TASNİF DIŞI

TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ

ELEKTRONİK MALİ MÜHÜR SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu
YON.01.10

Revizyon No
02

Revizyon Tarihi
30.01.2024

TASNİF DIŞI

REVİZYON GEÇMİŞİ		
Revizyon No	**Revizyon Nedeni**	**Revizyon Tarihi**
00	İlk yayın (YONG-001-011 kodu ve "Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Sertifika Uygulama Esasları" ismi ile kabul edilmiştir.)	01.02.2010
01	Aynı doküman içerisinde yer alan; Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Sertifika Uygulama Esasları iki ayrı doküman olacak şekilde düzenlenerek kodu ve şablonu güncellenmiştir. Doküman genelinde düzenlemeler yapılarak, web sitesi adresleri yeni altkök sertifikasına göre düzenlenmiştir.	28.10.2022
02	Kök ve alt kök sertifika adları, adresleri, imza algortiması ve özel algoritması bilgileri güncellenmiştir. Genel düzenlemeler yapılmıştır.	30.01.2024

İÇİNDEKİLER

1. GİRİŞ 10
1.1. Genel Bakış 10
1.2. Doküman Adı ve Tanımı 11
1.3. Sistem Bileşenleri 11
1.3.1. Elektronik Sertifika Hizmet Sağlayıcı 11
1.3.2. Kayıt Birimleri 11
1.3.3. Sertifika Sahipleri 12
1.3.4. Üçüncü Kişiler 12
1.3.5. Diğer Bileşenler 12
1.3.5.1. Kurum 12
1.3.5.2. Elektronik Mali Mühür Sertifikası Sorumlusu 12
1.4. Sertifika Kullanımı 12
1.4.1. Uygun Olan Sertifika Kullanımı 12
1.4.2. Sertifika Kullanımının Sınırları 13
1.5. Uygulama Esaslarının Yönetimi 13
1.5.1. Doküman Yönetimi 13
1.5.2. İletişim Bilgileri 13
1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi 14
1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri 14
1.6. Tanımlar ve Kısaltmalar 14
1.6.1. Tanımlar 14
1.6.2. Kısaltmalar 16

2. YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ 17
2.1. Bilgi Depoları 17
2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması 17
2.3. Yayım Sıklığı ve Zamanı 18
2.4. Erişim Kontrolleri 18

3. KİMLİK BELİRLEME VE DOĞRULAMA 18
3.1. İsimlendirme 18
3.1.1. İsim Alanı Tipleri 18
3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması 19
3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması 19
3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması 19
3.1.5. Kimlik Bilgilerinin Tekilliği 19
3.1.6. Markanın Tanınması, Doğrulanması ve Rolü 19
3.2. İlk Kimlik Belirleme 19
3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması 19
3.2.2. Kurumsal Kimliğin Belirlenmesi 20
3.2.3. Kişisel Kimliğin Belirlenmesi 20
3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri 20
3.2.5. Yetkinin Doğrulanması 20

3.2.6. Uyum Kriterleri ... 20
3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama ... 20
3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama ... 21
3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama ... 21
3.4. Sertifika İptal İsteğinde Kimlik Doğrulama ... 21
4. SERTİFİKA YAŞAM DÖNGÜSÜ İŞLEVSEL GEREKLİLİKLERİ ... 21
4.1. Sertifika Başvurusu ... 21
4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği ... 21
4.1.2. Kayıt İşlemleri ve Sorumluluklar ... 22
4.2. Sertifika Başvurusunun İşlenmesi ... 22
4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi ... 22
4.2.2. Sertifika Başvurusunun Kabul veya Redi ... 22
4.2.3. Sertifika Başvurusunun İşlenme Zamanı ... 22
4.3. Sertifikanın Oluşturulması ... 23
4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri ... 23
4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi ... 23
4.4. Sertifikanın Kabulü ... 23
4.4.1. Sertifikanın Kabul Koşulu ... 23
4.4.2. Sertifikanın ESHS Tarafından Yayımlanması ... 23
4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması ... 23
4.5. Sertifikanın ve Özel Anahtarın Kullanımı ... 24
4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı ... 24
4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı ... 24
4.6. Sertifika Süresinin Uzatılması ... 24
4.7. Sertifikanın Yenilenmesi ... 24
4.7.1. Sertifika Yenileme Koşulları ... 24
4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği ... 25
4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi ... 25
4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi ... 25
4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu ... 25
4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması ... 25
4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması ... 25
4.8. Sertifikada Bilgi Değişikliği ... 25
4.9. Sertifikanın İptali ve Askıya Alınması ... 25
4.9.1. Sertifikanın İptal Edildiği Durumlar ... 25
4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir ... 26
4.9.3. Sertifika İptal Başvurusunun İşlenmesi ... 26
4.9.4. İptal İsteği Ertelenme Süresi ... 27
4.9.5. İptal İsteğinin İşlenme Süresi ... 27
4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği ... 27
4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı ... 27
4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi ... 27
4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti ... 27

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi ... 28
4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri ... 28
4.9.12. Özel Anahtarın Güvenliğini Yitirmesi Durumu ... 28
4.9.13. Sertifikanın Askıya Alındığı Durumlar ... 28
4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği ... 29
4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi ... 29
4.9.16. Askıda Kalma Süresi ... 29
4.10. Sertifika Durum Servisleri ... 29
4.10.1. İşletimsel Özellikleri ... 29
4.10.2. Servisin Erişilebilirliği ... 29
4.10.3. İsteğe Bağlı Özellikler ... 30
4.11. Sertifika Sahipliğinin Sona Ermesi ... 30
4.12. Anahtar Yeniden Üretme ... 30

5. YÖNETİM, İŞLEMSEL VE FİZİKSEL KONTROLLER ... 30
5.1. Fiziksel Güvenlik Denetimleri ... 30
5.1.1. Tesis Yeri ve İnşaatı ... 30
5.1.2. Fiziksel Erişim ... 31
5.1.3. Güç Kaynağı ve Havalandırma ... 31
5.1.4. Su Baskınları ... 31
5.1.5. Yangın Önleme ve Korunma ... 31
5.1.6. Saklama ve Yedekleme Ortamlarının Korunması ... 32
5.1.7. Atıkların Yok Edilmesi ... 32
5.1.8. Farklı Mekanlarda Yedekleme ... 32
5.2. Prosedürsel Kontroller ... 32
5.2.1. Güvenilir Roller ... 32
5.2.2. Her İşlem İçin Gereken Kişi Sayısı ... 33
5.2.3. Kimlik Doğrulama ve Yetkilendirme ... 33
5.2.4. Görevlerin Ayrılmasını Gerektiren Roller ... 33
5.3. Personel Güvenlik Kontrolleri ... 33
5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri ... 33
5.3.2. Geçmiş Araştırması ... 33
5.3.3. Eğitim Gerekleri ... 34
5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı ... 34
5.3.5. Görev Değişim Sıklığı ve Sırası ... 34
5.3.6. Yetkisiz Eylemlerin Cezalandırılması ... 34
5.3.7. Anlaşmalı Personel Gereksinimleri ... 34
5.3.8. Sağlanan Dokümantasyon ... 34
5.4. Denetim Kayıtları ... 35
5.4.1. Kaydedilen İşlemler ... 35
5.4.2. Kayıtların İncelenme Sıklığı ... 36
5.4.3. Kayıtların Saklanma Süresi ... 36
5.4.4. Kayıtların Korunması ... 36
5.4.5. Kayıtların Yedeklenmesi ... 36

5.4.6. Kayıtların Toplanması ... 36
5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi ... 36
5.4.8. Saldırıya Açıklığın Değerlendirilmesi ... 37
5.5. Kayıt Arşivleme ... 37
5.5.1. Arşivlenen Kayıt Bilgileri ... 37
5.5.2. Arşivlerin Tutulma Süresi ... 37
5.5.3. Arşivlerin Korunması ... 38
5.5.4. Arşivlerin Yedeklenmesi ... 38
5.5.5. Kayıtların Zaman Damgası Gereksinimleri ... 38
5.5.6. Arşivlerin Toplanması ... 38
5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu ... 38
5.6. Anahtar Değişimi ... 38
5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar ... 39
5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi ... 39
5.7.2. Donanım, Yazılım veya Veri Bozulması ... 39
5.7.3. Özel Anahtarın Gizliliğinin Kaybedilmesi ... 39
5.7.4. Arıza Sonrası Yeniden Çalışırlık ... 40
5.8. Sertifika Hizmetlerinin Sonlandırılması ... 40

6. TEKNİK GÜVENLİK KONTROLLERİ ... 40
6.1. Anahtar Çifti Üretimi ve Kurulumu ... 40
6.1.1. Anahtar Çifti Üretimi ... 40
6.1.2. Elektronik Sertifika Hizmet Sağlayıcısı Anahtar Çiftinin Üretimi ... 40
6.1.3. Sertifika Sahibi Anahtar Çiftinin Üretimi ... 41
6.1.4. Sertifika Sahibine Özel Anahtarın Ulaştırılması ... 41
6.1.5. Elektronik Sertifika Hizmet Sağlayıcısı'na Açık Anahtarın Ulaştırılması ... 41
6.1.6. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması ... 42
6.1.7. Anahtar Uzunlukları ... 42
6.1.8. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü ... 42
6.1.9. Anahtar Kullanım Amaçları ... 42
6.2. Özel Anahtarın Korunması ... 42
6.2.1. Kriptografik Modül Standartları ... 42
6.2.2. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim ... 43
6.2.3. Özel Anahtarın Yeniden Elde Edilmesi ... 43
6.2.4. Özel Anahtarın Yedeklenmesi ... 43
6.2.5. Özel Anahtarın Arşivlenmesi ... 44
6.2.6. Özel Anahtarın Kriptografik Modüle Yüklenmesi ... 44
6.2.7. Özel Anahtarın Kriptografik Modülde Saklanması ... 44
6.2.8. Özel Anahtara Erişim ... 44
6.2.9. Özel Anahtara Erişimin Kesilmesi ... 44
6.2.10. Özel Anahtarın Yok Edilmesi ... 45
6.2.11. Kriptografik Modülün Değerlendirilmesi ... 45
6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular ... 45
6.3.1. Açık Anahtarın Arşivlenmesi ... 45

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri ... 45
6.4. Erişim Denetim Verileri ... 46
6.4.1. Erişim Denetim Verilerinin Oluşturulması ... 46
6.4.2. Erişim Denetim Verilerinin Korunması ... 46
6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular ... 46
6.5. Bilgisayar Güvenliği Denetimleri ... 46
6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler ... 46
6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi ... 47
6.6. Yaşam Döngüsü Teknik Kontrolleri ... 47
6.6.1. Sistem Geliştirme Kontrolleri ... 47
6.6.2. Güvenlik Yönetimi Kontrolleri ... 47
6.6.3. Yaşam Döngüsü Güvenlik Denetimleri ... 48
6.7. Ağ Güvenliği Denetimleri ... 48
6.8. Zaman Damgası ... 49

7. SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ ... 49
7.1. Sertifika Biçimi ... 49
7.1.1. Sürüm Numarası ... 49
7.1.2. Sertifika Uzantıları ... 49
7.1.3. Algoritma ve Nesne Tanımlayıcılar ... 52
7.1.4. İsim Alanı Biçimleri ... 52
7.1.5. İsim Kısıtları ... 53
7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası ... 53
7.1.7. İlke Kısıtları Uzantısının Kullanımı ... 53
7.1.8. İlke Niteleyiciler ... 53
7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi ... 53
7.2. Sertifika İptal Listesi Biçimi ... 53
7.2.1. Sürüm Numarası ... 53
7.2.2. Sertifika İptal Listesi Uzantıları ... 53
7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi ... 54
7.3.1. Sürüm Numarası ... 54
7.3.2. ÇİSDUP Uzantıları ... 54

8. UYGUNLUK DENETİMLERİ ... 55
8.1. Uygunluk Denetiminin Sıklığı ... 55
8.2. Denetçinin Nitelikleri ... 55
8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi ... 55
8.4. Denetimin Kapsamı ... 56
8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar ... 56
8.6. Sonucun Bildirilmesi ... 56

9. DİĞER İŞLER VE HUKUKSAL MESELELER ... 56
9.1. Ücretlendirme ... 56
9.1.1. Sertifika Oluşturma ve Yenileme Ücreti ... 56
9.1.2. Sertifika Erişim Ücreti ... 56
9.1.3. İptal Durum Kaydına Erişim Ücreti ... 57

9.1.4. Diğer Servis Ücretleri ... 57
9.1.5. İade Ücreti ... 57
9.2. Finansal Sorumluluk ... 57
9.2.1. Sigorta Kapsamı ... 57
9.2.2. Diğer Varlıklar ... 57
9.2.3. Sertifika Mali Sorumluluk Sigortası ... 57
9.3. Ticari Bilginin Korunması ... 58
9.3.1. Gizli Bilginin Kapsamı ... 58
9.3.2. Gizlilik Kapsamında Olmayan Bilgiler ... 58
9.3.3. Gizli Bilginin Korunma Sorumluluğu ... 58
9.4. Kişisel Bilginin Gizliliği ... 58
9.4.1. Gizlilik Planı ... 58
9.4.2. Gizli Olarak Tanımlanan Bilgiler ... 58
9.4.3. Gizli Olarak Tanımlanmayan Bilgiler ... 58
9.4.4. Gizli Bilginin Korunma Sorumluluğu ... 59
9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi ... 59
9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması ... 59
9.4.7. Diğer Başlıklar ... 59
9.5. Telif Hakları ... 59
9.6. Temsil Hakkı ve Yükümlülükler ... 59
9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri ... 59
9.6.2. Kayıt Birimi Yükümlülükleri ... 61
9.6.3. Sertifika Sahibinin Yükümlülükleri ... 61
9.6.4. Üçüncü Kişilerin Yükümlülükleri ... 62
9.6.5. Diğer Bileşenlerin Yükümlülükleri ... 63
9.6.5.1. Kurum/Kuruluş/Tüzel Kişi Yükümlülükleri ... 63
9.6.5.2. Sertifika Sorumlularının Yükümlülükleri ... 63
9.7. Yükümlülüklerden Feragat ... 63
9.8. Sorumlulukla İlgili Sınırlamalar ... 63
9.9. Tazminat Halleri ... 63
9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi ... 63
9.10.1. Anlaşma Süresi ... 64
9.10.2. Anlaşmanın Sona Ermesi ... 64
9.10.3. Anlaşmanın Sona Ermesinin Etkileri ... 64
9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme ... 64
9.12. Değişiklik Halleri ... 64
9.12.1. Değişiklik Metotları ... 64
9.12.2. Bilgilendirme Mekanizması ve Sıklığı ... 64
9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar ... 64
9.13. Anlaşmazlık Halleri ... 65
9.14. Uygulanacak Hukuk ... 65
9.15. Uygulanabilir Yasalarla Uyum ... 65
9.16. Diğer Hükümler ... 65

10. EK-A SERTİFİKA PROFİLLERİ 65
10.1. Kamu SM Kurumsal Kök Sertifikası 65
10.2. Kamu SM Mali Mühür Alt Kök Sertifikası 66
10.3. Güvenlik Hizmetleri Sertifikası (GÜS) 67
10.4. Mali Mühür Sertifikası (MÜS) 68
10.5. Güvenli Mali Sertifika 69

TABLOLAR

Tablo 1 MÜS ve GÜS Sertifikası Uzantıları 50

Tablo 2 Güvenli Mali Sertifikası Uzantıları 51

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti bünyesinde ticaret yapan kurum/kuruluş/tüzel/gerçek kişilere Elektronik Mali Mühür Sertifikası sağlayıcılığı konusundaki faaliyetlerini nasıl yürüttüğünü anlatmak amacıyla yazmış olduğu Sertifika Uygulama Esasları (SUE) dokümanıdır.

Kamu SM, 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Telekomünikasyon Kurumu'nun yayımladığı Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de tanımlandığı şekliyle Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) işlevlerini yerine getirir. 2009 yılında Maliye Bakanlığına bağlı Gelir İdaresi Başkanlığı'nca mali belgeleri imzalamak için Mali Mühür kavramı 397 No'lu Vergi Usul Kanunu'nda (VUK) kullanılmıştır ve Kamu SM tarafından Elektronik Mali Mühür Sertifikaları verilmeye başlanmıştır. Daha sonrasında VUK 397 yürürlükten kaldırılmıştır ve Elektronik Mali Mühür Sertifikaları 509 No'lu Vergi Usul Kanunu Genel Tebliğine uygun verilmeye devam edilmiştir. Kamu SM'den Elektronik Mali Mühür sertifikası talebinde bulunanlar bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Bu kapsamda oluşturulan sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmezler.

Kamu SM, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalışır. SUE dokümanı, Elektronik Mali Mühür Sertifikalarının yönetimi ve kayıt işlemleri sırasında yapılan işlerin hangi ortamlarda ve nasıl yürütüldüğünü Sİ dokümanına bağlı olarak detaylandırarak anlatır. Bu SUE dokümanı, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; Kamu SM'nin, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler.

Kamu SM'den Elektronik Mali Mühür Sertifikası talebinde bulunan gerçek, tüzel kişiler ile kurum, kuruluş ve işletmeler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır.

1.1. Genel Bakış

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

SUE dokümanı, “Internet Açık Anahtar Altyapısı Sertifika İlkeleri ve Sertifika Uygulama Esasları Çerçeve Planı” [IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)] referans alınarak hazırlanmış olup, doküman içeriğinde belirtilen bir kısım alt başlıkların altındaki “düzenlenmesine gerek duyulmamıştır” ibaresi, bu aşamada ihtiyaç duyulmadığından düzenleme yapılmadığını ifade etmektedir.

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kamu SM Elektronik Mali Mühür Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 02

Yayın Tarihi: 30.01.2024

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.4.1

Bu doküman, Kamu SM’nin Elektronik Mali Mühür Sertifikası hizmeti verirken uyguladığı esasları tanımlayan SUE dokümanıdır ve kurum/kuruluş/tüzel/gerçek kişilere verilen Elektronik Mali Mühür Sertifikalarını kapsar. SUE dokümanı http://depo.kamusm.gov.tr/ilke/ adresinde kamuya açık olarak kesintisiz yayımlanmaktadır.

1.3. Sistem Bileşenleri

Bu doküman kapsamında tanımlanan sistem bileşenleri, Kamu SM’nin ESHS faaliyetlerinde rol alan ve sertifika hizmetleriyle ilgili hak ve yükümlülükleri bulunan taraflardır. Bu taraflar, ESHS, kayıt birimleri, sertifika sahipleri ve üçüncü kişiler olarak tanımlanır. Kamu SM ESHS faaliyetlerinin tümü Kamu SM personeli tarafından yürütülmektedir.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcı

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

Kamu SM, Elektronik Mali Mühür Sertifika Hizmet Sağlayıcısı (Elektronik Mali Mühür SHS) olarak gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelere Elektronik Mali Mühür Sertifikası hizmeti sağlamaktadır.

1.3.2. Kayıt Birimleri

Tüm kayıt işlemleri doğrudan Kamu SM personeli veya Kamu SM tarafından kontrol edilen web servisler vasıtasıyla yürütülmektedir. Kayıt birimleri, Kamu SM’nin sertifika ve iptal başvurusu gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimidir. Bu birim, ilk müşteri kayıtlarını

oluşturur, gerekli tüzel/gerçek kişi tanımlamalarını ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim birimine yönlendirir.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından kendileri için sertifika oluşturulan ve sertifikalarını sertifika ilkeleri ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelerdir.

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 gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelerdir. Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

1.3.5.1. Kurum

Kamu SM'den Mali Mühür Sertifikası talep eden, Gelir İdaresi Başkanlığı'nda kaydı bulunan Mali Mühür Sertifikası almaya yetkisi olan gerçek, tüzel kişiler ile kurum, kuruluş ve işletmelerdir. Kurum/Kuruluş/Tüzel Kişi/Gerçek Kişi sözleşme veya başvuru formu ve taahhütnamesine uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda adı geçen yerlerdeki işlemleri yapmaktan sorumludur.

1.3.5.2. Elektronik Mali Mühür Sertifikası Sorumlusu

Sertifika başvurusunda bulunan Kurum/Kuruluş/Tüzel Kişi tarafından yetkilendirilen ve Elektronik Mali Mühür Sertifikası başvurusu sırasında gerekli bilgileri Kamu SM'ye ileten, sertifika yönetim süreçlerinde Kamu SM ile iletişim halinde olan kişi/kişilerdir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

Elektronik mali mühür sertifikası (MÜS), elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması için kullanılır.

Güvenlik hizmetleri sertifikası (GÜS), elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin gizliliğinin sağlanması için kullanılır.

Güvenli Mali Sertifika (İşletici Kuruluş Sertifikası), 507 Sıra No.lu VUK Genel Tebliğinde tanımlanan Finans Kuruluşu veya Ödeme Kaydedici Cihaz Üreticilerinden, sistemi işletmek üzere Hazine ve Maliye Bakanlığınca yetkilendirilen ve sistemin işletilmesi nedeniyle bakanlık, başkanlık ve sistem kapsamındaki hizmetlerden yararlananlara karşı asli sorumlu olan kuruluşların alması gereken sertifikadır.

1.4.2. Sertifika Kullanımının Sınırları

Kamu SM tarafından oluşturulan mali mühür sertifikası (MÜS), güvenlik hizmetleri sertifikası (GÜS) ve Güvenli Mali Sertifika Bölüm 1.4.1'de belirtilen amaçlar dışında kullanılamaz. Belirtilen kapsam dışında kullanımdan doğan zararlardan Kamu SM sorumlu tutulamaz.

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

1.5. Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

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

1.5.2. İletişim Bilgileri

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

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

Tel : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

URL : https://mm.kamusm.gov.tr

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

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

1.5.3. Sertifika Uygulama Esaslarının İlkelere 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

Açık Anahtar: İlgili özel anahtarın sahibinin herkes ile paylaşılabildiği, özel anahtarı ile oluşturduğu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşeni.

Akıllı Kart veya HSM Erişim Verisi: Sertifika sahibine ait Özel Anahtara erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

Akıllı Kart: Sertifika ve sertifika ile ilişkili özel anahtarın içinde bulunduğu güvenli donanım.

Anahtar Çifti: Özel anahtar ve onunla ilişkili olan açık anahtar.

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

ÇİSDUP (Çevrim İçi Sertifika Durum Protokolü): Üçüncü kişilerin sertifika iptal listesine alternatif olarak sertifika geçerlilik kontrol talebini yapıp, sertifikanın online olarak iptal durumunu öğrenmelerine imkân tanıyan standart iletişim kuralı.

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

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

Elektronik Mali Mühür Sertifikası Sorumlusu: Kurum/Kuruluş/Tüzel Kişilerin başvuru sırasında başvuru formu ile Kamu SM'ye bildirdiği ve Elektronik Mali Mühür Sertifikası ile ilgili süreçlerde kurumu temsil eden yetkili kişi.

Güvenlik Hizmetleri Sertifikası (GÜS): Sertifika sahibinin Vergi Kimlik Numarası/TCKN ve unvan bilgilerini içeren, e-fatura ve ilgili mevzuatla izin verilen diğer belgeleri şifreleyen şifreleme sertifikası.

Mali Mühür Sertifikası (MÜS): Sertifika sahibinin Vergi Kimlik Numarası/TCKN ve unvan bilgilerini içeren, e-fatura ve ilgili mevzuatla izin verilen diğer belgeleri mühürleyen imzalama sertifikası.

Güvenli Mali Sertifika: İşletici Kuruluş bu sertifikaya bağlı bir alt sertifika olarak; sistemini çalıştırdığı her bir uç nokta (web veya değil) güvenli mali uygulama yazılımı için, hizmet verilen mükellefe ait vergi kimlik numarası ile eşlenik, belirli süreli tekil bir sertifika üretir.

Elektronik Mali Mühür Sertifikası: Elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması için kullanılacak elektronik sertifikadır. Kurum/Kuruluş/Tüzel/Gerçek Kişilerin GİB ile elektronik ortamdaki belge ve bilgi paylaşımında kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifikalardır. İçerisinde GÜS ve MÜS bulunur.

Gelir İdaresi Başkanlığı (GİB): Devlet gelirleri politikasını uygulayan, vergiler ile diğer gelirleri tahsil eden, mükelleflerin vergiye uyumunu kolaylaştıran Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığına bağlı bir devlet kurumudur.

HSM (Hardware Security Module): Sertifikanın kriptografik anahtarlarının içinde bulunduğu harici aygıt; donanımsal güvenlik modülü.

Elektronik Mali Mühür Oluşturma Aracı: Kurum/Kuruluş/Tüzel/Gerçek Kişilere ait imza oluşturma verisi ve sertifikanın içinde bulunduğu akıllı kart ya da benzeri güvenli taşınabilir cihaz.

Elektronik Mali Mühür Oluşturma Aracı Erişim Verisi: Kurum/Kuruluş/Tüzel/Gerçek Kişilere ait imza oluşturma verisine erişimin kontrolünü sağlayan PIN ve PUK bilgisi.

Elektronik Mali Mühür Oluşturma Aracı Okuyucusu: Elektronik mali mühür oluşturma aracının içerisindeki bilgilere erişimi sağlayan donanım aracıdır (akıllı kart okuyucusu vb).

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

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

Kamu SM (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.

Nesne Tanımlama Numarası: Herhangi bir nesneyi eşsiz olarak tanımlayan, uluslararası standart belirleyen bir kuruluştan alınan Numara.

Özel Anahtar: Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluşturmak ve/veya ilgili Açık Anahtarla şifrelenmiş elektronik kayıtların, dosyaların şifresini çözmek için kullanılan anahtar.

SİL (Sertifika İptal Listesi): İptal olmuş sertifika bilgilerinin içinde yer aldığı, ESHS'nin imzasını taşıyan elektronik dosya.

Sertifika Süresi: Üretim anında sertifikanın içine yazılan, sertifikanın geçerlilik başlangıç ve bitiş tarihleri arasında kalan süre.

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

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

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

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

GİA: Güvenli İletişim Anahtarı

GİB: Gelir İdaresi Başkanlığı

GÜS: Güvenlik Hizmetleri Sertifikası

HSM: Donanımsal Güvenlik Modülü (Hardware Security Module)

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

MERSİS: Merkezi Sicil Kayıt Sistemi

MM ESHS: Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı

MÜS: Mali Mühür Sertifikası

PKI (Public Key Infrastructure): Açık Anahtarlı Altyapılar

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayımlama ve Bilgi Deposu Yükümlülükleri

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

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

2.1. Bilgi Depoları

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

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

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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

- Kamu SM'ye ait güncel Kök SHS ve Elektronik Mali Mühür SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Elektronik Mali Mühür SHS sertifikaları
- Kamu SM'ye ait Kök SHS sertifikalarının özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi
- Kamu SM Sİ ve SUE dokümanları
- Taahhütnameler

- Yönergeler
- Formlar
- Güncel sertifika iptal listeleri
- Kullanıcı test sertifikaları

2.3. Yayım Sıklığı ve Zamanı

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

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

2.4. Erişim Kontrolleri

Kamu SM bilgi deposuna bilgi edinme amaçlı erişim herkese açıktır. Bilgi deposunun güncellenmesi, yetkisi olan Kamu SM personeli tarafından gerçekleştirilmektedir.

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

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve değiştirilmeye karşı bütünlüğünü korumak
- Bilgi deposunda tutulan bilgilerin doğruluğunu ve güncelliğini sağlamak
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak
- Bilgi deposuna erişimi ücretsiz sağlamak

3. Kimlik Belirleme ve Doğrulama

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikalarında, sertifika sahibine isim/ünvan bilgilerinin belirtildiği DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediği isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Elektronik Mali Mühür Sertifikaları üzerinde yer alan kimlik bilgileri kurum/kuruluş/tüzel/gerçek kişileri tanımlayacak şekilde anlamlı olmalıdır.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Elektronik Mali Mühür Sertifikası içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Elektronik Mali Mühür Sertifikası içeriğinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kamu SM tarafından oluşturulan Elektronik Mali Mühür Sertifikaları içeriğindeki kimlik bilgileri kurum/kuruluş/tüzel/gerçek kişiler için ayırt edici niteliktedir.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

Elektronik Mali Mühür Sertifikası başvuru sahipleri başvuru esnasında başkalarına ait fikri ve sınai mülkiyet haklarına zarar verecek isimleri kullanamazlar. Kamu SM sertifika başvurusu esnasında kullanılan isimlerin fikri ve sınai mülkiyet haklarının başvuru sahibine ait olup olmadığını doğrulamaz. Ortaya çıkabilecek herhangi bir fikri ve sınai mülkiyet hakkı problemi ile ilgili olarak Kamu SM sertifika başvurusunu reddetme veya ürettiği sertifikaları iptal etme hakkına sahiptir. Problemin giderilmesine yönelik olarak Kamu SM herhangi bir arabuluculuk faaliyeti yürütmez.

3.2. İlk Kimlik Belirleme

Kamu SM, Elektronik Mali Mühür Sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kurum/kuruluş/tüzel/gerçek kişilerin doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliğinin Kanıtlanması

MÜS, GÜS ve Güvenli Mali Sertifika için açık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir. Sertifika sorumlusu tarafından Elektronik Mali Mühür Sertifikasının teslim alındığı teyit edilir. HSM yüklemelerinde ek olarak Mali Mühür Teslim Tutanağı düzenlenmektedir.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Elektronik Mali Mühür Sertifikası başvurusunda bulunan kurum/kuruluş/tüzel/gerçek kişilerin, talep edilen bilgileri, Kamu SM tarafından sunulan başvuru yöntemleriyle Kamu SM'ye bildirilir. Kamu SM, kurum/kuruluş/tüzel kişi tarafından iletilen bilgilere istinaden kurum kimliğini belirler. Kurumların vergi kimlik numaraları online işlemler sertifika başvurusu sırasında MERSİS üzerinden kontrol edilir. Online işlemler üzerinden başvuruda başarılı olamayan kurumların başvuruları GİB tarafından Kamu SM' ye gönderilir.

3.2.3. Kişisel Kimliğin Belirlenmesi

Elektronik Mali Mühür Sertifikası başvurusunda bulunan gerçek kişiler ve sertifika sorumluları, talep edilen bilgileri Kamu SM tarafından sunulan başvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, gerçek kişi tarafından iletilen bilgileri Kimlik Paylaşım Sistemi üzerinden doğrulayarak kişinin kimliğini belirler.

3.2.4. Doğrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi ve sertifika sorumluları tarafından başvuru sırasında ve daha sonra değişiklik sebebiyle beyan edilen aşağıdaki erişim bilgileri ve diğer bilgilerin doğruluğu Kamu SM tarafından kontrol edilmez:

- Telefon numaraları
- Elektronik Mali Mühür Sertifikası tesliminde kullanılacak adres bilgisi
- Elektronik posta adresleri

Bu bilgilerin doğruluğu kurum/kuruluş/tüzel/gerçek kişi beyanı üzerine kabul edilir.

Kurum/kuruluş/tüzel/gerçek kişi bu bilgileri Kamu SM'ye doğru beyan etmekle yükümlüdür. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı doğabilecek zararlardan, sertifikanın hatalı üretilmesinden ve sertifika yönetim sürecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin Doğrulanması

Elektronik Mali Mühür Sertifikası içeriğine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Bölüm 3.2'de anlatıldığı şekilde uygulanır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Elektronik Mali Mühür Sertifikası sahibi kurumun yetkilendirdiği sertifika sorumluları Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. GİB'den gelen iptal başvuruları ise doğrudan işleme alınır.

4. Sertifika Yaşam Döngüsü İşlevsel Gereklilikleri

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

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

Süreçler sertifika sahibi kurumlar ile kurum tarafından yetkilendirilen sertifika sorumluları ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

Elektronik mali mühür kullanmak isteyen kurum/kuruluş/tüzel/gerçek kişiler, başvurularını, https://onlineislemler.kamusm.gov.tr adresinden çevrim içi olarak yapabilirler. MERSİS sorgusundan başarılı geçen sertifika sahibi olmak isteyen kurum/kuruluş/tüzel/gerçek kişiler başarılı başvuru yapılabilir. Sertifika sorumlusunun çevrim içi olarak başvuru yapamaması durumunda, Elektronik Mali Mühür Sertifikası almak isteyenler başvurularını GİB'e yapar. GİB'in uygun gördüğü ve Kamu SM'ye bildirdiği tüm kurum/kuruluşlar/şirketler sertifika alabilirler.

Güvenli Mali Sertifika başvurusunda bulunmak isteyen kullanıcılardan GİB tarafından verilmiş onay yazısı beklenir. Onay yazısı alanlar Güvenli Mali Sertifika alabilirler.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Elektronik Mali Mühür Sertifikası başvurusu, kurum/kuruluş/tüzel/gerçek kişi tarafından Kamu SM'ye yapılır. Kamu SM'den alınacak sertifika hizmetlerinin şartları TÜBİTAK BİLGEM ile Gelir İdaresi Başkanlığı arasında imzalanan protokol, Kamu SM'nin web sitesi üzerinden yayımladığı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

Kurum/kuruluş/tüzel/gerçek kişi, Kamu SM Online İşlemler Mali Mühür Sertifika Başvurusu adresine gider, VKN ve/veya TCKN bilgisini girerek başvuru formuna ulaşır. Başvuru türüne göre formu doldurur, başvurusunu tamamlar ve son adım olan ödeme işlemini gerçekleştirir. Elektronik Mali Mühür Sertifikası HSM içerisinde kullanılacaksa başvuru formunu doldururken HSM başvuru türünü seçer ve başvuru tamamlandıktan sonra ödeme yapmadan önce Kamu SM ile iletişime geçer.

Kurum/kuruluş/tüzel/gerçek kişi başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kurum/kuruluş/tüzel/gerçek kişi, Kamu SM'ye göndermiş olduğu bilgilerin doğruluğunu takip etmekle ve bu bilgilerde değişiklik olması halinde belirlenmiş araç ve yöntemler ile Kamu SM'yi bilgilendirmekle yükümlüdür. Kamu SM, Elektronik Mali Mühür Sertifikası içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurum/kuruluş/tüzel/gerçek kişilerden veya GİB'den gelen dijital/ıslak imzalı verilerin/belgelerin Kamu SM tarafından incelenmesi sonucunda kimlik tanımlama ve doğrulama işlevleri yerine getirilir.

4.2.2. Sertifika Başvurusunun Kabul veya Redi

Elektronik Mali Mühür Sertifikası almak isteyen kurum/kuruluş/tüzel/gerçek kişi başvuruları vergi kimlik numaralarının MERSİS sorgusundan geçebilmesi ile kabul edilir. MERSİS sorgusundan geçemeyenler GİB üzerinden elektronik imzalı belge gelmesi sonucunda başvuru yapabilirler.

Güvenli Mali Sertifika başvurularının kabulü için GİB üzerinden onay yazısı gerekmektedir.

Başvurusu kabul edilen kurum/kuruluş/tüzel/gerçek kişiler Kamu SM sisteminde kullanıcı olarak tanımlanır ve sertifika üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ve ödeme işlemlerinin tamamlanmasının ardından sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

Bölüm 4.2.2'de yer alan esaslar uyarınca kabul edilen sertifika başvuruları Kamu SM tarafından işlenir. Kurum/kuruluş/tüzel/gerçek kişiler, işlem kapasitesini göz önünde bulundurarak başvuru sırasında sertifikanın yükleneceği donanım olarak akıllı kart ya da HSM tercih eder.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta yüklenen sertifika, sertifika sorumlusuna teslim edildiğinde Elektronik Mali Mühür sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

HSM cihazına sertifika yükleme işlemi, mali mühür sertifikası talebinde bulunan kurum/kuruluş/tüzel/gerçek kişinin HSM cihazı işlemleri için görevlendirdiği sertifika sorumlusu gözetiminde gerçekleştirilir. İşlem sonrasında teslim tutanağı imzalanır ve Elektronik Mali Mühür Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

4.4. Sertifikanın Kabulü

4.4.1. Sertifikanın Kabul Koşulu

Sertifika sorumlusu, kullanmaya başlamadan önce akıllı kart içerisindeki Elektronik Mali Mühür sertifikasının içeriğini kontrol eder ve doğrular. Sertifika içerisindeki bilgilerde eksik veya hata olması durumunda Kamu SM'yi bilgilendirir.

Elektronik Mali Mühür Sertifikasının HSM'ye yüklenmesi talebi durumunda yerinde ve uzaktan olmak üzere iki farklı yükleme seçeneği sunulmaktadır. Yerinde yükleme, kurum/kuruluş/tüzel/gerçek kişi tarafından belirtilen zorunlu hallerde Kamu SM personelinin sertifika isteyen kurum/kuruluş/tüzel/gerçek kişinin HSM cihazının bulunduğu yerleşkeye gidip HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini yerinde gerçekleştirdiği süreçlerdir. Uzaktan yükleme, Kamu SM ve kurum arasında yapılan güvenli uzak bağlantı sonrası Kamu SM personelinin HSM cihazına anahtar üretimi ve sertifika yükleme işlemlerini uzaktan gerçekleştirdiği süreçlerdir.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Elektronik Mali Mühür Sertifikaları, Kamu SM tarafından yayımlanmaz.

4.4.3. Sertifikanın Oluşturulmasının Diğer Taraflara Duyurulması

Sertifika oluşturulması ile ilgili bilgiler oluşturulan rapor sistemi üzerinden GİB'e iletilir.

4.5. Sertifikanın ve Özel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı

Sertifika sahibi; sertifikasını ve sertifikaya ait özel anahtarını, tabi olunan standartlar, Sİ ve SUE dokümanında ve ilgili sertifika sahibi taahhütnamesinde yer alan koşullar ve belirlenmiş sınırlar içinde kullanmalıdır.

4.5.2. Üçüncü Kişilerin Sertifika ve Açık Anahtarı Kullanımı

Sertifikaların içinde yer alan elektronik mali mühür imza doğrulama verisi üçüncü taraflarca doğrulama amacıyla kullanılır. Üçüncü taraflar, güvenecekleri sertifikanın ve sertifikayı oluşturan ESHS'nin sertifikasının geçerliliğini kontrol etmekle, sertifika "Anahtar kullanım" alanında belirtilen amaçlar doğrultusunda kullanıldığını doğrulamakla ve bu SUE'de belirtilen kullanım koşullarına uymakla yükümlüdürler.

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. Sertifikanın Yenilenmesi

Kamu SM, sertifika yenileme işlemini, yeni anahtar çifti üretmek suretiyle yerine getirir.

4.7.1. Sertifika Yenileme Koşulları

Sertifika yenileme işlemi aşağıdaki durumlarda yapılmaktadır:

- Elektronik Mali Mühür Sertifikasının kaybedilmesi veya çalınması
- Elektronik Mali Mühür Sertifikasının arızalanması
- Akıllı karta veya HSM'ye erişim verisinin kaybedilmesi, çalınması veya unutulması
- Elektronik Mali Mühür Sertifikasının iptal edilmesi ve yenisinin talep edilmesi
- Elektronik Mali Mühür Sertifikasının geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaşılması
- Elektronik Mali Mühür Sertifikasında bilgi değişikliği gerekmesi

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Bölüm 4.4.3'te tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

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

Kamu SM, sertifikada bilgi değişikliği gerçekleştirmez. Bilgi değişikliği gerekli olduğu durumlarda, sertifika yenileme süreci işletilir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

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

- Sertifika sahibinin kurum/kuruluş/tüzel/gerçek kişinin talebi
- Gelir İdaresi Başklanlığı tarafından gelen talep
- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi

- Sertifikanın hatalı üretilmesi
- Sertifika sahibi kurum/kuruluş/tüzel varlığın kapanması, iflasının öğrenilmesi
- Elektronik Mali Mühür özel anahtarlarının içinde bulunduğu elektronik mali mühür oluşturma aracının kaybolması, çalınması veya bozulması
- Akıllı kart veya HSM erişim verisinin unutulması veya kaybedilmesi
- Sertifikanın SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi
- Kamu SM'nin MÜS, GÜS veya Güvenli Mali Sertifikayı imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması
- Kamu SM'nin işleyişine son verilmesi ve verilen Elektronik Mali Mühür Sertifikalarının yönetim işlemlerinin başka bir ESHS tarafından devamlılığının sağlanamaması

4.9.2. Sertifika İptal Başvurusunu Kimler Yapabilir

Sertifika iptal başvurusu, sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi veya sertifika sahibi kurum/kuruluş/tüzel kişi tarafından yetkilendirilmiş Elektronik Mali Mühür Sertifika Sorumlusu veya GİB tarafından yapılabilir. Kamu SM, Bölüm 4.9.1'de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Elektronik Mali Mühür Sertifikasının iptal başvurusu, sertifika sahibi/sertifika sorumlusu veya GİB tarafından gerçekleştirilebilir. Sertifika sahibi veya sertifika sorumlusu, sertifika iptali için https://kamusm.bilgem.tubitak.gov.tr web sayfası üzerinden Online İşlemler menüsü aracılığı ile iptal başvurusu yapar.

GİB, iptal edilmesini istediği sertifika bilgilerini Kamu SM'ye resmi yazı ile bildirerek iptal talebinde bulunur. İptal talebinin Kamu SM'ye ulaşmasının ardından sertifika/sertifikalar iptal edilir.

İptal süreci, Kamu SM resmi web sitesinde ayrıntılı olarak anlatılmaktadır. Kamu SM, internet sitesi üzerinden iptal işleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar. Kamu SM iptal bilgilerini en kısa zamanda işler ve kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en azından Elektronik Mali Mühür Sertifikasının seri numarası ile Kamu SM'nin elektronik imzasını taşır. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da Elektronik Mali Mühür Sertifikasının durumunu iptal konumuna getirmek suretiyle duyurur.

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

Kurum/kuruluş/tüzel/gerçek kişi, Elektronik Mali Mühür Sertifikası iptal edildikten sonra yeniden Elektronik Mali Mühür Sertifikası talebinde bulunulabilir.

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen iptal başvurularını derhal işleme alır ve Elektronik Mali Mühür Sertifikasını en kısa sürede iptal eder. İptal edilen Elektronik Mali Mühür Sertifikası bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde işlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 4.9.7'de belirtilmiştir.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

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

Üçüncü kişiler Elektronik Mali Mühür Sertifikasına dayanarak işlem yapmadan önce Elektronik Mali Mühür Sertifikasının geçerliliğini SİL ya da ÇİSDUP yöntemlerinden birini kullanarak kontrol etmekle yükümlüdür.

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

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

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

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

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, Elektronik Mali Mühür Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduğu duyurulan imza oluşturma

verisiyle imzalanır. ÇİSDUP desteği olan uygulamalar Elektronik Mali Mühür Sertifikalarının geçerlilik durum kontrolünü ESHS Erişim Bilgisi (Authority Information Access) isimli sertifika uzantısında yer alan adres üzerinden gerçekleştirir.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi

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

SİL dosyası, iptal edilen her Elektronik Mali Mühür Sertifikası 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 Elektronik Mali Mühür Sertifikasının 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. Özel Anahtarın Güvenliğini Yitirmesi Durumu

Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişiye ait özel anahtarın güvenliğini yitirmesi durumunda Elektronik Mali Mühür Sertifikası iptal edilir. Elektronik Mali Mühür Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Elektronik Mali Mühür Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sağlamak amacıyla askıya alınabilir. Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi veya sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi tarafından yetkilendirilmiş Elektronik Mali Mühür Sertifika Sorumlusu aşağıda belirtilenlere benzer sebeplerden dolayı Elektronik Mali Mühür Sertifikasını askıya alabilir:

- Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişinin Elektronik Mali Mühür Sertifikasını kullanım dışı bırakmak istemesi

- Elektronik Mali Mühür Sertifikasının iptal sebebinin ortaya çıktığından şüphelenildiği durumlarda, yanlışlıkla iptalini engellemek amacıyla, Elektronik Mali Mühür Sertifikasının önce askıya alınmak istenmesi

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Elektronik Mali Mühür Sertifikasının askıya alma başvurusu, sadece sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi veya sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi tarafından yetkilendirilmiş Elektronik Mali Mühür Sertifika Sorumlusu tarafından yapılır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Elektronik Mali Mühür Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden yapılır. Askı başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi ve sertifika sorumlusunun kimlik belirlemesi ve doğrulaması yapılır. Askıya alınan Elektronik Mali Mühür Sertifikası için, SİL'de geçici olarak iptal edildiğini belirten sebep kodu kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir.

Sertifika sorumlusu, Kamu SM Online İşlemler üzerinden kurum/kuruluş/tüzel kişiye ait sertifikayı askıdan indirebilir. Askıya alınan sertifika en az bir defa SİL'e girmeden askıdan indirilemez. Kamu SM'ye ait Kök SHS ve Elektronik Mali Mühür SHS sertifikaları askıya alınmaz.

4.9.16. Askıda Kalma Süresi

Askıya alınan sertifikalar, en az bir kere SİL dosyasına girmeden askıdan indirilemez.

4.10. Sertifika Durum Servisleri

Üçüncü kişiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve ÇİSDUP servisleri aracılığıyla ulaşır.

4.10.1. İşletimsel Özellikleri

Üçüncü kişiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından erişebilirler. Kamu SM'ye ait SİL dosyalarına erişim bilgileri Bölüm 7.1.2 Tablo 1'de verilmiştir. Üçüncü kişiler, iptal durum kaydını her kontrol etmek istediklerinde güncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi Bölüm 7.1.2 Tablo 1'de verilmiştir. Üçüncü kişiler, Elektronik Mali Mühür Sertifikalarının 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

Elektronik Mali Mühür Sertifikasının kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM, Elektronik Mali Mühür Sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibi kurum/kuruluş/tüzel/gerçek kişileri ve Elektronik Mali Mühür sertifika sorumlularını bilgilendirir.

4.12. Anahtar Yeniden Üretme

Sertifika sahiplerine ait anahtarların yeniden üretilmesi veya yedeklenmesi işlemi uygulanmamaktadır.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Güvenlik Denetimleri

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

5.1.1. Tesis Yeri ve İnşaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yürütülmektedir. Kamu SM sisteminin çalıştığı binanın bulunduğu Gebze tesisi, yerleşim merkezinden uzak, yangın, su baskını, deprem, yıldırım ve hava kirliliğinden en az etkilenecek, giriş ve çıkışların kontrol edildiği bir bölgedir. Alanlara ve binalara erişim, tek kişinin girişine veya çıkışına izin veren HI-SEC kilitleme kapıları dahil olmak üzere fiziki güvenlik, video izleme ve kimlik doğrulama olmak üzere çoklu güvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrolü bulunan bir alandır. Yetkisiz personel ve kayıtsız ziyaretçiler bu hassas alanlara giremez.

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 üniteleri, yedekli iklimlendirme üniteleri, havalandırıcılar, yangın söndürücü sistemler mevcut olup, deprem, su ve afetlere karşı gerekli tedbirler alınmıştır.

5.1.2. Fiziksel Erişim

Kamu SM yazılım ve donanım modülleri ile arşivlere erişim denetim altındadır. Binaya girişler güvenlik görevlilerinin kontrolü altında, gelişmiş erişim kontrol cihazlarıyla sağlanmaktadır. Bina içinde Kamu SM sistemine ait yazılım ve donanım araçlarının bulunduğu, elektronik veya kağıt ortamdaki bilgilerin tutulduğu, sistemin işletildiği ve yönetildiği odalara erişim gelişmiş erişim kontrol cihazlarıyla yapılmaktadır. Güvenli alanlarda tek kişi çalışma yapamaz, en az biri yetkili olmak üzere 2 (iki) kişi ile çalışma yapılır. Yetkisi olmayan kişiler sistemin kurulu olduğu odalara giriş yapamamaktadır. Yetkisiz kişilerin donanım bakımı veya bunun gibi sıra dışı bir amaçla sistemin kurulu olduğu odalara girişleri özel erişim talimatları uyarınca düzenlenir.

5.1.3. Güç Kaynağı ve Havalandırma

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

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

Bina aşırı ısınmayı önleyebilecek kapasitede ve uygun nem seviyesini ayarlayabilecek özelliklerde kesintisiz/yedekli iklimlendirme sistemleri ile donatılmıştır.

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

Kullanılan veri saklama ortamları (disk, CD, kağıt vs.) bozulmaya, yıpranmaya karşı fiziksel ve elektronik olarak korunur. Buna ek olarak gerekli görülen ortamların yerinde yedeği alındığı gibi gerekli güvenlik kriterlerini sağlayan ayrı bir lokasyonda da yedekler alınmaktadır.

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduğu ve artık kullanılmayan elektronik veya kağıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir şekilde geri dönüşümsüz olarak imha edilir.

5.1.8. Farklı Mekanlarda Yedekleme

Kamu SM, farklı mekanda yedekleme işi için konum olarak tamamen ayrı, uzak bir felaket kurtarma merkezine sahiptir. Yedek sistemin bulunduğu mekan, asıl sistemin sağladığı tüm güvenlik ve işlevsellik şartlarını sağlar. Kamu SM, sisteminin sürekliliğini sağlayabilmek amacıyla gerekli gördüğü bileşenleri, farklı bir fiziksel mekanda güvenli kasalarda saklar.

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

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

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

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

Sistem Denetçisi: Sertifika hizmetleriyle ilgili iş ve işlemlerin denetlenmesinden sorumludur.

Sertifika Kayıt Sorumlusu: Sertifika üretim/iptal başvurusunun alınması, başvuru evraklarının ve kurum/kuruluş/tüzel/gerçek kişinin kimliğinin doğrulanmasından sorumlu personeldir.

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleştiren personeldir.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, Kök SHS ve Elektronik Mali Mühür SHS'ye ait sertifika üretilmesi ve iptal edilmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

Kamu SM, Kök SHS ve Elektronik Mali Mühür SHS'ye ait imza oluşturma verilerinin başka bir kriptografik modül içerisine yedeklenmesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar. Elektronik Mali Mühür Sertifikalarının üretimi iki kişinin kontrolünde gerçekleştirilir.

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilmektedir. Kamu SM sistemi içinde kimlik doğrulama güvenli donanım araçları, parolalar, gizli sorular ve biyometrik veri kullanılarak güncel kriptografik yöntemlerle yapılır. Kullanıcı hesapları yetkilendirme ve yönetiminde, Kamu SM Erişim Yönetimi Politikası temel alınmaktadır.

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

Aşağıda verilen roller arasında görevler ayrılığı vardır:

- Sertifika Üretim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında
- Sistem Denetçisi ile diğer roller arasında
- Sistem Yöneticisi ile Güvenlik Personeli ve Sistem Denetçisi arasında

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. Adli sicil kayıtları incelenir. Güvenlik soruşturması biten personel işe başlatılır. İşe başlayan personelin bilgi güvenliği farkındalık eğitimleri tamamlanmadan, sistemlere erişimine izin verilmez.

5.3.3. Eğitim Gerekleri

Çalışanlar, Kamu SM'deki işlerine aktif olarak başlamadan önce gerekli eğitimden geçirilirler. Çalışanlara verilen eğitimde Kamu SM'de uygulanan güvenlik ilkeleri, sistemin teknik ve idari işleyişi, işleriyle ilgili süreçler, süreç içindeki görev ve sorumluluklar anlatılır. Kamu SM, çalışanlarına yılda en az bir defa, siber güvenlik ve sosyal mühendislik saldırılarına karşı farkındalık oluşturmak amacıyla, bilgi güvenliği eğitimi vermektedir.

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

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

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

5.3.7. Anlaşmalı Personel Gereksinimleri

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

5.3.8. Sağlanan Dokümantasyon

Çalışanlara işleriyle ve Kamu SM süreçleriyle ilgili gerekli kılavuz ve destek dokümanlar ve bilgi güvenliği politikaları kapsamındaki ilgili dokümanlar 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 İşlemler

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

Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri

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

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

Sertifika yaşam döngüsü yönetimi işlemleri

- Sertifika başvurusunun işlenmesi
- Sertifika üretimi
- Sertifika yenileme
- Sertifika iptal etme
- SİL yayımlanması

Güvenlikle ilgili diğer işlemler

- Sisteme başarılı veya başarısız tüm erişim denemeleri
- Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
- Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
- Güvenlik profili değişiklikleri
- Sistemin çökmesi, donanım hataları ve diğer bozukluklar
- Güvenlik cihaz/yazılım işlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
- Kamu SM'ye ziyaretçi giriş ve çıkışı

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

5.4.2. Kayıtların İncelenme 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. 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. Talep edilmesi halinde kayıtlar yetkili denetçilere sunulur.

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

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

5.4.6. Kayıtların Toplanması

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

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

Elektronik ya da kağıt üzerinde tutulan kayıtlar ESHS tarafından arşivlenir.

5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi tarafından, başvuru sırasında verilen tüm bilgi ve belgeler
- Sertifika üretimi, yenileme, askıya alma, askıdaki sertifikayı kullanıma açma ve iptal başvuruları sırasında elektronik veya kağıt ortamda alınan formlar
- Sertifika işlemleriyle ilgili yapılan önemli yazışmalar
- Üretilen tüm sertifikalar
- Geçerlilik süresi dolan tüm Kamu SM kök ve alt kök sertifikaları
- Yayımlanan tüm sertifika iptal durum kayıtları
- Sertifika İlkeleri dokümanı
- Sertifika Uygulama Esasları dokümanı
- Sertifika yönetim prosedürleri
- Sertifika Sahibi Taahhütnameleri
- Sertifika Teslim Tutanakları
- Sertifikasyon süreçlerinde kullanılan sistemlerin NTP senkronizasyon logları

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler 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 Bölüm 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.

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 sertifikası kullanım süresinin dolmasından en geç 3 (üç) yıl önce; alt kök sertifikası kullanım süresinin dolmasından en geç 3 (üç) yıl önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalanmaya devam eder. Yeni üretilen sertifikalar için oluşturulan yeni SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.
- Kamu SM, anahtarlarının yenilendiği bilgisini Kamu SM resmi web sitesi üzerinden duyurur ve sertifika hizmeti verdiği kurumları bilgilendirir.

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

Donanım, yazılım veya veri bozulması durumları raporlanır ve arızanın/hatanın giderilmesi için gerekli süreç başlatılır. İş sürekliliğini sağlamak için sistemde kullanılacak aktif cihazlar ve depolama alan ağı bileşenleri yedekli yapıda çalışmaktadır ve kritik süreçler için felaket kurtarma merkezi oluşturulmuştur. 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. Özel Anahtarın Gizliliğinin Kaybedilmesi

Kamu SM'nin Elektronik Mali Mühür Sertifikalarını 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 Kamu SM resmi web sitesi üzerinden duyurur ve ilgili kurumları yazıyla bilgilendirir.
- Kamu SM, Elektronik Mali Mühür Sertifikası sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluşturulan Elektronik Mali Mühür Sertifikalarına güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikalarının gerekli görülen bir kısmı veya hepsi iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Elektronik Mali Mühür Sertifikası 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 Elektronik Mali Mühür Sertifikalarının 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 iş sürekliliği planlarında tanımlar. Kamu SM başka bir şehirde felaket kurtarma merkezine sahiptir. Kamu SM yedeklilik yönetim politikasına uygun olarak önemli veri ve uygulamaların yedeklerini almakta ve gerekli durumlarda yedekten geri dönme işlemlerini uygulamaktadır. İş sürekliliğinin devamı için Kamu SM merkez ofiste saklanan verilerin yedekleri felaket kurtarma merkezinde de saklanmaktadır. Kamu SM, arıza sonrası yeniden çalışırlığı sağlayacak Kamu SM iş sürekliliği planlarını periyodik olarak gözden geçirir ve test eder. Kamu SM arıza durumlarının tekrarlanmaması için gerekli önlemleri alır.

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM Hizmetleri Sonlandırma Planı dokümanında tanımlanmıştır.

6. Teknik Güvenlik Kontrolleri

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

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.2. Elektronik Sertifika Hizmet Sağlayıcısı Anahtar Çiftinin Üretimi

Kamu SM bünyesinde aşağıdaki anahtar çiftleri oluşturulur:

- Kök SHS'ye ait imza oluşturma ve doğrulama verisi
- Elektronik Mali Mühür SHS'ye ait imza oluşturma ve doğrulama verisi
- ÇİSDUP Yayımlayıcı'ya ait imza oluşturma ve doğrulama verisi
- Elektronik Mali Mühür Sertifikası sahiplerine ait anahtar çifti

Kök SHS, Elektronik Mali Mühür SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceği güvenli odada, birden fazla eğitimli personelin gözetiminde, ağ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiş, FIPS-140-2 seviye 3 veya EAL4+ standartlarını sağlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen özel anahtar güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dışarıya çıkarılmaz. Yapılan bütün işlemler kayıt altına alınır ve işlemi gerçekleştiren personel tarafından onaylanır.

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

6.1.3. Sertifika Sahibi Anahtar Çiftinin Üretimi

Elektronik Mali Mühür Sertifikası akıllı karta yüklenecekse, sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

Elektronik Mali Mühür Sertifikası HSM'e yüklenecekse, kurum/kuruluş/tüzel/gerçek kişinin HSM Cihaz Sorumlusu gözetiminde yetkili Kamu SM personeli tarafından, HSM içerisinde güvenli yazılım ve/veya donanım kullanılarak üretilir.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiş, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliği dünyaca kabul görmüş algoritmalar kullanılır.

Sertifika sahibine ait özel anahtarın yedeği alınmaz, bir kopyası hiçbir şekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandığı akıllı kart veya HSM Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.4. Sertifika Sahibine Özel Anahtarın Ulaştırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip; özel anahtar, sertifikayla birlikte akıllı kart veya HSM'ye yüklenir. Akıllı kart, imza karşılığı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye özel anahtar ve sertifika yükleme işlemi, kurum/kuruluş/tüzel/gerçek kişinin HSM Cihaz Sorumlusu gözetiminde gerçekleştirilir ve işlem sonrası Teslim Tutanağı doldurularak sorumlu kişi tarafından imzalanır.

Akıllı karta erişim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bağlantı protokolleri (HTTPS) kullanılmaktadır. Sertifika Sorumlusunun kimlik kontrolü için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu şekilde gerçekleştirilen kimlik doğrulaması sonrasında sertifika sahibi akıllı kart erişim verisine erişir. HSM'ye erişim verisinden Kamu SM sorumlu değildir, sertifika sahibinin insiyatifindedir.

6.1.5. Elektronik Sertifika Hizmet Sağlayıcısı'na Açık Anahtarın Ulaştırılması

Elektronik Mali Mühür Sertifikası HSM'ye yüklenecekse, PKCS#10 formatında sertifika imzalama isteği, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılığıyla Kamu SM'ye ulaştırılır.

Elektronik Mali Mühür Sertifikası akıllı karta yüklenecekse, Elektronik Mali Mühür Sertifikaları anahtar çiftleri Kamu SM tarafından üretildiği için açık anahtarın Kamu SM'ye ulaştırılması söz konusu değildir.

6.1.6. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

Kök SHS ve Elektronik Mali Mühür SHS sertifikaları, sertifikaların özet değeri ve özet algoritması Kamu SM resmi web sitesi Bilgi Deposu sayfası üzerinden yayımlanır.

6.1.7. Anahtar Uzunlukları

Kamu SM'ye ait kök ve alt köklerin ECDSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 384 bittir.

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

Kamu SM tarafından üretilen Elektronik Mali Mühür Sertifikalarına ait, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048 bittir.

6.1.8. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

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

6.1.9. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan anahtarların hangi amaçlar için kullanılabileceği sertifikadaki "Anahtar Kullanımı" uzantısı içerisinde belirtilir. Kamu SM kök anahtarı, alt kök sertifikasını ve SİL'i imzalamak için kullanılır. Kamu SM Elektronik Mali Mühür Sertifikalarının ve Güvenli Mali Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. ÇİSDUP yanıtlarının imzalanmasında alt kök ve kök tarafından yetkilendirilmiş ÇİSDUP sertifikası kullanılır.

6.2. Özel Anahtarın Korunması

6.2.1. Kriptografik Modül Standartları

Kamu SM'ye ait imza oluşturma verisi güvenli yazılım ve/veya donanım 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.
- Sistem kullanıcısına tanımlanan roller doğrultusunda, verdiği hizmetlere erişimi sınırlar.
- Düzgün çalıştığı test edilebilir, test sırasında hata oluştuğunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluşturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin özel anahtarının içinde bulunduğu akıllı kart veya HSM cihazı, özel anahtarın donanım dışına çıkmasını engelleyen ve donanıma erişimi parola ile sağlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibine ait akıllı kart veya HSM cihazı, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen aşağıdaki güvenlik standartlarından en azından birisini sağlar:
    - FIPS PUB 140-2'ye göre seviye 3 veya üzeri,
    - CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+.

6.2.2. Özel Anahtara Birden Fazla Kişi Kontrolünde Erişim

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

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. Özel Anahtarın Yedeklenmesi

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

Sertifika sahiplerine ait özel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahiplerine ait özel anahtarlar arşivlenmez. Kullanım süreleri sonunda geri dönüşsüz şekilde silinir.

6.2.6. Özel Anahtarın Kriptografik Modüle Yüklenmesi

Kamu SM'ye ait imza oluşturma verisi üretildikten hemen sonra kriptografik modüle yüklenir. İşlem, güvenilir yöntemlerle ve birden fazla yetkili personelin denetiminde yerine getirilir. Sertifika sahiplerine ait özel anahtarlar, sadece yetkili personelin kontrolünde akıllı kart veya HSM cihazına şifrelenerek yüklenir. Özel anahtar, akıllı kart veya HSM cihazına yüklendikten sonra kopyası sistemden silinir.

6.2.7. Özel Anahtarın Kriptografik Modülde Saklanması

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

Sertifika sahibinin özel anahtarı, kendisine ait akıllı kart veya HSM cihazı içinde saklanır, başka bir ortamda bulunmaz. Kamu SM, sertifika sahiplerine ait özel anahtarları kendi sistemi içinde saklamaz.

6.2.8. Özel Anahtara Erişim

Kamu SM'nin imza oluşturma verisine erişim birden fazla yetkili personelin 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 özel anahtar, akıllı kart veya HSM cihazı içinde sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

6.2.9. Özel Anahtara Erişimin Kesilmesi

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

Sertifika sahibinin kullandığı güvenli donanım araçları, özel anahtarı kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sahibinin erişim verisini yeniden girmesi gerekir. Erişim verisinin art arda 3 (üç) defa yanlış girilmesi durumunda güvenli donanım aracı kilitlenir ve araca erişim sağlanamaz.

6.2.10. Özel Anahtarın 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 özel anahtarların kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından akıllı kart veya HSM cihazı 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 İlgili Diğer Konular

6.3.1. Açık Anahtarın Arşivlenmesi

Kamu SM'ye ve sertifika sahibine ait açık anahtarlar, sertifikalar içinde tutulur ve Elektronik Mali Mühür Sertifikaları kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arşivlenir. Elektronik Mali Mühür Sertifikalarının arşivleri yetkisiz kişilerce tahrifatına ve silinmesine karşı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Elektronik Mali Mühür Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Elektronik Mali Mühür Sertifikasının kullanım süresinin dolmasıyla ya da Elektronik Mali Mühür Sertifikasının iptal edilmesiyle özel anahtarın kullanımı sona erer.

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan algoritmaya göre belirlenir. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 3 (üç) yıl için kullanılır.

Üretilen Elektronik Mali Mali Mühür Sertifikalarının son kullanma tarihi, Elektronik Mali Mühür SHS Sertifikasının son kullanma tarihini aşamaz.

6.4. Erişim Denetim Verileri

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

Sertifika sahibi kuruma ait iki farklı erişim denetim verisi tanımlanmıştır. Bunlar, akıllı karta erişim verisi ile sertifika işlemlerinin yapıldığı internet şubesine erişim verileridir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

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

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

6.4.2. Erişim Denetim Verilerinin Korunması

Kamu SM sistemi içinde kullanılan erişim denetim verileri yalnızca yetkili çalışanlar tarafından bilinir. Sertifika sahibi kuruma ait erişim parolaları sertifika sahibi kuruma güvenli yöntemlerle ulaştırılır.

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

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları, iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

Kamu SM sistemi içinde kötü niyetli yazılımlara karşı gereken önlemler alınır. Sistemde ağ ve sunucu bazlı sensörler içeren saldırı tespit sistemi bulunmaktadır. Bütün sunucular üzerinde merkezden yönetilebilen virüs tespit ve temizleme ajanları kurulmuştur, bunlar sürekli güncel tutulmaktadır. Kritik işlemlerin yapıldığı bilgisayarlar ağ ortamı dışında tutulur. Bilgilerin tahrifata, silinmeye ve kaçağa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliği konusunda bütün iyileştirme eylemleri gecikmesiz uygulanır. Güvenlik yamaları değerlendirilip daha büyük bir riske sebebiyet vermesi durumunda yüklenmez ve risk süreç takip sistemi üzerinde kayıt altına alınır. Ağ bileşenleri ve konfigürasyonları dönemsel olarak ağ güvenliği prosedürü yönergesine göre kontrol edilir.

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda verilmiştir:

- Yeterli düzeyde kalite ve güvenlik tedbirleri alınır.
- Belirlenen güvenlik kriterlerine uygun personel çalıştırılır.
- Her kurulan yazılımın yedek kopyası yaratılır.
- Sertifika işlemlerinin sürekliliğini sağlamak için sistem bilgilerini tutan bileşenlerin yedekleri oluşturulur.
- Sistemin açık ağa bağlantısında gerekli güvenlik önlemleri alınır.
- Kurulum sırasında dışarıdan gelen yazılımlar kullanılmadan önce virüs ve resmi olmayan yazılımların sisteme girmesi engellenir. Bu konuda tüm güvenlik gerekleri yerine getirilir, bütün iyileştirme eylemleri gecikmesiz uygulanır.
- Anormal sistem koşullarını yakalamak için ilk dönemlerde sistem durumları yakından gözlemlenir.
- Geliştirilmekte olan sisteme erişim kimlik, parola gibi tanıtıcı bilgilerin doğrulanmasıyla yapılır.
- Sistemin geliştirilmesi sırasında yapılan işler TS ISO/IEC 27001 gereklerini sağlar.
- Geliştirme faaliyetleri sırasında geliştirme, test ve canlı sistemler ayrılır. Canlıya alınma işlemi onay mekanizmalarından sonra gerçekleştirilir.
- Sistem bileşenlerine dair periyodik risk değerlendirmeleri yapılır ve yönetime sunulur.
- Sistemlerde gerçekleştirilen değişiklikler kayıt altına alınır ve izlenir.
- Uzaktan erişim dahil üçüncü tarafların sistemlere erişimine izin verilmez.

6.6.2. Güvenlik Yönetimi Kontrolleri

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

sonucunda açıklanır ve düzeltici önlemler alınır. Güvenlik kontrolleri için temel dayanak ISO 27001'in güncel sürümüdür.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

Son teknolojik gelişmeler göz önünde bulundurularak gerekli ağ güvenliği kontrolleri yapılır. Sertifikasyon işlemlerinde ağlar arası gereksinim duyulmayan protokoller güvenlik duvarları ile engellenmiştir. Sistem, dışa açık ağa bağlantısında saldırı engelleme özellikli yeni nesil güvenlik duvarları kullanır. Sistemdeki sunucu ve aktif cihazların durum ve performanslarını izlemek, geçmişe yönelik performans raporları çıkarmak ve geleceğe yönelik performans eğilimlerini saptamak amacı ile ağ ve sistem yönetimi altyapıları mevcuttur.

Sunucular üzerine ağ ve sistem yönetimi ve güvenliği ajanları kurulmuştur. Yönetim yazılımı bu ajanlardan disk, hafıza, işlemci kullanımı, dosya bütünlüğü, güvenlik kayıtları, harici depolama üniteleri takibi vb. bilgileri çeker ve bu bilgileri gerçek zamanlı görüntüler. Sunucuların çalışması için önem arz eden kaynaklar için eşik değerler belirlenir ve bu eşik değerlerin aşılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ağ ve sistem yönetimi ve güvenliği altyapısı çektiği bilgileri merkezi bir veri tabanında saklar. Böylece herhangi bir anda verilerin sorgulanmasına ve geçmişe dönük rapor üretilmesine imkan tanınır. Farklı güvenilir sistemlerle iletişim ihtiyacı olması durumunda, diğer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldığı sistemler (kök ve alt kök sunucuları gibi) için farklı ağ segmentleri oluşturulmuştur. Kritik işlemlerin yapıldığı sistemler ağa bağlı değildir. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıştır. Güvenli ve yüksek güvenli bölgelere erişimler erişim kontrol protokolüne göre belirlenir. Yüksek güvenlik gerektiren sistemlerde kullanılan donanımlar farklı yerlerde tekrar tekrar kullanılmaz, imha edilirler.

Bilgi işlem yöneticileri, uygulama geliştiricileri gibi farklı çalışan gruplarına ait farklı amaca hizmet eden ağlar da birbirinden ayrılmıştır. Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler, güvenlik ekibince kontrollü olarak verilir ve kayıtlar üzerinden izlenir. Farklı bölgelere olan iletişim ve erişim engellendiği gibi gerekli olmayan bağlantı ve hizmetler de ağ güvenliği açısından devre dışı bırakılır.

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller sıkılaştırma prosedürlerine göre kaldırılır ya da devre dışı bırakılır. Ağ ve sistem güvenliğine dair tüm işlemler siber olaylara müdahale ekibi tarafından izlenir ve gerektiğinde olay müdahale süreçleri doğrultusunda aksiyon alınır. Kamu SM çevrim içi açık anahtar altyapısı hizmetlerinin devamlılığı için Kamu SM ana merkez ve felaket kurtarma merkezinin dış ağ bağlantı hizmetlerini yedekli olarak kurgulamıştır.

Sistemler üzerinde periyodik olarak zafiyet taramaları ve yılda en az bir kez penetrasyon testi yapılır. Penetrasyon testini yapan kişi veya kurum; test metot ve araçlarını, testleri yapan kişilerin

yetkinliklerini içeren raporlar hazırlar. Bu raporlar Kamu SM tarafından saklanır. Sistemlerin belirlenen kural setlerine uygunluğu düzenli olarak gözden geçirilir.

6.8. Zaman Damgası

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

Zaman damgasıyla ilgili ayrıntılı bilgi Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esaslarında bulunur.

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından dağıtılan Elektronik Mali Mühür Sertifikalarının içeriği ile ilgili bilgilendirme yapılmaktadır.

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

Kamu SM tarafından dağıtılan Elektronik Mali Mühür Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geçerlilik tarihi, ilgili açık anahtar, sertifika sahibi kurum/kuruluş/tüzel/gerçek kişinin adı ve vergi kimlik numarası/TC numarası, 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. Elektronik Mali Mühür Sertifikasının içeriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine bağlı olarak belirlenir.

Tablo 1 MÜS ve GÜS Sertifikası Uzantıları

Sertifika Uzantısı	Kritik Uzantı	Açıklama
Temel Kısıtlar[1]	EVET	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
Yetkili Anahtar Tanımlayıcısı[2]	HAYIR	Kamu SM'ye ait Elektronik Mali Mühür SHS 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 Kullanımı[4]	EVET	MÜS anahtarlarının sadece mühürleme amaçlı kullanıldığının ifade edilmesi için "digitalSignature" [dijital imzalama] alanı seçilmiştir. GÜS anahtarlarının sadece anahtar şifreleme ve anahtar anlaşması amaçlı kullanıldığının ifade edilmesi için "keyAgreement" [anahtar anlaşması] alanı ve "keyEncipherment" [inkar edilemezlik] alanı seçilmiştir.
SİL Dağıtım Noktaları[5]	HAYIR	http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.crl
Yetkili Bilgi Erişimi[6]	HAYIR	http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.crt http://cisdupmms3.kurumsal.kamusm.gov.tr

[1] BasicConstraints

[2] AuthorityKeyIdentifier

[3] SubjectKeyIdentifier

[4] KeyUsage

[5] CRLDistributionPoints

[6] AuthorithyInformationAccess

Sertifika İlkeleri[7]	HAYIR	Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.4.1) ile SUE dokümanının bulunduğu http://depo.kamusm.gov.tr/ilke internet adresini içerir.
Genişletilmiş Anahtar Kullanımı[8]	HAYIR	MÜS için (2.16.792.1.2.1.1.5.7.50.1)[Kamu SM Mali Mühür] GÜS için (1.3.6.1.5.5.7.3.2)[istemci kimlik doğrulaması]

Tablo 1'de Kamu SM tarafından üretilen MÜS ve GÜS Sertifikalarında asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Tablo 2 Güvenli Mali Sertifikası Uzantıları

Sertifika Uzantısı	Kritik Uzantı	Açıklama
Temel Kısıtlar[9]	HAYIR	Sertifikanın son kullanıcı sertifikası olduğu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir.
Yetkili Anahtar Tanımlayıcısı[10]	HAYIR	Kamu SM'ye ait Elektronik Mali Mühür SHS açık anahtarının SHA-1 özet çıktısından oluşur.
Sertifika Anahtar Tanımlayıcı[11]	HAYIR	Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı[12]	EVET	MÜS anahtarlarının sadece mühürleme amaçlı kullanıldığının ifade edilmesi için "digitalSignature" [dijital imzalama] alanı seçilmiştir. GÜS anahtarlarının sadece anahtar şifreleme ve anahtar anlaşması amaçlı kullanıldığının ifade edilmesi için "keyAgreement" [anahtar anlaşması] alanı ve "keyEncipherment" [inkar edilemezlik] alanı seçilmiştir.

[7] CertificatePolicies

[8] ExtendedKeyUsage

[9] BasicConstraints

[10] AuthorityKeyIdentifier

[11] SubjectKeyIdentifier

[12] KeyUsage

SİL Dağıtım Noktaları[13]	HAYIR	http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.crl
Yetkili Bilgi Erişimi[14]	HAYIR	http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.crt http://cisdupmms3.kurumsal.kamusm.gov.tr
Sertifika İlkeleri[15]	HAYIR	Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.4.1) ile SUE dokümanının bulunduğu http://depo.kamusm.gov.tr/ilke internet adresini içerir.
Genişletilmiş Anahtar Kullanımı[16]	HAYIR	(2.16.792.1.2.1.1.5.7.50.4)[Güvenli Mali Sertifika]

Tablo 2'de Kamu SM tarafından üretilen İşletici Kuruluş (Güvenli Mali) Sertifikalarında asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

Kamu SM, kurumlara verdiği Elektronik Mali Mühür Sertifikalarını imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır. Sertifika sahiplerine ait anahtar çiftleri RSA algoritması anahtar çiftleridir. Kullanılan algoritmaların nesne tanımlama numaraları X.509 sertifikaları içinde belirtilir.

7.1.4. İsim Alanı Biçimleri

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

[13] CRLDistributionPoints

[14] AuthorithyInformationAccess

[15] CertificatePolicies

[16] ExtendedKeyUsage

7.1.5. İsim Kısıtları

Bölüm 3.1 de belirtilmiştir.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bağlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.4.1

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" Elektronik Malü Mühür Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. MÜS, GÜS ve Güvenli Mali Sertifika üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen sertifikaların "Sertifika edilen kurallara işaret eden Sİ/SUE dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen sertifikaların "Sertifika İlkeleri" uzantısının içinde yer alır. "Sertifika İlkeleri" uzantısının içinde "İlke Niteleyici" olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

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

İlke niteleyici olarak http://depo.kamusm.gov.tr/ilke/ yer alır.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

Üretilen SİL'ler "ITU X.509 V.2" SİL formatına uygun olarak aşağıdaki bilgileri içerir:

- SİL'i oluşturan Kamu SM'ye ait isim bilgileri

- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL'i imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL'in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanma tarihi
- İptal edilen Elektronik Mali Mühür Sertifikaları ile ilgili aşağıdaki bilgiler:
    - Sertifikanın seri numarası
    - Sertifikanın iptal tarihi
    - Sertifikanın neden iptal edildiği bilgisi
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM'ye ait sertifikanın "Yetkili Anahtar Tanımlayıcı" numarası

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir:

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

ÇİSDUP yanıtları aşağıdaki bilgileri içermektedir:

- Versiyon bilgisi
- Yanıtlayıcının adı
- Her bir sertifika için cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geçerlilik süresi)
- Kullanılan imza algoritmasının nesne tanımlama numarası

- ÇİSDUP Yanıtlayıcı imzası

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

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

Good [iyi]: Sertifika geçerli konumdadır.

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

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

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

8. Uygunluk Denetimleri

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

8.2. Denetçinin Nitelikleri

ISO/IEC 27001 BGYS'nin denetimi akredite edilmiş kuruluşlarca gerçekleştirilir. İç denetim, Kamu SM sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

BTK kanun gereği tüm ESHS'leri denetlemekle yetkili kılınmış düzenleyici kurumdur. ISO/IEC 27001 BGYS'nin denetimi bağımsız ve akredite edilmiş kuruluşlarca gerçekleştirillir. Dış denetçiler, herhangi bir çıkar çatışması olmaması ve bağımsızlığın zedelenmemesi için Kamu SM'den bağımsız kişilerden oluşur. İç denetim için seçilen denetçiler ise denetlenecek birimden seçilmez.

8.4. Denetimin Kapsamı

Kamu SM iç denetimlerinde, Sİ ve SUE dokümanına uygunluk denetlenir. İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli tarafından belirlenir. ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun şekilde bağımsız kurum denetçisi tarafından belirlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

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

ISO/IEC 27001 standardına göre gerçekleştirilen denetimlerde ortaya çıkan eksiklikler, Kamu SM tarafından planlı çalışma ile giderilir. Eksiklikler, BGYS'nin temel işleyişini etkileyecek kadar büyük ise Kamu SM, ISO/IEC 27001 uygunluk belgesi eksikler giderilinceye kadar askıya alınır. İç denetimlerde ortaya çıkan eksiklikler, Kamu SM ilgili personeli tarafından giderilir. Tüm denetimlerden elde edilen bulgular Uygunsuzluk veya Düzeltici/İyileştirici Faaliyetler açılarak takip edilir.

8.6. Sonucun Bildirilmesi

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

İç denetim sonucu, Kamu SM üst yönetimine raporlanır.

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen, yenilenen ve güncellenen Elektronik Mali Mühür Sertifikası için kurumlardan ücret alınır. Ücretin miktarı ve ödeme şekli Kamu SM web sitesinde bildirilir. Kamu SM'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması, sertifika ilkelerinin değişmesi ya da Elektronik Mali Mühür Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Elektronik Mali Mühür Sertifikalarının Kamu SM tarafından iptal edilmesi ve güncellenmesi halinde, hiçbir ücret talep edilmez.

9.1.2. Sertifika Erişim Ücreti

Kamu SM, kendisine ait sertifikaları resmi web sitesinde ücretsiz olarak yayımlar.

9.1.3. İptal Durum Kaydına Erişim Ücreti

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

9.1.4. Diğer Servis Ücretleri

Sertifika yönetim prosedürleri için elektronik ortamdan ve çağrı merkezi üzerinden otomatik olarak gerçekleştirilen işlemlerden ücret talep edilmez. Kamu SM, kuruma ait özel anahtar ve sertifikanın saklandığı akıllı kartın teminini kendi imkanlarıyla sağlayabilir. Elektronik Mali Mühür Sertifikaları ve güvenli donanım araçları için ödenecek bedelin miktarı Kamu SM web sitesinde bildirilir. Ödemenin usulüne uygun biçimde yapılmaması durumunda Elektronik Mali Mühür Sertifikası üretimi yapılmayabilir. Kamu SM, bilgi deposundan yayımladığı bilgi ve dokümanlara erişim için sertifika sahibi kurumdan veya üçüncü kişilerden ücret talep etmez.

9.1.5. İade Ücreti

Ön ödemeli olarak talepte bulunulan sertifikanın/sertifikaların üretimi tamamlanmamışsa sipariş Kamu SM tarafından incelenir ve kurumun talebi doğrultusunda yatırılan miktar kadar ücret iadesi yapılır. Üretilen sertifikalar için ücret iadesi söz konusu değildir.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

Düzenlenmesine gerek duyulmamıştır.

9.2.2. Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM tarafından oluşturulan Elektronik Mali Mühür Sertifikası'nın sertifika sorumlusu ve üçüncü taraflar tarafından kullanımı ile ilgili doğabilecek risklerden sertifika sorumlusu ve üçüncü taraflar sorumludur.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

Kamu SM resmi web sitesi bilgi deposu üzerinden yayımlanan doküman ve sertifikalar içerisinde yer alan bilgiler 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

Kamu SM verdiği hizmetlerde sertifika sahiplerinin ve diğer paydaşların kişisel verilerinin gizliliğini 2017/21 Sayılı Başbakanlık Genelgesi ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki mer'i mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurum/kuruluş/tüzel/gerçek kişiler ve yetkilendirdiği Elektronik Mali Mühür Sertifikası Sorumlusu, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği bilgiler 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

Elektronik Mali Mühür Sertifikası içeriğinde bulunan bilgiler, aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM, sertifika talep eden kurum/kuruluş/tüzel/gerçek kişilerden Elektronik Mali Mühür Sertifikası 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 sahibi kurumun bilgilerine erişirler.

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

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

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

9.4.6. Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM tarafından sertifika sorumlularına 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 Elektronik Mali Mühür Sertifikaları ve dokümanlar ile bu SUE dokümanına bağlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlülükler

Kamu SM, sertifika sahipleri ve üçüncü kişiler, sertifika sözleşmeleri ve taahhütnamelerde sözü geçen yükümlülükleri yerine getirirler.

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

ESHS olarak Kamu SM'nin yükümlülükleri aşağıda belirtilmiştir:

- Hizmetin gerektirdiği nitelikte personel istihdam etmek
- Belirlediği ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak
- Kök SHS ve Elektronik Mali Mühür SHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak
- Kök SHS ve Elektronik Mali Mühür SHS sertifikalarını son kullanıcıların erişebileceği ortamlarda yayımlamak
- Elektronik Mali Mühür Sertifikasının içeriğindeki bilgilerin doğruluğunu GİB'den gelen web servis cevaplarına dayanarak sağlamak
- GİB web servis cevabından olumsuz dönen ve GİB tarafından başvurusu gönderilmeyen başvuru sahiplerine Elektronik Mali Mühür Sertifikası vermemek
- Elektronik Mali Mühür Sertifikası başvurularını değerlendirerek, başvurunun sonucu hakkında kurumları ya da kurumların yetkilendirdikleri sorumlu kişileri bilgilendirmek
- Elektronik Mali Mühür Sertifikası başvurusu kabul edilmiş kurumlar için anahtar çifti ve Elektronik Mali Mühür Sertifikası üretmek
- Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişilere ait özel anahtarı oluşturduktan sonra özel anahtar ve üretiminde kullanılan gizli değişkenleri kendi sisteminden silmek, özel anahtarın kopyasını hiçbir şekilde tutmamak
- Sertifika sahibine akıllı kart temin etmesi durumunda, bu aracın güvenli olmasını sağlamak
- Üretilen Elektronik Mali Mühür Sertifikaları özel anahtarlarını Sİ ve SUE'de belirtilen şekilde güvenli olarak sertifika sahiplerine teslim etmek
- Elektronik Mali Mühür Sertifikalarının kullanım şartlarını belirleyen sertifika profillerini oluşturmak
- Elektronik Mali Mühür Sertifika başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli işlemlerini yapmak
- Elektronik Mali Mühür Sertifikası askıya alma başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli askıya alma işlemlerini yapmak
- Elektronik Mali Mühür Sertifikası askıdan indirme işlemlerini Sİ ve SUE'de belirtilen şekilde yapmak
- Elektronik Mali Mühür Sertifikası iptal başvurularını Sİ ve SUE'de belirtilen şekilde kabul etmek ve değerlendirerek gerekli iptal işlemlerini zamanında yapmak
- Yayımlanan Sİ ve SUE dokümanlarına uygun olmayan Elektronik Mali Mühür Sertifikası kullanımlarının tespit edilmesi durumunda ilgili Elektronik Mali Mühür Sertifikasını iptal etmek

- İptal edilmiş Elektronik Mali Mühür Sertifikası bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılığıyla duyurmak
- Elektronik Mali Mühür Sertifikalarının ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini sağlamak için her türlü tedbiri almak
- Sertifika sahiplerine ait elektronik veya kağıt ortamda tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek
- Elektronik Mali Mühür Sertifikası üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını tutmak
- İşleyiş sırasında kullanılan tüm kağıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen süreler boyunca güvenli olarak saklamak

9.6.2. Kayıt Birimi Yükümlülükleri

Kayıt birimlerinin yükümlülükleri Bölüm 9.6.1'de belirtilen ESHS yükümlülükleri ile aynıdır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri aşağıda belirtilmiştir:

- Elektronik Mali Mühür Sertifikası başvuru, askıya alma, iptal ve diğer işlemleri, ilgili Sİ ve SUE'de belirtildiği şekilde, detayları Kamu SM Elektronik Mali Mühür Sertifikası yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek
- Elektronik Mali Mühür Sertifikası başvurusu, yenileme ve iptal işlemleri sırasında doğru bilgi beyan etmek
- Kurum/kuruluş/tüzel/gerçek kişi adına düzenlenen Elektronik Mali Mühür Sertifikası üretildiğinde sertifikadaki bilgilerin doğruluğunu kontrol etmek
- SUE Bölüm 6.2.1'de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- Özel anahtarın güvenliğini sağlamak, kendisine ait özel anahtarın içinde bulunduğu akıllı kart veya HSM'in ve erişim verisinin gizliliğini korumak, bunları başkasına kullandırmamak ve bu konuda gerekli tedbirleri almak
- İnternet veya çağrı merkezi üzerinden sertifika işlemlerini yapabilmesi için kullandığı parolalarının gizliliğini ve güvenliğini sağlamak
- Özel anahtarın içinde bulunduğu akıllı kart veya HSM'in kaybolması, çalınması veya özel anahtarın gizliliğinin yitirildiğinden şüphelenmesi durumunda Elektronik Mali Mühür Sertifikasının iptal edilmesi için Kamu SM'ye en kısa zamanda başvurmak
- Akıllı kart veya HSM erişim verisini ve sertifika işlemlerinde kullandığı diğer parolaları düzenli olarak değiştirmek

- Elektronik Mali Mühür Sertifikası içeriğinde bulunan bilgilerin değişmesi durumunda derhal sertifikanın iptal edilmesi için Kamu SM'ye başvurmak
- Elektronik Mali Mühür Sertifikası başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri derhal Kamu SM'ye bildirmek
- İptal olmuş, kullanıma açılmamış, askıya alınmış veya geçerlilik süresi dolmuş Elektronik Mali Mühür Sertifikası ile işlem yapmamak
- Özel anahtarını imzalama amacıyla kullanmamak

Sertifika sahibi kurum/kuruluş/tüzel/gerçek kişi, Kamu SM Elektronik Mali Mühür Sertifikası Sİ ve SUE dokümanlarında belirtilen şartları okuduğunu, başvuru süreci ve sertifika geçerliliği boyunca Sİ ve SUE dokümanında belirtilen şartlara uygun olarak hareket edeceğini kabul ve taahhüt eder. Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin/kurumun zarara uğraması halinde TÜBİTAK BİLGEM'in ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, Elektronik Mali Mühür Sertifikasıyla işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Elektronik Mali Mühür Sertifikasının tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak
- Elektronik Mali Mühür Sertifikasının kullanım süresinin dolup dolmadığını kontrol etmek
- Elektronik Mali Mühür Sertifikasının geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek
- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikası içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak
- Elektronik Mali Mühür Sertifikasının doğruluğunu Elektronik Mali Mühür SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak
- Elektronik Mali Mühür SHS sertifikasının doğruluğunu Kök SHS sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak
- Kök SHS sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak
- Sertifika sahibinin Elektronik Mali Mühür Sertifikasının içindeki açık anahtarına karşılık gelen özel anahtara sahip olduğunu doğrulamak

9.6.5. Diğer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurum/Kuruluş/Tüzel Kişi Yükümlülükleri

Kamu SM'ye sertifika başvurusunda bulunan kurum/kuruluş/tüzel kişinin yükümlülükleri aşağıda belirtilmiştir:

• Sertifika yönetim süreçlerinde Kamu SM ile iletişim içinde olacak GİB sisteminde kayıtlı kurum yetkililerinden birini kurum sertifika sorumlusu olarak görevlendirmek ve başvuru sırasında sertifika sorumlularının bilgilerini Kamu SM'ye bildirmek

• Kurum sertifika sorumlusunun görevi sonlandırıldığında sertifika ile ilgili işlemleri gerçekleştirmek için yeni sorumlu bildirmek, bunu Kamu SM'ye dilekçe ve imza sürküsü göndererek bildirmek

• Yeni görevlendirdiği kurum sertifika sorumlularının bilgilerini Kamu SM'ye dilekçe ile bildirmek

9.6.5.2. Sertifika Sorumlularının Yükümlülükleri

Kurum/kuruluş/tüzel kişi adına Elektronik Mali Mühür Sertifikası başvurusunda bulunan Elektronik Mali Mühür Sertifikası Sorumlusunun yükümlülükleri aşağıda belirtilmiştir:

• Sertifika alınacak kurum/kuruluş/tüzel kişi ait bilgileri tam ve doğru bir şekilde Kamu SM'ye iletmek

• Sertifika yönetim süreçleri ile ilgili işleri Kamu SM ile koordineli bir şekilde yürütmek

9.7. Yükümlülüklerden Feragat

Düzenlenmesine gerek duyulmamıştır.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar Elektronik Mali Mühür Sertifika İlkeleri ve Uygulama Esasları ve varsa imzalanan sözleşmelerde belirlenir.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

T.C. Hazine ve Maliye Bakanlığı'nın yayımladığı 19/10/2019 tarih 509 sıra numaralı ve 01/09/2019 tarih 507 sıra numaralı Vergi Usul Kanunu Genel Tebliğ ve GİB ile TÜBİTAK-BİLGEM arasında imzalanan

protokol gereğince; GİB'in bildirdiği/uygun gördüğü tüm vergi mükelleflerine MÜS, GÜS, Güvenli Mali Sertifika üretilmektedir.

TÜBİTAK-BİLGEM vergi mükellefleri ile herhangi bir sözleşme imzalamamaktadır.

9.10.1. Anlaşma Süresi

Düzenlenmesine gerek duyulmamıştır.

9.10.2. Anlaşmanın Sona Ermesi

Düzenlenmesine gerek duyulmamıştır.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Düzenlenmesine gerek duyulmamıştır.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

Kamu SM, sertifika yönetim prosedürlerinde sertifika başvurusunun sonucu, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sorumlusunu ve/veya GİB'i bilgilendirir. Bilgilendirmeler telefon, faks veya e-posta aracılığıyla olur. Sertifika yönetimiyle ilgili kritik görünen işlemlerle ilgili bilgilendirmeler resmi yazıyla yapılır.

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metotları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan değişiklikler dokümanın yenilenerek Kamu SM bilgi deposu üzerinden erişime açılması ile duyurulur. Yenilenen doküman en fazla 1 (bir) hafta sonra bilgi deposundan yayımlanır ve yayımlandığı tarihte yürürlüğe girer.

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 Maliye Bakanlığı'nın yayınladığı 19/10/2019 tarih 509 sıra numaralı ve 01/09/2019 tarih 507 sıra numaralı Vergi Usul Kanunu Genel Tebliğ'ine başvurulur. İhtilafların sulhen çözümünün mümkün olmaması halinde, ihtilafların çözümünde görevli ve yetkili mahkeme Türkiye Cumhuriyeti Gebze Mahkemeleri'dir.

9.14. Uygulanacak Hukuk

SUE dokümanındaki hükümler, Maliye Bakanlığı'nın yayınladığı 19/10/2019 tarih 509 sıra numaralı ve 01/09/2019 tarih 507 sıra numaralı Vergi Usul Kanunu Genel Tebliğ'e uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. Kamu SM Kurumsal Kök Sertifikası

Alan	Değer
Sürüm	V3
Seri Numarası	00c301
İmza Algoritması	sha-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 2 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	11 Ağustos 2022 Perşembe 11:35:24
Geçerlilik Sonu	11 Ağustos 2042 Perşembe 11:35:24

Konu	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 2 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	**Değer**
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 14 06 5b 27 be 98 35 16 61 30 c6 af dc 25 29 31 6e e3 ca 20
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama , Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

10.2. Kamu SM Mali Mühür Alt Kök Sertifikası

Alan	**Değer**
Sürüm	V3
Seri Numarası	00e643
İmza Algoritması	sha-384 ile ECDSA {1 2 840 10045 4 3 3}
Sertifikayı Veren	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 2 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	28 Eylül 2023 Perşembe 16:15:11
Geçerlilik Sonu	28 Eylül 2033 Perşembe 16:15:11
Konu	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 C = TR
Ortak Anahtar	384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 14 06 5b 27 be 98 35 16 61 30 c6 af dc 25 29 31 6e e3 ca 20
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 39 68 11 2d 04 0b 80 14 bd b7 39 82 ab 04 c8 f6 d8 a9 7c
Anahtar Kullanımı	**Kritik=Evet**; Sertifika Imzalama , Çevrimdışı Sil Imzalama, Sil Imzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0

Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.4.1 [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/kurumsal/kurumsal-s2.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/kurumsal/kurumsal-s2.crt

10.3. Güvenlik Hizmetleri Sertifikası (GÜS)

Alan	Değer
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-256 ile RSA
Sertifikayı Veren	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 OU = Şube adı/ünvanı C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Sertifika sahibi adı/ünvanı SERIALNUMBER = VKN/TCKN
Ortak Anahtar	2048 bit RSA
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 39 68 11 2d 04 0b 80 14 bd b7 39 82 ab 04 c8 f6 d8 a9 7c
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Anahtar Anlaşması, Anahtar Şifreleme

Temel Kısıtlar	**Kritik=Evet**; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.4.1 [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.
Gelişmiş Anahtar Kullanımı	İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.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/kurumsal/mmeshs-s3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü(1.3.6.1.5.5.7.48.1) Diğer Ad: URL= http://cisdupmms3.kurumsal.kamusm.gov.tr

10.4. Mali Mühür Sertifikası (MÜS)

Alan	**Değer**
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-256 ile RSA
Sertifikayı Veren	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Sertifika sahibi adı/ünvanı SERIALNUMBER = VKN/TCKN
Ortak Anahtar	2048 bit RSA
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 39 68 11 2d 04 0b 80 14 bd b7 39 82 ab 04 c8 f6 d8 a9 7c

Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Dijital imza
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.4.1 [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.
Gelişmiş Anahtar Kullanımı	Kamu SM Mali Mühür (2.16.792.1.2.1.1.5.7.50.1)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.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/kurumsal/mmeshs-s3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü(1.3.6.1.5.5.7.48.1) Diğer Ad: URL= http://cisdupmms3.kurumsal.kamusm.gov.tr

10.5. Güvenli Mali Sertifika

Alan	**Değer**
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-256 ile RSA
Sertifikayı Veren	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3 C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	C=TR SERIALNUMBER = VKN CN = Sertifika sahibi adı/ünvanı
Ortak Anahtar	2048 bit RSA
Uzantılar	**Değer**

Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 06 39 68 11 2d 04 0b 80 14 bd b7 39 82 ab 04 c8 f6 d8 a9 7c
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-1 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Dijital imza
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.4.1 [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= 507 Sıra No.lu Vergi Usul Kanunu Genel Tebliği'ne göre Güvenli Mali sertifikadır.
Gelişmiş Anahtar Kullanımı	Güvenli Mali Sertifika (2.16.792.1.2.1.1.5.7.50.4)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s3.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/kurumsal/mmeshs-s3.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü(1.3.6.1.5.5.7.48.1) Diğer Ad: URL= http://cisdupmms3.kurumsal.kamusm.gov.tr