KAMU SM
SERTİFİKA İLKELERİ VE SERTİFİKA UYGULAMA ESASLARI (MOBİL İMZA KULLANIM AMAÇLI NİTELİKLİ ELEKTRONİK SERTİFİKALAR)

Doküman Kodu	Sürüm	Yayımlanma Tarihi
YONG-001-012	01	16.08.2011

DEĞİŞİKLİK KAYITLARI		
Sürüm	**Yayımlanma Sebebi**	**Yayımlanma Tarihi**
01	İlk sürüm	16.08.2011

CONTENTS

1. GİRİŞ 10
1.1. Genel bakış 10
1.2. Doküman adı ve tanımı 10
1.3. Açık anahtar altyapısı bileşenleri 11
1.3.1. Elektronik Sertifika Hizmet Sağlayıcılar 11
1.3.2. Kayıt makamları 11
1.3.3. Sertifika sahipleri 11
1.3.4. Üçüncü kişiler 11
1.3.5. Diğer bileşenler 11
1.4. Sertifika kullanımı 12
1.4.1. Uygun olan sertifika kullanımı 12
1.4.2. Yasaklanmış sertifika kullanımı 12
1.5. Sertifika ilkeleri yönetimi 12
1.5.1. Doküman yönetimi 12
1.5.2. İletişim bilgileri 12
1.5.3. Sertifika uygulama esaslarının ilkelere uygunluğunu belirleyen kişi 12
1.5.4. Sertifika uygulama esasları onay prosedürleri 12
1.6. Tanımlar ve kısaltmalar 13
1.6.1. Tanımlar 13
1.6.2. Kısaltmalar 14
2. YAYIMLAMA VE BİLGİ DEPOSU SORUMLULUKLARI 16
2.1. Bilgi deposu 16
2.2. Sertifika hizmetleri ile ilgili bilgilerin yayımlanması 16
2.3. Yayım zaman veya sıklığı 16
2.4. Bilgi deposu erişim kontrolleri 16
3. KİMLİK BELİRLEME VE DOĞRULAMA 16
3.1. İsimlendirme 16
3.1.1. İsim tipleri 16
3.1.2. İsimlerin anlamlı olması gerekliliği 17
3.1.3. Sertifika sahibinin takma isim veya lakap kullanması 17
3.1.4. Farklı isim alanı tiplerinin yorumlanması 17
3.1.5. İsimlerin benzersizliği 17
3.1.6. Ticari markanın tanınması, doğrulanması ve rolü 17
3.2. İlk kimlik belirleme 17
3.2.1. İmza oluşturma verisine sahip olmanın kanıtlanması 17
3.2.2. Kurumsal kimliğin belirlenmesi 17
3.2.3. Kişisel kimliğin belirlenmesi 17

3.2.4. Doğrulanmayan sertifika sahibi bilgileri 17
3.2.5. Yetkinin doğrulanması 18
3.2.6. Uyum kriterleri 18
3.3. Anahtar yenileme isteğinde kimlik doğrulama 18
3.3.1. Olağan anahtar yenileme isteğinde kimlik doğrulama 18
3.3.2. İptal sonrası anahtar yenileme için kimlik doğrulama 18
3.4. Sertifika iptal isteğinde kimlik doğrulama 18
4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEMSEL GEREKLER 19
4.1. Sertifika başvurusu 19
4.1.1. Kimler sertifika başvurusunda bulunabilir 19
4.1.2. Kayıt işlemleri ve sorumluluklar 19
4.2. Sertifika başvurusunun işlenmesi 19
4.2.1. Kimlik tanımlama ve doğrulama işlevlerinin yerine getirilmesi 19
4.2.2. Sertifika başvurusunun kabul veya reddi 20
4.2.3. Sertifika başvurusunun işlenme zamanı 20
4.3. Sertifikanın oluşturulması 20
4.3.1. Sertifika oluşturulmasında ESHS'nin işlevleri 20
4.3.2. Sertifika oluşturulması ile ilgili sertifika sahibinin bilgilendirilmesi 20
4.4. Sertifikanın kabulü 21
4.4.1. Sertifikanın kabul koşulu 21
4.4.2. Sertifikanın ESHS tarafından yayımlanması 21
4.4.3. Sertifikanın oluşturulmasının diğer taraflara duyurulması 21
4.5. Sertifikanın ve imza oluşturma verisinin kullanımı 21
4.5.1. Sertifika sahibinin sertifika ve imza oluşturma verisini kullanımı 21
4.5.2. Üçüncü kişilerin sertifika ve imza doğrulama verisini kullanımı 21
4.6. Sertifika süresinin uzatılması 21
4.7. Sertifika ve anahtar yenileme 21
4.7.1. Sertifika ve anahtar yenileme koşulları 22
4.7.2. Sertifika ve anahtar yenileme başvurusunu kimlerin yapabildiği 22
4.7.3. Sertifika ve anahtar yenileme başvurusunun işlenmesi 22
4.7.4. Sertifika ve anahtar yenileme ile ilgili sertifika sahibinin bilgilendirilmesi 22
4.7.5. Sertifika ve anahtar yenileme sonrası kabul koşulu 22
4.7.6. Sertifika ve anahtar yenileme sonrası sertifikanın yayımlanması 22
4.7.7. Sertifika ve anahtar yenilemenin diğer taraflara duyurulması 22
4.8. Sertifikada bilgi değişikliği 22
4.9. Sertifikanın iptali ve askıya alınması 22
4.9.1. Sertifikanın iptal edildiği durumlar 22
4.9.2. Sertifika iptal başvurusunu kimler yapabilir 23
4.9.3. Sertifika iptal başvurusunun işlenmesi 23

4.9.4. İptal isteği ertelenme süresi 24
4.9.5. İptal isteğinin işlenme süresi 24
4.9.6. Üçüncü kişilerin sertifika iptal durumunu kontrol gerekliliği 24
4.9.7. Sertifika iptal listesi yayımlama sıklığı 24
4.9.8. Sertifika iptal listesi yayımlama gecikme süresi 24
4.9.9. Çevrim içi sertifika iptal durum kaydı desteği 24
4.9.10. Çevrim içi sertifika iptal durum kaydı kontrol gereksinimi 24
4.9.11. Diğer sertifika durum bildirim yöntemleri 25
4.9.12. İmza oluşturma verisinin güvenliğini yitirmesi durumu 25
4.9.13. Sertifikanın askıya alındığı durumlar 25
4.9.14. Sertifika askıya alma başvurusunu kimlerin yapabildiği 25
4.9.15. Sertifika askıya alma başvurusunun işlenmesi 25
4.9.16. Askıda kalma süresi 25
4.10. Sertifika durum servisleri 26
4.10.1. İşletimsel özellikleri 26
4.10.2. Servisin erişilebilirliği 26
4.10.3. İsteğe bağlı özellikler 26
4.11. Sertifika sahipliğinin sona ermesi 26
4.12. İmza oluşturma verisi saklama ve yeniden oluşturma 26
5. Yönetim, işlemsel ve fiziksel kontroller 27
5.1. Fiziksel güvenlik denetimleri 27
5.1.1. Tesis yeri ve inşaatı 27
5.1.2. Fiziksel erişim 27
5.1.3. Güç kaynağı ve havalandırma 27
5.1.4. Su baskınları 27
5.1.5. Yangın önleme ve korunma 28
5.1.6. Saklama ve yedekleme ortamlarının korunması 28
5.1.7. Atıkların yok edilmesi 28
5.1.8. Farklı mekanlarda yedekleme 28
5.2. Prosedürsel kontroller 28
5.2.1. Güvenilir roller 28
5.2.2. Her işlem için gereken kişi sayısı 29
5.2.3. Her görev için kimlik doğrulama 29
5.2.4. Görevlerin ayrılmasını gerektiren roller 29
5.3. Personel güvenlik kontrolleri 29
5.3.1. Kişisel geçmiş, deneyim ve nitelik gerekleri 29
5.3.2. Geçmiş araştırması 29
5.3.3. Eğitim gerekleri 29
5.3.4. Sürekli eğitim gerekleri ve sıklığı 29
5.3.5. Görev değişim sıklığı ve sırası 29

5.3.6. Yetkisiz eylemlerin cezalandırılması 30
5.3.7. Anlaşmalı personel gereksinimleri 30
5.3.8. Personele sağlanan dokümantasyon 30
5.4. Denetim kayıtları 30
5.4.1. Kaydedilen işlemler 30
5.4.2. Kayıtların incelenme sıklığı 31
5.4.3. Kayıtların Saklanma Süresi 31
5.4.4. Kayıtların Korunması 31
5.4.5. Kayıtların Yedeklenmesi 31
5.4.6. Kayıtların Toplanması 32
5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi 32
5.4.8. Saldırıya Açıklığın Değerlendirilmesi 32
5.5. Kayıt arşivleme 32
5.5.1. Arşivlenen Kayıt Bilgileri 32
5.5.2. Arşivlerin Tutulma Süresi 32
5.5.3. Arşivlerin Korunması 32
5.5.4. Arşivlerin Yedeklenmesi 33
5.5.5. Kayıtların Zaman Damgası Gereksinimleri 33
5.5.6. Arşivlerin Toplanması 33
5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu 33
5.6. Anahtar değişimi 33
5.7. Güvenliğin yitirilmesi ve arıza durumunda yapılacaklar 33
5.7.1. Güvenilirliğin yitirilmesi durumunun düzeltilmesi 33
5.7.2. Donanım, yazılım veya veri bozulması 33
5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi 34
5.7.4. Arıza Sonrası Yeniden Çalışırlık 34
5.8. Sertifika hizmetlerinin sonlandırılması 34
6. TEKNİK GÜVENLİK KONTROLLERİ 36
6.1. Anahtar çifti üretimi ve kurulumu 36
6.1.1. Anahtar çifti üretimi 36
6.1.2. İmza oluşturma verisinin sertifika sahibine ulaştırılması 36
6.1.3. İmza doğrulama verisinin ESHS'ye ulaştırılması 36
6.1.4. ESHS sertifikalarına erişim sağlanması 36
6.1.5. Anahtar uzunlukları 36
6.1.6. Anahtar üretim parametreleri ve kalitesinin kontrolü 36
6.1.7. Anahtar kullanım amaçları 37
6.2. İmza oluşturma verisinin korunması ve Kriptografik modül kontrolleri 37
6.2.1. Kriptografik modül standartları ve kontroller 37
6.2.2. İmza oluşturma verisine birden fazla kişi kontrolünde erişim 37
6.2.3. İmza oluşturma verisinin yeniden elde edilmesi 37

6.2.4. İmza oluşturma verisinin yedeklenmesi 38
6.2.5. İmza oluşturma verisinin arşivlenmesi 38
6.2.6. İmza oluşturma verisinin kriptografik modüle yüklenmesi 38
6.2.7. İmza oluşturma verisinin kriptografik modülde saklanması 38
6.2.8. İmza oluşturma verisine erişim 38
6.2.9. İmza oluşturma verisine erişimin kesilmesi 38
6.2.10. İmza oluşturma verisinin yok edilmesi 39
6.2.11. Kriptografik modülün değerlendirilmesi 39
6.3. Anahtar çifti yönetimiyle ilgili diğer konular 39
6.3.1. İmza doğrulama verisinin arşivlenmesi 39
6.3.2. İmza oluşturma ve doğrulama verilerinin kullanım süreleri 39
6.4. Erişim denetim verileri 39
6.4.1. Erişim denetim verilerinin oluşturulması 39
6.4.2. Erişim denetim verilerinin korunması 40
6.4.3. Erişim denetim verileri ile ilgili diğer konular 40
6.5. Bilgisayar güvenliği denetimleri 40
6.5.1. Bilgisayar güvenliği ile ilgili teknik gerekler 40
6.5.2. Bilgisayar sisteminin sağladığı güvenlik seviyesi 40
6.6. Yaşam döngüsü teknik denetimleri 40
6.6.1. Sistem geliştirme denetimleri 40
6.6.2. Güvenlik yönetimi denetimleri 40
6.6.3. Yaşam döngüsü güvenlik denetimleri 40
6.7. Ağ güvenliği denetimleri 41
6.8. Zaman Damgası 41
7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ VE ÇİSDUP PROFİLLERİ 42
7.1. Sertifika profili 42
7.1.1. Sürüm numarası 42
7.1.2. Sertifika uzantıları 42
7.1.3. Algoritma nesne tanımlayıcıları 44
7.1.4. İsim biçimleri 44
7.1.5. İsim kısıtları 44
7.1.6. Sertifika ilkeleri nesne tanımlama numarası 45
7.1.7. İlke kısıtları uzantısının kullanımı 45
7.1.8. İlke niteleyiciler 45
7.1.9. Kritik belirlenmiş olan ilke belirleyici uzantılarının işlenmesi 45
7.2. Sertifika iptal listesi profili 45
7.2.1. Sürüm numarası 46
7.2.2. Sertifika iptal listesi uzantıları 46
7.3. ÇİSDUP profili 46

7.3.1. Sürüm numarası 46
7.3.2. ÇİSDUP uzantıları 46
8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER 47
8.1. Uygunluk denetiminin sıklığı 47
8.2. Denetçinin kimliği ve nitelikleri 47
8.3. Denetçinin denetlenen tarafla olan ilişkisi 47
8.4. Denetimin Kapsamı 47
8.5. Yetersizliğin tespiti durumunda yapılacaklar 47
8.6. Sonucun bildirilmesi 48
9. DİĞER İŞLER VE HUKUKSAL MESELELER 49
9.1. Ücretlendirme 49
9.1.1. Sertifika oluşturma ve yenileme ücreti 49
9.1.2. Sertifika erişim ücreti 49
9.1.3. İptal durum kaydına erişim ücreti 49
9.1.4. Diğer servis ücretleri 49
9.1.5. İade ücreti 49
9.2. Finansal sorumluluk 49
9.2.1. Sigorta kapsamı 49
9.2.2. Diğer varlıklar 49
9.2.3. Sertifika mali sorumluluk sigortası 50
9.3. Ticari bilginin korunması 50
9.3.1. Gizli bilginin kapsamı 50
9.3.2. Gizlilik kapsamında olmayan bilgiler 50
9.3.3. Gizli bilginin korunma sorumluluğu 50
9.4. Kişisel bilginin gizliliği 50
9.4.1. Gizlilik planı 50
9.4.2. Gizli olarak tanımlanan bilgiler 50
9.4.3. Gizli olarak tanımlanmayan bilgiler 50
9.4.4. Gizli bilginin korunma sorumluluğu 50
9.4.5. Gizli bilginin kullanımına izin verilmesi 51
9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması 51
9.4.7. Diğer Başlıklar 51
9.5. Telif hakları 51
9.6. Temsil hakkı ve yükümlülükler 51
9.6.1. Elektronik sertifika hizmet sağlayıcısı yükümlülükleri 51
9.6.2. Kayıt makamı yükümlülükleri 51
9.6.3. Sertifika sahibinin yükümlülükleri 52
9.6.4. Üçüncü kişilerin yükümlülükleri 52
9.6.5. Diğer bileşenlerin yükümlülükleri 52

9.7. Yükümlülüklerden feragat 52
9.8. Sorumlulukla ilgili sınırlamalar 52
9.9. Tazminat halleri 52
9.10. Sİ/SUE dokümanın geçerliliği ve geçerliliğinin sona ermesi 53
9.10.1. Sİ/SUE dokümanının geçerliliği ..... **Error! Bookmark not defined.**
9.10.2. Sİ/SUE dokümanının geçerliliğinin sona ermesi 53
9.10.3. Sİ/SUE dokümanının geçerliliğinin sona ermesinin etkileri 53
9.11. Bireysel bildirimler ve katılımcılar ile iletişim 53
9.12. Değişiklik halleri 53
9.12.1. Değişiklik metodları 53
9.12.2. Bilgilendirme mekanizması ve sıklığı 53
9.12.3. Nesne tanımlama numarasının değişmesini gerektiren durumlar 53
9.13. Anlaşmazlık halleri 53
9.14. Uygulanacak hukuk 54
9.15. Uygulanabilir yasalarla uyum 54
9.16. Çeşitli hükümler 54
9.17. Diğer hükümler 54

EK-A Sertifika biçimleri 55

a) CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 55
b) CN = KamuSM Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 2 55

1. GİRİŞ

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) Mobil imza kullanım amaçlı Nitelikli Elektronik Sertifika (MNES) hizmeti verirken uyguladığı esasları tanımlayan Sertifika İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE) dokümanıdır. Mobil imza deyimi, nitelikli elektronik sertifika sahibi tarafından, mobil iletişim cihazları ve ilgili iletişim/hizmet altyapısı kullanılarak oluşturulan güvenli elektronik imzayı tanımlamaktadır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Bilgi Teknolojileri ve İletişim 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.

Bu Sİ/SUE dokümanı şunları içerir:

- Kamu SM'nin ESHS olarak operasyonlarını gerçekleştirmek amacıyla oluşturduğu altyapı ve iş sürekliliğini sağlamak için uyguladığı prosedürler,
- Kök Sertifika ve kullanıcı sertifikalarının oluşturulması, yönetilmesi ve iptal edilmesi sırasında uygulanan prosedürler,
- Kamu SM'nin sahip olduğu özel anahtarların korunması amacıyla uygulanan fiziksel ve mantıksal güvenlik önlemleri.

Bu Sİ/SUE dokümanı sadece mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için geçerlidir. Kamu SM'den MNES talep etmiş olan başvuru sahipleri bu Sİ/SUE'de belirtilen hususları kabul etmiş sayılırlar.

1.1. Genel bakış

Bu Sİ/SUE dokümanı, Kamu SM açık anahtar altyapısı bileşenlerini tanımlar ve sertifika başvurusunun alınması, başvuru sahipleri için sertifika oluşturulması, yönetilmesi ve iptal edilmesi sırasında uygulanan politika ve prosedürleri anlatır.

Sİ/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.

1.2. Doküman adı ve tanımı

Bu dokümanın adı kapak sayfasında belirtildiği şekliyle "Kamu SM Sertifika İlkeleri ve Sertifika Uygulama Esasları (Mobil Imza kullanım amaçlı Nitelikli Elektronik Sertifikalar)" olarak tanımlanmıştır. Kamu SM tarafından bu Sİ/SUE'ye gore oluşturulan bütün kullanıcı sertifikaları, RFC 5280 bölüm 4.2.1.4 de belirtildiği şekliyle, sertifika içerisinde yer alan sertifika ilkeleri alanında aşağıdaki nesne tanımlama numarasını (OID) ve sertifika ilkelerinin cpsURI alt alanında bu Sİ/SUE web adresini içerecektir.

Bu Sİ/SUE dokümanına bağlı olarak oluşturulan sertifikalar tarafından kullanılan nesne tanımlama numarası (OID) 2.16.792.1.2.1.1.5.7.1.8 dir.

Sİ/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.

1.3. Açık anahtar altyapısı bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcılar

Kamu SM, mobil imza kullanım amaçlı nitelikli elektronik sertifika hizmetlerini sağlamak amacıyla aşağıdaki Kök ve alt kök sertifika hizmet sağlayıcıları kullanır.

Kök Sertifika Hizmet Sağlayıcısı
CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 Geçerlilik başlangıç tarihi : 11 Nisan 2011 Pazartesi 14:35:26 SHA1 Özeti : ea df 38 1a 51 df e4 28 94 0d 18 8e 01 7c 72 4f c9 96 8f 04

Alt Kök Elektronik Sertifika Hizmet Sağlayıcısı
CN = KamuSM Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 2 Geçerlilik başlangıç tarihi : 12 Nisan 2011 Salı 16:12:00 SHA1 Özeti: 7b 81 03 a5 4c 7e 13 52 a1 b7 db e9 c3 da 27 21 ff e4 93 60

1.3.2. Kayıt makamları

Mobil imza kullanım amaçlı nitelikli elektronik sertifika başvurularını ve ilgili belgeleri alan, başvuruları usulü dairesinde inceleyerek kabul, onay ve reddeden, sertifika iptal, yenileme ve askı taleplerini alan bunları usulü dairesinde inceleyerek kabul, onay ve reddeden, bahsi geçen onay ve red kararlarını usulü dairesinde Kamu SM'nin yetkili birimlerine ve/veya "Sertifika Sahibi"ne bildiren, yapmış olduğu tüm işlemlere ilişkin her türlü kaydı ve belgeyi düzenli olarak tutan ve bunları 20 (yirmi) yıl süre ile arşivleyen ve "KM" yükümlülüklerini Kamu SM ile aralarında akdedilen protokol koşulları dahilinde tam ve eksiksiz olarak yerine getiren tüzel kişiliktir.

1.3.3. Sertifika sahipleri

Kamu SM tarafından oluşturulan sertifikaların içeriğinde kimlik bilgileri 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.

1.3.5. Diğer bileşenler

Düzenlenmesine gerek duyulmamıştır.

1.4. Sertifika kullanımı

1.4.1. Uygun olan sertifika kullanımı

Kamu SM'nin kişiler adına ürettiği MNES güvenli elektronik imza uygulamalarında kullanılır. MNES 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.

Nitelikli elektronik sertifika içeriğindeki imza doğrulama verisi güvenli elektronik imzayı doğrulamak için kullanılır.

1.4.2. Yasaklanmış sertifika kullanımı

Uygun olan sertifika kullanımı bölüm 1.4.1'de tanımlanmıştır. Diğer kullanım şekilleri yasaklanmıştır.

1.5. Sertifika ilkeleri yönetimi

1.5.1. Doküman yönetimi

Bu Sİ/SUE dokümanı Kamu SM tarafından hazırlamıştır. Kamu SM, gerekli gördüğü durumlarda değişiklik yapabilir.

1.5.2. İletişim bilgileri

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

Adres : TÜBİTAK BİLGEM, PK. 74, 41470 Gebze-KOCAELİ
Tel : (262) 648 18 18
Faks : (262) 648 18 00
E Posta : bilgi@kamusm.gov.tr
URL : **Error! Hyperlink reference not valid.**

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

http:/depo.kamusm.gov.tr/ilke/mobilnes

1.5.3. Sertifika uygulama esaslarının ilkelere uygunluğunu belirleyen kişi

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

1.5.4. Sertifika uygulama esasları onay prosedürleri

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

1.6. Tanımlar ve kısaltmalar

1.6.1. Tanımlar

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

Başvuru sahibi: Mobil İmza kullanım amaçlı nitelikli elektronik sertifika almak için başvuruda bulunan kamu kurum ve kuruluşu çalışanları.

Bilgi deposu: Sertifika hizmetleri ile ilgili bilgileri internet üzerinden herkesin erişimine açık olarak yayımlamaya imkan veren web sayfaları ya da LDAP dizinleri.

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

Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt. Bu dokümanda bahsi geçen elektronik sertifika ya da sertifika ibaresi mobil imza kullanım amaçlı nitelikli elektronik sertifikayı ifade etmek amacıyla kullanılmıştır.

Güvenli elektronik imza: Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp 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 verisinin içinde bulunduğu taşınabilir güvenli cihaz. Bu Sİ/SUE kapsamında güvenli elektronik imza oluşturma aracı sertifika sahibi tarafından kullanılan cep telefonu içerisindeki SIM karttır.

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

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

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

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

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

Kayıt Makamı: Mobil imza kullanım amaçlı nitelikli elektronik sertifika başvurularını ve ilgili belgeleri alan, başvuruları usulü dairesinde inceleyerek kabul, onay ve reddeden, sertifika iptal, yenileme ve askı taleplerini alan bunları usulü dairesinde inceleyerek kabul, onay ve reddeden, bahsi geçen onay ve red kararlarını usulü dairesinde Kamu SM'nin yetkili birimlerine ve/veya "Sertifika Sahibi"ne bildiren, yapmış olduğu tüm işlemlere ilişkin her türlü kaydı ve belgeyi düzenli olarak tutan ve bunları 20 (yirmi) yıl süre ile arşivleyen ve "KM" yükümlülüklerini Kamu SM ile aralarında akdedilen protokol koşulları dahilinde tam ve eksiksiz olarak yerine getiren tüzel kişiliktir.

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

Kurum Yetkilisi: Kamu kurumları ile yapılan sözleşmelerde belirlenen ve MNES ile ilgili süreçlerde kurumu temsile yetkili kişi.

Mobil imza: Mobil imza kullanım amaçlı nitelikli elektronik sertifika sahibi tarafından, mobil iletişim cihazları ve ilgili iletişim/hizmet altyapısı kullanılarak oluşturulan güvenli elektronik imza.

Mobil operatör: Mobil imza kullanım amaçlı nitelikli elektronik sertifika sahiplerine, sahip olduğu GSM altyapısı üzerinden işlem yapma imkanı sağlayan taraftır.

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. Bu dokümanda bahsi geçen nitelikli elektronik sertifika (NES) ibaresi mobil imza kullanım amaçlı nitelikli elektronik sertifika (MNES) ile aynı anlamı ifade etmektedir.

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

Sertifika sahibi: Kamu SM'den mobil imza kullanım amaçlı nitelikli elektronik sertifika alan gerçek kişi.

Son Kullanıcı: Kamu SM sisteminde kimlik doğrulaması yapılmış ve sertifika almak üzere tanımlanmış kişiler. Sertifika sahibi olan kişiler, aynı zamanda Kamu SM son kullanıcılarıdır.

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

BTK	Bilgi Teknolojileri ve İletişim Kurumu
CEN	European Standardization Committee / Avrupa Standardizasyon Komitesi
CP/Sİ	Certificate Policy / Sertifika İlkeleri
CPS/SUE	Certificate Practice Statement / Sertifika Uyuglama Esasları
CRL / SİL	Certificate Revocation List / Sertifika İptal Listesi
CSR	Certificate Signing Request / Sertifika İmzalama İsteği
CWA	CEN Workshop Agreement / CEN Çalıştay Kararı
EAL	Evaluation Assurance Level / Değerlendirme Garanti Düzeyi
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
ETSI	European Telecommunications Standards Institute / Avrupa Telekomünikasyon Standartları Enstitüsü
ETSI TS	ETSI Technical Specification / ETSI Teknik Özellikleri

FIPS	Federal Information Processing Standards / Federal Bilgi İşleme Standartları
GSM	Global System for Mobile Communications / Mobil İletişim için Küresel Sistem
HSM	Hardware Security Module / Güvenlik Donanım Modülü
HTTP	Hypertext Transport Protocol / Hiper Metin Aktarım İletişim Kuralı
HTTPS	Secure Hypertext Transport Protocol using SSL,TLS / Güvenli Hiper Metin Aktarım İletişim Kuralı
IETF RFC	Internet Engineering Task Force Request for Comments / Internet Mühendisliği Görev Grubu Yorum Talebi
IP	Internet Protocol / İnternet Protokolü
ISO/IEC	International Organization for Standardization, International Electro technical Committee / Uluslararası Standardizasyon Teşkilatı, Uluslarası Elektroteknik Komitesi
ITU	International Telecommunications Union / Uluslararası Telekomünikasyon Birliği
Kamu SM	Kamu Sertifikasyon Merkezi
RA/KM	Registration Authority / Kayıt Makamı
LDAP	Lightweight Directory Access Protocol / Dizin Erişim Protokolü
MNES	Mobil imza kullanım amaçlı nitelikli elektroniik sertifika
NES	Nitelikli Elektronik Sertifika
OCSP (ÇİSDUP)	Online Certificate Status Protocol / Çevrim İçi Sertifika Durum Protokolü
OID	Object Identifier / Nesne Tanımlama Numarası
PIN	Personal Identification Number / Kişisel Kimlik Numarası
PKI	Public Key Infrastructure / Açık Anahtarlı Altyapılar
RSA	Rivest, Shamir, Adleman (Algoritmayı bulan kişilerin baş harfleri)
SHA	Secure Hash Algorithm / Güvenli Özet Algoritması
SSL	Secure Sockets Layer / Güvenli Yuva Katmanı
S/MIME	Secure/Multipurpose Internet Mail Extensions
URL	Uniform Resource Locator / Bir örnek kaynak konumlayıcı

2. YAYIMLAMA VE BİLGİ DEPOSU SORUMLULUKLARI

2.1. Bilgi deposu

Bilgi Deposu, sertifika hizmetleri ile ilgili bilgileri internet üzerinden herkesin erişimine açık olarak yayımlamaya imkan veren web sayfaları ya da LDAP dizinleridir.

Kamu SM aşağıdaki bilgileri herkesin erişebileceği şekilde web sayfasından ya da LDAP dizinlerinden yayımlar.

- Kök sertifikalar ve özet değerleri,
- Sertifika iptal durum kayıtları,
- Kamu SM Sİ/SUE dokümanları,
- Elektronik imza ile ilgili mevzuat, taahütnameler, sözleşmeler, formlar ve sertifika hizmetleri ile ilgili diğer dokümanlar,

2.2. Sertifika hizmetleri ile ilgili bilgilerin yayımlanması

Kamu SM, bölüm 2.1'de belirtilen bilgileri aşağıdaki Bilgi Depoları'ndan yayımlar.

- http://www.kamusm.gov.tr/BilgiDeposu
- http://depo.kamusm.gov.tr

2.3. Yayım zaman veya sıklığı

- Yeni bir kök sertifika ve özet değeri, oluşturulduğu an yayımlanır,
- Sertifika iptal listesi yayımlama sıklığı bölüm 4.9.7 de belirtilmiştir,
- Sİ/SUE dokümanları güncellendikleri anda yayımlanırlar,
- Elektronik imza ile ilgili mevzuat, taahütnameler, sözleşmeler, formlar ve sertifika hizmetleri ile ilgili diğer dokümanlar güncellendikleri anda yayımlanırlar,

2.4. Bilgi deposu erişim kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır. Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM personeli tarafından gerçekleştirilir. Kamu SM, bilgi deposunda yer alan bilgilerin yetkisiz olarak silinmesini ve değiştirilmesini önlemek amacıyla gerekli önlemleri alır.

3. KİMLİK BELİRLEME VE DOĞRULAMA

3.1. İsimlendirme

3.1.1. İsim tipleri

MNES içeriğindeki DN (Distinguished Name (Ayırt edici isim)) alanı içerisinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır. DN alanı X.501 printableString formatındadır ve boş değildir.

3.1.2. İsimlerin anlamlı olması gerekliliği

MNES içeriğindeki isim alanına yazılan bilgiler kişiyi tanımlayan ve kişinin kimliğinin tespit edilmesini sağlayan niteliklerdir. Bu nedenle anlamlı olması gerekmektedir.

3.1.3. Sertifika sahibinin takma isim veya lakap kullanması

Sertifika sahibinin MNES içeriğinde takma isim veya lakap kullamasına izin verilmez.

3.1.4. Farklı isim alanı tiplerinin yorumlanması

MNES içeriğinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. İsimlerin benzersizliği

Oluşturulan MNES içeriğindeki kimlik bilgileri her kişi için ayırt edici niteliktedir. Aynı kişiye ait sertifikaların içeriğindeki kimlik bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kişilere ait sertifikaların içeriğindeki kimlik bilgilerinin aynı olması engellenmektedir. Bunun sağlanabilmesi için sertifikaların isim alanı içinde benzersiz bir sayı olduğu kabul edilen, sertifika sahibinin T.C. kimlik numarası yer alır. Yabancı uyruklu sertifika sahipleri için isim alanı içinde pasaport numarası yer alır.

3.1.6. Ticari markanın tanınması, doğrulanması ve rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk kimlik belirleme

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

3.2.1. İmza oluşturma verisine sahip olmanın kanıtlanması

İmza oluşturma ve doğrulama verileri başvuru sahibinin SIM kartında oluşturulduğu için sertifika başvuru sahibinin imza oluşturma verisine sahip olduğunun kanıtlanması gerekir. Sertifika başvuru sahibinin imza oluşturma verisi tarafından imzalanmış bir verinin, ilgili imza doğrulama verisi kullanılarak doğrulanması neticesinde imza oluşturma verisine sahiplik kanıtlanır.

3.2.2. Kurumsal kimliğin belirlenmesi

Çalışanları adına MNES başvurusunda bulunan kurumlar, Kamu SM tarafından istenen kurum bilgilerini kurumu temsile yetkili kişilerin imzaladığı ve kurumun onayını taşıyan resmi yazıyla Kamu SM'ye bildirir. Kamu SM resmi yazıya istinaden kurum kimliğini belirler.

3.2.3. Kişisel kimliğin belirlenmesi

Mobil imza kullanım amaçlı nitelikli elektronik sertifika başvuru sahiplerinin kimlik bilgilerinin resmi belgelere dayanarak doğrulanması gereklidir. Bu amaçla, kayıt makamları tarafından, başvuru sahibine ait nüfus cüzdanı, sürücü belgesi ya da pasaport gibi resmi kimlik belgelerinden biri başvuru sırasında kontrol edilerek kimlik doğrulaması gerçekleştirilir. Kayıt makamı ilgili belgenin fotokopisini alır.

3.2.4. Doğrulanmayan sertifika sahibi bilgileri

Sertifika sahibi veya kurum tarafından başvuru sırasında ve daha sonra değişiklik sebebiyle beyan edilen aşağıdaki erişim bilgilerinin doğruluğu Kamu SM tarafından doğrulanmaz.

- Telefon numaraları

- Faks numaraları
- Adres bilgisi
- Sertifika sahibinin elektronik posta adresi

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

Başvuru sahibi 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

MNES başvurusunda bulunan kurumların imzaladıkları talep formunda, MNES başvuru listelerinin oluşturulması amacıyla yetkilendirilmiş kurum yetkilisi belirlenir. Kurum adına, sadece belirlenen kurum yetkilisi başvuru işlemlerini gerçekleştirebilir.

3.2.6. Uyum kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Anahtar yenileme isteğinde kimlik doğrulama

3.3.1. Olağan anahtar yenileme isteğinde kimlik doğrulama

Anahtar yenileme, sertifika içerisindeki kişisel bilgiler değişmeden, yeni bir anahtar çifti kullanılarak farklı bir seri numarasına sahip yeni bir sertifika oluşturulması anlamına gelmektedir.

Olağan anahtar yenileme isteğinde kimlik doğrulama, mobil operatör tarafından sertifika sahibine gönderilen sertifika yenileme talebinin mobil imza ile imzalanması ve imzanın doğrulanması ile gerçekleştirilir.

3.3.2. İptal sonrası anahtar yenileme için kimlik doğrulama

İptal sonrası anahtar yenileme isteğinde kimlik doğrulama, ilk başvuru sırasındaki yöntemler uygulanarak gerçekleştirilir.

3.4. Sertifika iptal isteğinde kimlik doğrulama

Sertifika sahibi, sertifika iptal talebini mobil operatör çağrı merkezi üzerinden sesli olarak ya da kayıt makamları aracılığıyla kağıt üzerinde ıslak imzalı form kullanarak yazılı olarak gerçekleştirebilir. Çağrı merkezi üzerinden gerçekleştirilen iptal taleplerinde kimlik doğrulama amacıyla sertifika sahibine ait kişisel bilgiler kullanılır. Kağıt üzerinde ıslak imzalı form ile yapılan iptal taleplerinde kimlik doğrulaması ıslak imzanın doğruluğunun kontrolü ve/veya resmi kimlik belgelerinin kontrolü ile yapılır.

4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEMSEL GEREKLER

4.1. Sertifika başvurusu

4.1.1. Kimler sertifika başvurusunda bulunabilir

MNES başvurusu, kurum veya kuruluşlar tarafından Kamu SM'ye kurumsal olarak yapılır. Kurum çalışanı, kurumun talebi olmadan bireysel olarak MNES başvurusunda bulunamaz. Aynı şekilde kurum, çalışanının haberi olmadan çalışanı adına sertifika başvurusunda bulunamaz. Kurum çalışanının durumdan haberdar olması ve sertifika almayı kendisinin talep etmesi gerekir. Bu talep, kurum çalışanı tarafından doldurulup imzalanan sertifika başvuru formunun Kamu SM'ye iletilmesi ile yapılır.

4.1.2. Kayıt işlemleri ve sorumluluklar

MNES başvurusu, sertifika sahipleri adına sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurum, alacağı ürün ve hizmetler için Ürün/Hizmet Talep Formu'nu doldurarak Kamu SM'ye resmi yazı ekinde iletir.

Kurum sertifika almak istediği personelinin listesini, personelin kimliklerinin belirlenmesi için istenen bilgilerle birlikte Kamu SM'ye gönderir. Başvurunun işleme alınabilmesi için sertifika alacak olan çalışanlar, kişisel bilgileri ile adres, telefon numarası gibi erişim bilgilerinin bulunduğu başvuru formunu doldurup ıslak imza ile imzalarlar. Başvuru formları kurumun yetkilendirdiği kişi 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 geçinceye kadarki zaman içerisinde gizliliğinin sağlanmasından kurum sorumludur.

Kurum ve sertifika 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 sertifikanın kullanımıyla ilgili maddi sınıra ilişkin bilgilendirmeyi Kamu SM'ye yapar. MNES başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kamu SM, sertifika oluşturulacak kişilerin kimlik belirlemelerini yaptıktan sonra başvuruları değerlendirmeye alır ve uygun görülen başvuruları kimlik doğrulaması amacıyla kayıt makamlarına yönlendirir. Başvuru sahibinin kimliği, kayıt makamları tarafından resmi kimlik belgeleri kullanılarak doğrulanır.

4.2. Sertifika başvurusunun işlenmesi

4.2.1. Kimlik tanımlama ve doğrulama işlevlerinin yerine getirilmesi

Sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşu tarafından gönderilen belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama işlevleri yerine getirilir. Bu kapsamda aşağıdaki belgeler incelenir:

- Kamu kurum veya kuruluşu tarafından gönderilen MNES alacak çalışanların, T.C. kimlik no (yabancı uyruklular için pasaport no), ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgisinin bulunduğu liste,
- MNES alacak çalışanların ıslak imzasını taşıyan başvuru formları,
- Yabancı uyruklular için noter onaylı pasaport sureti,

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

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

Bilgi ve belgeler hatasız ve tam ise kimlik tanımlama işlevi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik onay ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kimlik tanımlama yapılamaz. Bu durumda; Kamu SM, ilgili kurum yetkilisine hataları bildirir ve gerekli görülen bilgi ve belgeleri tekrar talep eder.

Yukarıdaki adımların tamamlanmasının ardından başvuru sahibi kendisine en yakın kayıt makamına gider ve resmi kimlik belgelerinini beyan ederek içerisinde imza oluşturma ve doğrulama verisinin oluşturulacağı SIM kartı teslim alır.

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, kurumun yetkili kıldığı kişiye ve/veya başvuru sahibi kişiye yapılır. Yazılı bilgilendirme, kuruma resmi yazı gönderme veya kurum yetkilisine ve/veya başvuru sahibine e-posta gönderme yoluyla yapılır. Sözlü bilgilendirme kurum yetkilisine ve/veya başvuru sahibine telefon açılarak yapılır. Sözlü bildirimler kayıt altına alınır. Kurum ve başvuru sahibine ait e-posta ve telefon bilgileri başvuru sırasında beyan edilen bilgilerdir. Gereken düzeltmeler yapılıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilenler Kamu SM sisteminde tanımlanır ve nitelikli elektronik sertifika üretim süreci başlatılır.

4.2.3. Sertifika başvurusunun işlenme zamanı

Başvuru ile ilgili geçerli tüm belgelerin Kamu SM'nin eline geçmesinin ardından en fazla 1 (bir) ay içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın oluşturulması

4.3.1. Sertifika oluşturulmasında ESHS'nin işlevleri

Mobil imza kullanım amaçlı nitelikli elektronik sertifika, başvuru sahibinin SIM kartında oluşturularak Kamu SM'ye ulaştırılmış olan olan imza doğrulama verisi ve sistemde onayı verilmiş kimlik bilgilerinin Kamu SM'ye ait imza oluşturma verisi ile imzalanması suretiyle üretilir. Nitelikli elektronik sertifikalar ETSI TS 101 862, ITU-T X.509 v.3 standartlarına ve Kanunun 9'uncu maddesinde belirtilen niteliklere uygun olarak üretilir.

4.3.2. Sertifika oluşturulması ile ilgili sertifika sahibinin bilgilendirilmesi

Sertifikanın oluşturulması ile ilgili bilgilendirme kısa mesaj servisi ya da e-posta yolu ile yapılır.

4.4. Sertifikanın kabulü

4.4.1. Sertifikanın kabul koşulu

Oluşturulan MNES'lerin sertifika sahibi tarafından kabul edildiğinin Kamu SM'ye bildirilmesi gerekmez. Sertifikanın oluşturulmasına müteakip 5 (beş) iş günü içerisinde sertifika içeriğinde hatalı olduğu düşünülen alanları da içerecek şekilde bir itiraz yapılmaması durumunda sertifika kabul edilmiş sayılır.

4.4.2. Sertifikanın ESHS tarafından yayımlanması

Mobil imza kullanım amaçlı sertifikalar herkesin erişimine açık dizin yada web servisi üzerinden yayımlanmaz.

4.4.3. Sertifikanın oluşturulmasının diğer taraflara duyurulması

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

4.5. Sertifikanın ve imza oluşturma verisinin kullanımı

4.5.1. Sertifika sahibinin sertifika ve imza oluşturma verisini kullanımı

Sertifika sahibi, imza oluşturma verisini bu Sİ/SUE dokümanına uygun olarak ve elektronik imza mevzuatında belirtildiği şekilde güvenli elektronik imza uygulamalarında kullanır.

İmza oluşturma verisi, sertifika geçerlilik süresi içinde, sertifika içeriğinde yer alan anahtar kullanımı, gelişmiş anahtar kullanımı ve para limiti alanlarına uygun olarak kullanılır.

4.5.2. Üçüncü kişilerin sertifika ve imza doğrulama verisini kullanımı

Sertifika sahibine ait nitelikli elektronik sertifikaların içinde yer alan imza doğrulama verileri, üçüncü kişilerce elektronik imzalı verilerin imzasının doğrulanması amacıyla kullanılır. İmza doğrulama verilerinin üçüncü kişilerce, güvenli elektronik imza doğrulama dışında kullanılması sonucu oluşabilecek zararlardan üçüncü kişiler sorumludur.

4.6. Sertifika süresinin uzatılması

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

4.7. Sertifika ve anahtar yenileme

Anahtar yenileme, sertifika içerisindeki kişisel bilgiler değişmeden, yeni bir anahtar çifti kullanılarak farklı bir seri numarasına sahip yeni bir sertifika oluşturulması anlamına gelmektedir.

Sertifika sahibi, mevcut sertifikasının kullanım süresi dolmadan önce sertifika ve anahtar yenileme talebinde bulunabilir. Bu amaçla, mobil operatör tarafından kendisine gönderilen sertifika yenileme talebini mobil imza ile imzalayarak talebini iletir. Yenileme talebinin imzasının doğrulanmasının ardından sertifika ve anahtar yenileme süreci başlatılır. Sertifika sahibi bölüm 4.7.1 de belirtilen durumlarda ilk başvuru sürecini işleterek yenileme talebinde bulunabilir.

4.7.1. Sertifika ve anahtar yenileme koşulları

Sertifika sahibi geçerli bir sertifikaya sahip, imza oluşturma verisini kullanabilir durumda ve çalıştığı kamu kurumu tarafından kendisi için sertifika yenileme onayı verilmiş ise sertifika ve anahtar yenileme talebini mobil imza kullanarak gerçekleştirebilir. Aşağıdaki koşulların ortaya çıkması durumunda ise ilk başvuru sürecindeki adımlar işletilir.

- Güvenli elektronik imza oluşturma aracının kayıp edilmesi, veya çalınması durumunda,
- Güvenli elektronik imza oluşturma aracının arızalanması durumunda,
- Sertifikanın iptal edilmesi ve yenisinin talep edilmesi durumunda,
- Sertifikanın geçerlilik süresinin sona ermesi durumunda,
- Sertifikada bilgi değişikliği gerekmesi durumunda,

4.7.2. Sertifika ve anahtar yenileme başvurusunu kimlerin yapabildiği

Geçerli bir sertifikaya sahip olan ve çalıştığı kamu kurumu tarafından kendisi için sertifika ve anahtar yenileme onayı verilmiş sertfika sahibi tarafından yapılabilir.

4.7.3. Sertifika ve anahtar yenileme başvurusunun işlenmesi

Mobil imza kullanılarak gerçekleştirilen sertifika ve anahtar yenileme başvuru talebi doğrulanarak işleme alınır.

4.7.4. Sertifika ve anahtar yenileme ile ilgili sertifika sahibinin bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika ve anahtar yenileme sonrası kabul koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika ve anahtar yenileme sonrası sertifikanın yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika ve anahtar yenilemenin diğer taraflara duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.

4.8. Sertifikada bilgi değişikliği

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

Sertifikada yer alan Ad, Soyad, T.C Kimlik No, Para Limiti Değeri, Doğum Tarihi bilgilerinde değişiklik olması sertifikada bilgi değişikliği gerektirmektedir. Kamu SM, sertifikada bilgi değişikliği gerçekleştirmez. Bilgi değişikliğinin gerekli olduğu durumlarda, yeni bir anahtar çifti ve sertifika üretilir.

4.9. Sertifikanın iptali ve askıya alınması

4.9.1. Sertifikanın iptal edildiği durumlar

Sertifikanın, kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda, sertifika iptal edilir. İptal edilen sertifika ile bir daha işlem yapılmaz. Sertifika, aşağıda belirtilen durumlarda iptal edilir:

- Sertifika sahibinin talebi,

- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflasının veya gaipliğinin ya da ölümünün öğrenilmesi,
- Sertifika sahibinin kurum ile ilişiğinin kesilmesinin bildirilmesi,
- İmza oluşturma verisinin güvenliğinin kaybedildiğinden şüphelenilmesi,
- İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, çalınması veya bozulması,
- Sertifikanın Sertifika Sahibi Taahhütnamesi ve Sİ/SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Kamu SM'nin sertifikayı imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması,
- Kamu SM'nin işleyişine son verilmesi ve verilen sertifikaların yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması.

4.9.2. Sertifika iptal başvurusunu kimler yapabilir

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir:

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

4.9.3. Sertifika iptal başvurusunun işlenmesi

Sertifika sahibi, sertifika iptal talebini mobil operatör çağrı merkezi üzerinden sesli olarak ya da kayıt makamları aracılığıyla kağıt üzerinde ıslak imzalı form kullanarak yazılı olarak gerçekleştirebilir. Bölüm 3.4'te belirtilen kimlik doğrulama adımlarının başarılı bir şekilde tamamlanmasından ardından iptal başvurusu yapılan sertifika ile ilgili bilgiler mobil operatör tarafından Kamu SM'ye iletilir ve iptal işlemi Kamu SM tarafından gerçekleştirilir.

Kurum yetkilisi tarafından resmi yazı ile bildirilen iptal başvuruları Kamu SM tarafından gerçekleştirilir.

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

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

Sertifika iptal başvuruların nasıl yapılacağı Kamu SM web sitesinde ayrıntılı olarak anlatılır. Geçmiş tarihe yönelik olarak sertifika iptal edilmez. Sertifika iptal başvurusu sırasında iptal sebebi sertifika sahibi tarafından belirtilir. Nitelikli elektronik sertifika iptal edildikten sonra, Kamu SM

sertifika sahibini ve gerekirse bağlı bulunduğu kurum tarafından yetkilendirilen kişiyi nitelikli elektronik sertifikanın iptal edildiğine dair bilgilendirir.

4.9.4. İptal isteği ertelenme süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal isteğinin işlenme süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve nitelikli elektronik sertifikayı iptal eder. İptal edilen nitelikli elektronik sertifika 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 iptal durumunu kontrol gerekliliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına herkes erişebilir. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

Üçüncü kişiler nitelikli elektronik sertifikalara dayanarak işlem yapmadan önce nitelikli elektronik sertifikaların geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

Üçüncü kişiler nitelikli elektronik sertifika 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 iptal listesi yayımlama sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 36 (otuzaltı) saattir. Ancak bu sürenin dolması beklenmeden SİL yayım zamanından sonra her 10 (on) dakikada bir SİL tekrar yayımlanır. Gün içinde yeni bir nitelikli elektronik sertifika iptali olmasa dahi SİL 10 (on) dakika da bir güncellenir. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduğu SİL dosyası 3 (üç) ayda bir yenilenir. Sertifikanın iptali durumunda SİL dosyası derhal yenilenir.

4.9.8. Sertifika iptal listesi yayımlama gecikme süresi

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

4.9.9. Çevrim içi sertifika iptal durum kaydı desteği

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

ÇİSDUP desteği olan uygulamalar nitelikli elektronik sertifikanın geçerlilik durum kontrolünü ESHS Erişim Bilgisi sertifika uzantısında yer alan adres üzerinden gerçekleştirir.

4.9.10. Çevrim içi sertifika iptal durum kaydı kontrol gereksinimi

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

SİL dosyası, iptal edilen her 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 getireceği yüke karşılık, ÇİSDUP ilgili nitelikli elektronik sertifikanın iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır.Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiği ölçüde ÇİSDUP kullanmaları gerekir.

4.9.11. Diğer sertifika durum bildirim yöntemleri

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

4.9.12. İmza oluşturma verisinin güvenliğini yitirmesi durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunda nitelikli elektronik sertifika iptal edilir. Nitelikli elektronik sertifikanın iptal edilmesi dışında herhangi bir husus uygulanmamaktadır.

4.9.13. Sertifikanın askıya alındığı durumlar

Nitelikli elektronik sertifikanın geçici bir süre için iptal durumunda olup sürenin sonunda yeniden kullanılabilir olmasını sağlamak amacıyla askıya alma işlemi tanımlanmıştır.

Sertifika sahibi, aşağıda belirtilenlere benzer sebeplerden dolayı nitelikli elektronik sertifikasını askıya almak isteyebilir:

- Sertifika sahibinin bir süreliğine görev başında olmaması ve nitelikli elektronik sertifikasını kullanım dışı bırakmak istemesi,
- Nitelikli elektronik sertifikanın iptal sebebinin ortaya çıktığından şüphelendiği halde, yanlışlıkla iptalini engellemek amacıyla, nitelikli elektronik sertifikayı önce askıya almak istemesi.

4.9.14. Sertifika askıya alma başvurusunu kimlerin yapabildiği

Nitelikli elektronik sertifika askıya alma başvurusu sertifika sahibi ve kurum yetkilisi tarafından yapılabilir.

4.9.15. Sertifika askıya alma başvurusunun işlenmesi

Sertifika sahibi, askı talebini mobil operatör çağrı merkezi üzerinden sesli olarak ya da kayıt makamları aracılığıyla kağıt üzerinde ıslak imzalı form kullanarak yazılı olarak gerçekleştirebilir. Kimlik doğrulama adımlarının başarılı bir şekilde tamamlanmasından ardından askı başvurusu yapılan sertifika ile ilgili bilgiler mobil operatör tarafından Kamu SM'ye iletilir ve askı işlemi Kamu SM tarafından gerçekleştirilir.

Askıya alınan nitelikli elektronik sertifika için, SİL'de tanımlı geçici olarak iptal edildiğini belirten ifade kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, nitelikli elektronik sertifika askıya alındıktan sonra, gerekli gördüğü durumlarda sertifika sahibini ve bağlı bulunduğu kurum tarafından yetkilendirilen kişiyi sertifikanın askıya alındığına dair bilgilendirir.

4.9.16. Askıda kalma süresi

Böyle bir süre öngörülmemiştir.

4.10. Sertifika durum servisleri

4.10.1. İşletimsel özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. 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. Üçüncü kişiler nitelikli elektronik sertifika veya sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin erişilebilirliği

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

4.10.3. İsteğe bağlı özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika sahipliğinin sona ermesi

Nitelikli elektronik sertifikanın kullanım süresinin dolması, iptal edilmesi ya da Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM nitelikli elektronik sertifikanın 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 bilgilendirmez. Sertifika sahibi nitelikli elektronik sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. İmza oluşturma verisi saklama ve yeniden oluşturma

Sertifika sahiplerine ait imza oluşturma verilerinin Kamu SM tarafından saklanması ve yeniden oluşturulması işlemi uygulanmamaktadır.

5. Yönetim, işlemsel 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 bilgi sistemleri bileşenlerinin bulunduğu binalar ve odalar, giriş ve çıkışların kontrol edildiği, yetkisiz kişilerin girişini engelleyen güvenlik önlemleri ile donatılmıştır.

5.1.1. Tesis yeri ve inşaatı

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

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

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

5.1.2. Fiziksel erişim

Kamu SM bilgi sistemleri bileşenleri ve arşivlere erişim denetim altındadır. Binaya girişler güvenlik görevlilerinin kontrolü altında, gelişmiş erişim kontrol cihazlarıyla sağlanmaktadır.

Bina içinde Kamu SM'ye ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kağıt ortamdaki bilgilerin tutulduğu, sistemin işletildiği ve yönetildiği odalara erişim gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Her çalışan sadece yetkisi bulunduğu odalara erişebilmektedir. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

5.1.3. Güç kaynağı ve havalandırma

Kamu SM faaliyetlerinin yerine getirilmesi ve sürekliliği için aşağıdaki güç kaynakları 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'nin faaliyetini sürdürdüğü ortamlarda su baskınlarından en az zarar görecek şekilde önlemler alınmıştır.

5.1.5. Yangın önleme ve korunma

Kamu SM'nin faaliyetini sürdürdüğü ortamlarda yangını önleyici ve olası yangınlarda zararı en aza indirecek önlemler alınmıştır.

5.1.6. Saklama ve yedekleme ortamlarının korunması

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

5.1.7. Atıkların yok edilmesi

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

5.1.8. Farklı mekanlarda yedekleme

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

5.2. Prosedürsel kontroller

5.2.1. Güvenilir roller

Kamu SM'de çalışan personelin rolleri aşağıda belirtildiği şekilde sınıflandırılmıştır:

Kamu SM Yöneticisi: Kamu SM iç işleyişinin yürütülmesini, Kamu SM'nin yasal yükümlülüklerinin yerine getirilmesini, talimat ve politikaların uygun olarak kullanılmasını, gerekli gördüğü durumlarda değişiklik ve düzenlemelerin yapılmasını sağlar.

Kamu SM Teknik Sorumlusu: Kamu SM birimleri arasında teknik uyumun gerçekleşmesini sağlar. Teknik faaliyetleri gözden geçirir. Bilgi sistemlerinin güvenliğini ve performansını izler.

Güvenlik Yöneticisi: Kamu SM güvenlik yöntemleri ve politikalarının uygulanmasını takip eder. Zaman içinde sistemin güvenlik ihtiyaçlarını belirler ve bu ihtiyaçların giderilmesini koordine eder.

Güvenlik İşletmeni: İşletmen sınır güvenliği ile ilgili varlıkların işlerliğinden sorumludur. Güvenlik duvarları, saldırı tespit sistemi, kayıt sistemi ve antivirüs sistemi idamesini sağlar.

Sistem Yöneticisi: Güvenlik bileşenleri hariç bütün sistemin işletiminden sorumludur. Sistemde zaman içerisinde yapılması gereken değişiklikleri koordine eder.

Sistem İşletmeni: Bütün sunucuların işletim sistemi ve donanım idamesinden sorumludur. Bileşenlerle ilgili gerekli güncellemeleri yapar.

Veri Sistemleri Yöneticisi: Veritabanı yığınlarının (cluster) yönetimini yapar. Veritabanı yönetim faliyetlerini gerçekleştirir, gerekli raporların hazırlanmasını sağlar.

Sertifika Üretim Ekip Lideri: Sertifikanın üretiminin planlanması ve gerçekleştirilmesi ilgili tüm çalışmaları yapar, sertifika üretim işletmenlerini koordine eder.

Sertifika Üretim İşletmeni: Nitelikli elektronik sertifika yaşam döngüsü işlemlerini gerçekleştirir. Sertifika yaşam döngüsü süreçleri kapsamında gelen ve giden evrakları kontrol eder.

Denetçi: Yönetim tarafından TÜBİTAK BİLGEM içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından görevlendirilen bir kişi olan denetçi, sistem denetim

profilinin kurulması, denetimlerin yönetimi ve gözden geçirilmesi ile sistemin teknik ve idari işleyişinin kontrolü ve raporlarının hazırlanmasından sorumludur.

5.2.2. Her işlem için gereken kişi sayısı

Kamu SM, kök ve alt kök imza oluşturma ve doğrulama verilerinin üretilmesi, sertifikaların oluşturulması ve iptal edimesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, kök ve alt kök imza oluşturma verilerinin başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

5.2.3. Her görev için kimlik doğrulama

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 bilgi sistemlerinde kimlik doğrulama, güvenli donanım araçları, parolalar, gizli sorular ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır.

5.2.4. Görevlerin ayrılmasını gerektiren roller

Tanımlanan roller içinde sertifika işletmenleri dışındakiler için bir kişi birden fazla rolden sorumlu olabilir.

5.3. Personel güvenlik kontrolleri

5.3.1. Kişisel geçmiş, deneyim ve nitelik gerekleri

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

5.3.2. Geçmiş araştırması

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

5.3.3. Eğitim 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 işleyişi, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır.

5.3.4. Sürekli eğitim gerekleri ve sıklığı

Kamu SM bilgi sistemleri bileşenlerinde yapılan değişikliklerin bildirilmesi amacıyla personele verilen eğitimler gerekli görüldükçe tekrarlanır. Yeni göreve başlayanlar için eğitimler düzenlenir.

5.3.5. Görev değişim sıklığı ve sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz eylemlerin cezalandırılması

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

5.3.7. Anlaşmalı personel gereksinimleri

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

5.3.8. Personele sağlanan dokümantasyon

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

5.4. Denetim kayıtları

Kamu SM işleyişi sırasında gerçekleştirilen anahtar ve sertifika yönetimi, sistemin güvenliği ile ilgili işlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diğer bir kısmı ise kağıt üzerindedir. Denetimler sırasında gerekli görüldüğü takdirde bu kayıtlar görevliler tarafından incelenir.

5.4.1. Kaydedilen işlemler

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

- Kamu SM kök ve alt kök ahtarlarının yaşam döngüsü yönetimi işlemleri
  - Anahtar üretimi
  - Anahtar yedekleme
  - Anahtar dağıtımı
  - Anahtar saklama
  - Anahtar arşivleme
  - Anahtar yok etme
  - Kriptografik modül yaşam döngüsü işlemleri
- Nitelikli elektronik sertifika 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
- Nitelikli elektronik sertifika yaşam döngüsü yönetimi işlemleri
  - Nitelikli elektronik sertifika başvurusunun işlenmesi

- Nitelikli elektronik sertifika üretimi
- Nitelikli elektronik sertifika yenileme
- Nitelikli elektronik sertifika askıya alma
- Nitelikli elektronik sertifika askıdan çıkarma
- Nitelikli elektronik sertifika iptal etme
- Nitelikli elektronik sertifika yayımlanması
- SİL yayımlanması
- ÇİSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtları

- Güvenlikle ilgili diğer işlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar

Kayıtlarda kayıt zamanı ve kaydın oluşmasına sebep olan çalışanın ismi bulunur

5.4.2. Kayıtların incelenme sıklığı

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

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

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

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

- Kayıtlar yetkisi olan personel tarafından oluşturulur.
- Yetkisi olmayan kişiler elektronik kayıtların bulunduğu sistemlere erişemezler.
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunurlar.
- 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.

5.4.6. Kayıtların Toplanması

Kayıtlar uygulama katmanında, ağ katmanında ve işletim seviyesi düzeyinde otomatik olarak toplanır.

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

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

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

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

5.5. Kayıt arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

Bölüm 5.4.1'de belirtilen kayıtlara ek olarak nitelikli elektronik sertifika başvurusu ve nitelikli elektronik sertifika 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
- Nitelikli elektronik sertifika yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Nitelikli elektronik sertifika işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm nitelikli elektronik sertifikalar
- Geçerlilik süresi dolan tüm kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Nitelikli elektronik sertifika yönetim prosedürleri
- Sertifika 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 iş 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:

- Kök sertifika kullanım süresinin dolmasından en geç 18 (onsekiz) ay önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış nitelikli elektronik sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyası aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş nitelikli elektronik sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalamaya devam eder. Yeni üretilen nitelikli elektronik sertifikalar için oluşturulan SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.

Kamu SM anahtarlarının yenilendiği bilgisini http://www.kamusm.gov.tr internet adresi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

5.7. Güvenliğin yitirilmesi ve arıza durumunda 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. İş sürekliliğin sağlanması amacıyla alınan günlük yedekler ihtiyaç durumunda tekrar geri yüklenir.

5.7.2. Donanım, yazılım veya veri bozulması

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

İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır. Depolama ünitesi fiziksel olarak farkı bir noktada bulunan veri depolama ünitesi ile veri senkronizasyonu yapabilecek niteliktedir. Arızanın giderilmesi süreci arıza

sebebinin araştırılmasını, hatanın giderilmesini ve gerekli görüldüğünde Kamu SM hizmetlerini güvenilir yedek ortama aktarmayı içerir.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin mobil imza kullanım amaçlı nitelikli elektronik sertifika imzalamada kullandığı imza oluşturma verisinin gizliğinin kaybedildiğinden şüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aşağıdaki işlemler yerine getirilir:

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

5.7.4. Arıza Sonrası Yeniden Çalışırlık

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

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

5.8. Sertifika hizmetlerinin sonlandırılması

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

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün kurumlara yazı ile, sertifika sahiplerine e-posta ile duyurur.
- Sertifika hizmetlerine son vereceği bilgisini internet sitesi üzerinden ve ulusal yayın yapan en yüksek tirajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurur.
- Sertifika hizmetlerine son vereceğini duyurmasından itibaren sertifika başvurusu kabul etmez ve yeni sertifika oluşturmaz.
- Dağıttığı nitelikli elektronik sertifikaları iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği nitelikli elektronik sertifikaların bilgisini kurumlara yazılı olarak, sertifika sahiplerine e-posta ile duyurur.

- İptal ettiği nitelikli elektronik sertifikaların kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı imza oluşturma verisine karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Nitelikli elektronik sertifikaları imzalamak için kullandığı imza oluşturma verisini imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde 20 (yirmi) yıl boyunca korur.

6. TEKNİK GÜVENLİK KONTROLLERİ

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

6.1. Anahtar çifti üretimi ve kurulumu

6.1.1. Anahtar çifti üretimi

Kök ve alt kök sertifika hizmet sağlayıcılara ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği odada, birden fazla eğitimli personelin gözetiminde, güvenli anahtar üretimi için gereken testlerden geçmiş, güvenli yazılım kullanılarak üretilir. Üretilen imza oluşturma verisi güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personeller tarafından onaylanır. İmza oluşturma verisinin saklandığı kriptografik modül Bölüm 6.2.1'de belirtilen standartlara uyar.

Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için anahtar çifti üretimi başvuru sahibinin SIM kartında gerçekleştirilir.

6.1.2. İmza oluşturma verisinin sertifika sahibine ulaştırılması

Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için anahtar çifti üretimi başvuru sahibinin SIM kartında gerçekleştiği için sertifika sahibi imza oluşturma verisine anahtar üretimi gerçekleştiği anda sahip olur.

6.1.3. İmza doğrulama verisinin ESHS'ye ulaştırılması

Mobil imza kullanım amaçlı nitelikli elektronik sertifika başvurusunda, başvuru sahibi tarafından SIM kart üzerinde üretilen imza doğrulama verisi sertifika üretimi için mobil imza hizmet altyapısı üzerinden Kamu SM'ye ulaştırılır.

6.1.4. ESHS sertifikalarına erişim sağlanması

Kamu SM kendisine ait kök ve alt kök sertifikaları internet ortamında bilgi deposu üzerinden üçüncü tarafların erişimine hazır bulundurur. Kök ve alt kök sertifikasının özet değeri ve özet algoritması sertifikaların oluşturulmasına müteakip 7 (yedi) gün içinde ulusal yayın yapan en yüksek trajlı 3 (üç) gazetede ilan vermek suretiyle kamuoyuna duyurulur.

6.1.5. Anahtar uzunlukları

Kamu SM'ye ait kök, alt kök ve ÇİSDUP yanıtlayıcı RSA anahtar çiftlerinin boyu en az 2048-bittir. Başvuru sahipleri için üretilen mobil imza kullanım amaçlı nitelikli elektronik sertifikalara ait RSA anahtar çiftlerinin boyu en az 1024-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.

6.1.7. Anahtar kullanım amaçları

Mobil imza kullanım amaçlı nitelikli elektronik sertifika sahiplerine ait imza oluşturma verileri Elektronik İmza Kanunu'nda tanımlı güvenli elektronik imzayı oluşturmak için kullanılırlar. Sertifika sahibi, güvenli elektronik imza oluşturma aracı içinde bulunan imza oluşturma verisini imza oluşturma dışında kullanmaz. Üçüncü kişiler, nitelikli elektronik sertifikalar içindeki imza doğrulama verilerini, sertifika sahibi tarafından oluşturulmuş elektronik imzanın doğruluğunu kontrol etmek için kullanır. Anahtar çiftlerinin güvenli elektronik imza oluşturma ve doğrulama dışında kullanımlarından doğan sorumluluk sertifika sahibine ve üçüncü kişilere aittir.

6.2. İmza oluşturma verisinin korunması ve Kriptografik modül kontrolleri

6.2.1. Kriptografik modül standartları ve kontroller

Kamu SM'ye ait imza oluşturma verisi güvenli yazılım kullanılarak üretilir, güvenli kriptografik modül içinde saklanır ve geçerli olduğu süre boyunca bu modül dışına çıkmaz.

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- İmza oluşturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- Erişim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluşturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.

Sertifika sahibinin imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracı, imza oluşturma verisinin aracın dışına çıkmasını engelleyen ve araca erişimi parola ile sağlayan teknik özelliklere sahiptir.

Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluşturma aracı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen aşağıdaki güvenlik standartlarından en azından birisini sağlar:

- FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzeri,
- CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+.

6.2.2. İmza oluşturma verisine birden fazla kişi kontrolünde erişim

Kriptografik modülde saklanmakta olan Kamu SM'ye ait imza oluşturma verilerinin, kullanılan uygulamalar tarafından erişilebilir olması (aktivasyonu) için en az 2 (iki) çalışanın aynı anda hazır bulunması gereklidir. Bu amaçla kullanılmakta olan bütün araçlar (erişim kartları, erişim denetim verileri vb.) sadece erişim yetkisi bulunan çalışanların erişebileceği fiziksel ortamlarda saklanır.

Mobil imza kullanım amaçlı nitelikli elektronik sertifikalara ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı içerisinde saklanır. İmza oluşturma verisine erişim amacıyla kullanılan erişim denetim verilerinin güvenliği sertifika sahibinin sorumluluğundadır.

6.2.3. İmza oluşturma verisinin yeniden elde edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza oluşturma verisinin yedeklenmesi

Yaşanacak herhangi bir felaket durumunda faaliyetlerin devam edebilmesi amacıyla Kamu SM'ye ait imza oluşturma verileri yedeklenir. Yedekleme işlemi için, imza oluşturma verilerini içeren kriptografik modülün yedekleme mekanizmaları kullanılır. Yedeklerin geri yüklenebilmesi için ilgili erişim kartları ve parolalara sahip en az 2 (iki) çalışanın aynı anda hazır bulunması gereklidir.

Sertifika sahiplerine ait imza oluşturma verileri yedeklenmez.

6.2.5. İmza oluşturma verisinin arşivlenmesi

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

6.2.6. İmza oluşturma verisinin kriptografik modüle yüklenmesi

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

Mobil imza kullanım amaçlı nitelikli elektronik sertifikalara ait imza oluşturma verisi güvenli imza oluşturma aracı içerisinde oluşturulur.

6.2.7. İmza oluşturma verisinin kriptografik modülde saklanması

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

Sertifika sahibine ait imza oluşturma verisi sertifika sahibinin güvenli elektronik imza oluşturma aracı içinde saklanır, başka bir ortamda bulunmaz.

6.2.8. İmza oluşturma verisine erişim

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

İmza oluşturma verisi kriptografik modül içinde şifreli durumdayken erişime kapalıdır. Erişime açılması için erişimi sağlayan verinin modüle sunulması gerekir. İmza oluşturma verisinin erişime açılması ve kullanılır duruma getirilmesi birden fazla yetkili çalışanın ortak denetimi altındadır.

Sertifika sahibine ait imza oluşturma verisi güvenli elektronik imza oluşturma aracı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

6.2.9. İmza oluşturma verisine erişimin kesilmesi

Kamu SM'nin imza oluşturma verisi imzalama için kullanıldıktan sonra oturum kapandığında veriye erişim otomatik olarak kesilir ve bir sonraki kullanımına kadar şifrelenerek erişime kapalı tutulur. Erişimin yeniden sağlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden işletilmesi gerekir.

Sertifika sahibinin kullandığı güvenli elektronik imza oluşturma araçları, imza oluşturma verisini kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir.

6.2.10. İmza oluşturma verisinin yok edilmesi

Kamu SM'ye ait imza oluşturma verileri kullanım süresinin dolmasının ardından, aslı ve bütün yedekleri bulundukları ortamlardan uygun yöntemlerle geri dönüşsüz şekilde silinir. Kamu SM'ye ait imza oluşturma verisinin silinmesi işlemi için Bölüm 6.2.8'de belirtilen şekilde yeterli sayıda yetkili personelin hazır bulunması gerekir.

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

6.2.11. Kriptografik modülün değerlendirilmesi

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

6.3. Anahtar çifti yönetimiyle ilgili diğer konular

6.3.1. İmza doğrulama verisinin arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait imza doğrulama verileri sertifikalar içinde tutulur ve nitelikli elektronik sertifikalar kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Nitelikli elektronik sertifikaların arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. İmza oluşturma ve doğrulama verilerinin kullanım süreleri

İmza oluşturma verisinin kullanım süresi, nitelikli elektronik sertifikanın içeriğinde belirtilen nitelikli elektronik sertifika kullanım süresi kadardır. Nitelikli elektronik sertifikanın kullanım süresinin dolmasıyla ya da nitelikli elektronik sertifikanın iptal edilmesiyle imza oluşturma verisinin kullanımı sona erer. Ancak, kullanım süresi dolsa bile nitelikli elektronik sertifikalar içindeki imza doğrulama verileri geçmişe yönelik imzaların doğrulanabilmesi için kullanılır.

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan imza algoritmasına göre belirlenir. Kamu SM'ye ait 2048 RSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 5 (beş) yıl için kullanılır. Sertifika sahiplerine ait 1024 bitlik RSA anahtar çiftleri en fazla 1 (bir) yıl için kullanılır.

Üretilen nitelikli elektronik sertifikaların son kullanma tarihi kendisine nitelikli elektronik sertifika veren Kamu SM'ye ait kök sertifikasının son kullanma tarihini aşamaz.

6.4. Erişim denetim verileri

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

Sertifika sahibine ait erişim denetim verisi güvenli elektronik imza oluşturma aracı erişim verisidir.

6.4.1. Erişim denetim verilerinin oluşturulması

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

Sertifika sahibine ait güvenli elektronik imza oluşturma aracı erişim denetim verisi sertifika sahibinin kontrolünde üretilir.

6.4.2. Erişim denetim verilerinin korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir. Sertifika sahibine ait güvenli elektronik imza oluşturma aracı erişim denetim verisini yetkisiz kişilerin erişimine karşı korumak sertifika sahibinin yükümlülüğü altındadır.

6.4.3. Erişim denetim verileri ile ilgili diğer konular

Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar güvenliği denetimleri

6.5.1. Bilgisayar güvenliği ile ilgili teknik gerekler

Kamu SM, uyguladığı bilgi güvenliği yönetim sisteminin gereği olarak yönetim tarafından onaylanmış ve bütün çalışanlara duyurulmuş bir bilgi güvenliği politikasına sahiptir. Bu politika ve ilgili diğer politika, talimat, yönerge ve rehberler kullanılarak bilgi güvenliği ile ilgili riskler azaltılmaya çalışılır. Kamu SM, ESHS faaliyetini gerçekleştirmek için birçok yazılım ve donanım sistemlerinden faydalanır. Bu sistemlerin güvenliğinin sağlanması amacıyla aşağıdaki kontroller uygulanır:

- Mantıksal olarak ayrılmış ağlar ve sertifika servisleri için erişim kontrolleri,
- Sıkılaştırılmış ve sürekli güncel tutulan işletim sistemleri,
- Virüs/kötücül yazılım önleme ve saldırı tespit sistemleri,
- İşletim sistemi ve uygulama yazılımları seviyesinde kullanıcı erişim denetimi ve yetkilendirme,
- Kritik sertifika servislerinde görevlerin ayrılması,
- Veritabanı servislerinde ve ağ erişimlerinde kriptografik kontrollerin kullanılması,
- Güvenlik ile ilgili olayların izlenmesi.

6.5.2. Bilgisayar sisteminin sağladığı güvenlik seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam döngüsü teknik denetimleri

6.6.1. Sistem geliştirme denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda verilmiştir:

- Uygulamalar kontrollü bir geliştirme ortamında geliştirilir. Hatalara ve güvenlik açıklarına karşı farklı kişiler tarafından çapraz kontroller yapılır,
- Bütün uygulamalar versiyon takibinin yapılabilmesi amacıyla bir versiyon takip sisteminde tutulur.

6.6.2. Güvenlik yönetimi denetimleri

Gerçekleştirilen güvenlik yönetimi denetimleri TS ISO/IEC 27001 gereksinimlerini sağlar. Her yıl iç ve dış denetimler gerçekleştirilir.

6.6.3. Yaşam döngüsü güvenlik denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ güvenliği denetimleri

Kamu SM ağı yedekli güvenlik duvarları kullanılarak farklı güvenlik bölgelerine ayrılmıştır. İhtiyaç duyulan web servisleri için internet üzerinden erişim izni sadece dış ağ ile iç ağı birbirinden ayıran bir bölgeye (DMZ) kontrollü olarak sağlanmaktadır. İnternet üzerinden ve yerel ağdan gelebilecek saldırılara karşı saldırı tespit sistemleri kullanılmaktadır. Kök sertifika hizmet sağlayıcıya ait anahtarların bulunduğu kriptografik modüller ve uygulamaların bulunduğu sunucu sistemleri sadece işlemlerin gerçekleşeceği sırada açık konumdadır, diğer durumlarda kapalı konumda bulundurulmaktadır.

6.8. Zaman Damgası

Kamu SM, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen şartlara uygun şekilde zaman damgası hizmeti sağlar. Zaman damgasıyla ilgili ayrıntılı bilgi Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları'nda bulunur. Çalışanlara ait internet erişim olay kayıtlarının saklanması aşamasında zaman damgası kullanılır.

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ VE ÇİSDUP PROFİLLERİ

7.1. Sertifika profili

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

Kamu SM tarafından oluşturulan sertifikalar içerisindeki temel alanlar aşağıdaki tablo da gösterilmiştir.

Alan Adı	Değeri
Sürüm	X.509 Sürüm 3
Seri numarası	Sertifikayı tanımlayan tekil değer
İmza Algoritması	Sertifikayı imzalamak için kullanılan algoritmayı gösteren nesne tanımlama numarası (Bölüm 7.1.3)
Üretici ESHS	Üretici ESHS
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıç tarihi
Geçerlilik Sonu	Sertifika geçerlilik bitiş tarihi
Sertifika Sahibi	X.500 standardına uygundur
İmza doğrulama verisi	Kullanılan açık anahtar algoritması ve imza doğrulama verisi (Bölüm 7.1.3)
Uzantılar	X.509 Sürüm 3 uzantıları (Bölüm 7.1.2)
ESHS İmzası	RFC 5280'e uygun olarak oluşturulmuş sertifika imzası

7.1.1. Sürüm numarası

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

7.1.2. Sertifika uzantıları

Kamu SM tarafından oluşturulan nitelikli elektronik sertifikalar 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. Nitelikli elektronik sertifikanın içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Aşağıdaki tabloda Kamu SM tarafından üretilen nitelikli elektronik sertifikada asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Sertifika Uzantısı	Kritik Uzantı	Açıklama

Temel Kısıtlar[1]	HAYIR	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
ESHS Anahtar Tanımlayıcı[2]	HAYIR	Kamu SM'ye ait Mobil 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.
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/mobil/mobil-s2.crl*
ESHS Erişim Bilgisi[6]	HAYIR	*http://depo.kamusm.gov.tr/mobil/mobil-s2.crt* *http://ocspmobils2.kamusm.gov.tr*
Sertifika İlkeleri[7]	HAYIR	Mobil imza kullanım amaçlı nitelikli elektronik sertifikalar için hazırlanmış olan Sİ/SUE dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.8) ile Sİ/SUE dokümanının bulunduğu *http://depo.kamusm.gov.tr/ilke/mobilnes* internet adresini ve BTK tarafından oluşturulan nitelikli elektronik sertifika ibaresine ait metni içerir.
Nitelikli Elektronik Sertifika İbaresi[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 sınır bilgisini içerir. Bilgi teknolojileri kurumu tarafından belirlenen nitelikli elektronik sertifika ibaresi ile bu ibareye ait nesne tanımlama numarası bilgisini içerir.

[1] BasicConstraints
[2] AuthorityKeyIdentifier
[3] SubjectKeyIdentifier
[4] KeyUsage
[5] CRLDistributionPoints
[6] AuthorithyInformationAccess
[7] CertificatePolicies
[8] QcStatement

Kullanıcı Dizin Bilgileri[9] (2.5.29.9)	HAYIR	Sertifika sahibinin doğum tarihi bilgisini içerir.

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

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

Sertifikanın nitelikli olduğu "Nitelikli Elektronik Sertifika İbaresi Uzantısı" içerisindeki ETSI ve Bilgi Teknolojileri ve İletişim Kurumu'na ait nitelikli elektronik sertifika ibareleri ile belirtilir.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belirlenen ibare "Nitelikli Elektronik Sertifika İbaresi Uzantısı" içinde yer alan "İbare Bilgisi[10]" alanının içine yazılır. Bu ibareye ait nesne tanımlama numarası ise "İbare Numarası[11]" 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-profili(5070) nes-ibaresi (1) nes-uygunlugu (1)}

Kamu SM tarafından mobil imza kullanım amaçlı nitelikli elektronik sertifikalara ait Kök ve Alt kök sertifikalarının içeriği EK-A da bulunmaktadır.

7.1.3. Algoritma nesne tanımlayıcıları

Kamu SM, kişilere verdiği nitelikli elektronik sertifikaları imzalamak için SHA-1 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır. Sertifika sahiplerine ait anahtar çiftleri RSA algoritması anahtar çiftleridir. Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları içinde belirtilir.

7.1.4. İsim biçimleri

Kamu SM tarafından üretilen nitelikli elektronik sertifikalardaki isim alanı "ITU X.500 Distinguished Name [Ayırt edici isim]" biçimine uygundur.

7.1.5. İsim kısıtları

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

Kamu SM tarafından farklı kişiler için üretilen nitelikli elektronik sertifikaların isim alanları aynı olamaz. İsim alanlarının benzersizliğinin sağlanması için T.C. Kimlik Numarası DN alanı içinde yer alır. Yabancı uyruklu nitelikli elektronik sertifika sahiplerinin isim alanlarının benzersizliğinin sağlanması için, pasaport numarası DN alanı içinde yer alır.

[9] SubjectDirectoryAttributes
[10] StatementInfo
[11] StatementId

Aşağıdaki tabloda nitelikli elektronik sertifika içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

Alan Adı	Nitelikli Elektronik Sertifika İçeriği
CN[12]	Sertifika sahibinin adı soyadı
Serial[13]	T.C. kimlik numarası / Pasaport numarası
C[14]	TR

7.1.6. Sertifika ilkeleri nesne tanımlama numarası

Bu Sİ/SUE dokümanına göre uygun olarak oluşturulan sertifikalar bölüm 1.2 de belirtilen nesne tanımlama numarasını içerir.

7.1.7. İlke kısıtları uzantısının kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke niteleyiciler

Mobil imza kullanım amaçlı nitelikli elektronik sertifikaların üretim ve yönetiminde takip edilen kurallara işaret eden SI dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen nitelikli elektronik sertifikanın "Sertifika İlkeleri Uzantısı[15]"nın içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici[16]" olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

Üçüncü kişiler "Sertifika İlkeleri Uzantısı"nı kontrol ettiğinde Sİ/SUE'de belirtilen ilke ve uygulama esasları çerçevesinde nitelikli elektronik sertifikaları kullanarak işlem yapar.

Kamu SM tarafından kişilere verilen elektronik sertifikaların nitelikli olduğunu belirten ibare "Sertifika İlkeleri Uzantısı" içindeki "Kullanıcı Bildirim Alanı[17]"nda tanımlanır. Kamu SM tarafından tanımlanan nitelikli sertifika ibaresi aşağıda verilmiştir:

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

7.1.9. Kritik belirlenmiş olan ilke belirleyici uzantılarının işlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika iptal listesi profili

Sertifika iptal listesi aşağıdaki temel alanları içerir:

Sürüm Numarası	Sürüm 2
Üretici	SİL'i oluşturan ESHS'ye ait isim bilgileri
Yayın Tarihi	SİL yayımlanma tarihi

[12] CN: Common Name [Genel isim]
[13] Serial: Serial Number [Seri Numarası]
[14] C: Country [Ülke]
[15] Certificate Policies
[16] Policy Identifier
[17] User Notice

Sonraki SİL Tarihi	Bir sonraki SİL yayımlanma tarihi
İmzalama Algoritması	SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL'i imzalamak için SHA-1 özet algoritması ile RSA açık anahtarlı imzalama algoritmasını kullanır.)
SİL Numarası	SİL seri numarası
ESHS Anahtar Tanımlayıcısı	SİL imzasını doğrulamak için kullanılan Kamu SM'ye ait sertifikanın "ESHS Anahtar Tanımlayıcı" numarası
İptal Edilen Sertifikalar	İptal edilen nitelikli elektronik sertifikalarla ilgili aşağıdaki bilgiler: • Sertifikanın seri numarası • Sertifikanın iptal tarihi • Sertifikanın neden iptal edildiği bilgisi

7.2.1. Sürüm numarası

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

7.2.2. Sertifika iptal listesi uzantıları

Kamu SM tarafından desteklenen sertifika iptal listesi uzantıları "ESHS Anahtar Tanımlayıcı[18]" ve "SİL Numarası[19]" dır.

7.3. ÇİSDUP profili

7.3.1. Sürüm numarası

Çevrim İçi Sertifika Durum Protokolü RFC 2560 V.1'i destekler.

7.3.2. ÇİSDUP uzantıları

Kamu SM tarafından sağlanan ÇİSDUP servisi aşağıdaki uzantıları destekler.

- Nonce

[18] AuthorityKeyIdentifier
[19] CRL Number

8. UYGUNLUK DENETİMİ VE DİĞER DEĞERLENDİRMELER

Bu dokümanda belirtilen uygulamalar ve ilgili prosedürler mevzuat gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından incelenir/denetlenir. Kamu SM iç işleyişini denetlemek için, ayrıca iç denetimler gerçekleştirilir.

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

8.1. Uygunluk denetiminin sıklığı

Kamu SM iki yılda en az bir defa Bilgi Teknolojileri ve İletişim Kurumu tarafından denetlenir.

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

8.2. Denetçinin kimliği ve nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiş kurum olan BTK tarafından gerçekleştilir.

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 ilişkisi

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

8.4. Denetimin Kapsamı

Denetim kapsamı aşağıdaki hususları da kapsayacak şekilde denetçi tarafından belirlenir.

- Kamu SM'nin fiziksel ortam güvenliği,
- Uygulanmakta olan politika ve prosedürler,
- Sİ/SUE dokümanlarına ve ilgili mevzuat'a uygunluk,
- Olay kayıtları,
- Kimlik doğrulama.

8.5. Yetersizliğin tespiti durumunda yapılacaklar

Kurum tarafından gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderililir. 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'sinin temel işleyişini etkileyecek kadar büyük ise, Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır.

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

8.6. Sonucun bildirilmesi

Denetim sonucunda BTK ve ISO/IEC 27001 denetçilerinin hazırladığı resmi raporlar Kamu SM'ye bildirilir. İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

9. DİĞER İŞLER VE HUKUKSAL MESELELER

9.1. Ücretlendirme

9.1.1. Sertifika oluşturma ve yenileme ücreti

Kamu SM tarafından üretilen ve yenilenen nitelikli elektronik sertifikalar için kurumlardan veya sertifika sahiplerinden ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında, kurumlarla yapılan sözleşmelerde ya da Kamu SM web sayfasında belirtilir.

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

9.1.2. Sertifika erişim ücreti

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

9.1.3. İptal durum kaydına erişim ücreti

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

9.1.4. Diğer servis ücretleri

Kamu SM, bilgi deposundan yayımladığı bilgi ve dokümanlara erişim için ve elektronik ortamdan ya da çağrı merkezi üzerinden otomatik olarak gerçekleşen işlemler için ücret talep etmez. Bunların dışında kalan servis ücretleri ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında, kurumlarla yapılan sözleşmelerde ya da Kamu SM web sayfasında belirtilir.

9.1.5. Ücret İadesi

Güvenli elektronik imza oluşturma aracının sertifika sahibinin yanlış kullanımından dolayı kullanılamaz duruma gelmesi durumunda ya da sertifikanın sertifika sahibi tarafından iptal edilmesi durumunda ücret iadesi yapılmaz. Kamu SM'den kaynaklanan sebeplerden dolayı sertifika içerisindeki bilgilerde hata olması durumunda sertifika iptal edilir ve yenisi ücretsiz olarak üretilir.

9.2. Finansal sorumluluk

9.2.1. Sigorta kapsamı

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

9.2.2. Diğer varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika mali sorumluluk sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, dağıttığı nitelikli elektronik sertifikaları elektronik imza mevzuatı gereğince mali sorumluluk sigortası ile sigortalar.

9.3. İş bilgisinin korunması

9.3.1. Gizli bilginin kapsamı

Kamu SM ve sertifika hizmeti verdiği taraflarca yapılan sözleşmeler ve iş birliği protokolleri; ayrıca kök ve alt kök sertifikalarının imza oluşturma verileri, sertifika yaşam döngüsünde oluşan işlem kayıtları, sistem kayıtları, iç ve dış denetim raporları, acil durum müdahale planları gizli 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 kurumsal web sayfasında (http://www.kamusm.gov.tr/) yayımlanan her türlü doküman ve bilgi gizli olarak değerlendirilmez. Sertifika içerisinde yer alan bilgiler de gizli olarak değerlendirilmez.

9.3.3. Gizli bilginin korunma sorumluluğu

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

9.4. Kişisel bilginin gizliliği

9.4.1. Gizlilik planı

Düzenlenmesine gerek duyulmamıştır.

9.4.2. Gizli olarak tanımlanan bilgiler

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

9.4.3. Gizli olarak tanımlanmayan bilgiler

Nitelikli elektronik sertifikanın içeriğinde bulunan bilgiler aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli bilginin korunma sorumluluğu

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

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

9.4.5. Gizli bilginin kullanımına izin verilmesi

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

9.4.6. Yetkili Merciilerin 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 nitelikli elektronik sertifikalar ve dokümanlar ile bu Sİ/SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları TÜBİTAK-BİLGEM'e aittir.

9.6. Temsil hakkı ve yükümlülükler

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

Kamu SM, sertifika sahipleri, sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları ile üçüncü kişiler yasa ve yönetmeliklerde belirtilmediği halde, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi'nde 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

Kamu SM, nitelikli elektronik sertifika yaşam döngüsündeki süreçleri, sözleşmede, işbirliği protokolünde, Kamu SM Nitelikli Elektronik Sertifika Taahhütnamesi'nde ve/veya bu dokümanda belirtilen gereklilikleri ve yükümlülükleri yerine getireceğini taahhüt eder.

9.6.2. Kayıt makamı yükümlülükleri

Kayıt makamı olarak hizmet veren merkez; işlemleri, imzalanan sözleşme, işbirliği protokolü ve/veya kayıt makamı taahhütnamesine uygun olarak yürüteceğini taahhüt eder.

Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin zarara uğraması halinde, TÜBİTAK BİLGEM'in ödemek zorunda olduğu tazminatlar için kayıt makamına rücu hakkı saklıdır.

9.6.3. Sertifika sahibinin yükümlülükleri

Sertifika sahibi, başvuru sürecinde imzalamış olduğu Kamu SM Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi ve bu dokümanda belirtilen yükümlülüklere uyacağını taahhüt eder. Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin zarara uğraması halinde, TÜBİTAK BİLGEM'in ödemek zorunda olduğu tazminatlar, sertifika sahibine rücu edilecektir.

9.6.4. Üçüncü kişilerin yükümlülükleri

Üçüncü kişiler, nitelikli elektronik sertifikalarla ilgili işlem yapmadan once; sertifikanın /elektronik imzanın geçerliliğini, finansal işlemler için maddi sınır kısıtlamasını ve kullanım amacına uygunluğunu kontrol etmekten kendileri sorumludur.

9.6.5. Diğer bileşenlerin yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.7. Yükümlülüklerin sona ermesi

Kamu SM ile sertifika sahipleri veya sertifika sahiplerinin bağlı bulunduğu kamu kurum veya kuruluşları arasındaki yükümlülük, Nitelikli Elektronik Sertifika Sözleşmesi, Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi, Kamu SM Taahhütnamesi ve NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi'nde belirtildiği şekilde sona erer.

9.8. Sorumlulukla ilgili sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları;

- 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, 2004/21 sayılı Başbakanlık Genelgesi, Bilgi Teknolojileri ve İletişim Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ,
- İmzalanan sözleşme veya işbirliği protokolleri,
- Nitelikli Elektronik Sertifika Sahibi Taahhütnamesi ve/veya NES Temini Sipariş Şartları ve Hizmet Esasları Yönergesi

ile belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diğer düzenlemeler dikkate alınır.

9.9. Tazminat halleri

Kamu SM'nin mücbir sebepler dışında, ESHS yükümlülüklerini yerine getiremediği durumda, sertifika sahibi veya üçüncü kişilerin uğrayacağı zarar, Kamu SM tarafından tazmin edilir.

Sertifika sahibi yükümlülüklerinin ihlali nedeniyle Kamu SM ve/veya üçüncü kişilerin zarara uğraması halinde, TÜBİTAK BİLGEM tarafından ödenmek zorunda olan tazminatlar sertifika sahibine rücu edilir.

9.10. Sİ/SUE dokümanın geçerliliği ve geçerliliğinin sona ermesi

9.10.1. Geçerliliği

Sİ/SUE dokümanı Kamu SM bilgi deposunda yayımlandığı anda geçerli olur ve yeni sürümü yayımlanana kadar yürürlükte kalır.

9.10.2. Sona ermesi

Sİ/SUE dokümanının yeni sürümü yayımlandığında, eski sürümün geçerliliği sona erer.

9.10.3. Sona ermesinin etkileri

Sİ/SUE dokümanında yapılan güncellemelerden sertifika sahiplerinin en az etkilenmesi için Kamu SM gereken özeni gösterir. Yeni sürüm Sİ/SUE dokümanı hazırlanır ve onay alındıktan sonra Kamu SM bilgi deposunda yayımlanır. Yapılan değişiklikler ilgili tüm taraflar için geçerli olur. Eski Sİ/SUE dokümanının bağlayıcılığı ortadan kalkar.

9.11. Bireysel bildirimler ve katılımcılar ile iletişim

Kamu SM ve ilgili taraflar arasındaki iletişim, e-posta, sms, resmi yazı, web sayfası duyuruları veya çağrı merkezi aracılığı ile gerçekleştirilir.

9.12. Değişiklik halleri

9.12.1. Değişiklik metodları

Sİ/SUE dokümanında yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, Kamu SM dokümanın tamamen yenilenmesine de karar verebilir.

Değişiklikler kayıt altına alınır ve Sİ/SUE'nin eski sürümleri Kamu SM bilgi deposunda yayımlanır.

9.12.2. Bilgilendirme mekanizması ve sıklığı

Sİ/SUE dokümanında yapılan değişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Sİ/SUE'de yapılan değişiklikler 7 (yedi) gün içinde BTK'ya 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, Bilgi Teknolojileri ve İletişim 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 dokümanlarına başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde T.C. Gebze Mahkemeleri ve İcra Daireleri görevli ve yetkili mahkemelerdir.

9.14. Uygulanacak hukuk

Bu Sİ/SUE dokümanındaki hükümlerin yorumlanması ve uygulanmasında Türk Hukuku esas alınacaktır.

9.15. Uygulanabilir yasalarla uyum

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

9.16. Çeşitli hükümler

Düzenlenmesine gerek duyulmamıştır.

9.17. Diğer hükümler

Düzenlenmesine gerek duyulmamıştır.

EK-A Sertifika biçimleri

a) CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1

Alan	Değer
Sürüm	V3
Seri Numarası	15
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	11 Nisan 2011 Pazartesi 14:35:26
Geçerlilik Sonu	11 Nisan 2021 Pazar 14:35:26
Konu	CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 d9 86 4d ec 10 4e d9 61 95 b3 f3 b0 18 84 b1 2d 36 df 1d
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama , Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

b) CN = KamuSM Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 2

Alan	Değer
Sürüm	V3
Seri Numarası	00 84 43 b0 0f 3e
İmza Algoritması	sha-1 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = KamuSM Mobil Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	12 Nisan 2011 Salı 16:12:00
Geçerlilik Sonu	09 Nisan 2021 Cuma 16:12:00
Konu	CN = KamuSM Mobil Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 2 OU = Kamu Sertifikasyon Merkezi OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli

	C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 d9 86 4d ec 10 4e d9 61 95 b3 f3 b0 18 84 b1 2d 36 df 1d
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 90 ce 87 cb 32 a0 6f 7a 8f ac 10 69 8a 15 0c 80 da 49 f8 cc
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama , Çevrimdışı Sil İmzalama, Sil İmzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.8 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici: http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/mobil/mobilkok-s1.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/mobil/mobilkok-s1.crt