

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu

YON.01.01

Revizyon No

17

Revizyon Tarihi

28.03.2024

TASNİF DIŐI

REVİZYON GEÇMİŐI		
Revizyon No	Revizyon Nedeni	Revizyon 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
12	Atıf yapılan dokümanların isimleri deđiştii için güncelleme yapıldı. Doküman genelinde düzenlemeler yapıldı. Dokümanın eski revizyonları Doküman Yönetim Sistemi'nde YONG-001-007 kodu ile yer almaktadır.	26.04.2018

NİTELİKLİ ELEKTRONİK SERTİFİKA UYGULAMA ESASLARI

13	Anahtar deęiŐimiyle Sürüm 6'ya geçiŐten ötürü gerekli deęiŐiklikler yansıtıldı.	06.01.2020
14	SİL ömrü 48 saat olarak deęiŐtirildi. http://www.kamusm.gov.tr olan web adresleri https://kamusm.bilgem.tubitak.gov.tr olarak güncellendi.	23.03.2021
15	SİL ömrü güncellendi.	02.04.2021
16	Bireysel baŐvuru ile ilgili eklemeler yapıldı, parola zarfı kullanımı kaldırıldı, sertifika iptal isteęininin iŐlenme süresi ve uygunluk denetiminin sıklıęı güncellendi. Doküman genelinde düzenlemeler yapıldı.	20.10.2022
17	Sertifika baŐvurusunun iŐlenme süresi belirtildi. Sertifikanın askıda kalma süresi baŐlıęındaki ifade güncellendi. Doküman genelinde düzenlemeler yapıldı.	28.03.2024

İÇİNDEKİLER

1.	GİRİŐ.....	11
1.1.	Genel Bakıő.....	11
1.2.	Doküman Adı ve Tanımı	12
1.3.	Sistem Bileőenleri	12
1.3.1.	Elektronik Sertifika Hizmet Saėlayıcısı	12
1.3.2.	Kayıt Birimleri	12
1.3.3.	Sertifika Sahipleri.....	12
1.3.4.	Üçüncü Kiőiler	13
1.3.5.	Diėer Bileőenler.....	13
1.4.	Sertifika Kullanımı	13
1.4.1.	Uygun Olan Sertifika Kullanımı	13
1.4.2.	Sertifika Kullanımının Sınırları.....	13
1.5.	Uygulama Esaslarının Yönetimi	14
1.5.1.	Doküman Yönetimi	14
1.5.2.	İletiőim Bilgileri	14
1.5.3.	Sertifika Uygulama Esaslarının İkelere Uygunluėunu Belirleyen Kiői	14
1.5.4.	Sertifika Uygulama Esasları Onay Prosedürleri	14
1.6.	Tanımlar ve Kısaltmalar	14
1.6.1.	Tanımlar	14
1.6.2.	Kısaltmalar	16
2.	YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ.....	18
2.1.	Bilgi Depoları	18
2.2.	Sertifika Hizmeti ile İlgili Bilgilerin Yayınlanması	18
2.3.	Yayın Sıklıėı ve Zamanı	18
2.4.	Eriőim Kontrolleri.....	18
3.	KİMLİK BELİRLEME VE DOėRULAMA.....	19
3.1.	İsmlendirme	19
3.1.1.	İsim Alanı Tipleri	19
3.1.2.	Kimlik Bilgilerinin Teőhise Elveriőli Olması	19
3.1.3.	Sertifika Sahibinin Takma İsim veya Lakap Kullanması	19
3.1.4.	Farklı İsim Alanı Tiplerinin Yorumlanması	19
3.1.5.	Kimlik Bilgilerinin Tekilliėi	19
3.1.6.	Markanın Tanınması, Doėrulanması ve Rolü	19
3.2.	İlk Kimlik Belirleme	20
3.2.1.	İmza Oluőturma Verisine Sahip Olmanın Kanıtlanması	20
3.2.2.	Kurumsal Kimliėin Belirlenmesi	20
3.2.3.	Kiőisel Kimliėin Belirlenmesi	20
3.2.4.	Doėrulanmayan Sertifika Sahibi Bilgileri	20
3.2.5.	Yetkinin Doėrulanması	21
3.2.6.	Uyum Kriterleri	21
3.3.	Sertifika Yenileme İsteėinde Kimlik Doėrulama	21
3.3.1.	Olaėan Sertifika Yenileme İsteėinde Kimlik Doėrulama	21

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

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi	30
4.9.16. Askıda Kalma Süresi.....	30
4.10. Sertifika Durum Servisleri.....	30
4.10.1. İşletimsel Özellikleri.....	31
4.10.2. Servisin Erişilebilirliği	31
4.10.3. İsteğe Bağlı Özellikler	31
4.11. Sertifika Sahipliğinin Sona Ermesi.....	31
4.12. Anahtar Yeniden Üretme	31
5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER.....	31
5.1. Fiziksel Güvenlik Denetimleri	32
5.1.1. Tesis Yeri ve İnşaatı.....	32
5.1.2. Fiziksel Erişim	32
5.1.3. Güç Kaynağı ve Havalandırma.....	32
5.1.4. Su Baskınları.....	33
5.1.5. Yangın Önleme ve Korunma	33
5.1.6. Saklama ve Yedekleme Ortamlarının Korunması	33
5.1.7. Atıkların Yok Edilmesi.....	33
5.1.8. Farklı Mekanlarda Yedekleme.....	33
5.2. Prosedürel Kontroller	33
5.2.1. Güvenilir Roller	33
5.2.2. Her İşlem İçin Gereken Kişi Sayısı.....	34
5.2.3. Kimlik Doğrulama ve Yetkilendirme	34
5.2.4. Görevlerin Ayrılmasını Gerektiren Roller	34
5.3. Personel Güvenlik Kontrolleri.....	34
5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri	34
5.3.2. Geçmiş Araştırması	34
5.3.3. Eğitim Gerekleri	35
5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı.....	35
5.3.5. Görev Değişim Sıklığı ve Sırası.....	35
5.3.6. Yetkisiz Eylemlerin Cezalandırılması.....	35
5.3.7. Anlaşmalı Personel Gereksinimleri	35
5.3.8. Sağlanan Dokümantasyon	35
5.4. Denetim Kayıtları.....	35
5.4.1. Kaydedilen İşlemler	35
5.4.2. Kayıtların İncelenme Sıklığı	36
5.4.3. Kayıtların Saklanma Süresi	37
5.4.4. Kayıtların Korunması	37
5.4.5. Kayıtların Yedeklenmesi	37
5.4.6. Kayıtların Toplanması.....	37
5.4.7. Kayda Sebepiyet Veren Tarafın Bilgilendirilmesi.....	37
5.4.8. Saldırıya Açıklığın Değerlendirilmesi.....	37
5.5. Kayıt Arşivleme.....	38
5.5.1. Arşivlenen Kayıt Bilgileri.....	38
5.5.2. Arşivlerin Tutulma Süresi	38
5.5.3. Arşivlerin Korunması	38

5.5.4.	Arşivlerin Yedeklenmesi	38
5.5.5.	Kayıtların Zaman Damgası Gereksinimleri	38
5.5.6.	Arşivlerin Toplanması	39
5.5.7.	Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu	39
5.6.	Anahtar Değişimi	39
5.7.	Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar	39
5.7.1.	Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi	39
5.7.2.	Donanım, Yazılım veya Veri Bozulması	39
5.7.3.	İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi	40
5.7.4.	Arıza Sonrası Yeniden Çalışırlık	40
5.8.	Sertifika Hizmetlerinin Sonlandırılması	40
6.	TEKNİK GÜVENLİK KONTROLLERİ	40
6.1.	Anahtar Çifti Üretimi ve Kurulumu	41
6.1.1.	Anahtar Çifti Üretimi	41
6.1.2.	Sertifika Sahibine İmza Oluşturma Verisinin Ulaştırılması	41
6.1.3.	Elektronik Sertifika Hizmet Sağlayıcısı'na İmza Doğrulama Verisinin Ulaştırılması	42
6.1.4.	Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması	42
6.1.5.	Anahtar Uzunlukları	42
6.1.6.	Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü	42
6.1.7.	Anahtar Kullanım Amaçları	42
6.2.	İmza Oluşturma Verisinin Korunması	43
6.2.1.	Kriptografik Modül Standartları	43
6.2.2.	İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim	43
6.2.3.	İmza Oluşturma Verisinin Yeniden Elde Edilmesi	43
6.2.4.	İmza Oluşturma Verisinin Yedeklenmesi	44
6.2.5.	İmza Oluşturma Verisinin Arşivlenmesi	44
6.2.6.	İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi	44
6.2.7.	İmza Oluşturma Verisinin Kriptografik Modülde Saklanması	44
6.2.8.	İmza Oluşturma Verisine Erişim	44
6.2.9.	İmza Oluşturma Verisine Erişimin Kesilmesi	45
6.2.10.	İmza Oluşturma Verisinin Yok Edilmesi	45
6.2.11.	Kriptografik Modülün Değerlendirilmesi	45
6.3.	Anahtar Çifti Yönetimiyle İlgili Diğer Konular	45
6.3.1.	İmza Doğrulama Verisinin Arşivlenmesi	45
6.3.2.	İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri	45
6.4.	Erişim Denetim Verileri	46
6.4.1.	Erişim Denetim Verilerinin Oluşturulması	46
6.4.2.	Erişim Denetim Verilerinin Korunması	46
6.4.3.	Erişim Denetim Verileri İle İlgili Diğer Konular	46
6.5.	Bilgisayar Güvenliğı Denetimleri	46
6.5.1.	Bilgisayar Güvenliğı İle İlgili Teknik Gereklere	46
6.5.2.	Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi	46
6.6.	Yaşam Döngüsü Teknik Denetimleri	46
6.6.1.	Sistem Geliştirme Denetimleri	46
6.6.2.	Güvenlik Yönetimi Denetimleri	47

6.6.3.	Yaşam Döngüsü Güvenlik Denetimleri	47
6.7.	Ağ Güvenliđi Denetimleri	47
6.8.	Zaman Damgası	47
7.	SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ.....	48
7.1.	Sertifika Biçimi.....	48
7.1.1.	Sürüm Numarası	48
7.1.2.	Sertifika Uzantıları	48
7.1.3.	Algoritma ve Nesne Tanımlayıcılar	50
7.1.4.	İsim Alanı Biçimleri	50
7.1.5.	İsim Kısıtları.....	50
7.1.6.	Sertifika İlkeleri Nesne Tanımlama Numarası	51
7.1.7.	İlke Kısıtları Uzantısının Kullanımı.....	51
7.1.8.	İlke Niteleyiciler	51
7.1.9.	Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi	52
7.2.	Sertifika İptal Listesi Biçimi.....	52
7.2.1.	Sürüm Numarası	52
7.2.2.	Sertifika İptal Listesi Uzantıları.....	52
7.3.	Çevrim İçi Sertifika Durum Protokolü Biçimi.....	52
7.3.1.	Sürüm Numarası	52
7.3.2.	ÇİSDUP Uzantıları.....	52
8.	UYGUNLUK DENETİMLERİ.....	53
8.1.	Uygunluk Denetiminin Sıklığı.....	53
8.2.	Denetçinin Nitelikleri	53
8.3.	Denetçinin Denetlenen Tarafı Olan İlişkisi.....	54
8.4.	Denetimin Kapsamı.....	54
8.5.	Yetersizliđin Tespiti Durumunda Yapılacaklar.....	54
8.6.	Sonucun Bildirilmesi	54
9.	DİĐER İŐLER VE HUKUKSAL MESELELER	54
9.1.	Ücretlendirme	54
9.1.1.	Sertifika OluŐturma ve Yenileme Ücreti.....	54
9.1.2.	Sertifika EriŐim Ücreti	55
9.1.3.	İptal Durum Kaydına EriŐim Ücreti	55
9.1.4.	Diđer Servis Ücretleri	55
9.1.5.	İade Ücreti.....	55
9.2.	Finansal Sorumluluk.....	55
9.2.1.	Sigorta Kapsamı	55
9.2.2.	Diđer Varlıklar	55
9.2.3.	Sertifika Mali Sorumluluk Sigortası.....	55
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.	Diđer BaŐlıklar	57
9.5.	Telif Hakları	57
9.6.	Temsil Hakkı ve Yüklümlülükler	57
9.6.1.	Elektronik Sertifika Hizmet Sađlayıcısı Yüklümlülükleri	57
9.6.2.	Kayıt Birimi Yüklümlülükleri	59
9.6.3.	Sertifika Sahibinin Yüklümlülükleri	59
9.6.4.	Üçüncü KiŐilerin Yüklümlülükleri	60
9.6.5.	Diđer BileŐenlerin Yüklümlülükleri	60
9.7.	Yüklümlülüklerden Feragat	61
9.8.	Sorumlulukla İlgili Sınırlamalar	61
9.9.	Tazminat Halleri.....	61
9.10.	AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi	61
9.10.1.	AnlaŐma Süresi.....	61
9.10.2.	AnlaŐmanın Sona Ermesi	62
9.10.3.	AnlaŐmanın Sona Ermesinin Etkileri	62
9.11.	Sistem BileŐenleri İle HaberleŐme ve KiŐisel Bilgilendirme	63
9.12.	DeđiŐiklik Halleri	63
9.12.1.	DeđiŐiklik Metotları	63
9.12.2.	Bilgilendirme Mekanizması ve Sıklıđı	63
9.12.3.	Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar	63
9.13.	AnlaŐmazlık Halleri	63
9.14.	Uygulanacak Hukuk	64
9.15.	Uygulanabilir Yasalarla Uyum.....	64
9.16.	Diđer Hükümler	64
10.	EK-A SERTİFİKA PROFİLLERİ.....	65
10.1.	KAMU SM NES KÖK SERTİFİKASI	65
10.2.	KAMU SM NES ALT KÖK SERTİFİKASI	66
10.3.	SON KULLANICI NES SERTİFİKA ŐABLONU	68

TABLolar

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

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) 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 Taahhünamesi'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, “Internet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı” [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki “Düzenlenmesine gerek duyulmamıştır” ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

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

1.2. Doküman Adı ve Tanımı

Doküman Adı: Nitelikli Elektronik Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 17

Yayın Tarihi: 28.03.2024

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.1

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

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluşturma verisiyle imzalamak olan ESHS'ler, sertifika başvurusunda bulunanların kayıt ve kimlik doğrulama işlemleri ile elektronik sertifika dağıtım, yenileme, askıya alma, askıdan indirme, 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, NES başvurularını alan ve inceleyerek onaylayan ya da reddeden, sertifika yenileme taleplerini alan ve inceleyerek onaylayan ya da reddeden, bahsi geçen onay ve red kararlarını sertifika sahibine bildiren, yapmış olduğu işlemlere ilişkin düzenli olarak her türlü kayıt ve belgeyi tutarak en az 20 (yirmi) yıl süre ile arşivleyen yetkilendirilmiş birimlerdir. Kayıt birimleri kayıtçı olarak da anılmaktadır. 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 bağın 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 veya kurumdan taahhütname/sipariş formu alınır. Kurum sözleşmeye/taahhünameye/sipariş formuna uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur. Kurum ile Kamu SM bu dokümanda adı geçen yerlerdeki işlemleri Kurumsal Taahhütname'ye uygun olarak yerine getirmekten sorumludur.

1.3.5.2. Kurum E-İmza Sorumlusu

Sertifika başvurusunda bulunan kurumların sertifika alınacak personeli ile ilgili bilgilerini Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim halinde olan e-imza sorumlusudur. Kurum e-imza sorumlusu Kamu SM E-İmza Sorumlusu Taahhütnamesi'ndeki 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 resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları dışındaki teminat sözleşmelerini, güvenli elektronik imza ile gerçekleştiremez. NES'lerin ve ilgili imza oluşturma verilerinin tanımlı maddi sınırları üzerinde değerde işlem yapmak, elektronik imzalı e-posta göndermek, açık ağlar üzerinde kimlik doğrulaması yapmak, iletilen mesajların bütünlüğünü ve gizliliğini sağlamak gibi amaçlarla kullanımından doğan zararlardan Kamu SM sorumlu tutulamaz.

Sertifikaya ait imza oluŐturma verisinin kullanılacađı güvenli elektronik imza uygulamasına bir sınırlama getirilmiŐ ise bununla ilgili bilgi sertifika ieriđine yazılır.

Kamu SM, rettiđi sertifikaların hangi uygulamalarda ne amalar dođrultusunda kullanıldıđının kontroln yapmakla ykml deđildir.

1.5. Uygulama Esaslarının Ynetimi

1.5.1. Dokman Ynetimi

SUE dokmanı Kamu SM tarafından yazılmıŐtır. Kamu SM, gerekli grdđ durumlarda SUE dokmanında deđiŐiklik yapabilir.

1.5.2. İletiŐim Bilgileri

Bu SUE dokmanının uygulanması ve ilgili ynetim ilkeleri hakkındaki sorular Kamu SM'nin aŐađıdaki eriŐim noktalarına ynlendirilebilir:

Adres : Kamu Sertifikasyon Merkezi, TBİTAK YerleŐkesi, PK. 74, 41470 Gebze-KOCAELİ

Tel. : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

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

Kamu SM, SUE dokmanını herkesin eriŐimine aık bulunan aŐađıdaki internet adresinden yayımlar:

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

1.5.3. Sertifika Uygulama Esaslarının İkelere Uygunluđunu Belirleyen KiŐi

Bu SUE dokmanının uygunluđu Kamu SM ynetimi ve ynetim tarafından yetki verilen kiŐiler tarafından belirlenir.

1.5.4. Sertifika Uygulama Esasları Onay Prosedrleri

Bu SUE dokmanının yayımlanma onayı, Kamu SM ynetimi ve ynetim tarafından yetki verilen kiŐiler tarafından gerekleŐtirilen incelemelerden sonra verilir.

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

Anahtar ifti: Elektronik imza oluŐturmak amacıyla kullanılan zel anahtar ve ilgili aık anahtar. İmza oluŐturma ve dođrulama verileri.

Bilgi deposu: Sertifikaların, sertifika iptal durum kayıtlarının ve diđer sertifika iŐlemleri ile ilgili bilgilerin yayımlandıđı 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.

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

Güvenli elektronik 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 akıllı kart ya da benzeri güvenli taşınabilir 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.

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

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

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

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

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.

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

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

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

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

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

BS (British Standards): İngiliz Standartları

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

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

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliđi

KPS: Kimlik Paylaşım Sistemi

Kamu SM: Kamu Sertifikasyon Merkezi

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

2. Yayımlama ve Bilgi Deposu Yükümlülükleri

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

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

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin 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
- 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,
- Güncel Sertifika iptal listeleri.

2.3. Yayımlama Sıklığı ve Zamanı

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

NES'lerin yayımlanma sıklığı Bölüm 4.4.2'de belirtilmektedir.

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

2.4. Erişim Kontrolleri

Kamu SM bilgi deposu, bilgi edinme amaçlı olarak herkesin erişimine açıktır.

Bilgi deposunun güncellenmesi, yetkili personel tarafından gerçekleştirilmektedir.

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

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve deęiŐtirilmeye karŐı bütünlüğünü korumak,
- Bilgi deposunda tutulan bilgilerin doğruluęunu ve güncellięini saęlamak,
- Bilgi deposunun kesintisiz olarak erişilebilirlięini saęlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz saęlamak.

3. Kimlik Belirleme ve Doğrulama

NES'lerle ilgili işlemler yapılmadan önce, işlemi talep etmeye yetkisi olan kişi (kurum e-imza sorumlusu) ve 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 belirtildięi DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin destekledięi isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

NES içerięindeki isim alanına yazılan bilgiler kişiyi tanımlayan ve kişinin kimliğinin tespit edilmesini saęlayan niteliktedir; bu sebeple anlamlı olması gerekir. NES içerięine konulacak bilgiler; kişiyi teşhis edebilecek kimlik bilgilerinden oluşur.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika sahibinin NES'i içerięinde 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 Tekillięi

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

3.1.6. Markanın Tanınması, Doğrulaması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM'ye NES hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kişi, kurum e-imza sorumlusu 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.

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/taahhünameyle Kamu SM'ye bildirir. Kamu SM resmi yazıya istinaden kurum kimliğini belirler. Resmi yazıda/taahhünameyle Kamu SM sertifika işlemlerini kurum adına yürütecek kurum e-imza sorumlusu da belirlenerek Kamu SM'ye iletilir. Kurum e-imza sorumlusunun Kamu SM'ye gönderdiği elektronik imzalı belgeler de kurum kimliğinin belirlenmesi için kabul görür. Belge üzerindeki kurum e-imza sorumlusuna ait elektronik imzanın doğrulanması yoluyla kurum e-imza sorumlusunun 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 e-imza sorumlusunun elektronik veya ıslak imzalı 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 ünvanı 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.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de belirtildiği gibi yapılır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de belirtildiği gibi yapılır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2'de belirtildiği gibi yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

NES sahibi internet üzerinden işlem yaparak veya telefonla sesli yanıt sistemiyle çağrı merkezinden NES'inin iptal edilmesini isteyebilir.

İnternet üzerinden ve çağrı merkezinden iptal isteklerinin kabul edilebilmesi için sertifika sahibine ait kişisel bilgiler kullanılarak kimlik doğrulaması yapılır. Bunun için sertifika sahibinin kişisel bilgileri, Kamu SM sisteminde kayıtlı bulunan bilgilerle kıyaslanarak doğruluğu kontrol edilir.

Sertifika iptal isteği kurum tarafından resmi yazı ile ya da kurumun yetkilendirdiği kurum e-imza sorumlusu tarafından e-imzalı talep ile yapılabilir.

4. Sertifika Yaşam Döngüsü İşlevsel Gereklilikleri

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

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

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

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiđi

NES başvurusu, kamu kurum veya kuruluşları tarafından kurumsal olarak veya web servis ile kurumda çalıştığı doğrulanan kişiler tarafından bireysel olarak yapılabilir.

Kurumsal başvuru süreci Bölüm 3.2.2’de anlatıldığı şekilde başlatılır. Kurumun, sertifika başvuru işlemlerini kurum adına yürütecek bir veya daha fazla sayıda kurum e-imza sorumlusu görevlendirmesi ve kurum e-imza sorumlularını Kamu SM’ye resmi yazı/taahhütname ile bildirmesi zorunludur.

Kurum veya kurum adına işlem sağlayan kurum e-imza sorumlusu başvuru sırasında NES almak istediđi çalışanlarının başvuru bilgilerini Kamu SM’ye bildirir. Bildirimler resmi yazı ile veya kurum e-imza sorumlusunun elektronik imzasını taşıyan formun Kamu SM’ye elektronik ortamdan gönderilmesi ile yapılır. Kurum, çalışanın haberi olmadan çalışanı adına sertifika başvurusunda bulunamaz. Kurum çalışanın durumdan haberdar olması ve NES almayı kendisinin de talep etmesi gerekir. NES başvurusu, kurum çalışanı tarafından doldurulup imzalanan;

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

olarak hazırlanan sertifika başvuru formlarının Kamu SM’ye iletilmesi ile işleme alınır.

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

4.1.2. Kayıt İşlemleri ve Sorumluluklar

NES başvurusu, sertifika sahipleri adına sertifika sahiplerinin bađlı bulunduğu kamu kurum veya kuruluşu tarafından yapılır. Web servis ile kurumda çalıştığı doğrulanan kişiler bireysel başvuruda da bulunabilir.

Kurum, Kamu SM’den alacağı sertifika hizmetlerinin şartlarını TÜBİTAK BİLGEM ile karşılıklı imzalanan sözleşmelerle veya kurum tarafından onaylanan taahhütnamelerle ve Kamu SM’nin internet üzerinden yayımladığı ilgili yönergeler ile Sİ ve SUE dokümanları doğrultusunda belirler.

Kurum NES almak istediđi 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 iletişim bilgilerinin bulunduğu NES başvuru formunu doldurup imzalarlar. Başvuru formları kurum, kişi veya kurum e-imza sorumlusu tarafından, Kamu SM’ye iletilir. Bilgi ve belgelerin gizliliğinin sağlanması için belgelerin kapalı zarf içinde Kamu SM’ye iletilmesi gerekmektedir. Belgelerin Kamu SM’nin eline geçene kadarki zaman içerisinde gizliliğinin sağlanmasından kurum sorumludur.

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

Sertifika başvurusunda bulunan kişi başvuru sırasında, 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 veya yabancı kimlik no) adı, soyadı, kurumsal e-posta adresi, kurum birimi, sertifika üretim nedeni ve sertifika süresi bilgisinin bulunduğu liste,
- Pasaport numarası ile işlem yapılan yabancı uyruklu kişiler için pasaport sureti,

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

- Kurumdan gelen yazının ve formların e-imza sorumlusu/sorumluları tarafından gönderildiği kontrol edilir ve formların imzalı olup olmadığına bakılır.
- Kurum tarafından gönderilen NES alacak çalışanlar listesindeki T.C. kimlik no (yabancı uyruklular için pasaport no veya yabancı kimlik no), adı, soyadı, kurumsal e-posta adresi, kurum birimi, sertifika üretim nedeni ve sertifika süresi bilgisinin eksik olup olmadığına ve bu bilgilerin doğruluğuna bakılır.
- NES'te kullanılacak bilgilerin doğruluğu, KPS kullanılarak tespit edilir. Pasaportla işlem yapılacak yabancı uyruklu başvuru sahipleri için pasaport suretleri kontrol edilir.

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

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

Bölüm 4.2.1'deki kontrollerin yapılması sonucunda, sertifika başvurusu sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik bilgi veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyenlerle ilgili bilgilendirme, kurum e-imza sorumlusu ve/veya başvuru sahibi kişiye yapılır ve gerekli görülen bilgi ve belgeler tekrar talep edilir. Yazılı bilgilendirme, kuruma resmi yazı gönderme veya kurum e-imza sorumlusuna ve/veya başvuru sahibine e-posta gönderme yoluyla yapılır. Kurum e-imza sorumlusu ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Geçerli bulunan başvurular için sertifikalandırma süreci başlar.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Geçerli başvuru belgelerinin Kamu SM'ye ulaşmasının ardından sertifika başvurusu en kısa süre içerisinde 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. Kamu SM verdiği hizmetler kapsamında BTK tarafından 2007/DK-77/207 sayılı Kurul Kararı ile yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Profilleri" dokümanına uyar.

İmza oluşturma verisi, imza doğrulama verisi ve NES güvenli elektronik imza oluşturma aracına yüklenir. İmza oluşturma verisi, güvenli elektronik imza oluşturma aracı içinde saklanır ve kopyası sistemde tutulmaz. Güvenli elektronik imza oluşturma aracı erişim verisi web servis üzerinden sertifika sahibi tarafından oluşturulur ve Kamu SM tarafından saklanmaz.

Sertifika üretim süreci tamamlandıktan ve güvenli elektronik imza oluşturma aracına yazıldıktan sonra; bilgilendirme amaçlı dokümanlar 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. Sertifika teslim bilgisi Kamu SM tarafından kaydedilir.

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

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

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

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

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

4.4.2. Sertifikanın ESHS Tarafından Yayınlanması

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

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

4.4.3. Sertifikanın Oluşturulmasının Diğer Tarafra Duyurulması

Sertifikanın oluşturulması, kurumun talep etmesi durumunda, ESHS tarafından, internetten erişimi sağlanan raporlar ya da e-posta yolu ile kurum e-imza sorumlusuna 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 belirtildiđi 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.

4.6. Sertifika Süresinin Uzatılması

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

4.7. Sertifika Yenileme

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

Sertifika yenileme işlemleri Bölüm 4.1'de anlatılan ilk sertifika başvuru işlemleri ile aynıdır. Ancak yenilemede kurum ile Kamu SM arasında sertifika hizmetleri ile ilgili yeniden sözleşme imzalanmasına veya kurumdan taahhütname formu alınmasına gerek yoktur.

Yenilenecek sertifika bilgileri resmi yazıyla Kamu SM'ye bildirilebileceđi gibi, kurum e-imza sorumlusunun elektronik imzasını taşıyan yenileme yapılacak sertifika bilgilerinin bulunduđu formun Kamu SM'ye elektronik ortamdan gönderilmesi ile de yenileme 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 deđişikliği gerekmesi durumunda yapılmaktadır.

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi

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 Diđer Taraplara Duyurulması

Bölüm 4.4.3'te tanımlanmaktadır.

4.8. Sertifikada Bilgi Deđişikliği

Sertifikada bilgi deđişikliği, anahtar çifti hariç sertifikada yer alan bilgilerin deđişmesi olarak tanımlanmaktadır.

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

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

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildięi Durumlar

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

- Sertifika sahibinin talebi,
- Sertifika içeriğindeki bilgilerin sahtelięinin veya yanlışlıęının ortaya ıkması veya bilgilerin deęiŐmesi,
- Sertifika sahibinin fiil ehliyetinin sınırlandıęının, iflasının veya gaiplięinin ya da ölümünün öğrenilmesi,
- Sertifika sahibinin kurum ile iliŐięinin kesilmesinin bildirilmesi,
- İmza oluŐturma verisinin güvenlięinin kaybedildięinden Őüphelenilmesi,
- İmza oluŐturma verisinin iinde bulunduęu güvenli elektronik imza oluŐturma aracının kaybolması, alınması veya bozulması,
- Güvenli elektronik imza oluŐturma aracı eriŐim verisinden PUK'un kilitlenmesi.
- Sertifikanın NES Sahibi Taahhütnamesi, kurumile imzalanan sözleşmeler, Kurumsal Taahhütnamesi veya SUE dokümanında belirtilen Őartlara aykırı kullanımının tespit edilmesi,
- Sertifikanın hatalı üretilmesi,
- Kamu SM'nin NES'i imzalamak iin kullandıęı imza oluŐturma verisinin bütünlüęünün bozulması veya gizlilięinin ortadan kalkması,
- Kamu SM'nin iŐleyiŐine son verilmesi ve verilen NES'lerin yönetim iŐlemlerinin baŐka bir ESHS tarafından devamlılıęının saęlanamaması.

4.9.2. Sertifika İptal BaŐvurusunu Kimler Yapabilir

Sertifika iptal baŐvurusu aŐaęıda tanımlanan kiŐiler tarafından yapılabilir:

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

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

NES iptal başvurusu, sertifika sahibi tarafından telefonla sesli yanıt sistemiyle veya internet sitesi üzerinden Kamu SM'ye yapılır. İptal başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibinin kimlik belirlemesi ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan iptal başvuruları işleme alınmaz.

İnternet üzerinden yapılan iptal başvurusunda, sertifika sahibi <https://onlineislemler.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. Sesli yanıt sistemiyle kimlik doğrulama işleminin yapılmasının ardından NES iptal edilir.

İptal başvurularının nasıl yapılacağı Kamu SM'nin <https://kamusm.bilgem.tubitak.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 e-imza sorumlusunu NES'in iptal edildiğine dair bilgilendirir.

Kurum, çalışanlarına ait sertifikaları gerekli gördüğünde iptal ettirebilir. Kurum iptal edilmesini istediği sertifika bilgilerini Kamu SM'ye resmi yazı ile bildirerek ya da kurumun yetkilendirdiği kurum e-imza sorumlusunun imzalı liste göndermesi ile iptal talebinde bulunur. İptal talebinin Kamu SM'ye ulaşmasının ardından sertifika/sertifikalar iptal edilir. Sertifika sahibi ve kurum e-imza sorumlusu e-posta ile veya telefonla sertifikanın iptal edildiğine dair bilgilendirilir.

Kamu SM iptal bilgilerini en kısa sürede 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 Erteleme 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 en kısa sürede iptal eder. Kamu SM; iptal edilen NES bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 4.9.7'de belirtilmiştir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliđi

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

Üçüncü kişiler NES'lere dayanarak işlem yapmadan önce NES'lerin geçerliliđini 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 72 (yetmiş iki) saattir. Ancak bu sürenin dolması beklenmeden her 4 (dört) saatte bir SİL tekrar yayımlanır. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliđini korur.

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

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

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

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

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

SİL dosyası, iptal edilen her nitelikli elektronik sertifika için iptal bilgisinin eklenmesiyle gittikçe büyüyen bir dosya niteliğindedir. Güncel iptal durum kaydına her ihtiyaç duyulduğunda dosyanın Kamu SM bilgi deposundan indirilmesi gerekir. Gittikçe büyüyen SİL dosyasının sisteme getireceđi yüke karşılık ÇİSDUP, ilgili nitelikli elektronik sertifikanın iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle anlık olarak iletilmesine olanak tanımaktadır. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiđi ölçüde ÇİSDUP kullanmaları önerilir.

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. İmza oluŐturma Verisinin GüvenliĐini Yitirmesi Durumu

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

4.9.13. Sertifikanın Askıya AlındıĐı Durumlar

Sertifika sahibi tarafından NES'in geĐici olarak iptal edilebilmesi ve talep etmesi durumunda da kullanılabilir olması 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 olmasını gerektirecek bir durumun ortaya çıktığından Őüphelenmesi halinde, yanlıŐlıkla 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 internet sitesi üzerinden Kamu SM'ye yapılır. Askı baŐvurusu alındığında öncelikle baŐvuruyu yapan sertifika sahibinin kimlik belirlemesi ve doĐrulaması yapılır. Kimlik doĐrulaması yapılamayan askı baŐvuruları iŐleme alınmaz.

İnternet üzerinden yapılan askı baŐvurusunda, sertifika sahibi <https://onlineislemler.kamusm.gov.tr> internet adresi üzerinden sisteme giriŐ yaparak askı talebinde bulunur. İnternet üzerinden kimlik doĐrulama iŐleminin yapılmasıyla, NES Kamu SM sisteminde otomatik olarak askıya alınır.

Askıya alınan NES için, SİL'de geĐici 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 alındığına dair bilgilendirir.

Sertifika sahibi, internet üzerinden sertifikasını askıdan indirebilir. Askıya aldırdığı 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

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

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. İşletimsel Özellikleri

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

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

4.10.2. Servisin Erişilebilirliği

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

Ancak buna rağmen erişimin bir süreliğine kesilmiş olması durumunda üçüncü kişiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken işlemlerini durdurmaları önerilir. Üçüncü kişilerin iptal durum kaydını, erişimin kesilmesi sebebiyle kontrol etmeden yaptıkları işlemlerden doğan zararlardan Kamu SM sorumlu tutulamaz.

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

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 uygulanmaz.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM'ye ait sistemlerin kurulu olduđu cihazlara yetkisiz kişilerce erişim engellenir; hırsızlık, kaybolma gibi tehlikelere karşı gerekli önlemler alınır. Cihazların bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiđi, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır.

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM'ye ait yazılım ve donanım modüllerinin bulunduğu binalar, konum olarak güvenli, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiđi bir bölgededir.

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

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

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

5.1.2. Fiziksel Erişim

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

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

5.1.3. Güç Kaynağı ve Havalandırma

Aşağıdaki güç kaynakları Kamu SM işlevlerinin yerine getirilmesi ve sürekliliđi 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 getirildiđi ortamlarda su baskınlarından en az zarar göreceđ şekilde önlemler alınmıŐtır.

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduđu ve kullanılmayan elektronik veya kađıt ortamda tutulan bilgiler geri dönüşümsüz olarak yok edilir.

5.1.8. Farklı Mekanlarda Yedekleme

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

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

Kamu SM'de çalışan personelin rolleri aŐađıda belirtildiđi şekilde sınıflandırılmıŐtır:

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 bileŐenlerinin işletiminden, yedeklenmesinden ve kurtarma faaliyetlerinin yürütülmesinden sorumludur.

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

Sertifika Kayıt Sorumlusu: Sertifika üretim başvurusunun alınması, başvuru evraklarının ve kurum kimliđinin dođrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretiminden sorumlu 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 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 gereklereni sağlayabilecek nitelikte, bilgili ve deneyimli kişilerden seçilir. Kamu SM'nin istihdam ettirdiği personel sistem güvenliği, veri tabanı yönetimi, elektronik imza teknolojileri ve uygulamaları, sertifika yönetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kişilerden oluşur.

5.3.2. Geçmiş Araştırması

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

5.3.3. Eğitim Gerekleri

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

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

5.3.4. Sürekli Eğitim Gerekleri ve Sıklıđı

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

5.3.5. Görev Deđişim Sıklıđı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

5.3.7. Anlaşmalı Personel Gereksinimleri

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

5.3.8. Sağlanan Dokümantasyon

Dokümantasyon; çalışanların görevleri ve Kamu SM süreçleriyle ilgili kılavuz ve destek dokümanları, ilave olarak bilgi güvenliđi politikaları kapsamındaki dokümanlar ile sağlanmaktadır.

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

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

Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri

- Anahtar üretimi
- Anahtar yedekleme

- Anahtar dağıtımı
- Anahtar saklama
- Anahtar arşivleme
- Anahtar yok etme
- Kriptografik modül yaşam döngüsü işlemleri

NES üretim, yenileme, askıya alma ve iptal başvuruları

- Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
- Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
- Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
- Kağıt belgelerin kopyalarının nerede saklandığı bilgisi
- Geçerli ve geçersiz alınan tüm başvuru bilgileri

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
- NES iptal etme
- NES yayımlanması
- SİL yayımlanması
- ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtları

Güvenlikle ilgili diğer işlemler

- Sisteme başarılı veya başarısız tüm erişim denemeleri
- Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
- Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
- Güvenlik profili değişiklikleri
- Sistemin çökmesi, donanım hataları ve diğer bozukluklar
- Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
- Kamu SM'ye ziyaretçi girişi ve çıkışı

Kayıtlarda kayıt zamanı ve kaydın oluşmasına sebep olan çalışanın ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklığı

Sistemin işleyişiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. Buna ek olarak, sistemde olağandışı 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, sistemin veri depolama kapasitesine göre, sistemde erişilebilir olarak tutulur. Kayıtlar incelenmelerinden sonra en az 2 (iki) ay sistemde tutulur. Ancak, yasalar gereğince daha uzun süre saklanması gereken kayıtlar bu süre sonunda arşivlenir. Arşivlenen kayıtlar ile ilgili bilgilendirme Bölüm 5.5'te yapılmıştır.

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur. Kritik kayıtlar ayrı bir şehirde bulunan güvenli felaket kurtarma merkezlerine yedeklenmektedir.

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 girişi yaptıklarında kayıt hazırlar.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

Kayıt oluşmasına sebep olan işlemi başlatan Kamu SM sertifika yönetim sistemi kullanıcısı, kayıt 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 bağlı 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
- Kurumsal Taahhütname
- NES Sahibi Taahhütnameleri
- Kamu SM Taahhütnameleri

5.5.2. Arşivlerin Tutulma Süresi

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

5.5.3. Arşivlerin Korunması

Arşivlenen bilgi ve belgeler, izinsiz izlenmeyi, değiştirmeyi ve silinmeyi engelleyecek şekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz çalışanların erişimine kapalıdır. Arşivlerin tutulduğu 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 İş Sürekliliği Politikası gereğince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

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

5.6. Anahtar Değişimi

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

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

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

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

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

Güvenilirliğin 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.

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 OluŐturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin NES imzalamada kullandığı imza oluŐturma verisinin gizliliğinin kaybedildiğinden Őüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aŐağıdaki iŐlemler yerine getirilir:

- Kamu SM kendisine ait sertifikanın iptal edildiğini, iptal sebebi ile birlikte en hızlı Őekilde <https://kamusm.bilgem.tubitak.gov.tr> internet adresi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, NES sahiplerinin durumdan ne Őekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluŐturulan 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 oluŐturma verisinin yok edilmesi sürecini iŐletir.
- 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 ÇalıŐırlık

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

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

5.8. Sertifika Hizmetlerinin Sonlandırılması

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

6. Teknik Güvenlik Kontrolleri

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

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

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

Kamu SM bünyesinde aşağıdaki imza oluŐturma ve dođrulama verileri oluŐturulur:

- Kök SHS'ye ait imza oluŐturma ve dođrulama verisi
- Kamu ESHS'ye ait imza oluŐturma ve dođrulama verisi
- ÇİSDUP Yanıtlayıcı'ya ait imza oluŐturma ve dođrulama verisi

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

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

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

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliđi dünyaca kabul görmüş algoritmalar kullanılır. Anahtar çiftleri, RSA veya ECDSA algoritmaları kullanılarak üretilirler.

Sertifika sahibine ait imza oluŐturma verisinin yedeđi alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait imza oluŐturma verisinin saklandığı güvenli elektronik imza oluŐturma aracı Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine İmza OluŐturma Verisinin UlaŐtırılması

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

Akıllı kart erişim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bađlantı protokolleri (https) kullanılmaktadır. Sertifika sahibinin kimlik kontrolü için, T.C. kimlik no ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik dođrulaması sonrasında sertifika sahibi güvenli elektronik imza oluŐturma aracı erişim verisine erişir.

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

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

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

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

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

6.1.5. Anahtar Uzunlukları

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

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

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

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.

6.1.7. Anahtar Kullanım Amaçları

Kök SHS'ye ait imza oluşturma verisi; kendi sertifikasını, Kamu ESHS'ye ait sertifikayı, yayımladığı SİL dosyasını ve yürüttükleri görevler açısından özel niteliđi haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Dışişleri Bakanlığı ve BTK onayıyla kurulabilecek olan ESHS'lerin sertifikalarını imzalamak amacıyla kullanılır.

Kamu ESHS'ye ait imza oluşturma verisi; Kamu ESHS tarafından oluşturulan NES'lerin, ÇİSDUP Yanıtlayıcı sertifikasının ve yayımlanan SİL dosyalarının imzalanması amacıyla kullanılır. Kamu SM NES Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır.

ÇİSDUP Yanıtlayıcı'ya 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 dışında kullanmaz. Üçüncü kişiler, NES'ler içindeki imza doğrulama verilerini, sertifika sahibi tarafından oluŐturulmuş elektronik imzanın doğruluğunu kontrol etmek için kullanır. Anahtar çiftlerinin güvenli elektronik imza oluŐturma ve doğrulama dışında kullanımlarından doğan sorumluluk sertifika sahibine ve üçüncü kişilere aittir; Kamu SM bu durumda sertifika sahibinin veya üçüncü kişilerin gördükleri zarardan sorumlu tutulamaz.

6.2. İmza OluŐturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

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

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- İmza oluŐturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- EriŐim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.
- Sistem kullanıcılarına tanımlanan roller doğrultusunda, verdiđi hizmetlere erişimi sınırlar.
- Düzgün çalıştığı test edilebilir, test sırasında hata oluŐtuđuunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluŐturma verisinin içinde bulunduđu güvenli elektronik imza oluŐturma aracı, imza oluŐturma verisinin aracın dışına çıkmasını engelleyen ve araca erişimi parola ile sağlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluŐturma aracı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliğ'de belirtilen aşağıdaki güvenlik standartlarından en azından birisini sağlar:
 - FIPS PUB 140-2'ye göre seviye 3 veya üzeri,
 - CWA 14169 standardına uygun ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+.

6.2.2. İmza OluŐturma Verisine Birden Fazla KiŐi Kontrolünde EriŐim

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

6.2.3. İmza OluŐturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza OluŐturma Verisinin Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi iin sađlanan gvenlik ile eŐdeđer gvenlik nlemleri altında yapılır. Yedeklenen imza oluŐturma verisi yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak gvenli kriptografik donanım cihazı iinde tutulur. Gvenli donanım cihazı hazırda kullanılmakta olan imza oluŐturma verisinin bulunduđu ortam ile aynı gvenlik Őartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait imza oluŐturma verileri Kamu SM tarafından yedeklenmez.

6.2.5. İmza OluŐturma Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait imza oluŐturma verileri arŐivlenmez. Kullanım sreleri sonunda geri dnŐsz Őekilde silinir.

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

Kamu SM'ye ait imza oluŐturma verisi retildikten hemen sonra kriptografik modle yklenir. İŐlem, gvenilir yntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir.

Sertifika sahiplerine ait imza oluŐturma verileri, sadece yetkili personelin giriŐ izninin bulunduđu odalarda gvenli elektronik imza oluŐturma aracına, Őifrelenerek yklenir. İmza oluŐturma verisi gvenli elektronik imza oluŐturma aracına ykledikten sonra kopyası sistemden silinir.

6.2.7. İmza OluŐturma Verisinin Kriptografik Modlde Saklanması

Kamu SM'ye ait imza oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak gvenli kriptografik donanım cihazı iinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına ıkması engellenmiŐtir. İmza oluŐturma verisi kriptografik modl iinde gvenli algoritma ve yntemlerle Őifreli olarak saklanır.

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

6.2.8. İmza OluŐturma Verisine EriŐim

Kamu SM'nin imza oluŐturma verisine eriŐim birden fazla yetkili personelin ortak denetimi altındadır. İmza oluŐturma verisinin bulunduđu odaya giriŐ iin, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin dođrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin dođrulanamadığı durumlarda imza oluŐturma verisinin bulunduđu odaya eriŐim sađlanamaz.

İmza oluŐturma verisi kriptografik modl iinde Őifreli durumdayken eriŐime kapalıdır. EriŐime aılması iin eriŐimi sađlayan verinin modle sunulması gerekir. İmza oluŐturma verisinin eriŐime aılması ve kullanılır duruma getirilmesi birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahibine ait imza oluŐturma verisi gvenli elektronik imza oluŐturma aracı iinde sertifika sahibinin eriŐim verisi ile korunmuŐ olarak saklanır. EriŐim denetimi eriŐim denetim verisi ile sađlanır.

6.2.9. İmza OluŐturma Verisine EriŐimin Kesilmesi

Kamu SM'nin imza oluŐturma verisi imzalama iin kullanıldıktan sonra oturum kapandıėında veriye eriŐim otomatik olarak kesilir ve bir dahaki kullanımına kadar Őifrelenerek eriŐime kapalı tutulur. EriŐimin yeniden saėlanabilmesi iin Blm 6.2.8'de belirtilen yntemin 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 iin sertifika sahibinin eriŐim verisini yeniden girmesi gerekir. EriŐim verisinin ard arda 3 () defa yanlıŐ girilmesi durumunda güvenli elektronik imza oluŐturma aracı kilitlenir ve araca eriŐim saėlanamaz.

6.2.10. İmza OluŐturma Verisinin Yok Edilmesi

Kamu SM'ye ait imza oluŐturma verileri kullanım sresinin dolmasından sonra, aslı ve btn yedekleri buldukları ortamlardan uygun yntemlerle geri dnŐsz Őekilde silinir. Kamu SM'ye ait imza oluŐturma verisinin silinmesi iŐlemi iin Blm 6.2.8'de belirtilen Őekilde yeterli sayıda yetkili personelin hazır bulunması gerekir.

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

6.2.11. Kriptografik Modln Deėerlendirilmesi

Kamu SM, Blm 6.2.1'de belirtilen standartlara uygun kriptografik modl kullanır.

6.3. Anahtar ifti Ynetimiyle İlgili Diėer Konular

6.3.1. İmza Doėrulama Verisinin ArŐivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doėrulama verileri sertifikalar iinde tutulur ve NES'ler kullanım srelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arŐivlenir. ArŐivlenen veriler yetkisiz kiŐilerce tahrifatına ve silinmesine karŐı gerekli nlemlerin alındıėı ortamlarda tutulur.

6.3.2. İmza OluŐturma ve Doėrulama Verilerinin Kullanım Sreleri

İmza oluŐturma verisinin kullanım sresi, NES'in ieriėinde belirtilen NES kullanım sresi kadardır. NES'in kullanım sresinin dolmasıyla ya da NES'in iptal edilmesiyle imza oluŐturma verisinin kullanımı sona erer. Ancak, kullanım sresi dolsa bile NES'ler iindeki imza doėrulama verileri gemiŐe ynelik imzaların doėrulanabilmesi iin kullanılır.

Kamu SM'ye ve sertifika sahibine ait anahtar iftlerinin kullanım sresi, anahtar uzunlukları ve kullanılan imza algoritmasına gre belirlenir. Kamu SM'ye ait 384 bitlik ECDSA anahtar iftleri en fazla 10 (on) yıl iin kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar iftleri en fazla 3 () yıl iin kullanılır.

retilen NES'lerin son kullanma tarihi kendisine NES veren Kamu SM'ye ait SHS sertifikasının son kullanma tarihini aŐamaz.

6.4. EriŐim Denetim Verileri

Kamu SM alıŐanlarının eriŐim denetim verileri eriŐim parolalarını, güvenli donanım araları iindeki eriŐim denetimi saėlayan diėer verileri ve biyometrik verileri ierir.

Sertifika sahibine ait eriŐim denetim verisi güvenli elektronik imza oluŐturma aracı eriŐim verisini ierir.

6.4.1. EriŐim Denetim Verilerinin OluŐturulması

Kamu SM sistemi iinde kullanılan eriŐim denetim verileri yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli ortamlarda, sistem tarafından yeterli uzunlukta, tahmin edilemez nitelikte ve rastgele retilir.

Sertifika sahibine ait güvenli elektronik imza oluŐturma aracı eriŐim denetim verisi sertifika sahibinin kontrolnde retilir.

6.4.2. EriŐim Denetim Verilerinin Korunması

Kamu SM sistemi iinde kullanılan eriŐim denetim verileri yalnızca yetkili alıŐanlar tarafından bilinir.

Sertifika sahibine ait güvenli elektronik imza oluŐturma aracı eriŐim denetim verisini yetkisiz kiŐilerin eriŐimine karŐı korumak sertifika sahibinin ykmllė altındadır.

6.4.3. EriŐim Denetim Verileri İle İlgili Diėer Konular

Dzenlenmesine gerek duyulmamıŐtır.

6.5. Bilgisayar Gvenliėi Denetimleri

6.5.1. Bilgisayar Gvenliėi İle İlgili Teknik Gereker

Kamu SM sistemi iinde kt niyetli yazılımlara karŐı gereken nlemler alınır. Sistemde aė ve sunucu bazlı sensrler ieren saldırı tespit sistemi bulunmaktadır. Btn sunucular zerinde merkezden ynetilebilen virs tespit ve temizleme ajanları kurulmuŐtur. Kritik iŐlemlerin yapıldıėı bilgisayarlar aė ortamı dıŐında tutulur. Bilgilerin tahrifata, silinmeye ve kaaėa karŐı korunması ve iŐletimin srekliėinin saėlanması iin gerekli gvenlik saėlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin gvenliėi konusunda btn iyileŐtirme eylemleri gecikmesiz uygulanır.

6.5.2. Bilgisayar Sisteminin Saėladıėı Gvenlik Seviyesi

Dzenlenmesine gerek duyulmamıŐtır.

6.6. YaŐam Dngs Teknik Denetimleri

6.6.1. Sistem GeliŐtirme Denetimleri

Sistem geliŐtirilirken genel anlamda yapılan denetimler aŐaėıda verilmiŐtir:

- Yeterli dzeyde kalite ve gvenlik tedbirleri alınır.
- Belirlenen gvenlik kriterlerine uygun personel alıŐtırılır.
- 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, dışı açık ağa bağlantısında güvenlik duvarlarını kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi sunucuları mevcuttur.

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

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

6.8. Zaman Damgası

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

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

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan 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 Uzantı	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-1 özet çıktısından oluşur.
Sertifika Anahtar Tanımlayıcı ³	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

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/nes/NESIL.v6.crl
ESHS Erişim Bilgisi ⁶	HAYIR	http://depo.kamusm.gov.tr/nes/neshs.v6.crt http://ocsp6.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://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan NES ibaresine ait metni içerir.
Nitelikli Elektronik Sertifika İbaresini ⁸	HAYIR	ETSI 101 862’ye göre, id-etsi-qcs-QcCompliance= 0.4.0.1862.1.1 nesne tanımlama numarasını ve varsa sertifikanın kullanımına ilişkin maddi sınırlamaları içerir. BTK tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası bilgisini içerir.

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

Kamu SM tarafından kişilere verilen 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.

⁴ KeyUsage

⁵ CRLDistributionPoints

⁶ AuthorityInformationAccess

⁷ CertificatePolicies

⁸ QcStatement

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 Tanımlayıcı”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-ibaresi (1) nes-uygunlugu (1)}

NES’in ETSI’ye uygunluğunun gösterilmesi amacıyla ETSI tarafından tanımlanan aşağıdaki “İbare Tanımlayıcı” uzantısının içinde bulunur.

Nesne Tanımlama Numarası: 0.4.0.1862.1.1

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

Sertifikanın kullanımına ilişkin, varsa maddi sınırlamalar ile ilgili bilgilendirme “Nitelikli Sertifika İbaresini” uzantısı içinde ETSI TS 101 862’de belirtilen biçimde yapılır. Bu amaçla aşağıdaki “İbare Tanımlayıcı” kullanılır:

Nesne Tanımlama Numarası: 0.4.0.1862.1.2

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kişilere verdiği NES’leri imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.

Sertifika sahiplerine ait anahtar çiftleri RSA algoritmali 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.

7.1.5. İsim Kısıtları

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

⁹ StatementInfo

¹⁰ StatementId

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, yabancı kimlik numarası veya 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

Bağı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.1

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 İlkeleri¹⁴” uzantısının içinde yer alır. “Sertifika İlkeleri” uzantısının içinde “İlke Niteleyici¹⁵” olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

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

¹¹ CN: Common Name [Genel isim]

¹² Serial: Serial Number [Seri Numarası]

¹³ C: Country [Ülke]

¹⁴ Certificate Policies

¹⁵ Policy Identifier

Kamu SM tarafından kişilere verilen elektronik sertifikaların nitelikli olduğunu belirten ibare “Sertifika İlkeleri” uzantısı içindeki “Kullanıcı Bildirim¹⁶” alanında tanımlanır. Kamu SM tarafından tanımlanan NES ibaresi Kamu SM Sİ dokümanında verilmiştir.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

- SİL’i oluşturan Kamu SM’ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL’i imzalamak için SHA-384 özet algoritması ile ECDSA 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 (opsiyonel)
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM’ye ait sertifikanın “ESHS Anahtar Tanımlayıcı” numarası

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

¹⁶ User Notice

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

ÇİSDUP cevapları aşağıdaki bilgileri içermektedir:

- Versiyon bilgisi
- Yanıtlayıcı adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritmasının Nesne Tanımlama Numarası.
- ÇİSDUP Yanıtlayıcı imzası

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

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

Good [iyi]: Sertifika geçerli konumdadır.

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

Unknown [bilinmiyor]: Sorgusu yapılan sertifika hakkında herhangi bir bilgi bulunmamaktadır.

RFC 6960, ÇİSDUP sorguları ve yanıtları içerisinde bazı uzantıların kullanımına imkan verir. Tekrarlama (replay) saldırılarını önlemek için sorgu ve yanıt birbirine bağlayan "nonce" uzantısı bunlardan biridir. Kamu SM ÇİSDUP Yanıtlayıcı, "nonce" uzantısını desteklemektedir. RFC 6960'da belirtilen diğer uzantılar ÇİSDUP yanıt formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

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

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

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

8.1. Uygunluk Denetiminin Sıklığı

BTK gerekli gördüğü durumlarda re'sen denetim yapabilir.

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

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

8.2. Denetçinin Nitelikleri

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

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

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

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

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

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

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

8.4. Denetimin Kapsamı

Kamu SM'nin denetim kapsamı BTK tarafından belirlenir.

BGYS standardına uygun denetim kapsamı bağımsız kurum denetçisi tarafından belirlenir.

İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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

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

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

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

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

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

9.1.2. Sertifika EriŐim Ücreti

Kamu SM, kendisine ve izni dahilinde sertifika sahiplerine ait sertifikaları ücretsiz olarak yayımlar.

9.1.3. İptal Durum Kaydına EriŐim Ücreti

Kamu SM, iptal durum kaydını SİL veya İSDUP aracılıėıyla duyurma hizmeti için, sertifika sahibinden veya üçüncü kişilerden ücret talep etmez.

9.1.4. Diėer Servis Ücretleri

Sertifika yönetim prosedürleri içinde elektronik ortamdan ve aėrı merkezi üzerinden otomatik olarak gerekleŐtirilen işlemler için ücret talep edilmez.

Kamu SM tarafından üretilen NES'ler için ödenecek bedelin miktarı ile ilgili bilgilendirme e-posta ile yapılır. Ödemenin usulüne uygun biçimde yapılmaması durumunda NES üretimi yapılmayabilir.

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

9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi tamamlanmamıŐsa kurum/kiŐinin talebi doėrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu deėildir.

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 karŐılamak amacıyla sigortalanmamıŐtır.

9.2.2. Diėer Varlıklar

Düzenlenmesine gerek duyulmamıŐtır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doėan zararların karŐılanması amacıyla, ürettiėi NES'leri 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalar.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. Kişisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

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

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibinin başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan edilen 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 taraflar arası sözleşmelerde aksi belirtilmediđi sürece gizli deđildir.

9.4.4. Gizli Bilginin Korunma Sorumluluđu

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

Sertifika sahiplerinden başvuru sırasında ve daha sonra sertifika yaşam döngüsü içinde istenen bilgilere erişimin ve yetkisiz kullanımın engellenmesi ve mahremiyetinin korunması için, Kamu SM tarafından gerekli güvenlik tedbirleri alınır. Sadece yetkilendirilmiş çalışanlar sertifika sahiplerinin kişisel bilgilerine erişirler.

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

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

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

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHS olarak Kamu SM'nin yükümlülükleri şunlardır:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek,
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek,
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak,
- Kök SHS ve 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,
- NES başvurularını değerlendirerek, 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, sertifika sahibinin başvuru sırasında belirtmesi koşuluyla 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 işlemlerini yapmak,
- NES askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemlerini yapmak,
- NES askıdan indirme işlemlerini 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 Taahhütnamesi'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 tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurmak ve gazete ilanlarının bir örneğini BTK'ya iletmek.

9.6.2. Kayıt Birimi Yüklümlükleri

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

9.6.3. Sertifika Sahibinin Yüklümlükleri

Sertifika sahibinin yükümlükleri şunlardır:

- 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 aracını 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 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, varsa NES içerisinde belirtilen maddi sınırları aşan finansal işlemlerde kullanmamak.

Yukarıda beyan edilen yükümlüklerin 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,
- NES'in geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikaların 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 e-imza sorumlusu görevlendirmek ve resmi yazı/taahhütname ile kurum e-imza sorumlusunun bilgilerini Kamu SM'ye bildirmek,
- Kurum e-imza sorumlusunun görevini sonlandırdığında bunu Kamu SM'ye resmi yazı/taahhütname ile bildirmek,
- Yeni görevlendirdiği kurum E-İmza Sorumlusunun bilgilerini Kamu SM'ye resmi yazı/taahhütname ile bildirmek,
- Sertifika yönetim süreçleri ile ilgili varsa Kamu SM ile imzalanan sözleşmeye uymak,
- Sertifika yönetim süreçleri ile ilgili Kurumsal Taahhütname'deki yükümlülükleri yerine getirmek,
- Kamu SM'nin internet sitesi üzerinden yayımladığı Kurumsal Taahhütname ve E-imza Sorumlusu Taahhütname'si'ni doldurarak ilk sertifika başvurusu sırasında Kamu SM'ye iletmek.

9.6.5.2. Kurum E-İmza Sorumlularının Yükümlülükleri

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

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

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri veya sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları arasındaki yükümlülük, NES Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve varsa imzalanan sözleşmelerde belirtildiği 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, Kurumsal Taahhütname ve varsa imzalanan sözleşmelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diğer 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 Kurumsal Taahhütname ve varsa imzalanan sözleşmelere uygun olarak Kamu SM ile işbirliği içinde çalışır.

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

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ, SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği Kamu SM Taahhütnamesi, Kurumsal Taahhütname 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
- Sözleşmenin süresinin sona ermesi
- Her iki tarafın da ortak karar alarak sözleşmeyi bitirmesi
- Taraflardan birisinin sözleşmeye aykırı davranması: Taraflardan biri sözleşme kapsamında üzerine düşen yükümlülükleri yerine getirmez ise diğer taraf sözleşmeye aykırı davranan tarafa bu yükümlülüğü yerine getirmesi için 20 (yirmi) günlük süre verir. Bu sürenin sonunda da sözleşmeye aykırılık ortadan kaldırılamaz veya doğacak zarar, ziyan talepleri saklı kalmak kaydıyla yükümlülük yerine getirilmez ise sözleşme tek tarafı 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. Sertifika sahibinin NES Sahibi taahhütnamesinden, Sİ veya SUE dokümanlarından kaynaklanan yükümlülüklerini yerine getirmemesi durumunda Kamu SM sertifikayı iptal eder. Sertifika sahibinin taahhütnameye uygun hareket etmemesinden dolayı uğrayacağı zararlardan Kamu SM sorumlu tutulamaz.

Sözleşme ve taahhütnameler sona erse bile Kamu SM, dağıttığı 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'te 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 sağlanır. Kişinin NES başvuru formunda belirtilen e-posta adresine, değişmesi halinde yeni bildirdiği e- posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

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

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

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan 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, Kurumsal Taahhütname dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleridir.

9.14. Uygulanacak Hukuk

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

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM NES KÖK SERTİFİKASI

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

10.2. KAMU SM NES ALT KÖK SERTİFİKASI

Alan	Değer
Sürüm	V3
Seri Numarası	74d0e9d40224
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	19 Ocak 2020 Cuma 15:35:47
Geçerlilik Sonu	6 Ağustos 2029 Pazartesi 19:25:08
Konu	CN = Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Açık anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	Değer
Yetkili Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 42 fc 32 d4 7e 02 4e 49 a8 d5 e0 a0 35 b7 21 a8 5c 9e 84 37
Anahtar Kullanımı	Kritik=Evet ; Sertifika İmzalama, Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlar	Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0

Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.1.1 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyicisi= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyicisi= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/nes/kokshs.v6.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL= http://depo.kamusm.gov.tr/nes/kokshs.v6.crt

10.3. SON KULLANICI NES SERTİFİKA ŐABLONU

Alan	Deęer
Sürüm	V3
Seri Numarası	64 bit rastsal sayı içeren tam sayı
İmza Algoritması	SHA-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifika Vereni	CN = Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = Kamu Sertifikasyon Merkezi O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Sertifika Sahibinin Ad ve Soyadı Serial = Sertifika Sahibinin TC Kimlik Numarası C = TR
Açık anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	Deęer
Yetkili Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= 42 fc 32 d4 7e 02 4e 49 a8 d5 e0 a0 35 b7 21 a8 5c 9e 84 37
Konu Anahtar Tanımlayıcısı	Kritik=Hayır; Anahtar Kimliği= Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak deęerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	Kritik=Evet; Dijital İmzalama, İnkâr Edilemezlik
Temel Kısıtlar	Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok

Sertifika İlkeleri	<p>[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.1</p> <p>[1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke</p> <p>[1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni= Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.</p>
SİL Dağıtım Noktaları	<p>[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/nes/NESIL.v6.crl</p>
Yetkili Bilgi Erişimi	<p>[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/nes/neshs.v6.crt</p> <p>[2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1) Diğer Ad: URL=http://ocsp6.kamusm.gov.tr/</p>
Nitelikli Elektronik Sertifika İbaresı	<ul style="list-style-type: none"> Telekomünikasyon Kurumu Nitelikli Elektronik Sertifika İbaresı (2.16.792.1.61.0.1.5070.1.1) "Bu sertifika, Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır."