KAMU SM ELEKTRONİK MALİ MÜHÜR SERTİFİKA İLKELERİ VE UYGULAMA ESASLARI

Doküman Kodu	Yayın Numarası	Yayın Tarihi
YONG-001-011	**01**	**01.02.2010**

DEĞİŞİKLİK KAYITLARI

Yayın No	Yayın Nedeni	Yayın Tarihi
01	İlk yayın	01.02.2010

İÇİNDEKİLER

KAMU SM ELEKTRONİK MALİ MÜHÜR SERTİFİKA İLKELERİ VE UYGULAMA ESASLARI

1. Giriş

Bu doküman, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) Müdürlüğü tarafından oluşturulan Kamu Sertifikasyon Merkezi'nin (Kamu SM) Elektronik Mali Mühür sertifikası hizmeti verirken uyguladığı esasları tanımlayan Sertifika İlkeleri ve Sertifika Uygulama Esasları (Sİ/SUE) dokümanıdır.

Kamu SM'den Elektronik Mali Mühür sertifikası talebinde bulunanlar bu dokümanda belirtilen esaslar çerçevesinde sertifikayı kullanmayı kabul etmiş sayılır. Bu kapsamda oluşturulan sertifikalar 5070 sayılı Elektronik İmza Kanunu'nda sözü geçen nitelikli elektronik sertifika kapsamında değerlendirilmezler.

1.1. Genel Bakış

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

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

1.2. Doküman Adı ve Tanımı

Doküman Adı: Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Uygulama Esasları

Doküman Sürüm Numarası: 01

Yayın Tarihi: 01.02.2010

Nesne Tanımlama Numarası: 2.16.792.1.2.1.1.5.7.4.1

1.3. Sistem Bileşenleri

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı

Kamu SM, Elektronik Sertifika Hizmet Sağlayıcısı olarak Elektronik Mali Mühür Sertifikası hizmeti vermektedir. Bu amaçla aşağıdaki hizmetleri yerine getirir.

- Sertifikaların üretilmesi, imzalanması ve ilgili kişi yada kurumlara ulaştırılması
- Sertifikaların askıya alınması ya da iptal edilmesi

- Sertifika durum bilgilerinin Sertifika İptal Listesi (SIL) şeklinde ya da diğer yöntemlerle yayınlanması

1.3.2. Kayıt Birimleri

Düzenlenmesine gerek duyulmamıştır.

1.3.3. Sertifika Sahipleri

Kamu SM tarafından kendileri için sertifika oluşturulan ve sertifikalarını sertifika ilke ve uygulama esaslarına uygun olarak kullanmakla yükümlü olan tüzel kişilerdir.

1.3.4. Üçüncü Kişiler

Kamu SM tarafından oluşturulan sertifikaların içindeki kimlik bilgileri ve imza doğrulama verisi arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan gerçek yada tüzel kişilerdir. Üçüncü kişiler sertifikaları kullanmadan önce gerekli gördüğü geçerlilik kontrollerini yapar.

1.3.5. Diğer Bileşenler

Düzenlenmesine gerek duyulmamıştır.

1.4. Sertifika Kullanımı

1.4.1. Uygun Olan Sertifika Kullanımı

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

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

1.4.2. Sertifika Kullanımının Sınırları

Kamu SM tarafından oluşturulan MÜS ve GÜS Madde 1.4.1 de belirtilen amaçlar dışında kullanılamaz.

1.5. İlke ve Uygulama Esaslarının Yönetimi

1.5.1. Doküman Yönetimi

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

1.5.2. İletişim Bilgileri

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

Adres : TÜBİTAK UEKAE, PK. 74, 41470 Gebze-KOCAELİ
Tel : (262) 648 18 18
Faks : (262) 648 18 00
E Posta : bilgi@kamusm.gov.tr
URL : http://mm.kamusm.gov.tr

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

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

1.5.3. Sertifika Uygulama Esaslarının İlkelere Uygunluğunu Belirleyen Kişi

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

1.5.4. Sertifika Uygulama Esasları Onay Prosedürleri

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

1.6. Tanımlar ve Kısaltmalar

1.6.1. Tanımlar

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

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

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

Elektronik Mali Mühür Oluşturma Aracı: MÜS'ü, GÜS'üve elektronik mali mühür oluşturma verisini barındıran; elektronik mali mühür oluşturma ve doğrulama verisinin güvenliğini ve gizliliğini sağlayan (akıllı kart, USB çubuk, donanımsal güvenlik modülü (HSM) vb) donanım aracıdır.

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

Elektronik Sertifika(lar): Sertifika sahibinin, elektronik mali mühür doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır (MÜS ve GÜS).

Elektronik Mali Mühür Oluşturma Verisi (Gizli Anahtar): Sertifika sahibine ait olan, sertifika sahibi tarafından elektronik mali mühür oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik özel anahtarlar gibi verileri tanımlar.

Elektronik Mali Mühür Doğrulama Verisi (Açık Anahtar): Elektronik mali mührü doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri tanımlar. Elektronik mali mühür oluşturma verisi ile matematiksel olarak ilişkilendirilmiş bir veridir.

Güvenlik Hizmetleri Seritifikası: Elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin gizliliğinin sağlanması için kullanılacak elektronik sertifikadır.

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

Kamu Sertifikasyon Merkezi: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü bünyesinde, elektronik sertifika hizmeti sağlamak üzere oluşturulan birim.

Kurum Yetkilisi: Kurum tarafından belirlenen ve elektronik sertifikalar ile işlem yapma görevi verilen gerçek kişidir.

Mali Mühür Sertifikası: Elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması için kullanılacak elektronik sertifikadır.

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

Sertifika yenileme: Sertifika sahibi olarak sistemde geçerli kaydı olan ve değişik sebeplerden dolayı sertifikanın farklı bir anahtar çifti ile yeniden üretilmesi sürecidir.

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

Sertifika Sahibi: Adına MÜS ve GÜS üretilen tüzel kişidir.

Sertifika Sorumlusu: Elektronik sertifikalar ile işlem yapma görev ve sorumluluğu verilen gerçek kişidir.

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

1.6.2. Kısaltmalar

BS (British Standards): İngiliz Standartları

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesi

CWA (CEN Workshop Agreement): CEN Çalıştay Kararı

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

DSA (Digital Signature Algorithm): Sayısal İmza Algoritması

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi

ESHS: Elektronik Sertifika Hizmet Sağlayıcısı

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

ETSI TS (ETSI Technical Specification): ETSI Teknik Özellikleri

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

GİB: Gelir İdaresi Başkanlığı

GÜS: Güvenlik Hizmetleri Sertifikası

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliği

Kamu SM: Kamu Sertifikasyon Merkezi

LDAP (Lightweight Directory Access Protocol): Dizin Erişim Protokolü

MM ESHS: Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı

MÜS : Mali Mühür Sertifikası

PKI (Public Key Infrastructure): Açık Anahtarlı Altyapılar

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

SHA (Secure Hash Algorithm): Güvenli Özet Algoritması

Sİ: Sertifika İlkeleri

SİL: Sertifika İptal Listesi

SUE: Sertifika Uygulama Esasları

2. Yayımlama ve Bilgi Deposu

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

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

2.1. Bilgi Depoları

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

http://mm.kamusm.gov.tr/belgeler internet adresi üzerinden SUE ve Sİ dokümanları, Kamu SM'ye ait sertifikalar ve SİL'lere erişilmektedir.

ldap://dizinkurumsal.kamusm.gov.tr/ adresinden erişilebilen LDAP dizin sunucusu üzerinden SİL'lere erişim sağlanır.

http://cisdupmms1.kamusm.gov.tr/ adresinden servis veren ÇİSDUP Yanıtlayıcısı üzerinden sertifika iptal listelerine alternatif olarak sertifikaların en güncel haliyle geçerlilik durumunun kontrolü yapılabilmektedir.

2.2. Sertifika Hizmeti ile İlgili Bilgilerin Yayımlanması

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

- Kamu SM'ye ait KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 ve Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1 sertifikaları,
- Kamu SM'ye ait KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 ve Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1 sertifikasının özet değeri ile özet değerinin hesaplanmasında kullanılan özetleme algoritmasının hangisi olduğu bilgisi,
- Kamu SM Elektronik Mali Mühür Sİ ve SUE dokümanları,
- Taahhütnameler,
- Formlar,
- Sertifika iptal durum kayıtları.

2.3. Yayın Sıklığı ve Zamanı

Taahhütnameler, sertifika yönetim prosedürleri, SUE ve Sİ dokümanları içeriğinin değişmesi üzerine güncellenir. Güncellenen dokümanlar, güncelleme yapılmasını müteakip derhal yayımlanır.

Kamu SM'ye ait sertifikalar 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 değiştirilmeye karşı bütünlüğünü korumak,
- Bilgi deposunda tutulan bilgilerin doğruluğu ve güncelliğini sağlamak,
- Bilgi deposunu sürekli olarak katılımcıların erişimine açık tutmak,
- Bilgi deposunun kesintisiz olarak erişilebilirliğini sağlamak için gerekli önlemleri almak,
- Bilgi deposuna erişimi ücretsiz sağlamak.

3. Kimlik Belirleme ve Doğrulama

3.1. İsimlendirme

3.1.1. İsim Alanı Tipleri

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

3.1.2. Kimlik Bilgilerinin Teşhise Elverişli Olması

Sertifikalar üzerinde yer alan kimlik bilgileri tüzel kişileri tanımlayacak şekilde anlamlı olmalıdır (kurum ismi, ünvan, vb).

3.1.3. Sertifika Sahibinin Takma İsim veya Lakap Kullanması

Sertifika içeriğinde takma isim veya lakap kullanılmasına izin verilmez.

3.1.4. Farklı İsim Alanı Tiplerinin Yorumlanması

Sertifika içeriği nde ITU X.500 biçimi dışında isim alanı tipi kullanılmaz.

3.1.5. Kimlik Bilgilerinin Tekilliği

Kamu SM tarafından oluşturulan sertifikaların içeriğindeki kimlik bilgileri tüzel kişiler için ayırt edici niteliktedir.

3.1.6. Markanın Tanınması, Doğrulanması ve Rolü

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

3.2. İlk Kimlik Belirleme

Kamu SM, sertifika hizmetlerinden faydalanmak için ilk defa başvuruda bulunulduğunda, ilgili tüzel kişiliğin kimlik doğrulanabilmesi için aşağıda tanımlanan yöntemler uygulanır.

3.2.1. İmza Oluşturma Verisine Sahip Olmanın Kanıtlanması

MÜS ve GÜS için imza oluşturma ve doğrulama verileri Kamu SM tarafından oluşturulup sertifika sorumlusuna ulaştırılır. Bu durumda imza oluşturma verileri sertifika sorumlusuna güvenli donanım aracında elden teslimat yapılarak ulaştırılır.

3.2.2. Kurumsal Kimliğin Belirlenmesi

Ticaret sicil gazetesi kontrol edilerek belirlenir.

3.2.3. Kişisel Kimliğin Belirlenmesi

3.2.4. GIB tarafından bildirilen sertifika sorumlusu kurum adına yetkili kabul edilir. Herhangi bir ek doğrulama yapılmaz.Doğrulanmayan Sertifika Sahibi Bilgileri

Kamu SM tarafından oluşturulan MÜS ve GÜS, doğrulanmayan bilgiler içermez.

3.2.5. Yetkinin Doğrulanması

GIB tarafından bildirilen sertifika sorumlusu kurum adına yetkili kabul edilir. Herhangi bir ek doğrulama yapılmaz.

3.2.6. Uyum Kriterleri

Düzenlenmesine gerek duyulmamıştır.

3.3. Sertifika Yenileme İsteğinde Kimlik Doğrulama

3.3.1. Olağan Sertifika Yenileme İsteğinde Kimlik Doğrulama

Geçerli bir sertifikası olan sertifika sahipleri, sertifikanın kullanım süresi dolmadan önce ve sertifikanın içeriğinde herhangi bir değişiklik olmaması durumunda, Kamu SM'ye olağan sertifika yenileme talebinde bulunabilirler. Olağan setifika yenileme isteğinde kimlik doğrulaması 3.2.2 ve 3.2.3 de belirtildiği şekilde yapılır.

3.3.2. İptal Sonrası Yeni Sertifika Talebinde Kimlik Doğrulama

Sertifikanın içeriğindeki bilgilerin değişmesi, kullanım süresinin dolması ve iptal sonrası yeni sertifika isteğinde bulunulması durumunda, yeniden sertifika almak isteyen sertifika sorumlusu yeni sertifika talebinde bulunur. İptal sonrası yeni sertifika talebinde kimlik doğrulaması 3.2.2 ve 3.2.3 de belirtildiği şekilde yapılır.

3.4. Sertifika İptal İsteğinde Kimlik Doğrulama

Sertifika sorumlusu, MÜS ve GÜS Kullanıma Açma/İptal Etme Formu'nu doldurup Kamu SM'ye fakslayarak veya talebini GİB'e ileterek iptal işlemini gerçekleştirebilir.

Islak imzalı form veya yazı ile yapılan iptal başvurularında kimlik doğrulaması sertifika sorumlusunun iletişim bilgileri kullanılarak irtibata geçilmesi yolu ile yapılır.

GİB'ten gelen iptal başvuruları doğrudan işleme alınır.

4. İşlemsel Gerekler

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 iptal etme

Süreçler sertifika sahipleri ve Kamu SM arasında gerçekleştirilen işlemlerden oluşmaktadır.

4.1. Sertifika Başvurusu

4.1.1. Sertifika Başvurusunu Kimlerin Yapabildiği

Elektronik fatura kullanmak isteyen kurumlar, MÜS ve GÜS için başvurularını, GİB'e yapmaktadır. GİB'in uygun gördüğü ve Kamu SM'ye bildirdiği tüm kurumlar sertifika başvurusunda bulunabilir.

4.1.2. Kayıt İşlemleri ve Sorumluluklar

GİB uygun gördüğü kurumlar ile ilgili elektronik belgeleri, elektronik imzalı olarak çevrim içi yöntemleri kullanarak Kamu SM ye iletir. Gerekli basılı/taranmış evraklar da uygun yöntemlerle (Kurye/Posta kullanılarak), kapalı zarf içerisinde Kamu SM'ye iletilir.

4.2. Sertifika Başvurusunun İşlenmesi

4.2.1. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında GİB'ten gelen taranmış ve elektronik olarak imzalanmış belgelerin, form olarak gelen elektronik veriler ile kaşılaştırılarak incelenmesi sonucunda sertifika sahibi kimlik tanımlama ve doğrulama işlevleri yerine getirilir.

4.2.2. Kimlik Tanımlama ve Doğrulama İşlevlerinin Yerine Getirilmesi

Başvuru sırasında GİB'ten gelen taranmış ve elektronik olarak imzalanmış belgelerin, form olarak gelen elektronik veriler ile kaşılaştırılarak incelenmesi sonucunda sertifika sahibi kimlik tanımlama ve doğrulama işlevleri yerine getirilir.

4.2.3. Sertifika Başvurusunun Kabul veya Reddi

Kurumların MÜS ve GÜS başvurularını GİB değerlendirmektedir. Kabul ve red kararı GİB tarafından verilmektedir.

Başvurusu kabul edilenler Kamu SM sisteminde kullanıcı olarak tanımlanır ve sertifika üretim süreci başlatılır.

4.2.4. Sertifika Başvurusunun İşlenme Zamanı

Başvuru ile ilgili geçerli tüm belgelerin Kamu SM'nin eline geçmesinin ardından en fazla 10 (on) gün içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

4.3. Sertifikanın Oluşturulması

4.3.1. Sertifika Oluşturulmasında ESHS'nin İşlevleri

GİB tarafından sertifika başvurusu kabul edilen ve Kamu SM'ye iletilen talepler için elektronik sertifika üretimi gerçekleştirilir.

Üretim öncesi kurum ve Kamu SM ile yapılan görüşmeler sonucunda, kullanılacak mali mühür oluşturma aracına karar verilir. Kapasite göz önünde bulundurularak akıllı kart ya da donanımsal güvenlik modülü seçilir.

Mali mühür oluşturma aracı seçildikten sonra, kurum hizmet bedelini öder ve ödeme belgesini Kamu SM'ye iletir.

Mali mühür oluşturma aracı olarak akıllı kart seçen kurumlara, asıl ve yedek olmak üzere iki adet donanım teslim edilir.

4.3.2. Sertifika Oluşturulması ile İlgili Sertifika Sorumlusunun Bilgilendirilmesi

Sertifika sorumlusu kendisine gonderilen mali mühür olusturma aracını teslim aldığında, elektronik sertifikalarının olusturulduğu konusunda bilgilendirilmis olur. .

4.4. Sertifikanın Kabül Edilmesi

4.4.1. Sertifikanın Kullanıma Açılma Biçimi

Sertifikalar, sertifika sorumlusu tarafından "MÜS ve GÜS Kullanıma Açma/İptal Etme Formu" doldurulup Kamu SM'ye faks ile iletilmesi suretiyle ya da çevrimiçi servis üzerinden kullanıma açılabilir..

4.4.2. Sertifikanın ESHS Tarafından Yayımlanması

Kamu SM ürettiği GÜS'leri herkesin erişimine açık dizin (LDAP) sunucusundan yayımlar.

4.4.3. Sertifikanın Oluşturulmasının Diğer Bileşenlere Duyurulması

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

4.5. Sertifikanın ve İmza Oluşturma Verisinin Kullanımı

4.5.1. Sertifika Sorumlusunun Sertifika ve İmza Oluşturma Verisini Kullanımı

Sertifika sorumlusu elektronik mali mühür imza oluşturma verilerini yetkisiz kişilerin erişimine karşı korumakla yükümlüdür.

4.5.2. Üçüncü Kişilerin Sertifika ve İmza Doğrulama Verisini Kullanımı

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

4.6. Sertifika Süresinin Uzatılması

Sertifika suresinin uzatılması, kullanım suresi dolan sertifikalarda, sertifikada yer alan

bilgiler değismeden aynı anahtar cifti kullanılarak sertifikanın yeni bir son kullanım tarihi ile tekrar üretilmesini tanımlamaktadır. Kamu SM bu islemi gerceklestirmez.

4.7. Sertifikanın Yenilenmesi

Kamu SM, sertifika yenileme işlemini, yeni anahtar çifti üretmek ve yeni bir başvuru olarak ele almak sureti ile yerine getirir.

4.7.1. Sertifikanın Yenileme Koşulları

Sertifika yenileme işlemi:

- Elektronik mali mühür imza oluşturma aracının kayıp edilmesi veya çalınması durumunda,
- Elektronik mali mühür imza oluşturma aracının arızalanması durumunda,
- Elektronik mali mühür imza oluşturma aracının erişim verisinin kayıp edilmesi, çalınması veya unutulması durumunda,
- Elektronik sertifikaların iptal edilmesi ve yenisinin talep edilmesi durumunda,
- Elektronik sertifikaların geçerlilik süresinin sona ermesi durumunda,
- Elektronik sertifikada bilgi değişikliği gerekmesi durumunda,

yapılmaktadır.

4.7.2. Sertifika Yenileme Başvurusunu Kimlerin Yapabildiği

Bölüm 4.1.1'de tanımlanmaktadır.

4.7.3. Sertifika Yenileme Başvurusunun İşlenmesi

Bölüm 4.2'de tanımlanmaktadır.

4.7.4. Sertifika Yenileme ile İlgili Sertifika Sorumlusunun Bilgilendirilmesi

Bölüm 4.3.2'de tanımlanmaktadır.

4.7.5. Sertifika Yenileme Sonrası Kabul Koşulu

Bölüm 4.4.1'de tanımlanmaktadır.

4.7.6. Sertifika Yenileme Sonrası Sertifikanın Yayımlanması

Bölüm 4.4.2'de tanımlanmaktadır.

4.7.7. Sertifika Yenilemenin Diğer Taraflara Duyurulması

Bölüm 4.4.3'de tanımlanmaktadır.

4.8. Sertifikada Bilgi Değişikliği

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

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

4.9. Sertifikanın İptali ve Askıya Alınması

4.9.1. Sertifikanın İptal Edildiği Durumlar

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

- Sertifika sorumlusunun talebi,
- GİB'in talebi,
- Sertifika içeriğindeki bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,
- Sertifika sahibinin iflasının öğrenilmesi,
- Elektronik mali mühür imza oluşturma verisinin içinde bulunduğu elektronik mali mühür oluşturma aracının kaybolması, çalınması veya bozulması,
- Elektronik mali mühür oluşturma aracının erişim verisinin unutulması veya kayıp edilmesi,
- İlgili mevzuata, Elektronik Mali Mühür Sertifika Sahibi Taahhütnamesi ve Sİ/SUE dokümanında belirtilen şartlara aykırı kullanımının tespit edilmesi,
- Kamu SM'nin MÜS'ü ve GÜS'ü imzalamak için kullandığı imza oluşturma verisinin bütünlüğünün bozulması veya gizliliğinin ortadan kalkması,

durumunda iptal edilir.

GÜS için iptal bölüm 4.12.1'de tanımlanan ilke ve esaslar göz önünde bulundurulmaktadır.

4.9.2. Sertifika İptal Başvurusunu Kimlerin Yapabildiği

Sertifika iptal başvurusu aşağıda tanımlanan kişiler tarafından yapılabilir;

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

4.9.3. Sertifika İptal Başvurusunun İşlenmesi

Elektronik mali mühür sertifikasının iptal başvurusu, sertifika sorumlusu veya GİB tarafından gerçekleştirilebilir. İptal başvurusu çevrimiçi veya yazılı olarak Kamu SM'ye yapılır. Yazılı olarak iptal başvurusu yapıldığında, öncelikle sertifika sorumlusunun kimlik tespiti ve doğrulaması yapılır. Kimlik doğrulaması yapılamayan iptal başvuruları işleme alınmaz.

GİB, çevrimiçi olarak iptal işlemini gerçekleştirebilir. İptal işlemi, yetkilendirilmiş kullanıcılar ile gerçekleştirilir.

Yazılı olarak yapılan taleplerde, sertifika sorumlusu, imzasını taşıyan iptal başvuru formunu Kamu SM'ye iletir. Form üzerindeki bilgiler ve sertifika sorumlusuna ait imza kontrol edilerek kimlik doğrulaması yapılır. Gerekli görüldüğü durumda Kamu SM, telefon

ile bilgi talep eder. Sertifika sorumlusunun kimliği doğrulandıktan sonra, elektronik mali mühür sertifikası Kamu SM sertifika işletmeni tarafından iptal edilir.

MÜS iptal edildikten sonra, Kamu SM sertifika sorumlusunu ve GİB'i bilgilendirir.

Kamu SM iptal bilgilerini en kısa zamanda işler ve duyurur. Kamu SM, iptal durum kayıtlarını SİL yayımlamak ve ÇİSDUP Yanıtlayıcı'da MÜS'ün durumunu iptal konumuna getirmek suretiyle duyurur.

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

4.9.4. İptal İsteği Ertelenme Süresi

Böyle bir süre öngörülmemiştir.

4.9.5. İptal İsteğinin İşlenme Süresi

Kamu SM, kendisine gelen geçerli iptal başvurularını derhal işleme alır ve gerekli doğrulamanın ardından sertifikayı iptal eder.

4.9.6. Üçüncü Kişilerin Sertifika İptal Durumunu Kontrol Gerekliliği

Kamu SM, iptal durum kayıtlarını ücretsiz olarak yayınlar. Kamu SM, iptal durum kayıtlarına erişimin sürekliliğini sağlar.

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

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

4.9.7. Sertifika İptal Listesi Yayımlama Sıklığı

Sertifika sahiplerine ait iptal bilgisinin bulunduğu SİL'lerin geçerlilik süresi 36 (otuzaltı) saattir. Ancak bu sürenin dolması beklenmeden SİL yayım zamanından 24 (yirmidört) saat sonra güncellenir. Gün içinde yeni bir sertifika iptali olmasa dahi SİL güncellenir. Ancak geçerli bir iptal başvurusunun alınıp sertifika sahibine ait sertifikanın Kamu SM sistemi içinde iptal edilmesi durumunda, SİL dosyasının geçerlilik süresinin dolması beklenmeden en geç 10 (on) dakika içinde yeni bir SİL dosyası yayımlanır. Eski SİL dosyaları geçerlilik süresinin sonuna kadar geçerliliğini korur.

Kamu SM'ye ait sertifikaların iptal bilgilerinin duyurulduğu SİL dosyası 4 (dört) ayda bir yenilenir. Sertifikanın iptali durumunda SİL dosyası derhal yenilenir.

4.9.8. Sertifika İptal Listesi Yayımlama Gecikme Süresi

Sertifika İptal Listesi, belirtilen yayımlama zamanından en geç 10 (on) dakika sonra yayımlanır.

4.9.9. Çevrim İçi Sertifika İptal Durum Kaydı Desteği

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

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

.

4.9.10. Çevrim İçi Sertifika İptal Durum Kaydı Gereksinimi

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

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

4.9.11. Diğer Sertifika Durum Bildirim Yöntemleri

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

4.9.12. İmza oluşturma Verisinin Güvenliğini Yitirmesi Durumu

Sertifika sahibine ait imza oluşturma verisinin güvenliğini yitirmesi durumunda sertifika iptal edilir. Sertifikanın iptal edilmesi dışında herhangi bir husus uygulanmamaktadır.

4.9.13. Sertifikanın Askıya Alındığı Durumlar

Askıya alma işlemi uygulanmaz.

4.9.14. Sertifika Askıya Alma Başvurusunu Kimlerin Yapabildiği

Düzenlenmesine gerek görülmemiştir.

4.9.15. Sertifika Askıya Alma Başvurusunun İşlenmesi

Düzenlenmesine gerek görülmemiştir.

4.9.16. Askıda Kalma Süresi

Böyle bir süre öngörülmemiştir.

4.10. Sertifika Durum Servisleri

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

4.10.1. İşletimsel Özellikleri

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

ÇİSDUP İstemci desteği olan üçüncü kişiler, sertifika iptal durumunu ÇİSDUP Yanıtlayıcı'dan öğrenebilirler. ÇİSDUP Yanıtlayıcı erişim adresi 2. Bölümde verilmiştir. Üçüncü kişiler elektronik sertifikaların geçerlilik durumunu her kontrol etmek istediklerinde, ÇİSDUP Yanıtlayıcı üzerinden sorgulama yaparlar.

4.10.2. Servisin Erişilebilirliği

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

4.10.3. İsteğe Bağlı Özellikler

Düzenlenmesine gerek duyulmamıştır.

4.11. Sertifika Sahipliğinin Sona Ermesi

Sertifikanın kullanım süresinin dolması, iptal edilmesi ve Kamu SM'nin sertifika hizmetlerini sonlandırmasıyla sertifika sahipliği sona erer. Kamu SM sertifikasının iptal edilmesi ve Kamu SM tarafından sertifika hizmetlerinin sonlandırılması durumunda; sertifika sorumlusu ve GİB bilgilendirir. Kullanım süresinin dolması durumunda, Kamu SM sertifika sorumlusu bilgilendirmez; sertifika sorumlusu sertifikasının kullanım süresinin dolduğu zamanı kendisi takip etmekle yükümlüdür.

4.12. İmza Oluşturma Verisinin Saklanması ve Geri Kazanımı

Veri şifreleme amacıyla kullanılan güvenlik hizmetleri sertifikasının, imza oluşturma verisi Kamu SM tarafından güvenli yöntemlerle şifreli olarak saklanmaktadır.

Elektronik mali mühür sertifikasının imza oluşturma verisi hiçbir şekilde saklanmamaktadır.

4.12.1. GÜS İmza Oluşturma Verisinin Saklanması ve Geri Kazanımı İlke ve Esasları

GÜS imza oluşturma verisinin geri kazanımı, elektronik mali mühür oluşturma aracının sertifika sorumlusunun elinde olup olmaması dikkate alınarak tanımlamaktadır:

- Elektronik mali mühür oluşturma aracı sertifika sorumlusunun elinde, fakat erişim verisinin kayıp edilmesi, unutulması veya elektronik mali mühür oluşturma aracının arızalanması durumunda; GÜS iptal edilmez, yedeklenen imza oluşturma verisi ile sertifika oluşturulur ve elektronik mali mühür oluşturma aracına yüklenir.

- Elektronik mali mühür oluşturma aracı sertifika sorumlusunun elinde değil ise, kayıp edilmiş veya çalınmış ise; GÜS iptal edilir. Yeni bir imza oluşturma verisi ile yeni bir sertifika oluşturulur ve elektronik mali mühür oluşturma aracına yüklenir. Yeni oluşturulan GÜS yanına ayrıca, daha önceki GÜS imza oluşturma verileri ve sertifikaları da yüklenir. Kart içerisinde yer kalmaması durumunda eski GÜS'ler PKCS#12 formatında sertifika sorumlusuna e-posta ile gönderilir.

4.12.2. Oturum Anahtarı Zarflama ve Geri Kazanım İlke ve Esasları

Düzenlenmesine gerek duyulmamıştır.

5. Yönetim, İşlemsel ve Fiziksel Kontroller

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

5.1. Fiziksel Güvenlik Denetimleri

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

5.1.1. Tesis Yeri ve İnşaatı

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

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

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

5.1.2. Fiziksel Erişim

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

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

5.1.3. Güç Kaynağı ve Havalandırma

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

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

Bina gerekli havalandırma sistemi ile donatılmıştır.

5.1.4. Su Baskınları

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

5.1.5. Yangın Önleme ve Korunma

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

5.1.6. Saklama ve Yedekleme Ortamlarının Korunması

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

5.1.7. Atıkların Yok Edilmesi

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

5.1.8. Farklı Mekanlarda Yedekleme

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

5.2. Prosedürsel Kontroller

5.2.1. Güvenilir Roller

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

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

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

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

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

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

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

Veri Sistemleri Yöneticisi: Dizin ve veritabanı yığınlarının (cluster) yönetimini yapar. Veritabanı yönetim faliyetlerini gerçekleştirir.

Sertifika Süreç Yöneticisi: Kamu SM internet sitesinde yayınlanan Sİ, SUE, ZDİ ve ZDUE dokümanlarını gerektiğinde güncellenmesini veya değiştirilmesini önerir, sertifika yönetim prosedürlerinde anlatılan prosedürlerin iyileştirilmesinden sorumludur.

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

Sertifika Üretim İşletmeni: Sertifika yaşam döngüsü işlemlerini Sertifika Yönetim Prosedürleri'nde belirtildiği şekilde yapar. Sertifika yaşam döngüsü süreçleri kapsamında gelen ve giden evrakı kontrol eder ve arşivler.

Sertifika Çağrı Destek İşletmeni: Kamu SM'ye gelen telefon çağrılarına cevap verir. Prosedürler içinde belirtilen durumlarda sertifika sorumlusunu bilgilendirir ve sertifika iptali isteklerini yerine getirir.

Elektronik Sertifika Yönetim Altyapısı (ESYA) ve Uygulama Destek Sorumlusu: Kamu SM'de kurulu olarak teslim aldığı ESYA sistemini yaşatmak için gerekli önlemleri alır.

Denetçi: Yönetim tarafından TÜBİTAK UEKAE içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından görevlendirilen bir kişi olan denetçi, sistem denetim profilinin kurulması, denetimlerin yönetimi ve gözden geçirilmesi ile sistemin teknik ve idari işleyişinin kontrolü ve raporlarının hazırlanmasından sorumludur.

5.2.2. Her İşlem İçin Gereken Kişi Sayısı

Kamu SM, kök ve alt köklere ait sertifika üretilmesi ve iptal edimesi için birden fazla kişinin aynı anda hazır bulunmasını sağlar.

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

5.2.3. Kimlik Doğrulama ve Yetkilendirme

Kamu SM işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanır. Sistemdeki bazı birimlere erişim, farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilmektedir.

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

5.2.4. Görevlerin Ayrılmasını Gerektiren Roller

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

5.3. Personel Güvenlik Kontrolleri

5.3.1. Kişisel Geçmiş, Deneyim ve Nitelik Gerekleri

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

5.3.2. Geçmiş Araştırması

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

5.3.3. Eğitim Gerekleri

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

5.3.4. Sürekli Eğitim Gerekleri ve Sıklığı

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

5.3.5. Görev Değişim Sıklığı ve Sırası

Düzenlenmesine gerek duyulmamıştır.

5.3.6. Yetkisiz Eylemlerin Cezalandırılması

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

5.3.7. Anlaşmalı Personel Gereksinimleri

Kamu SM kendi personeli dışındaki kişilerle çalışmak durumunda olduğunda, bu kişilerle ilgili olarak, kendi personeline uyguladığı güvenlik kontrollerini yapar.

5.3.8. Sağlanan Dokümantasyon

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

5.4. Denetim Kayıtları

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

5.4.1. Kaydedilen İşlemler

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

- Kamu SM anahtarlarının yaşam döngüsü yönetimi işlemleri
  - Anahtar üretimi
  - Anahtar yedekleme
  - Anahtar yok etme
  - Kriptografik modül yaşam döngüsü işlemleri
- Sertifika üretim, yenileme, güncelleme, askıya alma ve iptal başvuruları
  - Başvuru sahibi tarafından sunulan belgelerin neler olduğu bilgisi
  - Başvuru sırasında alınan kimlik tanımlamaya yarayan belgeler
  - Başvuru sırasında elektronik veya kağıt ortamda alınan form veya belgeler
  - Kağıt belgelerin kopyalarının nerede saklandığı bilgisi
  - Geçerli ve geçersiz alınan tüm başvuru bilgileri
- Sertifika yaşam döngüsü yönetimi işlemleri
  - Sertifika kullanıma açma
  - Sertifika yenileme
  - Sertifika iptal etme
  - SİL yayımlanması
- Güvenlikle ilgili diğer işlemler
  - Sisteme başarılı veya başarısız tüm erişim denemeleri
  - Çalışanlar tarafından gerçekleştirilen güvenlik sistemi işlemleri
  - Güvenli tutulması gereken hassas dosyaların okunması, yazılması ve değiştirilmesi
  - Güvenlik profili değişiklikleri
  - Sistemin çökmesi, donanım hataları ve diğer bozukluklar
  - Güvenlik duvarı (firewall) ve yönlendirici (router) işlemleri
  - Kamu SM'ye ziyaretçi giriş ve çıkışı

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

5.4.2. Kayıtların İncelenme Sıklığı

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

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

5.4.3. Kayıtların Saklanma Süresi

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

5.4.4. Kayıtların Korunması

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

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

5.4.5. Kayıtların Yedeklenmesi

Sistemin kritikliği göz önüne alındığında her gün düzenli olarak, sistemin yoğun olarak kullanılmadığı bir saatte gerekli görülen kayıtların çevrim içi yedeği alınmaktadır. Yedekleme ihtiyacını gidermek üzere teyp kütüphanesi ve yedekleme işlemlerini otomatikleştirmek için yedekleme yönetim yazılımı mevcuttur.

5.4.6. Kayıtların Toplanması

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

5.4.7. Kayda Sebebiyet Veren Tarafın Bilgilendirilmesi

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

5.4.8. Saldırıya Açıklığın Değerlendirilmesi

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

5.5. Kayıt Arşivleme

5.5.1. Arşivlenen Kayıt Bilgileri

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

- Sertifika sorumlusu veya GİB tarafından, başvuru sırasında verilen tüm bilgi ve belgeler

- Sertifika kullanıma açma, yenileme 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 ve Sertifika Uygulama Esasları dokümanı
- Elektronik Mali Mühür Sertifika Sahibi Taahhütnamesi dökümanı

5.5.2. Arşivlerin Tutulma Süresi

Arşivlenen bilgiler ve belgeler en az 5 (beş) yıl boyunca saklanır.

5.5.3. Arşivlerin Korunması

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

5.5.4. Arşivlerin Yedeklenmesi

Kritik bilgi içeren elektronik arşivler Kamu SM iş sürekliliği politikası gereğince yedeklenir.

5.5.5. Kayıtların Zaman Damgası Gereksinimleri

Kamu SM gerekli gördüğü kayıtlara zaman damgası ekler.

5.5.6. Arşivlerin Toplanması

Arşivler elektronik veya kağıt ortamda toplanır.

5.5.7. Arşiv Bilgilerinin Elde Edilme ve Doğrulanma Metodu

Arşiv bilgileri yetkili personelden edinilir. Aynı bilgiye ait birden fazla arşiv olması durumunda arşivler kıyaslanarak doğruluğu kontrol edilir.

5.6. Anahtar Değişimi

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

- Sertifika kullanım süresinin dolmasından en geç 6 (altı) ay önce işlemler başlatılır. Eski anahtarlarla sertifika verilmesi durdurulur.
- Kamu SM'nin eski imza oluşturma verisiyle imzalanmış sertifikaların doğrulanabilmesi için, eski Kamu SM sertifikası yayımlanmaya devam eder.
- SİL dosyası aynı Kamu SM imza oluşturma verisiyle imzalanıyorsa, Kamu SM'nin eski imza oluşturma verisiyle oluşturulmuş sertifikaların kullanım tarihleri dolana kadar, Kamu SM SİL'leri eski imza oluşturma verisiyle imzalamaya devam eder. Yeni

üretilen sertifikalar için oluşturulan SİL dosyası yeni Kamu SM imza oluşturma verisiyle imzalanır.

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

5.7. Güvenliğin Yitirilmesi ve Arıza Durumlarında Yapılacaklar

5.7.1. Güvenilirliğin Yitirilmesi Durumunun Düzeltilmesi

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

5.7.2. Donanım, Yazılım veya Veri Bozulması

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

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

Gerekli görüldüğü takdirde imza oluşturma verisinin çalınması durumunda uygulanacak süreçler işletilir ve yeniden çalışırlık sağlanır.

5.7.3. İmza Oluşturma Verisinin Gizliliğinin Kaybedilmesi

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

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

5.7.4. Arıza Sonrası Yeniden Çalışırlık

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

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

5.8. Sertifika Hizmetlerinin Sonlandırılması

Kamu SM'nin Elektronik Mali Mühür projesinde görevinin sona ermesi durumda aşağıdaki işlemleri yerine getirir:

- Sertifika hizmetlerine son vereceği tarihten 3 (üç) ay öncesine kadar durumu sertifika hizmeti verdiği bütün sertifika sahiplerine e-posta ile duyurur.
- Sertifika hizmetlerine son vereceği bilgisini internet sitesi üzerinden duyurur.
- Sertifika hizmetlerine son vereceğini duyurmasından itibaren sertifika başvurusu kabul etmez ve yeni sertifika oluşturmaz.
- Dağıttığı sertifikaları iptal eder, iptal bilgisini SİL ve ÇİSDUP aracılığıyla üçüncü kişilere duyurur. İptal ettiği sertifikaların bilgisini sertifika sahiplerine e-posta ile duyurur.
- İptal ettiği sertifikaların kullanım süreleri dolana kadar en son ürettiği SİL dosyasını yayımlamaya devam eder.
- SİL dosyasını imzalamada kullandığı imza oluşturma verisine karşılık gelen sertifikasını, SİL dosyasının geçerlilik süresi boyunca yayımlamaya devam eder.
- Sertifikaları imzalamak için kullandığı imza oluşturma verisini imha eder.
- İlgili tüm kayıtları ve arşivleri uygun bir şekilde 20 (yirmi) yıl boyunca korur.

6. Teknik Güvenlik Kontrolleri

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

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

6.1.1.1. Kök ve Alt Kök Anahtar Çifti Üretimi

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

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

6.1.1.2. Sertifika Sahibi Anahtar Çiftinin Üretimi

MÜS ve GÜS için anahtar çifti Kamu SM tarafından üretilir. Sertifika sahibinin anahtar çiftleri Kamu SM tarafından yetkisi olmayan personelin giremediği odalarda, güvenli yazılım kullanılarak üretilir ve şifrelenerek elektronik mali mühür oluşturma aracı içinde saklanır.

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

Sertifika sahibine ait MÜS anahtar çifti hiçbir şekilde sistemde tutulmaz. GÜS anahtar çifti geri kazanım için güvenli ortamda ve şifreli olarak tutulur. Elektronik mali mühür oluşturma aracı sertifika sorumlusuna teslim edilene kadar yetkisiz kişilerin erişemediği güvenli ve kilitli odalarda saklanır.

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

6.1.2. Sertifika Sorumlusuna İmza Oluşturma Verisinin Ulaştırılması

Sertifika sahibine ait anahtar çiftlerinin Kamu SM tarafından oluşturulmasına müteakip; imza oluşturma verisi, sertifika ile birlikte elektronik mali mühür oluşturma aracı içinde imza karşılığı ve kimlik kontrolü yapılarak sertifika sorumlusuna teslim edilir. Sertifika sorumlusu elektronik mali mühür sertifikasını teslim aldıktan sonra, MÜS ve GÜS Kullanıma Açma/İptal Etme Formu'nu (FORM-001-060) Kamu SM'ye faks ve/veya posta ile iletir.

MÜS ve GÜS Kullanıma Açma/İptal Etme Formu'nun Kamu SM'ye ulaşmasına müteakip elektronik mali mühür oluşturma aracı erişim verisi kapalı zarf içinde imza karşılığı ve kimlik kontrolü ile sahibine teslim edilir.

Teslimatlar kurye ile gerçekleştirilir.

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

MÜS ve GÜS imza oluşturma ve doğrulama verileri Kamu SM tarafından oluşturulduğu için başvuru sahibi tarafından imza doğrulama verisinin Kamu SM'ye ulaştırılması söz konusu değildir.

6.1.4. Elektronik Sertifika Hizmet Sağlayıcısı Sertifikalarına Erişim Sağlanması

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

Kamu SM'ye ait sertifikalar Kamu SM ye ait web sayfası üzerinden yayımlanır.

Kök ve alt kök sertifikalarının özet değeri ve özet algoritması http://mm.kamusm.gov.tr/belgeler/ web adresi üzerinden yayımlanır.

6.1.5. Anahtar Uzunlukları

Kamu SM'ye ait kök ve alt köklerin RSA açık anahtar algoritması imza oluşturma anahtar çiftinin boyu en az 2048 bittir.

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

Kamu SM tarafından üretilen MÜS ve GÜS, sertifika sahiplerine ait, RSA imza oluşturma anahtar çiftlerinin boyu en az 2048 bittir.

6.1.6. Anahtar Üretim Parametreleri ve Kalitesinin Kontrolü

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

6.1.7. Anahtar Kullanım Amaçları

Kamu SM tarafından oluşturulan imza oluşturma verilerinin hangi amaçlar için kullanılabileceği ilgili imza oluşturma verisine karşılık gelen sertifikadaki "Anahtar Kullanımı" ve "Geliştirilmiş Anahtar Kullanımı" uzantısı içerisinde belirtilir.

6.2. İmza Oluşturma Verisinin Korunması

6.2.1. Kriptografik Modül Standartları

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

Kriptografik modül aşağıda belirlenen güvenlik işlevlerine sahiptir:

- İmza oluşturma verisinin geçerlilik süresi boyunca gizlilik ve bütünlüğünü sağlar.
- Modüle erişimde kimlik belirleme ve doğrulama işlevlerini yerine getirir.
- Erişim yetkisi birden fazla kişinin kontrolünde olacak şekilde tanımlanabilir.

- Kullanıcıya tanımlanan roller doğrultusunda verdiği hizmetlere erişimi sınırlar.
- Düzgün çalıştığı test edilebilir, test sırasında hata oluştuğunda güvenli duruma geçer.
- Modüle izinsiz erişim ve kullanım ile tahrifata yol açabilecek her türlü fiziksel önlem alınmıştır.
- Yetkisiz erişime teşebbüs edilmesi durumunda, modül içindeki veriyi siler.
- İmza oluşturma verisinin yedeğinin güvenli biçimde alınmasına olanak verir.
- Sertifika sahibinin imza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracı, imza oluşturma verisinin aracın dışına çıkmasını engelleyen ve araca erişimi parola ile sağlayan teknik özelliklere sahiptir.

Kriptografik modül ve sertifika sahibinin güvenli elektronik imza oluşturma aracı aşağıdaki güvenlik standartlarından en azından birisini sağlar:

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

6.2.2. İmza Oluşturma Verisine Birden Fazla Kişi Kontrolünde Erişim

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

6.2.3. İmza Oluşturma Verisinin Yeniden Elde Edilmesi

Düzenlenmesine gerek duyulmamıştır.

6.2.4. İmza Oluşturma Verisinin Yedeklenmesi

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

Sertifika sahiplerine ait MÜS imza oluşturma verileri Kamu SM tarafından yedeklenmez.

Sertifika sahiplerine ait GÜS imza oluşturma verileri, geri kazanım amaçlı güvenli bir ortamda ve şifreli olarak yedeklenir.

6.2.5. İmza Oluşturma Verisinin Arşivlenmesi

Kamu SM'ye ve MÜS'e ait imza oluşturma verileri arşivlenmez. GÜS imza oluşturma verisi arşivlenir.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modüle Yüklenmesi

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

MÜS ve GÜS imza oluşturma verileri, sadece yetkili personelin giriş izninin bulunduğu odalarda güvenli elektronik imza oluşturma aracına yüklenir.

6.2.7. İmza Oluşturma Verisinin Kriptografik Modülde Saklanması

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

6.2.8. İmza Oluşturma Verisine Erişim

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

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

MÜS ve GÜS imza oluşturma verisi, elektronik mali mühür oluşturma aracı içinde, sertifika sahibinin erişim verisi ile korunmuş olarak saklanır. Erişim denetimi erişim denetim verisi ile sağlanır.

6.2.9. İmza Oluşturma Verisine Erişimin Kesilmesi

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

Sertifika sorumlusunun kullandığı elektronik mali mühür oluşturma araçları, imza oluşturma verisini kullanan oturumun kapanmasından sonra veriye erişimi kesecek biçimde çalışır. Erişimin yeniden sağlanabilmesi için sertifika sorumlusunun erişim verisini yeniden girmesi gerekir. Erişim verisinin ard arda 3 (üç) defa yanlış girilmesi durumunda elektronik mali mühür oluşturma aracı kilitlenir ve araca erişim sağlanamaz.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi

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

Sertifika sahiplerine ait imza oluşturma verileri kullanım süresinin sonunda veya sertifikanın iptal edilmesinden sonra sertifika sorumlusu tarafından elektronik mali mühür

oluşturma aracı üzerinden silinmelidir. Bu işlemin yapılmasından sertifika sorumlusu sorumludur.

6.2.11. Kriptografik Modülün Değerlendirilmesi

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

6.3. Anahtar Çifti Yönetimiyle İlgili Diğer Konular

6.3.1. İmza Doğrulama Verisinin Arşivlenmesi

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

6.3.2. İmza Oluşturma ve Doğrulama Verilerinin Kullanım Süreleri

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

Kamu SM'ye ve sertifika sahibine ait anahtar çiftlerinin kullanım süresi, anahtar uzunlukları ve kullanılan imza algoritmasına göre belirlenir. Kamu SM'ye ait 2048 RSA anahtar çiftleri en fazla 10 (on) yıl için kullanılır. Sertifika sahiplerine ait 2048 bitlik RSA anahtar çiftleri 3 (üç) veya 5 (beş) yıl için kullanılır.

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

6.4. Erişim Denetim Verileri

Kamu SM çalışanlarının erişim denetim verileri erişim parolalarını, elektronik mali mühür oluşturma araçları içindeki erişim denetimi sağlayan diğer verileri ve biyometrik verileri içerir.

Sertifika sahibi için tanımlanan erişim verisi, elektronik mali mühür oluşturma aracına ait erişim verisidir.

6.4.1. Erişim Denetim Verilerinin Oluşturulması

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

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

6.4.2. Erişim Denetim Verilerinin Korunması

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

Sertifika sahibine ait erişim parolaları kapalı zarf içinde sertifika sorumlusuna ulaştırılır ve kopyası Kamu SM tarafından tutulmaz.

Erişim parolaları ilk kullanımda sertifika sorumlusu tarafından değiştirilir. Parolayı ikinci kişilerin erişiminden korumak sertifika sorumlusunun yükümlülüğü altındadır.

6.4.3. Erişim Denetim Verileri İle İlgili Diğer Konular

Erişim denetimi verilerinin sahibine ulaştırılması güvenli yollarla yapılır. Sertifika sahibine ait erişim parolaları kapalı zarf içinde, kimlik kontrolü yapılarak imza karşılığı sahibine teslim edilir.

6.5. Bilgisayar Güvenliği Denetimleri

6.5.1. Bilgisayar Güvenliği İle İlgili Teknik Gerekler

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

6.5.2. Bilgisayar Sisteminin Sağladığı Güvenlik Seviyesi

Düzenlenmesine gerek duyulmamıştır.

6.6. Yaşam Döngüsü Teknik Denetimleri

6.6.1. Sistem Geliştirme Denetimleri

Sistem geliştirilirken genel anlamda yapılan denetimler aşağıda verilmiştir:

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

6.6.2. Güvenlik Yönetimi Denetimleri

Denetim 2 (iki) yılda bir gerçekleştirilir. Denetim kapsamında süreçler ve bilgi sistemleri bileşenleri ele alınır. Bulgular raporlanır; düzeltici faaliyet veya iş talebi ile gerekli iyileştirmeler gerçekleştirilir.

6.6.3. Yaşam Döngüsü Güvenlik Denetimleri

Düzenlenmesine gerek duyulmamıştır.

6.7. Ağ Güvenliği Denetimleri

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

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

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

6.8. Zaman Damgası

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

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

Dökümanlara bu adresten (http://www.kamusm.gov.tr/tr/BilgiDeposu/) ulaşılabilir.

7. Sertifika ve Sertifika İptal Listesi Biçimleri

7.1. Sertifika Biçimi

Bu bölümde Kamu SM tarafından oluşturulan Kök, Alt kök, MÜS ve GÜS içeriği ile ilgili bilgilendirme yapılmaktadır.

7.1.1. Sürüm Numarası

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

7.1.2. Sertifika Uzantıları

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

Kamu SM tarafından oluşturulan Kök, Alt kök, MÜS ve GÜS içeriği EK-A da bulunmaktadır.

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

7.1.3. Algoritma ve Nesne Tanımlayıcılar

EK-A da belirtilmiştir..

7.1.4. İsim Alanı Biçimleri

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

7.1.5. İsim Kısıtları

Bölüm 3.1 de belirtilmiştir.

7.1.6. Sertifika İlkeleri Nesne Tanımlama Numarası

Kamu SM tarafından oluşturulan her sertifika içeriğinde bir nesne tanımlama numarası bulunmaktadır.

7.1.7. İlke Kısıtları Uzantısının Kullanımı

Düzenlenmesine gerek duyulmamıştır.

7.1.8. İlke Niteleyiciler

"Sertifika İlkeleri Uzantısı" sertifikaların üretim ve yönetim işlemlerinde uyulan ilke ve esasların Kamu SM Sİ/SUE olduğuna işaret eder. MÜS ve GÜS üretim ve yönetiminde takip edilen kurallara işaret eden Sİ/SUE dokümanına ait nesne tanımlama numarası [Certificate Policy Object Identifier(s)] Kamu SM tarafından üretilen sertifikaların "Sertifika

İlkeleri Uzantısı[1]"nın içinde yer alır. "Sertifika İlkeleri Uzantısı"nın içinde "İlke Niteleyici[2]" olarak belirtilen alana Kamu SM SUE dokümanının bulunduğu internet adresi yazılır.

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

Kamu SM tarafndan oluşturulan MÜS ve GÜS'te "Sertifika İlkeleri Uzantısı" içeriğinde nesne tanımlama numarası olarak 2.16.792.1.2.1.1.5.7.4.1 ve ilke niteleyici olarak http://depo.kamusm.gov.tr/ilke/yer alır.

7.1.9. Kritik Belirtilmiş Olan İlke Belirleyici Uzantılarının İşlenmesi

Düzenlenmesine gerek duyulmamıştır.

7.2. Sertifika İptal Listesi Biçimi

7.2.1. Sürüm Numarası

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

7.2.2. Sertifika İptal Listesi Uzantıları

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

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

7.3. Çevrim İçi Sertifika Durum Protokolü Biçimi

7.3.1. Sürüm Numarası

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

7.3.2. ÇİSDUP Uzantıları

ÇİSDUP sorguları aşağıdaki bilgileri içermelidir.

- Protokol versiyonu

[1] Certificate Policies
[2] Policy Identifier

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

ÇİSDUP cevapları aşağıdaki bilgileri içermektedir.

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

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

Çevrim İçi Sertifika Durum Protokolü RFC 2560'da tarif edilen "ÇİSDUP" formatını destekler. ÇİSDUP Yanıtlayıcı'dan alınan cevaplar aşağıdaki şekilde değerlendirilir:

Good [iyi]: Sertifika geçerli konumdadır.

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

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

RFC 2560'da belirtilen uzantılar ÇİSDUP cevap formatında kullanılmamaktadır.

8. Uygunluk Denetimleri

Bu bölümde Kamu SM sertifika yönetim sisteminin Sİ/SUE dokümanına uygunluğunun denetlenmesi ile ilgili bilgilendirme yapılmaktadır.

8.1. Uygunluk Denetiminin Sıklığı

Kamu SM sertifika yönetim sisteminin bu Sİ/SUE dokümanında belirtilen şartları sağlayıp sağlamadığı 3 (üç) yılda en az bir kere denetlenir. Denetim Kamu SM'nin denetimle görevlendirdiği personel tarafından yerine getirilir.

8.2. Denetçinin Nitelikleri

Denetçinin Sİ/SUE dokümanında belirtilenleri iyi anlaması, açık anahtarlı altyapılar hakkında bilgi sahibi olması ve uygunluk denetimleri konusunda tecrübeli olması gerekir.

8.3. Denetçinin Denetlenen Tarafla Olan İlişkisi

Denetçi TÜBİTAK UEKAE içinde uygunluk denetimleri yapan birimlerden veya Kamu SM bünyesinde çalışan personel arasından seçilir.

8.4. Denetimin Kapsamı

Sertifika yönetim süreçlerini detaylandırarak anlatan sertifika yönetim prosedürlerinin, Kamu SM'nin iç işleyişindeki güvenlik ve işlevsel süreçlerin incelenerek işleyişin Sİ/SUE dokümanına uygunluğu denetlenir.

8.5. Yetersizliğin Tespiti Durumunda Yapılacaklar

Denetim sırasında Kamu SM'nin, Sİ ve SUE dokümanlarının gereklerini yerine getirmediğinin tespit edilmesi durumunda, denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu yazdığı raporla ilgililere bildirir. Kamu SM yönetiminin önderliğinde yetersizliği tespit edilen durumların giderilmesi için yapılacak işlemler belirlenir ve yetersizliğin giderilmesi için çalışma başlatılır.

Denetimde sistemin kurulum, işletim veya bakım aşamaları sırasında, Sİ ve SUE dokümanlarının gereklerinin yerine getirilmediğinin tespit edilmesi durumunda aşağıdaki işlemler gerçekleştirilir:

- Denetçi hangi süreçlerdeki aşamaların uygunsuz olduğunu not eder ve ilgili tarafları 2 (iki) gün içinde bilgilendirir.
- Kamu SM denetim sonucu tespit edilen yetersizliklerini Sİ/SUE dokümanında belirtilen uygulama esaslarına uygun olarak giderir.
- Sertifika yönetimiyle ilgili kritik bulunan işlemlerde yetersizliğin tespit edilmesi durumunda, Kamu SM ilgili işlemleri düzeltmeler yapılıncaya kadar durdurur.

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

8.6. Sonucun Bildirilmesi

Denetim sonucu rapor olarak Kamu SM yönetimine bildirilir. Kamu SM yönetimi raporda belirtilen, Sİ ve SUE'ye uygun olmadığı tespit edilen durumların en kısa zamanda düzeltilmesini sağlar.

9. Diğer İşler ve Hukuksal Meseleler

9.1. Ücretlendirme

9.1.1. Sertifika Oluşturma ve Yenileme Ücreti

Kamu SM tarafından üretilen veya yenilenen sertifikalar ve diğer hizmetler için sertifika sahiplerinden ücret talep eder. Ürün ve hizmet bedeli, Kamu SM tarafından belirlenir ve GİB onayı alınır. Ürün veya hizmet bedeli ve ödeme şekli Kamu SM tarafından gönderilen teklif mektuplarında bildirilir.

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

9.1.2. Sertifika Erişim Ücreti

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

9.1.3. İptal Durum Kaydına Erişim Ücreti

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

9.1.4. Diğer Servis Ücretleri

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

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

9.1.5. İade Ücreti

Sertrifika sorumlusu, sertifikasını ilk teslim aldığında yaptığı kontrol neticesinde, sertifikasını kullanamadığını tespit ederse ve sorunun Kamu SM'den kaynaklanan bir hata sebebiyle ortaya çıktığı anlaşılırsa, sertifika bilabedel yenilenir. Güvenli elektronik imza oluşturma aracı erişim verisinin kaybolması, unutulması, aracın yanlış erişim verisi girilmesi dolayısıyla kilitlenmesi, sertifika sorumlusunun yanlış kullanımından dolayı aracın kullanılamaz duruma gelmesi, sertifikanın iptali ve benzeri durumlarda sertifikanın kalan süresi kadar ve ücret karşılığı yenileme yapılır.

9.2. Finansal Sorumluluk

9.2.1. Sigorta Kapsamı

9.2.2. Düzenlenmesine gerek duyulmamıştır.Diğer Varlıklar

Düzenlenmesine gerek duyulmamıştır.

9.2.3. Sertifika Mali Sorumluluk Sigortası

Kamu SM tarafından oluşturulan MÜS ve GÜS'ün sertifika sorumlusu ve üçüncü taraflar tarafından kullanımı ile ilgili doğabilecek risklerden sertifika sorumlusu ve üçüncü taraflar sorumludur.

9.3. Ticari Bilginin Korunması

9.3.1. Gizli Bilginin Kapsamı

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

9.3.2. Gizlilik Kapsamında Olmayan Bilgiler

Kamu SM tarafından http://mm.kamusm.gov.tr/belgeler adresinden yayımlanan her türlü döküman ve sertifikalar içerisinde yer alan bilgiler gizli olarak değerlendirilmezler.

9.3.3. Gizli Bilginin Korunma Sorumluluğu

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

9.4. Kişisel Bilginin Gizliliği

9.4.1. Gizlilik Planı

Düzenlenmesine gerek duyulmamıştır.

9.4.2. Gizli Olarak Tanımlanan Bilgiler

Gizli bilgi, sertifika sahibinin, başvuru sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim prosedürleri içinde kullanılmak üzere Kamu SM'ye beyan ettiği adres, vergi kimlik numarası ve sertifika sorumlusunun kişisel bilgilerini kapsar. Kamu SM veya sertifika sorumlusu tarafından atanan parolalar, numara, sembol gibi diğer tanımlayıcıyı bilgiler de gizli bilgi kapsamına girer.

9.4.3. Gizli Olarak Tanımlanmayan Bilgiler

Kamu SM tarafından oluşturulan sertifikaların içeriğinde bulunan bilgiler aksi taraflar arası sözleşmelerde belirtilmediği sürece gizli değildir.

9.4.4. Gizli Bilginin Korunma Sorumluluğu

Kamu SM sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep etmez. Kamu SM elde ettiği kişisel bilgileri sertifika hizmeti vermek dışında başka amaçlar için kullanmaz ve üçüncü kişilere vermez. 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 sahibinin bilgilerine erişir.

9.4.5. Gizli Bilginin Kullanımına İzin Verilmesi

Kamu SM sertifika sorumlusunun yazılı veya e-imzalı rızası ile kişisel bilgileri üçüncü kişilerle paylaşabilir.

9.4.6. Yetkili Merciilerin Kararına Uygun Olarak Bilginin Açıklanması

Kamu SM sertifika sahiplerine ait gizli bilgileri, mahkeme kararı olması durumunda açıklayabilir.

9.4.7. Diğer Başlıklar

Düzenlenmesine gerek duyulmamıştır.

9.5. Telif Hakları

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

9.6. Temsil Hakkı ve Yükümlülükler

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

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

9.6.1. Elektronik Sertifika Hizmet Sağlayıcısı Yükümlülükleri

- Elektronik sertifikalar ile ilgili tüm işlemleri, Kamu SM Elektronik Mali Mühür Sertifika İlkeleri ve Uygulama Esasları'nda belirtilen şartlar altında yerine getirir.
- Başvuru sırasında sertifika sahibine ait kağıt üzerinde veya elektronik ortamdan verilen bilgileri sertifika hizmeti dışında başka herhangi bir amaç için kullanmaz, tutulan bilgilerin gizliliğinin korunması için gerekli önlemleri alır, bu bilgileri üçüncü kişilere mahkeme kararı veya sertifika sahibinin yazılı rızası olmaksızın vermez.
- Sertifika sahibine ait elektronik mali mühür oluşturma verisinin kopyasını hiçbir şekilde tutmaz.
- Sertifika sahibine ait güvenlik hizmetleri sertifikasının, şifreleme verisinin kopyasını, yedeklemek amacıyla güvenli olarak saklar.
- Elektronik sertifikaların, GİB tarafından yapılan düzenlemelere ve Kamu SM yönergelerine uygun kullanılmadığının tespiti durumunda; elektronik sertifikaları res'en iptal eder.
- Elektronik mali mühür oluşturma aracı ve elektronik mali mühür oluşturma verisine erişim verisinin basıldığı kapalı parola zarfını, sertifika sorumlusuna imza karşılığında teslim eder.
- Sertifikaların geçerlilik süresi boyunca, elektronik mali mühür oluşturma aracında ve/veya elektronik mali mühür oluşturma aracı okuyucusunda, kullanıcı kusurları hariç, bir donanım arızası oluşması halinde TÜBİTAK UEKAE oluşan donanım arızalarını giderir ve elektronik mali mühür oluşturma aracını ve/veya elektronik mali mühür oluşturma aracı okuyucusunu ücretsiz olarak yeniler. Bu maddede anılan nedenlerle yapılan yenileme işlemlerinde sağlanan yeni elektronik mali mühür oluşturma aracının kullanım süresi, arızalanan elektronik mali mühür oluşturma aracının arıza tarihi itibariyle kalan geçerlilik süresine eşit olacaktır.
- Madde 1.7.'de belirtilen durumlar haricindeki her türlü iptal, arıza, kayıp, kullanıcı hatası nedeniyle kullanımdan çıkan veya arızalanan elektronik mali mühür oluşturma aracı ve/veya elektronik mali mühür oluşturma aracı okuyucusu için ücret iadesi veya bilabedel yenileme yapılmaz.

- Bu kapsamda geliştirilen yazılımların ve akıllı kartların tüm fikri ve sınai mülkiyet hakları TÜBİTAK UEKAE'ye aittir.

9.6.2. Kayıt Birimi Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.6.3. Sertifika Sahibinin Yükümlülükleri

Sertifika sorumlusunun yükümlülükleri şunlardır:

- Yukarıda sayılan koşullar çerçevesinde hizmet verecek Kamu Sertifikasyon Merkezi tarafından teslim edilecek olan elektronik mali mühür oluşturma aracını ve elektronik mali mühür oluşturma verisini GİB tarafından yapılan düzenlemeler ve Kamu SM yönergeleri ile Maliye Bakanlığı'nca yayımlanan 05/03/2010 tarih 27512 sayılı Vergi Usul Kanunu Genel Tebliği (Sıra No: 397) hükümleri,dışında kullanmayacağını,
- Başvuru sırasında kimliğini belgeleme ve doğrulama amacıyla gerek duyulabilecek kurumsal bilgi ve belgelerini tam ve doğru olarak beyan ettiğini; elektronik sertifikaların geçerlilik süresi boyunca bu bilgilerin güncelliğini temin edeceğini,
- Sertifikaların geçerlilik süresi boyunca; beyan edilen bilgilerde meydana gelen ve sertifika içerisinde yer alan bilgilerin değiştirilmesini gerektiren değişiklikleri derhal GİB'e ve/veya Kamu SM'ye bildireceğini,
- Elektronik mali mühür oluşturma aracının ve/veya erişim verisinin (PIN/PUK) kayıp olmaması, açığa çıkmaması, değiştirilmemesi ve üçüncü kişilerin yetkisiz kulanımının engellenmesi için gerekli tedbirleri alacağını,
- Elektronik mali mühür oluşturma aracının ve/veya erişim verisinin kayıp edilmesi, unutulması veya üçüncü kişilerin eline geçmesi durumunda, Kamu SM'ye ve/veya GİB'e iptal talebinde bulunacağını,
- Kullanıma açılmamış (askıda), kullanım süresinin sonuna gelmiş veya iptal olmuş elektronik sertifikalar ile herhangi bir işlem gerçekleştirmeyeceğini,
- Hizmet kesintisinin yaşanmaması için oluşturulan, yedek elektronik mali mühür oluşturma aracını, sadece asıl elektronik mali mühür oluşturma aracının kullanım dışı kalması durumuda kullanacağını,
- Elektronik sertifikaların, GİB tarafından yapılan düzenlemeler ve Kamu SM yönergelerine uygun olarak kullanılmadığının tespit edilmesi durumunda; elektronik sertifikaların res'en iptal edileceğini,

kabul ve taahhüt eder. Yükümlülüklerin ihlali nedeniyle üçüncü kişilerin zarara uğraması halinde TÜBİTAK'ın ödemek zorunda olduğu tazminatlarla ilgili sertifika sahibine rücu hakkı saklıdır.

9.6.4. Üçüncü Kişilerin Yükümlülükleri

Üçüncü kişiler, sertifikalarla ilgili işlem yapmadan önce sertifikanın aşağıda belirtilen geçerlilik kontrollerini yapmakla yükümlüdür:

- Sertifikanın, tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek,
- Sertifikanın geçerliliğini SİL veya ÇİSDUP Yanıtlayıcı aracılığıyla kontrol etmek,

- SİL veya ÇİSDUP Yanıtlayıcı'dan aldığı iptal durum kaydının bütünlüğünü Kamu SM'nin ilgili sertifikalarının içinde mevcut olan imza doğrulama verilerini kullanarak doğrulamak,
- Sertifikanın doğruluğunu Kamu SM alt kök sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu SM alt kök sertifikasının doğruluğunu kök sertifikasının içinde mevcut olan imza doğrulama verisini kullanarak doğrulamak,
- Kamu SM kök sertifikasının doğruluğunu sertifika özet değerini kontrol etmek suretiyle doğrulamak,
- Sertifika sahibinin sertifikasının içindeki imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğunu doğrulamak.

9.6.5. Diğer Bileşenlerin Yükümlülükleri

Düzenlenmesine gerek duyulmamıştır.

9.7. Yükümlülüklerden Feragat

Kamu SM ile sertifika sahibi arasındaki yükümlülük, Elektronik Mali Mühür Sertifika Sahibi Taahhütnamesi'ndebelirtildiği şekilde sona erer.

9.8. Sorumlulukla İlgili Sınırlamalar

Kamu SM ve sertifika hizmetlerini alan tarafların sorumlulukları ilgili sınırlamalar Elektronik Mali Mühür Sertifika Sahibi Taahhütnamesi ve Elektronik Mali Mühür Sertifika İlkeleri ve Uygulama Esasları dökümanında belirlenir.

9.9. Tazminat Halleri

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

9.10. Anlaşma Süresi ve Anlaşmanın Sona Ermesi

Maliye Bakanlığı'nın yayınladığı 05/03/2010 tarih 27512 sayılı Vergi Usul Kanunu Genel Tebliğ (Sıra No:397) ve GİB ile TÜBİTAK-UEKAE arasında imzalanan protokol gereğince; GİB'in bildirdiği/uygun gördüğü tüm vergi mükelleflerine MÜS ve GÜS üretilmektedir.

TÜBİTAK-UEKAE vergi mükellefleri ile herhangi bir sözleşme imzalamamaktadır.

9.10.1. Anlaşma Süresi

Düzenlenmesine gerek duyulmamıştır.

9.10.2. Anlaşmanın Sona Ermesi

Düzenlenmesine gerek duyulmamıştır.

9.10.3. Anlaşmanın Sona Ermesinin Etkileri

Düzenlenmesine gerek duyulmamıştır.

9.11. Sistem Bileşenleri İle Haberleşme ve Kişisel Bilgilendirme

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

9.12. Değişiklik Halleri

9.12.1. Değişiklik Metodları

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

9.12.2. Bilgilendirme Mekanizması ve Sıklığı

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

9.12.3. Nesne Tanımlama Numarasının Değişmesini Gerektiren Durumlar

Düzenlenmesine gerek duyulmamıştır.

9.13. Anlaşmazlık Halleri

Düzenlenmesine gerek duyulmamıştır.

9.14. Uygulanacak Hukuk

Düzenlenmesine gerek duyulmamıştır.

9.15. Uygulanabilir Yasalarla Uyum

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

9.16. Diğer Hükümler

Düzenlenmesine gerek duyulmamıştır.

EK-A Sertifika Biçimleri

a) KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1

Alan	**Değer**
Sürüm	V3
Seri Numarası	02
İmza Algoritması	sha-256 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	12 Kasım 2009 Perşembe 12:29:14
Geçerlilik Sonu	12 Kasım 2030 Salı 12:29:14
Konu	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 81 e9 0f 46 16 9a 36 55 bd 48 49 a5 96 cf 92 fa d6 89 82 32
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama , Çevrimdışı SİL İmzalama, SİL İmzalama
Temel Kısıtlamalar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=Yok

b) Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1

Alan	**Değer**
Sürüm	V3
Seri Numarası	00 b6 e1 3c 1e 29
İmza Algoritması	sha256 ile RSA {1 2 840 113549 1 1 5}
Sertifikayı Veren	CN = KamuSM Kurumsal Kök Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Kamu Sertifikasyon Merkezi OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK L = Gebze - Kocaeli C = TR
Geçerlilik Başlangıcı	13 Kasım 2009 Cuma 14:36:09
Geçerlilik Sonu	11 Kasım 2019 Pazartesi 14:36:09
Konu	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1 C = TR
Ortak Anahtar	2048 bit RSA {1 2 840 113549 1 1 1}
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 81 e9 0f 46 16 9a 36 55 bd 48 49 a5 96 cf 92 fa d6 89 82 32
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; 46 20 a9 53 1b 28 0c 1c ae f2 28 51 83 b3 1e be f2 53 14 7c
Anahtar Kullanımı	**Kritik=Evet**; Sertifika İmzalama , Çevrimdışı Sil İmzalama, Sil İmzalama
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=CA; Yol Uzunluğu Kısıtlaması=0
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı=2.16.792.1.2.1.1.5.7.4.1 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici=http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni=Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
CRL Dağıtım Noktaları	[1]CRL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL=http://depo.kamusm.gov.tr/kurumsal/kurumsal-s1.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL=http://depo.kamusm.gov.tr/kurumsal/kurumsal-s1.crt

c) Güvenlik Hizmetleri Sertifikası (GÜS)

Alan	Değer
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-256 ile RSA
Sertifikayı Veren	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1 OU = Şube adı/ünvanı C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Sertifika sahibi adı/ünvanı OU = Şube adı/ünvanıSERIALNUMBER = Vergi kimlik numarası
Ortak Anahtar	2048 bit RSA
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 46 20 a9 53 1b 28 0c 1c ae f2 28 51 83 b3 1e be f2 53 14 7c
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-256 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Anahtar Anlaşması, Anahtar Şifreleme
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.4.1 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni= Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
Gelişmiş Anahtar Kullanımı	İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s1.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s1.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü(1.3.6.1.5.5.7.48.1) Diğer Ad: URL= http://cisdupmms1.kurumsal.kamusm.gov.tr

d) Mali Mühür Sertifikası (MÜS)

Alan	Değer
Sürüm	V3
Seri Numarası	Eşsiz bir sayı
İmza Algoritması	sha-256 ile RSA

Sertifikayı Veren	CN = Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 1 C = TR
Geçerlilik Başlangıcı	Sertifika geçerlilik başlangıcı
Geçerlilik Sonu	Sertifika geçerlilik sonu
Konu	CN = Sertifika sahibi adı/ünvanı OU = Şube adı/ünvanı SERIALNUMBER = Vergi kimlik numarası
Ortak Anahtar	2048 bit RSA
Uzantılar	**Değer**
Yetkili Anahtarı Tanımlayıcısı	Kritik=Hayır; 46 20 a9 53 1b 28 0c 1c ae f2 28 51 83 b3 1e be f2 53 14 7c
Konu Anahtarı Tanımlayıcısı	Kritik=Hayır; Sertifikanın içeriğindeki "subjectPublicKey" alanının "BIT STRING" olarak değerinin SHA-256 özet çıktısından oluşur.
Anahtar Kullanımı	**Kritik=Evet**; Dijital imza
Temel Kısıtlar	**Kritik=Evet**; Konu Türü=Son Varlık; Yol Uzunluğu Kısıtlaması=Yok
Sertifika İlkeleri	[1]Sertifika İlkesi: İlke Tanımlayıcısı= 2.16.792.1.2.1.1.5.7.4.1 [1,1]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=CPS Niteleyici= http://depo.kamusm.gov.tr/ilke [1,2]İlke Niteleyicisi Bilgisi: İlke Niteleyicisi Kimliği=Kullanıcı Uyarısı Niteleyici= Uyarı Metni= Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen web sitesini ziyaret ediniz.
Gelişmiş Anahtar Kullanımı	İstemci Kimlik Doğrulaması (1.3.6.1.5.5.7.3.2)
SİL Dağıtım Noktaları	[1]SİL Dağıtım Noktası Dağıtım Noktası Adı: Tam Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s1.crl
Yetkili Bilgi Erişimi	[1]Yetkili Bilgi Erişimi Erişim Yöntemi=Sertifika Yetkilisi Yayımcısı(1.3.6.1.5.5.7.48.2) Diğer Ad: URL= http://depo.kamusm.gov.tr/kurumsal/mmeshs-s1.crt [2]Yetkili Bilgi Erişimi Erişim Yöntemi=Çevrimiçi Sertifika Durum Protokolü(1.3.6.1.5.5.7.48.1) Diğer Ad: URL= http://cisdupmms1.kurumsal.kamusm.gov.tr