

SPK SERTİFİKA HİZMETLERİ

SERTİFİKA UYGULAMA ESASLARI

Sürüm 1.4

Aralık 2006



Sermaye Piyasası Kurulu



Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

Uzay Teknolojileri Araştırma Enstitüsü

İÇİNDEKİLER

KISALTMALAR.....	7
TANIMLAR	8
1 KAPSAM.....	9
1.1 Genel Bakış.....	9
1.2 Tanımlama	9
1.3 Sistem Bileşenleri ve Uygulanabilirlik.....	10
1.3.1 Sertifika Yönetim Birimi	10
1.3.2 Sertifika Kayıt Birimi	10
1.3.3 Son Kullanıcılar	10
1.3.4 Bilgi Deposu	11
1.3.5 Uygulanabilirlik	11
1.4 İletişim Bilgileri.....	11
2 GENEL HÜKÜMLER.....	12
2.1 Yükümlülükler	12
2.1.1 Sertifika Yönetim Birimi Yükümlülükleri.....	12
2.1.2 Sertifika Kayıt Birimi Yükümlülükleri.....	12
2.1.3 Sertifika Kullanıcısı Yükümlülükleri.....	13
2.1.4 Güvenen Taraf Yükümlülükleri.....	14
2.1.5 Bilgi Deposu Yükümlülükleri.....	14
2.2 Sorumluluklar	14
2.2.1 Sertifika Yönetim Birimi Sorumlulukları	15
2.2.2 Sertifika Kayıt Birimi Sorumlulukları	15
2.2.3 Sertifika Kullanıcısı Sorumlulukları.....	15
2.2.4 Güvenen Taraf Sorumlulukları	15
2.3 Hukuksal Sorumluluk	15
2.4 Yürütme	15
2.5 Ücretler	16
2.6 Yayınlama ve Bilgi Deposu.....	16
2.6.1 Sertifika Hizmet Sağlayıcısı'nın Yayınları.....	16
2.6.2 Yayın Sıklığı	16
2.6.3 Erişim Kontrolleri	16
2.6.4 Bilgi Depoları.....	16
2.7 Gizlilik	17

2.7.1	Gizli Tutulması Gereken Bilgiler.....	17
2.7.2	Gizli Tutulması Gerekmeyen Bilgiler.....	17
2.8	Fikri Mülkiyet Hakları	17
3	KİMLİK TANIMLAMA VE DOĞRULAMA.....	18
3.1	İlk Kayıt	18
3.1.1	İsim Tipleri.....	18
3.1.2	İsimlerin Anlamli Olması Gerekliliđi	18
3.1.3	İsim Alanı İçinde Bulunan Bilgiler.....	18
3.1.4	İsimlerin Benzersizliđi	18
3.1.5	Gizli Anahtara Sahip Olmanın Kanıtlanması	18
3.1.6	Kurumsal Kimliđin Doğrulanması.....	18
3.1.7	Kişisel Kimliđin Doğrulanması	19
3.2	Sertifika Sürdürülebilirlik ve Anahtar Yenileme	19
3.2.1	Sertifika Sürdürülebilirlik	19
3.2.2	Anahtar Yenileme	19
3.3	Sertifika Askıya Alma.....	19
3.4	Sertifika İptali	20
3.5	İptal Sonrası Yeni Sertifika Çıkarılması.....	20
4	İŞLEVSEL GEREKLİLİKLER.....	21
4.1	Sertifika Başvurusu.....	21
4.2	Sertifika Dağıtımı.....	21
4.2.1	Kullanıcı Sertifikalarının Dağıtımı	21
4.2.2	Kök ve Alt Kök Sertifikalarının Dağıtımı	21
4.3	Sertifikanın Teslim Alınması ve Kullanıma Açılması.....	22
4.4	Sertifikanın İptali ve Askıya Alınması	22
4.4.1	İptali Gerektiren Durumlar	22
4.4.2	İptal İsteminde Bulunabilecek Kişiler	22
4.4.3	İptal İstek Prosedürü	23
4.4.4	Askıya Almayı Gerektiren Durumlar.....	23
4.4.5	Askıya Alma İsteminde Bulunabilecek Kişiler.....	23
4.4.6	Askıya Alma İstek Prosedürü	23
4.4.7	Sertifika İptal Listesi Yayımlama Sıklığı	24
4.4.8	Sertifika İptallerinin Yayımlandığı Adres	24
4.4.9	Güvenen Tarafların Sertifika İptal Listesi Kontrol Gerekliliđi.....	24

4.4.10	Çevrim İçi Sertifika Durum Protokolü Desteği	24
4.5	Güvenlik Denetimi	24
4.5.1	Kaydedilen İşlemler	24
4.5.2	Kayıtların Tutulma Süresi	25
4.5.3	Kayıtların Korunması	25
4.6	Kayıt Arşivleme	25
4.6.1	Arşivlenen Kayıt Bilgileri	25
4.6.2	Arşivlerin Tutulma Süresi	26
4.6.3	Arşivlerin Korunması	26
4.7	Anahtar Değişimi	26
4.8	Güvenilirliğin Yitirilmesi ve Mücbir Sebep Durumlarında Yapılacaklar	26
4.9	Sertifika Hizmetlerine Son Verilmesi	26
5	FİZİKSEL, PROSEDÜREL VE PERSONEL GÜVENLİK KONTROLLERİ	27
5.1	Fiziksel Kontroller	27
5.1.1	Tesis Yeri ve İnşaatı	27
5.1.2	Fiziksel Erişim	27
5.1.3	Güç Kaynağı	27
5.1.4	Saklama ve Yedekleme Ortamlarının Korunması	27
5.2	Prosedürel Kontroller	27
5.2.1	Güvenilir Roller	27
5.2.2	Rollerin Ayrılması	28
5.2.3	Kimlik Doğrulama ve Yetkilendirme	28
5.3	Personel Kontrolleri	28
5.3.1	Kişisel Geçmiş, Nitelik ve Deneyim Gereklilikleri	28
5.3.2	Eğitim Gereklilikleri	28
5.3.3	Personele Sağlanacak Dokümantasyon	28
6	TEKNİK GÜVENLİK KONTROLLERİ	29
6.1	Anahtar Çifti Üretimi ve Kurulumu	29
6.1.1	Kök ve Alt Kök Sertifika Anahtar Çifti Üretimi	29
6.1.2	Kullanıcıya Gizli Anahtarın Ulaştırılması	29
6.1.3	Kök Sertifikalarına Taraflarca Erişimin Sağlanması	29
6.1.4	Anahtar Uzunlukları	29
6.1.5	Kullanıcı Anahtar Üretimi	29
6.1.6	Anahtar Kullanım Amaçları	29

6.2	Gizli Anahtarın Korunması.....	29
6.2.1	Kriptografik Modül Standartları	29
6.2.2	Gizli Anahtarın Saklanması	29
6.2.3	Gizli Anahtarın Yedeklenmesi.....	30
6.2.4	Gizli Anahtara Erişim Metodu.....	30
6.2.5	Gizli Anahtara Erişimin Kesilme Metodu	30
6.2.6	Gizli Anahtarın Yok Edilmesi	30
6.3	Anahtar Çifti Yönetimi ile İlgili Diğer Konular	30
6.3.1	Açık Anahtarın Arşivlenmesi	30
6.3.2	Açık ve Gizli Anahtarın Kullanım Süreleri	30
6.4	Erişim Şifreleri.....	30
6.4.1	Erişim Şifrelerinin Üretimi	30
6.4.2	Erişim Şifrelerinin Korunması.....	31
6.5	Bilgisayar Güvenlik Kontrolleri	31
6.6	Yaşam Döngüsü Teknik Kontrolleri.....	31
6.6.1	Güvenlik Yönetimi Kontrolleri.....	31
6.7	Ağ Güvenlik Kontrolleri.....	31
7	SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ PROFİLLERİ.....	32
7.1	Sertifika Profili.....	32
7.1.1	Sürüm Numarası	32
7.1.2	Sertifika Uzantıları.....	32
7.1.3	Algoritma Nesne Tanımlayıcıları	32
7.1.4	İsim Biçimleri	32
7.1.5	İsim Kısıtları	32
7.2	Sertifika İptal Listesi Profili.....	32
8	DOKÜMAN YÖNETİMİ.....	34
8.1	Doküman Değişim Prosedürleri.....	34
8.2	Yayın ve Duyuru Politikaları.....	34
8.3	Sertifika Uygulama Esasları Onay Prosedürleri	34
	SERTİFİKA SAHİBİ TAAHHÜTNAMESİ	35

KISALTMALAR

PKI : Açık Anahtarlı Altyapı (Public Key Infrastructure)

SİL : Sertifika İptal Listesi

OCSP : Çevrim içi Sertifika Durum Protokolü (Online Certificate Status Protokol)

Sİ : Sertifika İlkeleri

SUE : Sertifika Uygulama Esasları

IETF : Internet Engineering Task Force

TANIMLAR

Sertifika Hizmet Sağlayıcısı	Elektronik sertifika ile ilgili üretim, yönetim, yenileme, sürdürülebilirlik ve iptal etme işlemlerini yerine getirmekle yetkili gerçek veya tüzel kişiler
Sertifika Yönetim Birimi	Sertifika Hizmet Sağlayıcısı içinde, temel görevi üretilen sertifikaları ve sertifika iptal listelerini elektronik olarak imzalamak olan birim
Sertifika Kayıt Birimi	Sertifika Hizmet Sağlayıcısı içinde, sertifika üretim, yenileme, sürdürülebilirlik ve iptal başvurularını alan, kimlik doğrulaması, belgelerin kontrolü gibi hizmetleri yerine getiren birim
Gizli Anahtar (İmza Oluşturma Verisi)	Sertifika sahibine ait olan, sertifika sahibi tarafından elektronik imza oluşturma ve kendisine gönderilen şifreli mesajları çözme amacıyla kullanılan, bir eşi daha olmayan kriptografik gizli veri
Açık Anahtar (İmza Doğrulama Verisi)	Sertifika sahibine ait, fakat kamuya açık olan, sertifika sahibi tarafından atılmış elektronik imzayı doğrulamak ve sertifika sahibine şifreli mesaj göndermek için kullanılan, bir eşi daha olmayan, sertifikanın içinde mevcut bulunan kriptografik, gizli tutulması gerekmeyen veri
Sertifika	Gizli ve açık anahtar sahibinin açık anahtar verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt
Kök Sertifika	Sertifika Yönetim Birimi içinde oluşturulmuş ve en yetkili imza derecesi verilmiş olan kendi imzasını taşıyan sertifika
Alt Kök Sertifika	Sertifika Yönetim Birimi içinde kullanıcı sertifikalarını imzalama yetkisi verilmiş, kök sertifikanın imzasını taşıyan sertifika
Açık Anahtarlı Altyapılar (PKI)	Her kullanıcıya iki anahtar verilerek uygulanan, temelleri kriptoloji bilimine dayanan elektronik ortamda güvenliği sağlama yöntemlerinden birisi
PKI Uygulama Sistemi	Sertifika Hizmet Sağlayıcısı tarafından verilen sertifikalar kullanılarak, bilgi güvenliğinin PKI çözümleri ile sağlandığı uygulama ortamı
Sertifika İptal Listesi	İptal edilen sertifikaların kamuya duyurulması amacıyla oluşturulmuş, iptal edilen sertifika bilgilerinin tutulduğu, sertifikaları imzalayan alt kök sertifikanın imzasını taşıyan elektronik dosya
Çevrim içi Sertifika Durum Protokolü (OCSP)	Sertifikanın geçerlilik durumunun kamuya duyurulması için oluşturulmuş, ilgili sertifikanın geçerli veya iptal konumunda olduğu bilgisinin çevrim içi yöntemle alınmasını sağlayan standart protokol

1 KAPSAM

Bu doküman, SPK-İMKB KAP (Kamuyu Aydınlatma Projesi) kapsamındaki PKI (Public Key Infrastructure-Açık Anahtarlı Altyapılar) Uygulama Sistemi içinde çalışan Sertifika Hizmet Sağlayıcısı'nın sertifika üretim ve yönetimi işlemlerinde uyguladığı esasları belirlemek amacıyla hazırlanmış Sertifika Uygulama Esasları (SUE) dokümanıdır. 09.10.2003 tarih ve 52/1223 sayılı SPK İlke Kararı'yla çıkarılan "Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Gönderilmesine İlişkin Uygulama Esaslarının" 8. maddesine istinaden hazırlanmıştır.

SUE dokümanı, SPK'nın belirlediği, kullanımı İlke Kararı'nın 2. maddesinde belirtilen "elektronik imzanın kullanım alanları" ile sınırlandırılmış olan sertifikaları üreten Sertifika Hizmet Sağlayıcısı içinde yer alan sistem bileşenlerinin rollerini, sorumluluklarını ve ilişkilerini tanımlar, sertifikaların üretim ve yönetimi sırasında yapılan işlemlerin hangi ortamlarda ve ne şekilde yürütüldüğünü SPK Sertifika İlkeleri (Sİ) dokümanına bağlı olarak detaylandırarak anlatır.

Sertifika Hizmet Sağlayıcısı tarafından üretilen sertifikalar SPK-İMKB'nin kendi işleyişinde kullandığı PKI Uygulama Sistemi çerçevesinde ilgili kişilere verilir. Sertifika Hizmet Sağlayıcısı'ndan sertifika alacak ve kullanacak her kişi bu dokümanda belirtilen şartlar çerçevesinde sertifikasını kullanmayı kabul etmiş sayılır. Bununla ilgili kullanıcı taahhütnamesi bu dokümanın sonundaki ekte verilmektedir.

SUE dokümanı herkesin erişimine açık bulunan aşağıdaki web adresinden yayımlanmaktadır:

http://kap.bilten.tubitak.gov.tr/SiSue/SPK_SUE.pdf

Gerektiğinde bu SUE dokümanında değişiklik yapılabilir. Bu tür değişiklikler SPK'nın tasarrufundadır.

Sertifika başvuru, üretim, dağıtım ve iptali sırasında izlenen süreçler ile ilgili usul ve ayrıntılar, "SPK-İMKB Sertifika Yönetim Prosedürleri" dokümanında verilmektedir.

Sertifika Hizmet Sağlayıcısı işlevleri SPK, İMKB ve TÜBİTAK UZAY arasında 09.09.2002 tarihinde imzalanan "SPK-İMKB Kamuyu Aydınlatma Projesi" sözleşmesi gereğince TÜBİTAK UZAY tarafından yürütülmektedir.

1.1 Genel Bakış

SUE dokümanı, sertifika başvuru, üretim, yönetim ve iptal etme ile ilgili süreçler içinde yapılan işlemlerin Sertifika İlkeleri (Sİ) dokümanında belirlenen kurallar çerçevesinde nasıl yürütüldüğünü anlatır.

SUE dokümanı, "IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527)" referans alınarak hazırlanmıştır.

1.2 Tanımlama

Doküman başlığı:

"SPK Sertifika Hizmetleri-Sertifika Uygulama Esasları (SUE)"

Doküman sürüm numarası:

1.4

Dokümanın tarihi:

Aralık 2006

1.3 Sistem Bileşenleri ve Uygulanabilirlik

PKI Uygulama Sistemi içinde yer alan bileşenler şunlardır:

- Sertifika Hizmet Sağlayıcısı
 - Sertifika Yönetim Birimi
 - Sertifika Kayıt Birimi
- Son Kullanıcılar
 - Sertifika Sahipleri
 - Güvenen Taraflar

1.3.1 Sertifika Yönetim Birimi

Sertifika Hizmet Sağlayıcısı içinde tanımlı bir birim olan Sertifika Yönetim Birimi'nin görevi, SPK'nın belirlediği ilke ve uygulama esaslarına bağlı olarak sertifika üretmek, üretilen sertifikaları kendi bünyesinde oluşturduğu kök veya alt kök sertifikaya ait gizli anahtarla (imza oluşturma verisi) elektronik olarak imzalamak, yayımlamak, iptal etmek, iptal listelerini oluşturup yayımlamak ve ilgili her türlü sertifika yönetim işlemini "SPK-İMKB Sertifika Yönetim Prosedürleri" usulünce yürütmektir.

PKI Uygulama Sistemi içinde Sertifika Yönetim Birimi TÜBİTAK UZAY'dır.

1.3.2 Sertifika Kayıt Birimi

Sertifika Hizmet Sağlayıcısı içinde tanımlı bir birim olan Sertifika Kayıt Birimi'nin görevi, "SPK-İMKB Sertifika Yönetim Prosedürleri" usulünce sertifika verilecek kullanıcıların başvurularını, kimlik bilgileri ve ilgili resmi belgeleri toplamak ve doğrulamak suretiyle onaylamak, iptal ve yenileme/sürdürülebilirlik isteklerini alıp değerlendirmek, onaylanan sertifika başvuru ve iptal isteklerini Yönetim Birimi'ne aktarmaktır.

PKI Uygulama Sistemi içinde Sertifika Kayıt Birimi TÜBİTAK UZAY'dır.

1.3.3 Son Kullanıcılar

Sertifika Sahipleri

Sertifika sahipleri kendi adlarına düzenlenmiş olan sertifikalarını, Sİ ve SUE dokümanlarına uygun olarak PKI Uygulama Sistemi kapsamında kullanan, SPK ve İMKB ile diğer kurum, şirket, aracı kurum veya bağımsız denetim şirketi yetkililerinden oluşan kişilerdir.

Güvenen Taraflar

Güvenen taraflar PKI Uygulama Sistemi içindeki kullanıcılara ait sertifikaları kabul edip uygulamada kullanırlar. Uygulamaya aldıkları sertifikaların geçerliliğini kontrol edip etmemek güvenen tarafların kendi inisiyatifindedir. Güvenen taraflar sertifikaları, kendilerine iletilen bir mesajın bütünlüğünü ve gönderenin kimliğini doğrulamak veya sertifika sahibi ile güvenli ve Kurul İlke Kararının 2. maddesinde belirtilen kullanım alanları ile sınırlı olarak gizli iletişim sağlamak için kullanabilirler. Güvenen taraflar, sertifikaların bağlı bulunduğu SUE dokümanına dayanarak, sertifikanın belli bir uygulama için kullanımının uygun olup olmadığına karar verebilirler.

PKI Uygulama Sistemi içinde bildirimlerin elektronik olarak imzalanmasını sağlamak ve elektronik imzalı bildirimlerin imzalarının doğrulanması işlemlerini yapmak suretiyle

güvenen taraf SPK ve İMKB'dir. Bildirimler üzerindeki elektronik imzaların doğrulanması işlemlerini yapan bağımsız denetim şirketleri ile yatırımcı ve internet kullanıcıları da güvenen taraf olarak PKI Uygulama Sistemi içinde yer almaktadır.

1.3.4 Bilgi Deposu

Üretilen sertifikalar, sertifika iptal listeleri ve ilgili dokümanlar son kullanıcıların erişebileceği bir şekilde <http://kap.bilten.tubitak.gov.tr> web adresi üzerinden sürekli ve kesintisiz olarak yayımlanır.

1.3.5 Uygulanabilirlik

PKI Uygulama Sistemi kapsamında şirket veya kurum yetkilileri sertifikalarını sertifikanın içeriğinde adı geçen şirket veya kurum adına kullanacaktır.

Şirket, aracı kurum ve diğer kurumlar ile bağımsız denetim şirketi yetkililerine dağıtılacak sertifikalar PKI Uygulama Sistemi içinde şu amaçlar doğrultusunda kullanılacaktır:

- Bildirimlerin web ortamında gönderileceği güvenli sunucuya (Bildirim İşlemleri Yazılımı Sunucusu-BİY Sunucusu) erişim hakkının sağlanabilmesi,
- Bildirimlerin BİY Sunucusuna gönderilmeden önce elektronik olarak imzalanması.

SPK ve İMKB çalışanlarına dağıtılacak sertifikalar şu amaçlar doğrultusunda kullanılacaktır:

- Yazılım modüllerine erişim hakkının verilmesi,
- Kurulca hazırlanan bir mali tablo, özel durum açıklaması veya diğer tipinde bir bildirim şablonunun, onaylanması amacıyla elektronik olarak imzalanması,
- SPK ve İMKB duyurularının elektronik olarak imzalanması.

PKI Uygulama Sistemi içinde dağıtılan sertifikaların kullanım alanları ile ilgili ayrıntılar 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı'nın 2. maddesinde düzenlenmiştir.

1.4 İletişim Bilgileri

Uygulama Yönetim Merkezi

Bu SUE dokümanı, Sertifika Hizmet Sağlayıcısı tarafından hazırlanıp, SPK tarafından onaylanarak kamuya duyurulur. Sistem özellikleri SPK tarafından tanımlanır ve Sertifika Hizmet Sağlayıcısı tarafından uygulanır.

İletişim

Bu SUE dokümanının uygulanması ve ilgili yönetim politikaları hakkındaki sorular TÜBİTAK UZAY'in aşağıdaki erişim noktalarına yönlendirilebilir:

Adres : TÜBİTAK UZAY, ODTÜ, 06531, ANKARA

Tel. : 0 312 210 10 30

Faks : 0 312 210 18 24

URL : <http://kap.bilten.tubitak.gov.tr>

2 GENEL HÜKÜMLER

2.1 Yükümlülükler

Bu bölümde Sertifika Hizmet Sağlayıcısı'nın düzenli işleyebilmesi için, birbirleriyle karşılıklı ilişki içinde bulunan sistem bileşenlerinin yerine getirmesi gereken yükümlülükler belirtilmiştir.

2.1.1 Sertifika Yönetim Birimi Yükümlülükleri

Sertifika Yönetim Birimi, Sertifika Hizmet Sağlayıcısı'na bağlı olarak Sertifika İlke ve Uygulama Esaslarını Belirleyen Kurumun belirlediği ilke ve esaslara uygun olarak işletilir. Yükümlülükleri aşağıda belirtildiği gibidir:

- Kök ve alt kök için anahtar çifti üretmek ve tanımlamalarını yapıp sertifikalarını oluşturmak, bunları son kullanıcıların erişebileceği web ortamından yayımlamak,
- Başvurusu kabul edilmiş kişiler için sertifika üretip SPK adına sertifikaları imzalamak ve yayımlamak,
- Sertifika kullanıcıları için anahtar çifti üretmek,
- Sertifikaların kullanım alanlarını belirleyen sertifika yönergelerini oluşturmak,
- Gerektiğinde sertifika iptal işlemini gerçekleştirmek,
- İptal edilmiş sertifika bilgilerini bölüm 4.4.7'de belirtilen süreler içinde oluşturduğu sertifika iptal listelerini yayımlamak suretiyle veya OCSP (Online Certificate Status Protokol-Online Sertifika Durum Protokolü) Yanıtlayıcı aracılığıyla duyurmak,
- Sertifikaların ve sertifika iptal listelerinin taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak,
- Yayımlanan Sİ ve SUE dokümanları ile "Sertifika Kullanıcısı Taahhünamesine" uygun olmayan sertifika kullanımlarının tespit edilmesi durumunda ilgili sertifikayı iptal etmek,
- Sertifika kullanıcılarına ait elektronik veya kağıt ortamda tutulan bilgilerin korunması için gerekli önlemleri almak, bu bilgileri üçüncü kişilere mahkeme kararı olmaksızın vermemek,
- Sertifika üretim, yönetim ve iptali ile ilgili yapılan tüm işlemlerin kaydını almak,
- SPK-İMKB'nin belirlediği, sertifika almasında sakınca görülen kişilere sertifika vermemek,
- Kullanıcılara ait açık anahtarların içinde bulunduğu kullanıcı sertifikalarını herkesin erişimine açık ortamlardan yayımlamak.

2.1.2 Sertifika Kayıt Birimi Yükümlülükleri

Sertifika Kayıt Birimi, Sertifika Hizmet Sağlayıcısı'nın altında Sertifika Yönetim Birimi'ne bağlı olarak işletilir ve yükümlülükleri aşağıda belirtildiği gibidir:

- Şirket veya kurumlardan gelen sertifika başvurularını usulüne uygun biçimde kabul etmek ve başvuruda bulunan kişilerin belgeleri ile başvuru formlarını gerekli kontrollerden geçirmek suretiyle kimlik doğrulamalarını yapmak,

- Kendisine gelen sertifika başvurularını değerlendirerek, başvurunun geçersiz bulunması durumunda ilgili kişileri bilgilendirmek,
- Sertifika başvurusu geçerli bulunan kullanıcıların başvurularını sertifika üretilmek üzere Sertifika Yönetim Birimi'ne göndermek,
- Üretilen sertifikaları usulüne uygun ve güvenli yöntemle kullanıcılara teslim etmek,
- Sertifika sürdürülebilirlik ve sertifika askıya alma başvurularını usulüne uygun biçimde değerlendirmek,
- Sertifika iptal başvurularını usulüne uygun biçimde değerlendirerek iptali kabul edilen sertifikaları iptal edilmek üzere Sertifika Yönetim Birimi'ne bildirmek,
- Askıya alma başvurusu kabul edilen sertifikaları askıya alınmak üzere Sertifika Yönetim Birimi'ne bildirmek,
- İşleyişi sırasında kullanılan tüm bilgi, belge ve kayıtlar ile yapılan yazışmaları yasal düzenlemelerde gösterilen süreler boyunca saklamak,
- Sertifika kullanıcılarına ait elektronik veya kağıt ortamda tutulan bilgilerin korunması için gerekli tüm önlemleri almak.

2.1.3 Sertifika Kullanıcısı Yükümlülükleri

Şirket veya kurumlar içindeki sertifika kullanıcılarının yükümlülükleri aşağıda belirtildiği gibidir:

- Sertifika başvuru, yenileme/sürdürülebilirlik ve iptal işlemlerini usulüne uygun biçimde yerine getirmek,
- Sertifika başvurusu ile sürdürülebilirlik ve iptal işlemleri sırasında doğru bilgi beyan etmek,
- Adına düzenlenen, gizli anahtar (imza oluşturma verisi) bilgisinin içinde olduğu akıllı kart ve akıllı karta ait kapalı şifre zarfını şahsen teslim almak,
- İmza oluşturma verisinin güvenliğini sağlamak, kendisine ait imza oluşturma verisinin içinde bulunduğu akıllı kartın ve imza oluşturma verisi erişim şifresinin gizliliğini korumak,
- İmza oluşturma verisinin içinde bulunduğu akıllı kartın kaybolması, çalınması veya imza oluşturma verisinin gizliliğinin yitirildiğinden şüphelenmesi durumunda sertifikanın iptal edilmesi için Sertifika Hizmet Sağlayıcısı'na (TÜBİTAK UZAY) başvurmak,
- Çalıştığı şirket veya kurumdan ayrılması veya sertifikanın içeriğinde bulunan kimlik bilgilerinin değişmesi durumunda en kısa süre içinde sertifikanın iptal edilmesi için Sertifika Hizmet Sağlayıcısı'na başvurmak,
- Kendisine verilen sertifikayı Sİ ve SUE dokümanlarında belirtildiği biçimde, "Sertifika Kullanıcısı Taahhütnamesinde" yer alan taahhütleri yerine getirmek suretiyle kullanmak.

2.1.4 Güvenen Taraf Yükümlülükleri

PKI Uygulama Sistemi içinde güvenen taraf, sertifikaları kullanarak uygulamalarında güvenlik sağlayacak kurumlar olarak yine SPK ve İMKB'dir ve bu kapsamda yükümlülükleri aşağıda belirtildiği gibidir:

- Sertifikaların, içinde tanımlanan veriliş amacına uygun olarak kullanıldığını doğrulamak,
- Sertifikanın kullanım süresinin dolup dolmadığını kontrol etmek,
- Sertifikanın geçerliliğini sertifika iptal listesi veya OCSP Yanıtlayıcı aracılığıyla kontrol etmek,
- Sertifikayı veren kurumun güvenilirliğini sertifikayı elektronik olarak imzalayan alt kök sertifika ile kök sertifikanın geçerliliğini kontrol etmek suretiyle sağlamak,
- PKI Uygulama Sistemi içindeki elektronik imzalı bildirimlerin orijinallerini saklamak; imzalı bildirimlerin okunması, imzalarının doğrulanması için gerekli kriptografik yazılım veya donanımları imza doğrulamanın gerektirdiği süre sonuna kadar muhafaza etmek; gelişen teknoloji doğrultusunda kriptografik yazılım veya donanımda yapılabilecek yenilenme neticesinde, yeni sürümlerin eski sürümler kullanılarak atılmış olan elektronik imzaları doğrulamasında bir sorun yaşanmasını önlemek.

Bildirimler üzerindeki elektronik imzaların doğrulanması işlemlerini yapan bağımsız denetim şirketleri de güvenen taraf olarak PKI Uygulama Sistemi içinde aşağıdaki yükümlülükleri yerine getirir:

- Bildirimleri imzalamadan önce, üzerinde mevcut bulunan şirkete ait imzanın kim tarafından, hangi tarihte oluşturulduğu gibi bilgileri yazılım ekranından kontrol etmek,
- Bildirimleri imzalamadan önce bildirim üzerindeki şirkete ait imzanın geçerliliğini kontrol etmek (PKI Uygulama Sistemi içinde yer alan ilgili yazılım bu işlemi otomatik olarak gerçekleştirmektedir),
- Sertifikayı veren kurumun güvenilirliğini sertifikayı elektronik olarak imzalayan alt kök sertifika ile kök sertifikanın geçerliliğini kontrol etmek suretiyle sağlamak (PKI Uygulama Sistemi içinde yer alan ilgili yazılım bu işlemi otomatik olarak gerçekleştirmektedir).

2.1.5 Bilgi Deposu Yükümlülükleri

Sertifika Hizmet Sağlayıcısı, bilgi deposunda tutulan bilgilerin korunması, doğruluğu ve güncelliğinin sağlanması, yetkisiz kişilerin ilgili bilgi deposuna erişiminin engellenmesiyle yükümlüdür.

2.2 Sorumluluklar

Bu bölümde Sertifika Hizmet Sağlayıcısı işleyişi içinde birbirleriyle karşılıklı ilişki içinde bulunan sistem bileşenlerinin, yükümlü olduğu işlemleri usulünce yerine getirmekten dolayı aldığı sorumluluklar belirtilmiştir.

2.2.1 Sertifika Yönetim Birimi Sorumlulukları

Sertifika Yönetim Biriminin bu SUE, ilgili Sİ dokümanı, 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı ve konuya ilişkin diğer düzenlemelere aykırılık teşkil eden işlemlerinden doğan sorumluluğu, bu işlemlerle uygun illiyet bağı kurulabilecek zararlarla sınırlıdır. Sertifika Yönetim Birimi, işlemleri ile uygun illiyet bağı bulunmayan zararlardan sorumlu değildir.

Sertifika Yönetim Birimi, kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

2.2.2 Sertifika Kayıt Birimi Sorumlulukları

Sertifika Kayıt Biriminin bu SUE, ilgili Sİ dokümanı, 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı ve konuya ilişkin diğer düzenlemelere aykırılık teşkil eden işlemlerinden doğan sorumluluğu, bu işlemlerle uygun illiyet bağı kurulabilecek zararlarla sınırlıdır. Sertifika Kayıt Birimi, işlemleri ile uygun illiyet bağı bulunmayan zararlardan sorumlu değildir.

Sertifika Kayıt Birimi, kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

2.2.3 Sertifika Kullanıcısı Sorumlulukları

“Sertifika Sahibi Taahhünamesinde” belirtilen taahhütlerini yerine getirmekten, kendi gizli anahtarı kullanılarak sertifikanın geçerlilik süresi içinde oluşturulmuş tüm imzalar ve gizli anahtar kullanılarak yapılmış diğer işlemlerin getireceği sonuçlardan, başvuru sırasında beyan ettiği bilgilerin doğru olmasından, sertifikasını Sİ ve SUE dokümanları ile “Sertifika Sahibi Taahhünamesinde” belirtilen taahhütlere aykırı surette kullandığında uğrayacağı zararlardan kendisi sorumludur.

2.2.4 Güvenen Taraf Sorumlulukları

Bölüm 2.1.4’deki yükümlülükleri yerine getirmekten, aksi durumda göreceği zararlardan kendisi sorumludur.

2.3 Hukuksal Sorumluluk

SPK, elektronik sertifikaların 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı’nın 2. maddesinde belirtilen “elektronik imzanın kullanım alanları” dışındaki alanlarda kullanılmasından kaynaklanan zararlardan sorumlu değildir.

2.4 Yürütme

PKI Uygulama Sistemi’ne ait işlemler, 09.10.2003 tarih ve 52/1223 sayılı SPK İlke Kararı’yla çıkarılan “Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Gönderilmesine İlişkin Uygulama Esasları” ve 5070 sayılı Elektronik İmza Kanunu ve bu Kanuna dayanılarak çıkarılan tebliğ ve yönetmelikler çerçevesinde yürütülür.

PKI Uygulama Sistemi bileşenleri arasında çıkabilecek anlaşmazlıklarda, “Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Gönderilmesine İlişkin Uygulama Esasları”, SUE ve Sİ dokümanına başvurulur. Bu ilkeler ve uygulama dokümanlarının çözüme ulaştıramadığı durumlarda, anlaşmazlıkların çözümü için SPK yetkilidir.

Bu Sertifika Uygulama Esasları’nın tamamının geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybetse bile, diğer kısımları geçerliliğini korur ve uygulanır. Bu SUE

dokümanının güncellenmesi ile ilgili süreç bölüm 8’de “Doküman Yönetimi” başlığı altında anlatılmıştır.

2.5 Ücretler

Sertifika Hizmet Sağlayıcısı tarafından üretilen gizli anahtar ile sertifikanın içinde bulunduğu ve kullanıcıya teslim edilen donanım aracının bedeli sertifika kullanıcısı tarafından ödenecektir. Ödenecek bedelin miktarı ile ilgili bilgi <http://kap.bilten.tubitak.gov.tr> ana sayfasından duyurulmaktadır.

Ödemenin usulüne uygun biçimde yapılmaması durumunda kullanıcı için anahtar ve sertifika üretimi ya da donanım aracının teslimi yapılmayacaktır.

2.6 Yayınlama ve Bilgi Deposu

2.6.1 Sertifika Hizmet Sağlayıcısı’nın Yayınları

Sertifika Hizmet Sağlayıcısı’nın PKI Uygulama Sistemi bileşenlerinin erişimine açacağı bilgi deposunda sistemin iç işleyişi ile ilgili olanlar hariç olmak üzere aşağıdaki bilgiler bulunur:

- Sertifika Yönetim Birimi’ne ait kök ve alt kök sertifikalar,
- Bu dokümanda belirtilen ilkeler doğrultusunda Yayınlanan sertifikalar,
- SUE ve Sİ dokümanlarının kopyaları,
- Kullanıcı Taahhütnamesi,
- Sertifika Yönetim Prosedürleri ile ilgili formlar,
- Sertifika iptal listeleri.

2.6.2 Yayın Sıklığı

Sertifikalar üretildiği hafta içinde yayımlanır.

Kullanıcı Taahhütnamesi, Sertifika Yönetim Prosedürleri, SUE ve Sİ dokümanları, Sertifika Yönetim Birimi’ne ait kök ve alt kök sertifikaları güncellendikten hemen sonra yayımlanır.

Sertifika iptal listelerinin yayımlanma sıklığı bu dokümanda bölüm 4.4.7’de belirtilmektedir.

2.6.3 Erişim Kontrolleri

Sertifikalar, sertifika iptal listeleri, Kullanıcı Taahhütnamesi, SUE ve Sİ dokümanları, Sertifika Yönetim Birimi’ne ait kök ve alt kök sertifikalara erişim web üzerinden herkese açıktır. Sertifika Yönetim Prosedürleri ise sadece PKI Uygulama Sistemi içindeki bileşenlere dağıtılır.

Bilgi deposunun güncellenmesi sadece Sertifika Hizmet Sağlayıcısı’ndaki yetkili kişiler tarafından yapılmaktadır.

2.6.4 Bilgi Depoları

Sertifika Hizmet Sağlayıcısı bilgi deposu olarak aşağıdaki mekanizmaları kullanmaktadır:

- Kullanıcı Taahhütnamesi, SUE ve Sİ dokümanları, Sertifika Yönetim Birimi'ne ait kök ve alt kök sertifikaları, sertifika iptal listeleri Sertifika Hizmet Sağlayıcısı'nın ilgili web sitesi üzerinde tutulmaktadır, (Sertifika Yönetim Prosedürleri web sitesi üzerinden yayımlanmaz, PKI Uygulama Sistemi içindeki bileşenlere posta ile gönderilir.)
- Sertifika iptal listelerine alternatif olarak sertifikaların en güncel haliyle geçerlilik durumunun kontrolü web ortamından OCSP Yanıtlayıcısı üzerinden de yapılabilmektedir,
- Sertifikalar PKI Uygulama Sistemi'nin web üzerinden erişebileceği veri tabanlarında tutulacaktır.

2.7 Gizlilik

2.7.1 Gizli Tutulması Gereken Bilgiler

Sertifika başvurusu sırasında kimlik tanımlama ve doğrulama ile sertifika yönetim süreçleri içinde kullanılmak üzere toplanan ancak sertifikanın içinde yer almayan, kullanıcılara ve şirket/kurumlara ait bilgiler gizli tutulmaktadır. Bu bilgiler kişilere ait nüfus bilgileri, adres ve telefon numarası gibi erişim bilgilerini kapsar.

Sertifika Hizmet Sağlayıcısı içinde tanımlanmış olan kök ve alt kök sertifikalarına ait gizli anahtarlar kesinlikle üçüncü şahıslarla paylaşılmaz.

2.7.2 Gizli Tutulması Gerekmeyen Bilgiler

Sertifikalar, sertifika iptal listeleri, Sertifika Yönetim Prosedürleri, SUE ve Sİ dokümanları ile kullanıcı taahhütnamesi gizli tutulması gerekmeyen bilgilerdir.

2.8 Fikri Mülkiyet Hakları

Sertifika Hizmet Sağlayıcısı kapsamındaki tüm sertifikalar ve dokümanlar ile bu SUE dokümanına bağlı olarak geliştirilen tüm ürünlerin veya bilgilerin fikri mülkiyet hakları SPK'ya aittir.

3 KİMLİK TANIMLAMA VE DOĞRULAMA

3.1 İlk Kayıt

3.1.1 İsim Tipleri

Sertifika Hizmet Sağlayıcısı'nın ürettiği bütün sertifikalarda "ITU X.500 Distinguished Name (Ayırt edici isim)" biçimine uygun isim tipi kullanılır.

3.1.2 İsimlerin Anamlı Olması Gerekliliği

Sertifikalarda kullanılan isimlerin kişilerin resmi kayıtlarda geçen isimleri olması gerekmektedir. Takma ad kullanılması SPK sertifika ilkelerine aykırıdır.

Sertifikanın genel isim alanı içinde yazılı olan isim sertifika sahiplerinin nüfus cüzdanlarında, yabancı sertifika sahipleri için pasaportlarında yazan isim olmalıdır.

3.1.3 İsim Alanı İçinde Bulunan Bilgiler

Sertifikaların isim alanı içinde sertifika sahibine ait aşağıdaki bilgiler yer almaktadır:

- Adı, varsa ikinci adı, soyadı
- Çalıştığı kurum/şirketin ticari adı
- Çalıştığı şirket/kurum içindeki unvanı
- T.C. kimlik numarası
- Sertifikayı kullanma yetkisine işaret eden bir ibare
- Ülke bilgisi (tüm sertifikalar içinde TR olarak tanımlanmıştır)
- Müşteri numarası

3.1.4 İsimlerin Benzersizliği

Sertifika Hizmet Sağlayıcısı kapsamında dağıtılan sertifikaların isim alanları her kişi için ayırt edici niteliktedir. Farklı kişilere ait sertifikaların isim alanlarının birebir aynı olması engellenmektedir. Bunun sağlanabilmesi için sertifikaların isim alanında benzersiz bir sayı olduğu kabul edilen, sertifika sahibinin T.C. kimlik numarası yer almaktadır.

3.1.5 Gizli Anahtara Sahip Olmanın Kanıtlanması

PKI Uygulama Sistemi içinde anahtar çifti Sertifika Hizmet Sağlayıcısı tarafından üretildiğinden, doğru gizli anahtar dosyası ve gizli anahtar koruma şifresinin doğru kişiye teslim edildiğinden emin olunması kullanıcının gizli anahtara sahip olduğunun ispatı anlamına gelmektedir. Teslimatın bu şartları yerine getirmesi için bölüm 6.2'de belirtilen yöntemler uygulanır.

3.1.6 Kurumsal Kimliğin Doğrulanması

Sertifika Kayıt Birimi sertifika başvurusunda bulunan kişilerin bağlı buldukları kurum bilgilerini, yönetim kurulu karar yazısı veya yönetim kurulu karar yazısı ile atanan kişilerin onayladığı belgeler, gerekiyorsa noter onaylı olması istenen diğer belgeler aracılığı ile doğrular.

3.1.7 Kişisel Kimliğin Doğrulanması

Kişisel kimliklerin doğrulanması için izlenen sürecin içinde aşağıdaki şartların sağlanması gerekmektedir:

- Kişinin kimliği resmi kimlik belgelerine dayanılarak doğrulanır, gerektiğinde noter onaylı resmi kimlik suretleri istenebilir,
- Kurum veya şirket adına kullanılacak olan sertifikalarda kişinin kimlik bilgilerinin doğruluğu kurum veya şirket yetkilisi tarafından da ıslak imza ile imzalanarak onaylanmalıdır.

3.2 Sertifika Sürdürülebilirlik ve Anahtar Yenileme

3.2.1 Sertifika Sürdürülebilirlik

Uzun süre kullanılacak olan sertifikaların güvenliğinin sağlanması amacıyla sertifika sahibi Sertifika Hizmet Sağlayıcısı'nın belirlediği aralıklarla [yılıda 1 (bir) kere] sertifikasının içinde yer alan bilgilerin doğruluğunun devam ettiğini Sertifika Hizmet Sağlayıcısı'na yazılı ve onaylı olarak beyan etmelidir. Bu beyan sertifikanın kullanımına devam edilebilmesi için gerekli sürdürülebilirlik başvurusunun yapılması anlamına gelir. Sertifika Hizmet Sağlayıcısı'na yapılan sürdürülebilirlik başvurusunda gerekirse şirket/kurumda imza yetkisine sahip kişilerin de onay ve imzası aranabilir. Belirtilen sürelerde bu başvurunun alınmaması durumunda Sertifika Hizmet Sağlayıcısı ilgili sertifikayı askıya alarak kullanım dışı bırakır.

3.2.2 Anahtar Yenileme

Kullanım süresi içinde kimlik bilgilerinde veya sertifikanın içeriğinde değişiklik olması ya da gizli anahtarın güvenilirliğinin yitirilmesi gibi nedenlerden dolayı sertifikanın kullanılmaması durumlarında kullanıcı, anahtarlarını dolayısıyla sertifikasını yenileyebilir. Anahtarların yenilenebilmesi için öncelikle eski sertifikanın iptal edilmesi gerekir. Bu durumda, bu SUE dokümanında bölüm 3.4 ve bölüm 3.5'de anlatılan işlemler uygulanır.

Sertifika Hizmet Sağlayıcısı'nın kök veya alt kök anahtarlarının yenilenmesi durumunda Sertifika Hizmet Sağlayıcısı, SPK onayıyla bunu son kullanıcılara duyurur. Eski anahtar çifti kullanılarak imzalanmış olan kullanıcı sertifikalarının geçerliliğinin devam etmesi isteniyorsa, yeni anahtar çiftinin eski kök veya alt kök sertifika bilgilerini imzalamasıyla oluşturulan yeni bir sertifika yayımlanır. Eski anahtar çifti kullanılarak imzalanmış olan kullanıcı sertifikalarının geçerliliğinin devam etmesi istenmiyorsa, buradan verilmiş tüm sertifikalar iptal edilerek yenilenen kök veya alt kök sertifikayla imzalanmış yeni sertifikalar kullanıcılara dağıtılır.

3.3 Sertifika Askıya Alma

Sertifikanın askıya alınması geçici olarak iptal edilmesi ve gerektiğinde yeniden kullanıma açılabilmesi anlamını taşır. Sertifika Hizmet Sağlayıcısı kapsamında sertifika iptal işleminin hızlandırılabilmesi ve yanlılıkla iptali istenen sertifikaların yeniden kullanılabilmesi amacıyla sertifika askıya alma işlemi tanımlanmıştır.

Kullanıcı askıya alma talebini sadece kendisinin bildiği kullanıcı şifresi aracılığıyla web üzerinden veya telefonla gerçekleştirebilir.

Bölüm 3.4'de belirtilen sertifika iptal yönteminde iptal istek formunun geçersiz bulunması durumunda sertifika öncelikle askıya alınır, askıya alma talebinden itibaren 1 (bir) gün

içinde yetkili kişilerden sertifikanın iptal edilmesi için onaylı bir yazının gelmesi durumunda askıdaki sertifika iptal edilir. Yetkili kişiler iptal işlemini doğrulamayan onaylı bir yazıyı 1 (bir) gün içinde gönderirlerse askıdaki sertifika yeniden kullanıma açılır.

3.4 Sertifika İptali

Sertifika iptalinin güvenli bir şekilde gerçekleştirilebilmesi için, iptal isteği imzalı ve onaylı bir formla Sertifika Hizmet Sağlayıcısı'na bildirilir.

Sertifika iptal isteği kullanıcının kendisinden, çalıştığı kurum veya şirketten, gerekli görülen durumlarda SPK-İMKB yetkililerinden gelebileceği gibi Sertifika Hizmet Sağlayıcısı da gerektiğinde sertifikaları iptal yetkisine sahiptir.

3.5 İptal Sonrası Yeni Sertifika Çıkartılması

Sertifika herhangi bir nedenle iptal edildikten sonra, kullanıcının PKI Uygulama Sistemi içinde yer almaya devam etmesi durumunda, yeniden sertifika başvurusunda bulunması gerekir. Bu durumda kullanıcı adına yeni bir anahtar çifti üretilerek yeni bir sertifika düzenlenir.

4 İŞLEVSEL GEREKLİLİKLER

4.1 Sertifika Başvurusu

Sertifika başvurusu Kayıt Birimi'ne yapılır. SPK veya İMKB tarafından sertifika alması yasaklanan kişiler sertifika başvurusunda bulunamazlar. SPK veya İMKB tarafından sertifika alması yasaklanan kişilerin listesi SPK'nın <http://www.spk.gov.tr/hid/index.html?tur=imzayetkisikaldirilanlar> internet sitesi üzerinden yayımlanır. Kayıt Birimi, internet üzerinden yayımlanan bu listeyi kontrol eder ve listede olan kişilerin sertifika başvurusunu değerlendirmeye almaz.

Başvuruda bulunan kişi aşağıdaki şartları yerine getirir:

- Sertifika başvurusunda bulunan kişinin kimliğinin doğrulanabilmesi için başvuru sahibi resmi kimlik belgesinin noterden onaylanmış suretini getirir,
- Sertifika başvurusu kullanıcının kendisi, gerekiyorsa çalıştığı şirket veya kurum yetkilisi tarafından onaylanmış başvuru formu ile yapılır,
- Şirket veya kurumlar adına kullanılacak sertifikaların başvuru formlarına şirket/kurum imza sirküleri eklenir,
- Sertifika başvurusunun tamamlanıp sertifika üretim işlemine geçilebilmesi için, sertifika başvurusunda bulunan kişi Sertifika Hizmet Sağlayıcısı'nın belirlediği kullanıcı sorumluluklarını kabul ettiğini beyan eder. Bunu da SUE'nin ekinde yer alan "Kullanıcı Taahhünamesini" okuyup imzalamak suretiyle yapar,
- Geçerli bulunan her sertifika başvurusu için kullanıcı adına Sertifika Hizmet Sağlayıcısı tarafından bir anahtar çifti üretilir.

4.2 Sertifika Dağıtımı

4.2.1 Kullanıcı Sertifikalarının Dağıtımı

Sertifika Kayıt Birimi aldığı sertifika başvurularını değerlendirir ve geçerli olanları Sertifika Yönetim Birimi'ne gönderir.

Gizli ve açık anahtar çifti, başvuru sahibine kolaylık getirmesi açısından Sertifika Yönetim Birimi'nde başvuru sahibi adına oluşturulur. Bu durumda gizli anahtarın kopyası hiçbir şekilde Sertifika Hizmet Sağlayıcısı'nda tutulmaz. Gizli anahtar başvuru sahibine ulaştırılana kadar büyük bir titizlikle şifreli olarak saklanır. Açık anahtar ve sertifika içinde yer alacak başvuru bilgileri derlenerek sertifika oluşturulur. Sertifika ve gizli anahtar, gizli verilere erişimin şifreyle sağlandığı güvenli yazılım aracı içinde, gizli anahtar erişim şifresi ise kapalı bir zarfa basılı olarak kullanıcıya imza karşılığında teslim edilir. Gizli anahtar ve gizli anahtar erişim şifresinin tesliminin başvuru sahibine yapıldığından emin olunması bu dağıtım sisteminde güvenlik açısından en kritik noktadır.

4.2.2 Kök ve Alt Kök Sertifikalarının Dağıtımı

Güvenen tarafların sertifikaların geçerliliğini kontrol edebilmesi için sertifikayı imzalayan alt kök ve kök sertifikasına ihtiyaç vardır. Bu yüzden kök ve alt kök sertifikalarının herkesin erişimine açık ortamlarda yayımlanması gerekmektedir. Kök ve alt kök sertifikaların yayımlanması Sertifika Hizmet Sağlayıcısı'na ait olduğu bilinen güvenilir bir web sitesinden yapılır.

İlgili kök sertifikanın gerçekten Sertifika Hizmet Sağlayıcısı'na ait olduğundan emin olunabilmesi için sertifikanın parmakizi (sertifikanın özeti) olarak adlandırılan 15-20 basamaklı benzersiz rakam, bu rakamın oluşturulduğu algoritmanın da ne olduğu belirtilerek güvenilir yollardan SPK tarafından kamuya duyurulur.

4.3 Sertifikanın Teslim Alınması ve Kullanıma Açılması

Kullanıcı sertifika ve gizli anahtarını güvenli donanım aracı içinde, gizli anahtar erişim şifresini ise kapalı bir zarf içinde imza karşılığında teslim alır. Kullanıcının sertifika ve gizli anahtarını kullanabilmesi için, donanım aracı ve kapalı şifre zarfını aldığına dair imzasını taşıyan geri bildirim formunu Sertifika Hizmet Sağlayıcısı'na göndermesi gereklidir. Geçerli form Sertifika Hizmet Sağlayıcısı'nın eline geçtikten sonra sertifika aktif hale getirilecek, kullanıcı gizli anahtar ve sertifikasını kullanabilecektir. Kullanıcı halen kullanmakta olduğu sertifikanın kullanım süresinin dolması nedeniyle yeni başvuru yapmış ise yeni sertifikanın aktif hale getirilmesiyle birlikte önceden kullanmakta olduğu eski sertifikası otomatik olarak askıya alınır. Geçerli formun Sertifika Hizmet Sağlayıcısı tarafından belirtilen süre içinde [120 (yüziki) gün] gönderilmemesi durumunda yeni sertifika iptal edilir. Askıya alınan eski sertifika kullanım süresinin sonuna kadar askıda kalmaya devam eder.

4.4 Sertifikanın İptali ve Askıya Alınması

4.4.1 İptali Gerektiren Durumlar

Sertifikanın kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda sertifika iptal edilir ve artık kullanılamaz duruma gelir. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Gizli anahtarın kaybedilmesi, deşifre olması veya üçüncü kişilerin yetkisiz kullanımı tehlikesinin veya bu tehlikenin oluşmasına neden olabilecek şartların ortaya çıkması,
- Gizli anahtarın içinde bulunduğu donanım aracının kaybolması veya bozulması,
- Sertifika kullanıcısının 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı'nın 9. maddesinde belirtilen "elektronik sertifika tahsis edilmeyecek kimseler" listesine alınması,
- Kullanıcının, diğer olası nedenlerden ötürü sertifikayı kullanamayacak duruma gelmesi (görevden ayrılma, işyerinden ayrılma, sertifikanın Sİ ve SUE dokümanlarının gerekliliklerine aykırı olarak kullanılması, vb.),
- Sertifika içindeki kullanıcı bilgilerinde veya sertifikanın içeriğinde değişiklik olması,
- Sertifika Hizmet Sağlayıcısı'nın herhangi bir nedenle işleyişini durdurması.

İptal edilen sertifikalar sertifikanın geçerlilik süresinin sonuna kadar Sertifika İptal Listeleri ve OCSP Yanıtlayıcı aracılığıyla duyurulur.

4.4.2 İptal İsteminde Bulunabilecek Kişiler

Sertifika iptal isteği aşağıda belirtilen kişiler tarafından oluşturulabilir:

- Kullanıcının kendisi,
- Kullanıcının bağlı bulunduğu şirket veya kurum,

- İlgili SPK-İMKB yetkilileri,
- Sertifika Hizmet Sağlayıcısı yetkilileri.

4.4.3 İptal İstek Prosedürü

Yukarıda adı geçen Sertifika Hizmet Sağlayıcısı sistem bileşenleri sertifika iptal isteğinde bulunabilmek için iptal edilecek sertifikayı tanımlayan bilginin ve iptal sebebinin belirtildiği, üzerinde iptal isteminde bulunan kişinin imzası olan, geçerli bir formu Sertifika Hizmet Sağlayıcısı'na gönderir. Burada iptal isteğinde bulunan kişinin kimliğinin doğrulanabilmesi, sahte iptal isteklerinin engellenmesi açısından önem taşımaktadır. Bu şart iptal istek formunun üzerindeki ıslak imza ile sağlanır. Eğer gönderilen ıslak imzalı sertifika iptal istek formu Sertifika Hizmet Sağlayıcısı tarafından geçersiz bulunursa sertifika belli bir süreliğine askıya alınır. Böylece sahte veya yanlışlıkla yapılmış sertifika iptal taleplerinin önüne geçme imkanı tanınmış olduğu gibi, gerçek iptal isteklerinin de karşılanamama durumu engellenir. Belirlenen süre içinde sertifika askıya alma işlemi iptalle ya da sertifikanın yeniden kullanıma açılmasıyla sonuçlanır.

İptal edilen sertifika, iptal listesine alınır ve OCSP Yanıtlayıcıdan duyurulur.

Sertifika Hizmet Sağlayıcısı'na ait kök veya alt kök sertifikalardan birisi iptal edildiğinde, bu durum en geç iki saat içinde web sitesi üzerinden duyurulur ve ilgili taraflar aynı gün içinde yazıyla bilgilendirilir. Gerekliyse iptal olan sertifikaların imzasını taşıyan kullanıcı sertifikaları da iptal edilir ve kullanıcılar bilgilendirilir.

4.4.4 Askıya Almayı Gerektiren Durumlar

Sertifikanın askıya alınması geçici olarak kullanımının durdurulması anlamına gelmektedir. Askıya alma işleminin uygulanmasının sebebi hatalı ya da sahte iptal isteklerinden sonra sertifikanın yeniden kullanıma açılmasına imkan sağlamasıdır. Sertifikanın askıya alınma nedeni bölüm 4.4.1'de belirtilen iptal sebepleriyle aynıdır. Geçersiz olma ihtimali olan bir iptal isteği yürürlüğe konulmadan önce sertifika askıya alınır. Geçerli ve ıslak imzalı formun Sertifika Hizmet Sağlayıcısı'nın eline geçmesiyle sertifika iptal edilir.

4.4.5 Askıya Alma İsteminde Bulunabilecek Kişiler

Bölüm 4.4.2'de belirtilen kişiler tarafından gelen iptal talepleri doğrultusunda sertifikalar askıya alınır.

4.4.6 Askıya Alma İstek Prosedürü

Askıya alma işlemi aşağıda belirtilen şekillerde yapılabilir:

- Askıya alma isteğini sertifika kullanıcısının kendisi oluşturacaksa, Sertifika Hizmet Sağlayıcısı'nın ilgili web sitesi üzerinden kullanıcı adı ve şifresi ile askıya alma isteğini sisteme girer. Bu durumda askıya alma işlemi sistem tarafından otomatik olarak gerçekleştirilir. İlgili sertifikanın iptal edilmesi için kullanıcının usule uygun süre içinde geçerli bir sertifika iptal başvuru formunu Sertifika Hizmet Sağlayıcısına göndermesi gerekmektedir. Geçerli formun gönderilmemesi durumunda Sertifika Hizmet Sağlayıcısı kullanıcıya geri dönerek sertifikanın askıda olduğunu bildirir. Kullanıcının talebi doğrultusunda sertifika askıdan çıkarılarak yeniden kullanıma açılır veya iptal edilir.

- Kullanıcının bağlı olduğu şirket, kurum veya SPK-İMKB yetkilisinin sertifika iptali için gönderdiği formun geçersiz bulunması durumunda geçerli bir formun usule uygun süre içinde gelişine kadar Sertifika Hizmet Sağlayıcısı tarafından sertifika askıya alınır. Geçerli sertifika iptal başvuru formu veya sertifikanın yeniden kullanımına açımını talep eden yazı, 1 (bir) gün içinde gelmezse sertifikanın yeniden kullanıma açılma ihtimali ortadan kalkar.

4.4.7 Sertifika İptal Listesi Yayınlama Sıklığı

Sertifika Hizmet Sağlayıcısı tarafından yayımlanacak olan sertifika iptal listesi haftada en az bir kez, iptal edilen yeni sertifika ya da sertifikalar olması durumunda aynı gün ve en geç iki saat içinde güncellenerek yayımlanır.

Kök ve alt kök sertifikaların iptal edilmesi durumunda sertifika iptal listesi yayımlanmaz. Kök veya alt kök sertifikanın iptal edildiği bilgisi Sertifika Hizmet Sağlayıcısı web sayfasından en geç iki saat içinde duyurulur. İlgili taraflara da yazı ile bilgilendirme yapılır.

4.4.8 Sertifika İptallerinin Yayınlandığı Adres

İptal edilen sertifika bilgilerinin içinde bulunduğu SİL dosyası <http://kap.bilten.tubitak.gov.tr/spk.crl> web adresi üzerinden yayımlanmaktadır.

Kök veya alt kök sertifikanın iptal edilmesi durumunda yapılacak yazılı duyuru ise <http://kap.bilten.tubitak.gov.tr> ana sayfası üzerinden yapılır.

4.4.9 Güvenen Tarafların Sertifika İptal Listesi Kontrol Gerekliliği

Güvenen tarafların güvenip kullanacakları sertifikaların geçerlilik durumlarını, ilgili güncel SİL'lerden veya OCSP Yanıtlayıcılardan kontrol edip öğrenme sorumluluğu vardır.

4.4.10 Çevrim İçi Sertifika Durum Protokolü Desteği

Sertifika Hizmet Sağlayıcısı kapsamında sertifikaların geçerlilik durumlarının kontrolü için SİL yanında, <http://kap.bilten.tubitak.gov.tr:2560> web adresi üzerinden hizmet veren OCSP Yanıtlayıcı desteği de verilmektedir.

4.5 Güvenlik Denetimi

Sertifika Hizmet Sağlayıcısı, gerek Sertifika Kayıt Birimi gerekse Sertifika Yönetim Birimi ile ilgili bütün işlemlerin kayıtlarını tutar. Yapılan işlemlerin bir kısmı otomatik olarak elektronik ortama kaydedilir. Bazı işlemler ise kağıt üzerinde kayıt defterlerine yazılmak suretiyle kaydedilir. Güvenlik denetimleri sırasında elektronik veya kağıt ortamda saklanan tüm kayıtlar kontrol edilebilir.

4.5.1 Kaydedilen İşlemler

Elektronik olarak kaydı yapılan işlemler şunlardır:

- Sertifika başvuru kayıtları,
- Sertifika başvuru onay kayıtları,
- Üretilen sertifika kayıtları,
- Sertifika sürdürülebilirlik onay kayıtları,
- Sertifika askıya alma ve iptal başvurusu kayıtları,

- Sertifika iptal kayıtları,
- Sertifika ve SİL üretim kayıtları,
- Sertifika yönerge kayıtları,
- Tutulan tüm kayıtların tarihleri,
- Süreçlerin işleyişi sırasında yapılan işlemler,
- İşlemi yapan operatörün kimlik bilgisi.

Kağıt üzerinde kaydı yapılan işlemler şunlardır:

- Gelen ve giden kağıt evraklar defterlere kaydedilir.

4.5.2 Kayıtların Tutulma Süresi

Tutulan tüm kayıtlar en az beş yıl boyunca saklanır. Ancak yasalar gereğince daha uzun süre saklanması gereken kayıtlar arşivlenir. Arşivlenen kayıtlar ile ilgili bilgilendirme Bölüm 4.6.'da yapılmıştır.

4.5.3 Kayıtların Korunması

Sertifika Hizmet Sağlayıcısı'na ait kayıtların elektronik ve fiziksel olarak güvenlik altında tutulması için aşağıdaki önlemler alınmıştır:

- Elektronik olarak saklanan kayıtların hepsi işlemi yapan operatör tarafından elektronik imza ile imzalanarak saklanır. Bu sebepten dolayı, kayıtlarda oluşabilecek her değişiklik sistem tarafından farkedilir,
- Yetkisi olmayan kişiler elektronik kayıtların bulunduğu ortamlara erişemezler,
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda bulunurlar.

4.6 Kayıt Arşivleme

Sertifika Kayıt Birimi işleyişi sırasında oluşturulan elektronik kayıtlar her gün, Sertifika Yönetim Birimi'nin işleyişi sırasında oluşturulan elektronik kayıtlar ise her hafta düzenli olarak arşivlenir. Kağıt üzerindeki kayıtlar 5 (beş) yıl sonunda arşive kaldırılır.

4.6.1 Arşivlenen Kayıt Bilgileri

Elektronik olarak arşivlenen kayıtlar şunlardır:

- Güvenlik denetimi amacıyla elektronik olarak kaydı yapılan tüm işlemler,
- Verilen hizmetler sırasında yapılan e-posta yazışmaları,
- Üretilen tüm sertifikalar,
- Yayımlanan tüm Sertifika İptal Listeleri.

Kağıt ortamda arşivlenen kayıtlar şunlardır:

- Sertifika İlkeleri dokümanı,
- Sertifika Uygulama Esasları dokümanı,
- Kullanıcı taahhütnameleri,

- Sertifika başvuruları,
- İptal başvuruları,
- Sürdürülebilirlik başvuruları,
- Verilen hizmetler sırasında yapılan tüm yazışmalar, alınan ve gönderilen fakslar.

4.6.2 Arşivlerin Tutulma Süresi

Arşivler yasalar içinde öngörülen süre boyunca saklanır.

4.6.3 Arşivlerin Korunması

Sertifika Hizmet Sağlayıcısı'na ait arşivlerin elektronik ve fiziksel olarak güvenlik altında tutulması için aşağıdaki önlemler alınmıştır:

- Elektronik arşivlerin yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi veya silinmesi önlenmiştir,
- Kağıt üzerindeki kayıtlar sadece yetkililerin girme izni bulunan kilitli odalarda tutulurlar.

4.7 Anahtar Değişimi

SPK kök ve alt kök sertifikalarının anahtarlarının değişiminden itibaren yeni üretilecek olan kullanıcı sertifikaları yeni anahtarla imzalanır. Ancak eskiden üretilmiş olan kullanıcı sertifikalarının doğrulanabilmesi için eski anahtarın içinde bulunduğu eski kök veya alt kök sertifikasının kullanım süresi dolana kadar geçerliliğini koruması gerekmektedir. Eski kök veya alt kök sertifikalarına ait gizli anahtarlar kullanılarak üretilen kullanıcı sertifikalarının oluşturacağı SİL'in imzalanabilmesi için kök veya alt köke ait eski gizli anahtar saklanır ve korunur.

4.8 Güvenilirliğin Yitirilmesi ve Mücbir Sebep Durumlarında Yapılacaklar

Oluşabilecek her türlü mücbir sebep durumunda Sertifika Hizmet Sağlayıcısı'na ait kayıtların yitirilmesi veya SPK kök ve alt kök sertifikalarının anahtarlarının zarar görmesi, güvenilirliğini yitirmesi halinde yedekleme sistemleri aracılığıyla Sertifika Hizmet Sağlayıcısı sistemi tekrar işler hale getirilir. Eğer tam olarak işler hale getirilemez veya kayıtların bazıları yeniden elde edilemez ise, bu durumdan etkilenebilecek olan bütün Sertifika Hizmet Sağlayıcısı sistem kullanıcıları derhal bilgilendirilir. Gerekirse bazı sertifikalar iptal edilip, kullanıcılara bu SUE dokümanında yer alan şartlar uyarınca yeni sertifika üretilir.

4.9 Sertifika Hizmetlerine Son Verilmesi

Sertifika Hizmet Sağlayıcısı sertifika hizmetlerine son verecek olursa, bu durumu 6 (altı) ay öncesinden tüm PKI Uygulama Sistemi içindeki bileşenlere duyuracaktır. Sertifika Hizmet Sağlayıcısı sistemi ile ilgili tüm kayıtlar ve arşivler 5070 sayılı Elektronik İmza kanunu uyarınca çıkarılan Yönetmelik ve Tebliğlerde belirtilen süre boyunca korunacak, kamuya açık bilgilere erişim, sistemin işlerliğine son verilmesinden sonra anılan yönetmeliklerde belirtilen süre kadar devam edecektir.

SPK, böyle bir durumda Sertifika Hizmet Sağlayıcısı sistemindeki tüm sertifikaları iptal edecektir. Yayımlanan en son, güncel SİL'ler, sistemin kapanmasından sonra en az bir yıl süreyle erişime açık tutulacaktır.

5 FİZİKSEL, PROSEDÜREL VE PERSONEL GÜVENLİK KONTROLLERİ

5.1 Fiziksel Kontroller

Sertifika Hizmet Sağlayıcısı bütün birimlerinde güvenlik sağlamak amacıyla fiziksel kontroller uygular.

5.1.1 Tesis Yeri ve İnşaatı

Sertifika Yönetim ve Kayıt Birimleri'ne ait yazılım modüllerinin bulunduğu sunucu ve diğer donanım, güvenli ve korunaklı bina ve odalarda bulundurulur.

Sertifika Yönetim ve Kayıt Birimleri'nin bulunduğu bina ve odalar yetkisiz kişilerin girişine kapalıdır.

5.1.2 Fiziksel Erişim

Her modüle erişim hakkı, yalnızca o modülü işletmeye yetkili sistem yöneticilerine ve operatörlerine verilmiştir. Yetkisiz kişilerin yazılım, donanım ve diğer sistem bileşenlerine erişimi engellenir.

Sertifikaları imzalayan kök veya alt kök gizli anahtarlarının saklandığı ve gizli anahtarlarla ilgili işlemlerin yapıldığı modüller diğer modüllerin bulunduğu ortamdan ayrı, daha güvenli ortamlarda bulundurulur. Gizli anahtarın saklandığı ve işlem yapıldığı modüller sınırlı sayıdaki yetkili kişinin erişimine açık, girişi ancak güvenlik kartları ile mümkün olan çelik kapılı güvenli oda içinde bulundurulur.

5.1.3 Güç Kaynağı

Sertifika Yönetim ve Kayıt Birimleri bilgisayar donanımı ve havalandırma altyapısı, kesintisiz güç kaynağı ve jeneratörlerle desteklenir. Böylece güç kesintileri engellenerek sistemin sürekli işlerliği sağlanır.

5.1.4 Saklama ve Yedekleme Ortamlarının Korunması

Her tür kayıt malzemesi (hard disk, CD, disket, kağıt, vb.) güvenli ortamlarda korunmakta, bozucu, yıpratıcı dış etkenlerden uzak tutulur. Kayıtların üzerinde tutulduğu donanım veya yazılım ürünleri en güncel teknolojileri destekler.

5.2 Prosedürel Kontroller

5.2.1 Güvenilir Roller

Sertifika Yönetim ve Kayıt Birimlerinde çalışan personelin rolleri aşağıda belirtildiği şekilde sınıflandırılmıştır:

- *Sistem Yöneticisi:* Sertifika Yönetim ve Kayıt Birimlerindeki modüllerin kurulumu, konfigürasyonu ve devamlılığının sağlanması, sistemin işlemesi için gereken anahtarların üretimi, sertifika yönergelerinin tanımlanması ve kök/alt kök gizli anahtarları ile ilgili işlemlerin yapılmasından sorumludur.
- *Teknik Sorumlu:* Sistemin düzenli olarak yedeğinin alınması, işleyle ilgili teknik problemlerin giderilmesinden sorumludur.
- *Denetçi / Sertifika Hizmet Sağlayıcısı Yöneticisi:* Sistemin teknik ve idari işleyişinin kontrolü, iş planları ve raporlarının hazırlanmasından sorumludur.

- *Operatör*: Sertifika kullanıcısının tanımlanması, sisteme sertifika başvuru, iptal ve sürdürülebilirlik işlemleri ile ilgili girişlerin yapılması, gelen ve giden evrakların kontrolü ve saklanması gibi Sertifika Kayıt Biriminde yapılan işlerden sorumludur.

5.2.2 Rollerin Ayrılması

Sertifika Hizmet Sağlayıcısı'nda farklı kişiler olmak üzere en az 3 (üç) operatör, en az 2 (iki) sistem yöneticisi, en az 1 (bir) denetçi ve en az 2 (iki) teknik sorumlu olacaktır. Tanımlanan roller içinde operatörler dışındakiler için bir kişi birden fazla rolden sorumlu olabilir. Ancak bir operatör aynı zamanda sistem yöneticisi, teknik sorumlu veya denetçi olamaz.

5.2.3 Kimlik Doğrulama ve Yetkilendirme

Sertifika Hizmet Sağlayıcısı işleyişinin her adımında, işlemleri yerine getirecek kişilerin kimlik tanımlaması ve doğrulaması yapılmaktadır. Böylece her sistem birimine sadece yetkili kişilerin erişimi sağlanmaktadır. Sistemdeki bazı birimlere erişim farklı derecelerdeki yetkilendirme tanımlamalarıyla yapılmaktadır. Bu birimlere erişimin sağlanabilmesi için kimlik doğrulaması yapıldıktan sonra yetkilendirme tanımlamalarında verilen yetkiler çerçevesinde sistemde işlem yapılabilir.

5.3 Personel Kontrolleri

5.3.1 Kişisel Geçmiş, Nitelik ve Deneyim Gereklilikleri

Sertifika Hizmet Sağlayıcısı'nda çalışan personel, sistemin işleyişini sağlam ve güvenilir bir şekilde sağlayabilecek nitelikte, en az lise düzeyindeki okuldan mezun, bilgili, deneyimli ve güvenilir kişilerden oluşturulmuştur.

5.3.2 Eğitim Gereklilikleri

Sertifika Hizmet Sağlayıcısı'nda görev yapan tüm personel göreve başlamadan önce aşağıdaki konu başlıkları ile ilgili kapsamlı bir eğitimden geçirilmektedir:

- Sertifika Yönetim ve Kayıt Birimlerinin işleyiş mekanizması ve güvenlik prensipleri,
- Sertifika Yönetim ve Kayıt Birimlerinde yer alan modüllerin fonksiyonları ve işleyişi,
- Sertifika Yönetim ve Kayıt Birimlerindeki idari işleyişle ilgili prensiplerin anlatılması,
- Her kişinin yapacağı işin ve sorumluluklarının ne olduğu ile ilgili detaylı olarak bilgilendirilmesi.

5.3.3 Personele Sağlanacak Dokümantasyon

Sertifika Hizmet Sağlayıcısı'nda çalışan personele, yönetim ve kayıt modüllerinin kullanımı ile ilgili kullanım kılavuzu, Sertifika Hizmet Sağlayıcısı sistemleri hakkında genel bilgi ve Sertifika Hizmet Sağlayıcısı'nın teknik ve idari işleyiş prosedürleri ile yazışmalarda kullanılacak yazı metin şablonları sağlanmaktadır. Sertifika İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE) da personelin faydalanacağı dokümanlar arasındadır.

6 TEKNİK GÜVENLİK KONTROLLERİ

6.1 Anahtar Çifti Üretimi ve Kurulumu

6.1.1 Kök ve Alt Kök Sertifika Anahtar Çifti Üretimi

Sertifika Yönetim Birimi'nde mevcut bulunan kök ve alt kök sertifikalara ait anahtar çiftleri yetkisi olmayanların erişemeyeceği gizli oda içinde bulunan, ağ ortamına kapalı bilgisayarda, yazılım içinde, güvenlik altında üretilir ve buradan dışarıya çıkarılmaz.

6.1.2 Kullanıcıya Gizli Anahtarın Ulaştırılması

Gizli anahtar sertifika ile birlikte şifreli olarak yazılım veya donanım aracı içinde sertifika sahibine kimlik kontrolü ve imza karşılığında teslim edilir. Gizli anahtara erişim şifresi kapalı zarf içinde yine aynı şekilde kimlik kontrolü ve imza karşılığında kullanıcıya teslim edilir.

6.1.3 Kök Sertifikalarına Taraflarca Erişimin Sağlanması

Sertifika Hizmet Sağlayıcısı'na ait kök ve alt kök sertifikaları herkesin erişimine açık <http://kap.bilten.tubitak.gov.tr> web adresi üzerinden yayımlanır.

6.1.4 Anahtar Uzunlukları

SPK kök veya alt kök sertifikalarında en az 1024 bit uzunluğunda RSA (Rivest Shamir Adleman) anahtarları SHA-1 (Secure Hash Algorithm) veya MD5 (Message Digest) özet algoritmaları ile birlikte kullanılmaktadır. Kullanıcıların sertifikaları üretilirken ise, değişik uzunluklarda (1024 bit, 512 bit, vb.) RSA asimetrik anahtar çiftleri kullanılmaktadır.

6.1.5 Kullanıcı Anahtar Üretimi

Kullanıcı anahtar çiftleri, Sertifika Hizmet Sağlayıcısı yazılımı tarafından üretilmektedir.

6.1.6 Anahtar Kullanım Amaçları

PKI Uygulama Sisteminde anahtarlar kimlik doğrulama ve elektronik imza amaçlı kullanılabilirler. Bir anahtarın kullanım amacı, bağlı bulunduğu X.509 sertifikasındaki anahtar kullanım uzantısı ile belirlenir.

6.2 Gizli Anahtarın Korunması

6.2.1 Kriptografik Modül Standartları

Sertifika kullanıcılarının gizli anahtarı akıllı kart içinde tutulur. Akıllı kartlar gizli anahtarın modül dışına çıkarılmasını engelleyen güvenlik önlemleri ile donatılmıştır.

6.2.2 Gizli Anahtarın Saklanması

Sertifika Hizmet Sağlayıcısı'na bağlı olarak üretilen kök ve alt kök sertifikalara karşılık gelen gizli anahtarlar sadece yetkili kişilerin girebildiği kilitli odalar içindeki ağ ortamı dışında tutulan bilgisayarlarda saklanırlar. Bilgisayarlara ve gizli anahtarlara erişim hakkı sadece yetkili kişilere verilmiştir.

Kullanıcı sertifikalarına karşılık gelen gizli anahtarlar sadece kullanıcının kendi sorumluluğu altındaki akıllı kart içinde saklanır. Sertifika Hizmet Sağlayıcısı kullanıcılara ait gizli anahtarların bir kopyasını kendi sisteminde hiçbir şekilde tutmaz.

6.2.3 Gizli Anahtarın Yedeklenmesi

Sertifika Hizmet Sağlayıcısı'na bağlı kök ve alt kök sertifikaların gizli anahtarları, herhangi bir sorun anında hizmetlerin kesintiye uğramaması amacıyla, şifreli olarak yedeklenir. Yedek anahtarlar sadece yetkili kişilerin girebildiği kilitli odalar içindeki ağ ortamı dışında tutulan bilgisayarlarda veya elektronik medya içinde saklanırlar.

Kullanıcı sertifikalarına bağlı ve sadece kullanıcıların kendi sorumlulukları altında bulunan gizli anahtarlar ise kesinlikle yedeklenmez.

6.2.4 Gizli Anahtara Erişim Metodu

Sertifika Hizmet Sağlayıcısı içinde tanımlanmış kök veya alt kök sertifikalarına ait gizli anahtarlar şifreli dosyalarda saklanır. Sadece şifreyi bilen ve sistemde tanımlı olan yetkili kişiler gizli anahtarlara erişebilmektedir.

Kullanıcı gizli anahtarı kullanıcıya verilecek olan akıllı kart içinde şifreli olarak saklanır. Kullanıcı sadece kendisinin bildiği şifreyi kullanarak gizli anahtara erişir.

6.2.5 Gizli Anahtara Erişimin Kesilme Metodu

Gizli anahtarın kullanımından sonra akıllı kart yetkisiz erişime açık bırakılmaz, gizli anahtar hafızadan silinir. Gizli anahtara erişimin kesilmesi kullanım sonrası manuel “çıkış” işlemi ile ya da belirli bir süre sonra otomatik olarak gerçekleşir.

6.2.6 Gizli Anahtarın Yok Edilmesi

Gizli anahtarlar kullanım sürelerinin sona ermesinden sonra, kayıtlı olduğu sistemden güvenli ve kesin yöntemlerle silinerek yok edilir.

6.3 Anahtar Çifti Yönetimi ile İlgili Diğer Konular

6.3.1 Açık Anahtarın Arşivlenmesi

Açık anahtarlar sertifikalarla birlikte Sertifika Hizmet Sağlayıcısı bilgi deposunda arşivlenir.

6.3.2 Açık ve Gizli Anahtarın Kullanım Süreleri

Sertifika Hizmet Sağlayıcısı kök ve alt kök sertifikalarına ait gizli anahtarlar en çok 10'ar yıl, kullanıcı sertifikalarına ait gizli anahtarlar ise en çok 3 yıl geçerlidir.

6.4 Erişim Şifreleri

6.4.1 Erişim Şifrelerinin Üretimi

Sertifika Hizmet Sağlayıcısı sistemindeki bilgilere erişim için oluşturulan şifreler, kullanıcı anahtar çiftlerinin üretilmesi sırasında oluşturulan gizli anahtarlara erişim şifreleri ve kullanıcıların web üzerinden sertifika işlemlerini gerçekleştirmeleri için gerekli olan şifreler sistem tarafından rastgele ve tahmin edilemez nitelikte üretilirler.

Kullanıcılar için üretilen gizli anahtarlara erişim şifreleri sistemde tutulmaz, üretildiği anda kapalı zarfa basılır. Sadece kapalı zarf içinde mevcut olan gizli anahtara erişim şifresi kullanıcı dışında kimseye teslim edilmez.

Kullanıcıların web üzerinden sertifika işlemlerini gerçekleştirebilmeleri için üretilen erişim şifreleri hiçbir şekilde sistemde saklanmaz. Şifre doğrudan kullanıcıya iletilir.

6.4.2 Erişim Şifrelerinin Korunması

Sertifika Hizmet Sağlayıcısı sistemindeki bilgilere erişim şifreleri yetkili kişiler tarafından oluşturulur, yetkisi olmayanlarla paylaşılmaz ve gizli tutulur.

Kullanıcılar adına oluşturulan erişim şifreleri üretildiği an kapalı zarfa basılır ve kopyası alınmaz. Erişim şifreleri sadece kullanıcının kendisine teslim edilir. Kullanıcılar için oluşturulan erişim şifrelerinin kullanıcıya tesliminden sonra gizliliğinin ve güvenliğinin sağlanması tamamen kullanıcının sorumluluğundadır.

6.5 Bilgisayar Güvenlik Kontrolleri

Sertifika Hizmet Sağlayıcısı sisteminde PKI yöntemlerine dayanan aşağıdaki bilgisayar güvenlik kontrolleri uygulanmaktadır:

- Sisteme erişim hakları ve kimlik doğrulama sertifikalar kullanılarak sağlanmaktadır. Bu amaçla sistemi işletmekte olan personele sertifika verilmektedir.
- Sistemi işleten personelin erişim hakları tanımlanan rollerle sınırlanmıştır.
- Sistemi oluşturan birimler arasındaki veri iletişimi elektronik imzalı olarak yapılmaktadır.
- Yapılan tüm işlemler ve girilen verilerin kayıtları tutulur ve arşivlenir. İşlem tipi işlemi yapan operatör tarafından imzalanarak kaydedilir. İşlemler görüntülenmek istendiğinde ise imza doğrulaması yapılarak işlem kaydının bütünlüğünün bozulup bozulmadığı ve işlemi yapan kişinin kimliği tespit edilir.

6.6 Yaşam Döngüsü Teknik Kontrolleri

6.6.1 Güvenlik Yönetimi Kontrolleri

Sertifika Hizmet Sağlayıcısı sistem konfigürasyonu üzerinde yapılacak bütün değişiklik ve yenilemeler uygun bir şekilde dokümanite edilerek kontrol altında tutulmaktadır.

Sistem güvenliği, sistem erişim hesapları üzerindeki yetkilendirmelerle kontrol edilmektedir. Bu şekilde, sisteme yapılmaya çalışılan yetkisiz müdahalelerin saptanabileceği bir mekanizma kurulmuş durumdadır.

6.7 Ağ Güvenlik Kontrolleri

Sertifika Yönetim Birimi içinde tanımlanmış olan kök ve alt kök sertifikalarına ait gizli anahtarların üretimi, saklanması ve kullanımı ağ ortamı içinde bulunmayan çevrim dışı bilgisayarlar üzerinde yapılmaktadır. Ayrıca gizli anahtarların bulunduğu bu bilgisayarlar fiziksel olarak sadece yetkili kişilerin erişebildiği kilitli odalarda tutulmaktadır.

Sertifika Yönetim Birimi içindeki diğer sistem bileşenleri de ağ ortamı dışında fiziksel olarak güvenli odalarda tutulmaktadır.

Sertifika Kayıt Birimi içinde web üzerinden hizmet veren sistem bileşenleri güncel ağ güvenlik yöntemleri ile korunmakta, Yönetim Birimi'ne aktarılacak olan bilgiler manuel olarak taşınmaktadır.

7 SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ PROFİLLERİ

7.1 Sertifika Profili

7.1.1 Sürüm Numarası

Sertifika Hizmet Sağlayıcısı sisteminde oluşturulan kök ve alt kök sertifikalar ile kullanıcı sertifikaları X.509 v3 sertifika standardını destekler.

7.1.2 Sertifika Uzantıları

Sertifika Hizmet Sağlayıcısı X.509 v3 sertifika standardı içinde tanımlanmış olan ve PKI Uygulama Sistemi'nde sertifika kullanımı için gerekli uzantıların tamamını destekler. PKI Uygulama Sistemi içinde, sertifikaların kullanım amaçlarına uygun olan sertifika uzantıları sertifikaların içinde yer almaktadır.

Sertifika Hizmet Sağlayıcısı içinde tanımlı olan kök ve alt kök sertifikaları, sertifika ve sertifika iptal listesi imzalama, kullanıcı sertifikaları ise elektronik imza ve anahtar şifreleme amacıyla kullanılacaklarından dolayı sertifikaların içinde bu kullanım alanlarını tanımlayan uzantılar bulunmaktadır.

7.1.3 Algoritma Nesne Tanımlayıcıları

Sertifika Hizmet Sağlayıcısı'nın kök, alt kök ve kullanıcı sertifikalarının, elektronik olarak imzalanmasında kullandığı özet algoritmaları ile çift anahtarlı algoritmaların (SHA1-Secure Hash Algorithm, RSA-Rivest Shamir Adleman, vb.) neler olduğu belirlenmiştir. Kullanılan algoritmaların nesne tanımlayıcıları üretilen sertifikaların içeriğinde belirtilmektedir.

7.1.4 İsim Biçimleri

Üretilen kök ve alt kök sertifikalar SPK'nın, sertifika kullanıcılarına ait sertifikalar ise kişilerin X.500 formatındaki ayırt edilebilir adlarını içermektedir.

7.1.5 İsim Kısıtları

Sertifika Hizmet Sağlayıcısı'nda kök, alt kök ve kullanıcı sertifikalarında tanımlanan isim alanları ve bu isim alanlarına yazılacak bilgiler aşağıdaki tabloda gösterildiği biçimde belirlenmiştir.

Anonim ya da takma adlar Sertifika Hizmet Sağlayıcısı'nın ürettiği sertifikaların içinde kullanılamaz. Kullanıcının adı ve soyadı bilgisi ile çalıştığı şirket/kurumun bilgisi resmi kayıtlarda geçen isimlerden oluşmak zorundadır.

Kullanıcı sertifikalarında kullanıcı bilgilerinin tanımlandığı isim alanı içinde yer alan C (Country)-Ülke alanı yabancı uyruklu kullanıcılar için de uygulamanın Türkiye sınırları içinde yapılması sebebiyle TR olarak tanımlanır.

7.2 Sertifika İptal Listesi Profili

Sertifika Hizmet Sağlayıcısı sisteminde oluşturulan sertifika iptal listeleri X.509 v2 sertifika iptal listesi standardını destekler.

Alan Adı	SPK Kök Sertifikası	Kişiler Alt Kök Sertifikası	Sunucu ve Nesne İmzalama Alt Kök Sertifikası	Kullanıcı Sertifikaları
CN	Sermaye Piyasası Kurulu	Sermaye Piyasası Kurulu Bireysel Alt Kök	Sermaye Piyasası Kurulu Sunucu Alt Kök	Kullanıcının adı ve soyadı
O	-	-	-	Kullanıcının çalıştığı şirketin/kurumun ticari adı
OU	Kamuyu Aydınlatma	Kamuyu Aydınlatma	Kamuyu Aydınlatma	Kullanıcının unvanı
L	Ankara	Ankara	Ankara	Bildirim imzalama veya gönderme yetkisinin tanımı + Şirket/BDŞ ayrımı ¹
ST	-	-	-	T.C. kimlik numarası
C	TR	TR	TR	TR
E	-	-	-	Müşteri numarası

¹ Şirketler için;

0 --> İmza yetkisi yoktur.

1 --> Tek başına imzaya yetkilidir.

2 --> İmzaya diğer imzalarla birlikte yetkilidir.

BDŞ'ler için;

0 --> Bağımsız denetimde imza yetkisi yoktur.

1 --> Bağımsız denetimde tek başına imzaya yetkilidir.

2 --> Bağımsız denetimde imzaya diğer imzalarla birlikte yetkilidir.

8 DOKÜMAN YÖNETİMİ

8.1 Doküman Değişim Prosedürleri

SUE’de yapılan değişiklikler SPK’nın onayına tabidir. SPK, SUE dokümanını herkesin erişimine açık bulunan aşağıdaki web adresinden yayımlanmaktadır:

http://kap.bilten.tubitak.gov.tr/SiSue/SPK_SUE.pdf

Bu SUE dokümanına yapılabilecek değişiklikler ekleme ve değiştirme şeklinde olabileceği gibi, SPK, SUE dokümanının tamamen yenilenmesine de karar verebilir.

8.2 Yayın ve Duyuru Politikaları

SUE dokümanında yapılan değişiklikler Sertifika Hizmet Sağlayıcısı’nın ilgili web sitesi üzerinden yayımlanarak tüm PKI Uygulama Sistemi bileşenlerine duyurulur.

8.3 Sertifika Uygulama Esasları Onay Prosedürleri

Bu SUE dokümanının Sİ dokümanına uygunluğu, SPK tarafından onaylanır.

EK

SERTİFİKA SAHİBİ TAAHHÜTNAMESİ

Bu sayfa boş bırakılmıştır.

SERTİFİKA SAHİBİ TAAHHÜTNAMESİ

1. Bu taahhütnamede geçen “sertifika sahibi” ibaresi, halka açık anonim ortaklıklar, aracı kuruluşlar ve sermaye piyasası kurumları tarafından Sermaye Piyasası Kurulu’na ve/veya İstanbul Menkul Kıymetler Borsası’na gönderilecek her türlü bilgi, belge ve açıklamaların elektronik ortamda hazırlanması, imzalanması ve/veya gönderilmesi hususunda; şirketlerinin yönetim kurullarının atadığı şirket yetkilisi tarafından, belirtilen imza dereceleri ile yetkili kılınarak elektronik sertifika kullanacak olan gerçek kişiyi ifade etmektedir.

2. Sertifika Sahibi,

- a) Adına düzenlenen akıllı kart ve akıllı karta ait kapalı şifre zarfını şahsen teslim almayı,
- b) İmza oluşturma verisini, imza oluşturma aracını (akıllı kart, akıllı kart okuyucusu ve bu donanımlara ilişkin bilgisayarda kurulu bulunan yazılımların bütünü) ve ilgili şifreleri, kayıp, açığa çıkma, değişime uğrama ve üçüncü kişilerin yetkisiz kullanımı durumlarına karşı korumayı,
- c) Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği tüm kişisel bilgilerin tam ve doğru olduğunu,
- d) Sertifika başvurusu sırasında ve sertifikanın geçerlilik süresi boyunca beyan ettiği bilgilerde meydana gelen değişiklikleri gecikmeksizin elektronik sertifika hizmet sağlayıcısına bildirmeyi,
- e) İmza oluşturma verisinin ve/veya imza oluşturma aracının, kayıp, açığa çıkma, değişime uğrama ve yetkisiz kullanımı durumlarında, sertifikanın iptalini sağlamak üzere derhal elektronik sertifika hizmet sağlayıcısına bilgi vermeyi,
- f) İmza oluşturma verisini ve/veya imza oluşturma aracını, üçüncü kişilerce kullanılma tehlikesinin ve/veya bu tehlikenin oluşmasına neden olabilecek şartların ortaya çıkması halinde derhal elektronik sertifika hizmet sağlayıcısına bilgi vermeyi,
- g) Elektronik sertifika yönetim prosedürlerini, ilkelerini, uygulama esaslarını ve bu taahhütnameyi okuduğunu; sertifika yönetim sisteminden kaynaklanabilecek teknik hatalar dışında anılan prosedür, ilkeler ve esaslarda tanımlanan yükümlülüklerini yerine getirmekten sorumlu olduğunu; bu prosedür, ilkeler ve esasları ve bunlarda yapılan ve usulünce ilan edilen değişiklikleri kabul ettiğini,
- h) Elektronik sertifikasını, imza oluşturma aracı ve imza oluşturma verisini Kurul düzenlemelerinde belirtilen amaçlar dışında kullanmayacağını,
- i) SPK veya sertifika hizmet sağlayıcısı tarafından yapılacak güvenlik uyarıları sonucu internet erişimi için kullanılan tarayıcı programlarda gerekli güncellemeleri zamanında yapacağını,
- j) Bu taahhütnamede ve Kurul düzenlemelerinde öngörülen gizlilik kurallarına ve diğer kurallara uyulmaması sonucu veya sertifika sahibine atfedilecek kusurlu fiiller nedeniyle üçüncü kişilerin Kurul’ a ve İMKB’ye yöneltecekleri her türlü hukuki talebin muhatap tarafının kendisi olacağını,
- k) Yukarıda belirtilen taahhütleri yerine getirmemesi halinde doğan zararlardan sorumlu olduğunu, bu hususta SPK, İMKB ve elektronik sertifika hizmet sağlayıcısına sorumluluk yüklenemeyeceğini

kabul ve taahhüt eder.

3. Sertifika sahibi, Kurul düzenlemeleri çerçevesinde elektronik imza kullanımından doğan uyuşmazlıklarda, elektronik imzanın elle atılan imza ile aynı hukuki sonucu doğuracağını ve aynı ispat gücüne sahip olduğunu ve mahkemede aleyhine delil olarak kullanılacağını, elektronik sertifika hizmet sağlayıcısının elektronik imza ile ilgili her türlü evrakının, bilgisayar ortamında tutulan kayıtlarının ve elektronik verilerinin delil niteliğini taşıyacağını ve bunun bir delil anlaşması niteliğinde olduğunu kabul eder.

4. Bu taahhütname, imza tarihinde yürürlüğe girer.

SERTİFİKA SAHİBİNİN

Adı-Soyadı :
 T.C. Kimlik No. :
 Şirket/Kurum Adı :
 Unvanı :
 Tarih :
 İmza :