

SPK SERTİFİKA HİZMETLERİ

SERTİFİKA İLKELERİ

Sürüm 1.1

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	10
1.3.5 Uygulanabilirlik	10
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 Kullanıcı Yükümlülükleri	12
2.1.4 Güvenen Taraf Yükümlülükleri	12
2.1.5 Bilgi Deposu Yükümlülükleri	12
2.2 Sorumluluklar	12
2.2.1 Sertifika Yönetim Birimi Sorumlulukları	12
2.2.2 Sertifika Kayıt Birimi Sorumlulukları	13
2.2.3 Sertifika Kullanıcısı Sorumlulukları	13
2.2.4 Güvenen Taraf Sorumlulukları	13
2.3 Hukuksal Sorumluluk	13
2.4 Yürütme	13
2.5 Ücretler	14
2.6 Yayınlama ve Bilgi Deposu	14
2.6.1 Sertifika Hizmet Sağlayıcısı'nın Yayınları	14
2.6.2 Yayın Sıklığı	14
2.6.3 Erişim Kontrolleri	14
2.6.4 Bilgi Depoları	14

2.7	Gizlilik.....	14
2.7.1	Gizli Tutulması Gereken Bilgiler	14
2.7.2	Gizli Tutulması Gerekmeyen Bilgiler	14
2.8	Fikri Mülkiyet Hakları.....	14
3	KİMLİK TANIMLAMA VE DOĞRULAMA	15
3.1	İlk Kayıt.....	15
3.1.1	İsim Tipleri	15
3.1.2	İsimlerin Anlamlı Olması Gerekliliği.....	15
3.1.3	İsim Alanı İçinde Bulunan Bilgiler	15
3.1.4	İsimlerin Benzersizliği.....	15
3.1.5	Gizli Anahtara Sahip Olmanın Kanıtlanması	15
3.1.6	Kurumsal Kimliğin Doğrulanması	15
3.1.7	Kişisel Kimliğin Doğrulanması.....	15
3.2	Sertifika Sürdürülebilirlik ve Anahtar Yenileme.....	15
3.2.1	Sertifika Sürdürülebilirlik.....	15
3.2.2	Anahtar Yenileme.....	16
3.3	Sertifika Askıya Alma	16
3.4	Sertifika İptali.....	16
3.5	İptal Sonrası Yeni Sertifika Çıkartılması.....	16
4	İŞLEVSEL GEREKLİLİKLER	17
4.1	Sertifika Başvurusu	17
4.2	Sertifika Dağıtımı	17
4.2.1	Kullanıcı Sertifikalarının Dağıtımı	17
4.2.2	Kök ve Alt Kök Sertifikalarının Dağıtımı	17
4.3	Sertifikanın Teslim Alınması ve Kullanıma Açılması	17
4.4	Sertifikanın İptali ve Askıya Alınması	17
4.4.1	Sertifikanın İptali.....	17
4.4.2	Sertifikanın Askıya Alınması	18
4.4.3	Sertifika İptal Listesi Yayımlama Sıklığı	18
4.4.4	Güvenen Tarafların Sertifika İptal Listesi Kontrol Gerekliliği.....	18
4.4.5	Çevrim İçi Sertifika Durum Protokolü Desteği.....	18
4.5	Güvenlik Denetimi	18
4.5.1	Kaydedilen İşlemler.....	18
4.5.2	Kayıtların Tutulma Süresi	19

4.5.3	Kayıtların Korunması	19
4.6	Kayıt Arşivleme.....	19
4.6.1	Arşivlenen Kayıt Bilgileri	19
4.6.2	Arşivlerin Tutulma Süresi	19
4.6.3	Arşivlerin Korunması	19
4.7	Anahtar Değişimi.....	19
4.8	Güvenilirliğin Yitirilmesi ve Mücbir Sebep Durumlarında Yapılacaklar	19
4.9	Sertifika Hizmetlerine Son Verilmesi	19
5	FİZİKSEL, PROSEDÜREL VE PERSONEL GÜVENLİK KONTROLLERİ.....	20
5.1	Fiziksel Kontroller.....	20
5.1.1	Tesis Yeri ve İnşaatı	20
5.1.2	Fiziksel Erişim.....	20
5.1.3	Güç Kaynağı.....	20
5.1.4	Saklama ve Yedekleme Ortamlarının Korunması.....	20
5.2	Prosedürel Kontroller	20
5.2.1	Güvenilir Roller.....	20
5.2.2	Rollerin Ayrılması	20
5.2.3	Kimlik Doğrulama ve Yetkilendirme	20
5.3	Personel Kontrolleri.....	20
5.3.1	Kişisel Geçmiş, Nitelik ve Deneyim Gereklilikleri.....	20
5.3.2	Eğitim Gereklilikleri.....	20
5.3.3	Personele Sağlanacak Dokümantasyon	21
6	TEKNİK GÜVENLİK KONTROLLERİ.....	22
6.1	Anahtar Çifti Üretimi ve Kurulumu	22
6.1.1	Kök ve Alt Kök Sertifika Anahtar Çifti Üretimi	22
6.1.2	Kullanıcıya Gizli Anahtarın Ulaştırılması.....	22
6.1.3	Kök Sertifikalarına Taraflarca Erişimin Sağlanması.....	22
6.1.4	Anahtar Uzunlukları	22
6.1.5	Kullanıcı Anahtar Üretimi	22
6.1.6	Anahtar Kullanım Amaçları	22
6.2	Gizli Anahtarın Korunması	22
6.2.1	Kriptografik Modül Standartları.....	22
6.2.2	Gizli Anahtarın Saklanması.....	22
6.2.3	Gizli Anahtarın Yedeklenmesi	23

6.2.4	Gizli Anahtara Erişim Metodu	23
6.2.5	Gizli Anahtara Erişimin Kesilme Metodu	23
6.2.6	Gizli Anahtarın Yok Edilmesi	23
6.3	Anahtar Çifti Yönetimi ile İlgili Diğer Konular	23
6.3.1	Açık Anahtarın Arşivlenmesi	23
6.3.2	Açık ve Gizli Anahtarın Kullanım Süreleri	23
6.4	Erişim Şifreleri	23
6.4.1	Erişim Şifrelerinin Üretimi	23
6.4.2	Erişim Şifrelerinin Korunması	23
6.5	Bilgisayar Güvenlik Kontrolleri	23
6.6	Yaşam Döngüsü Teknik Kontrolleri	24
6.6.1	Güvenlik Yönetimi Kontrolleri	24
6.7	Ağ Güvenlik Kontrolleri	24
7	SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ PROFİLLERİ	25
7.1	Sertifika Profili	25
7.1.1	Sürüm Numarası	25
7.1.2	Sertifika Uzantıları	25
7.1.3	Algoritma Nesne Tanımlayıcıları	25
7.1.4	İsim Biçimleri	25
7.1.5	İsim Kısıtları	25
7.2	Sertifika İptal Listesi Profili	25
8	DOKÜMAN YÖNETİMİ	26
8.1	Doküman Değişim Prosedürleri	26
8.2	Yayın ve Duyuru Politikaları	26
8.3	Sertifika Uygulama Esasları Onay Prosedürleri	26

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 işletilmesinde uyulması gereken genel kural ve yapıları belirlemek amacıyla, SPK tarafından hazırlanmış Sertifika İlkeleri (Sİ) 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" 7. maddesine istinaden hazırlanmıştır.

Sertifika İlkeleri, kullanımı, İlke Kararı'nın 2. maddesinde belirtilen uygulama alanları ile sınırlı elektronik sertifikaları üreten elektronik sertifika hizmet sağlayıcısının işleyişi ile ilgili, uyulması gereken genel kurallardır.

Sertifika Hizmet Sağlayıcısı, bu Sİ dokümanına bağlı Sertifika Uygulama Esasları (SUE) uyarınca çalışır. Sertifika Hizmet Sağlayıcısı'nın sertifika hizmetleri verirken kullandığı işlem ve uygulamaların ayrıntılı bir bildirisi olan SUE dokümanı, ilgili Sİ dokümanına göre sertifika hizmet sağlayıcısının iç işleyişini teknik, iş ve yasal perspektiflere göre düzenleyen ve tanımlayan, ayrıntılı ve daha işlevsel nitelikli bir dokümandır.

Sertifika Hizmet Sağlayıcısı için, Sİ dokümanı "ne" yapılacağını tanımlarken, SUE dokümanı bunun "nasıl" yapılacağını tanımlar.

Sİ dokümanı herkesin erişimine açık bulunan aşağıdaki web adresinden yayımlanmaktadır:

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

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

Sertifika başvuru, üretim, yönetim 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

Sİ dokümanı, sertifika başvuru, üretim, yönetim ve iptal etme ile ilgili süreçler içindeki işlemleri tanımlar, PKI Uygulama Sistemi'ni oluşturan tüm bileşenlere uygulanan yönetim kurallarını içerir.

Sİ 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 İlkeleri (Sİ)"

Doküman sürüm numarası:

1.1

Dokümanın tarihi:

Aralık 2006

1.3 Sistem Bileşenleri ve Uygulanabilirlik

PKI Uygulama Sistemi içinde bulunan sistem bileşenleri sertifika üretim ve yönetimini yapan Sertifika Hizmet Sağlayıcısı ve üretilen sertifikaları kullanan son kullanıcılar olmak üzere iki alt başlık altında toplanır. Alt başlıklar altında tanımlanan diğer sistem bileşenleri aşağıda belirtilmiştir:

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

1.3.1 Sertifika Yönetim Birimi

Sertifikanın üretim ve yönetimini yapan birimdir.

Yönetim Birimi'nin ayrıntılı işleyişi bu Sİ dokümanına uygun olarak hazırlanmış olan SUE dokümanında belirtilmiştir.

1.3.2 Sertifika Kayıt Birimi

Sertifika Yönetim Birimi'ne bağlı olarak çalışan, kullanıcılar ile doğrudan iletişim içinde olan birimdir.

Kayıt Birimi'nin ayrıntılı işleyişi bu Sİ dokümanına uygun olarak hazırlanmış olan SUE dokümanında belirtilmiştir.

1.3.3 Son Kullanıcılar

Sertifika Sahipleri

Sertifika sahipleri, sertifikaların üzerinde adları bulunan ve sertifikalarını Sİ ve SUE dokümanlarına uygun olarak kullanan PKI Uygulama Sistemi bileşenleridir. PKI Uygulama Sistemi kapsamında sertifika sahipleri kişilerdir.

Güvenen Taraflar

Güvenen taraflar, PKI Uygulama Sistemi içindeki kullanıcılara ait sertifikaların üzerinde yer alan isim ve açık anahtarın arasındaki bağın doğruluğuna güvenerek sertifikaları kabul eden ve işlem yapan PKI Uygulama Sistemi bileşenleridir.

1.3.4 Bilgi Deposu

Sertifika Hizmet Sağlayıcısı ürettiği sertifikaları, sertifika iptal listelerini ve ilgili dokümanları son kullanıcıların erişebileceği ortamlardan yayımlar.

1.3.5 Uygulanabilirlik

Bu Sİ dokümanında belirlenen ilkeler çerçevesinde üretilen sertifikalar PKI Uygulama Sistemi içinde 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı'nın 2. maddesinde belirtilen "elektronik imzanın kullanım alanları" kapsamında kullanılmaktadır.

1.4 İletişim Bilgileri

Uygulama Yönetim Merkezi

Bu Sİ dokümanı, SPK veya SPK'nın onayıyla Sertifika Hizmet Sağlayıcısı tarafından hazırlanıp kamuya duyurulur. Sistem özellikleri SPK tarafından tanımlanır ve Sertifika Hizmet Sağlayıcısı tarafından uygulanır.

İletişim

Bu Sİ dokümanının uygulanması ve ilgili yönetim politikaları hakkındaki sorular TÜBİTAK UZAY 'ın 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

2.1.1 Sertifika Yönetim Birimi Yükümlülükleri

Sertifika Yönetim Birimi, SPK'nın belirlediği ilke ve esaslara uygun olarak sertifikaları üretmek, sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak, iptal işlemlerini gerçekleştirmek, iptal olmuş sertifika bilgilerini zamanında ve doğru olarak duyurmakla yükümlüdür.

Sertifika Yönetim Birimi'nin yükümlülükleri ile ilgili ayrıntılar SUE dokümanında yer almaktadır.

2.1.2 Sertifika Kayıt Birimi Yükümlülükleri

Sertifika Yönetim Birimi'ne bağlı olarak çalışan Sertifika Kayıt Birimi sertifika başvurusu, yenileme, sürdürülebilirlik ve iptal başvurularını usulüne uygun biçimde kabul etmek, uygun bulunduğu başvuruları Sertifika Yönetim Birimi'ne bildirerek sertifika üretilmesini veya diğer sertifika işlemlerinin gerçekleştirilmesini sağlamak, sertifikanın veya başvurunun durumu hakkında ilgili kişileri bilgilendirmekle yükümlüdür.

Sertifika Kayıt Birimi'nin yükümlülükleri ile ilgili ayrıntılar SUE dokümanında yer almaktadır.

2.1.3 Sertifika Kullanıcı Yükümlülükleri

Sertifika kullanıcısı başvuru, yenileme, sürdürülebilirlik ve iptal işlemlerini SUE dokümanında belirtilen yöntemlere uygun olarak tanımlanmış usule göre yerine getirmek, sertifikasını münhasıran Kurul İlke Kararının 2. maddesinde belirtilen amaçlar için ve imzalamış olduğu Sertifika Sahibi Taahhünamesine uygun olarak kullanmak, sadece kendisine ait gizli verileri ve akıllı kartını üçüncü kişilerin yetkisiz kullanımı durumlarına karşı korumakla yükümlüdür.

Sertifika kullanıcısının yükümlülükleri ile ilgili ayrıntılar SUE dokümanında yer almaktadır.

2.1.4 Güvenen Taraf Yükümlülükleri

PKI Uygulama Sistemi içinde güvenen taraflar, sertifikaların gerekli geçerlilik kontrollerini yapmakla yükümlüdür.

Güvenen tarafların yükümlülükleri ile ilgili ayrıntılar SUE dokümanında yer almaktadır.

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

2.2.1 Sertifika Yönetim Birimi Sorumlulukları

Sertifika Yönetim Biriminin, 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı, "Sertifika İlkeleri", "Sertifika Uygulama Esasları" 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, 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı, “Sertifika İlkeleri”, “Sertifika Uygulama Esasları” 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 sorumlulukları yerine getirmekten, kendisine ait gizli anahtar (imza oluşturma verisi) kullanılarak yapılan işlemlerden ve sertifikanın verilmiş amacı dışındaki kullanımlarda kendisinin ve üçüncü kişilerin görebileceği zararlardan sorumludur.

2.2.4 Güvenen Taraf Sorumlulukları

Sertifikaların geçerliliğine güvenmeden önce SUE dokümanında belirtilen gerekli geçerlilik kontrollerini yapmamasından doğan 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, 23.1.2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ve 09.10.2003 tarih ve 52/1223 sayılı SPK İlke Kararı'yla çıkarılan “Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Gönderilmesine İlişkin Uygulama Esasları” çerçevesinde yürütülür.

PKI Uygulama Sistemi bileşenleri arasında çıkabilecek anlaşmazlıklar “Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Gönderilmesine İlişkin Uygulama Esasları”, “Sertifika İlkeleri” ve “Sertifika Uygulama Esasları” uyarınca çözümlenir. Bu ilkeler ve uygulama dokümanlarının çözüme ulaştıramadığı durumlarda, anlaşmazlıkların çözümü için SPK yetkilidir.

Bu Sertifika İlkelerinin tamamının geçerliliğini etkilemeyen herhangi bir bölümü geçerliliğini kaybetse bile, diğer kısımları geçerliliğini korur ve uygulanır. Bu Sİ dokümanının güncellenmesi ile ilgili süreç bölüm 8'de “Doküman Yönetimi” başlığı altında anlatılmıştır.

2.5 Ücretler

Sertifika Hizmet Sağlayıcısı tarafından üretilen sertifikalar için kullanıcılardan ücret alınmayacak, ancak sertifika ile gizli anahtarın içinde bulunduğu ve kullanıcıya teslim edilen donanım aracının bedeli sertifika kullanıcısı tarafından ödenecektir. Ödenecek bedelin miktarı ile ilgili bilgilendirmenin ne şekilde yapıldığı SUE dokümanında belirtilmektedir.

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 kullanıcıların ve güvenen tarafların bilmesi gerekli görülen dokümanlar yayımlanmaktadır. Bu dokümanların neler olduğu SPK tarafından belirlenmektedir.

2.6.2 Yayın Sıklığı

Dokümanların yayımlanma sıklığı SUE dokümanında yer almaktadır.

2.6.3 Erişim Kontrolleri

Yayımlanan dokümanlara erişim kısıtlarıyla ilgili bilgiler SUE dokümanında yer almaktadır.

2.6.4 Bilgi Depoları

Sertifika Hizmet Sağlayıcısı bilgi deposu olarak web ortamını ve web üzerinden erişilebilen veri tabanlarını kullanmaktadır.

2.7 Gizlilik

2.7.1 Gizli Tutulması Gereken Bilgiler

Kullanıcılara, şirket ve kurumlara ait elektronik ortamda ya da kağıt üzerinde mevcut bulunan bilgiler gizli tutulacak, üçüncü kişilerle paylaşılmayacaktır. Ancak, mahkemelerden gelen talepler bu sınırlamanın dışındadır.

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

2.7.2 Gizli Tutulması Gerekmeyen Bilgiler

PKI Uygulama Sistemi'nin işlerliğinin sağlanması için sistem bileşenleri tarafından bilinmesi gereken bilgiler gizli tutulmayacaktır. Bu bilgilerin neler olduğu SUE dokümanında yer almaktadır.

2.8 Fikri Mülkiyet Hakları

PKI Uygulama Sistemi içindeki tüm sertifikalar ve dokümanlar ile bu Sİ 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, benzersiz isimler bulunur.

3.1.2 İsimlerin Anlamı Olması Gerekliliği

Sertifika Hizmet Sağlayıcısı tarafından üretilen sertifikalarda kullanılan isimlerin anlamlı ve kişiyi tanımlayıcı olması gerekmektedir.

3.1.3 İsim Alanı İçinde Bulunan Bilgiler

Sertifikaların isim alanlarının içinde kişiyi ve çalıştığı şirket/kurumu tanımlayan bilgiler bulunmaktadır.

3.1.4 İsimlerin Benzersizliği

Sertifika Hizmet Sağlayıcısı'nın ürettiği sertifikalardaki isim alanları benzersizdir. Farklı kişiler için aynı isim alanının tanımlanması engellenmektedir. Sertifikaların isim alanlarında hangi bilgilerin benzersiz isim oluşturma amacıyla kullanılacağı SUE dokümanında belirtilmektedir.

3.1.5 Gizli Anahtara Sahip Olmanın Kanıtlanması

PKI Uygulama Sistemi kullanıcıları için anahtar çifti Sertifika Hizmet Sağlayıcısı tarafından üretilmektedir. Gizli anahtar sertifika sahibine sertifikası ile birlikte teslim edilmektedir. Sertifika sahibinin gizli anahtara sahip olduğunun ispatı belirlenen bir yöntemle yapılır. Bu ispatın yöntemi SUE dokümanında anlatılmaktadır.

3.1.6 Kurumsal Kimliğin Doğrulanması

Sertifika Hizmet Sağlayıcısı Sertifika Kayıt Birimi aracılığıyla sertifika başvurusunda bulunan kişilerin bağlı oldukları kurum bilgilerini, resmi ve onaylı belgelere dayanarak doğrular.

3.1.7 Kişisel Kimliğin Doğrulanması

Kişilerin kimliği resmi kimlik belgelerine dayanılarak doğrulanır. Kişisel kimliklerin doğrulanması için izlenen sürecin ayrıntıları SUE dokümanında yer almaktadır.

3.2 Sertifika Sürdürülebilirlik ve Anahtar Yenileme

3.2.1 Sertifika Sürdürülebilirlik

Sertifikaların geçerliliğini koruması için sertifika içindeki bilgilerde herhangi bir değişim olmamalıdır. Bu sebepten dolayı, sertifika sahibinin Sertifika Hizmet Sağlayıcısı tarafından belirlenen sıklıkta, sertifika bilgilerinde herhangi bir değişim olmadığını Sertifika Hizmet Sağlayıcısı'na beyan etmesi gerekir. Uzun süre kullanılacak olan sertifikaların güvenliğinin sağlanması amacıyla gerekli görülen bu işlem, sürdürülebilirlik olarak tanımlanmıştır.

3.2.2 Anahtar Yenileme

Kullanıcılar sertifikalarını, dolayısıyla sertifikalarının içindeki açık anahtarlarını ve ilgili gizli anahtarlarını yenilemek istediklerinde kimlik doğrulama prosedürlerinin işletildiği yeni bir sertifika başvurusu yapmak zorundadırlar.

3.3 Sertifika Askıya Alma

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

3.4 Sertifika İptali

Sertifikanın geçerlilik süresi dolmadan önce kullanıma kapanması olan iptal işleminin yapılabilmesi için imzalı ve onaylı bir formla Sertifika Hizmet Sağlayıcısı'na başvurulur. Uygun görülen başvurular işleme alınarak sertifika iptal edilir.

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 Sertifika Kayıt Birimi'ne yapılır. Kayıt Birimi'nde başvuru sahibinin kimliği tanımlanır ve doğrulanır.

Sertifika başvurusunun işleme alınabilmesi için üzerinde ilgili imzaların bulunduğu başvuru formu Kayıt Birimi'ne iletilir.

Sertifika başvurusunda bulunmuş olması sertifika üretimini zorunlu kılmaz. Sertifika üretimi SPK ve İMKB'nin yetkisindedir. Usulüne uygun yapılmayan başvurular ile SPK web sayfasında yayımlanmakta olan "imza yetkisi kaldırılan kişiler" listesinde yer alan kişilerin yaptıkları sertifika başvuruları geri çevrilir ve sertifika üretimi yapılmaz.

4.2 Sertifika Dağıtımı

4.2.1 Kullanıcı Sertifikalarının Dağıtımı

Sertifika Kayıt Birimi tarafından değerlendirilen ve uygun bulunan sertifika başvuruları Sertifika Yönetim Birimi'ne iletilerek sertifika üretim aşamasına geçilir. Sertifikalar sadece Sertifika Hizmet Sağlayıcısı Yönetim Birimi tarafından üretilebilir. Üretilen sertifikaların kullanıcılara dağıtılması işlemi Kayıt Birimi tarafından gerçekleştirilir.

Sertifika ve gizli anahtar bir donanım aracı içinde, gizli anahtar erişim şifresi ise kapalı bir zarfa basılı olarak kullanıcıya imza karşılığında teslim edilir.

4.2.2 Kök ve Alt Kök Sertifikalarının Dağıtımı

Güvenen tarafların sertifikaların geçerliliğini kontrol edebilmesi için sertifikayı imzalayan alt kök sertifikaya ve hiyerarşik zincir yapısındaki diğer alt kök ve kök sertifikalarına ihtiyacı vardır. Bu yüzden kök ve alt kök sertifikalarının herkesin erişimine açık ortamlarda yayımlanması gerekmektedir. Kök ve alt kök sertifikaların dağıtımı Sertifika Hizmet Sağlayıcısı'na ait olduğu bilinen güvenilir bir web sitesinden kesintisiz olarak yapılır.

4.3 Sertifikanın Teslim Alınması ve Kullanıma Açılması

Kullanıcı sertifika ve gizli anahtarını bir donanım aracı içinde, gizli anahtar erişim şifresini ise kapalı bir zarfa basılı olarak imza karşılığında teslim alır. Teslim edilen sertifika ve gizli anahtarın geçerli konuma getirilebilmesi için, kullanıcının donanım aracı ve kapalı şifre zarfını aldığına dair imzasını taşıyan geri bildirim formunu Sertifika Hizmet Sağlayıcısı'na göndermesi gereklidir.

4.4 Sertifikanın İptali ve Askıya Alınması

4.4.1 Sertifikanın İptali

Sertifikanın kullanım süresi dolmadan geçerliliğini yitirdiği durumlarda sertifika iptal edilir ve artık kullanılamaz duruma gelir. Sertifikalar gizli anahtarın güvenliğinin kaybedildiğinden şüphelenilmesi, sertifika içeriğindeki bilgilerin değişmesi ve sertifika kullanıcısının 09.10.2003 tarih ve 52/1223 sayılı Kurul İlke Kararı'nın 9. maddesinde belirtilen "elektronik sertifika tahsis edilmeyecek kimseler" listesine alınması durumlarında iptal edilirler. İptali gerektiren koşullar SUE dokümanında detaylandırılmıştır.

İptal edilen sertifikalar, sertifikanın geçerlilik süresinin sonuna kadar Sertifika İptal Listelerinde ve OCSP (Çevrim içi Sertifika Durum Protokolü) Yanıtlayıcıda tutularak web üzerinden duyurulur. SİL ve OCSP Yanıtlayıcıya erişimin sağlanacağı web adresleri SUE dokümanında belirtilmektedir.

Sertifika iptal isteği kullanıcının kendisi, çalıştığı şirket/kurum yetkilisi, SPK veya İMKB yetkilileri tarafından yapılabilir.

Sertifika iptal isteğinin işleme konabilmesi için iptal edilecek sertifikayı tanımlayan bilginin ve iptal sebebinin belirtildiği ıslak imzalı, geçerli form Sertifika Hizmet Sağlayıcısı'na gönderilir.

Sertifika Hizmet Sağlayıcısı'na ait kök veya alt kök sertifikalardan birisi iptal edildiğinde, bu durum en az iki saat içinde web üzerinden duyurulur ve ilgili taraflar yazıyla bilgilendirilir. Duyurunun yapılacağı web adresi SUE dokümanında belirtilmektedir.

4.4.2 Sertifikanın Askıya Alınması

Sertifikanın askıya alınması geçici olarak iptal edilmesi demektir. Askıya alınmış bir sertifika iptal olmuş muamelesi görür. Ancak askıdan çıkartıldığında yeniden geçerli bir sertifika olarak kullanılabilir. Sertifika Hizmet Sağlayıcısı askıya alma işlemini sertifikayı iptal etmeden önce hatalı iptal isteklerinden geri dönüş imkanının verilebilmesi amacıyla desteklemektedir.

Askıya alma talebi iptal isteğinde bulunan kişilerce yapılabilir.

4.4.3 Sertifika İptal Listesi Yayımlama Sıklığı

Sertifika Hizmet Sağlayıcısı tarafından yayımlanacak olan Sertifika İptal Listeleri (SİL) web ortamından işleyişi aksatmayacak sıklıkta yayımlanacaktır. Bu sürelerin ne kadar olduğu ile ilgili ayrıntılar SUE dokümanında yer almaktadır.

4.4.4 Güvenen Tarafların Sertifika İptal Listesi Kontrol Gerekliliği

Güvenen tarafların PKI Uygulama Sistemi içindeki kullanıcılara ait sertifikaları işleme almadan önce, geçerlilik durumlarını Sertifika Hizmet Sağlayıcısı'nın işaret ettiği web ortamından edinebilecekleri SİL dosyasından veya duyurulan diğer yöntemler aracılığıyla kontrol edip öğrenme sorumluluğu vardır.

4.4.5 Çevrim İçi Sertifika Durum Protokolü Desteği

Sertifika Hizmet Sağlayıcısı kapsamında sertifikaların geçerlilik durumlarının kontrolü için SİL yanında, web üzerinden 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. Sertifika Hizmet Sağlayıcısı kapsamında çalışan yetkili personel tarafından gerekli görüldüğü durumlarda yapılan iç güvenlik denetimleri sırasında, elektronik veya kağıt ortamda saklanan tüm kayıtlar kontrol edilebilir.

4.5.1 Kaydedilen İşlemler

Yapılan işlemlerin bir kısmı otomatik veya manuel olarak elektronik ortama kaydedilir. Bazı işlemler ise kayıt defterlerine yazılmak suretiyle kaydedilir. Bu işlemlerle ilgili ayrıntılar SUE dokümanında yer almaktadır.

4.5.2 Kayıtların Tutulma Süresi

Tutulmuş tüm kayıtlar en az 5 (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 kayıtlar elektronik ve fiziksel olarak güvenlik altında tutulur.

4.6 Kayıt Arşivleme

Sertifika Hizmet Sağlayıcısı tarafından Sertifika Kayıt Birimi ve Sertifika Yönetim Birimi'nin işleyişi sırasında oluşturulan elektronik kayıtlar SUE'de belirtilen süreler içinde düzenli olarak arşivlenir. Kağıt üzerindeki kayıtlar bölüm 4.5.2'de belirtilen süre sonunda arşive kaldırılır.

4.6.1 Arşivlenen Kayıt Bilgileri

Elektronik olarak yapılan tüm işlemler ve üretilen bütün dosyalar arşivlenir.

Kağıt ortamda yapılan tüm yazışmalar, gönderilen form, belge ve yazılar arşive kaldırılır.

4.6.2 Arşivlerin Tutulma Süresi

Arşivler yasalar içinde öngörülen süre boyunca saklanır.

4.6.3 Arşivlerin Korunması

Sertifika Hizmet Sağlayıcısı'na ait arşivler elektronik ve fiziksel olarak güvenlik altında tutulur.

4.7 Anahtar Değişimi

SPK kök ve alt kök sertifikalarının anahtarlarının güvenlik sebeplerinden dolayı değiştirilmesi gerekebilir. Sertifika Hizmet Sağlayıcısı kök ve alt kök sertifikaların anahtar değişimine imkan verecektir. Bu durumda eski anahtarlar geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanacaktır. Anahtar değişimi işleminin nasıl yapılacağı ile ilgili ayrıntılar SUE dokümanında anlatılmaktadır.

4.8 Güvenilirliğin Yitirilmesi ve Mücbir Sebep Durumlarında Yapılacaklar

Sertifika Hizmet Sağlayıcısı'nda oluşabilecek her türlü mücbir sebep durumunda yapılacaklar SUE dokümanında tanımlanmıştır.

4.9 Sertifika Hizmetlerine Son Verilmesi

Sertifika hizmetlerine son verilmesi durumunda yapılacaklar SUE dokümanında tanımlanmıştır.

5 FİZİKSEL, PROSEDÜREL VE PERSONEL GÜVENLİK KONTROLLERİ

5.1 Fiziksel Kontroller

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.

5.1.2 Fiziksel Erişim

Sertifika Hizmet Sağlayıcısı içinde mevcut bulunan yazılım veya donanım ürünleri ve ilgili kağıt dokümantasyonlara fiziksel olarak erişimin sınırlandırılması için gerekli önlemler alınır.

5.1.3 Güç Kaynağı

Sertifika Yönetim ve Kayıt Birimleri bilgisayar donanımı 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 korunur, 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 Birimleri'nde görev alan personelin yazılım ve donanım bileşenlerine erişim hakları, SUE dokümanında tanımlanan roller ile belirlenmiştir.

5.2.2 Rollerin Ayrılması

Sertifika Hizmet Sağlayıcısı'nda görev alan personel yapılan iş doğrultusunda ayrı gruplar altında toplanmıştır.

5.2.3 Kimlik Doğrulama ve Yetkilendirme

Sertifika Hizmet Sağlayıcısı işleyişinin her adımında, işlemleri yerine getirecek yetkililerin kimlik doğrulaması ve yetkilendirme denetimi yapılır, bu şekilde her sistem birimine sadece yetkili kişilerin erişimi sağlanır.

5.3 Personel Kontrolleri

5.3.1 Kişisel Geçmiş, Nitelik ve Deneyim Gereklilikleri

Sertifika hizmetlerinde çalışan personel, sistemin işleyişini sağlam ve güvenilir bir şekilde sağlayabilecek nitelikte, en az lise düzeyindeki okuldan mezun, bilgili, deneyimli ve güvenilir kişilerden oluşur.

5.3.2 Eğitim Gereklilikleri

Sertifika Hizmet Sağlayıcısı'nda görev yapan tüm personel göreve başlamadan önce gerekli eğitimden geçirilir.

5.3.3 Personele Sağlanacak Dokümantasyon

Sertifika hizmetlerinde çalışan personele işleyle ilgili başvuruda bulunabilecekleri gerekli dokümanlar tedarik edilir.

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 güvenlik altında üretilir ve buradan dışarıya çıkarılmaz.

6.1.2 Kullanıcıya Gizli Anahtarın Ulaştırılması

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

6.1.3 Kök Sertifikalarına Taraflarca Erişimin Sağlanması

SPK'ya ait kök ve alt kök sertifikalarına taraflarca erişim web ortamı üzerinden kesintisiz olarak sağlanır.

6.1.4 Anahtar Uzunlukları

Sertifika Hizmet Sağlayıcısı'na ait kök veya alt kök sertifikalarında en az 10 (on) yıl boyunca kullanımı güvenli kabul edilebilecek uzunlukta anahtarlar kullanılır.

Kullanıcı sertifikalarında en az 3 (üç) yıl boyunca kullanımı güvenli kabul edilebilecek uzunlukta anahtarlar kullanılır.

6.1.5 Kullanıcı Anahtar Üretimi

Kullanıcı anahtar çiftleri, Sertifika Hizmet Sağlayıcısı yazılımı tarafından üretilmektedir.

6.1.6 Anahtar Kullanım Amaçları

PKI Uygulama Sistemi içinde anahtarların kullanım amacı, bağlı bulunduğu X.509 sertifikasındaki anahtar kullanım uzantısında belirtilen amaçlar doğrultusunda 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 yetkisiz kişilerin fiziksel ve elektronik olarak erişimine kapalı, güvenli ortamlar içinde tutulur.

Kullanıcı gizli anahtarları 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 anahtarlarının yedekleri yetkisiz kişilerin erişimine kapalı güvenli ortamlarda tutulur. Ancak kullanıcılara ait gizli anahtarlar kesinlikle yedeklenmez.

6.2.4 Gizli Anahtara Erişim Metodu

Gizli anahtar şifreli dosya içinde saklanır. Gizli anahtarın kullanılabilir duruma gelmesi ancak bu şifrenin bilinmesi ile mümkün olur.

6.2.5 Gizli Anahtara Erişimin Kesilme Metodu

Gizli anahtarın güvenliğinin korunması açısından kullanımından sonra erişimi kesilmektedir.

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 sertifikaların içinde Sertifika Hizmet Sağlayıcısı bilgi deposunda arşivlenir.

6.3.2 Açık ve Gizli Anahtarın Kullanım Süreleri

Sertifika Hizmet Sağlayıcısı kök/alt kök sertifikaları ve kullanıcı sertifikaları ile ilgili gizli anahtarlar, anahtarların teknik güvenlik sürelerinden daha kısa süreler içinde kullanılırlar. Anahtarların teknik güvenlik süreleri o günkü teknolojinin imkanlarına göre değişebildiğinden bu süreler gerekli görüldükçe yeniden gözden geçirilir. Bu günkü teknoloji göz önüne alınarak belirlenen anahtar kullanım süreleri SUE dokümanında belirtilmiştir.

6.4 Erişim Şifreleri

6.4.1 Erişim Şifrelerinin Üretimi

Sertifika Hizmet Sağlayıcısı sistemi veya kullanıcılar için üretilen erişim şifreleri tahmin edilemez nitelikte, sadece yetkisi olan kişinin erişebileceği güvenlik önlemlerinin alındığı yöntemlerle oluşturulurlar.

6.4.2 Erişim Şifrelerinin Korunması

Sertifika Hizmet Sağlayıcısı sistemi için üretilen erişim şifreleri sadece yetkili kişiler tarafından bilinmektedir.

Kullanıcılara ait erişim şifreleri üretildiği an kapalı zarfa basılır ve kopyası sistemde tutulmaz.

6.5 Bilgisayar Güvenlik Kontrolleri

Sertifika Hizmet Sağlayıcısı sisteminde uygulanan bilgisayar güvenlik kontrolleri PKI teknolojisine dayanan, ayrıntıları SUE dokümanında verilen yöntemlerle yapılmaktadır.

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 üzerindeki yetkilendirmelerle kontrol edilmektedir. Bu şekilde, sisteme yapılmaya çalışılan yetkisiz müdahalelerin saptanabileceği bir mekanizma kurulmuş durumdadır.

6.7 Ağ Güvenlik Kontrolleri

Sertifika Hizmet Sağlayıcısı'na bağlı bulunan Sertifika Yönetim ve Kayıt Birimleri'nde tüm sistem bileşenlerinin güvenliği güncel ağ güvenlik kontrolleri ile sağlanmaktadır.

7 SERTİFİKA VE SERTİFİKA İPTAL LİSTESİ PROFİLLERİ

7.1 Sertifika Profili

7.1.1 Sürüm Numarası

Sertifika Hizmet Sağlayıcısı X.509 v3 sertifika standardını destekler.

7.1.2 Sertifika Uzantıları

Sertifikanın PKI Uygulama Sistemi içinde kullanımı sırasında gerekli olan uzantıların tamamı Sertifika Hizmet Sağlayıcısı tarafından desteklenir.

7.1.3 Algoritma Nesne Tanımlayıcıları

Sertifika Hizmet Sağlayıcısı sisteminde kullanılan algoritmaların nesne tanımlayıcıları 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

Kök ve alt kök sertifikaları ile kullanıcılara ait sertifikaların içinde yer alacak isim alanları ve isim alanları ile ilgili kısıtlar SUE dokümanında belirtilmektedir.

7.2 Sertifika İptal Listesi Profili

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

8 DOKÜMAN YÖNETİMİ

8.1 Doküman Değişim Prosedürleri

Sİ’de yapılan değişiklikler SPK’nın onayına tabidir. Sİ dokümanı herkesin erişimine açık bulunan aşağıdaki web adresinden yayımlanmaktadır:

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

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

8.2 Yayın ve Duyuru Politikaları

Sİ 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

SUE’nin bu Sİ dokümanına uygunluğu, SPK tarafından onaylanır.