



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu	Yayın Numarası	Yayın Tarihi
YONG-001-007	11	20.10.2015

**NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA
ESASLARI****DEĞİŐİKLİK KAYITLARI**

Yayın No	Yayın Nedeni	Yayın Tarihi
01	İlk yayın	28.03.2005
02	RFC 3647 tam uyumluluđu için yeniden düzenleme yapıldı.	06.06.2005
03	Sİ ve SUE yayın adresleri ve tarihleri düzenlendi.	15.11.2005
04	Sertifika yönetim süreçlerinde deđişiklik yapıldı. Kurum logosunda deđişiklik yapıldı. NES Taahhütnamesi'ni yönetim süreçlerine eklendi.	13.02.2007
05	Planlı gözden geçirme sonrası küçük deđişiklikler yapıldı.	07.05.2008
06	BTK denetimi sonrası, kapsamlı bir güncelleme yapıldı.	05.10.2009
07	Sertifikaların askıya alınması ve kullanıma açılması ile ilgili hususlar tekrar düzenlendi.	30.12.2010
08	NES Temini Sözleşmesi süreçlerden kaldırıldı. Kurum, Kurum yetkilisi ve gözetmen rolleri ve sorumlulukları eklendi. Sertifika yenileme süreçleri yeniden düzenlendi.	25.01.2012
09	Kayıt Birimi ile ilgili eklemeler yapıldı. Sistem bileşenleri güncellendi. Anahtarların KSM dışında üretilmesi ile ilgili süreç eklendi. KSM'deki roller güncellendi.	11.01.2013
10	NES için SİL yayımlama sıklığı 4 saat olarak deđiştirildi. Kullanılan özet algoritmalarında mevzuat geređi yapılan deđişiklikler dokümana yansıtıldı. Kayıtçı hizmeti politikalardan kaldırıldı.	28.08.2013
11	Gözetmen rolü çıkarıldı. Doküman genelinde düzenlemeler yapıldı. Adresler yeni sertifikalara göre düzenlendi.	20.10.2015



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

TABLolar

Tablo 1 NES Uzantıları	48
Tablo 2 NES İsim Alanı Bilgileri	50



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

İÇİNDEKİLER

1. Giriş	10
1.1. Genel Bakış	10
1.2. Doküman Adı ve Tanımı	11
1.3. Sistem Bileşenleri	11
1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı	11
1.3.2. Kayıt Birimleri	11
1.3.3. Sertifika Sahipleri	11
1.3.4. Üçüncü Kişiler	11
1.3.5. Diğer Bileşenler	11
1.4. Sertifika Kullanımı	12
1.4.1. Uygun Olan Sertifika Kullanımı	12
1.4.2. Sertifika Kullanımının Sınırları	12
1.5. Uygulama Esaslarının Yönetimi	12
1.5.1. Doküman Yönetimi	12
1.5.2. İletişim Bilgileri	12
1.5.3. Sertifika Uygulama Esaslarının İlgelere Uygunluğunu Belirleyen Kişi	13
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri	13
1.6. Tanımlar ve Kısaltmalar	13
1.6.1. Tanımlar	13
1.6.2. Kısaltmalar	14
2. Yayımlama ve Bilgi Deposu	16
2.1. Bilgi Depoları	16
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması	16
2.3. Yayımlama Sıklığı ve Zamanı	16
2.4. Erişim Kontrolleri	16
3. Kimlik Belirleme ve Doğrulama	18
3.1. İsimlendirme	18
3.1.1. İsim Alanı Tipleri	18
3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması	18
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması	18
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması	18
3.1.5. Kimlik Bilgilerinin Tekilliği	18
3.1.6. Markanın Tanınması, Doğrulaması ve Rolü	18
3.2. İlk Kimlik Belirleme	18
3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması	18
3.2.2. Kurumsal Kimliğin Belirlenmesi	19
3.2.3. Kişisel Kimliğin Belirlenmesi	19
3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri	19
3.2.5. Yetkinin Doğrulaması	19
3.2.6. Uyum Kriterleri	19
3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama	20

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama	20
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama	20
3.4. Sertifika İptal İsteğinde Kimlik Doğrulama	20
4. İşlemsel Gereker	21
4.1. Sertifika Başvurusu	21
4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği.....	21
4.1.2. Kayıt İşlemleri ve Sorumluluklar.....	21
4.2. Sertifika Başvurusunun İşlenmesi	22
4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi.....	22
4.2.2. Sertifika Başvurusunun Kabul veya Reddi	22
4.2.3. Sertifika Başvurusunun İşlenme Zamanı.....	23
4.3. Sertifikanın Oluşturulması	23
4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri.....	23
4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi.....	24
4.4. Sertifikanın Kabulü	24
4.4.1. Sertifikanın Kabul Koşulu.....	24
4.4.2. Sertifikanın ESHS Tarafından Yayınlanması.....	24
4.4.3. Sertifikanın Oluşturulmasının Diğer Tarafra Duyurulması.....	24
4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı	24
4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı	24
4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı	24
4.6. Sertifika Süresinin Uzatılması.....	25
4.7. Sertifika Yenileme	25
4.7.1. Sertifikanın Yenileme Koşulları	25
4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği	25
4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi	25
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi.....	25
4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu.....	25
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması.....	25
4.7.7. Sertifika Yenilemenin Diğer Tarafra Duyurulması.....	25
4.8. Sertifikada Bilgi Değişikliği	26
4.9. Sertifikanın İptali ve Askıya Alınması.....	26
4.9.1. Sertifikanın İptal Edildiği Durumlar	26
4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir	26
4.9.3. Sertifika İptal Başvurusunun İşlenmesi	27
4.9.4. İptal İsteği Ertelenme Süresi.....	27
4.9.5. İptal İsteğinin İşlenme Süresi.....	27
4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği	28
4.9.7. Sertifika İptal Listesi Yayınlama Sıklığı	28
4.9.8. Sertifika İptal Listesi Yayınlama Gecikme Süresi	28
4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti.....	28
4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi.....	28
4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri	28

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.9.12.	İmza oluŐturma Verisinin GüvenliĐini Yitirmesi Durumu	29
4.9.13.	Sertifikanın Askıya AlındıĐı Durumlar	29
4.9.14.	Sertifika Askıya Alma BaŐvurusunu Kimlerin YapabildiĐi	29
4.9.15.	Sertifika Askıya Alma BaŐvurusunun İŐlenmesi	29
4.9.16.	Askıda Kalma Suresi	29
4.10.	Sertifika Durum Servisleri	29
4.10.1.	İŐletimsel Özellikleri	29
4.10.2.	Servisin EriŐilebilirliĐi	30
4.10.3.	İsteĐe BaĐlı Özellikler	30
4.11.	Sertifika SahipliĐinin Sona Ermesi	30
4.12.	Anahtar Yeniden Üretme	30
5.	Yönetim, İŐlemsel ve Fiziksel Kontroller	31
5.1.	Fiziksel Güvenlik Denetimleri	31
5.1.1.	Tesis Yeri ve İnŐaatı	31
5.1.2.	Fiziksel EriŐim	31
5.1.3.	Güç KaynaĐı ve Havalandırma	31
5.1.4.	Su Baskınları	31
5.1.5.	Yangın Önleme ve Korunma	32
5.1.6.	Saklama ve Yedekleme Ortamlarının Korunması	32
5.1.7.	Atıkların Yok Edilmesi	32
5.1.8.	Farklı Mekanlarda Yedekleme	32
5.2.	Prosedürel Kontroller	32
5.2.1.	Güvenilir Roller	32
5.2.2.	Her İŐlem İçin Gereken KiŐi Sayısı	32
5.2.3.	Kimlik Doğrulama ve Yetkilendirme	32
5.2.4.	Görevlerin Ayrılmasını Gerektiren Roller	33
5.3.	Personel Güvenlik Kontrolleri	33
5.3.1.	KiŐisel GeçmiŐ, Deneyim ve Nitelik Gerekleri	33
5.3.2.	GeçmiŐ AraŐtırması	33
5.3.3.	EĐitim Gerekleri	33
5.3.4.	Sürekli EĐitim Gerekleri ve SıklıĐı	33
5.3.5.	Görev DeĐiŐim SıklıĐı ve Sırası	33
5.3.6.	Yetkisiz Eylemlerin Cezalandırılması	33
5.3.7.	AnlaŐmalı Personel Gereksinimleri	34
5.3.8.	SaĐlanan Dokümantasyon	34
5.4.	Denetim Kayıtları	34
5.4.1.	Kaydedilen İŐlemler	34
5.4.2.	Kayıtların İncelenme SıklıĐı	35
5.4.3.	Kayıtların Saklanma Suresi	35
5.4.4.	Kayıtların Korunması	35
5.4.5.	Kayıtların Yedeklenmesi	35
5.4.6.	Kayıtların Toplanması	36
5.4.7.	Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi	36
5.4.8.	Saldırıya AçıklıĐın DeĐerlendirilmesi	36

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5.5. Kayıt Arşivleme	36
5.5.1. Arşivlenen Kayıt Bilgileri	36
5.5.2. Arşivlerin Tutulma Süresi	36
5.5.3. Arşivlerin Korunması	37
5.5.4. Arşivlerin Yedeklenmesi	37
5.5.5. Kayıtların Zaman Damgası Gereksinimleri	37
5.5.6. Arşivlerin Toplanması	37
5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu	37
5.6. Anahtar Değişimi	37
5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	37
5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi	37
5.7.2. Donanım, Yazılım veya Veri Bozulması	38
5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi	38
5.7.4. Arıza Sonrası Yeniden Çalışırılık	38
5.8. Sertifika Hizmetlerinin Sonlandırılması	38
6. Teknik Güvenlik Kontrolleri	40
6.1. Anahtar Çifti Üretimi ve Kurulumu	40
6.1.1. Anahtar Çifti Üretimi	40
6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması	40
6.1.3. Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması	41
6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması	41
6.1.5. Anahtar Uzunlukları	41
6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü	41
6.1.7. Anahtar Kullanım Amaçları	42
6.2. İmza Oluşturma Verisinin Korunması	42
6.2.1. Kriptografik Modül Standartları	42
6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim	43
6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi	43
6.2.4. İmza Oluşturma Verisinin Yedeklenmesi	43
6.2.5. İmza Oluşturma Verisinin Arşivlenmesi	43
6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi	43
6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması	43
6.2.8. İmza Oluşturma Verisine Erişim	43
6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi	44
6.2.10. İmza Oluşturma Verisinin Yok Edilmesi	44
6.2.11. Kriptografik Modülün Değerlendirilmesi	44
6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular	44
6.3.1. İmza Doğrulama Verisinin Arşivlenmesi	44
6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri	44
6.4. Erişim Denetim Verileri	45
6.4.1. Erişim Denetim Verilerinin Oluşturulması	45
6.4.2. Erişim Denetim Verilerinin Korunması	45

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

6.4.3. Eriřim Denetim Verileri İle İlgili Diđer Konular.....	45
6.5. Bilgisayar Güvenliđi Denetimleri.....	45
6.5.1. Bilgisayar Güvenliđi İle İlgili Teknik Gereker.....	45
6.5.2. Bilgisayar Sisteminin Sađladığı Güvenlik Seviyesi.....	45
6.6. Yařam Döngüsü Teknik Denetimleri	46
6.6.1. Sistem Geliřtirme Denetimleri.....	46
6.6.2. Güvenlik Yönetimi Denetimleri.....	46
6.6.3. Yařam Döngüsü Güvenlik Denetimleri.....	46
6.7. Ađ Güvenliđi Denetimleri.....	46
6.8. Zaman Damgası.....	47
7. Sertifika ve Sertifika İptal Listesi Biçimleri	48
7.1. Sertifika Biçimi.....	48
7.1.1. Sürüm Numarası	48
7.1.2. Sertifika Uzantıları	48
7.1.3. Algoritma ve Nesne Tanımlayıcılar	49
7.1.4. İsim Alanı Biçimleri	49
7.1.5. İsim Kısıtları.....	50
7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası	50
7.1.7. İlke Kısıtları Uzantısının Kullanımı	50
7.1.8. İlke Niteleyiciler.....	50
7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi.....	51
7.2. Sertifika İptal Listesi Biçimi.....	51
7.2.1. Sürüm Numarası	51
7.2.2. Sertifika İptal Listesi Uzantıları.....	51
7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi	51
7.3.1. Sürüm Numarası	51
7.3.2. ÇİSDUP Uzantıları.....	51
8. Uygunluk Denetimleri	53
8.1. Uygunluk Denetiminin Sıklığı.....	53
8.2. Denetçinin Nitelikleri.....	53
8.3. Denetçinin Denetlenen Tarafı Olan İliřkisi	53
8.4. Denetimin Kapsamı.....	53
8.5. Yetersizliđin Tespiti Durumunda Yapılacaklar	53
8.6. Sonucun Bildirilmesi.....	54
9. Diđer İşler ve Hukuksal Meseleler.....	55
9.1. Ücretlendirme.....	55
9.1.1. Sertifika Oluřturma ve Yenileme Ücreti.....	55
9.1.2. Sertifika Eriřim Ücreti	55
9.1.3. İptal Durum Kaydına Eriřim Ücreti	55
9.1.4. Diđer Servis Ücretleri.....	55
9.1.5. İade Ücreti.....	55
9.2. Finansal Sorumluluk.....	55

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

9.2.1. Sigorta Kapsamı	55
9.2.2. Diğer Varlıklar	56
9.2.3. Sertifika Mali Sorumluluk Sigortası	56
9.3. Ticari Bilginin Korunması	56
9.3.1. Gizli Bilginin Kapsamı	56
9.3.2. Gizlilik Kapsamında Olmayan Bilgiler	56
9.3.3. Gizli Bilginin Korunma Sorumluluđu	56
9.4. Kişisel Bilginin Gizliliđi	56
9.4.1. Gizlilik Planı	56
9.4.2. Gizli Olarak Tanımlanan Bilgiler	56
9.4.3. Gizli Olarak Tanımlanmayan Bilgiler	56
9.4.4. Gizli Bilginin Korunma Sorumluluđu	56
9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi	57
9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması	57
9.4.7. Diğer Başlıklar	57
9.5. Telif Hakları	57
9.6. Temsil Hakkı ve Yükümlölükler	57
9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlölükleri	57
9.6.2. Kayıt Birimi Yükümlölükleri	58
9.6.3. Sertifika Sahibinin Yükümlölükleri	58
9.6.4. Üçüncü Kişilerin Yükümlölükleri	59
9.6.5. Diğer Bileşenlerin Yükümlölükleri	60
9.7. Yükümlölüklerden Feragat	61
9.8. Sorumlulukla İlgili Sınırlamalar	61
9.9. Tazminat Halleri	61
9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi	61
9.10.1. Anlaşma Süresi	61
9.10.2. Anlaşmanın Sona Ermesi	61
9.10.3. Anlaşmanın Sona Ermesinin Etkileri	62
9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme	62
9.12. Deđişiklik Halleri	63
9.12.1. Deđişiklik Metodları	63
9.12.2. Bilgilendirme Mekanizması ve Sıklığı	63
9.12.3. Nesne Tanımlama Numarasının Deđişmesini Gerektiren Durumlar ..	63
9.13. Anlaşmazlık Halleri	63
9.14. Uygulanacak Hukuk	63
9.15. Uygulanabilir Yasalarla Uyum	63
9.16. Diğer Hükümler	63



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

1. Giriş

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

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

Kamu SM açık anahtar altyapısı mimarisi içinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı (Kök SHS) ile buna bağlı olarak çalışan Kamu Elektronik Sertifika Hizmet Sağlayıcısı (Kamu ESHS) bulunur. Kök SHS, sertifika sahipleri için sertifika üretmeyip, yürüttükleri görevler açısından özel niteliği haiz kamu kurum ve kuruluşları ile dileyen gerçek ve tüzel kişilerin kuracakları Elektronik Sertifika Hizmet Sağlayıcılarına kök sertifika hizmeti verir. Kamu ESHS, Kök SHS'nin imzasını taşıyan Elektronik Sertifika Hizmet Sağlayıcısı sertifikasına sahiptir. Kamu ESHS, Başbakanlığın 2004/21 sayılı Kamu Sertifikasyon Merkezi Oluşturulması konulu genelgesi uyarınca kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması amacıyla öncelikli olarak kamu çalışanlarına NES verir. NES'ler ile bağlantılı imza oluşturma verileri, elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza oluşturmak amacıyla kullanılır. Kamu çalışanları NES'lerini ve ilgili imza oluşturma verilerini kamu kurum ve kuruluşlarındaki veya kendi özel işlerindeki güvenli elektronik imza uygulamalarında kullanırlar.

Kamu ESHS, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalışır. SUE dokümanı, NES'lerin yönetimi ve kayıt işlemleri sırasında yapılan işlerin hangi ortamlarda ve nasıl yürütüldüğünü Sİ dokümanına bağlı olarak detaylandırarak anlatır.

Kamu SM'den NES talebinde bulunan tüzel ve gerçek kişiler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. NES talebinde bulunan kurumlar bununla ilgili olarak Kamu SM ile imzaladıkları sözleşmelerde SUE dokümanına atıfta bulunurlar. NES sahibi kişiler de NES Sözleşmesi veya NES Sahibi Taahhütnamesi'ni imzalayarak SUE dokümanında belirtilen esasları kabul ederler.

1.1. Genel Bakış

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

SUE dokümanı, "İnternet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı" [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

kısım alt başlıkların altındaki “Düzenlenmesine gerek duyulmamıştır” ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Nitelikli Elektronik Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 11

Yayın Tarihi: 20.10.2015

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

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

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

1.3.2. Kayıt Birimleri

Kayıt birimleri, sertifika başvurularının alınması, Kamu ESHS'ye onaylanmak üzere gönderilmesi, Kamu ESHS tarafından üretilen sertifikaların akıllı karta yüklenerek sahibine verilmesi görevi ile yetkilendirilmiş birimlerdir. Kayıt birimleri kayıtçı olarak da anılmaktadır. Kamu ESHS'nin kendi bünyesinde ve fiziksel ortamında kayıtçılar bulunmaktadır. Buna ek olarak gerekli gördüğü durumlarda kendi fiziksel ortamından uzakta başka mekanlarda da kayıtçı hizmeti verebilmektedir.

1.3.3. Sertifika Sahipleri

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

1.3.4. Üçüncü Kişiler

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

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Çalışanları adına Kamu SM'ye sertifika başvurusunda bulunan kamu kurum veya kuruluşudur. Kurum ile Kamu SM arasında sertifika hizmetleri ile ilgili sözleşme imzalanır. Kurum sözleşmeye uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur. Kurum ile Kamu SM bu dokümanda adı geçen yerlerdeki işlemleri NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi'ne (YONG-001-013) uygun olarak yerine getirmekten sorumludur.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

1.3.5.2. Kurum Yetkilileri

Sertifika başvurusunda bulunan kurumların sertifika alınacak personeli ile ilgili bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olan kişidir. Kurum yetkilisi Kamu SM tarafından kendisine imzalatılan taahhütnamedeki şartları yerine getirmekten sorumludur.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

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

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

1.4.2. Sertifika Kullanımının Sınırları

NES ve ilgili imza oluşturma verisi, güvenli elektronik imza oluşturma ve doğrulama dışında kullanılamaz. NES sahibi kişi, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmelerini güvenli elektronik imza ile gerçekleştiremez. NES'lerin ve ilgili imza oluşturma verilerinin tanımlı maddi sınırları üzerinde değerinde işlem yapmak, elektronik imzalı e-posta göndermek, açık ağlar üzerinde kimlik doğrulaması yapmak, iletilen mesajların bütünlüğünü ve gizliliğini sağlamak gibi amaçlarla kullanımından doğan zararlardan Kamu SM sorumlu tutulamaz.

Sertifikaya ait imza oluşturma verisinin kullanılacağı güvenli elektronik imza uygulamasına bir sınırlama getirilmiş ise bununla ilgili bilgi sertifika içeriğine yazılır.

Kamu SM, dağıttığı sertifikaların hangi uygulamalarda ne amaçlar doğrultusunda kullanıldığının kontrolünü yapmakla yükümlü değildir.

1.5. Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

SUE dokümanı Kamu SM tarafından yazılmıştır. Kamu SM, gerekli gördüğü durumlarda SUE dokümanında değişiklik yapabilir.

1.5.2. İletişim Bilgileri

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

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

Tel. : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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

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

- <http://depo.kamusm.gov.tr/ilke/>
- http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE/KSM_NES_SUE.pdf

1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluğunu Belirleyen Kişi

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

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

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

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

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

Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt.

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

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

Güvenli elektronik imza oluşturma aracı erişim verisi: Sertifika sahibine ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler.

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

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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

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

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

Kurum Yetkilisi: Kamu kurumlarının resmi yazı ile Kamu SM'ye bildirdiği ve NES ile ilgili süreçlerde kurumu temsile yetkili kişidir.

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

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

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

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

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

Sertifika sahibi: Güvenli elektronik imza oluşturmak amacıyla ESHS'den sertifika alan gerçek kişi.

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

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

BS (British Standards): İngiliz Standartları

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

DSA (Digital Signature Algorithm): Sayısal İmza Algoritması

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

KPS: Kimlik Paylaşım Sistemi

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

2. Yayımlama ve Bilgi Deposu

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

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

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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

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

2.3. Yayım Sıklığı ve Zamanı

NES, sahibi tarafından talep edilmesi durumunda üretildiği hafta içinde yayımlanır.

Taahhütnameler, yönergeler, formlar, Sİ ve SUE dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip derhal yayımlanır.

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

2.4. Erişim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır.

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

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

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

3. Kimlik Belirleme ve Doğrulama

NES'lerle ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kişi veya kurumun öncelikle kimlik tanımlama veya doğrulaması yapılır. Bu bölümde NES yönetim prosedürleri içinde uygulanan kimlik tanımlama ve doğrulama yöntemleri ile NES'in içinde yazılan kimlik bilgileri anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

NES'lerde Kamu SM ve sertifika sahibine ait kimlik bilgilerinin belirtildiği DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

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

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika sahibinin NES'i içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

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

3.1.5. Kimlik Bilgilerinin Tekilliği

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

3.1.6. Markanın Tanınması, Doğrulaması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

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

3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

Sertifika sahibine ait imza oluşturma ve doğrulama verileri, kişiler adına Kamu SM tarafından üretilerek sahibine güvenli elektronik imza oluşturma aracı içinde ulaştırılır. İmza oluşturma verisine sahiplik güvenli elektronik imza oluşturma aracının sertifika sahibi tarafından şahsen teslim alınması yoluyla kanıtlanır.

İmza oluşturma ve doğrulama verilerinin sertifika sahibi kişilerce üretilmesinin gerekli olduğu durumlar da oluşabilir. Böyle durumlarda Kamu SM anahtarların güvenli bir şekilde üretildiğinden

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

emin olmak için anahtar üretimi sırasında hazırda bulunmayı talep edebilir. Bu durumda anahtarlar üretilirken Kamu SM tarafından yetkilendirilmiş bir kişi anahtarların üretildiği ortama giderek gözlemler ve gerekli yönlendirmelerde bulunur. Anahtarlar üretildikten sonra açık anahtar, sertifika üretmek üzere Kamu SM'ye iletilir. Açık anahtar Kamu SM'ye iletilirken ilgili imza oluşturma verisi ile imzalanarak PKCS #10 formatında sertifika talep dosyası oluşturulur. Kamu SM sertifikayı üretmeden önce PKCS #10 formatındaki sertifika talep dosyasının imzasını doğrulayarak, sertifika talep eden kişinin imza oluşturma verisine sahip olduğunu kriptografik olarak kanıtlar.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Çalışanları adına NES başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazıyla Kamu SM'ye bildirir. Kamu SM resmi yazıya istinaden kurum kimliğini belirler. Resmi yazıda Kamu SM sertifika işlemlerini kurum adına yürütecek kurum yetkilisi de belirlenerek Kamu SM'ye iletilir. Kurum yetkilisinin Kamu SM'ye gönderdiği elektronik imzalı belgeler de kurum kimliğinin belirlenmesi için kabul görür. Belge üzerindeki kurum yetkilisine ait elektronik imzanın doğrulanması yoluyla kurum yetkilisinin temsil ettiği kurum kimliği belirlenir.

3.2.3. Kişisel Kimliğin Belirlenmesi

NES başvurusunda bulunan kurumlar, NES almak istediği çalışanlarına ait bilgileri, kurumun onayını taşıyan resmi yazıyla ya da kurum yetkilisinin elektronik olarak imzaladığı form ile Kamu SM'ye bildirir. Resmi yazının ekinde NES alınacak kişilerin listesini Kamu SM'ye iletir. Kişilere ait kimlik bilgileri Kimlik Paylaşım Sistemi ile kurumsal başvuru belgesine dayanılarak belirlenir.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi veya kurum tarafından başvuru sırasında ve daha sonra değişiklik sebebiyle beyan edilen aşağıdaki erişim bilgileri ve diğer bilgilerin doğruluğu Kamu SM tarafından kontrol edilmez.

- Telefon numaraları
- Faks numaraları
- Güvenli elektronik imza oluşturma aracı tesliminde kullanılacak adres bilgisi
- Sertifika sahibinin elektronik posta adresi
- Sertifika sahibinin unvanı veya görevi ile ilgili bilgiler
- Sertifika sahibinin çalıştığı kurum ile ilgili bilgiler
- Sertifika sahibinin çalıştığı birim ile ilgili bilgiler

Bu bilgilerin doğruluğu sertifika sahibinin veya kurumun beyanı üzerine kabul edilir.

Kurum ve sertifika sahibi bu bilgileri Kamu SM'ye doğru beyan etmekle yükümlüdür. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doğabilecek zararlardan, sertifika yönetim sürecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin Doğrulanması

Sertifika içeriğine sertifika sahibinin yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

3.2'de belirtildiği gibi yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

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

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

Sertifika iptal isteği kurum tarafından da yapılabilir. Kurum Kamu SM'ye resmi yazı yazarak iptal edilmesini istediği kurum çalışanına ait sertifika bilgilerini Kamu SM'ye bildirir. İptal talebini yapan kurumun kimlik doğrulaması gelen resmi yazıya dayanılarak yapılır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4. İşlemsel Gereklr

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

- Sertifika başvurusu
- Sertifika yenileme
- Sertifika askıya alma ve askıdan çıkarma
- Sertifika iptal etme

Süreçler sertifika sahipleri, kurumlar ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

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

Kurumsal başvuru süreci kamu kurumunun Kamu SM'ye resmi yazı yazarak çalışanları adına sertifika talep etmesi ile başlar. Kurumun, sertifika başvuru işlemlerini kurum adına yürütecek bir veya daha fazla sayıda kurum yetkilisi görevlendirmesi ve kurum yetkililerini Kamu SM'ye resmi yazı ile bildirmesi zorunludur.

Kurum veya kurum adına kurum yetkilileri, başvuru sırasında NES almak istediği çalışanlarının temel başvuru bilgilerini (T.C. kimlik no, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni) Kamu SM'ye bildirir. Bildirimler resmi yazı ile veya kurum yetkilisinin elektronik imzasını taşıyan formun Kamu SM'ye elektronik ortamdan gönderilmesi ile yapılır. Kurum, çalışanın haberi olmadan çalışanı adına sertifika başvurusunda bulunamaz. Kurum çalışanın durumdan haberdar olması ve NES almayı kendisinin talep etmesi gerekir. Bu talep, kurum çalışanı tarafından doldurulup imzalanan;

Basılı formlar için ıslak imzalı

Elektronik formlar için e-imzalı

sertifika başvuru formunun Kamu SM'ye iletilmesi ile yapılır.

NES başvuru formları kurum çalışanları tarafından internet üzerinden doldurulur. Başvuru formunun başvuru sahibi kurum çalışanı tarafından ıslak imzalı veya elektronik imzalı olması zorunludur.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

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

Kurum NES almak istediği personelinin listesini, personelin kimliklerinin belirlenmesi için istenen bilgilerle birlikte Kamu SM'ye gönderir. Başvurunun işleme alınabilmesi için NES alacak olan çalışanlar, kişisel bilgileri ile adres, telefon numarası gibi erişim bilgilerinin bulunduğu NES başvuru

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

formunu doldurup ıslak imza ile imzalarlar. Başvuru formları kurum veya kurum yetkilisi tarafından, Kamu SM'ye iletilir. Bilgi ve belgelerin gizliliğinin sağlanması için belgelerin kapalı zarf içinde Kamu SM'ye iletilmesi gerekmektedir. Belgelerin Kamu SM'nin eline geçene kadarki zaman içerisinde gizliliğinin sağlanmasından kurum sorumludur.

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

Sertifika başvurusunda bulunan kişi başvuru sırasında, NES'inin herkesin erişimine açık dizin sunuculardan yayımlanıp yayımlanmayacağı konusundaki talebini ve NES'in kullanımıyla ilgili maddi sınıra ilişkin bilgilendirmeyi Kamu SM'ye yapar. NES başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

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

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama ve doğrulama işlevleri yerine getirilir. NES başvurusunda bulunan kurumlar aşağıdaki bilgi ve belgeleri Kamu SM'ye gönderir:

NES alacak çalışanların, T.C. kimlik no (yabancı uyruklular için pasaport no), ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgisinin bulunduğu liste,

NES alacak çalışanların ıslak imzasını taşıyan NES başvuru formları,

Yabancı uyruklular için noter onaylı pasaport sureti,

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

- Kurum'dan gelen yazının ve formların imzalı ve onaylı olup olmadığına bakılır.
- Kurum tarafından gönderilen NES alacak çalışanlar listesindeki T.C. kimlik no (yabancı uyruklular için pasaport no), ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgisinin tamlığına ve doğruluğuna bakılır.
- NES'te kullanılacak bilgilerin doğruluğu, KPS kullanılarak tespit edilir.
- Yabancı uyruklu NES başvuru sahiplerinin noter onaylı pasaport suretlerine bakılır.

Bilgi ve belgeler hatasız ve tam ise kimlik tanımlama ve doğrulama işlevi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik onay ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kimlik tanımlama ve doğrulama yapılamaz.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, NES başvurusu sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik bilgi veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyenlerle ilgili bilgilendirme, kurum yetkilisine ve/veya başvuru sahibi kişiye yapılır ve gerekli görülen bilgi ve belgeler tekrar talep edilir. Yazılı bilgilendirme, kuruma resmi yazı gönderme veya kurum yetkilisine ve/veya başvuru sahibine e-posta gönderme yoluyla yapılır. Sözlü bilgilendirme kurum yetkilisine ve/veya başvuru sahibine telefon açılarak yapılır. Sözlü



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

bildirimler kayıt altına alınır. Kurum yetkilisi ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilenler Kamu SM sisteminde tanımlanır ve NES üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

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

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Sertifika başvurusu tamamlanarak, sistemde tanımlanan kişiler adına anahtar çifti ile güvenli elektronik imza oluşturma aracı erişim verisi Kamu SM tarafından üretilir. Anahtar çiftleri ve erişim verilerinin üretilmesi, güvenli elektronik imza oluşturma aracının ilklendirilmesi gibi işlemler NES üretim aşamasında gerçekleştirilir.

NES, imza doğrulama verisi ve sistemde onayı verilmiş kimlik bilgilerinin Kamu ESHS'ye ait imza oluşturma verisi ile imzalanması suretiyle üretilir. NES'ler ETSI TS 101 862, ITU-T X.509 v.3 standartlarına ve Kanunun 9'uncu maddesinde belirtilen niteliklere uygun olarak üretilir. İmza oluşturma verisi, imza doğrulama verisi ve NES güvenli elektronik imza oluşturma aracına yüklenir. İmza oluşturma verisi, güvenli elektronik imza oluşturma aracı içinde şifreli saklanır ve kopyası sistemde tutulmaz. Güvenli elektronik imza oluşturma aracı erişim verisi oluşturularak kapalı parola zarfına basılır ya da sistemde şifreli olarak tutulur. Güvenli elektronik imza oluşturma aracı erişim verisinin teslimatı kimlik ibrazı ile yapılır. Güvenli elektronik imza oluşturma aracı erişim verisi sertifika sahiplerine öncelikli olarak web servislerinden teslim edilir. Web servislerinin kullanılmadığı durumda parola zarfı ile teslimat gerçekleştirilir.

Kapalı parola zarfına basılan güvenli elektronik imza oluşturma aracı erişim verisi sistemden silinir. Kapalı parola zarfına basılan erişim verisi, NES teslim edildikten sonra, ikinci bir gönderim ile sertifika sahibine teslim edilir.

Web üzerinden erişimi sağlanan güvenli elektronik imza oluşturma aracı erişim verisi sertifika sahibi inisiyatifiyle sistemden silinebilir. Güncellenen veri Kamu SM sistemi ile senkronize edilmez.

Sertifika üretim süreci tamamlandıktan ve güvenli elektronik imza oluşturma aracına yazıldıktan sonra; bilgilendirme amaçlı belgeler ile birlikte zarflanır. Kurumun talebi doğrultusunda zarfın içine başka donanımlar da eklenebilir. Zarf kurye ile sertifika sahibine iletilir ve resmi kimlik belgesi ve imza karşılığı teslim edilir. İmzalanan sertifika teslim fişi Kamu SM'ye geri getirilir.

Sertifika teslim fişi barkod bilgisi okutularak, sertifikanın teslim edildiği bilgisi Kamu SM kayıtlarına işlenir. Kapalı parola zarfı ile erişim verisi teslim edilecek ise; ikinci adımda parola zarfı gönderilir. Parola zarfı da resmi kimlik ve imza karşılığı sertifika sahibine teslim edilir. İmzalanan parola teslim fişi Kamu SM'ye geri getirilir. Parola teslim fişi barkodu okutularak sisteme kayıt edilir ve teslimat tamamlanır.

Kamu SM'nin yükümlülüklerinin belirtildiği Kamu SM Taahhütnamesi <http://www.kamusm.gov.tr/BilgiDeposu> adresinden yayımlanır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifika sahibi kendisine gönderilen güvenli elektronik imza oluşturma aracını teslim aldığıında, NES'inin oluşturulduğu konusunda bilgilendirilmiş olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Kamu SM, NES'i içeren güvenli elektronik imza oluşturma aracını kurye veya görevli Kamu SM çalışanı ile sahibine teslim eder. Sertifika sahibi kullanmaya başlamadan önce sertifikasının içeriğini kontrol eder ve doğrular. Sertifikanın kendisine ait olmaması ya da sertifika içerisindeki bilgilerde hata olması durumunda, 10 (on) iş günü içerisinde iade sebebini belirterek güvenli elektronik imza oluşturma aracını Kamu SM'ye iade eder. 10 (on) iş günü içerisinde iade edilmemesi durumunda sertifika kabul edilmiş sayılır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

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

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

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Sertifikanın oluşturulması, internetten erişimi sağlanan raporlar ya da e-posta yolu ile kurum yetkilisine bildirilir.

4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve İmza Oluşturma Verisini Kullanımı

NES sahibi, imza oluşturma verisini elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza uygulamalarında kullanır. Güvenli elektronik imza oluşturma verisinin, güvenli elektronik imza oluşturma aracı içinde bulunması zorunludur. Güvenli elektronik imza oluşturma aracının Bölüm 6.2.1'de belirtilen güvenlik standartlarını sağlaması gerekmektedir.

NES'lerle ilgili imza oluşturma verilerinin güvenli elektronik imza oluşturma amacı dışında kullanımlarından doğan zararlardan Kamu SM sorumlu tutulamaz.

İptal olmuş veya geçerlilik süresi dolmuş NES'lere ait imza oluşturma verileri ile işlem yapılamaz.

4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

Sertifika sahibine ait NES'lerin içinde yer alan imza doğrulama verileri, üçüncü kişilerce elektronik imzalı verilerin imzasının doğrulanması amacıyla kullanılır. İmza doğrulama verisinin veya sertifikanın, güvenli elektronik imza doğrulaması dışında kullanılması sonucu oluşabilecek zararlardan, üçüncü kişiler sorumludur.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.6. Sertifika Süresinin Uzatılması

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

4.7. Sertifika Yenileme

Kamu SM, sertifika yenileme işlemini, yeni anahtar çifti üretmek sureti ile yerine getirir. Sertifika yenileme işlemleri Bölüm 4.1'de anlatılan ilk sertifika başvuru işlemleri ile aynıdır. Ancak yenilemede kamu kurumunun Kamu SM'ye resmi yazı yazarak yeniden sertifika talebinde bulunmasına gerek yoktur. Yenilenecek sertifika bilgileri resmi yazıyla Kamu SM'ye bildirilebileceği gibi, kurum yetkilisinin elektronik imzasını taşıyan yenileme yapılacak sertifika bilgilerinin bulunduğu formun Kamu SM'ye elektronik ortamdan gönderilmesi ile de yenileme başvurusu yapılabilir.

4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi:

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

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraplara Duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.8. Sertifikada Bilgi Değişikliği

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

Sertifika içeriğinde yer alan bilgiler Ad, Soyad, T.C Kimlik No, varsa sertifikaya ait imza oluşturma verisinin kullanılacağı güvenli elektronik imza uygulamasına getirilen kısıt ile ilgili bilgiler ve sertifika içeriğinde yazan diğer bilgilerdir.

Sertifika içeriğinde yer alan bilgilerde değişiklik olması, sertifikada bilgi değişikliği gerektirmektedir. Kamu SM, sertifikada bilgi değişikliği gerçekleştirmez. Bilgi değişikliği gerekli olduğu durumlarda, anahtarlar yenilenerek sertifika yeni bilgilerle yeniden üretir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

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

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

durumlarında iptal edilir.

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir;

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

NES iptal başvurusu, sertifika sahibi tarafından telefonla çağrı merkezinden, internet sitesi üzerinden veya yazılı olarak Kamu SM'ye yapılır. İptal başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibinin kimlik belirlenmesi ve doğrulanması yapılır. Kimlik doğrulanması yapılamayan iptal başvuruları işleme alınmaz.

İnternet üzerinden yapılan iptal başvurusunda, sertifika sahibi <https://nesbireysel.kamusm.gov.tr> internet adresi üzerinden sisteme giriş yaparak iptal talebinde bulunur. İnternet üzerinden kimlik doğrulama işleminin yapılmasıyla, NES Kamu SM sisteminde otomatik olarak iptal edilir.

Çağrı merkezi aracılığıyla yapılan iptal başvurularında, sertifika sahibi Kamu SM çağrı merkezini arar. Çağrı merkezi üzerinden kimlik doğrulama işleminin yapılmasının ardından NES, IVR üzerinden iptal edilir.

Yazılı olarak yapılan taleplerde sertifika sahibi, imzasını taşıyan iptal başvuru formunu Kamu SM'ye iletir. Form üzerindeki bilgiler ve sertifika sahibine ait imza kontrol edilerek kimlik doğrulanması yapılır. Kimlik doğrulanmasının yapılmasının ardından NES, Kamu SM sertifika işletmeni tarafından iptal edilir.

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

NES iptal başvurusu sırasında iptal sebebi Kamu SM'ye bildirilir. Geçmişe yönelik olarak NES iptal edilmez.

NES iptal edildikten sonra, Kamu SM sertifika sahibini ve gerekirse bağlı bulunduğu kurum yetkilisini NES'in iptal edildiğine dair bilgilendirir.

Kurum, çalışanlarına ait sertifikaları gerekli gördüğünde iptal ettirebilir. Kurum iptal edilmesini istediği sertifika bilgilerini Kamu SM'ye resmi yazı ile bildirerek iptal talebinde bulunur. Resmi yazının Kamu SM'nin eline geçmesinin ardından sertifika iptal edilir. Sertifika sahibi ve kurum yetkilisi e-posta ile veya telefonla sertifikanın iptal edildiğine dair bilgilendirilir.

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

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

NES iptal edildikten sonra yeniden NES talebinde bulunulabilir.

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve NES'i iptal eder. İptal edilen NES bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan derhal duyurur.

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 4.9.7'de belirtilmiştir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, sorgulama yapacak kişinin kimlik doğrulamasına gerek kalmadan dileyen herkes tarafından erişilebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

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

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

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 36 (otuzaltı) saattir. Ancak bu sürenin dolması beklenmeden her 4 (dört) saatte bir SİL tekrar yayımlanır. Gün içinde yeni bir NES iptali olmasa dahi SİL 4 (dört) saatte bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

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

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, NES'lerin iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma verisiyle imzalanır.

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

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

SİL dosyası, iptal edilen her NES için iptal bilgisinin eklenmesiyle gittikçe büyüyen bir dosya niteliğindedir. Güncel iptal durum kaydına her ihtiyaç duyulduğunda dosyanın Kamu SM bilgi deposundan indirilmesi gerekir. Gittikçe büyüyen SİL dosyasının sisteme getireceği yüke karşılık, ÇİSDUP ilgili NES'in iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları gerekir.

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

4.9.12. İmza oluŐturma Verisinin Güvenliđini Yitirmesi Durumu

Sertifika sahibine ait imza oluŐturma verisinin güvenliđini yitirmesi durumunda NES iptal edilir. NES'in iptal edilmesi dıŐında herhangi bir husus uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındıđı Durumlar

NES'in geçiici bir süre için iptal durumunda olup sürenin sonunda yeniden kullanılabilir olmasını sađlamak amacıyla askıya alma iŐlemi tanımlanmıŐtır.

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

- Sertifika sahibinin bir süreliđine görev baŐında olmaması ve NES'ini kullanım dıŐı bırakmak istemesi,
- NES'in iptal sebebinin ortaya çıktıđından Őüphelendiđi halde, yanlışlıkla iptalini engellemek amacıyla, NES'i önce askıya almak istemesi.

4.9.14. Sertifika Askıya Alma BaŐvurusunu Kimlerin Yapabildiđi

NES askıya alma baŐvurusu sadece sertifika sahibi tarafından yapılır.

4.9.15. Sertifika Askıya Alma BaŐvurusunun İŐlenmesi

NES askı baŐvurusu, sertifika sahibi tarafından telefonla çağrı merkezinden veya yazılı olarak Kamu SM'ye yapılır. Askı baŐvurusu alındıđında öncelikle baŐvuruyu yapan sertifika sahibinin kimlik belirlemesi ve dođrulaması yapılır. Kimlik dođrulaması yapılamayan askı baŐvuruları iŐleme alınmaz.

Askıya alınan NES için, SİL'de geçiici olarak iptal edildiđini belirten tanımlı sebep kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, NES askıya alındıktan sonra, gerekli gördüđü durumlarda sertifika sahibini ve bađlı bulunduđu kurum tarafından yetkilendirilen kiŐiyi sertifikanın askıya alındıđına dair bilgilendirir.

Sertifika sahibi, internet üzerinden sertifikasını askıdan indirebilir. Askıya aldırdıđı sertifikasını en az bir defa SİL'e girmeden askıdan indiremez.

Kamu SM'ye ait Kök SHS ve Kamu ESHS sertifikaları askıya alınmaz.

4.9.16. Askıda Kalma Süresi

Böyle bir süre öngörölmemiŐtir.

4.10. Sertifika Durum Servisleri

Üçüncü kiŐiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılıđıyla aŐađıda belirtilen Őekilde ulaŐır.

4.10.1. İŐletimsel Özellikleri

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

ÇİSDUP İstemci desteđi olan üçüncü kiŐiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi 2. Bölümde verilmiŐtir. Üçüncü kiŐiler NES veya



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin Erişilebilirliği

SİL ve ÇİSDUP servislerinin verildiği sistemlere erişimin kesintisiz olarak sağlanabilmesi için gereken tüm tedbirler Kamu SM tarafından alınır. Ancak buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurur. Üçüncü kişilerin iptal durum kaydını, erişimin kesilmesi sebebiyle kontrol etmeden yaptıkları işlemlerden doğan zararlardan Kamu SM sorumlu tutulamaz.

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

NES'in kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM NES'in iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibini ve varsa sözleşmelerde belirtilen kişileri bilgilendirir. Kullanım süresinin dolması durumunda Kamu SM sertifika sahibini bilgilendirmek zorunda değildir; sertifika sahibi NES'inin kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5. Yönetim, İşlemsel ve Fiziksel Kontroller

Bu bölümde Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan güvenlik kontrolleri anlatılmıştır.

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM sisteminin çalıştığı cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiği, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır.

5.1.1. Tesis Yeri ve İnşaatı

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

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

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

5.1.2. Fiziksel Erişim

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

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

5.1.3. Güç Kaynağı ve Havalandırma

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

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

Bina gerekli havalandırma sistemi ile donatılmıştır.

5.1.4. Su Baskınları

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5.1.5. Yangın Önleme ve Korunma

Kamu SM işlevlerinin yerine getirildiđi ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur.

5.1.7. Atıkların Yok Edilmesi

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

5.1.8. Farklı Mekanlarda Yedekleme

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

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

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

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

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

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

Sertifika Kayıt Sorumlusu: Sertifika üretim ve iptaliyle ilgili kayıtların giren personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleştiren personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

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

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

NES üretimi iki kişinin kontrolünde gerçekleştirilir.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilmektedir.

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

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

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

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gereklere

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

5.3.2. Geçmiş Araştırması

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

5.3.3. Eğitim Gereklere

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

5.3.4. Sürekli Eğitim Gereklere ve Sıklığı

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

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM verdiği hizmetler için dış kaynak kullanmak durumunda kaldığında, bu hizmeti sağlayacak firma personeli ile ilgili güvenlik kontrollerini firma ile yaptığı sözleşme ile belirler.

5.3.8. Sağlanan Dokümantasyon

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

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

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

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
- Anahtar üretimi
- Anahtar yedekleme
- Anahtar dağıtımı
- Anahtar saklama
- Anahtar arşivleme
- Anahtar yok etme
- Kriptografik modül yaşam döngüsü işlemleri
- NES üretim, yenileme, askıya alma ve iptal başvuruları
- Başvuru sahibi tarafından sunulan belgelerin neler olduđu bilgisi
- Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
- Başvuru sırasında elektronik veya kađıt ortamda alınan form veya belgeler
- Kađıt belgelerin kopyalarının nerede saklandıđı bilgisi
- Geçerli ve geçersiz alınan tüm başvuru bilgileri
- NES yaşam döngüsü yönetimi işlemleri
- NES başvurusunun işlenmesi
- NES sahibi için anahtar çifti üretimi
- NES üretimi
- NES sahibine ait güvenli elektronik imza oluşturma aracı ile ilgili yapılan işlemler
- Güvenli elektronik imza oluşturma aracı dağıtımı
- NES yenileme
- NES askıya alma
- NES askıdan indirme



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- NES iptal etme
- NES yayımlanması
- SİL yayımlanması
- ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtları
- Güvenlikle ilgili diđer işlemler
- Sisteme başarılı veya başarısız tüm erişim denemeleri
- Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
- Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve deđiştirilmesi
- Güvenlik profili deđişiklikleri
- Sistemin çökmesi, donanım hataları ve diđer bozukluklar
- Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
- Kamu SM'ye ziyaretçi giriş ve çıkışı
- Kayıtlarda kayıt zamanı ve kaydın oluşmasına sebep olan çalışanın ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyiőiyle ilgili tutulan kayıtlar düzgün zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açığı oluşup oluşmadığı kontrol edilir. Buna ek olarak, sistemde olađandışı hareketlerin görülmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görülen ve başlatılan işlemler de belgelenir.

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

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeđi alınmaktadır. Yedekleme ihtiyacını

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur.

5.4.6. Kayıtların Toplanması

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

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan işlemi başlatan Kamu SM sertifika yönetim sistemi kullanıcısı, kaydın yapıldığına dair sistem tarafından bilgilendirilir.

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

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

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

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

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

5.5.2. Arşivlerin Tutulma Süresi

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

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kağıt baskılar KONTROLSÜZ KOPYA’dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler izinsiz izlenmeyi, değiŐtirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduđu ortam 5.5.2’de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek şekilde seçilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş sürekliliđi politikası geređince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüđu kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kađıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Yasal gereksinimlerin ortaya çıkması ya da BTK tarafından denetim amacıyla talep edilmesi durumunda yetkili personel eşliđinde arşiv bilgileri elde edilebilir.

5.6. Anahtar DeđiŐimi

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

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

SİL dosyaları aynı Kamu SM imza oluŐturma verisiyle imzalanıyorsa, Kamu SM’nin eski imza oluŐturma verisiyle oluŐturulmuş NES’lerin kullanım tarihleri dolana kadar, Kamu SM SİL’leri eski imza oluŐturma verisiyle imzalanmaya devam eder. Yeni üretilen NES’ler için oluŐturulan yeni SİL dosyası yeni Kamu SM imza oluŐturma verisiyle imzalanır.

Kamu SM, anahtarlarının yenilendiđi bilgisini <http://www.kamusm.gov.tr> internet adresi üzerinden duyurur ve sertifika hizmeti verdiđi kurumları bilgilendirir.

5.7. Güvenliđin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliđin Yitirilmesi Durumunun Düzeltilmesi

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

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

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

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

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı şekilde <http://www.kamusm.gov.tr> internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, NES sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarlarıyla oluşturulan NES'lere güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen NES'lerin gerekli görünen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM NES isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM imza oluşturma verisinin yok edilmesi sürecini işletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtar çiftinin yenilenmesiyle, iptal edilen NES'lerin sertifika sahibinden gelen talep doğrultusunda sertifika yenileme süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalışırılık

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

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

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM, işleyişine Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde son verebilir. Bu durumda Kamu SM aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün kurumlara yazı, sertifika sahiplerine ise e-posta ile duyurur.
- Sertifika hizmetlerine son vereceği bilgisini internet sitesi üzerinden ve ulusal yayın yapan en yüksek tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur.

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- Sertifika hizmetlerine son vereceğini duyurmasından itibaren sertifika başvurusu kabul etmez ve yeni sertifika oluşturmaz.
- Dağıttığı NES'leri iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği NES'lerin bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.
- İptal ettiği NES'lerin kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı imza oluşturma verisine karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- NES'leri imzalamak için kullandığı imza oluşturma verisini imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde 20 (yirmi) yıl boyunca korur.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

6. Teknik Güvenlik Kontrolleri

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

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1. Kök SHS, Kamu ESHS, ÇİSDUP Yayınlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aşağıdaki imza oluşturma ve doğrulama verileri oluşturulur:

6.1.1.2. Kök SHS'ye ait imza oluşturma ve doğrulama verisi

- Kamu ESHS'ye ait imza oluşturma ve doğrulama verisi
- ÇİSDUP Yayınlayıcı'ya ait imza oluşturma ve doğrulama verisi
- NES sahiplerine ait imza oluşturma ve doğrulama verileri

Kök SHS, Kamu ESHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği gizli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen imza oluşturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personeller tarafından onaylanır.

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

6.1.1.3. Sertifika Sahibi Anahtar Çiftinin Üretimi

Sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir ve güvenli elektronik imza oluşturma aracı içinde saklanır.

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

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

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

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip, imza oluşturma verisi, sertifika ile birlikte güvenli elektronik imza oluşturma aracına yüklenir. Güvenli elektronik imza oluşturma aracı imza karşılığı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir.

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

Güvenli elektronik imza oluşturma aracı erişim verisi ise iki farklı yöntem ile teslim edilir;

Kapalı parola zarfı: Sertifika teslim fiőı Kamu SM'ye ulaőtıktan sonra, güvenli elektronik imza oluşturma aracı erişim verisi parola zarfına yazılarak kapatılır. Bu işlem operatörün bu verileri göremeyeceđi şekilde gerçekleşir. Kapalı parola zarfı sertifika sahibine iletilir ve kimlik kontrolü ve imza karşılığı teslim edilir.

Web üzerinden: Web üzerinden teslim edilen veriler için güvenli bağlantı protokolleri (https) kullanılmaktadır. Sertifika sahibinin kimlik kontrolü için, T.C. kimlik no, başvuru formunu doldururken tanımladığı güvenlik sözcüğü ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik doğrulaması sonrasında sertifika sahibi güvenli elektronik imza oluşturma aracı erişim verisine erişir.

Kamu SM'nin yükümlülüklerinin belirtildiđi Kamu SM Taahhütnamesi <http://www.kamusm.gov.tr/BilgiDeposu> adresinden yayımlanır.

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

Sertifika sahiplerine ait NES'lerle ilgili anahtar çiftleri Kamu SM tarafından üretildiđi için imza doğrulama verisinin Kamu SM'ye ulaőtırılması söz konusu değildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Eriőim Sağlanması

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

Kamu SM'ye ait sertifikalar internet üzerinden yayımlanır.

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

6.1.5. Anahtar Uzunlukları

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

Sertifika sahiplerine ait NES'leri imzalayan Kamu ESHS'ye ait, RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048-bittir.

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

Kamu SM tarafından üretilen NES sahiplerine ait, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048-bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

Kamu SM tarafından anahtar üretiminde kullanılan algoritmaların güvenliği ispatlanmış ve dünyaca kabul görmüştür. Algoritmaların gerçekleştiriminde kullanılan yöntemler gerekli güvenlik kriterlerini sağlar. Anahtarları üreten programlar gerekli güvenlik testlerinden geçirilirler.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

6.1.7. Anahtar Kullanım Amaçları

Kök SHS'ye ait imza oluŐturma verisi, kendi sertifikasını, Kamu ESHS'ye ait sertifikayı ve yürüttükleri görevler açısından özel niteliđi haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüđü, MİT MüsteŐarlıđı, Jandarma Genel Komutanlıđı, Sahil Güvenlik Komutanlıđı, DıŐıŐleri Bakanlıđı ve Telekomünikasyon Kurumu bünyesinde kurulabilecek olan ESHS'lerin sertifikalarını imzalamak amacıyla kullanılır.

Kamu ESHS'ye ait imza oluŐturma verisi, Kamu ESHS tarafından oluŐturulan NES'lerin ve yayımlanan SİL dosyalarının imzalanması amacıyla kullanılır.

ÇİSDUP yayımlayıcıya ait imza oluŐturma verisi, ÇİSDUP yanıtlayıcıdan duyurulan iptal durum kayıtlarının imzalanması amacıyla kullanılır.

NES sahiplerine ait imza oluŐturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı üretmek için kullanılır. Sertifika sahibi, güvenli elektronik imza oluŐturma aracı içinde bulunan imza oluŐturma verisini imza oluŐturma dıŐında kullanmaz. Üçüncü kişiler, NES'ler içindeki imza dođrulama verilerini, sertifika sahibi tarafından oluŐturulmuş elektronik imzanın dođruluđunu kontrol etmek için kullanır. Anahtar çiftlerinin güvenli elektronik imza oluŐturma ve dođrulama dıŐında kullanımlarından dođan sorumluluk sertifika sahibine ve üçüncü kişilere aittir; Kamu SM bu durumda sertifika sahibinin veya üçüncü kişilerin gördükleri zarardan sorumlu tutulamaz.

6.2. İmza OluŐturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

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

Kriptografik modül aŐađıda belirlenen güvenlik iŐlevlerine sahiptir:

- İmza oluŐturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüđünü sađlar.
- Modüle eriŐimde kimlik belirleme ve dođrulama iŐlevlerini yerine getirir.
- EriŐim yetkisi birden fazla kişinin kontrolünde olacak Őekilde tanımlanabilir.
- Sistem kullanıcıya tanımlanan roller dođrultusunda, verdiđi hizmetlere eriŐimi sınırlar.
- Düzgün çalıŐtıđı test edilebilir, test sırasında hata oluŐtuđunda güvenli duruma geçer.
- Modüle izinsiz eriŐim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıŐtır.
- Yetkisiz eriŐime teŐebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeđinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluŐturma verisinin içinde bulunduđu güvenli elektronik imza oluŐturma aracı, imza oluŐturma verisinin aracın dıŐına çıkmasını engelleyen ve araca eriŐimi parola ile sađlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluŐturma aracı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'de belirtilen aŐađıdaki güvenlik standartlarından en azından birisini sađlar:
 - FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzeri,



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

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

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

Kamu SM'ye ait imza oluşturma verisinin yedeğinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme işlemi hazırda kullanılmakta olan imza oluşturma verisi için sağlanan güvenlik ile eşdeğer güvenlik önlemleri altında yapılır. Yedeklenen imza oluşturma verisi yetkisiz kişilerin erişimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan imza oluşturma verisinin bulunduğu ortam ile aynı güvenlik şartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait imza oluşturma verileri Kamu SM tarafından yedeklenmez.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluşturma verileri arşivlenmez. Kullanım süreleri sonunda geri dönüşüz şekilde silinir.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

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

Sertifika sahiplerine ait imza oluşturma verileri, sadece yetkili personelin giriş izninin bulunduğu odalarda güvenli elektronik imza oluşturma aracına, şifrelenerek yüklenir. İmza oluşturma verisi güvenli elektronik imza oluşturma aracına yüklendikten sonra kopyası sistemden silinir.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

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

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

6.2.8. İmza Oluşturma Verisine Erişim

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

İmza oluŐturma verisi kriptografik modül içinde Őifreli durumdayken eriŐime kapalıdır. EriŐime aılması için eriŐimi saėlayan verinin modüle sunulması gerekir. İmza oluŐturma verisinin eriŐime aılması ve kullanılabilir duruma getirilmesi birden fazla yetkili alıŐanın ortak denetimi altındadır.

Sertifika sahibine ait imza oluŐturma verisi güvenli elektronik imza oluŐturma aracı içinde sertifika sahibinin eriŐim verisi ile korunmuŐ olarak saklanır. EriŐim denetimi eriŐim denetim verisi ile saėlanır.

6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

Kamu SM'nin imza oluŐturma verisi imzalama için kullanıldıktan sonra oturum kapandıėında veriye eriŐim otomatik olarak kesilir ve bir dahaki kullanımına kadar Őifrelenerek eriŐime kapalı tutulur. EriŐimin yeniden saėlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden iŐletilmesi gerekir.

Sertifika sahibinin kullandıėı güvenli donanım araları, imza oluŐturma verisini kullanan oturumun kapanmasından sonra veriye eriŐimi kesecek biimde alıŐır. EriŐimin yeniden saėlanabilmesi için sertifika sahibinin eriŐim verisini yeniden girmesi gerekir. EriŐim verisinin ard arda 3 (ü) defa yanlıŐ girilmesi durumunda güvenli elektronik imza oluŐturma aracı kilitletir ve araca eriŐim saėlanamaz.

6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

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

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

6.2.11. Kriptografik Modülün Deėerlendirilmesi

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

6.3. Anahtar ifti Yönetimiyle İlgili Diėer Konular

6.3.1. İmza Doğrulama Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doğrulama verileri sertifikalar içinde tutulur ve NES'ler kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arŐivlenir. NES'lerin arŐivleri yetkisiz kiŐilerce tahrifatına ve silinmesine karŐı gerekli önlemlerin alındıėı ortamlarda tutulur.

6.3.2. İmza OluŐturma ve Doğrulama Verilerinin Kullanım Süreleri

İmza oluŐturma verisinin kullanım süresi, NES'in içeriėinde belirtilen NES kullanım süresi kadardır. NES'in kullanım süresinin dolmasıyla ya da NES'in iptal edilmesiyle imza oluŐturma verisinin kullanımı sona erer. Ancak, kullanım süresi dolsa bile NES'ler içindeki imza doğrulama verileri gemiŐe yönelik imzaların doğrulanabilmesi için kullanılır.

Kamu SM'ye ve sertifika sahibine ait anahtar iftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan imza algoritmasına göre belirlenir. Kamu SM'ye ait 2048 ve 4096 bitlik RSA anahtar iftleri



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 5 (beş) yıl için kullanılır.

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

6.4. Erişim Denetim Verileri

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

Sertifika sahibine ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, güvenli elektronik imza oluşturma aracı erişim verisi ile bireysel işlemlerin yapıldığı internet şubesine erişim verileridir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

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

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

6.4.2. Erişim Denetim Verilerinin Korunması

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

Sertifika sahibine ait erişim parolaları sertifika sahibine güvenli yöntemlerle ulaştırılır.

Erişim parolaları ilk kullanımda sertifika sahibi tarafından değiştirilir. Parolayı yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları, kapalı zarf içinde, resmi kimlik kontrolü yapılarak imza karşılığı ya da iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gereker

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

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

6.6. Yaşam Döngüsü Teknik Denetimleri

6.6.1. Sistem Geliştirme Denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda verilmiştir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileşenlerin yedekleri oluşturulur.
- Sistemin açık ağa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileştirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan denetimler TS ISO/IEC 27001 gereklerini sağlar.

6.6.2. Güvenlik Yönetimi Denetimleri

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

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

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

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

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

6.8. Zaman Damgası

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

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan NES'lerin içeriği ile ilgili bilgilendirme yapılmaktadır.

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

Kamu SM tarafından dağıtılan NES'ler X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili imza doğrulama verisi, sertifika sahibine ve sertifikayı yayımlayan Kamu SM'ye ait isim bilgileri ve Kamu SM'nin elektronik imzası gibi zorunlu alanların yanı sıra X.509 V.3 sertifika uzantılarını içerir. NES'in içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

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

Tablo 1 NES Uzantıları

Sertifika Uzantısı	Kritik Uzanti	Açıklama
Temel Kısıtlar ¹	HAYIR	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılmayacağı belirtilir.
ESHS Anahtar Tanımlayıcı ²	HAYIR	Kamu SM'ye ait Kamu ESHS açık anahtarının SHA-256 özet çıktısından oluşur.
Sertifika Anahtar Tanımlayıcı ³	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-256 özet çıktısından oluşur.
Anahtar Kullanım ⁴	EVET	Anahtarların sadece elektronik imza amaçlı kullanıldığının ifade edilmesi için "nonRepudiation" [inkar edilemezlik] alanı ve "digitalSignature" [sayısal imza] alanı seçilmiştir.
SİL Yayımlama Adresi ⁵	HAYIR	http://depo.kamusm.gov.tr

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

⁴ KeyUsage

⁵ CRLDistributionPoints

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

ESHS Erişim Bilgisi ⁶	HAYIR	http://depo.kamusm.gov.tr http://ocsp3.kamusm.gov.tr/
Sertifika İlkeleri ⁷	HAYIR	Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.1) ile SUE dokümanının bulunduğu http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE internet adresini ve BTK tarafından oluşturulan NES ibaresine ait metni içerir.
Nitelikli Elektronik Sertifika İbaresini ⁸	EVET	ETSI 101 862'ye göre, id-etsi-qcs-QcCompliance= 0.4.0.1862.1.1 nesne tanımlama numarasını ve varsa sertifikanın kullanımına ilişkin maddi sınır bilgisini içerir. BTK tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası bilgisini içerir.

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

Kamu SM tarafından kişilere verilen NES'lerin kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme ETSI 101 862'ye göre "Nitelikli Elektronik Sertifika İbaresini Uzantısı" içinde yapılır.

Sertifikanın nitelikli olduğu "Nitelikli Elektronik Sertifika İbaresini Uzantısı" içerisindeki ETSI ve BTK' ya ait nitelikli elektronik sertifika ibareleri ile belirtilir.

BTK tarafından belirlenen ibare "Nitelikli Elektronik Sertifika İbaresini Uzantısı" içinde yer alan "İbare Bilgisi"⁹ alanının içine yazılır. Bu ibareye ait nesne tanımlama numarası ise "İbare Numarası"¹⁰ alanı içinde yer alır. Bu ibare ve ibareye ait nesne tanımlama numarası aşağıda belirtilmiştir.

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

Nesne tanımlama numarası: 2.16.792.1.61.0.1.5070.1.1

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kişilere verdiği NES'leri imzalamak için SHA-256 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.

Sertifika sahiplerine ait anahtar çiftleri RSA algoritması anahtar çiftleridir.

Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları içinde belirtilir.

7.1.4. İsim Alanı Biçimleri

Kamu SM tarafından üretilen NES'lerdeki isim alanı "ITU X.500 Distinguished Name [Ayırt edici isim]" biçimine uygundur.

⁶ AuthorityInformationAccess

⁷ CertificatePolicies

⁸ QcStatement

⁹ StatementInfo

¹⁰ StatementId



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

7.1.5. İsim Kısıtları

Üretilen NES'lerdeki isim bilgileri kişiyi tekil olarak tanımlamayı sağlayacak niteliktedir ve resmi kimlik belgelerinde geçen ad ve soyad bilgisinden oluşur.

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

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

Tablo 2 NES İsim Alanı Bilgileri

Alan Adı	NES İçeriği
CN ¹¹	Sertifika sahibinin adı soyadı
Serial ¹²	T.C. kimlik numarası / Pasaport numarası
C ¹³	TR

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası:

2.16.792.1.2.1.1.5.7.1.1

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

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

“Sertifika İlkeleri Uzantısı” NES'lerin üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. NES'lerin üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen NES'in “Sertifika İlkeleri Uzantısı¹⁴”nın içinde yer alır. “Sertifika İlkeleri Uzantısı”nın içinde “İlke Niteleyici¹⁵” olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

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

Kamu SM tarafından kişilere verilen elektronik sertifikaların nitelikli olduğunu belirten ibare “Sertifika İlkeleri Uzantısı” içindeki “Kullanıcı Bildirim Alanı¹⁶”nda tanımlanır. Kamu SM tarafından tanımlanan NES ibaresi Kamu SM Sİ dokümanında verilmiştir.

¹¹ CN: Common Name [Genel isim]

¹² Serial: Serial Number [Seri Numarası]

¹³ C: Country [Ülke]

¹⁴ Certificate Policies

¹⁵ Policy Identifier

¹⁶ User Notice



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL'ler "ITU X.509" SİL formatına uygun olarak aşağıdaki bilgileri içerir:

- SİL'i oluşturan Kamu SM'ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL'i imzalamak için SHA-256 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL'in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen NES'lerle ilgili aşağıdaki bilgiler:
 - Sertifikanın seri numarası
 - Sertifikanın iptal tarihi
 - Sertifikanın neden iptal edildiği bilgisi
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM'ye ait sertifikanın "ESHS Anahtar Tanımlayıcı" numarası

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

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

ÇİSDUP cevapları aşağıdaki bilgileri içermektedir:

- Versiyon bilgisi
- Cevaplayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritması-nın OID'-si.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- ÇİSDUP yanıtlayıcı imzası

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

Çevrim İçi Sertifika Durum Protokolü RFC 6960'da tarif edilen "ÇİSDUP" formatını destekler. ÇİSDUP Yanıtlayıcı'dan alınan cevaplar aşağıdaki şekilde değerlendirilir:

Good [iyi]: Sertifika geçerli konumdadır.

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

Unknown [bilinmiyor]: Sorgusu yapılan sertifika hakkında herhangi bir bilgi bulunmamaktadır. RFC 6960'da belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

8. Uygunluk Denetimleri

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

Kamu SM, ek olarak ISO/IEC 27001 bilgi güvenliđi yönetim standardına uygun olarak hizmet verir ve standart geređi düzenli olarak iç ve dış denetimlere tabi tutulur.

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

8.1. Uygunluk Denetiminin Sıklığı

Kamu SM iki yılda en az bir defa Kurum tarafından denetlenir.

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

İç denetim, altı ayda bir defa olmak üzere gerçekleştirilir.

8.2. Denetçinin Nitelikleri

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

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

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

8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi

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

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

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

8.4. Denetimin Kapsamı

Kamu SM'nin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

8.5. Yetersizliđin Tespiti Durumunda Yapılacaklar

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

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

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

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

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

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ve sertifika sahiplerine ait NES'leri ücretsiz olarak yayımlar.

9.1.3. İptal Durum Kaydına Erişim Ücreti

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

9.1.4. Diğer Servis Ücretleri

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

Kamu SM imza oluşturma verisinin saklandığı güvenli elektronik imza oluşturma aracı teminini kendi imkanlarıyla sertifika sahibine sağlayabilir. NES'ler ve güvenli donanım araçları için ödenecek bedelin miktarı ile ilgili bilgilendirme Kamu SM tarafından gönderilen teklif mektuplarında veya kurumlara yapılan sözleşmelerde yapılır. Ödemenin usulüne uygun biçimde yapılmaması durumunda NES üretimi yapılmaz.

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

9.1.5. İade Ücreti

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

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

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



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

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

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Düzenlenmesine gerek duyulmamıştır.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

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

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

NES'in içeriğinde bulunan bilgiler aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

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

Sertifika sahiplerinden başvuru sırasında ve daha sonra sertifika yaşam döngüsü içinde istenen bilgilere erişimin ve yetkisiz kullanımın engellenmesi ve mahremiyetinin korunması için, Kamu



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

SM tarafından gerekli güvenlik tedbirleri alınır. Sadece yetkilendirilmiş çalışanlar sertifika sahiplerinin kişisel bilgilerine erişirler.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

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

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM verdiği sertifika hizmetlerinde sistem bileşenleri olan Kamu SM, sertifika sahipleri ve üçüncü kişiler 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şekilde üzerlerine düşen yükümlülükleri sağlar.

Kamu SM, sertifika sahipleri, sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, NES Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi, NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi ve varsa taraflar arası yapılan sözleşmelerde sözü geçen yükümlülükleri yerine getirirler.

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHS olarak Kamu SM'nin yükümlülükleri şunlardır:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek,
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek,
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak,
- Kök SHS ve Kamu ESHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak,
- Kök SHS ve Kamu ESHS sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak,
- NES verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmek,
- Kurumlardan gelen NES başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek,
- NES'in içeriğindeki bilgilerin doğruluğunu beyan edilen belgelere dayanarak sağlamak,
- Gerekli başvuru şartlarını sağlamayan başvuru sahiplerine NES vermemek,

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- NES başvurularını değerlendiren, başvurunun sonucu hakkında ilgili kişileri bilgilendirmek,
- NES başvurusu kabul edilmiş kişiler için anahtar çifti ve NES üretmek,
- Sertifika sahibine ait imza oluşturma verisini oluşturduktan sonra imza oluşturma verisini ve üretiminde kullanılan gizli değişkenleri kendi sisteminden silmek, imza oluşturma verisinin kopyasını hiçbir şekilde tutmamak,
- Sertifika sahibine imza oluşturma aracı temin etmesi durumunda, bu aracın güvenli elektronik imza oluşturma aracı olmasını sağlamak,
- Üretilen NES'ler ile imza oluşturma verilerini Sİ ve SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek,
- Sertifika sahiplerinin NES'lerini aksi sertifika sahibi tarafından başvuru formunda belirtilmedikçe son kullanıcıların erişebileceği ortamlarda yayımlamak,
- NES'lerin kullanım şartlarını belirleyen sertifika profillerini oluşturmak,
- NES başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli işlemleri yapmak,
- NES askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemleri yapmak,
- NES askıdan çıkarma işlemleri Sİ ve SUE'de belirtilen şekilde yapmak,
- NES iptal başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak,
- Yayımlanan Sİ ve SUE dokümanları ile NES Sahibi Taahhünamesi'ne uygun olmayan NES kullanımlarının tespit edilmesi durumunda ilgili NES'i iptal etmek,
- İptal edilmiş NES bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak,
- NES'lerin ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak,
- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek,
- NES üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak,
- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen süreler boyunca güvenli olarak saklamak,
- Kök SHS sertifikasının özet değerini Kamu SM'ye ait internet ortamından yayımlamak, ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurmak ve gazete ilanlarının bir örneğini Telekomünikasyon Kurumu'na iletme.

9.6.2. Kayıt Birimi Yükümlülükleri

Kayıt birimlerinin yükümlülükleri 9.6.1. Bölümde belirtilen ESHS yükümlülükleri ile aynıdır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri şunlardır:



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- NES başvuru, askıya alma, iptal ve diğer işlemleri ilgili Sİ ve SUE'de belirtildiği şekilde, detayları Kamu SM NES yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek,
- NES başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- Adına düzenlenen, imza oluşturma verisini içeren güvenli elektronik imza oluşturma aracı ve kapalı parola zarfını şahsen teslim almak,
- Adına düzenlenen NES yayımlandığında NES'deki bilgilerin doğruluğunu kontrol etmek,
- SUE Bölüm 6.2.1'de belirtilen standartlara uygun güvenli elektronik imza oluşturma aracı kullanmak,
- İmza oluşturma verisinin güvenliğini sağlamak, kendisine ait imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının ve imza oluşturma verisi erişim verisinin gizliliğini korumak, bunları başkasına kullandırmamak ve bu konuda gerekli tedbirleri almak,
- İnternet veya çağrı merkezi üzerinden sertifika işlemlerini yapabilmesi için kullandığı parolalarının gizliliğini ve güvenliğini sağlamak,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya imza oluşturma verisinin gizliliğinin yitirildiğinden şüphelenmesi durumunda NES'in iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak,
- Güvenli elektronik imza oluşturma aracı erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları her ay düzenli olarak değiştirmek,
- NES'in içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak,
- NES başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri derhal Kamu SM'ye bildirmek,
- İptal olmuş, kullanıma açılmamış, askıya alınmış veya geçerlilik süresi dolmuş NES ile işlem yapmamak,
- İmza oluşturma verisini SHS sertifikası imzalamak amacıyla kullanmamak,
- Kendisine verilen NES'i Sİ ve SUE dokümanlarında belirtildiği biçimde varsa karşılıklı imzalanan sözleşmelere uygun ve NES Sahibi Taahhütnamesi'nde belirtilen şartlar dahilinde kullanmak.
- İmza oluşturma verisini, NES içerisinde belirtilen maddi sınırları aşan finansal işlemlerde kullanmamak.

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

9.6.4. Üçüncü Kişilerin Yükümlülükleri

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

- NES'lerin, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- NES'in kullanım süresinin dolup dolmadığını kontrol etmek,

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

- NES'in geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili NES'lerinin içinde mevcut olan imza doğrulama verilerini kullanarak doğrulamak,
- NES'in doğruluğunu Kamu ESHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu ESHS sertifikasının doğruluğunu Kök SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kök SHS sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,
- Sertifika sahibinin NES'inin içindeki imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğunu doğrulamak.
- Finansal işlemlerde sertifika içerisinde bulunan maddi sınır bilgisini kontrol etmek.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

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

- Sertifika alınacak kurum çalışanlarını belirlemek
- Sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olacak en az bir tane kurum yetkilisi görevlendirmek ve resmi yazı ile kurum yetkilisinin bilgilerini Kamu SM'ye bildirmek
- Kurum yetkilisinin görevini sonlandırdığında bunu Kamu SM'ye resmi yazı ile bildirmek
- Yeni görevlendirdiği kurum yetkililerinin bilgilerini Kamu SM'ye resmi yazı ile bildirmek
- Sertifika yönetim süreçleri ile ilgili varsa Kamu SM ile imzalanan sözleşmeye uymak
- Sertifika yönetim süreçleri ile ilgili NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi'ndeki yükümlülükleri yerine getirmek
- Kamu SM'nin internet sitesi üzerinden yayımladığı ÜRÜN/HİZMET TALEP FORMU'nu doldurarak ilk sertifika başvurusu sırasında resmi yazı ile Kamu SM'ye iletmek

9.6.5.2. Kurum Yetkililerinin Yükümlülükleri

Kurum yetkililerinin sertifika alınacak kurum çalışanlarına ait bilgileri Kamu SM'ye göndermekle ilgili yükümlülükleri aşağıda belirtilmiştir:

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

Kurum yetkililerinin sertifika teslimatları ile ilgili yükümlülükleri NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesinde belirtilmiştir.

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

9.7. Yükümlülüklerden Feragat

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

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlar ile sınırlıdır.

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar NES Sahibi Taahhütnamesi, NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi ve varsa imzalanan sözleşmelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diğere düzenlemeler dikkate alınır.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahipleri, NES Sahibi Taahhütnamesi ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile işbirliği içinde çalışır. Kamu SM'den NES hizmeti alan kamu kurumları NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesine ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile işbirliği içinde çalışır.

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

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ, SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiğı Kamu SM Taahhütnamesi, NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi ve varsa kurum ile imzaladığı sözleşmelerdeki şartları yerine getirir.

9.10.1. Anlaşma Süresi

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

Kurumla imzalanan sözleşmenin geçerlilik süresi sözleşme içerisinde belirtilir.

9.10.2. Anlaşmanın Sona Ermesi

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

- Taraflardan birisinin sözleşmeye uygun olarak, sözleşmenin sonlandırılması için talepte bulunması



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

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

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

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

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Kurumla imzalanan sözleşmenin sona ermesiyle hizmeti alan kurumun, sözleşme ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. Kamu SM kurumdan sertifika başvurularını almayı durdurur. Ancak daha önceden yapılmış başvurular ile ilgili işlemler, anlaşmanın sona erme sebebine bağlı olarak kurumun talep etmesi durumunda devam eder.

İmzalanan sözleşme veya NES Sahibi Taahhütnamesi'nin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sağlamakla ilgili yükümlülükleri ortadan kalkar. İmzalanan sözleşme veya NES Sahibi Taahhütnamesi'nin sona erme sebebi, sertifika sahibinin taahhütnameden, Sİ veya SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesinden dolayı, Kamu SM'nin sertifikayı iptal etmesi ise, bu durumda sertifika sahibinin 6 (altı) ay içinde yapacağı ikinci bir NES talebi kabul edilmeyecektir. Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

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

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, NES yönetim prosedürlerinde NES başvurusunun sonucu, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibini ve/veya ilgili kurumu bilgilendirir. Bilgilendirmeler telefon, faks veya e-posta aracılığıyla olur. Kişinin NES başvuru formunda belirtilen e-posta adresine,

Uyarı: Yalnız Kamu SM dosya sunucudan erişilen elektronik kopyalar güncel ve kontrollü olup, elektronik ortamdan alınacak kâğıt baskılar KONTROLSÜZ KOPYA'dır



NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

değişmesi halinde yeni bildirdiği e- posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

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

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

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metodları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

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

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilafların çözümünde 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, karşılıklı imzalanan sözleşmeler, taahhütnameler, Kamu SM Sertifika İlkeleri ve Kamu SM Sertifika Uygulama Esasları, NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

9.14. Uygulanacak Hukuk

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

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.