitiş zamanı
- Kullanılan elektronik imza oluşturma algoritmaları
- Sertifika sahibi imza doğrulama verisi
- Sertifika seri numarası
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı imzası

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalarda, Kanun gereği aşağıdaki bilgiler de yer alır:

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi,
- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri,
- Varsa sertifikanın kullanım şartları ve sertifika kullanımına yönelik maddi işlem sınırı.

#### 7.1.1. Sürüm Numaraları

TÜRKTRUST tarafından oluşturulan kök ve alt kök sertifikalar ile son kullanıcı sertifikaları, "IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002" dokümanı uyarınca X.509 v3 sürümünü destekler.

#### 7.1.2. Sertifika Uzantıları

TÜRKTRUST, RFC 3280 - X.509 v3 standardı uyarınca tanımlanmış olan tüm sertifika uzantılarını destekler. Sertifikanın çeşidine göre, anahtar kullanımı (key usage), sertifika ilkeleri (certificate policies extension), kullanıcı alternatif isimleri (subject alternative names), temel kısıtlar (basic constraints), uzatılmış anahtar kullanımı (extended key usage), SİL dağıtım noktaları (CRL distribution points), ESHS anahtar tanımlayıcısı (authority key identifier), kullanıcı anahtar tanımlayıcısı (subject key identifier) uzantıları uygun biçimde ayarlanır.

Nitelikli elektronik sertifikalar, "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile, January 2001" uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.

**7.1.3. Algoritma Nesne Tanımlayıcıları**

TÜRKTRUST tarafından üretilen sertifikalarda özetleme algoritması olarak SHA1; imza oluşturma ve doğrulama verilerinin üretimi ile elektronik imza için RSA kullanılır. Kullanılan algoritmaların nesne tanımlayıcıları üretilen sertifikaların ilgili alanında belirtilir.

**7.1.4. İsim Biçimleri**

TÜRKTRUST tarafından üretilen sertifikalarda X.500 biçiminde ayırt edilebilir isimler kullanılır.

**7.1.5. İsim Kısıtları**

TÜRKTRUST tarafından üretilen sertifikalarda anonim veya takma adlar kullanılmaz. TÜRKTRUST nitelikli elektronik sertifikalarındaki isimlerde ayırt edici özellik olarak T.C. kimlik numarası kullanılır.

**7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı**

TÜRKTRUST tarafından üretilen sertifikaların "sertifika ilkeleri" uzantısında, sertifikanın çeşidine göre bu Sİ kitapçığı Madde 1.2.'de belirtilen ilgili sertifika ilkeleri nesne tanımlayıcı numarası (OID) kullanılır.

**7.1.7. İlke Kısıtları Uzantısının Kullanımı**

TÜRKTRUST alt kök sertifikalarında ihtiyaca göre ilke kısıtları uzantısı kullanılabilir.

**7.1.8. İlke Niteleyicilerinin Yazımı**

TÜRKTRUST tarafından üretilen sertifikaların "sertifika ilkeleri" uzantısında, ilke niteleyicisi olarak SUE kitapçığına erişim bilgisi URL olarak verilmiştir.

**7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği**

Uygulama dışıdır.

**7.2. SİL Profili**

TÜRKTRUST tarafından yayımlanan SİL'lerde temel olarak, TÜRKTRUST elektronik imzasıyla birlikte yayımlayıcı bilgileri, SİL'in yayımlanma tarihi, bir sonraki SİL'in yayımlanma tarihi ve iptal edilen sertifikaların seri numarası ile iptal tarih ve zamanı yer alır.

**7.2.1. Sürüm Numarası**

TÜRKTRUST tarafından oluşturulan SİL'ler, "IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002" dokümanı uyarınca X.509 v2 sürümünü destekler.

**7.2.2. SİL ve SİL Giriş Uzantıları**

TÜRKTRUST tarafından yayımlanan SİL'lerde, RFC 3280 tarafından tanımlanan uzantılar kullanılır.

**7.3. OCSP Profili**

TÜRKTRUST gerçek zamanlı bir sertifika durum sorgusu olan OCSP desteğini kesintisiz olarak sağlar. Bu hizmetle, uygun sertifika durum sorguları alındığında, sorguda talep edilen sertifikaların durumu ve protokol gereği gereken diğer ek bilgiler sorgu cevabı olarak talep sahibine döndürülür.

**7.3.1. Sürüm Numarası**

TÜRKTRUST tarafından verilen OCSP hizmeti, "IETF RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999" dokümanı uyarınca v1 protokol sürümünü destekler.

**7.3.2. OCSP Uzantıları**

TÜRKTRUST tarafından verilen OCSP hizmeti içeriğinde, RFC 2560 tarafından tanımlanan uzantılar kullanılır. Ancak, temel OCSP bilgileri dışındaki tüm uzantıların kullanılması zorunlu değildir.

## **8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER**

TÜRKTRUST, ilgili mevzuat gereğince Telekomünikasyon Kurumu tarafından denetlenir.

Ayrıca, tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca periyodik olarak uygunluk denetimine tabi tutulur.

ESHS hizmetlerinin verilmesi ve işletmeye dair güvenlik koşulları bir iç denetim planı uyarınca kontrol altında tutulur.

### **8.1. Denetim Sıklığı ve Durumları**

Telekomünikasyon Kurumu, düzenleyici ve denetleyici Kurum olarak gerekli gördüğü durumlarda re'sen denetim yapar. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

Tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca her yıl uygunluk denetimine tabi tutulur. Her üç yılda bir bu sertifikasyon yenilenir.

İç denetim, plan gereği yılda en az bir defa, gerek görülmesi durumunda daha fazla sayıda tekrar edilir.

### **8.2. Denetçinin Kimliği ve Özellikleri**

Telekomünikasyon Kurumu, Kanunla belirlenmiş düzenleyici ve denetçi kurumdur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu yetkilendirilmiş bir denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal denetimi, TÜRKTRUST yetkili personeli tarafından yapılır. İç denetim, TÜRKTRUST bünyesindeki Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve Kalite Yönetim Sistemi Sorumlusu tarafından yürütülür.

### **8.3. Denetçinin ESHS'yle İlişkisi**

Denetçi kuruluş olan Kurum, Kanun gereği Türkiye'de nitelikli elektronik sertifikalarla ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu bağımsız ve yetkili bir denetçi tarafından gerçekleştirilir.

TÜRKTRUST'ın kurumsal denetimi, TÜRKTRUST yetkili personeli tarafından yapılır.

### **8.4. Denetimde Kapsanan Başlıklar**

Kurum'un denetimi Kanunla kendisine verilen yetki çerçevesinde, TÜRKTRUST'ın elektronik sertifika hizmetlerine dair tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri kapsar.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonu, TÜRKTRUST elektronik sertifika ve zaman damgası hizmetleri kapsamındadır.

İç denetimde de, yasal denetim altına giren tüm konular kapsanır.

### **8.5. Eksiklik Durumunda Yapılacaklar**

Yönetmelik gereği Kurum tarafından yapılan denetimler sırasında, TÜRKTRUST'ın faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önemli konuların belirlenmesi durumunda, ilgili mevzuatta öngörülen yaptırım ve cezalar uygulanır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetimleri sırasında saptanan eksikliklerin majör nitelikte olması sertifikanın geri alınmasına neden olur. Minör eksikler, bir sonraki denetim dönemine kadar TÜRKTRUST tarafından giderilir.

TÜRKTRUST tarafından yapılan iç denetimlerde belirlenen aksaklıklar hakkında düzeltici ve önleyici faaliyetler yürütülür.

### **8.6. Sonuçların Bildirilmesi**

Kanun gereği Kurum tarafından yapılan denetimin sonuçları gerek duyulduğu takdirde resmi yollarla TÜRKTRUST'a iletilir. Kurum'un bir geri bildirimde bulunmaması, olumsuz bir değerlendirmenin olmadığı anlamını taşır.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi denetim sonuçları, denetçi tarafından resmi olarak TÜRKTRUST'a bildirilir.

İç denetim sonuçları ise, iç denetim sonuç raporlarında yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

## **9. DİĞER İŞ KONULARI VE YASAL KONULAR**

Sİ kitapçığının bu kısmında, TÜRKTRUST'ın ticari ve yasal uygulamaları ile sertifika süreçleri uyarınca yerine getirilmesi gereken hizmet koşulları yer almaktadır.

### **9.1. Ücretler**

#### **9.1.1. Sertifika Üretim ve Yenileme Ücretleri**

TÜRKTRUST tarafından üretilen sertifikalar, çeşitlerine göre farklı fiyatlarla ücretlendirilir.

Nitelikli elektronik sertifikalar, içeriklerinde yer alan maddi işlem sınırı ölçüsünde, sertifika üretim maliyetleri ve piyasa koşulları uyarınca fiyatlandırılır. Artan maddi işlem sınırı, artan sertifika mali sorumluluk sigortası primleri üzerinden sertifika fiyatlarına yansıtılır.

Sunucu sertifikaları ile nesne imzalama sertifikaları, sertifika çeşidine, kullanım süresine ve özelliklerine bağlı olarak fiyatlandırılır.

Deneme sertifikaları ücretsizdir.

Güncel sertifika fiyat bilgileri, TÜRKTRUST web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

#### **9.1.2. Sertifika Erişim Ücretleri**

TÜRKTRUST tarafından üretilen sertifikalar, sertifika sahibinin yazılı rızası olması kaydıyla herkesin erişimine açık tutulur.

Sertifika erişim hizmetleri için ücret talep edilmez.

#### **9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri**

TÜRKTRUST tarafından üretilen sertifikalara ait iptal veya durum bilgisi, SİL'ler ve OCSP hizmeti aracılığıyla üçüncü kişilerin erişimine açık tutulur.

Kanun gereği, nitelikli elektronik sertifikaların iptal veya durum bilgisi erişim hizmetleri için ücret talep edilmez.

TÜRKTRUST'ın sunucu sertifikaları ve nesne imzalama sertifikaları için verdiği iptal veya durum bilgisi erişim hizmetleri de ücretsizdir.

#### **9.1.4. Diğer Hizmetlerin Ücretleri**

TÜRKTRUST, kamuya açık olarak yayımladığı Sİ, SUE, sertifika sahibi ve sertifika hizmetleri taahhütnameleri gibi kitapçık ve belgeler için ücret talep etmez.

Bunların dışında kalan ve katma değerli olarak üretilerek müşterilere sunulan diğer ürün ve hizmetler için uygulanacak ücretler, web sitesi ve uygun görülen diğer iletişim kanalları üzerinden müşterilere duyurulur.

#### **9.1.5. Bedel İadesi**

TÜRKTRUST, nitelikli elektronik sertifikalar, sunucu sertifikaları ve nesne imzalama sertifikalarında bedel iadesi yapmaz. Ancak, TÜRKTRUST'tan kaynaklanan nedenlerle, sertifika içeriğinde başvurudan farklı verilerin bulunması durumunda, herhangi bir ücret talep edilmeden yeni bir sertifika verilir.



## **9.2. Finansal Sorumluluk**

TÜRKTRUST, Kanun'dan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla sertifika mali sorumluluk sigortası yaptırmakla yükümlüdür. Sigortaya ilişkin koşullar 26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazetede yayımlanmış olan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" ve ilgili tebliğlerde yer almaktadır.

### **9.2.1. Sigorta Kapsamı**

"Sertifika Mali Sorumluluk Sigortası Yönetmeliği" Madde 6 uyarınca, sertifika mali sorumluluk sigortası, ESHS'nin güvenli ürün ve sistemleri kullanma, hizmeti güvenilir bir biçimde yürütme ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini yerine getirmemesi dolayısıyla zarar görecekt olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

TÜRKTRUST tarafından üretilen nitelikli elektronik sertifikalar sigorta kapsamındadır.

Deneme sertifikaları ile maddi işlem yapılamaz; bu sertifikalara sigorta uygulanmaz.

### **9.2.2. Diğer Varlıklar**

Uygulama dışıdır.

### **9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı**

TÜRKTRUST, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla, nitelikli elektronik sertifikayı elektronik imza sahibine teslim etmeden önce sertifika malî sorumluluk sigortası yaptırmakla yükümlüdür.

## **9.3. İş Bilgisinin Gizliliği**

### **9.3.1. Gizli Bilginin Kapsamı**

TÜRKTRUST'ın elektronik sertifika hizmet sağlayıcılığı işlevleriyle ilgili her türlü ticari gizli bilgi ve belge, TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarının imza oluşturma verileri, kullanılan yazılım ve donanım bilgileri, işlem kayıtları, denetim raporları, tesis içi bölge ve cihazlara ait erişim şifreleri, tesis planı ve iç tasarımı, acil eylem planları, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler, gizli bilgi kapsamına girer.

### **9.3.2. Gizlilik Kapsamı Dışındaki Bilgi**

TÜRKTRUST'ın ticari gizliliği olmayan, Kanun ve uygulamalar gereği kamuya açık olması gereken bilgi ve belgeleri gizlilik kapsamı dışında tutulur. Üretilen sertifikalar, SİL'ler, sertifika hizmetleriyle ilgili müşteri kılavuzları, Sİ kitapçığı, SUE kitapçığı, sertifika sahibi ve sertifika hizmetleri taahhünameleri içeriğindeki bilgiler gizlilik kapsamına girmez.

### **9.3.3. Gizli Bilginin Korunması Sorumluluğu**

TÜRKTRUST çalışanlarının tamamı gizli bilgilerin korunması konusunda sorumluluk sahibidir. Güvenlik politikaları gereği hiçbir gizli bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez. Bilgi güvenliğinin sağlanmasıyla ilgili tüm prosedürler çalışanlar tarafından eksiksiz uygulanır ve bu prosedürlerin uygulanması TÜRKTRUST iç denetimine tabidir.

## **9.4. Kişisel Bilgilerin Gizliliği/Özelliği**

### **9.4.1. Gizlilik Planı**

TÜRKTRUST, verdiği sertifika hizmetleri kapsamında, sertifika başvuru sahiplerine, sertifika sahibi müşterilerine ya da diğer taraflara ait kişisel bilgilerin gizliliğini korur.

**9.4.2. Özel Olarak Değerlendirilecek Bilgi**

TÜRKTRUST tarafından sertifika hizmetlerinin verilmesi sırasında ihtiyaç duyulan ve sertifika başvuru sahiplerinden alınmış olan kimlik doğrulama bilgi ve belgeleri ile TÜRKTRUST tarafından sertifika hizmetlerinin yürütülmesi için kullanılacak olup sertifika içeriğinde yer almayan nüfus bilgileri, iletişim bilgileri gibi müşteri bilgileri, özel bilgi olarak değerlendirilir.

**9.4.3. Özel Sayılmayacak Bilgi**

TÜRKTRUST müşterisi olan sertifika sahiplerine ait sertifikaların içeriğinde yer alan ve sertifikalarla birlikte üçüncü kişilere duyurulan bilgiler, aksi sertifika sahibi tarafından talep edilmedikçe özel bilgi sayılmaz.

**9.4.4. Özel Bilgiyi Koruma Sorumluluğu**

TÜRKTRUST çalışanlarının tamamı başvuru sahiplerine ve müşterilere ait özel bilgilerin korunması konusunda sorumluluk sahibidir. Hiçbir özel bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez.

**9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı**

Uygulama dışıdır.

**9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması**

Yargısal veya idari süreçler gereği ihtiyaç duyulan özel kişisel bilgiler, sadece talep sahibi resmi makama verilir.

**9.4.7. Bilginin Açıklandığı Diğer Durumlar**

Uygulama dışıdır.

**9.5. Fikri Mülkiyet Hakları**

TÜRKTRUST tarafından üretilen tüm sertifikalar, SİL'ler, sertifika hizmetleriyle ilgili müşteri kılavuzları, Sİ ve SUE kitapçıkları, sertifika sahibi ve sertifika hizmetleri taahhütnameleri, sertifika hizmetlerinin yürütülmesiyle ilgili her türlü iç ve dış doküman, veri tabanları, web siteleri ile sertifika hizmetlerine bağlı olarak geliştirilen tüm ürünlerin fikri mülkiyet hakları TÜRKTRUST'a aittir.

Sertifika sahipleri, sertifika içeriğinde yer alan ve kendilerine ait her türlü ayırt edici isim ve markanın mülkiyet haklarına sahiptir.

**9.6. Sorumluluklar****9.6.1. ESHS Sorumlulukları**

TÜRKTRUST'a bağlı sertifika üretim merkezleri, üretilen tüm sertifikaların içeriğinin doğru olduğunu, kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, doğru sertifikanın doğru başvuru sahibi adına üretildiğini ve doğru kişiye teslim edildiğini, yayımlanan sertifika durum bilgilerinin güncelliğini ve doğruluğunu; Sİ ve SUE'de yer alan tüm uygulama gereklilikleri ve yükümlülüklerini yerine getireceğini garanti eder.

TÜRKTRUST'a bağlı sertifika üretim merkezleri, nitelikli elektronik sertifika verebilmek için, Kanun Madde 10 ve Yönetmelik Madde 14'te yer alan ESHS yükümlülüklerini yerine getirir.

**9.6.2. Kayıt Merkezi Sorumlulukları**

TÜRKTRUST'a bağlı kayıt merkezleri, kendilerine başvuran kişilerin kimlik doğrulama adımlarının doğru ve güvenilir biçimde yürütüldüğünü, kayıtların doğru biçimde tutulduğunu, ESHS merkezine gönderilen sertifika üretim, yenileme ve iptal taleplerinin doğru ve eksiksiz olduğunu garanti eder.

**9.6.3. Sertifika Sahibi Sorumlulukları**

Sertifika sahipleri, sertifika başvurusu ile yenileme ve iptal talepleri sırasında TÜRKTRUST'a güncel ve doğru bilgi ve belgeler sunmayı, sertifikalarını Sİ ve SUE kitapçıklarında yer alan koşullar uyarınca kullanmayı, sertifika sahibi sözleşmesinde yer alan tüm yükümlülüklerini yerine getireceğini garanti eder.

Nitelikli elektronik sertifika sahipleri, sertifika sahibi sözleşmesiyle birlikte Yönetmelik Madde 15'te yer alan yükümlülükleri de yerine getirmek zorundadır.

**9.6.4. Üçüncü Kişilerin Sorumlulukları**

Sertifika sahipleri ile üçüncü kişiler, TÜRKTRUST nitelikli elektronik sertifikalarına dayanarak oluşturulmuş elektronik imzaların geçerliliğini doğrulamaktan kendileri sorumludur.

**9.6.5. Diğer Tarafların Sorumlulukları**

TÜRKTRUST'ın sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer taraflar, verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini ve TÜRKTRUST iş süreçleri ve müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti eder. TÜRKTRUST ile hizmet aldığı kuruluşlar arasında bu garantilerin açıkça belirtildiği hizmet sözleşmeleri imzalanır.

**9.7. Sorumlulukların Geçersiz Olduğu Durumlar**

Uygulama dışıdır.

**9.8. Sorumluluk Sınırları**

TÜRKTRUST tarafından verilen sertifikalar, parasal işlemlerde maddi işlem sınırları dahilinde sigortalıdır. Sertifikalar ve bu sertifikaların kullanımıyla ilgili sorumluluk sınırları, sertifika sahibi taahhütnamesinde açıkça belirtilmiştir.

**9.9. Tazminatlar**

TÜRKTRUST, bu Sİ ve SUE'de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getiremez ve bu durumdan üçüncü kişiler zarar görürse, ilgili zarar TÜRKTRUST tarafından tazmin edilir.

Nitelikli elektronik sertifika hizmetleri uyarınca, Kanun Madde 13 gereği, TÜRKTRUST Kanun ve Yönetmelik hükümlerinin ihlali suretiyle üçüncü kişilere vereceği zararları tazminle yükümlüdür. Bu durumlarda TÜRKTRUST kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Sertifika sahipleri, sertifika sahibi taahhütnamesi hükümleri gereği yükümlülüklerini yerine getirmez ve bu durumdan TÜRKTRUST ve/veya üçüncü kişiler zarar görürse, ilgili zararın sertifika sahibi tarafından tazmin edilmesi gerekir.

**9.10. Sİ Kitapçığının Geçerliliği****9.10.1. Sİ Kitapçığının Geçerlilik Dönemi**

Sİ kitapçığının bu sürümü, yeni bir sürüm çıkarılana kadar geçerlidir.

**9.10.2. Sİ Kitapçığının Geçerliliğinin Sona Ermesi**

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, Sİ kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, kitapçık kısmen ya da tamamen geçersiz duruma düşebilir. Bu durumda, ilgili değişikliklerin yansıtıldığı yeni bir Sİ kitapçığı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

**9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi**

Mevcut Sİ sürümünün geçerliliğinin sona ermesi durumunda, TÜRKTRUST faaliyetlerinin ve sertifika hizmetlerinin kesintiye uğramaması için gerekli önlemler alınır. Yeni Sİ sürümü, eski Sİ sürümünün geçerliliği sona ermeden hazırlanır ve değişim hizmet kesintisi olmadan gerçekleştirilir.

Değişiklikler gereği TÜRKTRUST tarafından üretilen sertifikalarda herhangi bir değişiklik yapılması gerekirse, sertifika sahipleriyle ve üçüncü kişilerle bu durum paylaşılır ve gerekli işlemler hızlıca tamamlanır. Yeni sürüm gereği değişen uygulamalar TÜRKTRUST tarafından hemen devreye alınır.

**9.11. Tarafalara Özel Duyurular ve İletişim**

TÜRKTRUST tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için e-posta kullanılır. Gerekli görülen durumlarda ise yazı ile duyurular gönderilebilir.

TÜRKTRUST'ın üçüncü kişilere yapacağı duyurular web üzerinden ya da basın yayın organları aracılığıyla yayımlanır.

**9.12. Değişiklikler**

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, Sİ kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir Sİ kitapçığı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

Sİ kitapçığında, önceden üretilmiş olan sertifikaların kullanımını ve kabul edilirliliğini etkilemeyecek olan küçük değişiklikler olabileceği gibi, sertifika kullanımına doğrudan etki edebilecek önemli değişiklikler de olabilir. Her iki durumda TÜRKTRUST uygulamaları farklı olacaktır.

**9.12.1. Değişiklik Prosedürü**

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, Sİ kitapçığının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir Sİ kitapçığı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

Sİ'de oluşan değişiklikler, SUE'deki ilgili uygulamalara da yansıtılır. Dolayısıyla yeni bir Sİ sürümü, yeni bir SUE sürümünü de gerektirir. TÜRKTRUST tarafından üretilen yeni sertifikaların "sertifika ilkeleri" uzantısında URL olarak verilen SUE kitapçığına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği SUE kitapçığı yeni sürümdür.

Küçük değişiklikler olması durumunda, önceden verilmiş olan sertifikalar da yeni Sİ ve SUE'ye uygun olarak kullanılmaya devam eder. Ancak önemli değişiklikler nedeniyle yeni bir Sİ sürümü çıkarılmışsa, önceden üretilmiş sertifikaların, değişiklik yapılan sertifika ilkelerine bağlı olanları, yeni Sİ'ye uyumlu olarak kullanılamayabilir.

### **9.12.2. Duyuru Mekanizması ve Süresi**

TÜRKTRUST faaliyetleri ve sertifika hizmetlerindeki uygulama değişiklikleri ile mevcut Sİ ve SUE kitapçıklarında değişiklik oluşması durumunda, çıkarılan güncel Sİ ve SUE sürümleri hakkında sertifika sahipleri ile üçüncü kişiler ivedilikle bilgilendirilir.

Özellikle önemli değişikliklerde, sertifikanın kullanılabilirliği ve kabul edilirliliği bazı uygulamalarda etkilenebileceğinden, TÜRKTRUST sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır. Değişiklik TÜRKTRUST web sitesinde yayımlanır, sertifika sahiplerine iletişim bilgileri aracılığıyla doğrudan ulaşılır, gerektiğinde basın ve yayın organları aracılığıyla tüm üçüncü kişilerin durumdan haberdar olması sağlanır.

Küçük değişikliklerde ise web sitesi aracılığıyla durum ilan edilir ve sertifika sahipleri e-posta ile bilgilendirilir.

Yeni Sİ ve SUE sürümleri, eski sürümlerle birlikte TÜRKTRUST bilgi deposunda, ayrıntılı sürüm bilgisi içerecek şekilde yayımlanır ve ilgili tarafların erişimine açık tutulur.

### **9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar**

Sertifika kullanımını ve kabul edilirliliğini doğrudan etkileyebilecek olan, kullanılan kimlik doğrulama adımlarını önemli ölçüde etkileyen veya sertifika hizmetlerinde sertifikanın güvenlik düzeyine etki edebilecek biçimde gerçekleşen önemli değişiklikler, Sİ kitapçığında tanımlanan ilgili sertifika ilkelerinin nesne tanımlayıcı numaralarının da değişmesini gerektirebilir. Bu durumda, yeni üretilen sertifikalarda, uygulanacak olan yeni sertifika ilkelerinin nesne tanımlayıcı numaraları yer alır.

### **9.13. Anlaşmazlıkların Çözümü**

TÜRKTRUST, sertifika sahipleri ve üçüncü kişiler arasında çıkabilecek anlaşmazlıklarda öncelikle, Sİ ve SUE kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler, taahhütnameler ve sözleşmeler uyarınca sorunun çözülmesine çalışılır.

Nitelikli elektronik sertifikalarla ilgili işlemler TÜRKTRUST tarafından Kanun ve Yönetmelikler ile bunlara bağlı Tebliğler uyarınca yürütülür.

Taraflar arasındaki anlaşmazlıklar sulhen çözüme kavuşmadığı takdirde, anlaşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

### **9.14. Yasal Düzenleme**

Türkiye’de, elle atılan imza ile aynı hukuki sonucu doğuran güvenli elektronik imzanın kullanımı, 5070 sayılı “Elektronik İmza Kanunu” ve Telekomünikasyon Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca düzenlenir. Kurum ESHS’lerin Kanun uyarınca işleyişinin düzenlenmesi ve denetlenmesinden sorumludur.

### **9.15. İlgili Yasalara Uygunluk**

TÜRKTRUST, nitelikli elektronik sertifika hizmetlerini 5070 sayılı “Elektronik İmza Kanunu” ve Telekomünikasyon Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca yürütür.

### **9.16. Çeşitli Hükümler**

#### **9.16.1. Bütün Anlaşma**

Uygulama dışıdır.

**9.16.2. Görevlendirme**

Uygulama dışıdır.

**9.16.3. Kitapçık Kısımlarının Ayrılabilirliği**

Sİ ve SUE kitapçıklarının diğer bölümlerinin geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybettiğinde, TÜRKTRUST tarafından ilgili değişikliklerin yansıtıldığı yeni sürümler çıkarılana kadar, kitapçığın etkilenmemiş diğer bölümleri geçerliliğini korur ve uygulanır.

**9.16.4. Yasal Haklardan Vazgeçme**

Uygulama dışıdır.

**9.16.5. Mücbir Sebepler**

TÜRKTRUST'ın elektronik sertifika hizmet sağlayıcılığıyla ilgili faaliyetlerini yerine getirmesini engelleyecek ve normal koşullar altında kontrol edilebilir olmayan durumlar mücbir sebep olarak adlandırılır. Bu durumlar devam ettiği sürece, TÜRKTRUST faaliyetleri aksaklığa veya kesintiye uğrayabilir. Doğal afetler, savaşlar, terör, telekomünikasyon, İnternet ve benzeri diğer altyapılarda oluşabilecek aksaklıklar mücbir sebep kabul edilir.

**9.17. Diğer Hükümler**

Uygulama dışıdır.