

TASNİF DIŐI



**TÜBİTAK BİLGEM
KAMU SERTİFİKASYON MERKEZİ**

KURUMSAL ŞİFRELEME SERTİFİKA UYGULAMA ESASLARI

Doküman Kodu

YON.05.02

Revizyon No

09

Revizyon Tarihi

06.03.2023

TASNİF DIŐI

| REVİZYON GEÇMİŐİ | | |
|------------------|--|-----------------|
| Revizyon No | Revizyon Nedeni | Revizyon Tarihi |
| 00 | İlk Çıkıő. | 15.01.2021 |
| 01 | Doküman formatı güncellenmiőtir. | 18.01.2021 |
| 02 | Sertifika yenileme süreci güncellenmiőtir. | 29.11.2021 |
| 03 | Elektronik mühür ve kurumsal Őifreleme sertifikaları başvuru formlarının birleőtirilmesi doęrultusunda "Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taahhütnamesi" dokümanının adı "Elektronik Mühür/Kurumsal Őifreleme Sertifikası Başvuru Formu ve Taaahhütnamesi" olarak deęiőtirilmiőtir. | 07.01.2022 |
| 04 | Sertifika üretiminin iki kiőtinin kontrolünde yapılması gerektięi ile ilgili ibare kaldırılmıőtir. | 17.02.2022 |
| 05 | Yenileme sürecinde üretimi gerçekleştirilen sertifikaların baŐlangıç tarihleri ile ilgili bilgilendirme kaldırılmıőtir. | 16.03.2022 |
| 06 | Yenileme sürecinde her iki sertifika sorumlusunun başvuru listesini imzalama koŐulu kaldırılarak yalnızca bir sorumlunun imzasıyla iŐlem yapılması saęlanmıőtir. | 31.03.2022 |
| 07 | Güvenli elektronik imza oluŐturma araçlarının güvenlik seviyelerinde düzenleme yapılmıőtir. Sertifika hizmetlerinin sonlandırılması baŐlıęında Kamu SM Hizmetleri Sonlandırma Planına referans eklenmiőtir. | 28.04.2022 |
| 08 | Sertifika İptal Listesi yayımlama gecikmesi süresi kısmında güncelleme yapılmıőtir. Doküman genelinde ek düzeltmeler uygunlanmıőtir. | 20.10.2022 |
| 09 | Sertifika sorumluları arasındaki asıl/yedek ayrımı kaldırılmıőtir. Sertifikanın askıda kalma süresi ile ilgili ifadeler düzenlenmiőtir. Dokümanda referans verilen mevzuatlar için tanım eklenmiőtir. Kullanılmayan "Kamu SM Taahhütnamesi" ve "SözleŐme" ibareleri kaldırılmıőtir. HSM'li üretimlerde istek dosyalarının parola korumalı zip içerisinde iletimi ile ilgili ifade eklenmiőtir. MERNİS tanımı eklenmiőtir. Doküman genelinde editöryal düzenlemeler yapılmıőtir. | 06.03.2023 |

İÇİNDEKİLER

| | | |
|--------|---|----|
| 1. | GİRİŐ | 10 |
| 1.1. | Genel Bakıő | 10 |
| 1.2. | Doküman Adı ve Tanımı | 11 |
| 1.3. | Sistem Bileőenleri | 11 |
| 1.3.1. | Elektronik Sertifika Hizmet Saęlayıcısı | 11 |
| 1.3.2. | Kayıt Birimleri | 11 |
| 1.3.3. | Sertifika Sahipleri | 11 |
| 1.3.4. | Üçüncü Kiőiler | 11 |
| 1.3.5. | Dięer Bileőenler | 12 |
| 1.4. | Sertifika Kullanımı | 12 |
| 1.4.1. | Uygun Olan Sertifika Kullanımı | 12 |
| 1.4.2. | Sertifika Kullanımının Sınırları | 12 |
| 1.5. | Uygulama Esaslarının Yönetimi | 12 |
| 1.5.1. | Doküman Yönetimi | 12 |
| 1.5.2. | İletiőim Bilgileri | 12 |
| 1.5.3. | Sertifika Uygulama Esaslarının İkelere Uygunluęunu Belirleyen Kiő | 13 |
| 1.5.4. | Sertifika Uygulama Esasları Onay Prosedürleri | 13 |
| 1.6. | Tanımlar ve Kısaltmalar | 13 |
| 1.6.1. | Tanımlar | 13 |
| 1.6.2. | Kısaltmalar | 15 |
| 2. | YAYIMLAMA VE BİLGİ DEPOSU YÜKÜMLÜLÜKLERİ | 16 |
| 2.1. | Bilgi Depoları | 16 |
| 2.2. | Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması | 16 |
| 2.3. | Yayım Sıklıęı ve Zamanı | 16 |
| 2.4. | Eriőim Kontrolleri | 16 |
| 3. | KİMLİK BELİRLEME VE DOęRULAMA | 17 |
| 3.1. | İsmlendirme | 17 |
| 3.1.1. | İsim Alanı Tipleri | 17 |
| 3.1.2. | Kimlik Bilgilerinin Teőhise Elveriőli Olması | 17 |
| 3.1.3. | Sertifika Sahibinin Takma İsim veya Lakap Kullanması | 17 |
| 3.1.4. | Farklı İsim Alanı Tiplerinin Yorumlanması | 17 |
| 3.1.5. | Kimlik Bilgilerinin Tekillięi | 17 |
| 3.1.6. | Markanın Tanınması, Doęrulanması ve Rolü | 17 |
| 3.2. | İlk Kimlik Belirleme | 17 |
| 3.2.1. | Özel Anahtar Sahiplięinin Kanıtlanması | 17 |
| 3.2.2. | Kurumsal Kimlięin Belirlenmesi | 18 |
| 3.2.3. | Kiőisel Kimlięin Belirlenmesi | 18 |
| 3.2.4. | Doęrulanmayan Sertifika Sahibi Bilgileri | 18 |
| 3.2.5. | Yetkinin Doęrulanması | 18 |
| 3.2.6. | Uyum Kriterleri | 18 |
| 3.3. | Sertifika Yenileme İsteęinde Kimlik Doęrulama | 18 |
| 3.3.1. | Olaęan Sertifika Yenileme İsteęinde Kimlik Doęrulama | 18 |
| 3.3.2. | İptal Sonrası Yeni Sertifika Talebinde Kimlik Doęrulama | 18 |
| 3.4. | Sertifika İptal İsteęinde Kimlik Doęrulama | 19 |

| | | |
|---------|--|----|
| 4. | SERTİFİKA YAŐAM DÖNGÜSÜ İŐLEVSEL GEREKLİLİKLERİ | 19 |
| 4.1. | Sertifika Başvurusu | 19 |
| 4.1.1. | Sertifika Başvurusunu Kimlerin Yapabildiđi | 19 |
| 4.1.2. | Kayıt İŐlemleri ve Sorumluluklar | 19 |
| 4.2. | Sertifika Başvurusunun İŐlenmesi | 20 |
| 4.2.1. | Kimlik Tanımlama ve Doğrulama İŐlevlerinin Yerine Getirilmesi | 20 |
| 4.2.2. | Sertifika Başvurusunun Kabul veya Reddi | 21 |
| 4.2.3. | Sertifika Başvurusunun İŐlenme Zamanı | 21 |
| 4.3. | Sertifikanın OluŐturulması | 21 |
| 4.3.1. | Sertifika OluŐturulmasında ESHS'nin İŐlevleri | 21 |
| 4.3.2. | Sertifika OluŐturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi | 21 |
| 4.4. | Sertifikanın Kabulü | 22 |
| 4.4.1. | Sertifikanın Kabul KoŐulu | 22 |
| 4.4.2. | Sertifikanın ESHS Tarafından Yayımlanması | 22 |
| 4.4.3. | Sertifikanın OluŐturulmasının Diđer Tarafra Duyurulması | 22 |
| 4.5. | Sertifikanın ve Özel Anahtarın Kullanımı | 22 |
| 4.5.1. | Sertifika Sahibinin Sertifika ve Özel Anahtar Kullanımı | 22 |
| 4.5.2. | Üçüncü KiŐilerin Sertifika ve Açık Anahtarın Kullanımı | 22 |
| 4.6. | Sertifika Süresinin Uzatılması | 23 |
| 4.7. | Sertifika Yenileme | 23 |
| 4.7.1. | Sertifikanın Yenileme KoŐulları | 23 |
| 4.7.2. | Sertifika Yenileme Başvurusunu Kimlerin Yapabildiđi | 23 |
| 4.7.3. | Sertifika Yenileme Başvurusunun İŐlenmesi | 23 |
| 4.7.4. | Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi | 23 |
| 4.7.5. | Sertifika Yenileme Sonrası Kabul KoŐulu | 24 |
| 4.7.6. | Sertifika Yenileme Sonrası Sertifikanın Yayımlanması | 24 |
| 4.7.7. | Sertifika Yenilemenin Diđer Tarafra Duyurulması | 24 |
| 4.8. | Sertifikada Bilgi DeđiŐikliđi | 24 |
| 4.9. | Sertifikanın İptali ve Askıya Alınması | 24 |
| 4.9.1. | Sertifikanın İptal Edildiđi Durumlar | 24 |
| 4.9.2. | Sertifika İptal Başvurusunu Kimler Yapabilir | 24 |
| 4.9.3. | Sertifika İptal Başvurusunun İŐlenmesi | 25 |
| 4.9.4. | İptal İŐteđi Ertelenme Süresi | 25 |
| 4.9.5. | İptal İŐteđinin İŐlenme Süresi | 25 |
| 4.9.6. | Üçüncü KiŐilerin Sertifika İptal Durumunu Kontrol Gerekliliđi | 25 |
| 4.9.7. | Sertifika İptal Listesi Yayımlama Sıklıđı | 26 |
| 4.9.8. | Sertifika İptal Listesi Yayımlama Gecikme Süresi | 26 |
| 4.9.9. | Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti | 26 |
| 4.9.10. | Çevrim İçi Sertifika İptal Durum Kaydı Kontrol Gereksinimi | 26 |
| 4.9.11. | Diđer Sertifika Durum Bildirim Yöntemleri | 26 |
| 4.9.12. | Özel Anahtarın Güvenliđini Yitirmesi Durumu | 26 |
| 4.9.13. | Sertifikanın Askıya Alındıđı Durumlar | 27 |
| 4.9.14. | Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiđi | 27 |
| 4.9.15. | Sertifika Askıya Alma Başvurusunun İŐlenmesi | 27 |
| 4.9.16. | Askıda Kalma Süresi | 28 |
| 4.10. | Sertifika Durum Servisleri | 28 |

| | | |
|---------|--|----|
| 4.10.1. | İřletimsel Özellikleri..... | 28 |
| 4.10.2. | Servisin Eriřilebilirliđi | 28 |
| 4.10.3. | İsteđe Bađlı Özellikler..... | 28 |
| 4.11. | Sertifika Sahipliđinin Sona Ermesi..... | 28 |
| 4.12. | Anahtar Yeniden Üretme | 28 |
| 5. | YÖNETİM, İŐLEMSEL VE FİZİKSEL KONTROLLER..... | 28 |
| 5.1. | Fiziksel Güvenlik Denetimleri | 29 |
| 5.1.1. | Tesis Yeri ve İnřaati..... | 29 |
| 5.1.2. | Fiziksel Eriřim | 29 |
| 5.1.3. | Güç Kaynađı ve Havalandırma | 29 |
| 5.1.4. | Su Baskınları..... | 30 |
| 5.1.5. | Yangın Önleme ve Korunma | 30 |
| 5.1.6. | Saklama ve Yedekleme Ortamlarının Korunması | 30 |
| 5.1.7. | Atıkların Yok Edilmesi | 30 |
| 5.1.8. | Farklı Mekanlarda Yedekleme..... | 30 |
| 5.2. | Prosedürel Kontroller..... | 30 |
| 5.2.1. | Güvenilir Roller | 30 |
| 5.2.2. | Her İřlem İin Gereken Kiři Sayısı..... | 30 |
| 5.2.3. | Kimlik Doğrulama ve Yetkilendirme..... | 31 |
| 5.2.4. | Görevlerin Ayrılmasını Gerektiren Roller | 31 |
| 5.3. | Personel Güvenlik Kontrolleri | 31 |
| 5.3.1. | Kiřisel Geçmiř, Deneyim ve Nitelik Gerekleri | 31 |
| 5.3.2. | Geçmiř Arařtırması | 31 |
| 5.3.3. | Eđitim Gerekleri | 31 |
| 5.3.4. | Sürekli Eđitim Gerekleri ve Sıklıđı | 31 |
| 5.3.5. | Görev Deđiřim Sıklıđı ve Sırası..... | 32 |
| 5.3.6. | Yetkisiz Eylemlerin Cezalandırılması | 32 |
| 5.3.7. | Anlařmalı Personel Gereksinimleri | 32 |
| 5.3.8. | Sađlanan Dokümantasyon | 32 |
| 5.4. | Denetim Kayıtları | 32 |
| 5.4.1. | Kaydedilen İřlemler | 32 |
| 5.4.2. | Kayıtların İncelenme Sıklıđı | 33 |
| 5.4.3. | Kayıtların Saklanma Süresi | 33 |
| 5.4.4. | Kayıtların Korunması | 33 |
| 5.4.5. | Kayıtların Yedeklenmesi | 34 |
| 5.4.6. | Kayıtların Toplanması | 34 |
| 5.4.7. | Kayda Sebepiyet Veren Tarafın Bilgilendirilmesi..... | 34 |
| 5.4.8. | Saldırıya Açıklıđın Deđerlendirilmesi..... | 34 |
| 5.5. | Kayıt Arřivleme | 34 |
| 5.5.1. | Arřivlenen Kayıt Bilgileri..... | 34 |
| 5.5.2. | Arřivlerin Tutulma Süresi | 34 |
| 5.5.3. | Arřivlerin Korunması | 35 |
| 5.5.4. | Arřivlerin Yedeklenmesi | 35 |
| 5.5.5. | Kayıtların Zaman Damgası Gereksinimleri..... | 35 |
| 5.5.6. | Arřivlerin Toplanması | 35 |
| 5.5.7. | Arřiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu..... | 35 |

| | | |
|---------|---|----|
| 5.6. | Anahtar DeęiŐimi..... | 35 |
| 5.7. | Güvenlięin Yitirilmesi ve Arıza Durumlarında Yapılacaklar | 35 |
| 5.7.1. | Güvenilirlięin Yitirilmesi Durumunun Düzeltilmesi | 35 |
| 5.7.2. | Donanım, Yazılım veya Veri Bozulması | 35 |
| 5.7.3. | İmza OluŐturma Verisinin Gizlilięinin Kaybedilmesi | 36 |
| 5.7.4. | Arıza Sonrası Yeniden ÇalıŐırlık | 36 |
| 5.8. | Sertifika Hizmetlerinin Sonlandırılması..... | 36 |
| 6. | TEKNİK GÜVENLİK KONTROLLERİ | 36 |
| 6.1. | Anahtar Çifti Üretimi ve Kurulumu | 37 |
| 6.1.1. | Anahtar Çifti Üretimi | 37 |
| 6.1.2. | Sertifika Sahibine Özel Anahtarın UlaŐtırılması..... | 37 |
| 6.1.3. | Elektronik Sertifika Hizmet Saęlayıcısı'na Açık Anahtarın UlaŐtırılması | 38 |
| 6.1.4. | Elektronik Sertifika Hizmet Saęlayıcısı Sertifikalarına EriŐim Saęlanması | 38 |
| 6.1.5. | Anahtar Uzunlukları..... | 38 |
| 6.1.6. | Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü..... | 38 |
| 6.1.7. | Anahtar Kullanım Amaçları | 38 |
| 6.2. | Özel Anahtarın Korunması | 38 |
| 6.2.1. | Kriptografik Modül Standartları | 38 |
| 6.2.2. | Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim | 39 |
| 6.2.3. | Özel Anahtarın Yeniden Elde Edilmesi | 39 |
| 6.2.4. | Özel Anahtarın Yedeklenmesi | 39 |
| 6.2.5. | Özel Anahtarın ArŐivlenmesi | 39 |
| 6.2.6. | Özel Anahtarın Kriptografik Modüle Yüklmesi | 39 |
| 6.2.7. | Özel Anahtarın Kriptografik Modülde Saklanması | 39 |
| 6.2.8. | Özel Anahtara EriŐim | 40 |
| 6.2.9. | Özel Anahtara EriŐimin Kesilmesi..... | 40 |
| 6.2.10. | Özel Anahtarın Yok Edilmesi | 40 |
| 6.2.11. | Kriptografik Modülün Deęerlendirilmesi | 40 |
| 6.3. | Anahtar Çifti Yönetimiyle İlgili Dięer Konular | 40 |
| 6.3.1. | Açık Anahtarın ArŐivlenmesi | 40 |
| 6.3.2. | Özel ve Açık Anahtarların Kullanım Süreleri | 41 |
| 6.4. | Aktivasyon Verileri | 41 |
| 6.4.1. | Aktivasyon Verilerinin OluŐturulması | 41 |
| 6.4.2. | Aktivasyon Verilerinin Korunması..... | 41 |
| 6.4.3. | EriŐim Denetim Verileri ile İlgili Dięer Konular | 41 |
| 6.5. | Bilgisayar Güvenlięi Kontrolleri | 41 |
| 6.5.1. | Bilgisayar Güvenlięi ile İlgili Teknik Gereker | 41 |
| 6.5.2. | Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi..... | 42 |
| 6.6. | YaŐam Döngüsü Teknik Kontrolleri..... | 42 |
| 6.6.1. | Sistem GeliŐtirme Kontrolleri | 42 |
| 6.6.2. | Güvenlik Yönetimi Kontrolleri..... | 42 |
| 6.6.3. | YaŐam Döngüsü Güvenlik Kontrolleri | 42 |
| 6.7. | Aę Güvenlięi Kontrolleri..... | 42 |
| 6.8. | Zaman Damgası..... | 43 |
| 7. | SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ BİÇİMLERİ..... | 43 |

| | | |
|--------|--|----|
| 7.1. | Sertifika Biçimi | 43 |
| 7.1.1. | Sürüm Numarası | 43 |
| 7.1.2. | Sertifika Uzantıları | 44 |
| 7.1.3. | Algoritma ve Nesne Tanımlayıcılar | 45 |
| 7.1.4. | İsim Alanı Biçimleri | 45 |
| 7.1.5. | İsim Kısıtları..... | 45 |
| 7.1.6. | Sertifika İlkeleri Nesne Tanımlama Numarası | 45 |
| 7.1.7. | İlke Kısıtları Uzantısının Kullanımı..... | 45 |
| 7.1.8. | İlke Niteleyiciler | 46 |
| 7.1.9. | Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi | 46 |
| 7.2. | Sertifika İptal Listesi Biçimi | 46 |
| 7.2.1. | Sürüm Numarası | 46 |
| 7.2.2. | Sertifika İptal Listesi Uzantıları..... | 46 |
| 7.3. | Çevrim İçi Sertifika Durum Protokolü Biçimi | 46 |
| 7.3.1. | Sürüm Numarası | 46 |
| 7.3.2. | ÇİSDUP Uzantıları..... | 47 |
| 8. | UYGUNLUK DENETİMLERİ..... | 47 |
| 8.1. | Uygunluk Denetiminin Sıklığı | 47 |
| 8.2. | Denetçinin Nitelikleri..... | 47 |
| 8.3. | Denetçinin Denetlenen Tarafı Olan İlişkisi | 48 |
| 8.4. | Denetimin Kapsamı | 48 |
| 8.5. | Yetersizliğin Tespiti Durumunda Yapılacaklar | 48 |
| 8.6. | Sonucun Bildirilmesi | 48 |
| 9. | DIŐER İŐLER VE HUKUKSAL MESELELER | 48 |
| 9.1. | Ücretlendirme | 48 |
| 9.1.1. | Sertifika OluŐturma ve Yenileme Ücreti..... | 48 |
| 9.1.2. | Sertifika EriŐim Ücreti | 49 |
| 9.1.3. | İptal Durum Kaydına EriŐim Ücreti..... | 49 |
| 9.1.4. | Diđer Servis Ücretleri | 49 |
| 9.1.5. | İade Ücreti..... | 49 |
| 9.2. | Finansal Sorumluluk | 49 |
| 9.2.1. | Sigorta Kapsamı | 49 |
| 9.2.2. | Diđer Varlıklar | 49 |
| 9.2.3. | Sertifika Mali Sorumluluk Sigortası..... | 49 |
| 9.3. | Ticari Bilginin Korunması | 49 |
| 9.3.1. | Gizli Bilginin Kapsamı..... | 49 |
| 9.3.2. | Gizlilik Kapsamında Olmayan Bilgiler..... | 50 |
| 9.3.3. | Gizli Bilginin Korunma Sorumluluđu | 50 |
| 9.4. | Kişisel Bilginin Gizliliđi..... | 50 |
| 9.4.1. | Gizlilik Planı | 50 |
| 9.4.2. | Gizli Olarak Tanımlanan Bilgiler | 50 |
| 9.4.3. | Gizli Olarak Tanımlanmayan Bilgiler | 50 |
| 9.4.4. | Gizli Bilginin Korunma Sorumluluđu | 50 |
| 9.4.5. | Gizli Bilginin Kullanımına İzin Verilmesi | 50 |
| 9.4.6. | Yetkili Mercilerin Kararına Uygun Olarak Bilginin Açıklanması | 50 |

| | | |
|---------|---|----|
| 9.4.7. | Diđer BaŐlıklar | 51 |
| 9.5. | Telif Hakları..... | 51 |
| 9.6. | Temsil Hakkı ve Yüklölölükler | 51 |
| 9.6.1. | Elektronik Sertifika Hizmet Sađlayıcısı Yüklölölükleri | 51 |
| 9.6.2. | Kayıt Birimi Yüklölölükleri | 52 |
| 9.6.3. | Sertifika Sahibinin Yüklölölükleri | 52 |
| 9.6.4. | Üçüncü KiŐilerin Yüklölölükleri | 53 |
| 9.6.5. | Diđer BileŐenlerin Yüklölölükleri..... | 54 |
| 9.7. | Yüklölölüklerden Feragat..... | 54 |
| 9.8. | Sorumlulukla İlgili Sınırlamalar..... | 54 |
| 9.9. | Tazminat Halleri | 54 |
| 9.10. | AnlaŐma Süresi ve AnlaŐmanın Sona Ermesi | 54 |
| 9.10.1. | AnlaŐma Süresi..... | 55 |
| 9.10.2. | AnlaŐmanın Sona Ermesi | 55 |
| 9.10.3. | AnlaŐmanın Sona Ermesinin Etkileri | 55 |
| 9.11. | Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme | 55 |
| 9.12. | DeđiŐiklik Halleri | 55 |
| 9.12.1. | DeđiŐiklik Metotları | 55 |
| 9.12.2. | Bilgilendirme Mekanizması ve Sıklıđı..... | 56 |
| 9.12.3. | Nesne Tanımlama Numarasının DeđiŐmesini Gerektiren Durumlar | 56 |
| 9.13. | AnlaŐmazlık Halleri | 56 |
| 9.14. | Uygulanacak Hukuk | 56 |
| 9.15. | Uygulanabilir Yasalarla Uyum..... | 56 |
| 9.16. | Diđer Hükümler | 56 |
| 10. | EK-A SERTİFİKA PROFİLLERİ..... | 57 |
| 10.1. | KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI | 57 |
| 10.2. | KAMU SM KURUMSAL ŐİFRELEME ALT KÖK SERTİFİKASI | 58 |
| 10.3. | SON KULLANICI KURUMSAL ŐİFRELEME SERTİFİKA ŐABLONU | 59 |

TABLolar

| | |
|--|----|
| Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları..... | 44 |
| Tablo 2 Kurumsal Őifreleme Sertifika İsim Alanı Bilgileri..... | 45 |

1. Giriő

Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) tarafından oluőturulan Kamu Sertifikasyon Merkezi (Kamu SM), 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, Bilgi Teknolojileri ve İletifim Kurumu'nun (BTK) yayımladıėı Elektronik İmza Kanunu'nun Uygulanmasına İliőkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliőkin Tebliė'de tanımlandıėı Őekliyle Elektronik Sertifika Hizmet Saėlayıcısı (ESHS) iőlevlerini yerine getirir.

2017/21 sayılı Baőbakanlık Genelgesi ile Kurumsal Őifreleme Sertifikalarının üretilmesi için TÜBİTAK bünyesindeki Kamu Sertifikasyon Merkezi (Kamu SM) yetkilendirilmiőtir. Kamu SM; 2019/DK-BTD/160 Sayılı Bilgi Teknolojileri ve İletifim Kurulu Kararı ile yayımlanan Kamu Kurum ve Kuruluőları Arasında Elektronik Ortamdaki Belge Paylaőımında Kullanılan Kurumsal Őifreleme ve Elektronik Mühür Sertifikalarına İliőkin Usul ve Esaslar'da belirtilen tanıma uygun olarak Kurumsal Őifreleme Sertifikası hizmeti saėlamaktadır.

Bu doküman, Türkiye Bilimsel ve Teknolojik Arařtırma Kurumu'na (TÜBİTAK) baėlı Biliőim ve Bilgi Güvenliėi İleri Teknolojiler Arařtırma Merkezi (BİLGEM) tarafından oluőturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Türkiye Cumhuriyeti Devleti'ne baėlı kamu kurum ve kuruluőlara Kurumsal Őifreleme Sertifikası saėlayıcılıėı konusundaki faaliyetlerini nasıl yürüttüėünü anlatmak amacıyla yazmıő olduėu Sertifika Uygulama Esasları (SUE) dokümanıdır.

Kamu SM, Sertifika İlkeleri (Sİ) dokümanında belirtilen ilkelere uygun olarak hazırlanan bu SUE dokümanında tanımlanan esaslar uyarınca çalıőır. SUE dokümanı, Kurumsal Őifreleme Sertifikalarının yönetimi ve kayıt iőlemleri sırasında yapılan iőlerin hangi ortamlarda ve nasıl yürütüldüėünü Sİ dokümanına baėlı olarak detaylandırarak anlatır. Bu SUE dokümanı, sertifika baővurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve sertifika iptal iőlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili esasları ortaya koyar; Kamu SM'nin, sertifika sahibinin ve üçüncü kiőilerin uygulama sorumluluklarını belirler.

Kamu SM'den Kurumsal Őifreleme Sertifikası talebinde bulunan tüzel kiőiler bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiőtir sayılır. Kurumsal Őifreleme Sertifikası talebinde bulunan kurumlar bununla ilgili olarak taahhütnamelerde SUE dokümanına atıfta bulunurlar. Kurumsal Őifreleme Sertifikası sahibi kurumlar baővuru formu ve taahhütnamesini imzalayarak SUE dokümanında belirtilen esasları kabul ederler.

1.1. Genel Bakıő

SUE dokümanı, Kamu SM içinde yer alan sistem bileőenlerinin rollerini, sorumluluklarını ve iliőkilerini tanımlar; sertifika yönetim ve kayıt iőlemlerinin gerçekteőirilmesi Őeklini anlatır. Sertifika yönetimi, sertifika sahipleri için anahtar çifti ve sertifika üretmek, sertifikaları yayımlamak, yenilemek, askıya almak, askıdan indirmek, iptal etmek, sertifika iptal bilgisini yayımlamak, sertifika iőlemleri ile ilgili kiőileri baővuru ve sertifikanın durumu hakkında bilgilendirmek, gerekli kayıtları tutmak ve kayıt iőlemlerini gerçekteőirmek gibi iőlerden oluőur. Kayıt iőlemleri sertifika verilecek kurumların baővurularını, kurum bilgileri ve ilgili resmi belgeleri toplama, kurum kimliėi doėrulama, onaylama, iptal, yenileme isteklerini alma, deėerlendirme, onaylanan sertifika baővuru ve iptal istekleri doėrultusunda gerekli iőlemleri baőlatmayı içerir.

SUE dokümanı, "İnternet Açıık 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: Kurumsal Őifreleme Sertifika Uygulama Esasları

Doküman Sürüm Numarası: 09

Yayın Tarihi: 06.03.2023

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.1.11

Bu doküman, Kamu SM'nin Kurumsal Őifreleme Sertifikası hizmeti verirken uyguladığı esasları tanımlayan SUE dokümanıdır ve kamu kurum ve kuruluşlarına verilen Kurumsal Őifreleme 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.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Temel görevi sertifika ve iptal durum kayıtlarını üretip kendisine ait imza oluşturma verisiyle imzalamak olan ESHS'ler, sertifika başvurusunda bulunan kurumların kayıt ve kimlik doğrulama işlemlerini yapmak, sertifikaların üretim, dağıtım, yenileme, askı, iptal, iptal olmuş sertifika bilgilerini tüm taraflara duyurma süreçlerini mevzuatta belirtilen şartlara uygun olarak yerine getirmekle yükümlüdür.

Kamu SM, Kurumsal Őifreleme Sertifika Hizmet Sağlayıcısı (Kurumsal Őifreleme SHS) olarak kamu kurum ve kuruluşlarına Kurumsal Őifreleme Sertifikası hizmeti sağlamaktadır.

1.3.2. Kayıt Birimleri

Tüm kayıt işlemleri doğrudan Kamu SM personeli tarafından yürütülmektedir. Kayıt birimleri, Kamu SM'nin sertifika ve iptal başvurusu gibi doğrudan son kullanıcılara yönelik hizmetlerini yürüten birimdir. Bu birim, ilk müşteri kayıtlarını oluşturur, gerekli kurum kimlik tanımlama ve doğrulama süreçlerini yürütür, ilgili sertifika taleplerini sertifika üretim birimine yönlendirir.

1.3.3. Sertifika Sahipleri

Kamu SM'den kurumsal Őifreleme sertifikası talep eden, DETSİS'te bilgileri bulunan, üretilen sertifikanın üzerinde kurum adları yer alan ve sertifikalarını Kamu SM sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan tüzel kişilerdir.

Sertifika sahibi kurum, taahhütnamelere uygun olarak sertifika başvuru, üretim ve dağıtım süreçlerinde bu dokümanda belirtilen işlemleri yapmaktan sorumludur.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kurum bilgileri ve açık anahtar arasındaki bağı doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan kişilerdir/kurumlardır.

Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diđer Bileőenler

1.3.5.1. Kurumsal Őifreleme Sertifikası Sorumlusu

Sertifika bařvurusunda bulunan kurum tarafından yetkilendirilen ve sertifika ynetim srelerinde Kamu SM ile iletiŐim iinde olan kiŐi/kiŐilerdir.

Kurumsal Őifreleme sertifikaları iin sertifika sahibi kurum tarafından onaylanan taahhtname ile Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları belirlenmektedir.

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları Kamu SM tarafından kendisine imzalatılan taahhtnamedeki Őartları yerine getirmekten sorumludur. Sertifika sorumluları, Kurumsal Őifreleme Sertifikasını kullanmaya yetkili olmak zorunda deđildir. Kurumsal Őifreleme Sertifikasını kullanmaya yetkili kiŐi/kiŐilerin belirlenmesi kurum inisiyatifindedir.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

2017/21 sayılı Bařbakanlık Genelgesi ile elektronik ortamda iletilen resmi yazıların Őifreli Őekilde gnderilebilmesine imkan sađlanmıŐtır. Kurumsal Őifreleme Sertifikası, kamu kurum ve kuruluŐları arasında elektronik ortamdaki belge paylaŐımında Őifreleme yapmak amacıyla e-YazıŐma Teknik Rehberi'ne uygun olarak kullanılmalıdır.

Kamu kurum ve kuruluŐları adına retilen Kurumsal Őifreleme Sertifikalarında bulunan aık anahtar, gnderici kurumların Őifreli paket oluŐturabilmesi; sertifika sahibi kurumun himayesinde bulunan zel anahtar ise kendisine gnderilen Őifreli paketlerin aılabilmesi amacıyla kullanılır. Kurumsal Őifreleme Sertifikaları elektronik imzalama iin kullanılmaz.

1.4.2. Sertifika Kullanımının Sınırları

Kurumsal Őifreleme Sertifikası Blm 1.4.1'de belirtilen amalar dıŐında kullanılamaz. Belirtilen kapsam dıŐında kullanımdan dođan zararlardan Kamu SM sorumlu tutulamaz.

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

1.5. Uygulama Esaslarının Ynetimi

1.5.1. Dokman Ynetimi

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

1.5.2. İletiŐim Bilgileri

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

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

Tel. : (262) 648 18 18

Faks : (262) 648 18 00

E Posta : bilgi@kamusm.gov.tr

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

Kamu SM, SUE 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 Kiři

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 paylaşılabilirdiđi, özel anahtarı ile oluşturduđu dijital imzaların doğrulanmasında ve/veya kendisine şifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileşenidir.

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

Akıllı Kart: Sertifika ve sertifika ile ilişkili özel anahtarın içinde bulunduđu güvenli donanımdır.

Anahtar Çifti: Özel anahtar ve onunla ilişkili olan açık anahtarı ifade eden tanımdır.

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

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

DETSİS (Devlet Teřkilatı Merkezi Kayıt Sistemi): Türkiye Cumhuriyeti Devlet yapısındaki tüm kurum ve kuruluşların ve alt birimlerin tekil ve deđişmez nitelikte numaralar ile elektronik ortamda kodlanarak tanımlandığı sistemidir.

EYP (e-Yazışma Projesi): Kamu kurum ve kuruluşları arasındaki resmi yazışmaların elektronik ortamda yürütülmesini amaçlayan projesidir.

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

HSM Cihaz Sorumlusu: HSM sahibi kurum tarafından yetkilendirilen, Kamu SM ile kurum arasında HSM cihazına anahtar çifti ve sertifika yükleme ile ilgili süreci yürütecek kişidir.

İlgili mevzuat: “5070 Sayılı Elektronik İmza Kanunu”, “2017/21 Sayılı Başbakanlık Genelgesi”, Bilgi Teknolojileri ve İletişim Kurulu Kararı ile yayımlanan “Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İliřkin Usul ve Esaslar” ve “Elektronik Mühre İliřkin Usul ve Esaslar Hakkında Yönetmeliđi” ifade eder.

İmza Doğrulama Verisi: Elektronik imzanın doğrulanmasında ve/veya kendisine Őifreli mesaj iletilmesinde kullanılan anahtar çiftinin gizli olmayan bileŐeni, kriptografik açık anahtarlar gibi verilerdir.

İmza OluŐturma Verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluŐturma ve/veya kendisine iletilen Őifreli mesajların Őifresini çözmek için kullanılan ve bir eŐi daha olmayan Őifreler, kriptografik özel anahtarlar gibi verilerdir.

İptal Durum Kaydı: Kullanım süresi dolmamıŐ sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkan veren ve üçüncü kiŐilerin hızlı ve güvenli bir biçimde ulaŐabileceği kayıtlardır.

Kamu SM (Kamu Sertifikasyon Merkezi): Türkiye Bilimsel ve Teknolojik AraŐtırma Kurumu'na (TÜBİTAK) baėlı BiliŐim ve Bilgi Güvenliėi İleri Teknolojiler AraŐtırma Merkezi (BİLGEM) bünyesinde, elektronik sertifika hizmeti saėlamak üzere oluŐturulan birimdir.

KAYSİS (Elektronik Kamu Bilgi Yönetim Sistemi): Kamu kurum ve kuruluşlarının teŐkilat yapısının tanımlanmasından, sunulan hizmetlere; hizmetlerde kullanılan belgelerden, kurumların iletiŐim ve yönetici bilgilerine kadar kamu yönetiminde yer alan unsurların mevzuat dayanaklarıyla birlikte tespit edilerek elektronik ortamda tanımlandığı, geliŐtirilen Dijital Türkiye (e-Devlet) uygulamalarının birbirine tek merkezden entegre edilmesini saėlayacak bilgi yönetim sistemidir.

KEP (Kayıtlı Elektronik Posta): E-postanın gönderim ve alımına dair kanıtların oluŐturulup saklandığı e-posta iletim hizmetidir.

Kök Sertifika Hizmet Saėlayıcısı: Kamu Sertifikasyon Merkezi içinde oluŐturulmuŐ, en yetkili imza derecesi verilmiŐ ve sertifikasını kendisi imzalamıŐ olan Sertifika Hizmet Saėlayıcısıdır.

Kurum: TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi'nden Kurumsal Őifreleme Sertifikası talep eden, DETSİS'te bilgileri bulunan ve Kurumsal Őifreleme Sertifikası almaya yetkisi olan tüzel kiŐiliktir.

Kurum Doküman Doğrulama Sistemi: Elektronik ortamda hazırlanan belgelerin doğrulanması iŐleminde kullanılacak kuruma ait sistem veya e-Devlet belge doğrulama sistemidir.

Kurumsal Őifreleme SHS (Kurumsal Őifreleme Sertifika Hizmet Saėlayıcısı): Kamu Sertifikasyon Merkezi içinde oluŐturulmuŐ, Kök Sertifika Hizmet Saėlayıcısı'nın imzasını taşıyan sertifikaya sahip olan ve son kullanıcıların sertifikalarını oluŐturup imzalamakla yetkili kılınmıŐ Elektronik Sertifika Hizmet Saėlayıcısıdır.

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları: Kamu kurumlarının başvuru formu ve taahhütname ile Kamu SM'ye bildirdiėi ve Kurumsal Őifreleme Sertifikası ile ilgili süreçlerde kurumu temsile yetkili kiŐi/kiŐilerdir.

Kurumsal Őifreleme Sertifikası: Elektronik ortamdaki belge paylaşımında Őifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifikadır.

MERNİS (Merkezi Nüfus İdare Sistemi): Kaėıt ortamında bulunan nüfus kayıtlarının elektronik ortama aktarılarak merkezi bir yapıda tutulmasını saėlayan projedir.

Nesne Tanımlama Numarası: Herhangi bir nesneyi eŐsiz olarak tanımlayan, uluslararası standart belirleyen bir kuruluŐtan alınan numaradır.

Özel Anahtar: Anahtar Çiftinin sahibi tarafından gizli tutulan ve dijital imza oluŐturmak ve/veya ilgili Açık Anahtarla ŐifrelenmiŐ elektronik kayıtların, dosyaların Őifresini çözmek için kullanılan anahtardır.

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

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

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 belgelerdir.

Tebliğ: 6/1/2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'dir.

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

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

1.6.2. Kısaltmalar

BGYS: Bilgi Güvenliği Yönetim Sistemi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

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

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

MERNİS: Merkezi Nüfus İdare Sistemi

PKI (Public Key Infrastructure): Açık Anahtar Altyapısı

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayınlama ve Bilgi Deposu Yüklümlükleri

Bilgi deposu, Kamu SM'nin kendisine ait sertifikaları, iptal durum kayıtlarını, Sİ ve SUE gibi ilgili dokümanları sertifika sahibi kurumların ve üçüncü kişilerin ulaşabileceđi 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, 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 Yayınlanması

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

- Kamu SM'ye ait güncel Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait geçmişte oluşturulmuş Kök SHS ve Kurumsal Şifreleme SHS sertifikaları
- Kamu SM'ye ait sertifikaların özet değerleri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi
- Kamu SM Sİ ve SUE dokümanları
- Taahhütnameler
- Yönergeler
- Formlar
- Sertifika iptal durum kayıtları

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, yönergeler, formlar, Sİ ve SUE dokümanları içeriğinin değışmesi 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 yapılmaktadır. Kamu SM, bilgi deposu ile ilgili olarak aşağıdaki yükümlülükleri yerine getirir:

- Bilgi deposunda tutulan bilgilerin izinsiz silinmeye ve değıştirilmeye karşı bütünlüğünü korumak
- Bilgi deposunda tutulan bilgilerin doğruluđu ve güncelliğini sağlamak
- Bilgi deposunu sürekli olarak katılımcıların erişimine açık tutmak
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak

- Bilgi deposuna eriŐimi ücretsiz sađlamak

3. Kimlik Belirleme ve Dođrulama

Kurumsal Őifreleme Sertifikası ile ilgili iŐlemler yapılmadan önce, iŐlemi talep etmeye yetkisi olan kurumun kimlik tanımlama ve dođrulaması yapılır. Bu bölümde Kurumsal Őifreleme Sertifikası yönetim prosedürleri içinde uygulanan kurum kimlik tanımlama ve dođrulama yöntemleri ile Kurumsal Őifreleme Sertifikası içinde yazılan kurum bilgileri anlatılmıştır.

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

Kurumsal Őifreleme Sertifikalarında Kamu SM ve sertifika sahibi kurumlara ait bilgilerin belirtildiđi DN [Distinguished Name (Ayırt edici isim)] alanı içinde "ITU X.500" biçiminin desteklediđi isim tipleri kullanılır.

3.1.2. Kimlik Bilgilerinin TeŐhise ElveriŐli Olması

Kurumsal Őifreleme Sertifikaları içeriđindeki isim alanına yazılan bilgiler kurumu tanımlayan ve kurumun kimliđinin tespit edilmesini sađlayan niteliktedir.

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Kurumsal Őifreleme Sertifikası içeriđinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Kurumsal Őifreleme Sertifikası içinde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliđi

Kurumsal Őifreleme Sertifikası içeriđindeki kurum bilgileri, DETSİS'te yer alan bilgilerdir ve her kurum için ayırt edici niteliktedir. Aynı kuruma ait Kurumsal Őifreleme Sertifikaları içeriđindeki kurum bilgilerinin aynı olmasına izin verilmektedir. Ancak farklı kurumlara ait Kurumsal Őifreleme Sertifikaları içeriđindeki kurum bilgilerinin aynı olması engellenmektedir. Bunun sađlanabilmesi için Kurumsal Őifreleme Sertifikalarının isim alanı içinde benzersiz bir sayı olduđu kabul edilen sertifika sahibi kuruma ait DETSİS numarası da yer alır.

3.1.6. Markanın Tanınması, Dođrulaması ve Rolü

Düzenlenmesine gerek duyulmamıştır.

3.2. İlk Kimlik Belirleme

Kamu SM Kurumsal Őifreleme Sertifikası hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili kurumun dođrulabilmesi için aŐađıda tanımlanan yöntemler uygulanır.

3.2.1. Özel Anahtar Sahipliđinin Kanıtlanması

Sertifika sahibine ait açık ve özel anahtar, kurumun talebi üzerine Kamu SM tarafından üretilerek Güvenli Donanım Modülü (HSM)'ne veya akıllı karta yüklenir.

Kurumsal Őifreleme Sertifikası, başvuru sırasında belirlenen sorumlusu/sorumlularına imza karŐılıđında teslim edilir. Akıllı kart içerisinde teslim edilen kurumsal Őifreleme sertifikasının teslim teyidi Online

İŐlemler üzerinden alınır. HSM'ye yüklenmesi talep edilen sertifikaların teslim teyidi için HSM Cihaz Sorumlusuna kurulum tutanađı imzalatılır.

3.2.2. Kurumsal Kimliđin Belirlenmesi

Kurumsal Őifreleme Sertifikası baŐvurusunda bulunan kurumlar, talep edilen kurum bilgilerini, Kamu SM tarafından sunulan baŐvuru yöntemleriyle Kamu SM'ye bildirir. Kamu SM, kurum tarafından iletilen bilgilere istinaden kurum kimliđini dođrular. Kurumların sertifika alma yetkisi DETSİS aracılıđıyla kontrol edilir. BaŐvuru esnasında sertifika işlemlerini kurum adına yürütecek Kurumsal Őifreleme Sertifikası Sorumluları da belirlenerek Kamu SM'ye iletilir.

3.2.3. KiŐisel Kimliđin Belirlenmesi

Kurumsal Őifreleme Sertifikaları, yalnızca Bölüm 1.3.3'te belirtilen kurumlar adına üretildiđinden bireysel baŐvurular kabul edilmemektedir. BaŐvuru formu ve taahhütnemelerde yer alan kiŐisel bilgiler MERNİS üzerinden kontrol edilmektedir. Kontrol edilemeyen bilgilerin dođruluđu kurumun sorumluluđundadır.

3.2.4. Dođrulanmayan Sertifika Sahibi Bilgileri

Sertifika sahibi kurum ve sertifika sorumlusu/sorumluları tarafından baŐvuru sırasında ve daha sonra deđiŐiklik sebebiyle beyan edilen aŐađıdaki eriŐim bilgileri ve diđer bilgilerin dođruluđu Kamu SM tarafından kontrol edilmez:

- Telefon numaraları
- Kurumsal Őifreleme Sertifikası tesliminde kullanılacak adres bilgisi
- Elektronik posta adresleri
- Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının unvanı veya görevi ile ilgili bilgiler
- Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının çalıŐtıđı birim ile ilgili bilgiler

Bu bilgilerin dođruluđu kurumun beyanı üzerine kabul edilir.

Kurum bu bilgileri Kamu SM'ye dođru beyan etmekle yükümlüdür. Bu bilgilerin Kamu SM'ye yanlış verilmesinden dolayı dođabilecek zararlardan, sertifikanın hatalı üretilmesinden ve sertifika yönetim sürecinde meydana gelebilecek gecikme veya aksaklıklardan Kamu SM sorumlu tutulamaz.

3.2.5. Yetkinin Dođrulanması

Sertifika içeriđine sertifika sahibi kurumun yetkisi ile ilgili bilgiler yazılmamaktadır.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıŐtır.

3.3. Sertifika Yenileme İsteđinde Kimlik Dođrulama

Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.3.1. Olađan Sertifika Yenileme İsteđinde Kimlik Dođrulama

Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Dođrulama

Bölüm 3.2'de anlatıldıđı Őekilde uygulanır.

3.4. Sertifika İptal İsteęinde Kimlik Doğrulama

Sertifika sahibi kurumun yetkilendirdięi sertifika sorumlusu/sorumluları Kamu SM resmi web sitesinde yer alan Online İşlemlere kimlik doğrulamasıyla giriş yaparak iptal işlemini gerçekleştirebilir. Online İşlemler adresine ulaşılamaması durumunda Kamu SM web sitesinde belirtilen yöntemlerle iptal işlemi gerçekleştirilebilir. Web sitesinde yer alan yöntemlerle yapılan iptal başvurularında başvuru sahibinden gelen evraklar doğrulanır ve sertifika sorumlusu bilgileri kontrol edilir. Ayrıca Kurumsal Şifreleme Sertifika Sorumlusu/Sorumluları telefon ile aranarak kimlik doğrulama gerçekleştirilir ve iptal talebi teyit edilir.

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 sorumlusu/sorumluları ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildięi

DETSİS'te bilgileri bulunan ve DETSİS tarafından Kurumsal Şifreleme Sertifikası alma yetkisi olduęu belirtilen kamu kurum ve kuruluşları Kurumsal Şifreleme Sertifikası başvurusunda bulunabilirler.

Başvuru süreci, kamu kurumunun resmi yazısı ekinde Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesi ile HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhünamesini Kamu SM'ye göndermesiyle başlar. Belgelerin iletim yöntemi Kamu SM resmi internet sitesinden yayımlanır. Kurumun sertifika başvuru işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumlusu/sorumluları tarafından yürütülür.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

Kurumsal Şifreleme Sertifikası başvurusu, kamu kurum veya kuruluşu tarafından Kamu SM'ye yapılır. Kurumun Kamu SM'den alacağı sertifika hizmetlerinin şartları sertifika sahibi kurumun imzaladıęı başvuru formu ve taahhünamesi, Kamu SM'nin internet üzerinden yayımladıęı ilgili yönergeler, Sİ ve SUE dokümanları doğrultusunda belirlenir.

Kurum, Kamu SM web sitesinde yayımlanan Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesini doldurur. Ardından üst yazısıyla birlikte Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesi eki de imzaya dahil olacak şekilde EYP dosyası oluşturularak e-posta veya KEP üzerinden Kamu SM'ye iletir. Kurum, Kurumsal Şifreleme Sertifikasını HSM içerisinde kullanmayı tercih ederse HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhünamesi dosyasını da EYP formatı imzalı eklerine dahil etmelidir. EYP dosyası, başvuru formunda yetkili olarak belirtilen sertifika sorumlularından birine ait kurumsal e-posta veya KEP adresi üzerinden

iletilmelidir. Bunun mümkün olmadığı durumlarda başvuru evrakları Kamu SM ile görüşülerek alınan onaya istinaden harici depolama aygıtı ile gönderilebilir.

Cumhurbaşkanlığı tarafından 10.06.2020 tarihli ve 2646 sayılı Resmî Gazetede yayımlanan “Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik” in, 4. Maddesi gereğince; kamu kurum ve kuruluşlarınca resmi yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli elektronik imza ile imzalanan belgelerle yapılır. Bu kapsamda, zorunlu haller veya olağanüstü durumlar dışında EYP dosyası ile başvuru dışında başvurular kabul edilmeyecektir. Zorunlu hallerde veya olağanüstü durumlarda resmi yazışmalar, KEP veya kurumsal e-posta yoluyla iletilen ilgili başvuru formu ve taahhünamelerin doğrulanmasının ardından ıslak imzalı ve mühürlü olacak şekilde üst yazısıyla birlikte Kamu SM'ye posta yoluyla iletilir. Kurumsal Şifreleme Sertifikası başvurusunun nasıl yapılacağı ile ilgili ayrıntılar Kamu SM'nin internet sitesinde yayımlanmaktadır.

Kurum başvuru sırasında Kamu SM'ye doğru bilgi beyan etmekle sorumludur. Kurum, 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, Kurumsal Şifreleme Sertifikası içinde yer alacak bilgilerin doğruluğunu kontrol eder ve kendisine beyan edilen bilgilerin gizliliğini sağlamak için gerekli tedbirleri alır.

Kamu SM, sertifika verilecek kurumların kimlik tanımlama ve doğrulama işlemlerini yaptıktan sonra başvurularını değerlendirir ve uygun görülen başvuruları onaylayarak işleme alır.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında kurumdan gelen belgelerin Kamu SM tarafından incelenmesi sonucunda kurum kimlik tanımlama ve doğrulama işlevleri yerine getirilir. Kurumsal Şifreleme Sertifikası başvurusunda bulunan kurumların Kamu SM'ye gönderdiği bilgi ve belgeler aşağıda sıralanmıştır:

- Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesi
- Kurum tarafından yazılan resmi yazı
- HSM kullanılacaksa HSM Cihazına Anahtar ve Sertifika Yükleme Bilgi Formu ve Taahhünamesi

Kurumdan gönderilen belgelerin doğrulanması için aşağıdaki kontroller yapılır:

- Kurum tarafından gönderilen EYP dosyası kontrol edilerek üst yazı ve eklerinin e-imza doğrulanması yapılır.
- EYP dosyası içerisinde üst yazıda yer alan belge doğrulama kodu ile Kurum Doküman Doğrulama Sistemi üzerinden kurum doğrulanması gerçekleştirilir.
- Başvuru evraklarında yer alan kurum DETSİS numarası, DETSİS üzerinden sağlanan servis aracılığıyla kontrol edilerek kurumun Kurumsal Şifreleme Sertifikası almaya yetkili olup olmadığı sorgulanır.
- Kurum tarafından gönderilen Elektronik Mühür/Kurumsal Şifreleme Sertifikası Başvuru Formu ve Taahhünamesinde yer alan kurumun adı, vergi kimlik numarası, yetkilendirilen Kurumsal Şifreleme Sertifikası Sorumlusu/Sorumlularının T.C. kimlik numarası, ad, soyad, kurumsal e-posta adresi, kurum birimi ve sertifika üretim nedeni bilgilerinde eksiklik olup olmadığı kontrol edilir.

- Belgelerin elektronik ortamdan iletimi mümkün olmadığı durumda kurumdan evrak asılları talep edilir. Evrak asılları ulaşan kurumların başvurularını doğrulamak için, KEP ile gönderilen evraklar ile evrakların asılları karşılaştırılarak birbirinin aynı olduğu doğrulanır. KEP kullanmayan kurum başvurularını doğrulayabilmek için kuruma iki seçenek sunulur; resmi olarak sahibi oldukları web sitelerinin belirlenen dosya yoluna elektronik ortamda ilettikleri başvuru evraklarının özet değeri eklenmeli veya başvuru formunda kurum onayını veren üst düzey yetkili ses kaydı alabilen telefon ile aranarak doğrulama onayı alınmalıdır.

Bilgi ve belgeler hatasız ve tam ise kurum kimlik tanımlama ve doğrulama işlemi tamamlanır. Belgelerde gözle görülen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda kurum kimlik tanımlaması ve doğrulaması yapılamaz. Başvuru evraklarının, tanımlanan yöntemler dışında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

4.2.2. Sertifika Başvurusunun Kabul veya Reddi

“Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar”ın ikinci bölüm, 5’inci maddesinin ikinci fıkrasının (a) bendine dayanarak, Kamu SM, DETSİS’te bilgileri bulunmayan veya Kurumsal Şifreleme Sertifikası almaya yetkisi olmayan tarafların başvurusunu reddeder.

Buna ek olarak, Bölüm 4.2.1’deki kontrollerin yapılması sonucunda, başvuru sırasında beyan edilen belgelerde tahrifat, hata, eksik onay, eksik veya yanlış bilgi olması durumlarında başvuru geri çevrilir. Başvurusu kabul edilmeyen kurumlarla ilgili yazılı bilgilendirme, Kurumsal Şifreleme Sertifikası Sorumlusu/Sorumlularının başvuru sırasında beyan ettikleri e-posta adresleri aracılığı ile yapılır ve gerekli görülen bilgi ve belgeler tekrar talep edilir. Gereken düzeltmeler yapıp eksiklikler tamamladıktan sonra başvuru tekrarlanabilir.

Başvurusu kabul edilen kurumlar, Kamu SM sisteminde tanımlanır ve sertifika üretim süreci başlatılır.

4.2.3. Sertifika Başvurusunun İşlenme Zamanı

Başvuru evraklarının eksiksiz bir şekilde Kamu SM’ye ulaşması ve doğrulanmasının ardından en fazla 15 (on beş) iş günü içerisinde 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, işlem kapasitesini göz önünde bulundurarak başvuru sırasında sertifikanın yükleneceği donanım olarak akıllı kart ya da HSM tercih eder.

Kurumsal Şifreleme Sertifikası, kayıp veya arıza gibi durumlarda kurumun işlemlerinde aksaklık yaşanmaması amacıyla biri yedek olmak üzere 2 adet üretilir.

Kamu SM tarafından üretilen kurumsal şifreleme sertifikaları; BTK tarafından yayımlanan 2019/DK-BTD/160 sayılı Kurul Kararı Madde 5’de belirtilen hüküm ve niteliklere uygun olarak üretilir.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Akıllı karta yüklenen sertifika, sertifika sorumlusuna teslim edildiğinde Kurumsal Şifreleme Sertifikasının oluşturulduğu konusunda bilgilendirilmiş olur.

HSM cihazına sertifika ykleme iŐlemi, HSM Cihaz Sorumlusu gzetiminde gerekleŐtirilir. İŐlem sonrasında kurulum tutanađı imzalanır ve Kurumsal Őifreleme Sertifikasının oluŐturulduđu konusunda HSM sorumlusu bilgilendirilmiŐ olur.

4.4. Sertifikanın Kabul

4.4.1. Sertifikanın Kabul KoŐulu

Akıllı karta yklenen Kurumsal Őifreleme Sertifikası anlaşmalı kurye ile kurum adresine gnderilir. Kurumsal Őifreleme Sertifikası, baŐvuru formunda belirtilen sertifika sorumlusu/sorumlularına teslim edilir. Sertifika sorumlusu kendisine teslim edilen zarf ierisinde sertifika bulunmuyorsa zarfı teslim almadan iade eder.

Kurumsal Őifreleme Sertifikasının HSM'ye yklenmesi talebi durumunda kuruma yerinde ve uzaktan olmak zere iki farklı ykleme seeneđi sunulmaktadır. Yerinde ykleme, kurum tarafından belirtilen zorunlu hallerde Kamu SM personelinin kurum yerleŐkesine gidip HSM cihazına anahtar retimi ve sertifika ykleme iŐlemlerini yerinde gerekleŐtirdiđi sretir. Uzaktan ykleme, Kamu SM ve kurum arasında yapılan gvenli uzak bađlantı sonrası Kamu SM personelinin HSM cihazına anahtar retimi ve sertifika ykleme iŐlemlerini uzaktan gerekleŐtirdiđi sretir. Her iki sre de ilk baŐvuruda HSM Cihazına Anahtar ve Sertifika Ykleme Bilgi Formu ve Taahhtnamesinde belirtilen HSM Cihaz Sorumlusu gzetiminde gerekleŐtirilmektedir.

Sertifika sorumlusu/sorumluları, sertifikanın ieriđini kontrol eder, herhangi bir eksiklik veya hata olması durumunda 5 (beŐ) iŐ gn ierisinde Kamu SM'yi bilgilendirir, aksi halde sertifikayı kabul etmiŐ sayılır.

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM tarafından retilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e yklenmektedir.

4.4.3. Sertifikanın OluŐturulmasının Diđer Tarafalara Duyurulması

Kamu SM tarafından retilen ve kurum tarafından teslim alındıktan sonra askıdan indirilen Kurumsal Őifreleme Sertifikası, DETSİS'e yklenmektedir.

4.5. Sertifikanın ve zel Anahtarın Kullanımı

4.5.1. Sertifika Sahibinin Sertifika ve zel Anahtar Kullanımı

Sertifika sahibi, sertifikasını ve sertifikaya ait zel anahtarını; tabi olunan standartlar, ilgili mevzuat, Sİ/SUE dokmanı ve ilgili baŐvuru formu ve taahhtnamesinde yer alan koŐullar ve belirlenmiŐ sınırlar iinde kullanmalıdır.

Sertifika sahibi, zel anahtarı yetkisiz kiŐilerin eriŐimine karŐı korumakla ykmldr. Kurumsal Őifreleme Sertifikasına karŐılık gelen zel anahtar yalnızca sertifikada "Anahtar Kullanımı" alanında belirtilen amalar dahilinde kullanılabilir.

4.5.2. nc KiŐilerin Sertifika ve Aık Anahtarı Kullanımı

Sertifika sahibine ait Kurumsal Őifreleme Sertifikasının iinde yer alan aık anahtar, nc kiŐilerce EYP 2.0 kapsamında verilerin Őifreli iletimi amacıyla kullanılır. Aık anahtarın veya sertifikanın, belirtilen ama dıŐında kullanılması sonucu oluŐabilecek zararlardan nc kiŐiler sorumludur.

4.6. Sertifika Süresinin Uzatılması

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

4.7. Sertifika Yenileme

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

4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi aşağıdaki durumlarda yapılmaktadır:

- Kurumsal Şifreleme Sertifikasının kaybedilmesi veya çalınması
- Kurumsal Şifreleme Sertifikasını içeren donanımın arızalanması
- Akıllı karta veya HSM'ye erişim verisinin kaybedilmesi, çalınması veya unutulması
- Kurumsal Şifreleme Sertifikasının iptal edilmesi ve yenisinin talep edilmesi
- Kurumsal Şifreleme Sertifikasının geçerlilik süresinin sona ermesi veya geçerlilik süresinin sonuna yaklaşılması
- Kurumsal Şifreleme Sertifikasında bilgi deęişikliği gerekmesi

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildięi

DETSİS'te bilgileri bulunan ve DETSİS tarafından Kurumsal Şifreleme Sertifikası alma yetkisi olduęu belirtilen kamu kurum ve kuruluşları Kurumsal Şifreleme Sertifikası yenileme başvurusunda bulunabilirler.

Yenileme süreci, Elektronik Mühür/Kurumsal Şifreleme Başvuru Listesinin eksiksiz bir şekilde doldurularak Kamu SM'ye iletilmesiyle başlar. Kurumun sertifika yenileme işlemleri, kurum tarafından yetkilendirilmiş sertifika sorumluları tarafından yürütülür.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Yenileme süreci, sertifikanın bitimine 2 ay kala başlatılabilir. Kamu SM, yenileme sürecinde kurumların sorun yaşamaması amacıyla kurum sertifika sorumlularının kayıtlı kurumsal e-posta adresleri üzerinden sertifika bitiş tarihine 3 ay, 2 ay, 1 ay, 15 gün ve 1 hafta kala kuruma hatırlatma maili göndermektedir.

Elektronik Mühür/Kurumsal Şifreleme Başvuru Listesi eksiksiz şekilde doldurularak sertifika sorumlularından biri tarafından elektronik imzalanmış bir şekilde (BES formatında ve .p7s uzantılı olarak), bilgi@kamusm.gov.tr veya kurumsal_bilgi@kamusm.gov.tr e-posta adresine iletilir. Kurum tarafından HSM kullanılacaksa başvuru listesi içerisindeki "HSM Bilgileri" de doldurulmalı ve liste HSM Cihaz Sorumlusu tarafından da seri olarak imzalanmalıdır.

Bilgi ve belgeler hatasız ve tam ise gerekli doğrulamalar yapılır. Belgelerde gözle görülen tahrifat, hata, eksik sayfa, eksik onay/paraf ya da eksik bilgi olması veya bilgilerin yanlışlığının tespit edilmesi durumunda doğrulama yapılamaz. Başvuru evraklarının, tanımlanan yöntemler dışında bir yöntemle iletilmesi veya evraklarda hata/eksiklik bulunması durumunda kurum, e-posta ile bilgilendirilir.

Başvurusu kabul edilen kurumların sertifika yenileme süreci başlatılır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sahibinin Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koőulu

Bölüm 4.4.1’de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayınlanması

Bölüm 4.4.2’de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diđer Tarafllara Duyurulması

Bölüm 4.4.3’te tanımlanmaktadır.

4.8. Sertifikada Bilgi Deęiőiklięi

Sertifikada bilgi deęiőiklięi, anahtar çifti hariç sertifikada yer alan bilgilerin deęiőmesi olarak tanımlanmaktadır. Sertifika içerięinde yer alan bilgilerde deęiőiklik olması, sertifikanın yenilenmesini gerektirmektedir. Bilgi deęiőiklięinin gerekli olduęu durumlarda, kurum Bölüm 4.7’de belirtilen sertifika yenileme sürecini iőletmelidir.

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildięi Durumlar

Sertifikanın kullanım süresi dolmadan geçerlilięini yitirdięi durumlarda, sertifika iptal edilir. İptal edilen sertifikayla bir daha iőlem yapılamaz. Sertifika, aőaęıda belirtilen durumlarda iptal edilir:

- Sertifika sahibi kurumun talebi
- Sertifika içerięindeki bilgilerin sahtelięinin veya yanlıőlıęının ortaya çıkması veya bilgilerin deęiőmesi
- Sertifika sahibi kurumun kapanması
- Sertifika sahibi kurumun KAYSİS unvanının deęiőmesi
- Sertifika sahibi kurumun DETSİS numarasının deęiőmesi
- Özel anahtarın güvenlięinin kaybedildięinden őüphelenilmesi
- Özel anahtarın içinde bulunduęu aracın kaybolması, çalınması veya bozulması
- Akıllı kart veya HSM eriőim verisinin unutulması veya kaybedilmesi
- Sertifikanın taahhütnameler veya SUE dokümanında belirtilen őartlara aykırı kullanımının tespit edilmesi
- Kamu SM’ye evrakları gönderen sertifika sorumlusu/sorumlularının kurumun onayını almadıęının tespit edilmesi veya ilgili kurum tarafından söz konusu durumun Kamu SM’ye bildirilmesi
- Sertifikanın hatalı üretilmesi
- Kamu SM’nin Kurumsal Őifreleme Sertifikasını imzalamak için kullandıęı imza oluőturma verisinin bütünlüęünün bozulması veya gizlilięinin ortadan kalkması
- Kamu SM’nin iőleyiőine son verilmesi ve verilen Kurumsal Őifreleme Sertifikalarının yönetim iőlemlerinin baőka bir ESHS tarafından devamlılıęının saęlanamaması

4.9.2. Sertifika İptal Baővurusunu Kimler Yapabilir

Sertifika iptal baővurusu, sertifika sahibi kurum veya sertifika sahibi kurum tarafından yetkilendirilmiş Kurumsal Őifreleme Sertifikası Sorumluları tarafından yapılabilir. Kamu SM, Bölüm 4.9.1’de tanımlanan tüm durumlarda iptal yetkisine sahiptir.

4.9.3. Sertifika İptal Başvurusunun İőlenmesi

Kurumsal Őifreleme Sertifikası iptal iőlemi, kurum tarafından yetkilendirilen Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından Kamu SM resmi internet sitesinde yer alan Online İőlemler menüsü aracılıđı ile yapılır.

Kamu SM Online İőlemler üzerinden yapılan iptal başvurusunda, Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları sisteme kimlik dođrulamasıyla giriő yaparak iptal talebinde bulunur. İlgili talebin ardından, Kurumsal Őifreleme Sertifikası Kamu SM sisteminde otomatik olarak iptal edilir ve DETSİS sisteminden silinir.

İptal iőlemlerinin Kamu SM Online İőlemler üzerinden yapılamadıđı durumda Kamu SM web sitesinde belirtilen yöntemlerle iptal iőlemi gerçekleştirilebilir. Kamu SM, web sitesi üzerinden iptal iőleminin gerçekleştirilebilmesi için gerekli hizmetleri kesintisiz olarak sunar.

İptal sürecinin web sitesinde belirtilen yöntemle fiziksel olarak yürütölmesi durumunda sürecin başlatılmasının ardından evrak asılları Kamu SM'ye ulaőana kadar kurum yazıőmalarında yaőanabilecek aksaklıkların en aza indirgenmesi amacıyla Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları telefon ile aranarak iptal talebi teyit edilir ve iptali talep edilen sertifika askıya alınır. Evrak asıllarının ulaőmasının ardından Kamu SM'ye e-posta üzerinden gönderilen evraklar ile asılları karőılaőtırılır ve askıya alınan sertifika iptal edilir.

Kurumsal Őifreleme Sertifikası iptal edildikten sonra, Kamu SM sertifika sahibi kurumu ve gerekirse sertifika sorumlularını iptal iőlemine dair bilgilendirir. Kurumsal Őifreleme Sertifikaları geçmiőe yönelik olarak iptal edilmez.

Kamu SM iptal bilgilerini en kısa zamanda iőleyerek SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da Őifreleme sertifikasının durumunu iptal konumuna getirmek suretiyle kamuya duyurur. Kamuya duyurulan iptal durum kayıtları en az Őifreleme sertifikasının seri numarası ile Kamu SM'nin elektronik imzasını taőır. SİL dosyası, Kamu SM'ye ait imza oluőturma verisi ile imzalanır. İptal edilen Kurumsal Őifreleme Sertifikaları geçerlilik süresinin sonuna kadar SİL içinde tutulur. Geçerlilik süresi dolduktan sonra Kurumsal Őifreleme Sertifikası SİL içinden çıkarılır. ÇİSDUP Yanıtlayıcı'da geçerlilik süresi dolan iptal edilmiő Kurumsal Őifreleme Sertifikalarının durumu iptal edilmiő olarak görünmeye devam eder.

Kurum, Kurumsal Őifreleme Sertifikası iptal edildikten sonra yeniden Kurumsal Őifreleme Sertifikası talebinde bulunulabilir.

4.9.4. İptal İsteđi Ertelenme Süresi

Böyle bir süre öngörölmemiőtir.

4.9.5. İptal İsteđinin İőlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal iőleme alır ve Kurumsal Őifreleme Sertifikasını en geç 24 saat içerisinde iptal eder. İptal edilen Kurumsal Őifreleme Sertifikası bilgisini bir sonraki SİL içinde yayımlar, ÇİSDUP Yanıtlayıcı'dan derhal duyurur. Sertifika iptal talebinin Kamu SM sistemi içinde iőlenmesinin ardından bir sonraki SİL'in yayımlanma süresi Bölüm 4.9.7'de belirtilmiőtir.

4.9.6. Üçüncü Kiőilerin Sertifika İptal Durumunu Kontrol Gerekliliđi

Kamu SM, iptal durum kayıtlarını ücretsiz olarak kamuya açar. Sertifika iptal durum kayıtlarına, sorgulama yapacak kiőinin kimlik dođrulamasına gerek kalmadan dileyen herkes tarafından eriőilebilir. Kamu SM, iptal durum kayıtlarına eriőtimin sürekliliđini sađlar.

Üçüncü kişiler Kurumsal Őifreleme Sertifikasına dayanarak işlem yapmadan önce Kurumsal Őifreleme Sertifikasının geçerliliğini SİL ya da ÇİSDUP üzerinden kontrol etmekle yükümlüdür.

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

4.9.7. Sertifika İptal Listesi Yayımına Sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduđu 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 Kurumsal Őifreleme 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 duyurulduđu SİL dosyası, en geç 12 (on iki) ayda bir yenilenir. Kamu SM'ye ait bu sertifikalardan birinin iptali durumunda SİL dosyası derhal yenilenir.

4.9.8. Sertifika İptal Listesi Yayımına Gecikme Süresi

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

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Hizmeti

Kamu SM, Kurumsal Őifreleme Sertifikalarının iptal durum bilgisini ÇİSDUP üzerinden yayımlar. ÇİSDUP Yanıtlayıcı'dan yayımlanan iptal durum kaydı Kamu SM'ye ait olduđu duyurulan imza oluŐturma verisiyle imzalanır.

ÇİSDUP desteđi olan uygulamalar Kurumsal Őifreleme Sertifikalarının geçerlilik durum kontrolünü ESHS EriŐim 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 sađladığı için, SİL yanında çevrim içi sertifika iptal durum kaydı desteđini de vermektedir.

SİL dosyası, iptal edilen her Kurumsal Őifreleme 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 getireceđi yüke karşılık, ÇİSDUP ilgili Kurumsal Őifreleme Sertifikasının iptal olup olmadığı bilgisinin talep eden tarafa soru cevap yöntemiyle iletilmesine olanak tanımaktadır. Bu nedenle, üçüncü tarafların teknolojik altyapıları el verdiđi ölçüde ÇİSDUP kullanmaları önerilir.

4.9.11. Diđer 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 kuruma ait özel anahtarın güvenliğini yitirmesi durumunda Kurumsal Őifreleme Sertifikası iptal edilir. Kurum Őifreleme Sertifikasının iptal edilmesi dışında herhangi bir işlem uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Kurumsal Őifreleme Sertifikası, üretim veya kullanım aşamasında geçici iptal durumunu sağlamak amacıyla askıya alınabilir.

Kurumsal Őifreleme Sertifikaları biri yedek olmak üzere 2 adet üretilir. Sertifikalar akıllı kart içerisinde kullanılıyorsa askı durumunda kuruma gönderilir. Kullanılacak sertifika, kurumun sertifika sorumlusu/sorumluları tarafından Kamu SM Online İşlemler üzerinden askıdan indirilir. Aynı anda sertifikalardan sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

İlk başvuruda talep edilen sertifika HSM içerisinde kullanılıyorsa asıl sertifika geçerli; yedek sertifika askıda olacak şekilde yükleme gerçekleştirilir. Asıl sertifikanın yüklemesi geçerli olarak yapıldığından, kurumun sertifika sorumlusu/sorumluları tarafından Kamu SM Online İşlemler üzerinden askıdan indirilmesine ihtiyaç bulunmamaktadır.

Kurum sertifika yenileme talebinde bulunduysa, yeni üretilen sertifikalar askıda üretilir (HSM cihazına askıda olmak üzere yüklenir) ve geçerlilik süreleri başladığında askıdan indirilerek kullanılabilir hale gelir.

Sertifika sahibi kurum veya kurumun yetkilendirdiği sorumlusu/sorumluları, aşağıda belirtilenlere benzer sebeplerden dolayı Kurumsal Őifreleme Sertifikasını askıya alabilir:

- Sertifika sahibi kurumun Kurumsal Őifreleme Sertifikasını kullanım dışı bırakmak istemesi
- Kurumsal Őifreleme Sertifikasının iptalini gerektirebilecek bir durumun ortaya çıktığından şüphelenildiği durumlarda, yanlışlıkla iptalini engellemek amacıyla, Kurumsal Őifreleme Sertifikasının önce askıya alınmak istenmesi
- Aktif kullanılan geçerli sertifikanın kayıp/çalıntı/arıza durumunda yedek sertifikanın kullanıma açılabilmesi

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Kurumsal Őifreleme Sertifikasının askıya alma başvurusu, sadece sertifika sahibi kurum veya kurumun yetkilendirdiği Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumluları tarafından yapılır.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Kurumsal Őifreleme Sertifikası askı başvurusu, Kamu SM web sitesinde yer alan Online İşlemler menüsünden veya Online İşlemlerin Kamu SM kaynaklı erişilemez olması durumunda sertifika sorumlusu/sorumluları tarafından telefonla Kamu SM'ye bildirilerek yapılır. Telefonla yapılan görüşme kayıt altına alınır. Askı başvurusu alındığında öncelikle başvuruyu yapan sertifika sahibi kurumun ve yetkililerinin kimlik belirlemesi ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan askı başvuruları işleme alınmaz.

Askıya alınan Kurumsal Őifreleme Sertifikası için, SİL'de geçici olarak iptal edildiğini belirten sebep kodu kullanılır, ÇİSDUP Yanıtlayıcı'da sertifika durum bilgisi iptal konumuna getirilir. Kamu SM, Kurumsal Őifreleme Sertifikası askıya alındıktan sonra, gerekli gördüğü durumlarda sertifika sahibi kurumu ve sertifika sorumlusu/sorumlularını sertifikanın askıya alındığına dair bilgilendirir.

Kurumsal Őifreleme Sertifika Sorumlusu/Sorumluları, Kamu SM Online İşlemler üzerinden kuruma ait sertifikayı askıdan indirebilir. Askıya alınan sertifika en az bir defa SİL'e girmeden askıdan indirilemez.

Kuruma ait Kurumsal Őifreleme Sertifikalarından aynı anda sadece biri aktif olabilir. Aktif olan sertifika askıya alınmadan ya da iptal edilmeden yedek sertifika askıdan indirilemez.

Kamu SM'ye ait K k SHS ve Kurumsal Őifreleme SHS sertifikaları askıya alınmaz.

4.9.16. Askıda Kalma Suresi

İlk üretim sonrasında askıdan indirmeyle ilgili bir s re kısıtı bulunmamakla birlikte kurum tarafından askıya alınan sertifikalar en az bir defa SİL'e girmeden askıdan indirilemez.

4.10. Sertifika Durum Servisleri

 ç nc  kiŐiler, Kamu SM sertifika iptal durum kayıtlarına SİL ve  İSDUP servisleri aracılıđıyla ulaŐır.

4.10.1. İŐletimsel  zellikleri

 ç nc  kiŐiler, sertifika iptal durum kayıtlarına Kamu SM'ye ait SİL dosyalarından eriŐebilirler. Kamu SM'ye ait SİL dosyalarına eriŐim bilgileri B l m 7.1.2 Tablo 1'de verilmiŐtir.  ç nc  kiŐiler, iptal durum kaydını her kontrol etmek istediklerinde g ncel SİL dosyasını Kamu SM bilgi deposundan kendi sistemlerine kopyalar ve gerekli kontrolleri yaparlar.

 İSDUP İstemci desteđi olan  ç nc  kiŐiler, sertifika iptal durumunu  İSDUP Yanıtlayıcı'dan  ğrenebilirler.  İSDUP Yanıtlayıcı eriŐim adresi B l m 7.1.2 Tablo 1'de verilmiŐtir.  ç nc  kiŐiler, Kurumsal Őifreleme Sertifikalarının ge erlilik durumunu her kontrol etmek istediklerinde,  İSDUP Yanıtlayıcı  zerinden sorgulama yaparlar.

4.10.2. Servisin EriŐilebilirliđi

SİL ve  İSDUP servislerinin verildiđi sistemlere eriŐimin kesintisiz olarak sađlanabilmesi i in gereken t m tedbirler Kamu SM tarafından alınır. Ancak buna rađmen eriŐimin bir s reliđine kesilmiŐ olması durumunda  ç nc  kiŐiler, problem giderilinceye kadar sertifika iptal durum kaydını kontrol etmeleri gereken iŐlemlerini durdurur.  ç nc  kiŐilerin iptal durum kaydını, eriŐimin kesilmesi sebebiyle kontrol etmeden yaptıkları iŐlemlerden dođan zararlardan Kamu SM sorumlu tutulamaz.

4.10.3. İsteđe Bađlı  zellikler

D zenlenmesine gerek duyulmamıŐtır.

4.11. Sertifika Sahipliđinin Sona Ermesi

Kurumsal Őifreleme Sertifikasının kullanım s resinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliđi sona erer. Kamu SM, Kurumsal Őifreleme Sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda sertifika sahibi kurumu ve Kurumsal Őifreleme Sertifikası Sorumlusunu/Sorumlularını bilgilendirir. Kamu SM, Kurumsal Őifreleme Sertifikalarının s resi dolmadan en az 15 (on beŐ) g n  nce sertifika sahibi kurumu bilgilendirir.

4.12. Anahtar Yeniden  retme

Sertifika sahiplerine ait anahtarların yeniden  retilmesi veya yedeklenmesi iŐlemi uygulanmamaktadır.

5. Y netim, İŐlemsel ve Fiziksel Kontroller

Bu b l mde Kamu SM tarafından sertifika hizmeti verilirken yerine getirilmesi gereken teknik olmayan g venlik kontrolleri anlatılmıŐtır.

5.1. Fiziksel Güvenlik Denetimleri

Kamu SM sisteminin alıŐtıĐı cihazların bulunduĐu binalar ve odalar, giriŐ ve ıkıŐların kontrol edildiĐi yetkisiz kiŐilerin giriŐini engelleyen güvenlik nlemleri ile donatılmıŐtır. Güvenli alanlara eriŐimlerin kaydı tutulmaktadır.

5.1.1. Tesis Yeri ve İnŐaatı

Kamu SM operasyonları Gebze ve Ankara'daki tesislerde yrtlmektedir. Kamu SM sisteminin alıŐtıĐı binanın bulunduĐu Gebze tesisi, yerleŐim merkezinden uzak, yangın, su baskını, deprem, yıldıırım ve hava kirliliĐinden en az etkilenecek, giriŐ ve ıkıŐların kontrol edildiĐi bir blgedir. Alanlara ve binalara eriŐim, tek kiŐinin giriŐine veya ıkıŐına izin veren HI-SEC kilitleme kapıları dahil olmak zere fiziki güvenlik, video izleme ve kimlik doĐrulama olmak zere oklu güvenlik ile korunmaktadır. Ankara tesisi farklı seviyelerde fiziksel kontrol bulunan bir alandır. Yetkisiz personel ve kayıtsız ziyaretiler bu hassas alanlara giremez.

Bina, yksek güvenlik gerektiren iŐlerin yapılmasına imkan saĐlayan yapıdadır. Bina, esnek (elik yapı) ve sert (elik atıyla desteklenmiŐ beton yapı veya desteklenmiŐ beton yapı) yapı Őartlarını saĐlamaktadır.

Kamu SM'nin kurulduĐu yer ve binada g birimleri, haberleŐme niteleri, yedekli iklimlendirme niteleri, havalandırıcılar, yangın sndrc sistemler mevcut olup, deprem, su ve afetlere karŐı gerekli tedbirler alınmıŐtır.

5.1.2. Fiziksel EriŐim

Kamu SM yazılım ve donanım modlleri ile arŐivlere eriŐim denetim altındadır. Binaya giriŐler güvenlik grevlilerinin kontrol altında, geliŐmiŐ eriŐim kontrol cihazlarıyla saĐlanmaktadır.

Bina iinde Kamu SM sistemine ait yazılım ve donanım aralarının bulunduĐu, elektronik veya kaĐıt ortamdaki bilgilerin tutulduĐu, sistemin iŐletildiĐi ve ynetildiĐi odalara eriŐim geliŐmiŐ eriŐim kontrol cihazlarıyla yapılmaktadır. Güvenli alanlarda tek kiŐi alıŐma yapamaz, en az biri yetkili olmak zere 2 (iki) kiŐi ile alıŐma yapılır. Yetkisi olmayan kiŐiler sistemin kurulu olduĐu odalara giriŐ yapamamaktadır. Yetkisiz kiŐilerin donanım bakımı veya bunun gibi sıra dıŐı bir amala sistemin kurulu olduĐu odalara giriŐleri zel eriŐim talimatları uyarınca dzenlenir.

5.1.3. G KaynaĐı ve Havalandırma

AŐaĐıdaki g kaynakları Kamu SM iŐlevlerinin yerine getirilmesi ve srekliliĐin saĐlanması iin kullanılmaktadır:

- G alma ve devŐirme (transformatr) birimleri
- DaĐıtım paneli
- Trafo
- UPS
- Kuru ak
- Acil jeneratr

Bina aŐırı ısınmayı nleyebilecek kapasitede ve uygun nem seviyesini ayarlayabilecek zelliklerde kesintisiz/yedekli iklimlendirme sistemleri ile donatılmıŐtır.

5.1.4. Su Baskınları

Kamu SM işlevlerinin yerine getirildiđi ortamlarda su baskınlarından en az zarar göreceđek Őekilde önlemler alınmıŐtır.

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

Hassas bilgilerin bulunduđu ve artık kullanılmayan elektronik veya kađıt ortamda tutulan bilgiler/cihazlar imha prosedürüne uygun bir Őekilde 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 bulunduđu mekan, asıl sistemin sađladığı tüm güvenlik ve işlevsellik şartlarını sađlar.

Kamu SM, sisteminin sürekliliđini sađlayabilmek amacıyla gerekli gördüđu bileŐenleri, farklı bir fiziksel mekanda güvenli kasalarda saklar.

5.2. Prosedürel Kontroller

5.2.1. Güvenilir Roller

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

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

Güvenlik Personeli: Kamu SM güvenlik politikalarının uygulanmasından sorumludur.

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

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

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

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

Sertifika Üretim Sorumlusu: Sertifika üretimini gerçekleŐtiren personeldir.

5.2.2. Her İşlem İçin Gereken KiŐi Sayısı

Kamu SM, Kök SHS ve Kurumsal Őifreleme SHS'ye ait sertifika üretilmesi ve iptal edilmesi için birden fazla kiŐinin aynı anda hazır bulunmasını sađlar.

Kamu SM, Kk SHS ve Kurumsal Őifreleme SHS'ye ait imza oluŐturma verilerinin baŐka bir kriptografik modl ierisine yedeklenmesi iin birden fazla kiŐinin aynı anda hazır bulunmasını saėlar.

5.2.3. Kimlik Doėrulama ve Yetkilendirme

Kamu SM iŐleyiŐinin her adımında, iŐlemleri yerine getirecek kiŐilerin kimlik tanımlaması ve doėrulaması yapılır. Bylece her sistem birimine sadece yetkili kiŐilerin eriŐimi saėlanır. Sistemdeki bazı birimlere eriŐim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere eriŐimin saėlanabilmesi iin kimlik doėrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler erevesinde sistemde iŐlem yapılabilir.

Kamu SM sistemi iinde kimlik doėrulama gvenli donanım araları, parolalar, gizli sorular ve biyometrik veri kullanılarak gncel kriptografik yntemlerle yapılır.

Kullanıcı hesapları yetkilendirme ve ynetiminde, Kamu SM EriŐim Ynetimi Politikası temel alınmaktadır.

5.2.4. Grevlerin Ayrılmasını Gerektiren Roller

AŐaėıda verilen roller arasında grevler ayrılıėı vardır:

- Sertifika retim Sorumlusu ile Sertifika Kayıt Sorumlusu arasında
- Sistem Denetisi ile diėer roller arasında
- Sistem Yneticisi ile Gvenlik Personeli arasında

5.3. Personel Gvenlik Kontrolleri

5.3.1. KiŐisel GemiŐ, Deneyim ve Nitelik Gerekleri

alıŐanlar sistemin iŐleyiŐ ve gvenlik gereklerini saėlayabilecek nitelikte, bilgili ve deneyimli kiŐilerden seilir. Kamu SM'nin istihdam ettirdiėi personel sistem gvenliėi, veri tabanı ynetimi, elektronik imza teknolojileri ve uygulamaları, sertifika ynetimi ile ilgili konularda bilgi ve deneyimi olan nitelikli kiŐilerden oluŐur.

5.3.2. GemiŐ AraŐırtması

alıŐanların Kamu SM'nin iŐletilmesinde gvenlik ihtiyalarının gerektirdiėi gvenilirliėe sahip olması gerekmektedir. Personelin gvenilirliėi gemiŐine ynelik yapılan araŐtırmalar ile belirlenir. Őe alınmadan nce gemiŐe ynelik yapılan araŐtırmalarda personelin herhangi bir sebepten dolayı hkm giyip giymemiŐ olduėu araŐtırılır. Adli sicil kayıtları incelenir. Gvenlik soruŐturması biten personel Őe baŐlatılır. Őe baŐlayan personelin bilgi gvenliėi farkındalık eėitimleri tamamlanmadan, sistemlere eriŐimine izin verilmez.

5.3.3. Eėitim Gerekleri

alıŐanlar, Kamu SM'deki iŐlerine aktif olarak baŐlamadan nce gerekli eėitimden geirilirler. alıŐanlara verilen eėitimde Kamu SM'de uygulanan gvenlik ilkeleri, sistemin teknik ve idari iŐleyiŐi, iŐleriyle ilgili sreler, sre iindeki grev ve sorumluluklar anlatılır.

5.3.4. Srekli Eėitim Gerekleri ve Sıklıėı

Kamu SM sisteminde yapılan deėiŐikliklerin bildirilmesi amacıyla personele verilen eėitimler gerekli grldke tekrarlanır. Yeni greve baŐlayanlar iin eėitimler tekrarlanır.

Kamu SM, alıŐanlarına yılda en az bir defa, siber gvenlik ve sosyal mhendislik saldırılarına karŐı farkındalık oluŐturmak amacıyla, bilgi gvenliĐi eĐitimi vermektedir.

5.3.5. Grev DeĐiŐim SıklıĐı ve Sırası

Dzenlenmesine gerek duyulmamıŐtır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

Kamu SM personelinin tamamen veya kısmen sahte elektronik sertifika oluŐturması, geerli olarak oluŐturulan elektronik sertifikaları taklit veya tahrif etmesi, yetkisi olmadan elektronik sertifika oluŐturması veya bu elektronik sertifikaları bilerek kullanması halinde ve diĐer yetkisiz eylemlerde ilgili mevzuat gereĐince bilgi gvenliĐi politikaları ihlali ve ihlalin boyutuna gre hukuki soruŐturma ve disiplin sreci baŐlatılır.

5.3.7. AnlaŐmalı Personel Gereksinimleri

Kamu SM verdiĐi hizmetler iin dıŐ kaynak kullanmak durumunda kaldıĐında, bu hizmeti saĐlayacak firma personeli ile ilgili gvenlik kontrollerini, firma ile yaptıĐı szleŐme ile belirler.

5.3.8. SaĐlanan Dokmantasyon

alıŐanlara iŐleriyle ve Kamu SM sreleriyle ilgili gerekli kılavuz ve destek dokmanlar ve bilgi gvenliĐi politikaları kapsamındaki ilgili dokmanlar saĐlanır.

5.4. Denetim Kayıtları

Kamu SM iŐleyiŐi sırasında gerekleŐtirilen anahtar ve sertifika ynetimi, sistemin gvenliĐi ile ilgili iŐlerin kayıtları tutulur. Tutulan kayıtların bir kısmı elektronik ortamda, diĐer bir kısmı ise kaĐıt zerindedir. Denetimler sırasında gerekli grldĐ takdirde bu kayıtlar grevliler tarafından incelenir.

5.4.1. Kaydedilen iŐlemler

Kamu SM sisteminde aŐaĐıda yapılan iŐlemler ile ilgili elektronik veya kaĐıt ortamda yapılan iŐlerin kayıtları tutulur:

- Kamu SM anahtarlarının yaŐam dngs ynetimi iŐlemleri
 - Anahtar retimi
 - Anahtar yedekleme
 - Anahtar daĐıtımı
 - Anahtar saklama
 - Anahtar arŐivleme
 - Anahtar yok etme
 - Kriptografik modl yaŐam dngs iŐlemleri
- Sertifika retim, yenileme, askıya alma ve iptal baŐvuruları
 - BaŐvuru sahibi tarafından sunulan belgelerin neler olduĐu bilgisi
 - BaŐvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
 - BaŐvuru sırasında elektronik veya kaĐıt ortamda alınan form veya belgeler
 - KaĐıt belgelerin kopyalarının nerede saklandıĐı bilgisi
 - Geerli ve geersiz alınan tm baŐvuru bilgileri

- Sertifika yaŐam dđngüsü yđnetimi iŐlemleri
 - Sertifika baŐvurusunun iŐlenmesi
 - Sertifika üretimi
 - Sertifika yenileme
 - Sertifika iptal etme
 - SİL yayımlanması
- Güvenlikle ilgili diđer iŐlemler
 - Sisteme baŐarılı veya baŐarısız tüm eriŐim denemeleri
 - ÇalıŐanlar tarafından gerçekteŐirilen güvenlik sistemi iŐlemleri
 - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve deđiŐtirilmesi
 - Güvenlik profili deđiŐiklikleri
 - Sistemin çökmesi, donanım hataları ve diđer bozukluklar
 - Güvenlik cihaz/yazılım iŐlemleri (Güvenlik Duvarları, IPS, HIDS, Router vb.)
 - Kamu SM'ye ziyaretçi giriŐ ve çıkıŐı

Kayıtlarda genellikle kayıt zamanı ve kaydı oluŐturan personelin ismi bulunur.

5.4.2. Kayıtların İncelenme Sıklıđı

Sistemin iŐleyiŐiyle ilgili tutulan kayıtlar belirli zaman aralıklarıyla incelenir. İncelemeler haftalık olarak yapılır ve herhangi bir güvenlik açıđı oluŐup oluŐmadıđı kontrol edilir. Buna ek olarak, sistemde olađandıŐı hareketlerin görölmesi ya da alarm durumlarında tutulan kayıtlar incelenir. Yapılan incelemeler sonucu gerek görölün ve baŐlatılan iŐlemler de belgelenir.

Sertifika baŐvurusu sırasında sertifika sahiplerinden gelen bilgilerin elektronik veya kađıt ortamda tutulan kayıtları, sertifika yaŐam dđngüsü süresi içinde gerek göröldükçe veya yasal iŐlemler sebebiyle incelenebilir.

5.4.3. Kayıtların Saklanma Süresi

Kayıtlar incelenmelerinden sonra, en az 2 (iki) ay sistemde tutulur. Ardından arŐivlenir. 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 aŐađıdaki önlemler alınmıŐtır:

- Yetkisi olmayan kiŐiler, elektronik kayıtların bulunduđu sistemlere eriŐemezler.
- Kađıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunur.
- Kayıtların deđiŐtirilmesine izin verilmez, bunun için gerekli güvenlik önlemleri alınmıŐtır.
- Elektronik olarak saklanan ve sistemin iŐleyiŐi aŐısından kritik olan kayıtlar, iŐlemi yapan personel tarafından gerektiđinde elektronik imza ile imzalanarak saklanır. Böylece kritik kayıtlarda oluŐabilecek her deđiŐiklik sistem tarafından fark edilir.
- Kritik bilgiler gerektiđinde Kamu SM'ye ait anahtarlarla Őifreli olarak saklanır.

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliđi göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeđi 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. Otomatik kayıt toplama işlemi sistemin başlatılmasından kapanmasına kadar çalışır.

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 Deđerlendirilmesi

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

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sahibi kurum 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
- Zaman Damgası Sİ-SUE dokümanları
- Sertifika yönetim prosedürleri
- Başvuru Formu ve Taahhütnameler
- 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, deęiřtirmeyi ve silinmeyi engelleyecek řekilde elektronik ve fiziksel olarak güvenli tutulur. Arşivler yetkisiz alıřanların eriřimine kapalıdır. Arşivlerin tutulduęu ortam Bölüm 5.5.2’de belirtilen süre boyunca arşivlerin zarar görmesini engelleyecek řekilde seilir.

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi ieren elektronik arşivler Kamu SM iř süreklilięi politikası gereęince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüęü kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kaęıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir.

5.6. Anahtar Deęiřimi

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 iftinden yeni anahtar iftine geiř iřlemleri yapılır. Anahtar deęiřimi iřlemleri řunları gerektirir:

- Kök sertifikası kullanım süresinin dolmasından en ge 3 (ü) yıl önce; alt kök sertifikası kullanım süresinin dolmasından en ge 1 (bir) yıl önce iřlemler bařlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM’nin eski imza oluřturma verisiyle imzalanmıř sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyaları aynı Kamu SM imza oluřturma verisiyle imzalanıyorsa, Kamu SM’nin eski imza oluřturma verisiyle oluřturulmuř sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL’leri eski imza oluřturma verisiyle imzalanmaya devam eder. Yeni üretilen sertifikalar için oluřturulan yeni SİL dosyası yeni Kamu SM imza oluřturma verisiyle imzalanır.
- Kamu SM, anahtarlarının yenilendięi bilgisini Kamu SM resmi web sitesi üzerinden duyurur ve sertifika hizmeti verdięi tarafları bilgilendirir.

5.7. Güvenlięin Yitilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirlięin Yitilmesi Durumunun Düzeltilmesi

Güvenilirlięin yitilmesi durumlarında, sertifika yönetim sisteminin en kısa zamanda yeniden güvenli olarak alıřmaya bařlaması, durumdan etkilenen tarafların haberdar edilmesi, zararlarının en aza indirgenmesi için belirlenen süreçler iřletilir.

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

iř süreklilięini saęlamak için sistemde kullanılacak aktif cihazlar ve depolama alan aęı bileřenleri yedekli yapıda alıřmaktadır ve kritik süreçler için felaket kurtarma merkezi oluřturulmuřtur. Depolama ünitesi

fiziksel olarak farkı bir noktada bulunan veri depolama ünitesi ile veri senkronizasyonu yapabilecek niteliktedir. Arızanın giderilmesi süreci arıza sebebinin araştırılmasını, hatanın giderilmesini ve gerekli görüldüğünde Kamu SM hizmetlerini güvenilir yedek ortama aktarmayı içerir.

5.7.3. İmza Oluřturma Verisinin Gizliliğinin Kaybedilmesi

Kamu SM'nin Kurumsal Őifreleme Sertifikalarını imzalamada kullandığı imza oluřturma verisinin gizliliğinin kaybedildiğinden Őüphelenilmesi ya da bunun öğrenilmesi durumunda ilgili sertifika en kısa zamanda iptal edilir ve aőağıdaki 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, Kurumsal Őifreleme Sertifikası sahiplerinin durumdan ne şekilde etkileneceğini belirten açıklamayı yapar, eski özel anahtarıyla oluřturulan Kurumsal Őifreleme Sertifikalarına güvenilmemesi için ilgili taraflara ihtarda bulunur.
- Kamu SM, kendisine ait sertifikanın iptal edildiği bilgisini yayımladığı SİL dosyasında belirtir.
- Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikaları iptal edilir. İptal bilgisi sertifika sahipleri ile ilgili kurumlara en kısa zamanda bildirilir.
- Kamu SM Kurumsal Őifreleme Sertifikası isteklerine yanıt vermeyi durdurur.
- İlgili taraflar Kamu SM'nin durumuyla ilgili sürekli bilgilendirilir.
- Kamu SM imza oluřturma verisinin yok edilmesi sürecini iřletir.
- Kamu SM, yeni bir anahtar çifti ve sertifika üreterek yeni sertifikayı taraflara bildirir.
- Kamu SM anahtar çiftinin yenilenmesiyle, iptal edilen Kurumsal Őifreleme Sertifikalarının sertifika sahibinden gelen talep doğrultusunda sertifika yenileme süreci başlatılır.

5.7.4. Arıza Sonrası Yeniden Çalıřırlık

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, Elektronik İmza Kanunu'nun Uygulanmasına İliřkin Usul ve Esaslar Hakkında Yönetmelik'te belirtilen şekilde faaliyetlerine son verebilir. Bu durumda gerçekleştirilecek işlemler [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 gerçekleřtirdiği sistemler CWA 14167-1, ETSI TS 101 456 ve TS ISO/IEC 27001 veya ISO/IEC 27001 gereklerini sağlar.

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1. Kök SHS, Kurumsal Őifreleme SHS, ÇİSDUP Yanıtlayıcı Anahtar Çifti Üretimi

Kamu SM bünyesinde aŐağıdaki anahtar çiftleri oluşturulur:

- Kök SHS'ye ait imza oluŐturma ve dođrulama verisi
- Kurumsal Őifreleme SHS'ye ait imza oluŐturma ve dođrulama verisi
- ÇİSDUP Yanıtlayıcı'ya ait imza oluŐturma ve dođrulama verisi

Kök SHS, Kurumsal Őifreleme SHS ve ÇİSDUP Yanıtlayıcı'ya ait anahtar çiftleri, yetkisi olmayan personelin giremeyeceđi güvenli odada, birden fazla eđitimi personelin gözetiminde, ađ ortamına kapalı sistemlerde, güvenli anahtar üretimi için gereken testlerden geçmiŐ, FIPS PUB 140-2 seviye 3 veya EAL4+ standartlarını sađlayan güvenli yazılım ve/veya donanım kullanılarak üretilir. Üretilen özel anahtar güvenli kriptografik modül içinde saklanır. Modül güvenli odadan dıŐarıya çıkarılmaz. Yapılan bütün iŐlemler kayıt altına alınır ve iŐlemi gerçekteŐiren personel tarafından onaylanır.

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

Kurumsal Őifreleme Sertifikası akıllı karta yüklenecekse, sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediđi odalarda, güvenli yazılım ve/veya donanım kullanılarak üretilir.

Kurumsal Őifreleme Sertifikası HSM'ye yüklenecekse, HSM Cihaz Sorumlusu gözetiminde Kamu SM yetkili personeli tarafından, HSM yükleme bilgi formu dokümanında belirtilen Őekilde güvenli yazılım kullanılarak üretilir.

Anahtar çiftleri güvenli anahtar üretimi için gereken testlerden geçmiŐ, güvenilir programlar kullanılarak üretilir. Anahtar çifti üretmek için güvenilirliđi dünyaca kabul görmüŐ algoritmalar kullanılır. Sertifika sahibine ait özel anahtarın yedeđi alınmaz, bir kopyası hiçbir Őekilde sistemde tutulmaz. Sertifika sahibine ait özel anahtarın saklandıđı akıllı kart veya HSM Bölüm 6.2.1'de belirtilen güvenlik standartlarına uyar.

6.1.2. Sertifika Sahibine Özel Anahtarın UlaŐtırılması

Sertifika sahiplerine ait anahtar çiftlerinin Kamu SM tarafından oluŐturulmasına müteakip, özel anahtar, sertifikayla birlikte akıllı kart veya HSM'ye yüklenir. Akıllı kart, imza karŐılıđı ve resmi kimlik kontrolü yapılarak sahibine teslim edilir. HSM'ye özel anahtar ve sertifika yükleme iŐlemi, HSM Cihaz Sorumlusu gözetiminde gerçekteŐirilir ve iŐlem sonrası Kurulum Tutanađı doldurularak imzalanır.

Akıllı karta eriŐim verisi web üzerinden teslim edilir. Web üzerinden teslim edilen veriler için güvenli bađlantı protokolleri (HTTPS) kullanılmaktadır. Sertifika sorumlusunun/sorumlularının kimlik kontrolü için, T.C. kimlik numarası ve mobil telefona gönderilen SMS onay mesajı kullanılmaktadır. Bu Őekilde gerçekteŐirilen kimlik dođrulaması sonrasında sertifika sahibi akıllı kart eriŐim verisine eriŐir. HSM'ye eriŐim verisinden Kamu SM sorumlu deđildir, kurum inisiyatifindedir.

6.1.3. Elektronik Sertifika Hizmet Saęlayıcısı'na Aık Anahtarın Ulaőtırılması

Kurumsal Őifreleme Sertifikası HSM'ye yklenecekse, imza doęrulama verisini ieren PKCS#10 formatında sertifika imzalama isteęi, Kamu SM yetkili personeli tarafından kurumsal e-posta aracılıęıyla Kamu SM'ye parola korumalı ZIP dosyası ierisinde ulaőtırılır.

Kurumsal Őifreleme Sertifikası akıllı karta yklenecekse, Kurumsal Őifreleme Sertifikaları anahtar iftleri Kamu SM tarafından retildięi iin aık anahtarın Kamu SM'ye ulaőtırılması sz konusu deęildir.

6.1.4. Elektronik Sertifika Hizmet Saęlayıcısı Sertifikalarına Eriőtme Saęlanması

Kamu SM'ye ait Kk SHS ve Kurumsal Őifreleme SHS sertifikaları internet ortamında tarafların eriőtme hazırlanır. Sertifikanın yayımlandıęı ortamın izinsiz deęiőtirmeye ve silinmeye karőt gvenlięi saęlanır.

Kk SHS ve Kurumsal Őifreleme SHS sertifikaları, sertifikaların zet deęeri ve zet algoritması Kamu SM resmi web sitesi Bilgi Deposu sayfası zerinden yayımlanır.

6.1.5. Anahtar Uzunlukları

Kamu SM Kk SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

Kurumlara ait Kurumsal Őifreleme Sertifikalarını imzalayan Kurumsal Őifreleme SHS'ye ait ECDSA anahtar boyu en az 384-bittir.

İSDUP Yanıtlayıcı'dan duyurulan iptal durum kayıtlarını imzalamak iin kullanılan RSA anahtar boyu en az 2048-bittir.

Kamu SM tarafından retilen Kurumsal Őifreleme Sertifikaları, RSA anahtar boyu en az 2048-bittir.

6.1.6. Anahtar retim Parametreleri ve Kalitesinin Kontrol

Kamu SM tarafından anahtar retiminde Teblię'de belirtilen kriterlere uygun algoritmalar kullanılmaktadır. Algoritmaların gerekleőtirmesinde kullanılan yntemler gerekli gvenlik kriterlerini saęlar.

6.1.7. Anahtar Kullanım Amaları

Kamu SM tarafından oluőturulan anahtarların hangi amalar iin kullanılabilereceęi sertifikadaki "Anahtar Kullanımı" ve "Geniőtletilmiőt Anahtar Kullanımı" uzantısı ierisinde belirtilir.

Kamu SM kk anahtarı, alt kk sertifikasını ve SİL'i imzalamak iin kullanılır. Kamu SM Kurumsal Őifreleme Sertifikalarının imzalanmasında kullanılan sertifika zinciri Ek-A'da detaylı olarak bulunmaktadır. İSDUP yanıtlarının imzalanmasında alt kk ve kk tarafından yetkilendirilmiőt İSDUP sertifikası kullanılır.

6.2. zel Anahtarın Korunması

6.2.1. Kriptografik Modl Standartları

Kamu SM'ye ait imza oluőturma verisi gvenli yazılım ve/veya donanım kullanılarak retilir, gvenli kriptografik modl iinde saklanır ve geerli olduęu sre boyunca bu modl dıőtına ıkılmaz.

Kriptografik modl aőtayıda belirlenen gvenlik iőtlevlerine sahiptir:

- İmza oluőturma verisinin geerlilik sresi boyunca gizlilik ve btnlęn saęlar.
- Modle eriőtme kimlik belirleme ve doęrulama iőtlevlerini yerine getirir.

- EriŐim yetkisi birden fazla kiŐinin kontrolünde olacak Őekilde tanımlanabilir.
- Sistem kullanıcılarına tanımlanan roller dođrultusunda, verdiđi hizmetlere eriŐimi sınırlar.
- Düzgün çalıŐtıđı test edilebilir, test sırasında hata oluŐtuđunda güvenli duruma geçer.
- Modüle izinsiz eriŐim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıŐtır.
- Yetkisiz eriŐime teŐebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluŐturma verisinin yedeđinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin özel anahtarının içinde bulunduđu akıllı kart veya HSM cihazı, özel anahtarın donanım dıŐına çıkmasını engelleyen ve donanıma eriŐimi parola ile sađlayan teknik özelliklere sahiptir.
- Kriptografik modül ve sertifika sahibine ait akıllı kart veya HSM cihazı, Tebliđ'de belirtilen güvenlik standartlarını sađlar.

6.2.2. Özel Anahtara Birden Fazla KiŐi Kontrolünde EriŐim

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

6.2.3. Özel Anahtarın Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıŐtır.

6.2.4. Özel Anahtarın Yedeklenmesi

Kamu SM'ye ait imza oluŐturma verisinin yedeđinin alınması birden fazla yetkili personel tarafından yapılır. Yedekleme iŐlemi hazırda kullanılmakta olan imza oluŐturma verisi için sađlanan güvenlik ile eŐdeđer güvenlik önlemleri altında yapılır. Yedeklenen imza oluŐturma verisi yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. Güvenli donanım cihazı hazırda kullanılmakta olan imza oluŐturma verisinin bulunduđu ortam ile aynı güvenlik Őartlarına sahip ortamda saklanır.

Sertifika sahiplerine ait özel anahtarlar Kamu SM tarafından yedeklenmez.

6.2.5. Özel Anahtarın ArŐivlenmesi

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

6.2.6. Özel Anahtarın Kriptografik Modüle Yüklenmesi

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

Sertifika sahiplerine ait özel anahtarlar, sadece yetkili personelin kontrolünde akıllı kart veya HSM cihazına Őifrelenerek 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 oluŐturma verileri, yetkisiz kiŐilerin eriŐimine kapalı, fiziksel ve elektronik olarak güvenli kriptografik donanım cihazı içinde tutulur. İmza oluŐturma verisinin yedekleme amacı haricinde cihaz dıŐına çıkması engellenmiŐtir. İmza oluŐturma verisi kriptografik modül içinde güvenli algoritma ve yöntemlerle Őifreli 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 Eriřim

Kamu SM'nin imza oluřturma verisine eriřim birden fazla yetkili personelin ortak denetimi altındadır. İmza oluřturma verisinin bulunduđu odaya giriř için, tanımlanan yetkililerin aynı anda hazır bulunması ve elektronik olarak kimliklerinin ve yetkilerinin dođrulanması gerekir. Yeterli sayıda yetkili personelin hazır bulunmadığı ve kimliklerinin dođrulanamadığı durumlarda imza oluřturma verisinin bulunduđu odaya eriřim sađlanamaz.

İmza oluřturma verisi kriptografik modül içinde Őifreli durumdayken eriřime kapalıdır. Eriřime açılması için eriřimi sađlayan verinin modüle sunulması gerekir. İmza oluřturma verisinin eriřime açılması ve kullanılabilir duruma getirilmesi birden fazla yetkili personelin ortak denetimi altındadır.

Sertifika sahibine ait özel anahtar, akıllı kart veya HSM cihazı içinde sertifika sahibinin eriřim verisi ile korunmuř olarak saklanır. Aktivasyon, eriřim verisi ile sađlanır.

6.2.9. Özel Anahtara Eriřimin Kesilmesi

Kamu SM'nin imza oluřturma verisi imzalama için kullanıldıktan sonra oturum kapandıđında veriye eriřim otomatik olarak kesilir ve bir dahaki kullanımına kadar Őifrelenerek eriřime kapalı tutulur. Eriřimin yeniden sađlanabilmesi için Bölüm 6.2.8'de belirtilen yöntemin yeniden iřletilmesi gerekir.

Sertifika sahibinin kullandıđı güvenli donanım araçları, özel anahtarı kullanan oturumun kapanmasından sonra veriye eriřimi kesecek biçimde çalıřır. Eriřimin yeniden sađlanabilmesi için sertifika sahibinin eriřim verisini yeniden girmesi gerekir. Eriřim verisinin art arda 3 (üç) defa yanlış girilmesi durumunda güvenli donanım aracı kilitletir ve araca eriřim sađlanamaz.

6.2.10. Özel Anahtarın Yok Edilmesi

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

Sertifika sahiplerine ait özel anahtarlar, kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sahibi tarafından akıllı kart veya HSM cihazında yer alan imza oluřturma verisi güvenli Őekilde silinmelidir. Bu iřlemin yapılmasından sertifika sahibi sorumludur.

6.2.11. Kriptografik Modülün Deđerlendirilmesi

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

6.3. Anahtar Çifti Yönetimiyle İlgili Diđer Konular

6.3.1. Açık Anahtarın Arřivlenmesi

Kamu SM'ye ve sertifika sahibine ait açık anahtarlar, sertifikalar içinde tutulur ve Kurumsal Őifreleme Sertifikaları kullanım sürelerinin dolmasından itibaren 20 (yirmi) yıl boyunca arřivlenir. Kurumsal Őifreleme Sertifikalarının arřivleri yetkisiz kişilerce tahrifatına ve silinmesine karřı gerekli önlemlerin alındığı ortamlarda tutulur.

6.3.2. Özel ve Açık Anahtarların Kullanım Süreleri

Özel anahtarın kullanım süresi, Kurumsal Őifreleme Sertifikasının içeriğinde belirtilen kullanım süresi kadardır. Kurumsal Őifreleme Sertifikasının kullanım süresinin dolmasıyla ya da Kurumsal Őifreleme 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. Kamu SM'ye ait 384 bitlik ECDSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri en fazla 1 (bir) yıl için kullanılır. Üretilen Kurumsal Őifreleme Sertifikalarının son kullanma tarihi, Kurumsal Őifreleme SHS Sertifikasının son kullanma tarihini aşamaz.

6.4. Aktivasyon Verileri

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

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

6.4.1. Aktivasyon Verilerinin Oluşturulması

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

6.4.2. Aktivasyon Verilerinin Korunması

Kamu SM sistemi içinde kullanılan aktivasyon verileri yalnızca yetkili personeller tarafından bilinir.

Sertifika sahibi kuruma ait erişim parolaları, iki kademeli kimlik doğrulama ile erişilen web sayfası üzerinden sahibi tarafından belirlenir.

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

6.4.3. Erişim Denetim Verileri ile İlgili Diğer Konular

Düzenlenmesine gerek duyulmamıştır.

6.5. Bilgisayar Güvenliđi Kontrolleri

6.5.1. Bilgisayar Güvenliđi ile İlgili Teknik Gereklere

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 kaçađa karşı korunması ve işletimin sürekliliğinin sağlanması için gerekli güvenlik sağlanır. Her kurulan yazılımın yedek kopyası yaratılır ve sistemin güvenliđi 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 güvenliđi prosedürü yönergesine göre kontrol edilir.

6.5.2. Bilgisayar Sisteminin Saęladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

Sistem geliştirilirken genel anlamda yapılan denetimler aŐağıda 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 aęa 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 saęlar.
- 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 aę 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 Kontrolleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Aę Güvenlięi Kontrolleri

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

Sunucular üzerine ađ ve sistem yönetimi ve güvenliđi ajanları kurulmuŐtur. 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 çalıŐması için önem arz eden kaynaklar için eşik deđerler belirlenir ve bu eşik deđerlerin aŐılması durumunda sistem yöneticisi otomatik olarak uyarılır. Ađ ve sistem yönetimi ve güvenliđi altyapısı çektiiđi 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, diđer iletişim kanallarından mantıksal olarak farklı olan güvenilir iletişim kanalları kurulur.

Yüksek güvenlik gerektiren işlemlerin yapıldıđı sistemler (kök ve alt kök sunucuları gibi) için farklı ađ segmentleri oluşturulmuŐtur. Kritik işlemlerin yapıldıđı sistemler ađa bađlı deđildir. Canlı ortam servis ve sistemleri, geliştirme ve test ortamlarından ayrılmıŐtır. 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 geliŐtiricileri gibi farklı çalıŐan gruplarına ait farklı amaca hizmet eden ađlar da birbirinden ayrılmıŐtır. Sistemlerdeki ayrıcalıklı erişim hesaplarına yetkiler, güvenlik ekibince kontrollü olarak verilir ve kayıtlar üzerinden izlenir. Farklı bölgelere olan iletişim ve erişim engellendiđi gibi gerekli olmayan bađlantı ve hizmetler de ađ güvenliđi açısından devre dıŐı bırakılır.

Güvenlik politikası yönetim uygulamaları farklı amaçlarda kullanılmaz. Kök ve alt kök üzerinde bulunan gereksiz hesaplar, uygulamalar, hizmetler, port ve protokoller sıkılaŐtırma prosedürlerine göre kaldırılır ya da devre dıŐı bırakılır. Ađ ve sistem güvenliđine 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 devamlılıđı için Kamu SM ana merkez ve felaket kurtarma merkezinin dıŐ ađ bađlantı hizmetlerini yedekli olarak kurgulamıŐtır.

Sistemler üzerinde periyodik olarak zafiyet taramaları ve yılda en az bir kez penetrasyon testi yapılır. Penetrasyon testini yapan kiŐi veya kurum; test metot ve araçlarını, testleri yapan kiŐilerin yetkinliklerini içeren raporlar hazırlar. Bu raporlar Kamu SM tarafından saklanır. Sistemlerin belirlenen kural setlerine uygunluđu düzenli olarak gözden geçirilir.

6.8. Zaman Damgası

Kamu SM sistemi içinde kullanılan zaman damgası Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İliŐkin Tebliđ'de belirtilen Őartlara uyarak gerekli kesinlik ve bütünlük Őartlarını sađlar.

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 verilen Kurumsal Őifreleme Sertifikalarının içeriđi 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 verilen Kurumsal Őifreleme Sertifikaları X.509 V.3 formatında tanımlanan sertifikanın seri numarası, geerlilik tarihi, ilgili aık anahtar, sertifika sahibi kurumun adı ve DETSİS 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 ierir. Kurumsal Őifreleme Sertifikasının ieriğinde bulunan sertifika uzantıları sertifikanın kullanılacağı uygulamanın gereklerine baėlı olarak belirlenir.

Tablo 1'de Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikalarında asgari düzeyde bulunması gereken uzantılar tanımlanmıştır.

Tablo 1 Kurumsal Őifreleme Sertifika Uzantıları

| Sertifika Uzantısı | Kritik Uzantı | Aıklama |
|--|---------------|--|
| Temel Kısıtlar ¹ | HAYIR | Sertifikanın son kullanıcı sertifikası olduėu, ESHS sertifikası amacıyla kullanılamayacağı belirtilir. |
| Yetkili Anahtar Tanımlayıcısı ² | HAYIR | Kamu SM'ye ait Kurumsal Őifreleme SHS aık anahtarının SHA-1 özet ıktısından oluşur. |
| Sertifika Anahtar Tanımlayıcısı ³ | HAYIR | Sertifikanın ieriğindeki "subjectPublicKey" alanının "BIT STRING" olarak deėerinin SHA-1 özet ıktısından oluşur. |
| Anahtar Kullanımı ⁴ | EVET | Anahtarların sadece Őifreleme amaçlı kullanıldığının ifade edilmesi için "keyEncipherment" [anahtar Őifreleme] alanı seçilmiştir. |
| SİL Daėıtım Noktaları ⁵ | HAYIR | http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crl |
| Yetkili Bilgi Eriřimi ⁶ | HAYIR | http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt http://ksifrelemeocspv1.kamusm.gov.tr/ |
| Sertifika İlkeleri ⁷ | HAYIR | Kamu SM Sİ dokümanına ait nesne tanımlama numarası (2.16.792.1.2.1.1.5.7.1.11) ile SUE dokümanının bulunduğu |

¹ BasicConstraints

² AuthorityKeyIdentifier

³ SubjectKeyIdentifier

⁴ KeyUsage

⁵ CRLDistributionPoints

⁶ AuthorityInformationAccess

⁷ CertificatePolicies

| | | |
|--|-------|--|
| | | http://depo.kamusm.gov.tr/ilke internet adresini ve BTK tarafından oluşturulan Kurumsal Őifreleme Sertifikası ibaresine ait metni içerir. |
| Geniřletilmiş Anahtar Kullanımı ⁸ | HAYIR | Kurumsal Őifreleme Sertifikası nesne tanımlama numarasını (2.16.792.1.2.1.1.5.7.51.1) içerir. |

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 Kurumsal Őifreleme 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 Kurumsal Őifreleme Sertifikalarındaki isim alanı "ITU X.500 Distinguished Name [Ayrırt edici İsim]" biçimine uygundur.

7.1.5. İsim Kısıtları

Bölüm 3.1'de belirtilmiştir.

Tablo 2'de Kurumsal Őifreleme Sertifikası içinde yer alan isim alanları ve bu alanlar içine yazılacak bilgiler belirtilmiştir.

Tablo 2 Kurumsal Őifreleme Sertifika İsim Alanı Bilgileri

| Alan Adı | Kurumsal Őifreleme Sertifika İçeriđi |
|----------------------|--------------------------------------|
| CN ⁹ | Kurum DETSİS adı |
| Serial ¹⁰ | Kurum DETSİS numarası |
| C ¹¹ | TR |

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Bađlı olunan Kamu SM Sİ dokümanına ait nesne tanımlama numarası: 2.16.792.1.2.1.1.5.7.1.11

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

⁸ ExtendedKeyUsage

⁹ CN: Common Name [Genel isim]

¹⁰ Serial: Serial Number [Seri Numarası]

¹¹ C: Country [Ülke]

7.1.8. İlke Niteleyiciler

“Sertifika İlkeleri Uzantısı” Kurumsal Őifreleme Sertifikalarının üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ ve Kamu SM SUE olduğuna işaret eder. Kurumsal Őifreleme Sertifikalarının üretim ve yönetiminde takip edilen kurallara işaret eden Sİ dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikasının “Sertifika İlkeleri Uzantısı¹²”nın içinde yer alır. “Sertifika İlkeleri Uzantısı”nın içinde “İlke Niteleyici¹³” 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 Kurumsal Őifreleme Sertifikalarını kullanarak işlem yapar.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

- SİL’i oluşturan Kamu SM’ye ait isim bilgileri
- SİL imzalamak için kullanılan algoritmalara ait nesne tanımlama numarası (Kamu SM yayımladığı SİL’i imzalamak için SHA-384 özet algoritması ile ECDSA açık anahtarlı imzalama algoritmasını kullanır.)
- SİL’in yayımlanma tarihi
- SİL numarası
- Bir sonraki SİL yayımlanması için son tarih
- İptal edilen Kurumsal Őifreleme Sertifikaları ile ilgili aşağıdaki bilgiler:
 - Sertifikanın seri numarası
 - Sertifikanın iptal tarihi
 - Sertifikanın neden iptal edildiği bilgisi (opsiyonel)
- Kamu SM tarafından oluşturulan elektronik imza
- SİL imzasını doğrulamak için kullanılan Kamu SM’ye ait sertifikanın “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.

¹² Certificate Policies

¹³ Policy Identifier

7.3.2. ŐİSDUP Uzantıları

ŐİSDUP sorguları aŐağıdaki bilgileri iermelidir:

- Protokol versiyonu
- Hedef sertifika belirteci (kullanılan zetleme algoritması, sertifikayı veren ESHS'nin DN zeti, sertifikayı veren ESHS'nin imza doęrulama verisi zeti, sertifika seri numarası)

ŐİSDUP yanıtları aŐağıdaki bilgileri iermektedir:

- Versiyon bilgisi
- Yanıtlayıcının adı
- Her bir sertifika iin cevap bilgisi (sertifika belirteci (sertifika seri numarası), sertifika durumu, cevap geerlilik sresi)
- Kullanılan imza algoritmasının nesne tanımlama numarası
- ŐİSDUP Yanıtlayıcı imzası

Btn geerli ŐİSDUP cevapları ŐİSDUP Yanıtlayıcı tarafından imzalanır. Geersiz ŐİSDUP sorguları iin dnen hata mesajları imzalanmaz.

evrim İi Sertifika Durum Protokol RFC 6960'ta tarif edilen "ŐİSDUP" formatını destekler. ŐİSDUP Yanıtlayıcı'dan alınan cevaplar aŐağıdaki Őekilde deęerlendirilir:

Good [iyi]: Sertifika geerli konumdadır.

Bad [kt]: Sertifika iptal edilmiŐtir (askı durumu da dahil).

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

RFC 6960, ŐİSDUP sorguları ve yanıtları ierisinde bazı uzantıların kullanımına imkan verir. Tekrarlama (replay) saldırılarını nlemek iin sorgu ve yanıtı birbirine baęlayan "nonce" uzantısı bunlardan biridir. Kamu SM ŐİSDUP Yanıtlayıcı, "nonce" uzantısını desteklemektedir. RFC 6960'da belirtilen dięer uzantılar ŐİSDUP yanıt formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

Kamu SM, mevzuat gereęi Bilgi Teknolojileri Kurumu (BTK) tarafından incelenir/denetlenir.

Kamu SM ek olarak, ISO/IEC 27001 Bilgi Gvenlięi Ynetim Sistemi (BGYS) standardına uygun olarak hizmet verir ve standart gereęi dzenli olarak i ve dıŐ denetimlere tabi tutulur. Kamu SM i iŐleyiŐini denetlemek iin ayrıca i denetimler gerekleŐtirilir.

8.1. Uygunluk Denetiminin Sıklıęı

BTK, gerekli grdę durumlarda re'sen denetim yapabilir.

Kamu SM, ISO/IEC 27001 Bilgi Gvenlięi Ynetim Sistemi (BGYS) standardı gereęince yılda bir defa uygunluk denetimi geirir. Her  yılda bir sertifika yenilenir.

İ denetim, yılda en az 1 (bir) defa olmak zere gerekleŐtirilir.

8.2. Denetinin Nitelikleri

Kamu SM faaliyetlerinin denetimi, kanunla yetkilendirilmiŐ olan BTK tarafından gerekleŐtirilir.

ISO/IEC 27001 BGYS'nin denetimi akredite edilmiŐ kuruluşlarca gerekleŐtirilir.

İç denetim, Kamu SM sertifika süreçlerini bilen ve denetim konusunda tecrübeli Kamu SM personeli tarafından gerçekleştirilir.

8.3. Denetçinin Denetlenen Tarafı Olan İlişkisi

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

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

İç denetim, Sİ dokümanının gereklerini iyi anlayan ve uygunluk denetimi konusunda tecrübeli ESHS personeli tarafından gerçekleştirilir. İç denetim için seçilen denetçiler denetlenecek birimden seçilmez.

8.4. Denetimin Kapsamı

ESHS'lerin denetim kapsamı BTK tarafından belirlenir. ISO/IEC 27001 BGYS denetiminin kapsamı BGYS standardına uygun şekilde bağımsız kurum denetçisi tarafından belirlenir.

Kamu SM iç denetimlerinde, Sİ ve SUE dokümanına uygunluk denetlenir. İç denetim kapsamı denetimi gerçekleştirecek Kamu SM personeli 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 Kurumsal Şifreleme 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 deđiřmesi ya da Kurumsal Şifreleme Sertifikasının hatalı üretilmesi gibi sertifika sahibi kurumun kusurunun bulunmadığı durumların sonucunda Kurumsal Şifreleme Sertifikalarının Kamu SM tarafından iptal edilmesi ve güncellenmesi halinde, hiçbir ücret talep edilmez.

9.1.2. Sertifika EriŐim Ücreti

Kamu SM, kendisine ait sertifikaları resmi web sitesinde ücretsiz olarak yayımlar. Kamu SM tarafından üretilen Kurumsal Őifreleme Sertifikaları DETSİS'e yüklenir.

9.1.3. İptal Durum Kaydına EriŐim 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. Diđer 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. Kurumsal Őifreleme Sertifikaları ve güvenli donanım araçları için ödenecek bedelin miktarı ile ilgili bilgilendirme Kamu SM tarafından gönderilen teklif mektuplarında veya Kamu SM web sitesinde bildirilir. Ödemenin usulüne uygun biçimde yapılmaması durumunda Kurumsal Őifreleme Sertifikası üretimi yapılmayabilir veya mevcut sertifika kullanım dışı bırakılabilir.

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 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

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

9.2.2. Diđer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM, yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla, ürettiği Kurumsal Őifreleme Sertifikalarını 15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu gereğince mali sorumluluk sigortası ile sigortalar.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

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

9.3.3. Gizli Bilginin Korunma Sorumluluđu

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

9.4. Kişisel Bilginin Gizliliđi

9.4.1. Gizlilik Planı

Kamu SM verdiđi hizmetlerde sertifika sahiplerinin ve diđer paydaşların kişisel verilerinin gizliliđini ilgili mevzuat ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamındaki mer'î mevzuata uygun olarak sağlar.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Kişisel bilgi, sertifika sahibi kurumun ve yetkilendirdiđi Kurumsal Şifreleme Sertifikası Sorumlusu/Sorumluları ile HSM Cihaz Sorumlusunun, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiđi bilgiler ile adres ve telefon numarası gibi erişim bilgilerini kapsar. Kamu SM veya sertifika sahibi kurum tarafından atanan parolalar, numara, sembol gibi diđer tanımlayıcıyı bilgiler de kişisel bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kurumsal Şifreleme Sertifikası içeriğinde bulunan bilgiler, aksi taraflarca belirtilmediđi sürece gizli deđildir.

9.4.4. Gizli Bilginin Korunma Sorumluluđu

Kamu SM, sertifika talep eden kurumdan Kurumsal Şifreleme Sertifikası vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiđi kişisel bilgileri sertifika hizmeti vermek dışında başka amaçlar için kullanmaz, sertifika sahibi kurumun izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceđi ortamlarda bulundurmaz.

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

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

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM elde ettiđi kişisel bilgileri kişilerin yazılı rızası ile izin almak şartıyla yapılacak iş geređi 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. Diđer BaŐlıklar

Düzenlenmesine gerek duyulmamıŐtır.

9.5. Telif Hakları

Kamu SM tarafından üretilen tüm Kurumsal Őifreleme Sertifikaları ve dokümanlar ile bu SUE dokümanına bađlı olarak geliştirilen tüm bilgilerin fikri mülkiyet hakları Kamu SM'ye aittir.

9.6. Temsil Hakkı ve Yükümlölükler

Kamu SM tarafından verilen sertifika hizmetlerinde sistem bileŐenleri olarak tanımlanan Kamu SM, sertifika sahipleri ve üçüncü kişiler ilgili mevzuatlarda belirtilen şekilde üzerlerine düşen yükümlölükleri sađlar.

Kamu SM, sertifika sahibi kamu kurum veya kuruluşları ile üçüncü kişiler, yasa ve yönetmeliklerde belirtilmediđi halde imzalanmıŐ olan başvuru formu ve taahhütnamelerde yer alan yükümlölüklerini de yerine getirirler.

Kamu SM'nin ESHS olarak işleyişinin güvenli olabilmesi için, sistem bileŐenlerinin yerine getirmesi gereken yükümlölükler aŐađıda belirtilmiŐtir.

9.6.1. Elektronik Sertifika Hizmet Sađlayıcısı Yükümlölükleri

ESHS olarak Kamu SM'nin yükümlölükleri aŐađıda belirtilmiŐtir:

- Hizmetin gerektirdiđi nitelikte personel istihdam etmek
- Belirlediđi ilke ve esaslara uygun olarak sertifika işlemlerini yürütmek
- Sİ ve SUE dokümanlarını herkesin erişimine açık bilgi deposundan yayımlamak
- Kök SHS ve Kurumsal Őifreleme SHS için anahtar çifti üretmek ve bu anahtar çiftleri için sertifikalar oluşturmak
- Kök SHS ve Kurumsal Őifreleme SHS sertifikalarını son kullanıcıların erişebileceđi ortamlarda yayımlamak
- Kurumsal Őifreleme Sertifikası verdiđi kurumların kimliđini DETSİS üzerinden güvenilir bir biçimde dođrulamak
- Kurumlardan gelen Kurumsal Őifreleme Sertifikası başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kurumların belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek
- Kurumsal Őifreleme Sertifikasının içeriđindeki bilgilerin dođruluđunu beyan edilen belgelere dayanarak sađlamak
- Gereklili başvuru şartlarını sađlamayan başvuru sahiplerine Kurumsal Őifreleme Sertifikası vermemek
- Kurumsal Őifreleme Sertifikası başvurularını deđerlendirerek, başvurunun sonucu hakkında kurumları ya da kurumların yetkilendirdikleri sorumlu kişileri bilgilendirmek
- Kurumsal Őifreleme Sertifikası başvurusu kabul edilmiŐ kurumlar için anahtar çifti ve Kurumsal Őifreleme Sertifikası üretmek
- Sertifika sahibi kuruma ait özel anahtarı oluşturduktan sonra özel anahtar ve üretiminde kullanılan gizli deđerşkenleri kendi sisteminden silmek, özel anahtarın kopyasını hiçbir şekilde tutmamak
- Sertifika sahibine akıllı kart temin etmesi durumunda, bu aracın güvenli olmasını sađlamak

- Üretilen Kurumsal Őifreleme Sertifikaları özel anahtarlarını Sİ ve SUE'de belirtilen Őekilde güvenli olarak sertifika sahiplerine teslim etmek
- Sertifika sahiplerinin Kurumsal Őifreleme Sertifikalarını DETSİS'e yüklemek
- Kurumsal Őifreleme Sertifikalarının kullanım Őartlarını belirleyen sertifika profillerini oluŐturmak
- Kurumsal Őifreleme Sertifika başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli iŐlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıya alma başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli askıya alma iŐlemlerini yapmak
- Kurumsal Őifreleme Sertifikası askıdan indirme iŐlemlerini Sİ ve SUE'de belirtilen Őekilde yapmak
- Kurumsal Őifreleme Sertifikası iptal başvurularını Sİ ve SUE'de belirtilen Őekilde kabul etmek ve deęerlendirerek gerekli iptal iŐlemlerini zamanında yapmak
- Yayımlanan Sİ ve SUE dokümanları ile taahhünelere uygun olmayan Kurumsal Őifreleme Sertifikası kullanımlarının tespit edilmesi durumunda ilgili Kurumsal Őifreleme Sertifikasını iptal etmek
- İptal edilmiŐ Kurumsal Őifreleme Sertifikası bilgilerini sertifika iptal listelerinde yayımlamak veya ÇİSDUP Yanıtlayıcı aracılıęıyla duyurmak
- Kurumsal Őifreleme Sertifikalarının ve iptal durum kayıtlarının bütünlüğünü ve erişilebilirliğini saęlamak için her türlü tedbiri almak
- Sertifika sahiplerine ait elektronik veya kaęıt ortamda tutulan bilgilerin gizlilięinin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kiŐilere mahkeme kararı olmaksızın vermemek
- Kurumsal Őifreleme Sertifikası üretim, yönetim ve iptali ile ilgili yapılan tüm iŐlemlerin kaydını tutmak
- İŐleyiŐ sırasında kullanılan tüm kaęıt ve elektronik kayıtları ilgili Sİ ve SUE'de belirtilen süreler boyunca güvenli olarak saklamak

9.6.2. Kayıt Birimi Yükümlülükleri

Kayıt biriminin sorumlulukları Őunlardır:

- Kurumsal Őifreleme Sertifika başvurularını almak,
- Kurum kimlięini ve kurum adına iŐlem yapan yetkili kimlięini bu dokümanda belirtilen yöntemlerle gerekli belgelere dayanarak doęrulamak,
- Başvuruları deęerlendirerek, başvurunun sonucu hakkında ilgili kiŐileri bilgilendirmek,
- Sertifika iptal başvurularını almak,
- Doęrulanan sertifika iptal başvurularını Kamu SM'nin ilgili birimlerine iletme,
- İptal edilen sertifikalar hakkında sahiplerini bilgilendirmek.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sahibinin yükümlülükleri aŐaęıda belirtilmiŐtir:

- Kurumsal Őifreleme Sertifikası başvuru, askıya alma, iptal ve dięer iŐlemleri, ilgili Sİ ve SUE'de belirtildięi Őekilde, detayları Kamu SM Kurumsal Őifreleme Sertifikası yönetim prosedürlerinde anlatılan usule uygun biçimde yerine getirmek

- Kurumsal Őifreleme Sertifikası baŐvurusu, yenileme ve iptal iŐlemleri sırasında dođru bilgi beyan etmek
- Kurum adına dūzenlenen Kurumsal Őifreleme Sertifikası ũretildiđinde sertifikadaki bilgilerin dođruluđunu kontrol etmek
- SUE Bōlüm 6.2.1’de belirtilen standartlara uygun akıllı kart veya HSM kullanmak
- Őzel anahtarın gūvenliđini sađlamak, kendisine ait Őzel anahtarın iinde bulunduđu akıllı kart veya HSM’in ve eriŐim verisinin gizliliđini korumak, bunları baŐkasına kullandırmamak ve bu konuda gerekli tedbirleri almak
- İnternet veya ađrı merkezi ũzerinden sertifika iŐlemlerini yapabilmesi iin kullandıđı parolalarının gizliliđini ve gūvenliđini sađlamak
- Őzel anahtarın iinde bulunduđu akıllı kart veya HSM’in kaybolması, alınması veya Őzel anahtarın gizliliđinin yitirildiđinden Őūphelenmesi durumunda Kurumsal Őifreleme Sertifikasının iptal edilmesi iin Bōlüm 3.4’te belirtilen kanallar ũzerinden baŐvurmak
- Akıllı kart veya HSM eriŐim verisini ve sertifika iŐlemlerinde kullandıđı diđer parolaları dūzenli olarak deđiŐtirmek
- Kurumsal Őifreleme Sertifikası ieriđinde bulunan bilgilerin deđiŐmesi durumunda derhal sertifikanın iptal edilmesi iin Kamu SM’ye baŐvurmak
- Kurumsal Őifreleme Sertifikası baŐvurusu sırasında ve sertifikanın geerlilik sūresi boyunca beyan ettiđi bilgilerde meydana gelen deđiŐiklikleri derhal Kamu SM’ye bildirmek
- İptal olmuŐ, kullanıma aılmamıŐ, askıya alınmıŐ veya geerlilik sūresi dolmuŐ Kurumsal Őifreleme Sertifikası ile iŐlem yapmamak
- Őzel anahtarını imzalama amacıyla kullanmamak

Sertifika sahibi kurum, Kamu SM Kurumsal Őifreleme Sertifikası Sİ ve SUE dokūmanlarında belirtilen Őartları okuduđunu, baŐvuru sūreci ve sertifika geerliliđi boyunca taahhūname, ilgili mevzuatlar ile Sİ ve SUE dokūmanında belirtilen Őartlara uygun olarak hareket edeceđini kabul ve taahhū eder. Yūkūmlūluklerin ihlali nedeniyle ũūncū kiŐilerin/kurumun zarara uđraması halinde TŪBİTAK BİLGEM’in ũdemek zorunda olduđu tazminatlarla ilgili sertifika sahibine rūcu hakkı saklıdır.

9.6.4. ũūncū KiŐilerin Yūkūmlūlukleri

ũūncū kiŐiler, Kurumsal Őifreleme Sertifikasıyla iŐlem yapmadan ũnce sertifikanın aŐađıda belirtilen geerlilik kontrollerini yapmakla yūkūmlūdūr:

- Kurumsal Őifreleme Sertifikasının tanımlanan verilif amacına uygun olarak kullanıldıđını dođrulamak
- Kurumsal Őifreleme Sertifikasının kullanım sūresinin dolup dolmadıđını kontrol etmek
- Kurumsal Őifreleme Sertifikasının geerliliđini SİL veya İSDUP Yanıtlayıcı aracılıđıyla kontrol etmek
- SİL veya İSDUP Yanıtlayıcı’dan aldıđı iptal durum kaydının bütūnlūđünü Kamu SM’nin ilgili sertifikası iinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kurumsal Őifreleme Sertifikasının dođruluđunu Kurumsal Őifreleme SHS sertifikasının iinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kurumsal Őifreleme SHS sertifikasının dođruluđunu Kōk SHS sertifikasının iinde mevcut olan imza dođrulama verisini kullanarak dođrulamak
- Kōk SHS sertifikasının bütūnlūđünü sertifika ũzet deđerini kontrol etmek suretiyle dođrulamak

- Sertifika sahibinin Kurumsal Őifreleme Sertifikasının içindeki açık anahtarına karşılık gelen özel anahtara sahip olduğunu doğrulamak

9.6.5. Diđer Bileşenlerin Yükümlülükleri

9.6.5.1. Kurumun Yükümlülükleri

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

- Sertifika başvurusunu Kamu SM web sitesinde belirtilen yöntemleri kullanarak Kamu SM'ye iletmek ve Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularını görevlendirerek belirlenen sorumluları Kamu SM'ye bildirmek
- Sertifika sorumlusunun/sorumlularının görevi sonlandırıldığında ya da yeni bir sorumlu görevlendirildiğinde Kamu SM'ye Kamu SM web sitesinde yer alan sorumlu deęişikliği yönergesi kapsamında bildirmek
- Sertifika yönetim süreçleri ile ilgili taahhütnamelerdeki yükümlülükleri yerine getirmek

9.6.5.2. Kurum Sertifika Sorumlularının Yükümlülükleri

Kurum adına Kurumsal Őifreleme Sertifikası başvurusunda bulunan Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının yükümlülükleri aşağıda belirtilmiştir:

- Sertifika alınacak kuruma ait bilgileri tam ve doğru bir şekilde Kamu SM'ye iletmek
- Sertifika yönetim süreçleri ile ilgili işleri Kamu SM ile koordineli bir şekilde yürütmek
- Kamu SM'nin kendisine imzalattığı taahhütnamedeki yükümlülükleri yerine getirmek

Kurumsal Őifreleme Sertifikası Sorumlusu/Sorumlularının sertifika teslimatları ile ilgili yükümlülükleri taahhütnamelerde belirtilmiştir.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahipleri olan kamu kurum veya kuruluşları arasındaki yükümlülük, taahhütnamelerde belirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmeti alan tarafların sorumlulukları ilgili mevzuatta belirtilen şartlar ile sınırlıdır. Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ile ilgili sınırlamalar taahhütnamelerde belirlenir. Ayrıca sertifika mali sorumluluk sigortası genel şartları ile diđer düzenlemeler dikkate alınır.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Sertifika sahibi kurum, taahhütnamelere uygun olarak Kamu SM ile iş birliği içinde çalışır.

Sertifika sahibi kurumlar sertifika hizmetlerini aldıkları süre boyunca Sİ ve SUE dokümanları ile sertifika yönetim prosedürlerinde belirtilen şartları yerine getirmeyi kabul ederler.

Kamu SM sertifika hizmeti verdiği süre boyunca Sİ ve SUE dokümanları, sertifika yönetim prosedürleri, sertifika sahibine ilettiği taahhütnamelerdeki şartları yerine getirir.

9.10.1. AnlaŐma Suresi

Sertifika sahibi kurumun imzaladıđı taahhütnemelerin süresi sertifikanın geçerlilik süresi veya taahhütnamede belirtilmiŐse hizmetin alınma süresi kadardır. Ancak, sertifikanın iptal edilmesi durumunda taahhütnamenin süresi de sona erer.

9.10.2. AnlaŐmanın Sona Ermesi

Kamu SM, imzalanan taahhütnemeleri aŐađıdaki durumlarda sonlandırılabilir:

- Sertifika sahibi kurumun sertifikasını iptal etmesi
- Sertifikanın kullanım süresinin sona ermesi
- Sertifika sahibi kurumun imzalanan taahhütnemelere aykırı davranması durumunda Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Bölüm 5.7.3'te belirtilen güvenlik açığıının ortaya çıkması sebebiyle Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi
- Kamu SM Bölüm 5.8'de belirtildiđi biçimde sertifika hizmetlerini sonlandırırssa, Kamu SM'nin sertifika sahibi kuruma ait sertifikayı iptal etmesi

9.10.3. AnlaŐmanın Sona Ermesinin Etkileri

İmzalanan taahhütnemelerin sona ermesiyle sertifika sahibinin, taahhütname ile Sİ ve SUE dokümanlarında belirtilen şartları sađlamakla ilgili yükümlölükleri ortadan kalkar. Sertifika sahibi kurumun taahhütnemelerden, Sİ ve SUE dokümanlarından kaynaklanan yükümlölüklerini yerine getirmemesi durumunda, Kamu SM sertifikayı iptal eder. Sertifika sahibi kurumun taahhütnemeye uygun hareket etmemesinden dolayı uğrayacađı zararlardan Kamu SM sorumlu tutulamaz.

Taahhütnemeler sona erse bile Kamu SM, ürettiđi Kurumsal Őifreleme Sertifikaları ile ilgili mevzuatta belirtilen yükümlölükleri yerine getirmeye devam eder. Kamu SM, ürettiđi Kurumsal Őifreleme Sertifikalarının iptal durum kayıtlarına taraflarca eriŐimin sađlanması ile Bölüm 5.4 ve 5.5'te belirtilen kayıtların ve arŐivlerin saklanması ile ilgili hizmetleri sürdürür.

9.11. Sistem BileŐenleri ile HaberleŐme ve KiŐisel Bilgilendirme

Kamu SM, Kurumsal Őifreleme Sertifikaları baŐvuru, iptal ve yenileme taleplerinin sonuçları hakkında sertifika sahibi kurumu bilgilendirir. Bilgilendirmeler telefon veya kurumsal e-posta aracılıđıyla sađlanır. BaŐvuru Formu ve Taahhütnamede belirtilen sertifika sorumlularının kurumsal e-posta adresine, deđiŐmesi halinde yeni bildirdiđi kurumsal e-posta adresine yapılan bilgilendirmeler resmi bildirim olarak kabul edilir.

Sertifika yönetim iŐlemleri sırasında sertifika sorumluları veya sertifika sahibi kurumlarla yapılan haberleŐmenin hangi durumlarda, ne Őekilde yapılacađı Kamu SM'nin Kurumsal Őifreleme Sertifikası yönetim prosedürlerinde detaylı olarak belirtilir.

9.12. DeđiŐiklik Halleri

9.12.1. DeđiŐiklik Metotları

SUE dokümanı Kamu SM tarafından yazılmıŐtır. Bu SUE dokümanında yapılabilecek deđiŐiklikler ekleme ve deđiŐtirme Őeklinde olabileceđi gibi Kamu SM dokümanının tamamen yenilenmesine de karar verebilir. Bu SUE dokümanının herhangi bir kısmının yanlış ya da geçersiz olduđu ortaya çıksa bile SUE dokümanının diđer kısımları, SUE dokümanı güncellenene kadar geçerliliđini sürdürür.

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

SUE dokümanında yapılan deęişiklikler 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 Deęişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

Taraflar arasında çıkan tüm anlaşmazlıkların sulhen çözümü esastır. İhtilaf durumlarında ilgili mevzuata 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, ilgili mevzuata uygun olarak yazılmıştır.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

10. EK-A SERTİFİKA PROFİLLERİ

10.1. KAMU SM KURUMSAL ŐİFRELEME KÖK SERTİFİKASI

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

10.2. KAMU SM KURUMSAL ŐİFRELEME ALT KÖK SERTİFİKASI

| Alan | Deęer |
|-------------------------------|--|
| Sürüm | V3 |
| Seri Numarası | 00f4dfbe9d0289 |
| İmza Algoritması | SHA-384 ile ECDSA {1 2 840 10045 4 3 3} |
| Sertifika Vereni | CN = Kamu SM Kök Sertifika Hizmet Sağlayıcısı - Sürüm 6 OU = BİLGEM O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR |
| Geçerlilik Başlangıcı | 20 Kasım 2020 Cuma 15:56:15 |
| Geçerlilik Sonu | 6 Ağustos 2029 Pazartesi 19:25:08 |
| Konu | CN = Kurumsal Őifreleme Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR |
| Açık anahtar | 384 bit ECC {1 2 840 10045 2 1} ECDSA_P384 {1 3 132 0 34} |
| Uzantılar | Deęer |
| Yetkili Anahtar Tanımlayıcısı | Kritik=Hayır; Anahtar Kimliği= 30 cb d6 81 10 23 2c 9f 44 32 0f e0 ba 7b f1 89 c2 c0 39 da |
| Konu Anahtar Tanımlayıcısı | Kritik=Hayır; Anahtar Kimliği= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab |
| Anahtar Kullanımı | Kritik=Evet ; Sertifika İmzalama, SİL İmzalama |
| Temel Kısıtlar | Kritik=Evet ; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0 |

| | |
|-----------------------|---|
| Sertifika İlkeleri | <p>[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=CPS Niteleyicisi= http://depo.kamusm.gov.tr/ilke</p> <p>[1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliđi=Kullanıcı Uyarısı Niteleyicisi= Uyarı Metni=Bu sertifika ile ilgili sertifika ilke ve uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.</p> |
| SİL Dađıtım Noktaları | <p>[1]SİL Dađıtım Noktası Dađıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crl</p> |
| Yetkili Bilgi EriŐimi | <p>[1]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Sertifika Yetkilisi Yayımıcısı (1.3.6.1.5.5.7.48.2) Diđer Ad: URL=http://depo.kamusm.gov.tr/nes/kokshs.v6.crt</p> |

10.3. SON KULLANICI KURUMSAL ŐİFRELEME SERTİFİKA ŐABLONU

| Alan | Deđer |
|-----------------------|---|
| Sürüm | V3 |
| Seri Numarası | En fazla 64 bit rassal sayı içeren tam sayı |
| İmza Algoritması | SHA-384 ile ECDSA {1 2 840 10045 4 3 3} |
| Sertifikayı Veren | <p>CN = Kurumsal Őifreleme Sertifika Hizmet Sađlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi O = TÜBİTAK - BİLGEM L = Gebze - Kocaeli C = TR</p> |
| Geçerlilik BaŐlangıcı | Sertifika geçerlilik baŐlangıcı |
| Geçerlilik Sonu | Sertifika geçerlilik sonu |

| | |
|---------------------------------|--|
| Konu | CN = Kurum DETSİS adı Serial = Kurum DETSİS numarası C = TR |
| Açık anahtar | 2048 bit RSA {1 2 840 113549 1 1 1} |
| Uzantılar | Deęer |
| Yetkili Anahtar Tanımlayıcısı | Kritik=Hayır; Anahtar Kimlięi= ab 71 39 0b 21 74 35 cb 23 40 79 a7 3f d1 2c 21 73 94 a0 ab |
| Konu Anahtar Tanımlayıcısı | Kritik=Hayır; Anahtar Kimlięi= Sertifikanın içerięindeki "subjectPublicKey" alanının "BIT STRING" olarak deęerinin SHA-1 özet çıkıtısından oluşur. |
| Anahtar Kullanımı | Kritik=Evet ; Anahtar Őifreleme |
| Temel Kısıtlar | Kritik=Hayır; Konu Türü=Son Varlık; Yol Uzunluęu Kısıtlaması=Yok |
| Sertifika İlkeleri | [1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.1.11 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimlięi=CPS Niteleyicisi= http://depo.kamum.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimlięi=Kullanıcı Uyarısı Niteleyicisi= Uyarı Metni=Bu sertifika, 2017/21 sayılı Başbakanlık Genelgesi kapsamında belirtilen kurumsal Őifreleme sertifikasıdır. |
| Geniřletilmiş Anahtar Kullanımı | Kurumsal Őifreleme Sertifikası (2.16.792.1.2.1.1.5.7.51.1) |
| SİL Daęıtım Noktaları | [1]SİL Daęıtım Noktası Daęıtım Noktası Adı: Tam Ad: URL= http://depo.kamum.gov.tr/ksifreleme/ksifreleme.v1.crl |

| | |
|-----------------------|---|
| Yetkili Bilgi EriŐimi | <p>[1]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Sertifika Yetkilisi Yayımcısı (1.3.6.1.5.5.7.48.2) Diđer Ad: URL=http://depo.kamusm.gov.tr/ksifreleme/ksifreleme.v1.crt</p> <p>[2]Yetkili Bilgi EriŐimi EriŐim Yöntemi=Çevrimiçi Sertifika Durum Protokolü (1.3.6.1.5.5.7.48.1) Diđer Ad: URL=http://ksifrelemeocspv1.kamusm.gov.tr/</p> |
|-----------------------|---|