SERTİFİKA İLKELERİ (Sİ)

SÜRÜM : 07

TARİH : 15.07.2013

1. GİRİŞ 10
1.1. Genel Bakış 10
1.2. Kitapçık Adı ve Tanımlama 11
1.3. Taraflar 11
1.3.1. Sertifika Üretim Merkezleri 11
1.3.2. Sertifika Kayıt Merkezleri 11
1.3.3. Sertifika Sahipleri 12
1.3.4. Üçüncü Kişiler 12
1.3.5. Diğer Katılımcılar 12
1.4. Sertifika Kullanımı 12
1.4.1. Geçerli Sertifika Kullanım Şekilleri 12
1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri 13
1.5. Sertifika İlkeleri Yönetimi 13
1.5.1. Sİ Dokümanından Sorumlu Organizasyon 13
1.5.2. İletişim Noktası 13
1.5.3. Sİ'nin İlkelere Uygunluğunu Belirleyen Yetkili 13
1.5.4. Sİ Onaylama Prosedürleri 13
1.6. Kısaltmalar ve Tanımlar 13
1.6.1. Kısaltmalar 13
1.6.2. Tanımlar 14
2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI 19
2.1. Bilgi Deposu 19
2.2. Sertifika Bilgilerinin Yayımlanması 19
2.3. Yayımın Zamanı veya Sıklığı 19
2.4. Bilgi Deposuna Erişim Kontrolleri 19
3. KİMLİĞİN DOĞRULANMASI 20
3.1. İsimlendirme 20
3.1.1. İsim Tipleri 20
3.1.2. İsimlerin Anlamlı Olması Gerekliliği 20
3.1.3. Sertifika Sahiplerinin Anonimliği ve Takma Ad Kullanılabilirliği 20
3.1.4. İsim Biçimlerinin Değerlendirilmesi 20
3.1.5. İsimlerin Benzersizliği 20
3.1.5.1. NES 20
3.1.5.2. SSL ve EV SSL (Türkiye'de yerleşik ticari kişiler) 20
3.1.5.3. SSL ve EV SSL (Türkiye'de yerleşik olmayan ticari kişiler) 20
3.1.5.4. NİMS 20
3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü 20

3.2. İlk Kimlik Doğrulama 21
3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi 21
3.2.2. Tüzel Kişiliğin Doğrulanması 21
3.2.2.1. NES, SSL ve NİMS 21
3.2.2.2. EV SSL 21
3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması 21
3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler 22
3.2.5. Yetkinin Doğrulanması 22
3.2.6. Karşılıklı Çalışma Kriterleri 22

3.3. Anahtar Yenileme Taleplerinin Doğrulanması 22
3.3.1. Rutin Anahtar Yenileme için Kimlik Doğrulama 22
3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama 23

3.4. İptal Talebi için Kimlik Doğrulama 23

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ 24

4.1. Sertifika Başvurusu 24
4.1.1. Kimler Sertifika Başvurusunda Bulunabilir? 24
4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar 24

4.2. Sertifika Başvurusunun İşlenmesi 25
4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi 25
4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi 25
4.2.3. Sertifika Başvurularının İşlenme Süresi 25

4.3. Sertifika Üretimi 25
4.3.1. Sertifika Üretimi Sırasındaki ESHS Faaliyetleri 25
4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi 25

4.4. Sertifikanın Kabulü 26
4.4.1. Kabulün Şekli 26
4.4.2. ESHS Tarafından Sertifikanın Yayımlanması 26
4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi 26

4.5. Anahtar Çifti ve Sertifika Kullanımı 26
4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı 26
4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı 26

4.6. Sertifika Yenileme 27
4.6.1. Sertifika Yenilemeyi Gerektiren Durumlar 27
4.6.2. Yenileme Talebinde Bulunabilecek Kişiler 27
4.6.3. Sertifika Yenileme Talebinin İşlenmesi 27
4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması 28
4.6.5. Yenilenen Sertifikanın Kabulü 28
4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması 28
4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi 28

4.7. Anahtar Yenileme 28
4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar 28
4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler 28
4.7.3. Anahtar Yenileme Talebinin İşlenmesi 28

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması 28
4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü 28
4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması 28
4.7.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi 28

4.8. Sertifika Değişikliği 29
4.8.1. Sertifika Değişikliğini Gerektiren Durumlar 29
4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler 29
4.8.3. Sertifika Değişiklik Talebinin İşlenmesi 29
4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması 29
4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli 29
4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması 29
4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi 29

4.9. Sertifika İptali ve Askıya Alma 29
4.9.1. Sertifika İptalini Gerektiren Durumlar 29
4.9.1.1. Son Kullanıcı Sertifikaları 29
4.9.1.2. TÜRKTRUST Alt Kök Sertifikaları 30
4.9.1.3. Alt ESHS Sertifikaları 31
4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler 31
4.9.3. Sertifika İptal Talebi Prosedürleri 32
4.9.4. Sertifika İptal Talebi Gecikme Periyodu 32
4.9.5. TÜRKTRUST'ın Sertifika İptal Talebini İşleme Süresi 33
4.9.6. Üçüncü Kişilerin İptal Kontrol Gerekliliği 33
4.9.7. Sertifika İptal Listesi (SİL) Yayımlama Sıklığı 33
4.9.8. SİL'lerin En Geç Yayımlanma Zamanı 33
4.9.9. Çevrim İçi Sertifika İptal/Durum Kontrol İmkânı (OCSP) 33
4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri 33
4.9.11. Diğer İptal Durumu Yayımlama Çeşitlerinin Varlığı 33
4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler 33
4.9.13. Sertifika Askıya Alma Gerektiren Durumlar 34
4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler 34
4.9.15. Sertifika Askıya Alma Talebi Prosedürü 34
4.9.16. Sertifikanın Askıda Kalma Süresinin Sınırları 34

4.10. Sertifika Durum Servisleri 35
4.10.1. İşlevsel Özellikler 35
4.10.2. Hizmetin Sürekliliği 35
4.10.3. İsteğe Bağlı Özellikler 35

4.11. Sertifika Sahipliğinin Sona Ermesi 35

4.12. İmza Oluşturma Verisi Saklama ve Yeniden Oluşturma 35
4.12.1. Anahtar Saklama ve Yeniden Oluşturma İlke ve Esasları 35
4.12.2. Oturum Anahtarı Zarflama ve Yeniden Oluşturma İlke ve Esasları 35

5. TESİS, YÖNETİM VE İŞLETMEYLE İLGİLİ KONTROLLER 36

5.1. Fiziksel Kontroller 36
5.1.1. Tesis Yeri ve İnşaatı 36
5.1.2. Fiziksel Erişim 36
5.1.3. Güç Kaynakları ve Havalandırma 36
5.1.4. Su Baskınları 36
5.1.5. Yangın Önleme ve Yangından Korunma 36

5.1.6. Saklama Ortamları 36
5.1.7. Atıkların Atılması 36
5.1.8. Tesis Dışı Yedekleme 36

5.2. Prosedürel Kontroller 37
5.2.1. Güvenilir Roller 37
5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı 37
5.2.3. Her Görev için Kimlik Doğrulama 37
5.2.4. Görevlerin Ayrılmasını Gerektiren Roller 37

5.3. Personel Kontrolleri 37
5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri 37
5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri 38
5.3.3. Eğitim Gereklilikleri 38
5.3.4. Tekrar Eğitimi Sıklığı ve Gereklilikleri 38
5.3.5. İş Rotasyonu Sıklığı ve Sırası 38
5.3.6. Yetkisiz İşlemler için Yaptırımlar 38
5.3.7. Bağımsız Alt Yüklenici Gereklilikleri 38
5.3.8. Personele Sağlanan Dokümantasyon 38

5.4. Denetim Kayıtları Alma Prosedürleri 38
5.4.1. Kaydedilen Olay Tipleri 38
5.4.2. Kayıtları İşleme Sıklığı 39
5.4.3. Denetim Kayıtlarının Saklanma Süresi 39
5.4.4. Denetim Kayıtlarının Korunması 39
5.4.5. Denetim Kayıtlarının Yedeklenme Prosedürleri 39
5.4.6. Denetim Bilgisi Toplama Sistemi (İç ve Dış) 39
5.4.7. Olayı Yaratan Kişiyi Bilgilendirme 39
5.4.8. Zarar Görebilirlik Değerlendirmesi 39

5.5. Kayıtların Arşivlenmesi 39
5.5.1. Arşivlenen Kayıt Tipleri 39
5.5.2. Arşivlerin Saklanma Süresi 40
5.5.3. Arşivlerin Korunması 40
5.5.4. Arşivlerin Yedeklenme Prosedürleri 40
5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri 40
5.5.6. Arşiv Toplama Sistemi 40
5.5.7. Arşiv Bilgisinin Edinilmesi ve Doğrulanması Prosedürleri 40

5.6. Anahtar Değişimi 40

5.7. Güvenliğin Yitirilmesi ve Felaket Kurtarma 40
5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar 40
5.7.2. Bilgisayar Kaynakları, Yazılım ve/veya Verilerin Bozulmuş Olması 40
5.7.3. İmza Oluşturma Verilerinin Güvenliğinin Yitirilmesi 40
5.7.4. İş Sürekliliği Yetenekleri ve Felaket Kurtarma 41

5.8. TÜRKTRUST'ın Faaliyetinin Son Bulması 41

6. TEKNİK GÜVENLİK KONTROLLERİ 42

6.1. Anahtar Çifti Üretimi ve Kurulumu 42
6.1.1. Anahtar Çifti Üretimi 42
6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması 42

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması 43
6.1.4. TÜRKTRUST İmza Doğrulama Verilerinin Üçüncü Kişilere Ulaştırılması 43
6.1.5. Anahtar Uzunlukları 43
6.1.6. Anahtar Üretimi ve Kalite Kontrolü 43
6.1.7. Anahtar Kullanım Amaçları 44

6.2. İmza Oluşturma Verisinin Korunması ve Kriptografik Modül Mühendislik Kontrolleri 44
6.2.1. Kriptografik Modül Standartları ve Kontroller 44
6.2.2. İmza Oluşturma Verisinin Çok Kullanıcılı Kontrolü 44
6.2.3. İmza Oluşturma Verisinin Saklanması 45
6.2.4. İmza Oluşturma Verisinin Yedeklenmesi 45
6.2.5. İmza Oluşturma Verisinin Arşivlenmesi 45
6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi 45
6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması 45
6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi 45
6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi 46
6.2.10. Gizli Anahtarı Yok Etme Metodu 46
6.2.11. Kriptografik Modül Değerlendirmesi 46

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular 46
6.3.1. İmza Doğrulama Verilerinin Arşivlenmesi 46
6.3.2. Sertifikanın İşlevsel Süreleri ve Anahtar Çifti Kullanım Süreleri 46

6.4. Erişim Şifreleri 47
6.4.1. Erişim Şifrelerinin Oluşturulması ve Kurulumu 47
6.4.2. Erişim Şifrelerinin Korunması 47
6.4.3. Erişim Şifreleriyle İlgili Diğer Konular 47

6.5. Bilgisayar Güvenlik Kontrolleri 48
6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri 48
6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi 48

6.6. Yaşam Döngüsü Teknik Kontrolleri 48
6.6.1. Sistem Geliştirme Kontrolleri 48
6.6.2. Güvenlik Yönetimi Kontrolleri 49
6.6.3. Yaşam Döngüsü Güvenlik Kontrolleri 49

6.7. Ağ Güvenlik Kontrolleri 49

6.8. Zaman Damgası 49

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (SİL) VE OCSP PROFİLLERİ 50

7.1. Sertifika Profili 50
7.1.1. Sürüm Numaraları 50
7.1.2. Sertifika Uzantıları 50
7.1.3. Algoritma Nesne Tanımlayıcıları 50
7.1.4. İsim Biçimleri 51
7.1.5. İsim Kısıtları 51
7.1.6. Sertifika İlkeleri Nesne Tanımlayıcısı 51
7.1.7. İlke Kısıtları Uzantısının Kullanımı 51
7.1.8. İlke Niteleyicilerinin Yazımı 51

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği 51

7.2. SİL Profili 51
7.2.1. Sürüm Numarası 51
7.2.2. SİL ve SİL Giriş Uzantıları 52

7.3. OCSP Profili 52
7.3.1. Sürüm Numarası 52
7.3.2. OCSP Uzantıları 52

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER 53

8.1. Denetim Sıklığı ve Durumları 53

8.2. Denetçinin Kimliği ve Özellikleri 53

8.3. Denetçinin ESHS'yle İlişkisi 54

8.4. Denetimde Kapsanan Başlıklar 54

8.5. Eksiklik Durumunda Yapılacaklar 54

8.6. Sonuçların Bildirilmesi 54

9. DİĞER İŞ KONULARI VE YASAL KONULAR 56

9.1. Ücretler 56
9.1.1. Sertifika Üretim ve Yenileme Ücretleri 56
9.1.2. Sertifika Erişim Ücretleri 56
9.1.3. İptal veya Durum Bilgisi Erişim Ücretleri 56
9.1.4. Diğer Hizmetlerin Ücretleri 56
9.1.5. Bedel İadesi 56

9.2. Finansal Sorumluluk 57
9.2.1. Sigorta Kapsamı 57
9.2.2. Diğer Varlıklar 57
9.2.3. Son Kullanıcılar için Sigorta veya Garanti Kapsamı 57

9.3. İş Bilgisinin Gizliliği 57
9.3.1. Gizli Bilginin Kapsamı 57
9.3.2. Gizlilik Kapsamı Dışındaki Bilgi 57
9.3.3. Gizli Bilginin Korunması Sorumluluğu 58

9.4. Kişisel Bilgilerin Gizliliği/Özelliği 58
9.4.1. Gizlilik Planı 58
9.4.2. Özel Olarak Değerlendirilecek Bilgi 58
9.4.3. Özel Sayılmayacak Bilgi 58
9.4.4. Özel Bilgiyi Koruma Sorumluluğu 58
9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı 58
9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması 58
9.4.7. Bilginin Açıklandığı Diğer Durumlar 58

9.5. Fikri Mülkiyet Hakları 58

9.6. Sorumluluklar 59
9.6.1. ESHS Beyan ve Garantileri 59
9.6.2. Kayıt Merkezi Sorumlulukları 60
9.6.3. Sertifika Sahibi Sorumlulukları 60
9.6.4. Üçüncü Kişilerin Sorumlulukları 60
9.6.5. Diğer Katılımcıların Sorumlulukları 60

9.7. Sorumlulukların Geçersiz Olduğu Durumlar 60

9.8. Sorumluluk Sınırları 60

9.9. Tazminatlar 61

9.10. Sİ dokümanının Geçerliliği 61
9.10.1. Sİ dokümanının Geçerlilik Dönemi 61
9.10.2. Sİ dokümanının Geçerliliğinin Sona Ermesi 61
9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi 61

9.11. Taraflara Özel Duyurular ve İletişim 61

9.12. Değişiklikler 62
9.12.1. Değişiklik Prosedürü 62
9.12.2. Duyuru Mekanizması ve Süresi 62
9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar 62

9.13. Anlaşmazlıkların Çözümü 63

9.14. Yasal Düzenleme 63

9.15. İlgili Yasalara Uygunluk 63

9.16. Çeşitli Hükümler 63
9.16.1. Bütün Anlaşma 63
9.16.2. Görevlendirme 63
9.16.3. Kitapçık Kısımlarının Ayrılabilirliği 63
9.16.4. Yasal Haklardan Vazgeçme 63
9.16.5. Mücbir Sebepler 63

9.17. Diğer Hükümler 63

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 Bilgi Teknolojileri ve İletişim 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 uyması gereken ilke ve kuralları belirlemek amacıyla, Bilgi Teknolojileri ve İletişim Kurumu'nun kanun kapsamında yayımlamış olduğu "Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ"in 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.

SSL (Secure Socket Layer) Sertifikası ve EV (Extended Validation) SSL Sertifikası hizmetleri için TÜRKTRUST, "ETSI TS 102 042 Electronic Signatures Infrastructure (ESI); Policy Requirements for Certification Authorities Issuing Public Key Certificates" standardının güncel sürümüne uyar. TÜRKTRUST ayrıca, SSL ve EV SSL sertifikaları için, ETSI TS 102 042 standardında referans verilen ve http://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates" dokümanına uyum sağlar. Daha ileri düzeyde doğrulama gereklilikleri olan EV SSL sertifikaları içinse, TÜRKTRUST yine ETSI TS 102 042 standardında referans verilen ve http://www.cabforum.org adresinde yayımlanan "CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates" dokümanının güncel sürümüne uyar. Sertifika Uygulama Esasları (SUE) kitapçığı ile bu dokümanlar arasında herhangi bir uyuşmazlık olması durumunda ilgili dokümanlardaki gereklilikler geçerli olacaktır. İlgili dokümanlara uyum, ETSI TS 102 042 standardında yer alan "Publicly-Trusted Certificate Policy - Baseline Requirements – BR Gerekliliklerini Kapsayan Kamuoyunca Güvenilen Sertifika İlkesi"ni ve "Extended Validation Certificate Policy – Genişletilmiş Doğrulamalı Sertifika İlkesi"ni (PTC-BR ve EVCP) kapsamaktadır.

Sİ dokümanı, 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 dokümanı, TÜRKTRUST'ın verdiği tüm elektronik sertifika hizmetlerini kapsar. Sİ'de yer alan ilke ve kurallar, TÜRKTRUST'ın tüm müşteri hizmetleri birimlerini, kayıt merkezlerini ve sertifika üretim merkezi birimlerini kapsar.

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

Sertifika İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE) kitapçıkları mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısında değerlendirilir. Bu değerlendirmeler sonucunda ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçıklar güncellenir.

1.2. Kitapçık Adı ve Tanımlama

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

TÜRKTRUST, bu Sİ dokümanını 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 NES 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. Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar da aynı ilkelere bağlıdır.
- TÜRKTRUST SSL Sertifikası İlkeleri (2.16.792.3.0.3.1.1.2): Sunuculara yönelik SSL sertifikalarını kapsar. SSL Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.
- TÜRKTRUST NİMS İlkeleri (2.16.792.3.0.3.1.1.4): Nesne imzalama işlemlerine yönelik sertifikaları kapsar. NİMS Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Normalized Certificate Policy – Standartlaştırılmış Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.
- TÜRKTRUST EV SSL Sertifikası İlkeleri (2.16.792.3.0.3.1.1.5): Sunuculara yönelik EV SSL sertifikalarını kapsar. EV SSL Sertifikaları, ETSI TS 102 042 standardında tanımlanan "Extended Validity Certificate Policy – Genişletilmiş Onay Sertifika İlkeleri" uyarınca üretilir ve idame ettirilir.

Sİ dokümanı "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.

TÜRKTRUST ile Türkiye Barolar Birliği (TBB) arasında yapılan anlaşma gereği TBB, avukatlardan veya Türk Yargısında görev yapan hakim, savcı ve benzeri her türlü görevliden oluşan kapalı bir kullanıcı kitlesine yönelik olarak, TÜRKTRUST Sİ ve SUE dokümanları uyarınca ve hizmet sözleşmesi çerçevesinde, TÜRKTRUST kök sertifikasına bağlı TBB NES alt kökü aracılığıyla, NES üretim ve dağıtım faaliyetleri yürütmektedir.

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, kimlik veya unvanları doğrulanan ve buna bağlı olarak adlarına sertifika üretilen kişilerdir.

Kimlik veya unvan doğrulaması, başvuru yapılan sertifika türüne bağlı olarak ilgili mevzuat ve standartlara göre yapılır. Sertifika sahibinin sorumluluğu ve sertifika kullanımından doğan sonuçlar, ilgili mevzuatla ve sertifika sahibi taahhütnamesi veya sözleşmesiyle belirlenir.

1.3.4. Üçüncü Kişiler

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

TÜRKTRUST tarafından verilmiş sertifikaların kullanımına bağlı üçüncü kişilere karşı TÜRKTRUST'ın sorumluluğunun sınırları işbu kitapçıkta belirtilmiştir.

1.3.5. Diğer Katılımcılar

TÜRKTRUST sertifika hizmetleri kapsamında sertifika üretimi, bilgi deposu yayımlama ve benzeri sertifika hizmetlerinin tümü TÜRKTRUST tarafından verilir.

TÜRKTRUST, sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcıların verecekleri hizmeti güvenilir ve doğru biçimde vereceklerini iş süreçleri ve müşterilerle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti etmelerini sağlamak amacıyla sözleşmeler imzalar.

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 NES, ilgili mevzuat uyarınca 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 veya resmi belgeleri imzalamak, e-posta mesaj metinlerini imzalamak, web üzerindeki işlem talimatlarını imzalamak, kimlik tanımlama ve doğrulama gerektiren ağ ortamlarında kimliği ispat etmek geçerli sertifika kullanım şekilleridir.

SSL ve EV SSL sertifikaları, sertifika sahipleri tarafından sadece sertifikada yer alan sunucu için ve SSL işleminde kullanılır.

NİMS, sertifikada yer alan kişi tarafından veya onun uhdesinde geliştirilen yazılım kodu için kullanılır.

1.4.2. Yasaklanmış Sertifika Kullanım Şekilleri

TÜRKTRUST NES, mevzuatta belirlenen şartlar dışında kullanılamaz.

Diğer TÜRKTRUST sertifikalarının, sertifika sahiplerinin uhdesi dışında kullanılması yasaktır. Sertifikalar, işbu Sİ ve SUE dokümanında belirtilen amaçlar ve sınırlar dışında kullanılamaz.

1.5. Sertifika İlkeleri Yönetimi

TÜRKTRUST, sertifika ilkelerini oluşturan otorite olarak, işbu Sİ dokümanının yönetimi ve kayıt altına alınmasından sorumludur.

1.5.1. Sİ Dokümanından Sorumlu Organizasyon

İşbu Sİ dokümanının 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 696.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
Web : http://www.turktrust.com.tr

1.5.3. Sİ'nin İlkelere Uygunluğunu Belirleyen Yetkili

TÜRKTRUST Sİ dokümanının uygunluğu ve uygulanabilirliği TÜRKTRUST üst yönetimi tarafından belirlenir.

1.5.4. Sİ Onaylama Prosedürleri

Sİ dokümanı TÜRKTRUST Yönetim Kurulu tarafından onaylanır. Gerekli onayı alan Sİ, ESHS faaliyetlerine ilişkin ilke ve kuralları düzenlemek için kullanılır.

TÜRKTRUST EV SSL sertifikaları için, CA/Browser Forum tarafından yayımlanan ve http://www.cabforum.org web sitesinde ilan edilen "Guidelines for the Issuance and Management of Extended Validation Certificates" rehber dokümanının güncel sürümüne uyar. Bu rehber doküman ve işbu Sİ veya SUE dokümanı arasında bir tutarsızlık olması durumunda belirtilen rehber doküman esas alınır.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

BR : CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – CA/Browser Forum Temel Gereklilikler dokümanı

CSR : Certificate Signing Request –Sertifika İmzalama Talebi

DN : Distinguished Name – Ayırt Edici İsim

DNS : Domain Name System – Alan Adı Sistemi

ESHS : Elektronik Sertifika Hizmet Sağlayıcısı

ETSI : European Telecommunication Standards Institute – Avrupa Telekomünikasyon Standartları Enstitüsü

EV : Extended Validation – Genişletilmiş Onay

FKM : Felaket Kurtarma Merkezi

IETF : Internet Engineering Task Force – İnternet Mühendisliği Görev Grubu

NES : Nitelikli Elektronik Sertifika

NİMS : Nesne İmzalama Sertifikası

OID : Object Identifier – Nesne Tanımlayıcı Numarası

OCSP : On-line Certificate Status Protokol – Çevrim İçi Sertifika Durum Protokolü

PKI : Public Key Infrastructure – Açık Anahtarlı Altyapı

PTC-BR: Publicly-Trusted Certificate - Baseline Requirements – BR gerekliliklerini kapsayan ve kamuoyunca güvenilen sertifikalar

RFC : IETF tarafından yayımlanan, kılavuz niteliğinde yorum talebi dokümanları

SAN : Subject Alternative Name – Özne Alternatif Adı

Sİ : Sertifika İlkeleri

SİL : Sertifika İptal Listesi

SSL : Secure Sockets Layer

SUE : Sertifika Uygulama Esasları

TCKN : T.C. Kimlik Numarası

TSE : Türk Standartları Enstitüsü

1.6.2. Tanımlar

Açık Anahtar: Bir çift anahtarlı şifreleme algoritmasında diğer kişilerin de bilgisine açık olan kriptografik anahtar; Kanun'da imza doğrulama verisi olarak isimlendirilmiştir.

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.

Aktivasyon: İmza oluşturma verisi erişim şifresinin, kullanıcıya şifre zarfıyla gönderilmesi yerine, kendisi tarafından belirlenmesine imkân sağlayan güvenli yöntem. Buna göre kullanıcı, TÜRKTRUST tarafından sağlanan yazılımı kullanır. Akıllı kartı bilgisayara takılıyken, bu yazılım içinden "aktivasyon kodu" talebinde bulunur ve "aktivasyon kodu" başvurusu sırasında verdiği cep telefonuna gönderilir. Kullanıcı, aynı yazılımı ve "aktivasyon kodunu" kullanarak imza oluşturma verisi erişim şifresini belirler.

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.

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

Ayırt Edici İsim Alanı (Distinguished Name [DN] Field): Ayırt edici isim alanı, sertifika sahibinin veya sertifikayı veren kuruluşun kimlik bilgilerini içeren bilgi alanıdır. Bu alan içinde CN, O, OU, T, L, C ve SERIALNUMBER gibi farklı alt alanlar sertifika tipine göre uygun içerikle yer alabilir.

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 ve standartlara uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin tespit edilmesi ve ilgili mevzuatta veya standartlarda 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: Açık anahtarlı alt yapıda, açık anahtar ile anahtar sahibinin kimliğini, elektronik sertifika hizmet sağlayıcısının gizli anahtarını kullanarak birbirine bağladığı elektronik kayıttır. Metin içinde "elektronik" sözcüğü yer almaksızın da "sertifika" aynı anlamda kullanılmıştır.

Elektronik Sertifika Hizmet Sağlayıcısı: Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Metin içinde, "elektronik" sözcüğü yer almaksızın da "sertifika hizmet sağlayıcısı" aynı anlamda kullanılmıştır.

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

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

EV SSL Sertifikası: ETSI TS 102 042 standardında tanımlanan "Extended Validity Certificate Policy – Genişletilmiş Onay Sertifika İlkeleri" uyarınca üretilen ve idame edilen SSL sertifikasıdır.

Gizli Anahtar: PKI yapısında, bir çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin bilgisinde olan kriptografik anahtar; Kanun'da imza oluşturma verisi olarak isimlendirilmiştir.

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. maddesinde sayılan niteliklere sahip imza doğrulama aracıdır.

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

Hat Kullanıcısı: Mobil iletişim cihazı hat sahibi tarafından kullanılıyorsa hat sahibinin kendisidir; mobil iletişim cihazı hat sahibinin bilgisi ve onayı ile başka bir kişi tarafından kullanılıyorsa, mobil imza hizmetini de kapsayan mobil operatör hizmetlerinin kullanıcısı olan kişidir.

Hat Sahibi: Mobil operatörün kurmuş olduğu GSM sisteminde verilen hizmetlerden yararlanmak üzere, kendi isteğiyle ve abonelik sözleşmesinde belirtilen hükümler çerçevesinde mobil operatör şebekesine kaydını yaptırmak için bizzat veya vekili ya da yetkilisi aracılığıyla başvurarak abonelik sözleşmesini imzalayan ve hükümlerine uymayı taahhüt eden gerçek veya tüzel kişidir.

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.

İmzalı Sertifika Talebi (CSR): Talep sahibi tarafından üretilen ve sahip olduğu gizli anahtarla imzaladığı sertifika talebidir. Genellikle PKCS#10 formatında üretilir.

İnceleme: Kuruma yapılan bildirimin gerekli şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalardır.

İptal Durum Kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıttır.

Kamuoyunca Güvenilen Sertifika: Karşılık gelen kök sertifikanın, güvenilir bir referans noktası olarak yaygın kullanılan yazılım uygulamalarında dağıtılması uyarınca güvenilen sertifikadır (Publicly-Trusted Certificate – PTC)

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: Bilgi Teknolojileri ve İletişim Kurumu'dur.

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

Mobil İmza: Mobil iletişim cihazlarıyla, ilgili ağ ve hizmet altyapısı kullanılarak nitelikli elektronik sertifika sahibi tarafından oluşturulan güvenli elektronik imzadır.

Mobil İmza Hizmeti: Kanun ve ilgili mevzuat koşullarına uyan ve kullanıcılar tarafından mobil iletişim cihazları aracılığıyla çeşitli servislerde kullanılacak imzaya ilişkin verilen hizmettir.

Mobil Operatör: Mobil imza kullanıcısı nitelikli elektronik sertifika sahiplerine GSM altyapısı üzerinden işlem yapma imkânı sağlayan ve mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için kurumsal başvuru sahibi olan operatördür.

Nesne İmzalama Sertifikası (NİMS): Bilgisayarda çalıştırılabilen bir yazılım kodunun kaynak sahibini doğrulayan sertifikadır.

Nitelikli Elektronik Sertifika (NES): Kanunun 9 uncu maddesinde sayılan niteliklere sahip elektronik sertifikadır.

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

Özne: Sertifikanın CN alanında yer alan kişi veya sunucu adıdır.

Sertifika: Bkz. "Elektronik Sertifika"

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 Sahibi: Adına, sertifika hizmetlerinin koşullarına ilişkin ESHS ile sertifika sahibi taahhütnamesi veya sözleşmesi imzalanan kişidir.

Sertifika Uygulama Esasları: Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgedir.

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 talepler doğrultusunda sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birimdir.

Sertifika Yenileme: İmza doğrulama verisi de dâhil 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.

SIM Kart: Hat sahiplerinin mobil operatörden temin edeceği, çeşitli özel uygulamaları barındıran, mobil iletişim cihazlarıyla entegre çalışan ve mobil imza hizmetinde kullanılabilen SIM karttır.

SSL (Secure Sockets Layer): İnternet haberleşmesinde veri gizliliğinin sağlanması, veriyi sunan sunucu kaynağının doğrulanması ve opsiyonel olarak veriyi alan istemcinin doğrulanması amacıyla geliştirilmiş güvenlik protokolüdür.

SSL Sertifikası: Veriyi sunan sunucu kaynağının kimliğini doğrulayan sertifikadır.

Tebliğ: Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmzaya İlişkin Süreçler ile Teknik Kriterlere İlişkin Tebliğ'dir.

Yönetmelik: Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliktir.

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. Sertifika Bilgilerinin Yayımlanması

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 dokümanı, bu ilkelerin nasıl uygulandığını gösteren SUE dokümanı, sertifika sahibi ve ESHS sertifika hizmetleri taahhütnameleri veya anlaşmaları, 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 sunucularda ve bilgi deposunda yayımlanır. Güncel iptal durum kayıtları, hem OCSP desteğiyle hem de SİL'ler aracılığıyla erişime açık tutulur.

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

Bu bölümde sözü geçen bilgilere erişim, http://www.turktrust.com.tr adresli TÜRKTRUST web sitesinden kamuya açık olarak sağlanır.

2.3. Yayımın 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 yayımlanır. SİL, 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle yayımlanır.

TÜRKTRUST, OCSP ve SİL yayımlama hizmetlerinin cevap verme süresinin 10 (on) saniyenin altında kalması sağlar.

2.4. Bilgi Deposuna Erişim Kontrolleri

Bilgi deposu herkesin erişimine açıktır. TÜRKTRUST bu amaçla, yayımlanan bilgilerin gerçekliğini sağlamak üzere, http://www.turktrust.com.tr adresi için 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 Anlamlı 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 sertifika üretmez.

3.1.4. İsim Biçimlerinin Değerlendirilmesi

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

3.1.5. İsimlerin Benzersizliği

TÜRKTRUST tarafından verilen sertifikalar, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin eşsiz biçimde belirlenmesine olanak tanır. Mevzuata bağlı nedenlerle sertifika tiplerine göre ayırt edici isim alanları farklı bilgileri içerir.

3.1.5.1. NES

TÜRKTRUST NES'lerde kullanılan isimler, kendi aralarında benzersizdir.

3.1.5.2. SSL ve EV SSL (Türkiye'de yerleşik ticari kişiler)

TÜRKTRUST SSL ve EV SSL sertifikalarında sertifika sahibini eşsiz biçimde ayırt edilmesi amacıyla ayırt edici isim alanı tüzel kişiliğin türüne göre biçimlendirilir.

3.1.5.3. SSL ve EV SSL (Türkiye'de yerleşik olmayan ticari kişiler)

SSL sertifikalarında, ayırt edici isim alanında Türkiye'de yerleşik olan kişiler için aranan şartlar, ilgili yerel mevzuata göre muadil resmi dayanak belgeleri istenerek uygulanır.

3.1.5.4. NİMS

TÜRKTRUST NİMS sertifikaları için ayırt edici isim alanı, kişisel veya kurumsal bilgi içeren alanlardır.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

Sertifika sahipleri, sertifika başvurularında ticari marka isimlerinin doğru biçimde yer almasından sorumludur. Bu bağlamda, sertifika sahipleri diğer kişilere ait fikri mülkiyet veya isim haklarının her türlü ihlalinden sorumlu olurlar. TÜRKTRUST, SSL ve EV SSL sertifika başvurularında yer alan ticari marka isimlerini kontrol eder. Bununla birlikte TÜRKTRUST, sertifika başvurusunda ticari marka isimlerinin kullanımına ilişkin bir ihlali tespit ederse başvuruyu reddetme, veya sertifika iptal etme hakkını saklı tutar.

3.2. İlk Kimlik Doğrulama

3.2.1. Gizli Anahtara Sahip Olunduğunun Kanıtlanma Yöntemi

Sertifika başvuru sahibinin, gizli anahtara sahip olduğunun doğrulanması gerekir. Gizli anahtarın TÜRKTRUST tarafından sertifika başvuru sahibi adına üretildiği durumlarda bu şart aranmaz.

3.2.2. Tüzel Kişiliğin Doğrulanması

Bir sertifikada bir tüzel kişiliğin isminin veya unvanının yer alması halinde, tüzel kişiliğin ismi veya unvanı sertifika türüne göre aşağıdaki ilke ve kurallar çerçevesinde doğrulanır.

3.2.2.1. NES, SSL ve NİMS

Sertifikada yer alacak tüzel kişiliğin ismi veya unvanı, sertifika sahibinin bulunduğu ülkedeki yasal belgelere bağlı olarak doğrulanır. Burada yapılan doğrulama işlemi TÜRKTRUST prosedürlerinde belirlendiği gibi yürütülür.

SSL ve NİMS başvurularında, sertifika başvuru sahibi adına başvuru işlemlerini yürüten yetkilinin beyan ettiği e-posta adresinin yetkili kişi tarafından doğrulanması gerekir.

3.2.2.2. EV SSL

EV SSL başvuru sahiplerinin kimlik doğrulamalarında en az aşağıdaki şartlar aranır:

- Sertifikada yer alacak tüzel kişiliğin ismi veya unvanı, sertifika sahibinin bulunduğu ülke mevzuatına göre düzenlenmiş yasal belgelere göre doğrulanır. Bu doğrulamaya ek olarak, sertifika başvuru sahibinin ilgili tüzel kişiliği temsil ve ilzama yetkili olduğunu gösteren imza sirküleri veya ilgili mevzuata göre geçerli yasal belge de aranır.
- Sertifika başvuru sahibinin sunduğu hizmet veya sattığı malı kullanan üçüncü bir kişiden, sertifika başvuru sahibinin faaliyetinin devamı teyit edilir. Mümkün olan hallerde, sertifika başvuru sahibinin bir kamu idaresinden veya kamu adına resmi belge düzenlemeye yetkili kişilerce ibraz edilebilecek güncel resmi belge de faaliyetinin devamının doğrulanması için yeterlidir.
- Sertifika başvuru sahibinin merkez adresi, sertifika sahibinin bulunduğu ülke mevzuatına göre düzenlenmiş yasal belgelere göre doğrulanır. Ayrıca sertifika başvuru sahibi tarafından başvuru belgelerinde ibraz edilen telefon numaralarıyla yasal kayıtların uyuşup uyuşmadığı kontrol edilir ve uyuşmaması halinde düzeltme talep edilir. Buna göre doğrulanan telefon numaralarından sertifika başvuru sahibi aranarak başvurusunu teyit etmesi istenir.
- Sertifika başvuru sahibi adına başvuru işlemlerini yürüten yetkilinin beyan ettiği e-posta adresinin, yetkili kişi tarafından gönderildiğinin doğrulanması gerekir. Sertifika başvuru sahibinin, sertifikada yer alacak alan adına ilişkin olmak üzere;
  - Alan adının üzerine kayıtlı olması şartı veya
  - Alan adının kayıtlı sahibi tarafından, alan adının kullanımına ilişkin münhasır hak ve yetki verilmiş olması şartı aranır.

EV SSL sertifika başvurularında tüzel kişiliğin doğrulanmasında aranan tüm şartlar, SUE dokümanı EK'te sunulmuştur. Tüzel kişiliğin doğrulanmasına ilişkin süreç burada belirlenen şartlara bağlı kalmak kaydıyla TÜRKTRUST prosedürlerine göre yürütülür.

3.2.3. Gerçek Kişinin Kimliğinin Doğrulanması

NES başvurusunda bulunan kişilerin sertifikada yer alacak bilgileri, yasal düzenlemelerle belirlendiği şekilde ve resmi belgelere dayandırılarak doğrulanır. NES

başvuruları alınırken, mevzuat gereği kişinin birinci başvurusu sırasında yüz yüze kimlik doğrulaması yapılır.

İkinci ve daha sonraki başvurularda,

- Geçerli son sertifikanın kullanım süresi sonundan itibaren 6 (altı) aydan daha uzun bir süre geçmiş olması veya
- Geçerli son sertifikanın içeriğinde "DN" alanındaki TCKN veya isimde değişiklik olması

halinde yüz yüze kimlik doğrulaması yapılır İkinci veya daha sonraki başvurularda kimlik doğrulamasına ihtiyaç olmayan hallerde, telefon, faks veya e-posta gibi yollarla doğrulama TÜRKTRUST prosedürlerine göre yapılır.

3.2.4. Doğrulama Yapılmaksızın Sertifikada Yer Alabilen Bilgiler

NES başvurularında e-posta adresi sertifika başvuru sahibinin yazılı beyanıyla alınır ve doğrulama yapılmaksızın sertifika içeriğinde yer alır.

Sertifikalarda bulunabilen "S" ve "OU" gibi ayırt edici isim alanında yer alan diğer bilgilerde de sertifika başvuru sahibinin beyanına göre doğru kabul edilir.

3.2.5. Yetkinin Doğrulanması

NES içeriğinde bir tüzel kişiliğin isminin yer alması söz konusu ise sertifika başvuru sahibinin bu tüzel kişiliği temsil ve ilzama yetkili olduğunu gösterir resmi belgeleri ibraz etmesi zorunludur.

3.2.6. Karşılıklı Çalışma Kriterleri

TÜRKTRUST, başka bir ESHS ile karşılıklı çalışma amacıyla çapraz veya tek yönlü sertifikasyon yapmaz.

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 NES başvurusunda bulunmasıyla gerçekleştirilir. Yeni sertifika başvurusu, sertifikanın kullanım süresi içinde, elektronik ortamda ve mevcut sertifikaya bağlı imza oluşturma verisiyle imzalanarak yapılabilir. Bu durumda eğer anahtar çifti sertifika sahibi tarafından üretiliyorsa sertifika talebiyle birlikte imza doğrulama verisi de ESHS'ye gönderilir.

Yeni sertifika içinde yer alacak bir bilgide değişiklik gerekmesi durumunda, bu değişikliğin resmi belgeye dayandırılması zorunludur. Sertifikada yer almayan diğer kullanıcı bilgilerindeki değişiklikler de NES sahibinin yazılı veya elektronik beyanıyla kabul edilir.

Anahtar yenilemesinde, NES sahibinin yeniden yüz yüze kimlik tespiti yapması aranmaz. Ancak, telefon veya faks ile yapılan kimlik doğrulamasında bir tereddüt olması halinde yüz yüze kimlik tespiti istenir.

Geçerli bir NES sahibi için anahtar yenileme talebi, sertifikasının süre sonundan en erken 30 (otuz) gün önce yapılabilir. Yapılmış bir talep en fazla 30 (otuz) gün süreyle geçerliliğini korur.

SSL, EV SSL ve NİMS için sertifika ve anahtar yenileme yapılmaz.

Sertifika sahibinin ilk başvurusundan yenileme başvurusuna kadar geçen sürede TÜRKTRUST sertifika hizmetlerinin sağlanmasına ilişkin kayıt ve şartlarda değişiklik olmuş ise bu değişiklikler uygun biçimde sertifika sahibine bildirilir.

3.3.2. İptal Sonrası Anahtar Yenileme için Kimlik Doğrulama

Aşağıda sayılan "iptal nedeni" haller dışında iptal sonrası anahtar yenilemesi sırasındaki kimlik doğrulaması Madde 3.3.1'de açıklandığı şekilde yapılır:

- Sertifika içeriğinde yer alan bilgilerdeki eksik, kusur veya hataya bağlı iptaller.
- Sertifika başvurusuyla birlikte alınan yetki belgesi, adres ve benzeri belgelerde eksikliğe, kusura veya hataya veya bu belgelerin geçerliliğini yitirmiş olmasına bağlı iptaller.
- Sertifika sahibinin faaliyetinin devam etmemesi veya yasal varlığının ortadan kalkması veya bunlara ilişkin kuvvetli şüpheye bağlı iptaller.

Burada sayılan haller için anahtar yenileme yapılmaz ve ilk kez başvuru yapılıyormuş gibi sertifika başvuru prosedürleri uygulanır.

3.4. İptal Talebi için Kimlik Doğrulama

TÜRKTRUST, NES iptal taleplerini aşağıda açıklandığı gibi güvenilir yollarla alır ve kimlik doğrulaması yapar:

- Sertifika sahibi, başvuru sırasında belirlenmiş kendisine özel bilgileri doğrulayarak TÜRKTRUST web sayfasından, sesli yanıt sisteminden veya kendisine sağlanmış diğer TÜRKTRUST yazılımlarıyla sertifikasını askıya alır veya iptal eder.
- Sertifika sahibi iptal talebini, TÜRKTRUST'a faksla iletebilir. Bu durumda, sertifika derhal askıya alınır. Yazılı iptal talebinin ulaşmasıyla veya askı süresinin dolmasıyla birlikte sertifika iptal edilir. Askı süresi içinde sertifika sahibi iptal nedeninin ortadan kalktığını yazılı olarak tebliğ ederse, sertifika askıdan çıkarılır.

TÜRKTRUST SSL, EV SSL ve NIMS için iptal taleplerini aşağıda açıklandığı gibi güvenilir yollarla alır ve kimlik doğrulaması yapar:

- Sertifika sahibi, iptal talebini TÜRKTRUST'a kurum yetkilisi imzalı faksla bildirir. Bu faksın ulaşmasının ardından kurum yetkilisine telefonla ulaşılarak iptal talebi doğrulanır ve sertifika iptal edilir.
- Sertifika sahibi, web üzerinden iptal başvurusunu tercih ederse, sunucu sorumlusu sertifika tipi, sertifika seri numarası gibi sertifika bilgilerini girerek TÜRKTRUST web sitesinde interaktif işlemler alanına bağlanır. İkincil kimlik doğrulama aşamasını da geçildikten sonra sertifika iptal nedeni girer. Sistem üzerinden çevrim içi iptal işlemi 7 gün 24 saat ilkesine göre tamamlanır. İşlem sonrası iptal durumu yetkiliye e-postayla bildirilir.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ

TÜRKTRUST, sertifikalarını bu Sİ dokümanında yer alan ilke ve kurallar uyarınca üretir ve yaşam döngüsünü yönetir. İzleyen bölümde, farklı sertifika çeşitleri için yürütülen ilkeler açıklanmıştır.

4.1. Sertifika Başvurusu

4.1.1. Kimler Sertifika Başvurusunda Bulunabilir?

Herhangi bir yasal engeli olmayan her gerçek kişi NES veya NİMS başvurusunda bulunabilir.

SSL, EV SSL ve NİMS sertifikaları için özel hukuk tüzel kişileri ile kamu kurum ve kuruluşları dâhil olmak üzere her tüzel kişi sertifika başvurusunda bulunabilir.

TÜRKTRUST, bir sertifika başvurusu sırasında sunulacak tüm gerekli bilgileri 20 (yirmi) yıllık bir süre boyunca saklama ve arşivleme hakkı olduğunu beyan eder.

4.1.2. Sertifika Başvuru, Kayıt Süreci ve Sorumluluklar

Sertifika başvuru kaydı, aşağıda açıklandığı gibi iki ana adımdan oluşur:

- Kayıt: Sertifika başvurusunun dayanak belgelerine göre doğrulanması ve eksiksiz ve doğru biçimde kaydedilmesi.
- Anahtar üretimi: Açık ve gizli anahtar çifti, sertifika başvuru sahibi veya TÜRKTRUST tarafından üretilir. Anahtar çiftinin sertifika başvuru sahibi tarafından üretilmesi durumunda, açık anahtarın belirlenen prosedür ve standartlara göre TÜRKTRUST'a elektronik ortamında gönderilmesi gerekir. Bu durumda TÜRKTRUST, sertifika başvuru sahibinin açık anahtara karşılık gelen gizli anahtara sahip olduğunu gösteren bu elektronik kaydı doğrular.

Çeşitli sertifika türlerine göre yukarıda sayılan adımların uygulamasına ilişkin ayrıntılar aşağıda açıklanmıştır.

TÜRKTRUST NES başvurusu farklı yöntemlerle gerçekleştirilebilir. TÜRKTRUST'ın ofisi bulunan yerlerde, başvuru sahibi TÜRKTRUST ofisine şahsen giderek başvuru yapabileceği gibi kendi bulunduğu yerde başvurusu alınmak üzere ücret karşılığında TÜRKTRUST yetkilisinin gelmesini talep edebilir. TÜRKTRUST'ın doğrudan hizmet vermediği yerlerde başvuru sahibinin noterde yüz yüze kimlik tespiti yaptırması zorunludur. Tüm TÜRKTRUST NES başvuruları TÜRKTRUST'ın web sitesinde yapılan çevrimiçi başvuruyla başlatılabilir. Doğrudan hizmet alınmasının söz konusu olması halinde (eksprEs-İmza) web başvurusu ön şarttır. NES başvurusu sırasında, başvuru sahibi, sertifika başvuru formunu eksiksiz bir biçimde doldurur ve imzalar. İstenilen kimlik doğrulama belgelerini ve imzalı sertifika sahibi taahhütnamesini başvuru formuyla birlikte TÜRKTRUST'a iletir. eksprEs-İmza başvurularında sertifika sahibinin başvuru belgeleri elden alınır ve kimlik doğrulaması yapılır.

Mobil imza kullanım amaçlı NES başvuruları, kurumsal başvuru sahibi olan mobil operatör tarafından hat kullanıcıları adına, gerekli bilgi ve belgeler hat kullanıcılarından alınarak, mobil imza hizmet altyapısı kullanılarak yapılır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Doğrulama İşlemlerinin Yerine Getirilmesi

NES başvurusu sırasında, başvuru sahibinin kimliği yasal düzenlemeler uyarınca resmi belgelere dayandırılarak doğrulanır. İlk başvuru sırasında kimlik doğrulama işlemi TÜRKTRUST tarafından yüz yüze yapılır. Sonraki başvurularda bu şart aranmayabilir.

Mobil imza kullanım amaçlı NES başvuruları, mobil operatörü tarafından sağlanan kanallar üzerinden ön kayıt işlemi başlatılır. Ardından, mobil operatörün sağladığı kayıt merkezleri üzerinden hat sahibinin ve/veya hat kullanıcısının başvuru bilgi ve belgeleri alınır.

SSL, EV SSL ve NİMS sertifikaları başvuruları Bölüm 3.2'de açıklanan esaslar ve buna bağlı TÜRKTRUST prosedürleri uyarınca yürütülür.

4.2.2. Sertifika Başvurularının Kabulü veya Reddedilmesi

Aşağıdaki koşulların yerine gelmesi halinde bir sertifika başvurusu kabul edilir:

- Bölüm 3.2'de açıklanan esaslar ve TÜRKTRUST başvuru prosedürlerine göre gerekli form ve belgelerin eksiksiz olarak tamamlanmış olması.
- Ödemenin yapılmış olması.

TÜRKTRUST, aşağıdaki hallerin herhangi birinin oluşması halinde sertifika başvurusunu reddeder:

- Bölüm 3.2'de açıklanan esaslar ve TÜRKTRUST başvuru prosedürlerine göre gerekli form ve belgelerin tamamlanmaması.
- Bilgi ve belgelerin doğrulanmasına ilişkin sorgulamalara başvuru sahibinin zamanında veya tatminkâr yanıt vermemesi.
- SSL, EV SSL ve NİMS için, başvuru kaydından sonra CSR dosyasının en geç 30 (otuz) gün içinde TÜRKTRUST'a ulaşmaması.
- SSL, EV SSL veya NİMS için yapılan bir başvuruda sertifika üretilmesinin, TÜRKTRUST'ın itibarını zedeleyebileceğine ilişkin kuvvetli bir kanaatinin oluşması.
- Ödemenin yapılmamış olması.

4.2.3. Sertifika Başvurularının İşlenme Süresi

TÜRKTRUST'a ulaşan NES başvurularının işlenme süresi en çok 5 (beş) iş günüdür. TÜRKTRUST "eksprEs-İmza" başvuruları, başvuruyla aynı gün içinde işlenir.

SSL, EV SSL ve NİMS başvuruları TÜRKTRUST'a ulaştıktan sonraki en geç 5 (beş) iş günü içinde işlenir.

Bu madde altında sertifika başvurularının işlenmesine ilişkin verilen süreler, sertifika başvurularının Bölüm 3.2'de yer alan esaslar ve TÜRKTRUST prosedürlerine göre eksiksiz ve doğru olması halinde geçerlidir.

4.3. Sertifika Üretimi

4.3.1. Sertifika Üretimi Sırasındaki ESHS Faaliyetleri

Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları TÜRKTRUST prosedürlerinde belirlendiği şekliyle sertifika üretim merkezlerinde işlenir ve sertifikalar üretilir.

4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika üretimi tamamlandıktan sonra, sertifika sahibine e-posta veya SMS ile üretimin yapıldığı bilgisi gönderilir.

4.4. Sertifikanın Kabulü

4.4.1. Kabulün Şekli

Sertifika sahipleri, tüm sertifika tipleri için sertifikayı yüklemeden veya kullanmadan önce sertifika içeriğindeki bilgileri gözden geçirmek ve doğrulamakla, doğru olmayan veya başvuruyla tutarsız bilgiler olması durumunda TÜRKTRUST'ı bilgilendirmek ve sertifikanın iptalini talep etmekle yükümlüdür.

4.4.2. ESHS Tarafından Sertifikanın Yayımlanması

Sertifikalar, sertifika sahiplerinin yazılı rızası olması kaydıyla web üzerinde veya dizin sunucularda yayımlanır.

4.4.3. Diğer Katılımcıların 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 sahibi, sertifikasını ve sertifikaya ait gizli anahtarı, Kanun, Yönetmelik ve diğer düzenlemeler ile Sİ ve SUE kitapçıklarında ve ilgili sertifika sahibi taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanılabilir.

Sertifika sahibi, sertifikasına karşılık gelen gizli anahtarı diğer kişilerin erişimine karşı korumak ve kendisine mevzuat ile Sİ ve SUE kitapçıklarında ve ilgili sertifika sahibi taahhütnamesinde tanınan yetki ve sınırlar içinde kullanmakla yükümlüdür.

NES için imza oluşturma verisi erişim şifresi, aktivasyon kullanılmayan durumlarda sertifika sahibine şifre zarfıyla gönderilir. Şifre zarfı yerine aktivasyon uygulanması halinde, sertifika sahibi TÜRKTRUST'ın sağlamış olduğu yazılım aracılığıyla erişim şifresini kendisi belirler.

NES sahibi,

- Adına düzenlenen güvenli elektronik imza oluşturma aracını ve bu araca ait varsa erişim şifrelerini şahsen teslim almalıdır.
- Aktivasyonla belirlenen erişim şifreleri için cep telefonunun veya e-posta adresinin diğer kişilerce kullanımına izin vermez.
- 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 verir.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

Üçüncü kişiler, güvenecekleri sertifikaların geçerliliğini kontrol etmekle ve sertifikaları Kanun, Yönetmelik ve diğer düzenlemeler ile Sİ ve SUE kitapçıklarında belirlenmiş kullanım amaçları dâhilinde kullanmakla yükümlüdürler.

Sertifikanın geçerliliğinin kontrolü makul ve güvenli koşullar altında yapılmalıdır. Aksi yönde bir durumun oluştuğuna dair bir tereddüt olması halinde, üçüncü kişiler gerekli tedbirleri alır. Bu bağlamda üçüncü kişiler sertifikaya güvenmeden önce;

- Sertifikanın kullanım amacına uygun kullanıldığını; özel olarak bir hatanın yaralanma, ölüm veya çevresel zarara yol açabildiği nükleer tesis, hava trafik kontrol, uçak navigasyon veya silah kontrol gibi sistemlerde kullanılmadığını,

- Sertifika içeriğinde yer alan "anahtar kullanımı" alanının kullanım durumuyla uyumlu olduğunu,
- Sertifikanın dayandığı kök ve alt kök sertifikalarının geçerli olduğunu, diğer bir deyişle sertifikanın askıya alınmadığını, iptal edilmediğini veya süresinin dolmadığını ve sertifikayı veren ESHS'yi tanıdığını,

kontrol etmekle yükümlüdür.

Bu işlemler sırasında, mevzuat ve standartlarca belirlenmiş güvenli yazılım ve donanım araçlarının kullanılması üçüncü kişilerin sorumluluğundadır.

Sertifikaya güvenmeden önce üçüncü kişilerin imza doğrulama verisi ve sertifika kullanımında burada sayılan şartları yerine getirmemelerinden TÜRKTRUST sorumlu tutulamaz.

4.6. Sertifika Yenileme

Sertifika yenileme, sertifika içeriğinde açık anahtar dâhil aynı bilgiler yer almak kaydıyla, sertifika geçerlilik süresinin uzatıldığı yeni bir sertifika üretilmesiyle yapılır.

Sertifika yenilemenin yapılabilmesi için, sertifikanın gizli anahtarının açığa çıkmamış olması zorunludur.

Sertifika türlerine göre, sertifika yenilemedeki farklılıklar aşağıdaki gibidir:

NES için, geçerlilik süresi dolan sertifikalara dayanılarak sertifika yenileme başvurusu yapılamaz. Anahtarların kriptografik güvenliği bakımından, aynı içerikle bir sertifikanın toplam geçerlilik süresi 3 (üç) yıldan fazla olamaz.

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.

Geçerlilik süresi içinde yenileme başvurusunun yapılmış olması kaydıyla, süresi dolmuş sertifika da yenilenebilir. Bu yenileme işlemi en geç 30 (otuz) gün içinde yapılır, aksi takdirde sertifika başvurusu reddedilir.

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Sertifika sahibi veya sertifika sahibini temsile yetkili kişi tarafından yenileme talebinde bulunulabilir.

4.6.3. Sertifika Yenileme Talebinin İşlenmesi

Sertifika yenileme işlemi sadece NES için gerçekleştirilir. Yukarıda açıklandığı gibi, gizli anahtarın açığa çıkmış olması veya yenileme süresiyle birlikte anahtarların kriptografik güvenliğinin tehlikeye düşecek olması veya yenileme talebinin 30 (otuz) günlük geçerlilik süresini doldurması hallerinde sertifika yenileme talebi reddedilir.

NES için sertifika yenileme süresi her durumda 1 (bir) yıldır. Geçerlilik süresi içinde NES sahibi, sertifika yenileme başvurusunu sadece İnternet üzerinden ve elektronik imza ile yapabilir. Bu işlemle sertifika sahibi sertifika yenileme talebini imzaladığı gibi, sertifikaya bağlı imza oluşturma verisine sahip olduğunu da göstermiş olur. Yenileme talebinin kabulü aşağıdaki şartların tamamının sağlanmasına bağlıdır:

- Sertifika başvuru sahibinden önceki başvuru sırasında verilen bilgilerin hala geçerli olduğunu açıkça gösteren yazılı bir taahhüt alınır. Böyle bir yazılı bir

taahhüdün olmaması veya sertifika içeriğinde bilgi değişikliği olduğuna dair bir malumat alınması durumunda, Bölüm 4.7'de yer alan esaslar uygulanır.

- Yenilenecek sertifikayla birlikte toplam anahtar süresi 3 (üç) yılı aşamaz. Öznenin gizli anahtarının ortaya çıkmasına ilişkin bir belirti bulunması durumunda, anahtar yenileme işlemi gerekir.
- Ödemenin yapılmış olması.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür.

4.6.5. Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.6.6. ESHS Tarafından Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.7. Anahtar Yenileme

Aşağıda NES için açıklanan özel hal dışında, anahtar yenileme uygulama dışıdır.

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

NES için geçerlilik süresinin ilk 3 (üç) ayı içinde sertifika sahibinin kartından sertifikanın silinmiş olması, kartın kaybolması veya kartın bir biçimde çalışamaz olması durumunda, yeniden belge istenmeksizin anahtar yenilemeyle yeni bir sertifika üretilir. Sertifika sahibinin ilk başvuruda sağlamış olduğu hiçbir bilginin değişmemiş olması ön koşuldur. Gerekli görülen hallerde bilgilerin değişmemiş olduğu kontrol edilir.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

NES için sertifika sahibi gerçek kişidir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

NES'te herhangi bir bilgide değişiklik olduğuna dair bir belirti veya şüphe olması durumunda, ilgili bilgi ve destekleyici belgeler yeniden alınır.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.7.6. ESHS Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.7.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.8. Sertifika Değişikliği

4.8.1. Sertifika Değişikliğini Gerektiren Durumlar

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

Yeni sertifika başvurusu Bölüm 4.1'de belirtilen ilkeler uyarınca yürütülür.

4.8.2. Sertifika Değişiklik Talebinde Bulunabilecek Kişiler

Bölüm 4.1.1'de yer alan ilkeler uyarınca yürütülür.

4.8.3. Sertifika Değişiklik Talebinin İşlenmesi

Bölüm 3.2'de yer alan ilkeler uyarınca yürütülür.

4.8.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uyarınca yürütülür..

4.8.5. Değişiklik Yapılmış Sertifikanın Kabul Şekli

Bölüm 4.4.1'de yer alan ilkeler uyarınca yürütülür.

4.8.6. ESHS Tarafından Değişiklik Yapılmış Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan ilkeler uyarınca yürütülür.

4.8.7. Diğer Katılımcılarının Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

Uygulama dışıdır.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

4.9.1.1. Son Kullanıcı Sertifikaları

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. NES için iptal işlemi talebin ulaşmasının ardından derhal; SSL, EV SSL ve NİMS için en geç 24 (yirmi dört) saat içinde gerçekleştirilir. SSL, EV SSL ve NİMS için askıya alma işlemi uygulanmaz. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifika sahibinin veya temsile yetkili kişinin talebi,
- Sertifika başvurusunda veya sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması; TÜRKTRUST bu şartın oluştuğuna dair makul kanıta dayalı kanaat oluşturabileceği gibi aynı şart sertifika sahibi veya temsili yetkili kişinin bildirimiyle de oluşabilir.
- NES için, eksprEs-İmza üretimi sonrası ilgili sertifika kayıt merkezi aracılığıyla teslim edilecek olan e-imza paketinin 1 (bir) ay içinde sertifika başvuru sahibi tarafından teslim alınmaması veya standart NES üretimi sonrası kurye ile gönderilen e-imza paketinin 1 (bir) ay boyunca sertifika başvuru sahibi tarafından teslim alınmaması,
- Sertifika içeriğinde yer alan özne veya sertifika sahibi bilgilerinde bir değişiklik olması,

- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin veya ölümünün öğrenilmesi,
- SSL ve EV SSL sertifikaları için, sertifika sahibi tüzel kişinin yasal varlığının veya faaliyetinin devamının ortadan kalktığına dair TÜRKTRUST'a bir bildirimde bulunulması veya böyle olduğunun anlaşılması,
- Sertifikanın amacı dışında kullanıldığına dair kanaat veya kanıt oluşması,
- Bir Wildcard sertifikasının sahtecilikle yanlış yönlendirebilecek bir tam nitelikli alt alan adını doğruladığının anlaşılması halinde,
- SSL veya EV SSL sertifikasının oltalama, sahtecilik, zararlı yazılım dağıtma gibi suç unsuru oluşturan eylemlerde kullanıldığının tespit edilmesi halinde,
- Gizli anahtarın kaybedilmesi, çalınması, ortaya çıkma şüphesinin veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
- Gizli anahtara erişim şifresinin ortaya çıkması veya benzer bir nedenle sertifika sahibinin gizli anahtar üzerindeki kontrolünü kaybetmesi,
- Gizli anahtarın içinde bulunduğu yazılım veya donanım aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
- TÜRKTRUST'ın, sertifikanın Sİ ve SUE rehber kitapçıkları ile TÜRKTRUST sertifika sahibi taahhütnamesi veya anlaşması hükümlerine aykırı olarak kullanıldığına ilişkin bir bildirim alması veya böyle olduğunun anlaşılması,
- SSL ve EV SSL sertifikaları için, bir mahkemenin veya bir yetkilinin sertifika sahibinin alan adı sahipliğini veya kullanma yetkisini ortadan kaldırdığına dair TÜRKTRUST'a bir bildirimde bulunulması veya bunun TÜRKTRUST tarafından anlaşılması,
- Mobil imza kullanım amaçlı NES sahiplerinin, kullanmakta oldukları GSM hatlarına dair aboneliğin son bulması,
- TÜRKTRUST'ın tamamen kendi takdiri sonucu, sertifikanın verilişi sırasında işbu SUE rehber kitapçıklarının uygulama esaslarına ilişkin bir uygunsuzluk tespit etmesi.
- NES için, Kanun'a dayalı sertifika verme hakkının ortadan kalkması.
- SSL veya EV SSL sertifikaları için, TÜRKTRUST'ın sertifika verme hakkının ortadan kalkması.
- TÜRKTRUST kök veya alt kök sertifikalarına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması.
- SSL ve EV SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması,
- TÜRKTRUST'ın sertifika hizmetleri vermeyi durdurması ve başka bir ESHS ile anlaşmaması.

4.9.1.2. TÜRKTRUST Alt Kök Sertifikaları

Alt kök sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir. Aşağıda yer alan koşullar alt kök sertifikasının iptalini gerektirir:

- Üretimde kullanılan alt kök sertifikasına ait gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,

- Alt kök sertifikasının amacı dışında kullanıldığının ortaya çıkması,
- Alt kök sertifikanın TÜRKTRUST Sİ ve SUE rehber kitapçıkları ve BR gerekliliklerine uygun olarak üretilmediğinin ortaya çıkması,
- Alt kök sertifikanın içinde yer alan bilgilerin hatalı veya yanıltıcı olduğunun ortaya çıkması,
- TÜRKTRUST'ın herhangi bir nedenle faaliyetlerine son vermesi ve iptal desteğini sağlamak amacıyla herhangi başka bir ESHS ile anlaşmaması,
- TÜRKTRUST'ın sertifika verme yetkisinin süresinin dolması sona ermesi veya iptal edilmesi (SİL ve OCSP hizmetleri için gerekli düzenlemeler sağlanmışsa),
- TÜRKTRUST Sİ ve SUE rehber kitapçıkları uyarınca sertifika iptali gerekiyorsa,

TÜRKTRUST'ın, SSL ve EV SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması.

4.9.1.3. Alt ESHS Sertifikaları

Alt ESHS sertifikasının kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir. Aşağıda yer alan koşullar alt kök sertifikasının iptalini gerektirir:

- Alt kök sertifika kullanıcısı olan ESHS'nin yazılı iptal talebi,
- Alt kök sertifika kullanıcısı olan ESHS'nin, sertifika talebinin geçersiz olduğu bilgisini TÜRKTRUST'a bildirmesi,
- Alt kök sertifika kullanıcısı olan ESHS'nin sertifika üretimde kullandığı gizli anahtarların açığa çıkma şüphesinin oluşması veya açığa çıkması,
- Alt kök sertifikasının amacı dışında kullanıldığının ortaya çıkması,
- Alt kök sertifikanın TÜRKTRUST Sİ ve SUE rehber kitapçıkları ve BR gerekliliklerine uygun olarak üretilmediğinin ortaya çıkması,
- Alt kök sertifikanın içinde yer alan bilgilerin belirsiz veya yanıltıcı olduğunun ortaya çıkması,
- Alt kök sertifika kullanıcısı olan ESHS'nin veya TÜRKTRUST'ın herhangi bir nedenle faaliyetlerine son vermesi ve başka bir ESHS ile anlaşmaması.
- Alt kök sertifika kullanıcısı olan ESHS'nin veya TÜRKTRUST'ın sertifika verme yetkisinin sona ermesi veya iptal edilmesi (SİL ve OCSP hizmetleri için gerekli düzenlemeler sağlanmışsa),
- TÜRKTRUST Sİ ve SUE rehber kitapçıkları uyarınca sertifika iptali gerekiyorsa,
- Alt kök sertifika kullanıcısı olan ESHS'nin, SSL ve EV SSL sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması.

4.9.2. Sertifika İptal Talebinde Bulunabilecek Kişiler

Aşağıda belirtilen kişiler sertifika iptal talebinde bulunabilir:

- NES ve NİMS için, sertifika sahibi ile sertifikada kurum bilgisinin yer alması halinde ilgili kurumu temsile yetkili kişi,
- NES için, güvenli elektronik imza oluşturma aracının sahibi,

- SSL, EV SSL ve NİMS için sertifika sahibi tüzel kişiliği temsile yetkili kişi,
- Mobil imza kullanım amaçlı NES için mobil operatör,
- TBB alt kök sertifikası altında kalan sertifikalar için TBB yetkilileri,
- TÜRKTRUST yetkilileri.

4.9.3. Sertifika İptal Talebi Prosedürleri

NES iptal talepleri, sertifika sahibinden

- 7 gün 24 saat ilkesine göre TÜRKTRUST web sitesi üzerinden
- 7 gün 24 saat ilkesine göre, tüm müşterilere duyurulan ve açıkça ilan edilen telefon numarası üzerinden sesli çağrı sistemi aracılığıyla
- Mesai saatleri içinde yazıyla (faks ya da posta aracılığıyla gelen imzalı yazılar)

olmak üzere farklı yollarla alınabilir.

İşlem sonrası iptal durumu sertifika sahibine e-posta ile bildirilir.

Mobil imza kullanım amaçlı NES iptali için, sertifika sahibi mobil operatör çağrı merkezine ulaşarak iptal talebini bildirir. İşlem sonrası iptal durumu mobil imza hizmet altyapısı aracılığıyla sertifika sahibine bildirilir.

İçeriğinde kurum bilgisi de yer alan NES iptal talepleri, sertifika sahiplerinin yanı sıra onaylı iptal başvuruları ile ilgili kurumu temsile yetkili kişilerden de alınabilir. İşlem sonrası iptal durumu yetkili ile sertifika sahibine e-posta ile bildirilir.

Mobil imza kullanım amaçlı NES'lerin mobil operatör tarafından iptal edilmesinin gerektiği durumlarda, iptal talebi mobil imza hizmet altyapısı aracılığıyla TÜRKTRUST'a iletilir.

SSL, EV SSL ve NİMS için sertifika iptal talepleri sertifika sahibi tüzel kişiliği temsile yetkili kişi imzasıyla yazılı olarak veya 7 gün 24 saat ilkesine göre TÜRKTRUST web sitesi üzerinden alınır. İşlem sonrası iptal durumu yetkiliye e-postayla 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 kaynaklı tüm sertifika iptal işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur. Gereken durumlarda, yeni sertifika üretim işlemleri ücretsiz olarak, iptal işleminden sonra hemen başlatılır.

İptal edilmiş bir sertifikanın yeniden kullanılabilir hale gelmesi için bir prosedür olmadığı gibi, iptal edilmiş bir sertifikanın yeniden kullanılabilir hale getirilmesi için sunulan bir araç da yoktur. İptal işlemi, veri tabanında farklı güncellemelere yol açar; OCSP hizmetinde anlık güncelleme ve bir sonraki SİL'in güncellemesi. İptal edilmiş bir sertifika, geçerlilik süresinin sonuna kadar SİL'de yayımlanmaya devam eder.

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 sertifikanın imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar e-postayla bilgilendirilir.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Sertifika iptal talebi teknik ve ticari imkânların elverdiği en kısa süre içinde işleme alınır.

4.9.5. TÜRKTRUST'ın Sertifika İptal Talebini İşleme Süresi

TÜRKTRUST, kendisine web ve sesli çağrı sistemi 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. Yazıyla kağıt ortamında alınan sertifika iptal talepleri mesai saatleri içinde derhal değerlendirmeye alınır ve gerekli işlemler ivedilikle tamamlanır.

Mobil imza kullanım amaçlı NES iptal talepleri, kurumsal başvuru sahibi olan mobil operatör tarafından gerekli doğrulamaların yapılmasının ardından mobil imza hizmet altyapısı aracılığıyla TÜRKTRUST'a iletilir ve anında sonuçlandırılır.

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, Kanun'a göre oluşturulan güvenli elektronik imzalı doğrulamada 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 İmkânı (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.

TÜRKTRUST OCSP hizmeti kapsamında, sorgu yapan sistemlere verilen cevaplar, OCSP cevabı imzalama amacıyla üretilmiş olan OCSP hizmet sertifikaları kullanılarak imzalanırlar. Durumu sorgulanan ve TÜRKTRUST tarafından üretilmiş herhangi bir sertifika için oluşturulan cevap, bu sertifikayı imzalamış olan kök veya alt kök sertifika tarafından imzalanmış bir OCSP hizmet sertifikası kullanılarak imzalanır.

4.9.10. Çevrim İçi Sertifika İptal/Durum Kontrol Gereklilikleri

Üçüncü kişilerin sertifika durum sorgusu yaparken, eğer teknik imkânları 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 Yitirilmesine İlişkin 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'a ait bir güvenlik sorununun duyurulması durumunda, sertifika sahiplerinin sertifikalarını kullanmaya devam etmelerine izin verilmez.

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

4.9.13. Sertifika Askıya Alma Gerektiren Durumlar

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

SSL, EV SSL ve NİMS için askıya alma işlemi uygulanmaz. İkincil doğrulama adımları tamamlanarak sertifika iptal edilir.

4.9.14. Sertifika Askıya Alma Talebinde Bulunabilecek Kişiler

Bölüm 4.9.2'de yer alan ilkeler uyarınca yürütülür.

4.9.15. Sertifika Askıya Alma Talebi Prosedürü

Aşağıdaki istisnai haller saklı kalmak kaydıyla Bölüm 4.9.3'de yer alan ilkeler uyarınca yürütülür. TÜRKTRUST'a ait bir güvenlik sorunu oluşması ya da mevcut sertifikalarla ilgili ihbar alınması durumunda, SSL, EV SSL ve NIMS ikincil kimlik doğrulama adımı yapılarak ivedilikle iptal edilir, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur.

TÜRKTRUST'a ait bir güvenlik sorunu oluşması ya da mevcut sertifikalarla ilgili ihbar alınması durumunda NES'ler için iptal 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, NES iptal talep kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikaları, doğrulama işlemi sonuçlanıncaya veya süre sınırı aşılana 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.

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

SSL, EV SSL ve NİMS için askıya alma işlemi uygulanmaz.

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 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 12 (oniki) saatte bir olmak üzere günde 2 (iki) kez ve 24 (yirmidört) saatlik geçerlilik süresiyle, sertifika durumlarında hiçbir değişiklik olmasa bile yeni bir SİL yayımlar.

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.

TÜRKTRUST merkezinde sunulan sertifika hizmetleri, erişilebilirlik ve yeniden devreye alma amaçları uyarınca her zaman yeterli düzeyde bir altyapı ile idame ettirilir. Hizmetlerde kesintiye yol açan ve TURKTRUST'ın kontrolünün ötesinde bir durum ortaya çıktığında, TÜRKTRUST FKM, olayın ardından en geç 2 saat içinde sertifika hizmetlerinin yönetimini devreye alır.

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, imza oluşturma verisinin kendisi tarafından oluşturulması halinde, bu veriyi hiçbir biçimde 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 dokümanının 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 güvenlikli bölgeler ve çeşitli güvenlik alanları oluşturulmuştur.

5.1.2. Fiziksel Erişim

TÜRKTRUST merkezindeki ve Türkiye Barolar Birliği'ndeki NES üretim 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 kâğıt 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 yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Kayıt ve Müşteri Hizmetleri Yetkilileri:** Müşteri hizmetleri, evrak kontrolü, sertifika başvuru kaydı, üretim, nitelikli elektronik sertifikaları askıya alma ve iptal gibi rutin sertifika hizmetlerinden sorumlu çalışanlardır
- **Güvenlik Yetkilileri:** Güvenlik politikaları ve uygulamalarının yönetimi ve yürütülmesinden sorumlu çalışanlardır.
- **Sistem Yöneticileri:** Sertifika hizmetlerine ilişkin sistemlerin kurulumu, konfigürasyonu ve devamlılığının sağlanması ve aynı zamanda sistem yedekleme ve geri yükleme işlemleri için yetkilendirilmiş çalışanlardır.
- **Sistem Denetçileri:** Sertifika hizmetlerine ilişkin arşivlerin ve denetim kayıtlarının izlenmesi için yetkilendirilmiş çalışanlardır.
- **Güvenlik Görevlileri:** Tüm TÜRKTRUST tesislerinin fiziksel güvenliğini sağlamaktan sorumlu çalışanlardır.

5.2.2. Her Görev İçin Gereken En Az Kişi Sayısı

TÜRKTRUST'ta sertifika süreçleri dâhilindeki 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, iptal ve yedekleme 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 bütününü 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 eğitimli, benzer çalışma alanlarında deneyimli ve güvenlik kontrollerinden geçmiştir.

5.3.2. Kişisel Geçmiş Kontrol Gereklilikleri

TÜRKTRUST'ta çalışan personelin özgeçmişi 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 dâhilinde 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 dokümanları, sertifika süreçleriyle ilgili kurumsal prosedürler ve güvenlik prosedürleri ile talimatları, çalışanların rollerine göre düzenlenmiş görev tanımları, 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 işlemin tanımı, işlemi yapan kişi, işlemin tarih ve zaman bilgisi ve işlemin sonucu 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, aktif kullanım süresince 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

İlgili prosedürler 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 taahhütnamesi, 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

NES'lerle ilgili TÜRKTRUST işleyişine ait arşivler, yasal düzenlemeler uyarınca en az 20 (yirmi) yıl süreyle saklanır. SSL, EV SSL ve NİMS'lere ilişkin arşivler de TÜRKTRUST tarafından 20 (yirmi) yıl süreyle korunur.

5.5.3. Arşivlerin Korunması

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

5.5.4. Arşivlerin Yedeklenme Prosedürleri

İlgili prosedürler uyarınca, elektronik ortamdaki arşivlerin yedekleri tutulur. Kağıt ortamdaki arşivlerin ise yedekleri alınmaz.

5.5.5. Kayıtların Zaman Damgası Altına Alınması Gereklilikleri

TÜRKTRUST elektronik arşiv kayıtları zaman bilgisiyle birlikte saklanır.

5.5.6. Arşiv Toplama Sistemi

Arşiv kayıtları, TÜRKTRUST arşiv yönetim sistemi kullanılarak, ilgili prosedürler uyarınca 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 Yitirilmesi ve Felaket Kurtarma

5.7.1. Güvenlik Kaybına Neden Olabilecek Olaylar

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST bilgi güvenliği ihlal olayı ve iş sürekliliği yönetimi 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 yitirilmesi 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. İş Sürekliliği Yetenekleri ve Felaket Kurtarma

TÜRKTRUST merkezi dışında felaket kurtarma merkezi (FKM) tesis etmiştir. Afet sonrasında iş sürekliliğini temin etmek üzere TÜRKTRUST merkezinde bulunan veriler yedeklenir.

TÜRKTRUST işleyişini engelleyecek nitelikte olayların ya da güvenlik sorunlarının oluşması durumunda, TÜRKTRUST iş sürekliliği prosedürü ve planı uyarınca duruma müdahale edilir.

5.8. TÜRKTRUST'ın Faaliyetinin Son Bulması

TÜRKTRUST'ın faaliyetlerinin son bulması halinde, 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.

SSL, EV SSL ve NİMS sertifika sahipleri de bu durumdan haber edilir. NES için zorunlu olarak yapılan devir işlemi ilkesel olarak bu sertifikalar için de yapılmaya çalışılır. Bu kapsamda geçerlilik süresi içinde olan sertifikaların, bunlara ilişkin TÜRKTRUST yükümlülüklerinin ve geçerli sertifikaların durum bilgilerinin yayımlanmasının devam edilmesine ilişkin hususlar yapılacak devirde düzenlenir.

6. TEKNİK GÜVENLİK KONTROLLERİ

Sİ dokümanının bu kısmında, TÜRKTRUST'ın sertifika hizmetleriyle ilgili iş süreçlerinde kullanılan gizli anahtarlarının 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

TÜRKTRUST kök ve alt kök sertifikalarına ait anahtar çiftleri, sadece yetkili kişilerin kontrolünde, iki yetkilinin hazır bulunmasıyla, Bölüm 5.2.2'de belirtildiği gibi teknik ve idari güvenlik önlemleri alınmış ortamlarda, TÜRKTRUST kök sertifika üretim ve yayımlama prosedürü uyarınca üretilir ve uygun biçimde yedeklenir. İmza oluşturma verisi yetkisiz erişime karşı fiziksel ve teknik güvenlik önlemleriyle korunur.

TÜRKTRUST kök ve alt kök sertifikaları anahtar çifti üretiminde en az EAL4+ veya FIPS 140-2 Düzey 3 güvenlik düzeyinde kriptografik güvenlik donanım modülü kullanılır. Anahtar çiftlerinin uzunluğu ve kullanılacak algoritmalar güncel mevzuat ve standartlarla uyumlu olacak şekilde yapılır. Aynı şekilde üretilen anahtar çiftinin ömrü güncel mevzuat, standartlar ve anahtarların kriptografik güvenlik süresiyle sınırlandırılmıştır. Bir kök veya alt kök sertifikasının geçerlilik süresi sonundan yeterince makul bir süre önce yeni bir anahtar çifti ve sertifika üretilerek hizmetin kesintisiz bir biçimde devam etmesi sağlanır.

TÜRKTRUST donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri ilgili prosedürlere göre alınır ve saklanır. Böylece fiziksel ve ekonomik ömrünü tamamlamış bir modülün içindeki anahtarlar Bölüm 6.2.10'da belirtildiği gibi yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır.

TBB NES alt kök sertifikaları anahtar çiftlerinin üretimi, TBB tesisindeki üretim merkezinde yer alan donanım güvenlik modülü kullanılarak gerçekleştirilir. Üretilen açık anahtar, PKCS#10 standardında, gizli anahtar tarafından imzalanmış bir elektronik dosya ile çevrimdışı medya kullanılarak TÜRKTRUST sertifika merkezine getirilir ve TBB NES alt kök sertifikasının üretimi gerçekleştirilir. Üretilen TBB NES alt kök sertifikası TBB üretim merkezi sistemine yüklenerek TBB NES'lerinin imzalanması işleminde kullanılabilir duruma getirilir. TBB tesisindeki donanım güvenlik modülü, TÜRKTRUST'ın diğer kök ve alt kök sertifika anahtarlarını tutan donanım güvenlik modülleriyle aynı güvenlik düzeyinde bulunur.

Sunucu sertifikaları için başvuruda bulunan sunucu sorumluları ve NİMS başvurunda bulunan teknik yöneticiler, güvenli bir şekilde anahtar üretiminin yürütülmesinden sorumludur.

6.1.2. İmza Oluşturma Verisinin Sertifika Sahibine Ulaştırılması

NES 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.

Mobil imza kullanım amaçlı NES başvurularında, anahtar çifti hat kullanıcısının SIM kartında üretilir ve imza doğrulama verisi sertifika üretimi için mobil imza hizmet altyapısı üzerinden TÜRKTRUST'a ulaştırılır.

Anahtar çiftini kendisi üreten NES başvurusu sahipleri, bir güvenli elektronik imza oluşturma aracı kullanmaktan kendileri sorumludur.

SSL, EV SSL ve NİMS başvurusunda bulunacak sertifika başvuru sahibi, sertifika başvurusu sırasında anahtar üretiminin güvenli yapılmasından sorumludur.

Anahtar çifti TÜRKTRUST tarafından oluşturulan NES 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 şifresi zarfı da kurye ile kimlik kontrolü ve imza karşılığında sertifika sahibine teslim edilir. Şifre zarfı yerine aktivasyon uygulaması olan hallerde bu gönderim gerçekleşmez.

"eksprEs-İmza" uygulaması kapsamında imza oluşturma ve doğrulama veri çiftleri önceden TÜRKTRUST merkezinde üretilir; imza oluşturma verileri ön tanımlı olarak ilgili güvenli elektronik imza oluşturma araçları üzerinde TÜRKTRUST yerel ofislerine gönderilir. Sertifika üretimi sonrası ilgili ofiste sertifika başvuru sahibinin güvenli elektronik imza oluşturma aracına yüklenen sertifika, varsa şifre zarfıyla birlikte sertifika sahibine kimlik kontrolü ve imza karşılığında TÜRKTRUST yetkilisi tarafından teslim edilir.

Mobil imza kullanım amaçlı NES'de imza oluşturma verisi hat kullanıcısının SIM kartında üretilir.

6.1.3. İmza Doğrulama Verisinin ESHS'ye Ulaştırılması

Anahtar üretiminin sertifika başvuru sahibi tarafından gerçekleştirildiği durumlarda, sertifika talebinin gizli anahtarla imzalanmış olması şarttır. 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 2048 bit RSA anahtar çiftleri kullanılır.

TÜRKTRUST tarafından üretilen tüm son kullanıcı sertifikaları için 2048 bit RSA anahtar çifti kullanılır.

TÜRKTRUST tarafından üretilen sertifikalarda kullanılan özetleme algoritmaları hakkında bilgi, Bölüm 7.1.3'te verilmiştir.

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. Ancak bu durumda TÜRKTRUST, müşteri tarafından gönderilen CSR dosyasının geçerliliğini, dosyanın imzasının yanında, kullanılan anahtar uzunluğuna ve diğer parametrelere göre doğrular. CSR dosyalarının bilinen zayıf anahtarlardan biriyle oluşturulup oluşturulmadığı otomatik olarak kontrol edilir ve zayıf anahtar bulunması halinde başvuru reddedilir.

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.

TÜRKTRUST OCSP hizmet sertifikalarına ait anahtarlar, OCSP sunucularına gelen sorgulara karşılık üretilen OCSP cevaplarını 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. Satınalma sonrası donanım güvenlik modülünün ilk kullanımından önce, sevkiyat ve depolama sırasında cihazların zarar görmediğinden emin olmak için kontroller uygulanır. Cihazların kabulü sırasında fabrika paketlemesi ve güvenlik mühürleri kontrol edilir ve cihazlar fiziksel ve teknik bakımdan güvenliği sağlanmış alanlarda saklanır ve kullanılır. Cihazların tüm kullanım ömürleri boyunca, cihazlar işlevsellikleriyle ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu bilgi güvenliği ihlal olayı prosedürü uyarınca yönetilir.

NES 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 Kullanıcılı 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, hiçbir yetkilinin tek başına TÜRKTRUST imza oluşturma verilerini kullanabilmesine izin vermez.

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

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.

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 NES 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.

NES 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.

6.2.8. Gizli Anahtarın Aktive Edilme Yöntemi

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

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

SSL, EV SSL ve NİMS sertifikaları için gizli anahtarın aktivasyonu sertifika sahibine ait yazılım veya donanım üzerinde yapılır.

Sertifika sahibi aktivasyon verisinin diğer kişilerce izinsiz kullanımını, verinin çalınmasını veya kaybolmasını önlemek üzere gerekli tedbirleri almaktan sorumludur.

6.2.9. Gizli Anahtarın Deaktive Edilme Yöntemi

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

NES'e bağlı imza oluşturma verileri güvenli elektronik imza oluşturma aracı üzerinde şifre girişiyle belirli bir süre için aktive edilir ve işlem süresi 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.

SSL, EV SSL ve NİMS sertifikaları için gizli anahtarın deaktive edilmesi sertifika sahibine ait yazılım veya donanım üzerinde yapılır.

6.2.10. Gizli Anahtarı Yok Etme Metodu

TÜRKTRUST sertifika üretim merkezlerinin kök ve alt kök sertifikalarına bağlı imza oluşturma verilerinin tüm kopyaları, sertifika geçerlilik süreleri sonunda, içinde bulundukları donanım güvenlik modüllerinin anahtar silme özelliği kullanılarak sadece yetkili kişiler tarafından yok edilir ve yapılan işlemler prosedürler uyarınca kayıt altına alınır. Bu işlem için en az iki kişinin aynı anda hazır bulunması gerekir.

NES'e bağlı olan ve güvenli elektronik imza oluşturma aracı içinde saklanan imza oluşturma verileri, imza oluşturma verilerinin silinmesiyle veya donanımın imha edilmesiyle yok edilebilir.

SSL, EV SSL ve NİMS son kullanıcı sertifikalarına ait gizli anahtarların sertifika iptali ya da sertifika süresinin dolmasından sonra yok edilmesiyle ilgili bir koşul yoktur. Sertifika sahibi isteği halinde gizli anahtarı 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.

NES 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 NES'lerin, SSL sertifikalarının ve NİMS'lerin geçerlilik süreleri 1 (bir), 2 (iki) veya 3 (üç) yıldır. Anahtarların kriptografik güvenliği bakımından, aynı içerikle bir sertifikanın toplam geçerlilik süresi 3 yıldan fazla olamaz.

TÜRKTRUST EV SSL sertifikalarının geçerlilik süreleri ise 1 (bir) yıl, 2 (iki) yıl veya en çok 27 (yirmiyedi) ay olabilir.

TÜRKTRUST'a ait kök ve alt kök sertifikaların 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

Erişim şifresi, gizli anahtar yönetiminde kullanılan parola, şifre, PIN ya da benzeri özel verilere karşılık gelir.

TÜRKTRUST alt kök ve kök sertifikalarına ait anahtarların üretimi ve bu anahtarlara ait erişim şifrelerinin oluşturulması, Kök ve Alt Kök Sertifika Üretim Yayımlama ve İmha Prosedürü'nde açıklanan törene göre yapılır. Bölüm 6.2.2'de açıklandığı gibi kök ve alt kök sertifikaların gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip iki yetkilinin aynı anda bulunmasıyla mümkündür.

NES sahiplerinin imza oluşturma verilerine ait erişim şifreleri şifre zarfı veya aktivasyon yöntemiyle kendilerine iletilir. Şifre zarfı yönteminde, erişim şifresi üretilir. Aktivasyon yönteminde, benzer biçimde sertifika üretim aşamasında bir erişim şifresi üretilir. Aynı işlem sırasında sertifika ve sertifikanın yazıldığı karta bağlı aktivasyon kodu da üretilir ve şifrelenerek veri tabanına kaydedilir.

Aktivasyon kodunun üretilme yöntemi, sertifika ve akıllı kart ile bir araya geldiğinde erişim şifresini yeniden oluşturucak biçimde tasarlanmıştır. TÜRKTRUST NES sahipleri için erişim şifrelerini oluştururken aşağıdaki güvenlik kurallara uyulmasını kuvvetle tavsiye eder:

- En az 6 (altı) karakter kullanılması,
- Bir karakterin fazla sayıda tekrar etmemesi,
- Doğum günü, isim ve benzeri tahmin edilmesini kolaylaştıran verilerin kullanılmaması.

TÜRKTRUST, sertifika sahiplerine en geç 6 (altı) ayda bir erişim şifrelerini değiştirmelerini ve öncekilerden farklı yeni bir şifre belirlemelerini önerir.

SSL, EV SSL ve NİMS sertifika sahipleri sertifikalarına ait anahtarlara erişim şifrelerini güvenli biçimde oluşturmaktan ve korumaktan sorumludur.

6.4.2. Erişim Şifrelerinin Korunması

TÜRKTRUST kök ve alt kök sertifikalarına ait gizli anahtarları kullanan yetkili kişiler, erişim şifrelerini en geç 90 (doksan) günde bir değiştirirler. Yetkili kişiler, erişim şifrelerinin gizliliğinden ve korunmasından sorumludur.

TÜRKTRUST sertifika sahipleri gizli anahtarlarına ait erişim şifrelerini yukarıda belirtilen tavsiyelere uygun şekilde belirlemek ve korumaktan sorumludur.

6.4.3. Erişim Şifreleriyle İlgili Diğer Konular

TÜRKTRUST sertifika hizmetleri kapsamında sadece NES sahiplerinin PIN'leri taşınmaktadır. Bu taşınmanın şifre zarfıyla olması halinde, sözleşmeye bağlı güvenli kurye hizmeti alınır. Güvenli kurye sadece sertifika sahibine elden imza karşılığı teslimat yapar. Sertifikanın bulunduğu kart ile şifre zarfı birbirini izleyen iki ayrı günde gönderilerek diğer kişilerin aynı anda eline geçmesi konusunda tedbir alınır.

NES aktivasyon yönteminde erişim şifresi elektronik veya fiziksel hiçbir biçimde taşınmaz. NES aktivasyon kodu TÜRKTRUST veri tabanında şifrelenmiş halde tutulur ve herhangi bir kullanıcının erişimine kapalıdır. NES aktivasyon kodunun veri tabanından deşifre edilerek çıkması ancak sertifika sahibinin kartını bilgisayarına takması ve TÜRKTRUST yazılımı

içinden aktivasyon talep etmesiyle mümkündür. Bu durumda bile sertifika sahibinin bilgisayarıyla TÜRKTRUST sunucusu arasında şifreli haberleşme yapılır. Böylece sertifika sahibine teslim edilmek üzere gönderilen kartın erişim şifresi güvenliği, kartın yaşam döngüsü içinde herhangi bir andan daha az değildir.

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, virüslere, kötü niyetli ve yetkisiz yazılımlara karşı korunmaktadır.
- Bilgisayar sistemleri ağ güvenliği saldırılarına karşı korunmaktadır.
- Bilgisayar sistemlerine erişim hakları ve kimlik doğrulama, TÜRKTRUST personeline verilen şifrelerle sağlanmaktadır.
- Bilgisayarlara erişim hakları, yetkili personele tanımlanan rollerle sınırlanmıştır.
- Özellikle, sertifika kaydı, üretimi, askıya alma, iptali gibi sertifika hizmetlerine özgü tüm işlemler veri tabanında kaydedilir. Veri tabanına yetkisiz erişimi ve istenmeden yapılan değişiklikleri önlemek için kimlik doğrulamanın farklı erişim seviyelerinde çeşitli fiziksel ve elektronik önlemler alınır. Veri tabanı seviyesindeki mantıksal tutarlılık, aksi halde geri dönüşü olmayan sonuçlar doğurabilecek iptal durumu değişikliklerini önlemek için ilave bir güvenlik katmanı oluşturur.
- 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.
- TÜRKTRUST, değişikliklere karşı korunmuş güvenilir sistemler ve ürünler kullanır. Bu bağlamda, Bilgi Teknolojileri ve İletişim Kurumu'nun sürekli denetimi altında, CWA 14167-1 standardının önerileri kesin olarak uygulanır.

6.5.2. Bilgisayar Güvenliğinin Derecelendirilmesi

Uygulama dışıdır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirme kontrolleri, geliştirme tesisi güvenliği (tesis güvenlik belgeleri aracılığıyla), geliştirme ortamı güvenliği, geliştirme personeli güvenliği, ürün bakımı sırasında konfigürasyon yönetimi güvenliği ve yazılım geliştirme metodolojisi (ISO/IEC 27001 ve ISO 9001 belgeleri aracılığıyla) için uygulanır. Bu konular ve değişim yönetimi hakkındaki ayrıntılar, Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedüründe dokümante edilmiştir.

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 sertifika kayıt merkezleri, sertifika işlemlerine ilişkin kayıtları güvenli ağ bağlantısıyla, internet üzerinden TÜRKTRUST'a 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 dokümanının bu kısmında, TÜRKTRUST tarafından üretilen sertifikalar ile SİL'lerin profilleri ve verilen OCSP hizmetinin yapısı yer almaktadır.

7.1. Sertifika Profili

TÜRKTRUST sertifikaları genel olarak "ISO/IEC 9594-8/ ITU-T Recommendation X.509: "Information Technology- Open Systems Interconnection- The Directory: Public –key and attribute certificate frameworks" ile "IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanlarına uygundur. Ayrıca, TÜRKTRUST tarafından oluşturulan NES'ler Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

TÜRKTRUST sertifikalarında temel olarak aşağıdaki alanlar bulunur:

Alan Adı	Açıklama
Seri No	(Aynı sertifika veren için) Eşsiz numara
İmza Algoritması	Nesne tanımlayıcı numarası (Bkz. 7.1.3)
Sertifikayı Veren	Bkz. 7.1.4
Geçerlilik Başlangıcı	RFC 5280'e göre kodlanmış UTC zamanı
Geçerlilik Sonu	RFC 5280'e göre kodlanmış UTC zamanı
Özne	Bkz. 7.1.4
Açık Anahtar	RFC 5280'e göre kodlanmış anahtar değeri
İmza	RFC 5280'e göre kodlanmış imza değeri

TÜRKTRUST NES "Sertifika İlkeleri" alanı içinde Kanun gereği, "Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır." ibaresi zorunlu olarak yer alır.

7.1.1. Sürüm Numaraları

TÜRKTRUST tarafından oluşturulan kök ve alt kök sertifikalar ile son kullanıcı sertifikaları, "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" 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, yetkili anahtar tanımlayıcısı (authority key identifier), özne anahtar tanımlayıcısı (subject key identifier), anahtar kullanımı (key usage), sertifika ilkeleri (certificate policies), temel kısıtlar (basic constraints), özne alternatif adı (subject alternative name), SİL dağıtım noktaları (CRL distribution points), genişletilmiş anahtar kullanımı (extended key usage) uzantıları uygun biçimde ayarlanır.

NES'ler, "IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile" ve "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanları uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.

7.1.3. Algoritma Nesne Tanımlayıcıları

TÜRKTRUST tarafından oluşturulan tüm sertifikaların imzalanmasında aşağıdaki algoritmalardan biri kullanılır.

Algoritma Adı	Nesne Tanımlayıcı Numarası
SHA-1 with RSA	1.2.840.113549.1.1.5
SHA-256 with RSA	1.2.840.113549.1.1.11
SHA-384 with RSA	1.2.840.113549.1.1.12
SHA-512 with RSA	1.2.840.113549.1.1.13

SSL, EV SSL ve NIMS için SHA-1 algoritması kullanımından, belirtilen diğer algoritmalardan en az bir tanesinin güncel elektronik imza uygulamalarının tamamında desteklendiğinin kesinleşmesi sonrasında vazgeçilecektir. NES için ilgili algoritmalar yasal düzenlemelerin gerektirdiği şekilde kullanılacaktır.

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 dokümanı 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 kullanabilir.

7.1.8. İlke Niteleyicilerinin Yazımı

TÜRKTRUST tarafından üretilen sertifikaların "sertifika ilkeleri" uzantısında, ilke niteleyicisi olarak SUE dokümanına 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. TÜRKTRUST tarafından yayımlanan SİL'ler Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.2.1. Sürüm Numarası

TÜRKTRUST tarafından oluşturulan SİL'ler, "IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" dokümanı uyarınca X.509 v2 sürümünü destekler.

7.2.2. SİL ve SİL Giriş Uzantıları

TÜRKTRUST tarafından yayımlanan SİL'lerde, RFC 5280 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. TÜRKTRUST tarafından verilen OCSP cevap mesajları, Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygundur.

7.3.1. Sürüm Numarası

TÜRKTRUST tarafından verilen OCSP hizmeti, "IETF RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" 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 e-imza mevzuatı gereğince Bilgi Teknolojileri ve İletişim Kurumu tarafından denetlenir. Bu denetimin yanı sıra, ETSI TS 102 042 standardı kapsamında da yetkili bir denetçi kurum tarafından SSL, EV SSL ve NİMS süreçleri denetime tabi tutulur.

Ayrıca, tüm ESHS süreçleri, bilgi güvenliği yönetim sisteminin sürekliliği açısından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi veTS EN ISO 9001 Kalite Yönetim Sistemi sertifikaları uyarınca periyodik olarak uygunluk denetimine tabi tutulur.

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

TÜRKTRUST, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemine göre risk değerlendirmelerini gerçekleştirir. Bunun sonucunda, iş riskleri değerlendirilir ve gerekli güvenlik koşulları ve işletim prosedürleri belirlenir. Risk analizi düzenli olarak gözden geçirilir ve gerektiğinde güncelleme yapılır.

8.1. Denetim Sıklığı ve Durumları

Bilgi Teknolojileri ve İletişim 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.

ETSI TS 102 042 denetim standardı kapsamında SSL, EV SSL ve NİMS hizmet süreçleri her yıl uygunluk denetimine tabi tutulur ve her üç yılda bir bu sertifikasyon yenilenir.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası uyarınca, her yıl takip denetiminden ve her üç yılda bir de belge yenileme denetiminden geçilir.

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

8.2. Denetçinin Kimliği ve Özellikleri

Bilgi Teknolojileri ve İletişim Kurumu, Kanunla belirlenmiş düzenleyici ve denetçi kurumdur.

ETSI 102 042 denetimi, aşağıdaki hususlara sahip olan yetkin bir denetçi tarafından gerçekleştirilir:

- Açık anahtarlı altyapı (PKI) teknolojisi, bilgi güvenliği araçları ve teknikleri, bilgi teknolojileri ve güvenliği denetimi ve üçüncü parti bağımsız raporlamaları alanında yetkinliğine sahip olmalıdır.
- Denetçi, European Cooperation for Accreditation gibi resmi bir akreditasyon kuruluşu tarafından ISO/IEC 17021'e uyumlu olduğuna dair akredite edilmiş olmalıdır.
- Denetçi ayrıca, CEN Workshop Agreement (CWA) 14172-2 standardının 3.4 maddesi uyarınca da akredite edilmiş olmalıdır.

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

TÜRKTRUST'ın kurumsal iç 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 NES ile ilgili faaliyet gösteren tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kuruluştur.

ETSI TS 102 042 denetimi, bağımsız ve yetkili bir denetçi tarafından yapılır.

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.

ETSI TS 102 042 denetimi, SSL, EV SSL ve NİMS hizmetlerine ilişkin tüm süreçleri, bu hizmetlerin yerine getirilmesi sırasında kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri içermektedir.

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.

SSL, EV SSL ve NİMS süreçlerinin ETSI TS 102 042 standardına uyumu kapsamında gerçekleştirilen denetimlerde ortaya çıkan minör eksiklikler için TÜRKTRUST, düzeltici ve önleyici faaliyetleri belirler ve gerekli işlemleri yerine getirir. Eksiklerin major nitelikte olması, geçerli olan yetkilendirme belgesinin geri alınmasına neden olur.

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.

Bağımsız denetim firması tarafından ETSI TS 102 042 uyarınca gerçekleştirilen SSL, EV SSL ve NİMS süreçleri denetim sonuçları resmi olarak TÜRKTRUST'a bildirilir.

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 dokümanının 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.

NES, geçerlilik sürelerine göre ve 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.

SSL ve EV SSL sertifikaları ile NİMS, sertifika çeşidine, kullanım süresine ve özelliklerine bağlı olarak fiyatlandırılır. Ayrıca, SSL ve EV SSL sertifikası fiyatlandırmasında artan maddi işlem sınırı, genel sorumluluk sigortası ve mesleki sorumluluk sigortası primleri de dikkate alınır.

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, NES iptal veya durum bilgisi erişim hizmetleri için ücret talep edilmez.

TÜRKTRUST'ın SSL ve EV SSL sertifikaları ile NİMS 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, NES, SSL, EV SSL ve NİMS hizmetlerinde bedel iadesi yapmaz. Ancak, TÜRKTRUST'tan kaynaklanan nedenlerle, sertifika içeriğinde başvurudan farklı verilerin bulunması durumunda, her hangi bir ücret talep edilmeden yeni bir sertifika verilir veya talep edilmesi durumunda bedel iadesi yapılır.

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.

TÜRKTRUST, SSL ve EV SSL hizmetleri için ETSI TS 102 042 standardı uyarınca ticari genel sorumluluk sigortası ve mesleki sorumluluk sigortası yaptırmakla yükümlüdür.

9.2.1. Sigorta Kapsamı

"Sertifika Mali Sorumluluk Sigortası Yönetmeliği" Madde 6 uyarınca, zorunlu 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 görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

NES'ler için yaptırılan sertifika mali sorumluluk sigortasına ek olarak SSL ve EV SSL sertifikaları, aşağıda özellikleri belirtilen ticari genel sorumluluk sigortası ve mesleki sorumluluk sigortası kapsamındadır.

"Ticari Genel Sorumluluk Sigortası (Commercial General Liability Insurance)", SSL ve EV SSL hizmetlerine doğrudan veya dolaylı bağlı olarak oluşabilecek her türlü zarara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar. "Mesleki Sorumluluk Sigortası (Professional Liability/Errors and Omissions Insurance)", SSL ve EV SSL hizmetlerine bağlı olarak TÜRKTRUST'ın mesleki faaliyeti çerçevesinde oluşabilecek zarara karşı doğacak hukuki sorumlulukların teminat altına alınmasını içerir.

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, NES'leri sertifika sahiplerine teslim etmeden önce sertifika malî sorumluluk sigortası yaptırmakla yükümlüdür.

Ayrıca TÜRKTRUST, SSL ve EV SSL sertifikaları için ETSI TS 102 042 standardı uyarınca ticari genel sorumluluk sigortası ve mesleki sorumluluk sigortasını 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 dokümanı, SUE dokümanı, sertifika sahibi ve sertifika hizmetleri taahhütnameleri 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 katılımcılara 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 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

TÜRKTRUST, Sİ ve SUE dokümanında ve sertifika sahibi sözleşmesi veya taahhütnamesinde düzenlenmiş amaçlar için sertifikayı, mührü veya sertifika başvurusunda sağlanmış bilgi içeriğini kullanabilir.

9.4.6. Yargısal ve İdari Süreçlere Uygun Olarak Bilginin Açıklanması

Hukuki veya idari süreçler gereği ihtiyaç duyulan sertifika sahibinin özel bilgileri, sadece talep sahibi resmi makama veya sertifika sahibinin kendisine 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 Beyan ve Garantileri

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.

SSL ve EV SSL sertifikaları bağlamında, TÜRKTRUST aşağıdakileri garanti eder:

- Yasal Varlık: TÜRKTRUST, SSL ve EV SSL sertifikasının üretildiği tarihte, SSL ve EV SSL sertifikası içinde belirtilen Özne'nin yasal olarak var olduğunu ve geçerli bir organizasyon ya da varlık olduğunu teyit eder;
- Kimlik: TÜRKTRUST, SSL ve EV SSL sertifikasının üretildiği tarihte, SSL ve EV SSL sertifikası içinde belirtilen Özne'nin yasal adının, resmi devlet kayıtlarındaki isimle uyuştuğunu teyit eder;
- Alan Adı Kullanma Hakkı: TÜRKTRUST, SSL ve EV SSL sertifikasının üretildiği tarihte, SSL ve EV SSL sertifikası içinde belirtilen Özne'nin SSL ve EV SSL sertifikası içinde belirtilen tüm alan adlarını münhasıran kullanma hakkına sahip olduğunu doğrulamak için gerekli tüm adımları uygular;
- SSL ve EV SSL Sertifikası için Yetkilendirme: TÜRKTRUST, SSL ve EV SSL sertifikası içinde belirtilen Özne'nin, SSL ve EV SSL sertifikasının üretimini yetkilendirdiğini doğrulamak için gerekli tüm adımları uygular;
- Bilginin Doğruluğu: TÜRKTRUST, SSL ve EV SSL sertifikasının üretildiği tarihte, SSL ve EV SSL sertifikası içinde yer alan diğer tüm bilgilerin doğru olduğunu teyit etmek için gerekli tüm adımları uygular;
- ***Yanıltıcı Bilgi Olmaması:*** TÜRKTRUST, SSL ve EV SSL sertifikasının üretildiği tarihte, SSL ve EV SSL sertifikası içinde yer alan bilgilerde herhangi bir yanıltıcı bilgi bulunmaması için SUE'de açıklanan doğrulama adımlarını prosedür ve talimatlarında detaylı şekilde uygular;
- Taahhütname: SSL ve EV SSL sertifikasında belirtilen Özne, TÜRKTRUST ile SUE'nin gerekliliklerini sağlayan, yasal olarak geçerli ve bağlayıcı bir taahhütname imzalamıştır veya başvuru sahibinin temsilcisi ilgili şartları onaylamış ve kabul etmiştir;
- Durum: TÜRKTRUST bu SUE dokümanının gerekliliklerini sağlar ve SSL ve EV SSL sertifikalarının durumuyla ilgili geçerli ya da iptal şeklinde güncel bilgileri içeren bir Bilgi Deposunu 24 x 7 olarak online erişime açık biçimde idame ettirecektir.
- İptal: TÜRKTRUST bu SUE dokümanının gerekliliklerini sağlar ve CA-Browser Forum kılavuzunda belirtilen iptal nedenleri gereği SSL ve EV SSL sertifikasının iptalini gerçekleştirir.

Özellikle, aşağıda belirtilen EV SSL sertifikası taraflarına, bu bölümde belirtilen garantiler uygulanır:

- EV SSL sertifikası için sertifika sahibi sözleşmesi ya da taahhütnamesini imzalayan sertifika sahibi;
- EV SSL sertifikası içindeki Özne;

- ESHS'nin, uygulama yazılımı sağlayıcıları tarafından dağıtılan yazılımlara sertifikasının eklenmesi için sözleşme imzaladığı tüm uygulama yazılımı sağlayıcıları;
- Geçerlilik süresi boyunca, EV SSL sertifikasına güvenen tüm üçüncü kişileri.

TÜRKTRUST'a bağlı sertifika üretim merkezleri, NES verebilmek için, Kanun Madde 10 ve Yönetmelik Madde 14'te yer alan ESHS yükümlülüklerini, SSL, EV SSL ve NİMS hizmetlerini yürütebilmek için ETSI TS 102 042 standardında ve BR'da belirtilen yükümlülükleri yerine getirir.

9.6.2. Kayıt Merkezi Sorumlulukları

TÜRKTRUST'a bağlı kayıt merkezleri, kendilerine başvuran gerçek veya tüzel kişilerin sertifika tiplerine göre işbu SUE dokümanında belirtilen 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 veya taahhütnamesinde yer alan tüm yükümlülüklerini yerine getireceğini garanti eder.

NES sahipleri, sertifika sahibi sözleşmesinde veya taahhütnamesinde yer alan koşullarla birlikte, Yönetmelik Madde 15'te yer alan yükümlülükleri de yerine getirmek zorundadır.

9.6.4. Üçüncü Kişilerin Sorumlulukları

Sertifika sahipleri ile üçüncü kişiler, TÜRKTRUST NES'lerine dayanılarak oluşturulmuş elektronik imzaların geçerliliğini doğrulamaktan kendileri sorumludur.

SSL, EV SSL ve NİMS sertifika sahipleri ile üçüncü kişiler, TÜRKTRUST tarafından oluşturulmuş sertifikaların kabulü sırasında ve bu sertifikalara güvenirken sertifikaların içeriğini doğrulamaktan sorumludur.

9.6.5. Diğer Katılımcıların Sorumlulukları

TÜRKTRUST'ın sertifika hizmetlerini verirken işbirliği yaptığı ve hizmet aldığı tüm kişi ve kuruluşlardan oluşan diğer katılımcılar, 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.

NES'ler için zorunlu sertifika mali sorumluluk sigortası, 10.000 TL tutarında olay başına teminat limitini ve 1.000.000 TL tutarında yıllık azami teminat limitini kapsar.

SSL'ler için sertifika mali sorumluluk sigortası, 10.000 TL tutarında olay başına teminat limitini ve 1.000.000 TL tutarında yıllık azami teminat limitini kapsar. SSL ve EV SSL sertifikalarında, genel sorumluluk sigortası 2.000.000 USD tutarında olay başına teminat limitini ve yıllık azami teminat limitini, mesleki sorumluluk sigortasıysa 5.000.000 USD tutarında olay başına teminat limitini ve yıllık azami teminat limitini kapsar

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

9.10. Sİ dokümanının Geçerliliği

9.10.1. Sİ dokümanının Geçerlilik Dönemi

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

9.10.2. Sİ dokümanının Geçerliliğinin Sona Ermesi

TÜRKTRUST faaliyetlerinde ve sertifika hizmetlerinde oluşabilecek değişikliklere ve düzenlemelere bağlı olarak, Sİ dokümanının 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 dokümanı 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. Taraflara Özel Duyurular ve İletişim

TÜRKTRUST tarafından sertifika sahiplerine yapılacak olan kişisel duyurular için sertifika sahiplerinin uygun olan iletişim bilgileri kullanılır.

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 dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir Sİ dokümanı sürümü TÜRKTRUST tarafından hazırlanır ve TÜRKTRUST Yönetim Kurulu'nun onayının ardından yayımlanır.

Sİ dokümanında, önceden üretilmiş olan sertifikaların kullanımını ve kabul edilirliğini 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 dokümanının mevcut sürümünün içeriğinin değişmesini gerektiren herhangi bir durum ortaya çıktığında, ilgili değişikliklerin yansıtıldığı yeni bir Sİ dokümanı sürümü TÜRKTRUST tarafından hazırlanır ve yayımlanır.

Sİ ve SUE dokümanında yer alan ilgili ilkeler ve uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir.

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 dokümanına erişim bilgisi aynı kalır, ama bu adresin işaret ettiği SUE dokümanı 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 edilirliği bazı uygulamalarda etkilenebileceğinden, TÜRKTRUST sertifika sahipleri ile üçüncü kişileri bilgilendirebilmek için tüm makul imkanları kullanır.

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 edilirliğini doğrudan etkileyebilecek olan, kullanılan kimlik doğrulama adımlarını önemli ölçüde etkileyen veya sertifika hizmetlerinde sertifikanın güvenlik düzeyine etki edebilecek biçimde gerçekleşen önemli değişiklikler, Sİ dokümanında 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 çözümlenmesine 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 Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler uyarınca düzenlenir. Kurum ESHS'lerin Kanun uyarınca işleyişinin düzenlenmesi ve denetlenmesinden sorumludur.

9.15. İlgili Yasalara Uygunluk

TÜRKTRUST, NES hizmetlerini 5070 sayılı "Elektronik İmza Kanunu" ve Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanmış Yönetmelik ve Tebliğler ile diğer ilgili düzenlemeler 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.