# TBD Kamu-BİB
# Kamu Bilişim Platformu VII
## 26-29 Mayıs 2005
## Antalya

# e-imza
# NİTELİKLİ SERTİFİKASYON ALTYAPISI VE YETKİLENDİRME

## 1. ÇALIŞMA GRUBU

**Hazırlayanlar :**

**Muzaffer YILDIRIM**
**A. Altuğ YAVAŞ**
**Önder ÖZDEMİR**
**Adnan METE**
**Esin DEMİRBAĞ**
**A.Coşkun SARIKAYA**
**Meral DURGUT**
**Zülfi GÜREN**
**Şuayb SÖZBİLİCİ**
**Cemal GEMCİ**
**Semih IŞIKSAL**

# İÇİNDEKİLER

# 1 Özet

Ülkemizde dünyayla eş zamanlı olarak elektronik hayata geçiş çalışmaları sürdürülmektedir. Bu konu hem hükümet, hem de sistemi oluşturacak sektör (yazılım, donanım, akıllı kart gibi) tarafından büyük destek görmektedir. Günlük hayatımızda yaşadığımız birçok olayın, hizmetin elektronik ortama aktarılmasının sayısız faydalı sonuçlar doğuracağı açıktır. Elektronik ortamda yapılan uygulama ve hizmetler, kağıt ortamına oranla zaman, iş gücü, para tasarrufu sağlayacak, hizmetlerin 7 gün 24 saat alınıp verilebilmesine olanak sağlayacak, bütün dünyayı bir ağ ortamında birleştirebilecektir. Elektronik ortama geçiş farklı bir döneme geçişi sağlayacak, hizmet konusundaki anlayışı değiştirerek hizmetin vatandaşın ayağına gitmesine imkan tanıyacak, elektronik ticaret müşteri kitlesini sadece çevrenizdeki insanlar olmaktan çıkarıp dünyanın tümüne yaygınlaştırabilecektir. Ancak elektronik ortama geçiş birçok riski de beraberinde getirecektir. Ağ ortamında yapılan işlemlerden karşı tarafın kim olduğundan emin olmak güçleşecek, gönderilen bilgilerin bozulmadan/değiştirilmeden gitmesinden şüphe duyulacak, yapılan işlemlerin inkar edilme endişesi yaşanacaktır. Elektronik ortamda bu risklerden kurtulmak için kullanılacak araç elektronik imzadır.

Elektronik imza, gerçek hayatta ıslak imza ile yapılan her işin (kanunla hariç tutulanlar dışında: evlenme, tapu işlemleri gibi) elektronik ortamda yapılabilmesi için bir araçtır. Elektronik imza da tıpkı ıslak imzada olduğu gibi evrakla kişinin kimliği arasında bir ilişki oluşturur. Ancak elektronik imzanın ıslak imzaya oranla üstünlükleri de vardır. Islak imzaya oranla taklit edilmeleri imkansız denecek oranda zordur, ayrıca sadece kişinin kimlik bilgisiyle değil ayrıca mesajın içeriğiyle de ilişkilidir. Mesajdaki en küçük değişikliklerde bile elektronik imza değişir. Bu nedenle mesajın bütünlüğünü (bir yerden bir yere giderken bozulmadan, değiştirilmeden, orijinal haliyle gitmesi) sağlamada oldukça önemli bir rol oynar. Elektronik imza ıslak imza gibi görsel bir ifade değildir. Elektronik ortamdaki bir uygulamada mesajın sonuna eklenen bir veridir. Elektronik imza sayesinde kimlik doğrulama, veri bütünlüğü ve inkar edememe özellikleri sağlanır. Ancak elektronik imza verinin gizliliğine ilişkin bir çözüm yaratmaz. Mesajların başkaları tarafından görülmemesi, başkalarından gizlenmesi isteniyorsa şifreleme tekniğinin kullanılması gereklidir. Elektronik uygulamalarda hem gizlilik hem de yukarıda sayılan üç özelliğin sağlanması için imzalama ve şifreleme teknikleri birlikte kullanılırlar.

Elektronik imza sadece bir altyapıdır. Elektronik uygulamalarda elektronik imzanın kullanılabilmesi için birçok uygulama ile entegrasyonu için ek yazılımlara ihtiyaç olacaktır. Örneğin kullanılmakta olan bir doküman yönetim sisteminde elektronik imza kullanımının sağlanması için yazılıma entegrasyon modüllerinin eklenmesi gerekecektir. Benzetme yapmak gerekirse elektronik imza doğalgaz olarak düşünülürse, doğalgazın kullanımı için ya doğal gaz uyumlu soba/ocak/kombi alınacaktır ya da kömürle çalışan araçlar doğalgazla çalışır hale getirilecektir. Kısacası elektronik imza kullanımına geçilmesi için öncelikle uygulamaların elektronik ortama aktarılması ve elektronik imza ile çalışabilir hale getirilmesi gerekecektir.

Elektronik imza hukuksal olarak ıslak imzaya eşdeğerdir. Bu anlamda Türkiye'de gerekli kanun, yönetmelik ve tebliğler hazırlanmıştır. İlgili yayımlanan mevzuatlarda konuyla ilgili gerekli açıklamalar yapılmıştır. Mevzuata göre sertifikaların hukuksal olarak geçerli olması için nitelikli olması gerekmektedir. Nitelikli sertifikalar da ancak Telekomünikasyon Kurumu tarafından yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcıları tarafından temin edilebilir. Ülkemizde henüz

yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcısı yoktur (henüz başvurular yapılıyor, kanuna göre başvurudan sonra minimum 2 ay onaylama süreci var). Ancak yılın ikinci yarısında bu sistemin yerleşeceği tahmin edilmektedir. Yayınlanan Başbakanlık genelgesi ile Türkiye'de kamu çalışanlarına ait sertifikalar için bir düzenleme getirilmiş (kamu çalışanları sertifikalarını TÜBİTAK'tan alacaklar), vatandaş sertifikaları konusu düzenlemeye açık bırakılmıştır. Vatandaş elektronik imza anahtarı ve sertifikasını nitelikli elektronik sertifika sağlayan özel kuruluşlardan alacaktır (aday kuruluşlar TÜRKTRUST ve E-GÜVEN). Vatandaş sertifikasını bu kuruluşların yönlendirdiği Kayıt Merkezleri'nden (örneğin banka şubeleri, noterler, üniversiteler, belediyeler, vb.) kişisel başvuru yaparak alabilir. İmzalama anahtarı ve sertifikalar yönetmeliğe göre akıllı kart ya da akıllı çubuk (token) denen araçlarda taşınacak ve her imzalama işleminde bu araçlar bilgisayar, "kiosk" ya da benzeri cihazlara takılacaktır. Vatandaş imzalama anahtarı ve sertifikasını alırken ya ücretini kendi ödeyecek ya da kampanyalardan yararlanacak. İmzalama anahtarı ve sertifikanın ömrü özel bir tanımlama olmazsa 1 (bir) yıl. Sertifikanın ömrü bittiğinde ücreti ödenerek yenilenecektir.

Elektronik imza konusu oldukça yeni bir konudur ve dikkatli davranılmadığı durumda riskler taşıyabilir. Konu doğrudan güvenlikle ilgili olduğu için önemi oldukça yüksektir. Bu nedenle alınacak yazılım, donanım ve hizmetler konusunda çok dikkatli olunması, bilinçli yaklaşılması, yabancı ülke katkısının incelenmesi, güvenilirlik/süreklilik/kurumsallık sorgulamalarının iyi yapılması ve hizmet kalitesinin doğru değerlendirilmesi faydalı olacaktır.

Elektronik hizmetlerin hızla yaygınlaşmasının, hem bu hizmetleri veren hem de bu hizmetlerden faydalananlar açısından en çabuk akla gelen nedenleri şunlardır:

- Erişim tarifelerin ucuzlaması
- Erişim hızının artması
- Zaman, iş gücü, para tasarrufu
- Kullanım kolaylığı
- Elektronik olarak verilen hizmetin hukuki olarak geçerlilik kazanması.

Bunlar gibi sayılabilecek daha birçok nedenden dolayı tüm dünyada olduğu gibi ülkemizde de kamu kurumları, vatandaşa verdikleri hizmetleri ve kendi kurumsal iş akışlarını elektronik ortama taşımak için kapsamlı projeler başlattılar. Maliye Bakanlığı'nın "Vergi Dairesi Otomasyon Projesi", Adalet Bakanlığı'nın "Ulusal Yargı Ağı Projesi", Sağlık Bakanlığı'nın "Aile Hekimliği Bilgi Sistemi", günlük hayatta toplumu en çok etkileyen ve etkileyecek olan projelere örnek olarak verilebilir.

Mevcut e-Devlet projelerinden sağlanan verimin artarak devam ettirilmesi ve yeni projelerin hayata geçmesi aşamasında, kurumların karşı karşıya olduğu en önemli risklerden biri iletilen bilginin güvenliğinin sağlanmasıdır. "**Elektronik imza**", değerli ve kişiye/kuruma özel bilgilerin İnternet gibi açık ve korumasız ağlar üzerinden güvenli olarak iletilmesinde kullanılan bir teknolojidir. Elektronik İmza teknolojisi ve Elektronik İmza teknolojisi kullanılarak oluşturulan Açık Anahtar Altyapısı Bölüm 2'de açıklanmıştır.

Ülkemizde elektronik imza teknolojisinin etkin kullanımına yönelik olarak gerçekleştirilen çabalar 15 Ocak 2004'de 5070 nolu **Elektronik İmza Kanunu**'nun

ve bu kanunla ilişkili yönetmelik ve tebliğin yayınlanması ile sonuç verdi. Bu kanunla "Elektronik İmza" teknolojisinin ülkemizdeki kamu ve özel sektör uygulamalarında nasıl hayata geçirileceği ile ilgili hukuki bir altyapı oluşturulmuş oldu. Bu yasa ile tanımlanan güvenli elektronik imza, ıslak imza ile aynı hukuki sonuçları doğurmaktadır (Madde 5).

Elektronik imza teknolojisinin en önemli parçası, kurum ve kişiler arasında bir güven köprüsü kurulmasını sağlayan **Elektronik Sertifika Hizmet Sağlayıcılar (ESHS)**'dır. Bölüm 0'de oluşturulan yasal altyapı ile ESHS'lere yüklenen görevler belirtilmiştir. Daha sonra Bölüm 4'de bir ESHS'nin bu görevleri yerine getirebilmek için sahip olması gereken nitelikler tarif edilmiştir. Ayrıca herhangi bir elektronik imza ve yasal hükme sahip "güvenli elektronik imza" arasındaki farklar açıklanmıştır.

Bölüm 5'de Türkiye'deki kamu ve özel sektörde ESHS yapılanması, Kamu Sertifikasyon Yapısı'nın oluşturulması ile ilgili bilgiler verilmiştir.

Elektronik imzanın temel işlevi uygulamalar için güvenli bir iletişim ortamının kurulmasıdır. Elektronik imzanın, uygulamalardan farkı ve birlikte çalışabileceği uygulamalar Bölüm 6'da gerçek örnekler de verilerek açıklanmıştır.

Elektronik imza, Avrupa Birliği, Amerika Birleşik Devletleri ve diğer ülkelerde de yasal altyapısı oluşturulmuş olan ve devlet ve özel sektörde kullanılmakta olan bir teknolojidir. Bu yönden yurtdışındaki uygulamalarla birlikte çalışabilirliğin sağlanması gereken noktalarda yapılması gerekenlerle ilgili bilgiler Bölüm 7'de verilmiştir.

Elektronik imzaların istenen düzeyde bir güven altyapısı sağlayabilmesi için önemli bir halka, bu teknolojinin matematiksel altyapısını içinde barındıran akıllı kart ve akıllı çubuk gibi Kriptografik araçlardır. Bölüm 6'de bu araçlar hakkında bilgiler verilmiş ve günlük hayatta kullanımları ile ilgili karşılaşılabilecek hususlar ele alınmıştır.

# 2 Güvenli Veri İletimi ve Elektronik İmza

## 2.1 Temel Gereksinimler

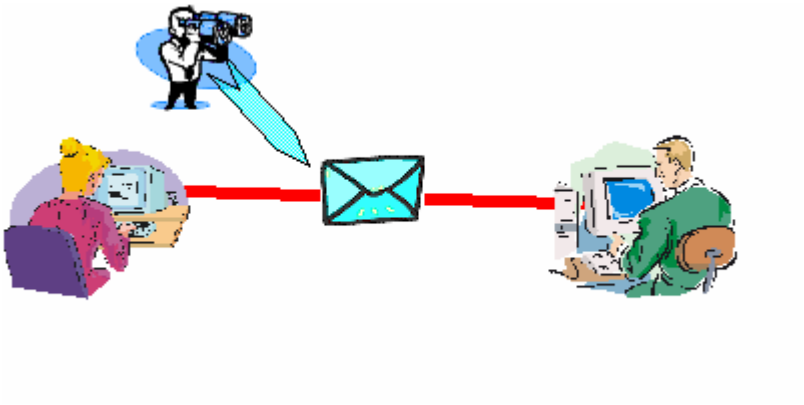
Elektronik İmza Yasası'nda Elektronik imza şöyle tanımlanmaktadır (Bkz. EK- A):

"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri." (Yasa Madde 3b)

Elektronik imza, iletişim ve veri güvenliğini sağlamak amacıyla geliştirilmiş bir teknolojidir. Günümüzde İnternet başta olmak üzere açık ve korunmasız ağlar üzerinden gerçekleşen veri iletişiminin güvenliğinin sağlanması için bir takım gereksinimler belirlenmiştir. Elektronik işlemlerdeki temel güvenlik gereksinimleri şunlardır:

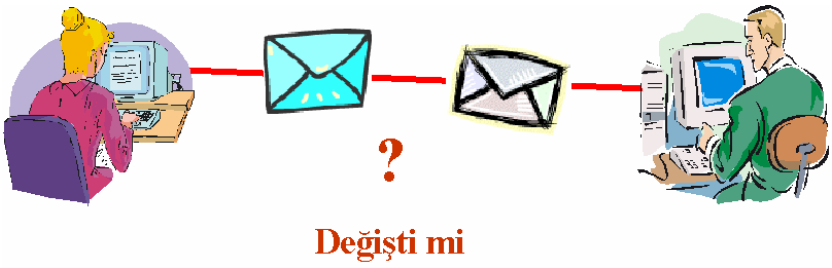
**1. Gizlilik:** Verinin/içeriğin görüntülenmesinin sadece veriyi görüntülemeye izin verilen şahısların erişimiyle kısıtlanmasıdır (Bkz. Şekil 1). Bu şekilde, artık çok da zor olmayan ve kişisel bilgi mahremiyetini tehdit eden iletişim

trafiğinin yetkisiz olarak dinlenmesine karşı bir önlem alınmış olur. Gizlilik bilginin şifrelenmesi ile gerçekleştirilebilir.



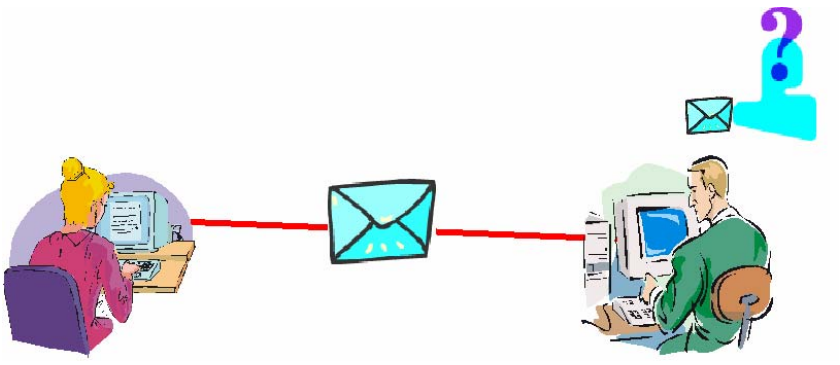
**Şekil 1 Gizlilik**

**2. Bütünlük:** Verinin izinsiz olarak veya yanlışlıkla değiştirilmesinin, silinmesinin veya veriye ekleme yapılmasının önlenmesidir (Bkz. Şekil 2). Bu şekilde verinin göndericiden alıcıya, göndericiden çıktığı haliyle değişmeden ulaşması sağlanır. Alıcı, iletinin göndericiden çıktığı haliyle kendisine ulaştığını bir bütünlük sınaması yapar anlar. Bütünlük gereksinimi, elektronik imza ile gerçekleştirilebilir.



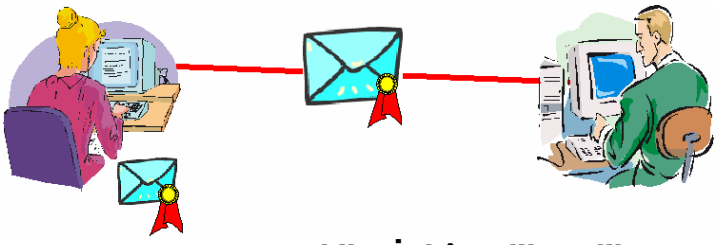

**Şekil 2 Bütünlük**

**3. Kimlik doğrulama:** Mesajın iletiminin geçerliliğinin ve mesaj sahibinin kimliğinin doğrulanmasının sağlanmasıdır. Örneğin bir elektronik posta mesajı üzerinde yer alan gönderici adresi, mesajın asıl göndericisi olmayabilir (Şekil 3). Bu nedenle alıcı, göndericinin kimliğini doğrulamak için bir takım yöntemler kullanır. Elektronik imza, kimlik doğrulama için kullanılabilecek yöntemlerden biridir.



**Şekil 3 Kimlik Doğrulama**

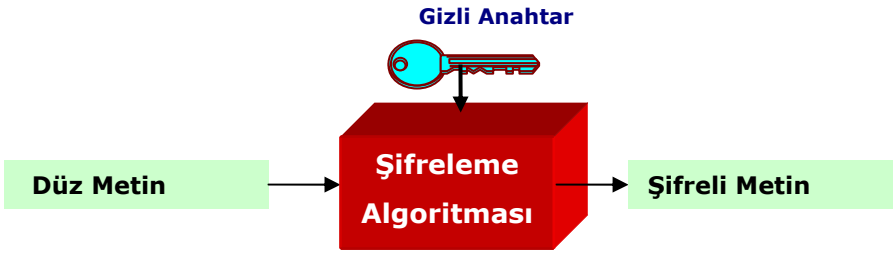
**4. İnkâr Edilmezlik:** Bireylerin elektronik ortamda gerçekleştirdikleri işlemleri inkar etmelerinin önlenmesidir (Şekil 4).



**Şekil 4 İnkâr Edilmezlik**

Yukarıdaki 1. gereksinimde de bahsedildiği gibi gizliliğin sağlanması bilginin şifrelenmesi ile gerçekleştirilebilir. Şifrelemede en yaygın kullanılan yöntem "*gizli anahtarlı şifreleme*" denen yöntemdir. Bu yöntemde mesaj şifrelenirken bir "anahtar" kullanılır ve şifrenin açılması için şifrelemede kullanılan anahtara ihtiyaç vardır (Şekil 5). Bu şifreleme yönteminin güvenliği anahtarın gizli tutulmasına bağlıdır. Anahtar "0" ve "1"lerden oluşan bir bit dizisidir ve her şifreleme algoritmasında farklı boylarda anahtarlar kullanılır. Örneğin gizli anahtarlı şifreleme algoritmasına örnek olarak verilebilecek AES algoritmasında 128 bit anahtar kullanılır. Anahtarlar, üretilirken rasgele sayı üreteci denen fonksiyonlardan yararlanılır.

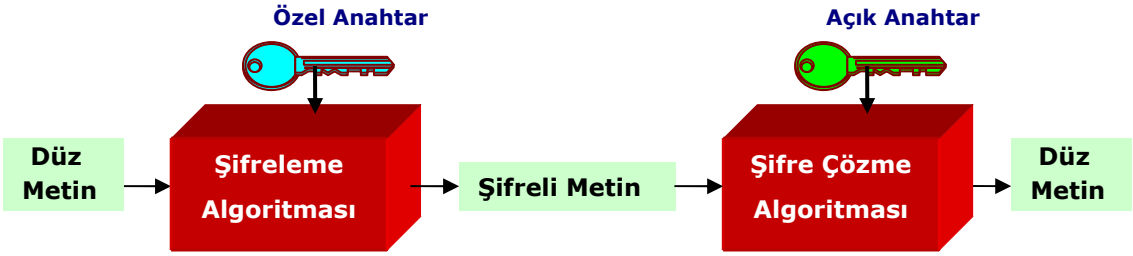
Ancak yüzyıllar boyu kullanılan ve birçok mesajı yabancılardan ve düşmanlardan korumaya yarayan gizli anahtarlı şifrelemenin de kendine özgü sorunları bulunmaktadır. Mesajın değiştirilmesinin önlenmesi, şifrelemede ve şifre çözmede kullanılan anahtarın gönderici ve alıcı arasında paylaşımı, mesajı gönderenin kimlik doğrulamasının yapılamaması çözülmesi gereken sorunlardır.




**Şekil 5 Gizli Anahtarlı Şifreleme**

Gizli anahtarlı şifrelemenin bu gibi sorunlarını aşmak için açık anahtarlı şifreleme yöntemleri geliştirilmiştir. Burada biri **açık** diğeri **özel** olarak nitelenen bir anahtar çiftinin bulunduğu (asimetrik) bir yöntem kullanılmaktadır. Bu iki anahtar, üretilirken birlikte üretilirler. Yani matematiksel olarak aralarında gizli bir bağ bulunur. Bu sayede bir anahtar çiftindeki bir anahtar ile, diğer anahtarla şifrelenmiş bir metnin şifresi çözülebilir (Şekil 6). Bununla birlikte bir anahtara sahip olan bir kişinin, matematiksel yollarla diğer anahtarı elde etmesi mümkün değildir. Şekil 7'de örnek olarak bir açık anahtar verilmiştir.

Açık anahtarlı şifreleme elektronik imza teknolojisinin temelini oluşturur. Bölüm 2.2'de açık anahtarlı şifreleme kullanılarak nasıl bir elektronik imza oluşturulduğu açıklanmıştır.




**Şekil 6 Açık Anahtarlı Şifreleme**

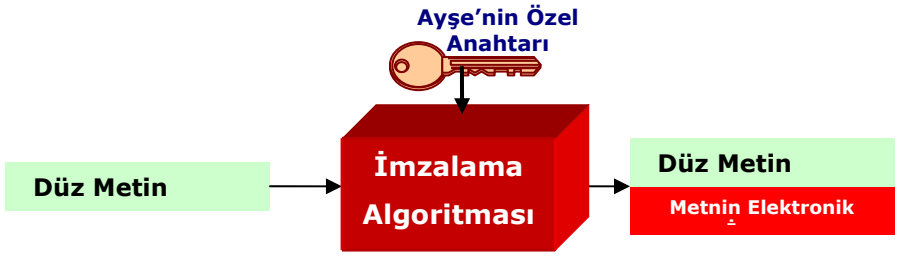
```
MIIF4jCCBMqgAwIBAgIKQg6ypAAAAAAAJjANBgkqhkiG9w0BAQUFADCBsDELMAkGA1UEBhMCVVMxC
zAJBgNVBAgTAlVUMRcwFQYDVQQHEw5TYWx0IExha2UgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUl
VTVCBOZXR3b3JrMSEwHwYDVQQLExhodHRwOi8vd3d3LnVzZXJ0cnVzdC5jb20xODA2BgNVBAMTL1VU
TiAtIFVTRVJUcnVzdCBDbGllbnQgQXV0aGVudGljYXRpb24gYW5kIEVtYWlsMB4XDTAwMDQyNzE3NDQy
M1oXDTAxMDQyNzE3MzU1MFowgbQxKDAmBgkqhkiG9w0BCQEWGW1tZXJyaWxsQG1lcnJpbGx0aXRs
ZS5jb20xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJVVDEQMA4GA1UEBxMHTWlkdmFsZTEZMBcGA1UE
ChMQTWVycmlsbCBUaXRsZSBDbzElMCMGA1UECxMcaHR0cDovL3d3dy51c2VydHJ1c3QuY29tL2NwczE
aMBgGA1UEAxMRTWFydGluIFcuIE1lcnJpbGwwXDANBgkqhkiG9w0BAQEFAANLADBIAkEA1LD07KIbyq
mOx+sUT5QKZMR8gZDtG3rDK6ii8xirrYccLQDbyttNGTYGzqTJ3Fmpi4PIAdvdJRoFlek
```

**Şekil 7 Açık Anahtar**

## 2.2 Elektronik İmzanın İşleyişi

Ayşe kendi oluşturduğu bir elektronik postayı Barış'a güvenli bir şekilde ulaştırmak istemektedir. Ayşe'nin bir açık, bir de özel anahtarı vardır ve açık anahtarını Barış'a daha önceden ulaştırmıştır. Bu gönderim şu şekilde gerçekleşir:

1) Ayşe özel anahtarı ile metni şifreler, böylelikle metnin imzasını oluşturmuş olur (Bkz. Şekil 8). Ayşe'nin özel anahtarı, Ayşe'den başkasında olmadığından ve başka bir anahtar kullanarak bu imzanın birebir aynısını oluşturmak mümkün olmadığından, üretilen bu imza bilgisi Ayşe'ye özeldir.




**Şekil 8 Elektronik İmzanın Oluşturulması**

Ayşe imzalı metni Barış'a gönderir.

2) Barış, Ayşe'nin açık anahtarını kullanarak imzayı onaylama işlemini gerçekleştirir (Şekil 9 - 1. adım). Ortaya çıkan onaylanmış imza metni ile düz metin aynı ise imza doğrulanmış olur (Şekil 9 - 2. adım).


**Şekil 9 Elektronik İmzanın Onaylanması**

Buradaki senaryoda, Ayşe, imza bilgisini düz metnin sonuna ekleyerek Barış'a gönderdi. Barış, Ayşe'nin elektronik imzasını onayladıktan sonra şu sonuçlara varabilir:

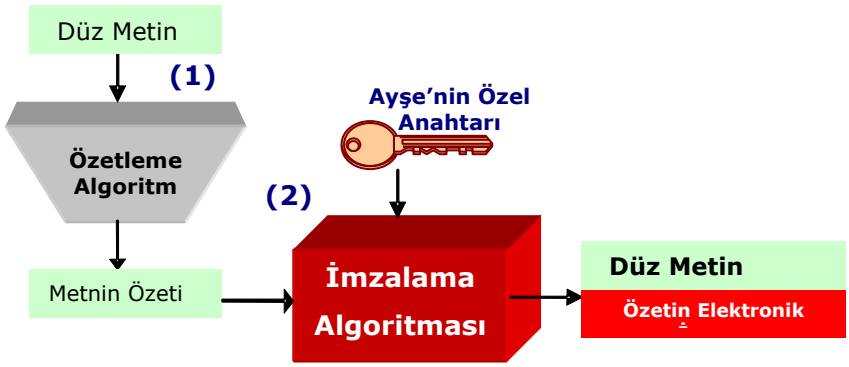
- "Düz metin değiştirilmeden bana ulaştı"
- "Metnin elektronik imzası Ayşe'nin açık anahtarı ile doğrulandı. Demek ki bu imza Ayşe'den başkası tarafından atılmış olamaz. Öyleyse mesajı gerçekten Ayşe gönderdi"
- "Daha sonra Ayşe bana gönderdiği bu mesajı göndermediğini iddia ederse, ona yalnızca kendisi tarafından özel anahtarını kullanarak oluşturulabilecek elektronik imzasını gösterebilirim"

Şifrelemede genel olarak, şifrelenecek/imzalanacak metnin boyu ne kadar artarsa, işlem süresi de ona bağlı olarak artar. İmzalanacak metnin boyu büyüdükçe de imzalama süresi ona bağlı olarak dramatik bir şekilde yükselir. Pratik uygulamalarda açık anahtar algoritmaları uzun metinlerin imzalanmasında, imzalama süresinin saniyeler hatta dakikalar alması nedeniyle başarım açısından çok yetersiz kalmaktadır. Metin boyutlarının çok değişken olması imzalama sürecinin ne kadar zaman alacağına ilişkin net bir tahmin yapılmasını engellemektedir. Buna ek olarak, imzalanacak veri ile elektronik imza aynı boydadır. Yani elektronik imza verisinin boyu, imzalanan verinin boyuna eşittir. Yukarıdaki örnekte olduğu gibi düz metnin doğrudan imzalanması, iletim hattının iki kat daha fazla kullanılmasına neden olacaktır.

Bu iki problemi çözmek ve başarımı arttırmak için elektronik olarak imzalama yapılmadan önce **tek-yönlü özet algoritması** (hash) kullanılarak metnin sabit uzunlukta bir özeti üretilir. Özet algoritmaları metnin boyu ne olursa olsun sabit uzunlukta bir çıktı üretmektedir.

Yukarıdaki senaryoyu özetlemeyi de içine alacak şekilde şöyle değiştirebiliriz:

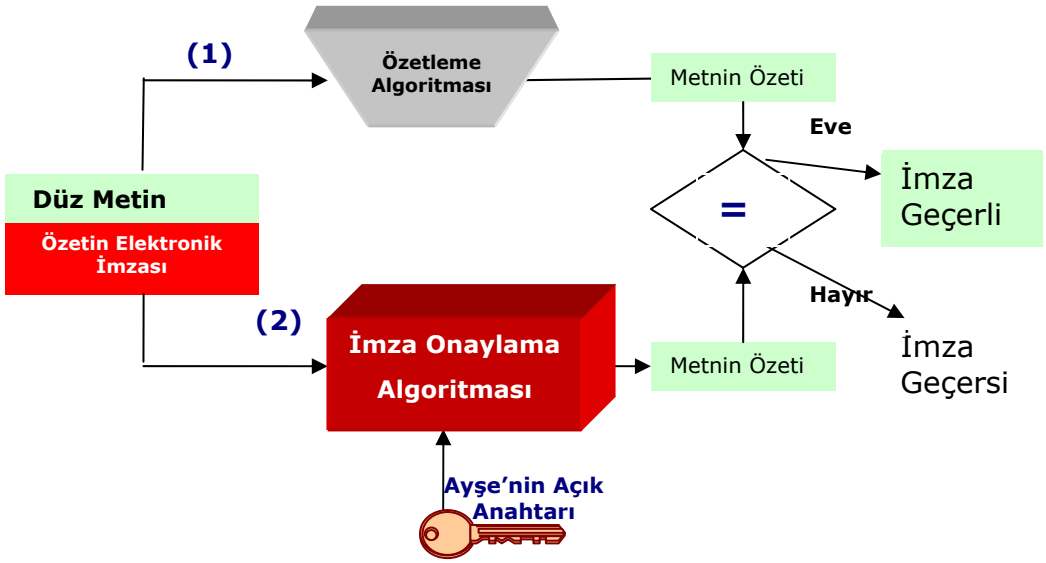
1. Ayşe gönderilecek metni tek-yönlü özet fonksiyonundan geçirir ve metnin boyundan bağımsız olarak ancak metnin karakterini içerecek şekilde sabit uzunluklu bir özet oluşturmuş olur (Şekil 10 – 1. adım).
2. Ayşe tek-yönlü fonksiyon çıktısını özel anahtarı ile şifreler. Böylece metnin elektronik imzasını oluşturmuş olur (Şekil 10 – 2. adım).
3. Ayşe metnin sonuna 2. adımda oluşturduğu metnin elektronik imzasını ekleyerek Barış'a gönderir.




**Şekil 10 Elektronik İmzanın Metnin Özeti Alınarak Oluşturulması**

4. Barış Ayşe'nin gönderdiği düz metnin tek-yönlü fonksiyon ile özetini üretir (Şekil 11 - 1. adım). Ardından, imza onaylama algoritmasını kullanarak, Ayşe'nin açık anahtarıyla bu metnin elektronik imzasının şifresini çözer (Şekil 11 – 2. adım).

5. Eğer 1. adım ve 2. adımda elde edilen sonuçlar birbirinin eşi ise, metnin elektronik imzası geçerli anlamın gelir.




**Şekil 11 Elektronik İmzanın Onaylanması**

## 2.3 Açık Anahtar Altyapısı

Elektronik İmza'nın kullanılması için elverişli bir ortam sağlayan açık anahtarlı şifreleme yöntemleri, hedeflenen güvenlik gereksinimlerini karşılamakla birlikte bir takım zorluklara da sahiptir. Bunlar kısaca şöyle özetlenebilir:

- Anahtar çiftlerinin üretimi
- Anahtarla sahibinin eşleştirilmesi
- Anahtarların tanınması
- Özel anahtarın korunması

- Farklı uygulamalarda aynı imzanın kullanılabilmesi

Yukarıda sıralanan sorunlara çözüm getirmek, açık anahtarlı şifreleme yöntemlerinin kullanımı yoluyla yukarıda bahsedilen bütünlük, kimlik doğrulama ve inkâr edilmezlik hizmetlerini kullanıcılara vermek ve elektronik imza teknolojisinin kolay kullanımını sağlamak için gerekli teknoloji, standart, yasa, yönetmelik, kuruluş, ürün ve hizmetlerin bütününe "*Açık Anahtar Altyapısı (AAA)*" denir.

AAA'nın temel bileşenleri şunlardır:

**Elektronik sertifikalar**: Kişinin kimlik bilgileriyle açık anahtarını birbirine bağlayan elektronik kayıttır. Sertifika için genel olarak Uluslararası Telekomünikasyon Birliği'nde (ITU) geliştirilen X.509 standardı kabul görmektedir. Elektronik sertifika sayesinde, kişilerin elektronik anahtarlara sahip olması sağlanır. Elektronik sertifika, sanal ortamdaki kimlik kartımızdır.

**Elektronik sertifika hizmet sağlayıcısı**: Elektronik sertifikada yer alan bilgilerin doğruluğundan emin olunması için bir güven modeline ihtiyaç duyulmaktadır. Elektronik imza yasasında tanımlanan elektronik sertifika hizmet sağlayıcılar (ESHS), sertifika veren kuruluşlar olarak tanımlanmaktadır. ESHS, güven ve itibarın tesisi için belirlenmiş kurallara bağlı olarak faaliyetlerini yürütmek ve yasa ile belirlenen bir kuruluş tarafından denetime açık olmak zorundadır. Türkiye'de ESHS faaliyetlerini düzenleyici kurum olarak Telekomünikasyon Üst Kurulu (TK) görevlendirilmiştir.

**Elektronik imza algoritmaları**: Elektronik imza üretmek ve bir elektronik imzanın doğruluğunu onaylama için kullanılan karmaşık matematiksel fonksiyonlar grubudur. Bu algoritmalara örnek olarak RSA, EC, SHA-1, MD5 verilebilir.

**Güvenlik protokolleri**: Elektronik imzanın, uygulamaların bir parçası olarak kullanılmasını sağlayan iletişim kuralları dizisidir. Örneğin, SSL (secure socket layer) Web sunucusuyla İnternet tarayıcısı arasında çalışan ve güvenli haberleşme sağlayan açık anahtar altyapısı temelli bir iletişim protokolüdür.

**Uygulamaya ilişkin diğer standartlar**: Anahtarların saklanması, değiştirilmesi, elektronik imzanın oluşturulması, taşınması konularıyla ilgili oluşturulmuş standartlardır. Bugün RSA Laboratuarları öncülüğünde geliştirilmiş olan PKCS ("public key cryptography standards" – açık anahtar kriptografisi standardları) geniş kabul gören ve kullanılan Standartlardan biridir.

**Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları**: Anahtarların ve sertifikanın güvenlik içinde taşınması ve elektronik imza oluşturmak ve doğrulamak amaçlarıyla kullanılan USB çubuk (token), akıllı kart (smart card) ve akıllı kart okuyucular gibi cihazlardır (Bkz. Bölüm 6)

**ESHS'nin çalışma ilkeleri ve esasları ve yönetmelikler**: ESHS'ler, çalışma ilkelerinin ve kurallarının ne olduğunu ve bu ilke ve kurallara uygun olarak faaliyetlerini nasıl yerine getirdiklerini yayınladıkları belgelerle açıklarlar. Ayrıca TK, hizmet sağlayıcılarının uyması gereken kuralları yönetmeliklerle düzenler.

Bir AAA'nın sağlıklı bir şekilde işleyişi, yukarıda özetlenen bileşenlerin birbirleriyle uyum içinde çalışmasına bağlıdır.

# 3 Elektronik Sertifika Hizmet Sağlayıcının Görevleri

Bu bölümde bir Elektronik Sertifika Hizmet Sağlayıcı'nın (ESHS) yasal olarak yerine getirmesi gereken görevlere ilişkin bilgiler verilmiştir. Yasaya göre ESHS şöyle tanımlanmaktadır (Madde 8):

"ESHS, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuki tüzel kişilerdir."

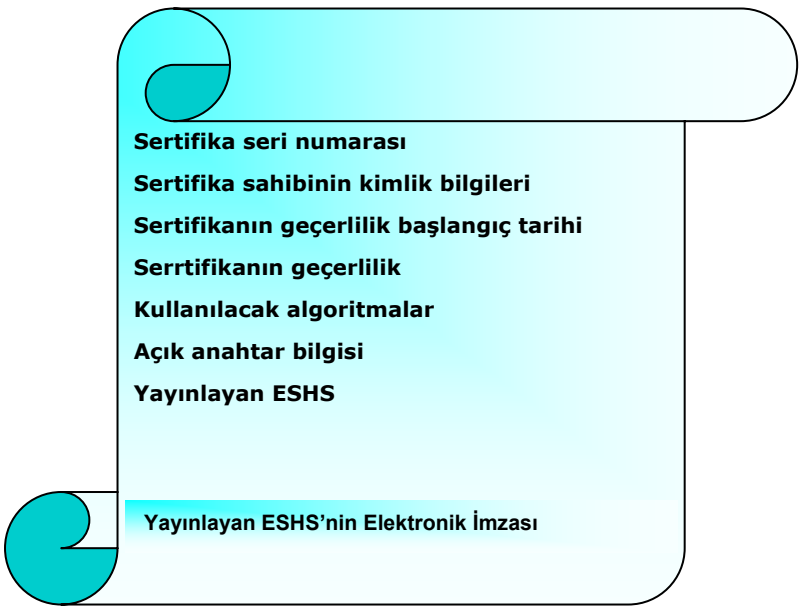
Elektronik imzanın tanımı Bölüm 2'de verilmişti. Bu bölümde de öncelikle yasada tanımlanan elektronik sertifika, zaman damgası hakkında gerekli bilgiler verilmiştir.

## 3.1 Elektronik Sertifika

Bir ESHS'nin temel görevi elektronik sertifika yayınlamaktır. Yasada elektronik sertifika şöyle tanımlanır (Madde 3ı): "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı".

Bir elektronik sertifika, kullanıcı kimliği ile kullanıcı için üretilen imza doğrulama verisini, yani kullanıcının açık anahtarını birbiri ile ilişkilendiren bir veri yapısıdır. Bu özelliği ile elektronik sertifika kullanıcıların sanal ortamdaki kimlik kartı olarak nitelendirilebilir.

Elektronik Sertifika, bir ESHS tarafından yayınlanır. Temel olarak bir elektronik sertifika içinde yer alan bilgiler Şekil 12'de belirtilmiştir. Aşağıda bu bilgilerin kısa açıklamaları verilmiştir:




**Şekil 12 Elektronik Sertifika**

**Sertifika seri numarası**: Yayınlayan tarafından üretilen sertifikaya ait tekil kimlik numarasıdır.

**Sertifika sahibinin kimlik bilgileri:** Sertifika sahibini tekil olarak tanımlayabilen kimlik bilgileri. Bu bilgilere örnek olarak T.C. Kimlik Numarası, adı, soyadı, e-posta bilgileri verilebilir.

**Sertifika geçerlilik başlangıç tarihi:** Sertifika belirtilen bu tarihten önce kullanılamaz.

**Sertifika geçerlilik sonlanma tarihi:** Sertifika belirtilen bu tarihten sonra kullanılamaz.

**Sertifikanın kullanım amacı:** Bu sertifika ve içinde yer alan açık anahtar bilgisinin ne amaçla kullanılmak üzere yayınlandığı belirtilir. Bir sertifika, örneğin, elektronik imzalama, şifreleme, kimlik doğrulama gibi amaçlarla kullanılabilir.

**Kullanılacak algoritmalar:** Bu açık anahtar bilgisinin hangi algoritmalarla birlikte kullanılabileceği yazılır. Örnek olarak RSA, DSA, EC, DH verilebilir.

**Açık anahtar bilgisi:** Bu sertifikada kimliği tanımlanan kullanıcıya ait açık anahtar.

**Yayınlayan ESHS:** Bu sertifikayı yayınlayan ESHS'nin kimlik bilgileri.

**Yayınlayanın elektronik imzası:** Bu sertifikayı yayınlayan ESHS, sertifika bilgilerini kendi özel anahtarını kullanarak imzalar. Bu sertifikayı kullanacak bir kullanıcı, imzayı ESHS'nin açık anahtarı ile onaylayarak, gerçekten belirtilen ESHS tarafından yayınlandığından emin olur.

Yukarıda özellikleri belirtilen bir elektronik sertifikanın yasal olarak geçerli olan güvenli elektronik imza oluşturmak amacıyla kullanılabilmesi için, yasada tarif edilen "Nitelikli Elektronik Sertifika" özelliklerine sahip olması gerekir.

## 3.2 Nitelikli Elektronik Sertifika

5070 sayılı Kanun uyarınca gereken şartları sağlayan ve TK tarafından yetkilendirilmiş nitelikli bir ESHS tarafından verilmiş sertifikalardır. Nitelikli elektronik sertifikalar ITU-T Rec. X.509V.3 standardına uymak zorundadır (Tebliğ Madde 5). Buna göre bir nitelikli elektronik sertifikada yer alması zorunlu olan bilgiler şunlardır (Madde 9):

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare
- ESHS'nin kimlik bilgileri ve kurulduğu ülkenin adı
- İmza sahibinin teşhis edilebileceği kimlik bilgileri
- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi (yani kullanıcının açık anahtarı)
- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri
- Sertifikanın seri numarası

- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi
- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri
- Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgiler
- ESHS'nin sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası

## 3.3 Zaman Damgası

Özellikle belirli bir son işlem tarihi olan vergi beyannamesi vermek, fatura ödemesi yapmak gibi işlemlerde, elektronik hizmetten önce son gün beyannamesini vermeyen ya da ödemesini yapmayan rahatlıkla tespit edilebilirdi. Çünkü vergi dairesi ya da bankalar belli bir saatte kapanırlardı. O saate kadar da işlemi gerçekleştirmeyen yükümlüler geç kalmış sayılırdı. Ancak elektronik ortamda gerçekleşen işlemlerde alıcının saati ile göndericinin saati birbirinden farklı olabilir. Bu nedenle işlemin gerçekleştiği tam saatin bilinmesi bir gereklilik halini almıştır. Elektronik bir veriye, bu veriye ilişkin tarih/saat bilgisinin güvenilir bir kaynaktan edinilerek eklenmesine "Zaman Damgası" denir. Yasanın 3h maddesinde Zaman Damgası şöyle tanımlanmaktadır:

*"Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespiti amacıyla, ESHS tarafından elektronik imza ile doğrulanan kaydı." (Bkz. Ek-A)*

Buna göre ESHS'nin temel görevlerinden biri de kullanıcılara zaman damgası hizmeti vermektir. ESHS bu hizmeti verirken bir takım uluslararası standartlara uygun olarak vermekle yükümlüdür. (Tebliğ Madde 10)

Ayrıca ESHS zaman damgası hizmetlerini vermesi ile ilgili ilke ve uygulama esaslarının belirtildiği belgeleri yayınlamakla yükümlüdür.

Kullanıcının bu hizmeti almak için ESHS'den talep etmesi gerekir (Yönetmelik Madde 31).

## 3.4 Elektronik Sertifika Hizmet Sağlayıcısı

Yasaya göre Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir (Yasa Madde 8).

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

- Güvenli ürün ve sistemleri kullanmak,
- Hizmeti güvenilir bir biçimde yürütmek,
- Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Her sertifika hizmet sağlayıcısı, çalışma ilkesi ile ilgili ayrıntılı bilgilerin bulunduğu Sertifika Uygulama Esasları (SUE) ve Sertifika İlkeleri (Sİ) adlı belgeleri yayınlamalıdır.

## 3.5 ESHS'nin Yükümlülükleri

TK tarafından nitelikli sertifika vermek üzere yetkilendirilen ESHS'lerin yükümlülükleri şunlardır (Yasa Madde 10):

- Hizmetin gerektirdiği nitelikte personel istihdam etmek
- Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere dayanan güvenilir bir biçimde tespit etmek
- Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemek
- İmza oluşturma verisinin ESHS tarafından veya sertifika talep eden kişi tarafından ESHS'ye ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya ESHS'nin sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamak
- Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmek
- Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmek
- Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamak
- Faaliyetine son vereceği tarihten en az üç ay önce durumu TK'na ve elektronik sertifika sahibine bildirmek

ESHS'ye yüklenen yukarıdaki yükümlülükler ile yasa şunları garanti etmektedir:

- İmzası doğrulanan şahıs, gerçekten kimliği belirtilen şahıstır.
- ESHS'nin faaliyetleri sonlansa bile, ondan elektronik sertifika almış kişilere hizmetin devamlılığını sağlamak için gerekli önlemler alınmıştır.
- Kullanıcının, kullanım konusunda bilinçlendirilmesi sağlanmıştır.
- ESHS, üretilen imza oluşturma verisinin (yani sertifika sahibinin özel anahtarının) bir kopyasını alamaz veya bu veriyi saklayamaz. Bu demektir ki ESHS sadece nitelikli elektronik sertifikanın yayınlanma aşamasında devreye girer. Bir ESHS'nin yaptığı iş esas olarak, kendisi tarafından verilmiş nitelikli elektronik sertifikayı kullanan imza sahibinin kimliğini tarafsız 3. şahıs sıfatıyla doğrulamaktır. Bu sertifikayı kullanarak gerçekleşen güvenli iletişim yalnızca iletişime katılan tarafları ilgilendirir.

## 3.6 Sunucu Sertifikası

Sunucu sertifikaları, Web sunucularının kimlik bilgilerini ve açık anahtarını taşıyan ve bu sunuculara bağlanan kullanıcılara sunulan elektronik sertifikalardır. Özellikle son dönemlerde artan ve ülkemizde de görülen internet üzerinden dolandırıcılık faaliyetlerinin bir kısmı, gerçeğine çok benzeyen taklit Web siteleri aracılığı ile gerçekleştirilmektedir. Sunucu sertifikaları ile bağlanılan web sitesinin kimliği güvenilen bir ESHS aracılığı ile doğrulanabilir.

Sunucu sertifikası, kişisel sertifikalar gibi X.509 standardına uygun üretilirler. Bu sertifika sayesinde, bağlanılan Web sunucusunun, kullanıcılar açısından kimlik doğrulaması yapılmış olur. Bu yöntemde kullanıcı, bağlandığı web sitesinde hiçbir işlem yapmadan önce sunucu sertifikasının doğruluk sınamasını gerçekleştirir. Sertifikadaki sunucu kimlik bilgisi, sertifika geçerlilik süresi gibi bilgiler elle kontrol edilir. Bunun yanında, en önemlisi, bu sertifikanın TK tarafından yetkilendirilmiş bir ESHS tarafından yayınlanıp yayınlanmadığına bakılır.

İsteğe bağlı olarak, bu kimlik doğrulaması çift taraflı olarak gerçekleşebilir. Bu yöntemle hem Web sunucusu, karşısındaki kullanıcının kimliğinden hem de kullanıcı Web sunucusunda emin olabilir. Bu kimlik doğrulama işleminde bugün yaygın olarak kullanılan yöntem, aynı zamanda kullanıcı ile Web sunucusu arasında şifreli haberleşmeye de olanak tanıyan SSL protokolüdür.

## 3.7 Sertifika İlkeleri ve Sertifika Uygulama Esasları

ESHS tarafından yayınlanması zorunlu olan bir belgelerdir (Tebliğ Madde 7). Sertifika İlkeleri, sertifika kullanımı, sertifika yaşam çevrimi ile ilgili kurallar listelenir. ESHS, elektronik sertifikalar ve kurduğu AAA ile ilgili tüm iş sürecini bu belge ile tanımlar.

Sertifika Uygulama Esasları'nda, Sertifika İlkeleri belgesinde belirtilen kuralların nasıl uygulanacağı ayrıntılı bir biçimde ifade edilir. Genellikle Sertifika Uygulama Esasları, Sertifika İlkeleri'ne göre daha uzun, kapsamlı ve teknik bilgiler içeren bir belgedir.

ESHS, bu iki belgeyi IETF RFC 3647'ye uygun olarak hazırlamalıdır.

### 3.7.1 Elektronik Sertifikaların Kullanım Süresi

Her elektronik sertifikanın belli bir kullanım süresi vardır. Bir kişi için bir ESHS tarafından yayınlanan elektronik sertifika, sertifika sahibi tarafından hayatı boyunca kullanılamaz. Sertifikanın kullanımının bir başlangıç bir de bitiş süresi vardır. Elektronik imza uygulamaları, elektronik sertifikalarla işlem yapmadan önce sertifikanın geçerlilik süresini kontrol ederler. Genellikle bu süre bir yıldır.

ESHS'nin sertifikasının da bir geçerlilik süresi vardır. Bu süre 10 yılı aşamaz. (Yönetmelik Madde 18)

## 3.8 Sertifika Yaşam Çevrimi

Bir sertifikanın üretilmesinden iptaline kadar geçirdiği aşamalara "Sertifika Yaşam Çevrimi" denir. Bu çevrim, ESHS tarafından net bir şekilde Sertifika İlkeleri ve Sertifika Uygulama Esasları belgeleri içinde tanımlanır. Aşağıda bir sertifika yaşam çevrimi, genel hatlarıyla tarif edilmiştir. Gerçek uygulamalarda bazı farklılıklar olabileceği unutulmamalıdır.

### 3.8.1 Sertifikanın Yayınlanması

1. Kullanıcı, elektronik sertifika almak için ESHS'ye başvurur. Bu başvuru adımında, kimlik doğrulamanın güvenliği için yüz yüze görüşme gereklidir.
2. ESHS, kullanıcının kimliğini doğrular ve sertifikayı yayınlar.
3. ESHS, sertifikayı, herkese açık bir ortama (örneğin bir dizin hizmeti üzerine) aktarır.

### 3.8.2 Sertifikanın Kullanımı

1. Kullanıcı gerçekleştirdiği işlemi ya da göndereceği mesajı kendi özel anahtarı ile imzalar ve alıcıya iletir (**Error! Reference source not found.**).

2. Alıcı mesajı alır, mesajdaki sayısal imzayı göndericinin açık anahtarıyla doğrulaması gerekir. Bunun için kullanıcının nitelikli elektronik sertifikasını ESHS'nin herkese açık dizin hizmeti üzerinden sorgular ve sertifikayı elde eder.

3. Sertifikadaki geçerlilik süresini, nitelikli sertifika olup olmadığını ve imzalayan ESHS'nin imzasının doğruluğunu kontrol eder.

4. 2. ve 3. aşamadan sorunsuz geçildikten sonra, mesajdaki elektronik imzanın alıcıya ait olup olmadığını kontrol eder. Bunu imza onaylama işlemi ile gerçekleştirir (Şekil 11). İmza onaylanırsa alıcı, mesajı gönderinin kimliğinden, mesajın alıcıdan çıktığı şekliyle kendisine ulaştığından ve göndericinin bu mesajı gönderdiğini daha sonra inkâr edemeyeceğinden emin olur.

### 3.8.3 Sertifikanın İptali ve Askıya Alınması

Bir nitelikli elektronik sertifika, özel anahtarın kaybolması veya sertifikanın geçerlilik süresinin sonuna gelmesi durumlarında iptal edilebilir. Geçici süreyle kullanımdan kaldırılacak olan sertifikalar ise askıya alınır. İptal edilen sertifika tekrar kullanılamaz. Askıya alınan sertifika, askıda olduğu süre boyunca kullanılamaz. Ancak askıda olan bir sertifika askıdan indirildiğinde normal kullanımına devam edilebilir.

ESHS, iptal edilen sertifikaları Sertifika İptal Listesi (SİL) adında bir liste ile periyodik olarak yayınlar. SİL için genel kabul görmüş X.509 v2 standardı kullanılmaktadır. ESHS, aynı yayınladığı sertifikalarda olduğu gibi yayınladığı SİL'leri de elektronik olarak imzalar. Bir sertifika iptal edildiğinde, bir sonraki SİL içerisinde iptal edilen sertifikaya ilişkin bilgileri yayınlanır. Sertifikaların tutarlı bir şekilde kullanılabilmesi için SİL her kullanımda kontrol edilmelidir.

SİL'de üç tür sertifika yer alır:

- İptal edilen sertifikalar
- Geçerlilik süreleri dolan sertifikalar
- Geçici olarak kullanımdan kaldırılan (askıya alınan) sertifikalar

Türkiye'deki nitelikli elektronik sertifikaların askıya alınması yasal olarak tanımlanmış bir işlem değildir. Bu nedenle bu bölümde askıya alma konusunda verilen bilgiler sadece okuyucuyu bilgilendirme amaçlıdır.

## 3.9 Kök Sertifika

ESHS'nin elektronik sertifikasına **kök sertifika** denir. ESHS'nin, kendisinden elektronik sertifika alan kullanıcılar gibi bir çift anahtarı vardır. Bu anahtarlardan özel anahtar, yayınlanan elektronik sertifikaları imzalamak için kullanılır. ESHS'nin açık anahtarı ise ESHS'nin kök sertifikası içinde yer alır ve kullanıcılar tarafından bu ESHS'nin yayınladığı elektronik sertifikalara attığı elektronik imzasının doğrulanması için kullanılır. Bir nitelikli elektronik sertifika, ancak yayınlayan ESHS'nin sertifika üzerindeki imzası geçerliyse kullanılabilir. Bir nitelikli elektronik sertifikaya ulaşan bir kullanıcı, öncelikle bu sertifikanın geçerliliğini, sertifika üzerindeki ESHS imzasının geçerliliğini kontrol ederek sınar Kök sertifika açık anahtarın ESHS'nin olduğunu onaylar.

ESHS'nin özel anahtarı, bir AAA sistemindeki güven zincirinin en önemli halkasıdır. ESHS'nin özel anahtarı, yetkisiz bir kullanıcının eline geçerse, AAA üzerinde verilen tüm güvenlik hizmetleri ve kurulan güvenli iletişim altyapısı tehlikeye düşer. Bu nedenle ESHS'nin özel anahtarını saklamak için özel ve yüksek güvenlik içeren saklama ortamları kullanılır. Küçük bir kutuya benzeyen ve yalnızca yetkili kullanıcıların ve programların erişmesine izin verecek şekilde ESHS'nin özel anahtarını saklayan bu cihazlara Donanım Güvenlik Modülü (Hardware Security Module) denir.

## 3.10 Elektronik Sertifikaların Uygulama Alanları

Elektronik imza ve buna bağlı olarak elektronik sertifikalar, sağladıkları güven altyapısı sayesinde kendisine birçok uygulama alanı bulmuştur. Bu alanlardan bazıları şöyle özetlenebilir:

- **Bütünlük, Kimlik Denetimi ve İnkar Edememezlik Hizmetleri:** Kurumlar mesajların doğru kişi tarafından, içeriği değiştirilmeden ve karşı tarafın inkar edemeyeceği şekilde iletimini sağlamak için elektronik sertifikalar kullanırlar. Yönetmeliğin 15d maddesine göre nitelikli elektronik sertifikalar yalnızca bütünlük hizmetini karşılamak amacıyla yayınlanabilir ve kullanılabilir. Bununla birlikte bir belgenin elektronik imzasını doğrulama işlemi, o belgenin bütünlüğünü garanti ederken, göndericinin kimlik doğrulamasını da otomatik olarak gerçekleştirdiği unutulmamalıdır. Kimlik doğrulama hizmetinin kapsam dışı bırakılmasının sonucunda kamu kurumları ya eski zayıf kimlik doğrulama yöntemlerinde devam edecekler ya da güçlü kimlik doğrulama sistemleri kurmak için yüksek maliyetli yatırımlar yapacaklardır. Bu bağlamda yönetmeliğin 15d maddesi hakkında Kamu SM yetkilileri görüşlerini gerekçeleri ile birlikte daha net bir şekilde ortaya koymalıdırlar

- **Erişim Denetimi:** Bilgisayar sistem ve terminallerine, İnternet sitelerine, kurum içi ağ üzerindeki hizmetlere erişim denetimini sağlamak amacıyla kullanılırlar.
- **Belge İletiminin ve İletim Zamanının İspatı:** Kritik belgelerin hukuksal açıdan zamanını ve tarihini doğrulamak için elektronik imza yasası ile birlikte gelen zaman damgası hizmeti kullanılabilir.
- **Elektronik İş Akışı:** Kağıt üzerinde işleyen bürokrasi, ıslak imza yerine geçebilen güvenli elektronik imza sayesinde elektronik ortamda çok daha hızlı, düşük maliyetli ve güvenilir bir şekilde gerçekleştirilebilir.
- **Resmi başvuru işlemleri**: Bu işlemler, devlet dairesine gitmeden, zaman kaybetmeksizin, bilgisayar başından gerçekleştirilebilir. İşlemlerin sonuçları da aynı yolla izlenebilir.
- **Arşivleme:** Depolanmış elektronik belgelere ya da mesajlara erişildiğinde, belgenin değiştirilmeden orijinal haliyle saklandığından emin olunması amacıyla kullanılabilir.

Bütün bu hizmetlerin yanında elektronik imzanın verinin gizliliği için kullanılamayacak bir teknoloji olduğu unutulmamalıdır. Elektronik imzanın dayandığı açık anahtarlı kriptografik sistem ile veri şifrelemek yüksek maliyetli ve uzun süreler gerektiren bir işlemdir. Bu nedenle elektronik imza teknolojisi, teknolojik olarak mümkün olsa bile, dünyadaki uygulamalarda da gizlilik hizmetini sağlamak için kullanılmaz. Gizlilik hizmeti, elektronik imzanın da birlikte çalışabildiği SSL protokolünün kullanımı ile sağlanabilir.

## 3.11 Secure Sockets Layer (SSL)

İnternet üzerindeki iletişimlerde kimlik doğrulaması ve şifreli veri iletimi için Netscape Communications tarafından tasarlanmış iletişim protokolüdür. En yaygın kullanımı alanı Web sunucuları ve tarayıcıları arasındaki iletişimin güvenli hale getirilmesidir.

Kimlik doğrulama işlemi için elektronik sertifikalar kullanılmaktadır. Şifreleme, kimlik doğrulama ve veri bütünlüğü kontrol özellikleri, ihtiyaca göre hem sunucu hem de istemci tarafında gerçekleştirilmek üzere ayarlanabilir. Örneğin, yalnız sunucunun kimliğinin doğrulanması için SSL protokolü aracılığı ile sunucu sertifikasının tarayıcıya iletilmesi kontrol için yeterlidir.

## 3.12 Elektronik Sertifika Hizmet Sağlayıcılı ile Noterlerin Farkı

Elektronik Sertifika Sağlayıcılığı ile noterler arasında bir takım benzerlikler bulunmakla beraber aslında hizmet yapılarında farklılıklar bulunmaktadır. Noterler, bir işlemin vaki olduğunun resmi kaydını zaman mührüyle birlikte tutarlar. Bu anlamda işleme ve/veya kişilere güvenilir tanık durumundadırlar. Örneğin noterde bir sözleşme yapıldığında, noter açısından sözleşme içeriğinin hukuki boyutları önemli değildir. Önemli olan, evrakın ilgili taraflarca belirtilen tarihte noterin huzurunda ve tanıklığında imzalandığıdır. Noterin kimlik tespiti de beyan usulünde çalışır. Kimliği doğrulamak yerine evraktaki kimlikle kişinin beyan ettiği kimlik belgesini karşılaştırır. Bir noter, noterlik hizmeti alan bir vatandaşla daha önce çalışmış olmak zorunda değildir.

Kimlik doğrulamada ESHS, noterde olmayan bir sorumluluk taşımaktadırlar. ESHS, işlemi gerçekleştiren şahsın kimliğin doğruluğunu da kontrol eder. Bununla birlikte gerçekleştirilen işlemle ilgisi yoktur. Gerçekleştirilen işlem veya gönderilen belge tamamen iletişim kuran tarafları ilgilendirir. ESHS, bu iletişimde güven altyapısının oluşmasını sağlayan ve iletişimin temel güvenlik gereksinimlerine uygun bir biçimde çalışır. ESHS, bir kimyasal tepkimede, uygun ortam şartlarını sağlayan bir katalizör gibi görev yapar.

İletişim esnasında, elektronik imzanın onaylanması aşamasında sertifikanın geçerliliğinin kontrolüne ihtiyaç duyulabilir.

Ayrıca belgeye eklenmek üzere zaman damgası hizmeti alınabilir. Bu hizmet, belgeyi görmeden zaman bilgisinin belgeye iliştirilmesi olarak düşünülebilir. Bu işlemde de ESHS, tam olarak noter gibi davranmaz. Çünkü noter, noterlik hizmeti alınan belgenin bir kopyasını alır, içini görür, yapılan sözleşmenin/anlaşmanın miktarına bağlı olarak bir hizmet bedeli ve devlet adına damga vergisi alır. Bununla birlikte ESHS belgenin içeriği ile ilgilenmez. Ancak mesaj sahibi, mesajı imzalamakta kullanacağı nitelikli elektronik sertifika için ya da zaman damgası hizmeti için ESHS'ye bir ücret ödediğinden, dolaylı olarak da olsa bir ücretlendirme söz konusudur.

ESHS belgenin içeriği ile hiç ilgilenmez sadece belgenin gönderenin gönderdiği gibi alıcıya ulaştırılmasını yani değiştirilmediğini ve inkar edilemeyeceğini garanti eder. Öte yandan, noter huzurunda yapılan diğer pek çok işlemin (alım-satım işlemleri, vekaletler, ve benzeri) yasal olarak elektronik işlem çeklinde gerçekleşmesi mümkün değildir. Çünkü yasaya göre, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri işlemleri elektronik imza ile gerçekleştirilmesi mümkün değildir (Yasa Madde 5).

Kısaca, hem işlevsel olarak hem de Türk Hukuku açısından, noterler ile ESHS'ler birbirine benzer ve farklı yanları olan ve birbirlerini tamamlayan işlevlere sahip iki kurum gibi düşünülmelidir.

### 3.13 ESHS'lerin Yetkilendirilmesi

Yasaya göre ESHS'ler faaliyete geçmek üzere TK'na bildirimde bulunurlar. Düzenleyici kurum olan TK, bildirim yapan ESHS üzerinde yaptığı denetimlerde yasada belirtilen şartların sağlandığına kanaat getirdikten sonra, bekleme süresinin sonunda ESHS çalışmaya başlamaktadır. Bu süreç ayrıntılı olarak aşağıda tarif edilmiştir:

1. **Bildirimin Yapılması:** Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini, gerekli bilgi ve belgeleri eksiksiz olarak TK'na ibraz etmek suretiyle bildirimde bulunur.

2. **Bildirimin İncelenmesi ve Sonuçlandırılması:** TK, yapılan bildirim üzerindeki incelemesini iki ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki ay sonra faaliyete geçer. TK, ESHS'nin gerekli şartları sağlamadığını tespit ederse ESHS'ye ek süre verir. Eksiklerini verilen süre içerisinde gidermeyen ESHS, ESHS olma vasfını kaybeder.

3. **Bildirimdeki Değişiklikler:** ESHS, faaliyete geçtikten sonra, yapmış olduğu bildirimde herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri 7 gün içinde TK'na bildirir.

# 4 ESHS'nin Nitelikleri

Bölüm 3'de bir ESHS'nin ne olduğu ve nasıl işlediği anlatılmıştı. Bu bölümde ise yasa ve yönetmelikler gereği ülkemizde kurulacak ESHS'lerin ne tür niteliklere sahip olacağından bahsedilecektir.

## 4.1 Süreklilik

Gerek kamuya hizmet veren KSM gerekse ticari ESHS'ler, verdikleri hizmetler bakımından kesintisiz hizmet vermesi gereken bir kurumdur. Gerek özel gerekse kamu sektöründeki uygulamalarda, ESHS'lerden 7 gün 24 saat kesintisiz hizmet ihtiyacı olacaktır. Bunun yanında ESHS'nin kök sertifikasını, sertifika başvuru bilgilerini koruması ve saklaması ile ilgili kriterlere uygun davranması da önemli bir gereksinimdir.

## 4.2 ESHS'nin uyacağı Kriterler, Standardlar, Parametreler

Hizmet verecek olan ESHS'lerin kullanabilecekleri kriptografik fonksiyonlar ve parametreler ile ilgili sınırlamalar açıkça tarif edilmiştir (Tebliğ Madde 5,6,7,8,9, 10). Bu nitelikler şunlardır:

- ESHS'nin işleyişi ile ilgili sağlayacağı standardlar (Bkz Tebliğ Madde 9)
- İmza oluşturma ve doğrulama verileri (yani özel ve açık anahtarlar)
- Sertifika ilkeleri ve Sertifika Uygulama Esasları (Bkz. Bölüm 3.7)
- Kullanılacak güvenli elektronik imza oluşturma ve doğrulama araçlarının uyacağı standardlar (Bkz. Bölüm 6)
- ESHS'nin uyacağı güvenlik kriterleri (Bkz. Tebliğ Madde 11)

Kriptografi çok hızlı ilerleyen bir bilim dalıdır. Bu nedenle bugün güvenli sayılan bir algoritma bir sene sonra güvensiz hale gelebilir. Bu nedenle örneğin Tebliğ'in 6. maddesinde belirtildiği üzere geçerli sayılan parametreler 31/12/2005 tarihine kadar geçerlidir. ESHS'ler belirtilen tarihten sonra TK tarafından yayınlanacak yeni parametrelere uygun olarak kendi altyapılarını güncellemek zorundadırlar.

## 4.3 ESHS'lerin Denetimi

Yasaya göre ESHS yetkisi alındıktan sonra TK, ESHS'leri bu niteliklerin devamlılığını garanti etmek amacıyla denetlemeye devam edecektir. Bu nedenle yetki belgesine sahip olan ESHS, ancak sahip olduğu nitelikleri sürdürdüğü takdirde hizmet vermeye devam edebilecektir. Kamu kurumlarına hizmet veren KSM de bu kapsama dahildir.

# 5 Türkiye'deki ESHS Yapılanması

## 5.1 Kamudaki Yapılanma

6 Eylül 2004 tarihinde yayınlanan ve 2004/21 numaralı Kamu Sertifikasyon Merkezi (KSM) oluşturulması konulu bir Başbakanlık Genelgesi yayınlanmıştır.

Genelge, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaları durumunda ortaya çıkacak sistemsel karmaşaya ve emek ve kaynak israfına engel olunmasını hedeflemektedir. Ayrıca, ulusal güvenlik gerekleri göz önünde bulundurularak KSM'de, ulusal yazılım ürünleri kullanılacağı belirtilmektedir.

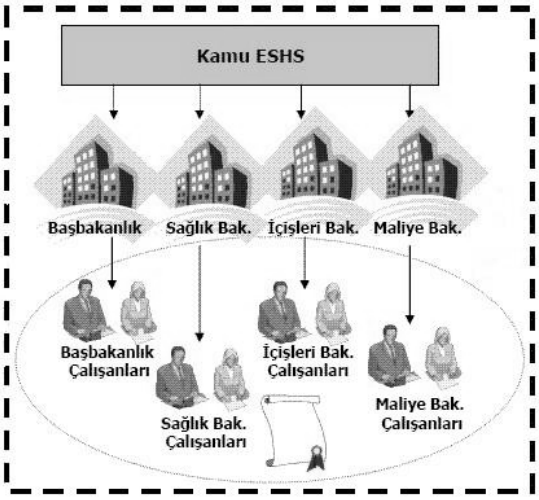
Genelge ile istisnalar dışındaki hiçbir kamu kurumu, elektronik sertifika ihtiyaçlarını karşılamak amacıyla kendi bünyelerinde yeni bir yatırım yapmayacaktır. Kamu kurumları ve çalışanları, bu ihtiyaçlarını KSM'den temin edilecek elektronik sertifikalar ile karşılayacaklardır (Şekil 13). Bu konuda daha önceden başlamış olan ve devam eden çalışmalar durdurulacak, halihazırda kullanılmakta olan sistemler ise TK'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

Bunun sonucunda tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını, kamu kurumlarının kurum içi ve kurumlar arası elektronik sertifika ihtiyaçlarının karşılanmasını ve sertifika yaşam çevriminin yönetilmesini sağlayacak KSM, TÜBİTAK UEKAE bünyesinde oluşturulmuştur (www.kamusm.gov.tr). KSM, yetki belgesi almak üzere TK'na başvuruda bulunmuştur. Haziran 2005 ayı içerisinde sertifika dağıtımına başlaması beklenmektedir.

Kamu kurumlarının, KSM'den hizmet alması için kendi altyapılarının uygunlaştırılması için gerekli çalışmaları Devlet Planlama Teşkilatı (DPT) ile eşgüdümlü olarak yürüteceklerdir.

Elektronik imza hukuki olarak ıslak imzanın yerine geçebildiğinden mahkemede delil olarak da sunulabilir. Bu bağlamda geçmişe dönük olarak elektronik imza işlemleri ile ilgili bir takım verilerin saklanması gereklidir. Kanuna ve yönetmeliklere göre bilgiler 20 yıla kadar saklanmalıdır. Bu şekilde geçmişte yapılmış işlemlerde kullanılan imza oluşturma anahtarları, oluşturulan imzalar ve imzalanan veri saklanır.

Ayrıca bir süre sonra devreye girecek olan E-Devlet Kapısı projesi, tüm kurumları bu tür bilgiler saklamaktan kurtararak merkezi bir elektronik kayıt saklama hizmeti verebilir.




**Şekil 13 Kamuda Sertifikasyon Yapılanması**

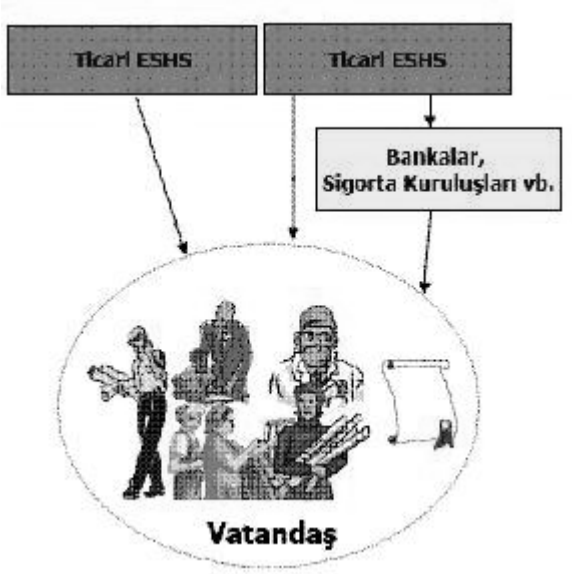
## 5.2 Özel Sektörde Yapılanma

Önümüzdeki zaman içerisinde kademeli bir şekilde, elektronik olarak verilmekte ve verilecek olan kamu hizmetlerinde vatandaşın elektronik imzası istenmeye başlanacaktır. Bu hizmetler sadece kamu kurumlarıyla sınırlı değildir. Örneğin bir özel banka da İnternet şubesinden hizmet almak isteyen müşterilerine nitelikli elektronik sertifika sahibi olma zorunluluğu getirebilir. Vatandaşların bu tür hizmetlerden yararlanabilmek için ticari ESHS'lerden birinden elektronik sertifika temin etmek zorundadır (Bkz. Şekil 14).

Yasanın ve yönetmeliğin çıkması ile ticari olarak ESHS hizmeti verecek olan kurumların TK'na başvuruları başlamıştır. TK'na ESHS hizmeti vermek üzere şu ana kadar başvuran kurumlar şunlardır:

- E-güven Elektronik Bilgi Güvenliği A.Ş.
- Türktrust Bilgi iletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Ticari ESHS olmak üzere başvuru yapmanın en son tarihi diye bir kavram söz konusu değildir. İsteyen her gerçek ya da özel hukuk tüzel kişileri, ESHS olmak üzere başvuruda bulunabilir.

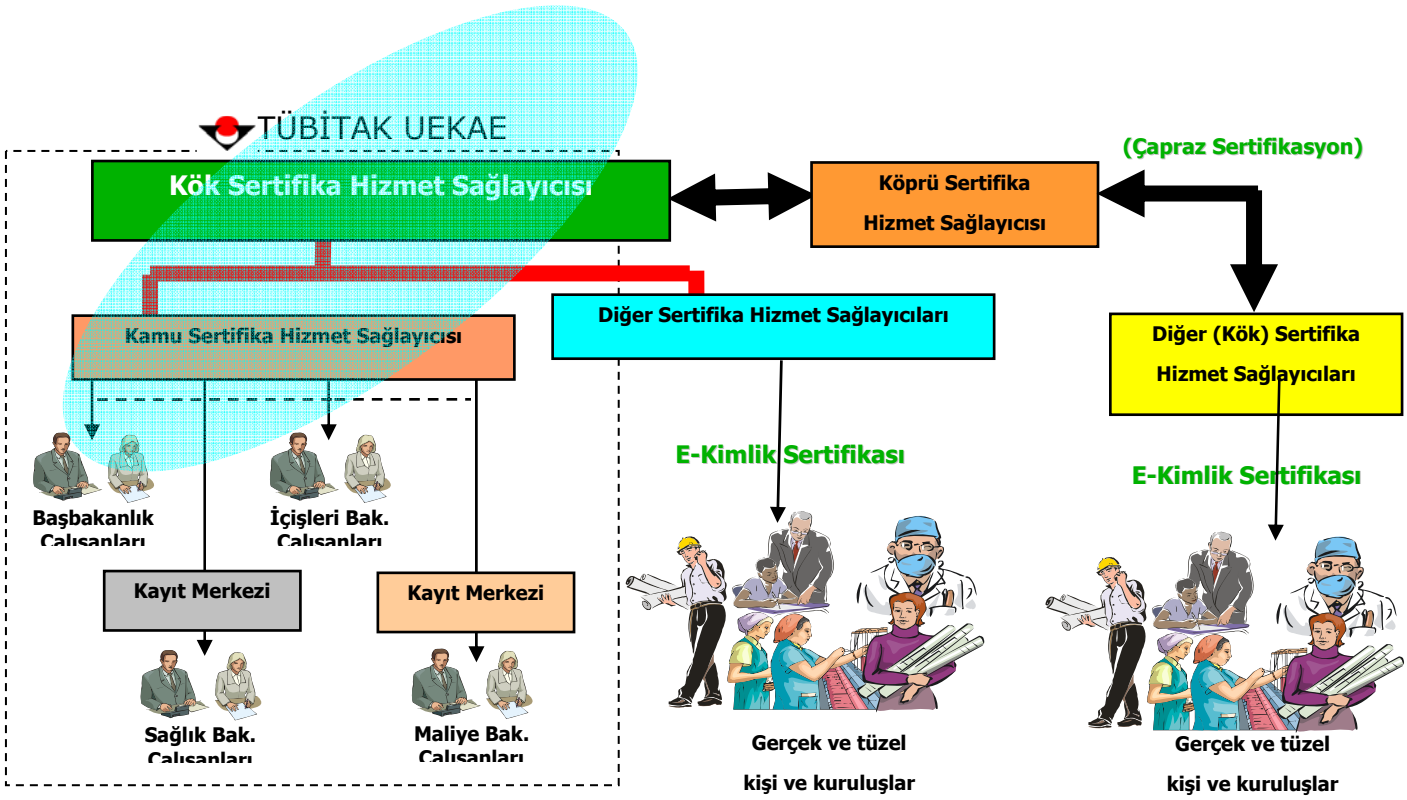



**Şekil 14 Türkiye'de Ticari ESHS Yapılanması**

TK'na ticari ESHS hizmeti vermek üzere başvuracak kurumlar yasa, tebliğ ve yönetmelikte belirtilen şartları sağlamak zorundadır.

## 5.3 Ayrıcalıklı Durumlar

KSM Kök Sertifika Hizmet Sağlayıcısı ile buna bağlı olarak Kamu Sertifika Hizmet Sağlayıcısı olarak hizmet verecektir. Yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet sistemlerini kendi bünyelerinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları, sertifikalarını, KSM'den temin edeceklerdir (Bkz. Şekil 15).




**Şekil 15 Türkiye'deki ESHS Yapısı**

## 5.4 Avrupa Birliğinde Durum

Avrupa Birliği'ne üye tüm ülkelerde elektronik imzaya yönelik olarak yayınlanmış olan 1999/93/EC direktifi yerine getirilmiştir. İrlanda hariç 14 üye ülkede en az bir nitelikli sertifika üreten ESHS vardır. Fransa ve İrlanda hariç 13 üye ülkede nitelikli sertifika üreticilere lisans veren bir kurum vardır. İrlanda ve İngiltere dışında 13 üye ülkede nitelikli sertifika üreticileri düzenleyen ve denetleyen bir kurum vardır. 9 üye ülkede ise ESHS'lere ilişkin yukarıda belirtilen lisanslama ve denetleme işlevleri aynı kurum tarafından yerine getirilmektedir.

## 5.5 ABD'de Durum

ABD Kongresi e-imza yasasını (Electronic Signatures in Global and National Commerce Act) 2000 yılında kabul etti. Bu çerçeve yasası e-imzanın uluslararası geçerliliğine değiniyor olmakla birlikte daha önce yayınlanmış olan AB Yönergesi ile tam bir uyum içerisinde olduğunu söylemek mümkün değildir.

UNCITRAL (United Nations Comission on International Trade Law) Birleşmiş Milletler bünyesinde oluşturulmuş ve uluslararası ticaret yasalarının uyumluluğunu amaçlayan bir komisyon. Çalışma alanları arasına e-ticareti de alan UNCITRAL 2001 yılında e-imza konusunda bir model yasa metni oluşturdu. Bu metin 2003 yılında Meksika ve Tayland e-imza yasaları hazırlanırken temel kaynak olarak kullanıldı.

# 6 Elektronik İmzanın Kullanılacağı Uygulamalar

## 6.1 Elektronik İmzanın Yaygınlaştırılması İçin Yapılabilecekler

Elektronik imza yasası ile birlikte kamuda ve özel sektörde elektronik imza yavaş yavaş hayatımıza girmeye başlayacaktır. Bu sürecin ekonomik bir yarar sağlayabilmesi ise teknolojik değişikliklere ayak uydurabilecek özellikle eşgüdümlü bir planın uygulanmasıyla mümkündür. Bu amaçla devlet, diğer ülkelerdeki devletlerin üstlendiği role benzer olarak, iş dünyası, son kullanıcı, AR-GE birimleri, üniversiteler gibi bu teknolojinin ülkemizde kullanılması, benimsenmesi ve üretilmesi aşamalarında işbirliği yapması gereken kurumlar arasında katalizör görevini üstlenmelidir.

Devlet elektronik imzanın yaygınlaşması için önayak olmalıdır. Bu kapsamda elektronik imzanın bir cep telefonunu kullanmak kadar kolay kullanımının sağlanması için çalışmalar yapılması düşünülebilir. Geçen dönemlerde YTL geçişi sırasında Sanayi Bakanlığı tarafından yapılan tanıtım ve reklam çalışmalarının benzerleri elektronik imzanın yaygınlaştırılması sürecinde de düşünülebilir.

Eşgüdümü sağlamak amacıyla bilişim teknolojileri kapsamındaki tüm tarafların (donanım üreticileri, altyapı/iletişim ağı kurucuları ve işleticileri, yazılım hizmetleri üreticileri, hizmet sunucuları, içerik üreticileri/sunucuları) ilgililerinin temsil edildiği bir kurumsal yapılanma en kısa zamanda oluşturmalıdır. Benzer düzenleyici kurumlar Almaya, Norveç, Danimarka, İtalya, Fransa ve İspanya gibi bir çok ülkede bakanlık olarak bulunmaktadır. Ayrı bir bakanlık çatısı altında olmasa da İngiltere, Finlandiya ve İsviçre'de düzenleyici erk enformatik alanında tek bir otoritededir. Amerika Birleşik Devletleri'nde ise düzenleyici kuruluş Kongre'ye doğrudan bağlı olarak çalışmaktadır. Bu modellerden de yararlanılarak oluşturulan düzenleyici kurum, bilişim teknolojileri alanındaki düzenlemelerde doğrudan ya da dolaylı olarak taraf olan Radyo Televizyon Üst Kurulu, Telekomünikasyon Kurumu, Türk Telekom, Türk Standartları Enstitüsü arasındaki eşgüdümü ve onların da katkıda bulunmasını sağlamalıdır.

Ülkemizde bilişim teknolojileri alanında oluşturulacak bir mastır planı, bilişim teknolojilerinin gerektireceği altyapı, sunulabilecek hizmetler ve hizmetlerin sunulmasıyla değişecek ekonomik, toplumsal/kurumsal yapılanma ve düzenlemeler başlıkları ile birlikte elektronik imzanın yaygınlaşması ve bu konuda bir kültür ve bilinç oluşması ile ilgili bilgiler de içermelidir. Bu planda gerekli insan kaynağının yetiştirilmesi, teknoloji geliştirme / uyarlama, topluma yaygınlaştırabilme, uluslararası rekabet gücü olan ürünler üretebilme gibi temel sorulara cevap üretebilecek yapabilirlik incelemelerine, diğer konular gibi elektronik imza konusu da dahil edilmelidir.

## 6.2 Altyapı

Elektronik imza teknolojisini kullanabilmenin temel gereksinimi tabii ki bilgisayar kullanabilmektir. Bilgisayar kullanabilmek için de bilgisayara ihtiyaç vardır. Bu nedenle, bilgisayar sahipliği oranının yükseltilmesi konusunda projeler üretilmelidir. Benzerleri başka ülkelerde görülen, doğrudan ve düşük faizli kredi desteği ve vergi indirimi sağlanması gibi yöntemlerle bilgisayar sahipliği oranı arttırılmaya çalışılmalıdır.

Ayrıca devlet dairelerinde veya halka açık devlet kontrolündeki merkezlerde, halka e-Devlet uygulamalarına erişmekte kullanılmak üzere ücretsiz bilgisayar ve

internet erişim hizmeti verilebilir. Bu merkezlerde bilgi eksikliği olan vatandaşa eğitimli ve güvenilir personel tarafından uygulamaların kullanımında yardım edilebilir.

Muhtarlar, halka en yakın devlet görevlisi olarak halkın E-Devlet uygulamalarını kullanmasında ön ayak olabilir. Mahalle muhtarının ofisinde sağlanacak bir E-Devlet erişim noktası sayesinde, halkın işlemlerini başka bir devlet dairesine gitmeden gerçekleştirmesi sağlanabilir.

E-Devlet hizmetlerinin vatandaşa yönelik olarak artması, vatandaşın da bu konuda istekli olmasına bağlıdır. Bununla birlikte E-Devlet uygulamalarını kullanmak istemeyen ya da kullanamayacak derecede engelli vatandaşlar için de çözümler oluşturulmalıdır. E-Devlet hizmetlerini kullanmak istemeyen kullanıcılar için normal yoldan (kağıt tabanlı) işlem yapma faaliyeti devam ettirilmelidir. Engelli vatandaşlar yine muhtar ya da devletin oluşturduğu hizmet merkezlerindeki görevliler aracılığı ile bu hizmetlerden yararlanabilirler.

## 6.3 Elektronik İmzanın Kullanılabileceği Kamu Hizmetleri

Elektronik imzanın kullanılabileceği kamu hizmetleri genel olarak şu şekilde sıralanabilir:

- **Elektronik Belgeler:** Bireylerin devletten almak zorunda olduğu ve devletin tuttuğu diğer kayıtlarda (nüfus kağıdı, pasaport, tapu ve kadastro, nüfus, adli kayıt ve sicil, askerlik, ithalat/ihracat vb.)
- **Ödemeler:** Vergi, harç v.b. ödemeleri
- **Veri Aktarımı:** Devlet içi yazışmaların, belge ve veri aktarımların yapılması.
- **Elektronik Oylama:** Elektronik oylama ya da referandum ile vatandaşın ve kamu görevlilerinin yönetime katılımı
- **Sağlık Hizmetleri:** Sağlık veri bankaları
- **Yargı Hizmetleri:** Yargı sistemindeki etkileşimlerin kağıt ortamından elektronik ortama taşınması.

Burada belirtilen hizmetlerde elektronik imzanın tek başına kullanımı mümkün değildir. Örneğin bir elektronik ödeme uygulamasında elektronik imzanın kullanılabilmesi için önce, o uygulamanın mevzuatta yer alan iş akışının tanımlanması ve bunun için gerekli donanım ve iletişim altyapısının oluşturularak, iş akışının bir yazılım uygulamasında gerçekleştirilmesi gereklidir. Elektronik imzanın kullanılabilmesi, bu yazılım uygulamasının sahip olduğu özelliklerden biri olacaktır.

E-Devlet konusunda henüz yatırım yapmamış olan kurumlarım, mevzuatın getirdiği elektronik imza ihtiyaçlarını da göz önünde bulundurarak yatırım yapmaları, ihale şartnamelerini buna uygun hazırlamaları gereklidir. Bu konuda Kamu İhale Kurumu, mükerrer yatırımları önlemek için devreye girmelidir. Ayrıca TÜBİTAK UEKAE, yatırım yapacak kurumlara, elektronik imza teknolojisi konusunda önerilerde bulunmalı ve danışmanlık hizmeti vermelidir.

## 6.4 Uygulamalar ve Hizmetler

Elektronik imzanın kullanılabilecek E-Devlet hizmetleri ve uygulamalarından ilk akla gelen birkaç tanesi burada listelenmiştir. Liste elbette çok uzayabilir. Burada amaç, vatandaşın ve devlet kurumlarının ilk anda ihtiyaç duyabileceği ve elektronik imzanın yararlarından en çok faydalanılabilecek bir liste sunmaktır:

| | |
|---|---|
| Maliye Bakanlığı | e-Beyanname |
| Sanayi ve Ticaret Bakanlığı | e-Esnaf, Ticaret Sicil Memurlukları Otomasyonu, e-Tüketici |
| Bayındırlık Bakanlığı | Yapı Denetim Uygulaması |
| Adalet Bakanlığı | Ulusal Yargı Ağı Projesi |
| SSK | e-Bildirge |
| Emekli Sandığı | e-Sağlık (Sağlık Harcamalarının Uygulama ve Denetimi) |
| Emniyet Genel Müdürlüğü | e-Pasaport, e-Ehliyet hizmetleri |
| Dış Ticaret Müsteşarlığı | Dahilde İşleme Rejimi |
| Türk Patent Enstitüsü | e-Marka, e-Patent, e-Tasarım |
| İşkur | e-iş |
| Sermaye Piyasası Kurulu | Kamuyu Aydınlatma Projesi |

**Tablo 1 Elektronik İmzanın Kullanılabileceği Hizmetler**

## 6.5 Kamu Yatırımlarının Önündeki Engeller ve Olası Çözüm Önerileri

Kağıt üzerinde işleyen bir sistemi elektronik ortama geçirmek, elektronik ortamdaki bir uygulamaya elektronik imza ile ilgili özellikleri dahil etmek ciddi yatırımlardır. Özellikle Elektronik İmza mevzuatında ayrıcalık tanınmış altı kurum (Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Dışişleri Bakanlığı, Emniyet Genel Müdürlüğü ve Milli İstihbarat Teşkilatı), kendi Açık Anahtar Altyapısı sistemlerini kuracaklarından diğer kurumlara göre yapacakları yatırım çok daha fazladır. Bu ayrıcalık tanınan kurumlar örneğin kendi ESHS'lerini, Donanım Güvenlik Modüllerini, gerekli iletişim altyapısını kuracaklar, bu altyapıyı ayakta tutacak personeli eğitip istihdam edeceklerdir. Özellikle önümüzdeki dönemden itibaren geçilecek üç yıllık bütçe uygulaması nedeniyle yatırımlarda gecikmeler yaşanması olasıdır.

Yukarıda bahsedilen problemlere çözüm olarak elektronik imza ile ilgili yatırımlar ayrıcalıklı bir kapsamda düşünülebilir. Bu konuda E-Dönüşüm İcra Kurulu'nun da kararları doğrultusunda planlanan yatırımların bir an önce yapılması sağlanabilir.

Bunun yanında ayrıcalıklı altı kurumun yapacağı yatırımın ve bu konuda

## 6.6 Kamu Kurumlarının Elektronik İmza Hizmetini Verme Konusundaki Yeterliliği

Elektronik imza yasası ile birlikte tüm kamu kurumları Başbakanlık Genelgesi'nde belirtildiği gibi ESHS olarak Kamu SM'yi kullanacaklardır. Bu kapsamda

Kamu SM sertifika yayınlama hizmetini vermenin yanı sıra, kamu kurumlarını bu konuda bilgilendirici ve bilinçlendirici bir rol de oynamalıdır. Yüz yüze bilgilendirmenin yanında, İnternet üzerinde herkesin erişebileceği bilgilerin hazırlanması düşünülebilir.

TBD de üstlendiği toplumsal rolün bir parçası olarak vatandaşı ve kamu kurumlarını bilgilendirme çalışmaları düzenleyebilir. Halihazırda TBD'nin bu yönde bir planı mevcuttur.

İhtiyaç duyulursa kamu kurumları birlikte çalışılabilirliği sağlamak amacıyla farklı kurumlardan temsilcilerin olduğu çalışma grupları oluşturabilir.

Genel olarak tüm eğitim faaliyetlerine katılan kamu kurum personeli, kurumlarına döndüklerinde bu eğitim bilgilerini mutlaka yöneticileri ve diğer çalışma arkadaşlarıyla paylaşırlarsa, bilinçlenme düzeyi çok daha hızlı yükselecektir.

Teknik yönden problemler aşılsa bile, idari olarak kamu kurumu yöneticilerinde ve çalışanlarında yıllar boyu oluşmuş ve değişime dirençli iş yapma yaklaşımları, elektronik imzanın yaygınlaşmasında ve kurumlar tarafından kullanımına geçilmesinde en önemli engel olarak görülmektedir. Bu yaklaşımların mümkün olduğunca hızlı bir şekilde değiştirilmesi sağlanmalıdır. Elektronik imza teknolojisinin devlete ve çalışma verimine getireceği yararlar, kurum çalışanlarının anlayabileceği örneklerle anlatılmalıdır. Bu şekilde değişime direncin kırılması sağlanmalıdır.

Tüm kamu kurumların erişebileceği bir çağrı merkezinin oluşturulması ve bu çağrı merkezinin ileride vatandaşa dönük olarak genişletilmesi düşünülmelidir. Bu şekilde akla gelen her türlü soru, bu çağrı merkezi aracılığı ile cevaplanabilir.

# 7 Elektronik İmza ve Uluslararası Geçerliliği

Elektronik sertifikaların, yayınlandığı ESHS kapsamı içerisinde kullanılması ile beraber diğer ulusal ve yabancı ESHS'ler ile de çalışabilmesi gerekmektedir. Faktör, bilginin gizliliği, bütünlüğü, iki tarafta da kimlik belirleme, zaman kavramının sabitlemesi, Ulusal ve Uluslararası Kanun/Mevzuat ihtilaflarının giderilmesi için elektronik kayıtların ihtilaflarda ispat gücünün ihtilafsız kabulü, uç kullanıcıya kadar güvenli altyapı gibi temel işlemler için Ulusal bazda Hukuki Altyapı, İdari, Teknik ve Uluslararası altyapının kurulması gerekir. ESHS'lerin karşılıklı çalışabilirliği sağlanırsa, Elektronik Sertifikaların Uluslararası kullanımı mümkün olacaktır. Teknik özellikler, ilkeler, iş ilişkileri ve yasal değerlendirmeler de göz önüne alınarak ESHS'ler arasında karşılıklı çalışabilirliği sağlamak üzere önerilmiş ve geliştirilmiş birçok yöntem vardır. Bu yöntemler Dünya'nın çeşitli ülkelerinde ortak çalışmalarla test edilmekte ve uygulanmaktadır. Henüz çok kesin ve net standartlar ortaya konulmamış olsa da bu metotlardan bazıları ön plana çıkmayı başarmıştır. Bu çalışmada, önerilmiş ve bazıları uygulanmakta olan yöntemler avantaj ve dezavantajları göz önüne alınarak incelenmiştir.

## 7.1 ESHS'ler Arası Karşılıklı Çalışabilirliğin Gerekliliği

ESHS'ler arasında teknik, ilke, iş ve yasal bakımdan farklılıklar bulunabilmesinden dolayı karşılıklı çalışabilirlik, üzerinde özenle durulması gereken bir konudur. Bir ESHS'nin kendi sınırları içerisinde hizmet vermesi ile birlikte, diğer ulusal ESHS'ler ve uluslararası ESHS'ler ile de karşılıklı olarak belirlenmiş güven ilişkileri içerisinde çalışabilmesi gerekir. Ülkelerarası ve farklı AAA etki alanları arasında

karşılıklı çalışabilirliği sunmak amacıyla, standartlaşma sağlamak üzere birçok çalışma devam etmektedir.

Karşılıklı çalışabilirlik, bir ESHS tarafından yayınlanan Elektronik Sertifikaların, yurt içindeki ve yurt dışındaki güven duyabileceği başka ESHS'ler ile de sorunsuz olarak iletişim ve güven ilişkileri kurabilmesi yeteneğidir. Karşılıklı çalışabilirliği sağlamak üzere önerilen seçenekler arasından seçim yapmak üzere aşağıdaki üç ana alan üzerinde belirginlik sağlanmalıdır (Lloyd, 2001):

- Karşılıklı anlaşma düzeyine bağlı olarak karşılıklı çalışabilirliği kolaylaştırmaya yardımcı olacak protokol, veri yapısı, sertifika ilkeleri, sertifika uygulama esasları, sertifika ve sertifika iptal listelerinin paylaşılması gibi teknik değerlendirmelerin göz önüne alınmasıdır.
- Karşılıklı ilkeler ve iş ilişkileri ile ilgili konuların değerlendirilmesidir. Bu alan, ESHS'ler arasındaki ilişkileri tesis etmek üzere, teknik olmayan detayları kapsar. Kuruluşlar arası ilişkilerin elektronik bilgi alışverişine dayanacak şekilde kurulması mantığıdır. Bu "elektronik ilişki", mevcut gereksinimlerden dolayı bir veya birden fazla uygulamaya bağlı olarak bilgi alışverişinde bulunmak üzere gerçekleştirilebilirken, zamanla ortaya çıkabilecek gereksinimleri de içerebilir. Kısacası, yabancı bir ESHS tarafından çıkarılan sertifikaların yerel ESHS'da ve yerel ESHS tarafından çıkarılan sertifikaların yabancı ESHS'da nasıl kullanılacağını açıklar.
- Bu alanda ise, yasal değerlendirmeler göz önüne alınır. Karşılıklı çalışabilirlik konusunda karşılaşılabilecek en önemli sorun, farklı hukuki altyapılara sahip ortamlardır. Bu kapsamda ESHS'ye ve kullanıcıya düşen sorumluluk ve yükümlülüklerin iyi anlaşılması gerekir. Buna, göz önüne alınması gereken "Yasal bildirimler ne içerecek ve bu bildirimler güvenen tarafa nasıl taşınacak?" gibi kullanıcı bilgilendirme gereksiniminin kapsadığı yükümlülükler örnek olarak verilebilir.

### 7.1.1 Hukuki Altyapı

Elektronik imza ile ilgili hukuki altyapının oluşturulması ile ilgili şu çalışmalar gerçekleştirilmiştir:

- Her türlü ikili ve kurumsal iş ve işlemlerde kayıt tutma, standart ve tekniklerinin belirlenmesi,
- Elektronik kayıtların kamu kurum ve kuruluşları tarafından belge olarak kabulü ile ilgili standart ve iç mevzuatlarının düzenlenmesi,
- Ticaret Kanunu, Sayıştay denetim usulleri, Borçlar Kanunu, Bankalar ve Vergi Usul kanunlarının elektronik belge tutma ve gönderme şartları göz önüne alınarak tekrardan düzenlenmesi,
- Elektronik ortamda oluşturulan yabancı belgelerin geçerliliği konusunda Dış Ticaret, Gümrük ve Bankalar Kanununda değişiklik, Uluslararası/Ulusal olarak yapılan Elektronik Sözleşmelerde ve sanal ticarette oluşabilecek ihtilaflar konusunda Elektronik Tahkim Yasasının çıkarılması,

- Özel ve kurumsal bilgilerin gizliliği, bütünlüğü için Ulusal Bilgi Güvenliği Yasasının çıkarılması buna bağlı olarak SPK gibi kurumların ve ürün borsalarında kontrat bazlı, spot ve opsiyon piyasalarında sanal işlem uygulama yönetmelikleri ile Uluslararası sanal ticaret için akreditasyon kurumları için yeni mevzuatların çıkarılması,
- Açık anahtar (public key) ile ilgili onay kurumlarının (Nitelikli Elektronik Sertifika sağlayan kurumların) kurulum izinleri ve denetimi kamu tarafından yapılmalı, %51 hissesi kamu elinde bulunan kurumların bu pazardan ivedi çekilmesi gerekmektedir, Uluslararası kredi ve finans kurumlarının ticarette uyguladığı kriterlerin devlet kurumlarının hizmet ve mal alımında da uygulanması için Devlet İhale Kanunu, Elektronik İmza Kanunu ile Elektronik İmza Yönetmeliği'ne kesin ve bağlayıcı maddelerin ilave edilmesi,
- Elektronik suçların evrenselliği konusunda yapılan uluslar arası mevzuat çalışmaları ve yapılacak ikili anlaşmaların hızlı bir şekilde yapılması, işlerlik açısında delil toplama ve alma/verme standartlarının belirlenmesi.
- Elektronik Kontrat ve Elektronik İmza gerektiren sanal işlemlerde Tüketicinin Korunması ile ilgili mevzuatın elektronik ticaret açısından yeniden gözden geçirilmesi, e-ticaret yapan kurumların uyacağı kuralların ivedilikle yayınlanması, Bankacılık kanunu ile ilişkilendirilmeli ve geri ödeme (charge-back) sisteminin sanal ticarette uygulamaya sokulması,
- Elektronik ödeme araçları arasında yer alan elektronik paranın (elektronik senet, elektronik çek, elektronik teminat, gibi) uygulanacağı standart, teknikler ve güvenlik kriterleri ile ulusal ve uluslar arası dolaşımı mevzuat ve anlaşmaların yapılması,
- Elektronik imza yasası,
- Elektronik imza ile ilgili yönetmelik,
- Elektronik arşivle ilgili yasal mevzuat.

### 7.1.2 İdari Altyapı

Elektronik İmza Yasası ile idari sorumlu tamamen Türk Telekomünikasyon Üst Kurumu olarak tayin edilmiştir. Yönetmelik gereği Nitelikli sertifika sağlayıcı kurumların yetkilendirme işlemlerinden tutun uygulamadaki kurallara kadar hazırlanmış bulunmaktadır. Uluslararası bilgi değişim modülü ve anlaşmalar konusunda Adalet Bakanlığı, Dış Ticaret Müsteşarlığı, Gümrük Müsteşarlığı ve Bankalar Birliği ile ortak çalışma başlatması beklenilmektedir.

Elektronik Arşiv konusu ve veri değişim standartları konusunda Başbakanlık Arşivler Genel Müdürlüğü ilgili mevzuatı çıkarmış ve bundan sonra kurumların yazışma ve değişim modüllerinde uyacağı kurallar belirlenmiştir.

Tüm kamu kurum ve kuruluşlarında ivedi olarak iş yapış tekniklerini ve uygulamaya dönük mevzuat çalışmasını ulusal ve uluslararası e-imza normlarına göre tekrar düzenleyip yayımlaması gerekmektedir.

### 7.1.3 Teknik Altyapı

ESHS'lerin yayınladığı Nitelikli Elektronik Sertifikalar'ın uluslararası çapta da geçerliliğine ihtiyaç olabilir. Bu amaçla, ulusal ve uluslararası çapta birlikte çalışabilirliği ve uyumluluğu sağlamak üzere önerilmiş ve geliştirilmiş birçok yöntem vardır. ESHS'ler arası karşılıklı çalışabilirlik, herhangi bir yöntemle ESHS'ler arasında kurulan güven ilişkisine dayanır. Çeşitli uluslararası ESHS'lar tarafından kullanılmakta ve/veya test edilmekte olan bazı yöntemler aşağıda sıralanmıştır:

- Çapraz-Sertifikasyon
- Köprü ESHS
- Çapraz-Tanıma
- Sertifika Güven Listeleri
- Akreditasyon Sertifikası
- Mutlak Hiyerarşi
- Yetkilendirilmiş Yol Onaylama ve Bulma

Karşılıklı çalışabilirlik için AAA'lar ve ESHS'ler tarafından gerçekleştirme biçimine ve düzeyine bağlı olarak bu önerilerden biri veya birkaç tanesi kullanılabilmektedir. Oluşturulmak istenen güven ilişkileri sağlanırken, belirli durumlarda ortaya çıkabilecek riskleri hafifletmek ve farklı türdeki problemleri gidermek üzere seçenekler arasından tercihler yapılabilir. Hangi güven formunun seçileceği genellikle kuruluş politikaları ile belirlenir (Entrust, 2000).

#### 7.1.3.1 Çapraz Sertifikasyon

Çapraz-sertifika, bir ESHS tarafından başka bir ESHS'ya, karşıdaki ESHS'nin genel anahtarını içerecek şekilde dijital olarak imzalayıp yayınladığı genel anahtar sertifikasıdır (Kiran, 2002). Temel olarak bir ESHS kullanıcılarının, kendi ESHS'leri ile çapraz-sertifikalandırılmış diğer ESHS kullanıcılarına güven duymasıdır (Entrust, 2000). ESHS'ler arasında Çapraz-Sertifikasyon gerçekleştirilirken çalışma ilkeleri, birbirlerine duyacakları güven düzeyi (tamamen eş-düzeyli veya belirledikleri güven düzeyleri arasında eşleştirme biçiminde olabilir) ve teknik bağlantılarla ilgili karşılıklı uzlaşmaya varmış olmaları gerekir (Entrust, 2003).

Çapraz-Sertifikasyon terimi ile kastedilen iki işlem biçimi vardır (Turnbull, 2000).

Genellikle seyrek olarak gerçekleştirilen ilk işlem biçimi, iki ESHS arasında "Çapraz-Sertifika" diye adlandırılan bir sertifikada diğer ESHS'nın genel anahtarının imzalanması ile ESHS'lar arasında güven ilişkisinin kurulmasıdır.

İstemci uygulaması tarafından sıklıkla kullanılmakta olan diğer işlem biçimi ise, AAA ağı içerisinde bir ESHS tarafından imzalanan kullanıcı sertifikasının güvenilirliğinin onaylanmasını gerektirir.

Ölçekleme nedenleriyle birden çok ESHS gerçekleştiren kuruluşlar için çapraz sertifikalandırılmış ESHS'ların kendi aralarında tam güven ilişkisi uygun olabilir. Ancak, belirli ve sınırlı iş ilişkilerine sahip farklı kuruluşlar için ESHS'ler arasında tam güven ilişkisinin kurulması genellikle uygun olmaz. Bu yüzden güven ilişkilerinin sınırlandırılması gerekmektedir.

Çapraz-Sertifikasyonda karşılaşılan diğer eleştirilerden birisi de, birden çok ESHS boyunca "Geçişli Güven" diye de adlandırılan, istenmeyen güven zincirleri ortaya çıkarabilmesidir. Örneğin ESHS1, ESHS2'ye güveniyor ve ESHS2'de ESHS3'e güveniyorsa, ESHS1'in ESHS3'e güveniyor olmasını önlemek gerekebilir. Çapraz-Sertifikalarda bu güven zincirini önlemek ve güven ilişkilerini sınırlandırmak üzere geliştirilmiş bazı eklentiler mevcuttur. Bunlar: İsim Sınırlamaları, İlke Sınırlamaları ve Yol Uzunluğu Sınırlamalarıdır.

#### 7.1.3.1.1 İsim Sınırlamaları

İsim sınırlamaları, çapraz-sertifikalandırılmış ESHS'ler arasındaki güven ilişkisinin, ayırt edici isim ile belirli nesne alt grubu veya gruplarına sınırlandırılması için kullanılmaktadır (Turnbull, 2000). Örneğin, A kuruluşunda çalışanların alt kuruluş birimleri şeklinde organize edildiğini ve muhasebe birimindeki kullanıcıların '*cn=Ahmet Ozturk, ou=Muhasebe, o=A, c=TR*' şeklinde, satış birimindekilerin de '*cn=Serap Ozdemir, ou=Satis, o=A, c=TR*' biçiminde olduğunu varsayalım. B kuruluşunda da böyle bir yapılandırma varsa, A ve B kuruluşları için sadece muhasebe birimlerindeki kullanıcılar arasında sınırlandırılmış bir güven ilişkisi oluşturulabilir (Şekil 16).

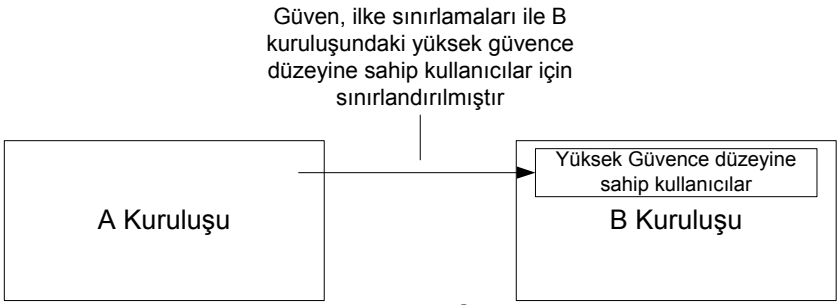

**Şekil 16 İsim Sınırlaması**

#### 7.1.3.1.2 İlke Sınırlamaları

İlke sınırlamaları, çıkarılan sertifikaların yabancı AAA etki alanındaki belirli ilke değerlerine sahip nesnelerle güven ilişkisi kuracak şekilde kullanımını sınırlamak üzere kullanılabilmektedir (Turnbull, 2000).

İlke sınırlamalarına örnek olarak, kullanıcı güvence düzeyleri verilebilir. Güvence ile kastedilen, sertifikada belirtilen kişinin gerçekten o kişi olup olmadığından emin olma derecesidir. Organizasyonlar, kullanıcısına sertifikasını çıkarmadan önce kullanıcıyı doğrulamak üzere kullanılan yöntem için farklı düzeyler kullanabilirler. Düşük güvence gerektiren bir ilke için telefonla, etkinleştirme kodu istenmesi yeterli olabilecekken, daha yüksek güvence gerektiren bir ilke içinse, kişinin kendisini uygun bir tanıtma biçimiyle tanımlamasını sağlayacak bir etkinleştirme kodu talep edilebilmektedir. Organizasyonun ihtiyaçlarına ve ilkelerine bağlı olarak, kullanıcının yetki ve erişim kontrol gereksinimleri de göz önüne alınarak, bu iki güvence düzeyinden herhangi birisi kullanılabilir.

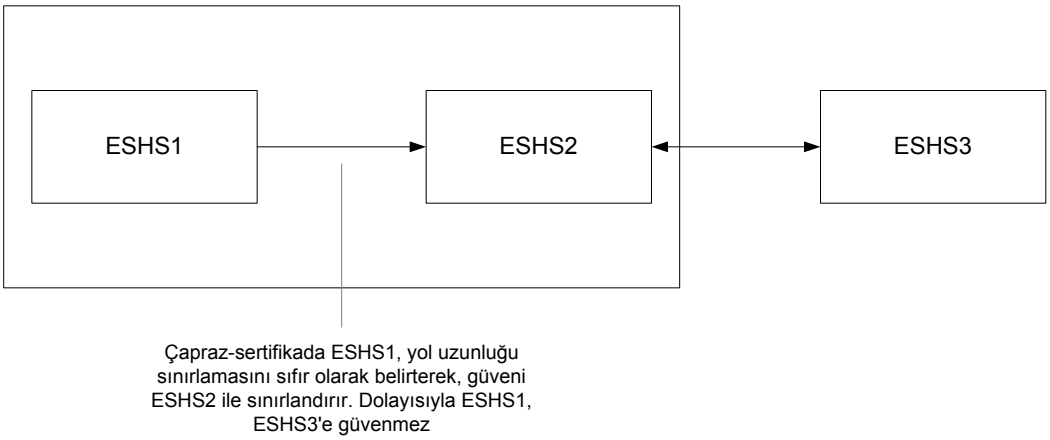
A kuruluşu, B kuruluşundaki sadece yüksek güvence düzeyine sahip kullanıcılar ile güven ilişkisi kurmak üzere çapraz-sertifikasyon sağlamak istiyorsa, ilke sınırlamaları bu amaçla gerçekleştirilebilmektedir (Şekil 17).




**Şekil 17 İlke Sınırlaması**

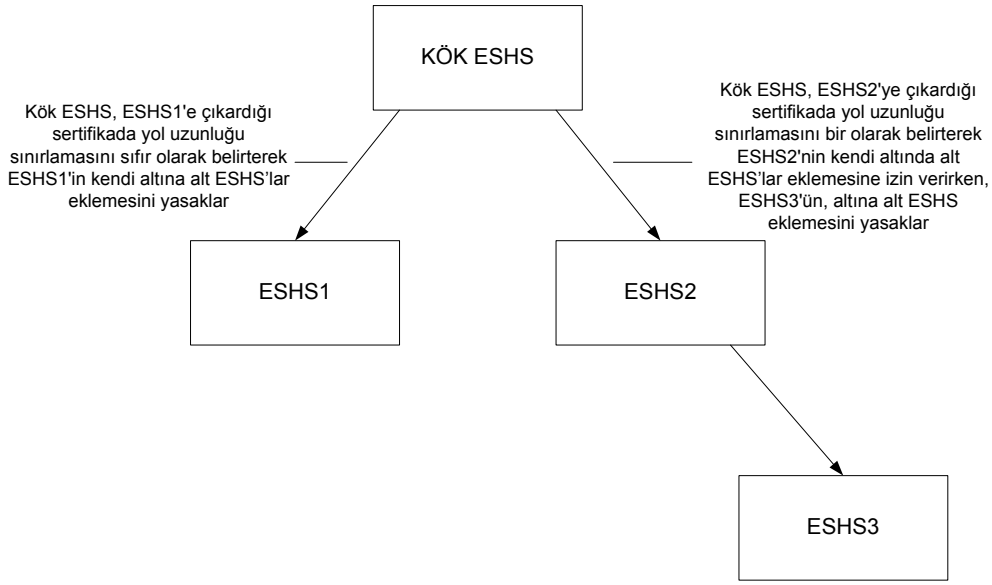
#### 7.1.3.1.3 Yol Uzunluğu Sınırlamaları

Yol uzunluğu sınırlamaları, eş-düzeyli çapraz-sertifikasyonda, geçişli güveni kontrol altında tutmak üzere kullanılabilir (Turnbull, 2000). Çapraz-Sertifikasyon ilişkisine sahip olduğunuz bir ESHS ile kurulmuş bulunan diğer Çapraz-Sertifikasyon ilişkilerine güven duyup duymayacağınız kontrol altına alınır. Şekil 18'de verilen örnekte; ESHS1, ESHS2 ile tek yönlü Çapraz-Sertifikaya sahip, ESHS2 ile ESHS3 ise birbirine çift yanlı Çapraz-Sertifikaya sahiptir.




**Şekil 18 Yol Uzunluğu Sınırlaması**

Hiyerarşik Çapraz-Sertifikasyonda yol uzunluğu sınırlamaları, alt ESHS'lerin eklenmesi durumunu kontrol altına almak üzere kullanılır. Hiyerarşinin tüm üyeleri birbirlerine güvendiği için bu kontrol, Hiyerarşik Çapraz-Sertifikasyonda oldukça önemlidir. Şekil 19'da örnek bir Hiyerarşik Çapraz-Sertifikasyon yapısında yol uzunluğu sınırlamaları gösterilmiştir**.**




**Şekil 19 Hiyerarşik Çapraz Sertifikasyon Yapısı**

### 7.1.3.2 Köprü ESHS

Köprü ESHS, "merkez-ve-konuşma" diye de adlandırılan özel bir güven modeline dayanır. Ve kendisine üye olan ESHS'ler arasında "güven aracısı" olarak işlev görerek bu ESHS'lerin birbirini tanımasını kolaylaştırır (Şekil 20). Köprü ESHS'ler, etki alanları arasındaki karşılıklı çalışabilirlik için geçerli eğilim olarak Çapraz-Sertifikasyon kullanırlar (Lloyd, 2001).

Çapraz-Sertifikasyonun ESHS'lerin birbirleri arasında iki yönlü uygulanmasının ortaya çıkardığı en önemli sorunlardan birisi ölçeklenebilme problemidir. Az sayıda ESHS arasında iki yanlı Çapraz-Sertifikasyon kurulsa bile, bu durum oldukça önemsenecek bir yük getirebilmektedir. Köprü ESHS uygulanarak, bu yük ciddi anlamda azaltılabilir. ESHS'ler birbirleri ile iki yanlı Çapraz-Sertifikasyon kurmak yerine, Köprü ESHS ile bir veya birden fazla sertifika ilkesi kullanarak Çapraz-Sertifikasyon sağlarlar. Sertifika ilkelerinin eşleşmesi durumunda, Köprü ESHS üzerinden ESHS'ler arasında bir güvenilen yol ortaya çıkar.


**Şekil 20 Köprü ESHS**

- Gerçekleştirilmiş bazı Köprü ESHS'ler aşağıda verilmiştir:
- Federal Bridge CA (ABD)
- DoD Bridge CA (ABD Savunma Birimi)
- EuroPKI (İtalya)

- European Bridge CA (Almanya)

#### 7.1.3.3 Çapraz Tanıma

Çapraz-Tanıma, tanımlı bir kullanıcı topluluğunun, başka bir ESHS tarafından çıkarılan sertifikalara, belirli uygulamalarda kullanmak üzere güven duyabilmesi durumudur (Wilson, 2001). Çapraz-Tanıma, Çapraz-Sertifikasyon ile birkaç bakımdan farklılığa sahiptir. Örneğin, ESHS'ler arasında iki yanlı tanınma söz konusu değildir. Diğer farklılıklardan bir diğeri ise, güven kararlarını ESHS'lerin değil, güvenen kısmın kendisinin yapmasının beklenmesidir (Lloyd, 2001). Çapraz-Tanıma, yüksek düzeyde güvencenin gerekli olduğu durumlarda pek kabul edilebilir çözüm olarak görünmemektedir.

#### 7.1.3.4 Sertifika Güven Listeleri

Sertifika Güven Listesi (SGL), güvenilen ESHS'leri içeren listedir. Güvenilen bir ESHS'nin genel anahtar sertifikasının bir özeti, Sertifika Güven Listesi içerisinde tanıtılır. SGL'ler, ilke tanımlayıcılarını ve eklentilerin kullanım desteğini de içerir. SGL'lerin güvenen tarafa taşınması için tanımlanmış bazı yöntemlerin dışında bant-dışı dağıtım mekanizması da kullanılabilmektedir (Lloyd, 2001).

#### 7.1.3.5 Akreditasyon Sertifikası

ESHS'ler arasında karşılıklı çalışabilirlik için çapraz-sertifikasyon ve çapraz-tanıma ile karşılaşılan bazı sorunların yaşanmaması için Geçiş Denetimi Akreditasyon Sertifikası uygulanabilir. Bu Akreditasyon Sertifikası, ulusal bazda kamu kurumları arasında merkezi ESHS tarafından akredite edilen ESHS'ler için verilebileceği gibi, uluslararası boyutta da verilebilmektedir. Temel olarak, akredite edilmiş ESHS, akredite eden ESHS tarafından imzalanan kendi genel anahtarına sahip olmaktadır (Lloyd, 2001).

Görünüşte, bir sonraki maddede bahsedilecek olan kök hiyerarşi kavramına çok benzese de, kök hiyerarşiden iki önemli farkı vardır. Birincisi, akredite edilmiş her ESHS'nin her biri kendisine has Sertifika İlkeleri ve Sertifika Uygulama Esaslarına sahip olabilmektedir. Diğeri de, ESHS'lerin, mutlak hiyerarşide genellikle izin verilmeyen kendi-imzalı genel anahtar sertifikasına sahip olabilmesine engel durumun olmamasıdır. Dolayısı ile, akredite edilmiş ESHS'ler özerk yapılardır.

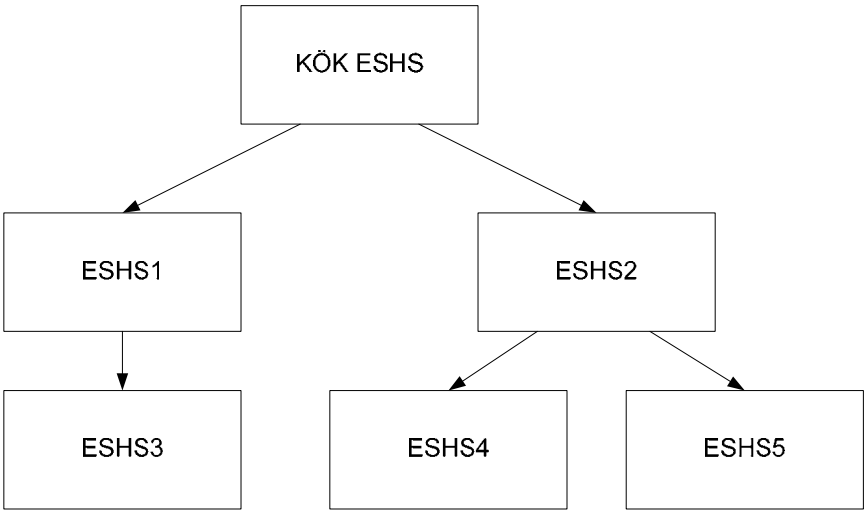
Akreditasyon Sertifikası, Çapraz-Tanımada olduğu gibi, Çapraz-Sertifika yayınlanmasını gerektirmez. Akreditasyon işlemi, akredite edecek ESHS'nin tanımladığı kriterlere göre gerçekleştirilir.

#### 7.1.3.6 Mutlak Hiyerarşi

Mutlak Hiyerarşide, tüm "güven" ortak bir kök ESHS'den çıkar. Dolayısı ile, etki alanındaki tüm güvenen taraflar için kök ESHS, güven noktasıdır. Alt ESHS'ler gerçekleştirilebiliyor olsa da, kök ESHS'ya dayandırılmış olmadığı takdirde alt

ESHS'den yayınlanan herhangi bir sertifikaya güven duyulmayacaktır. Alt ESHS'lerin kendi-imzalı sertifikasına sahip olmasına izin verilmez, sadece kök ESHS kendi-imzalı sertifikasına sahip olabilir (Lloyd,2001).

Mutlak Hiyerarşideki yapılar bir kök ESHS ve sıfır veya daha fazla alt ESHS'den oluşur. Şekil 21'de örnek bir Mutlak Hiyerarşi yapısı gösterilmiştir. Bu örnekte, kök ESHS sertifikaları iki alt ESHS'ye (ESHS1 Ve ESHS2) yayınlar ve daha sonra bu ESHS'ler de kendi alt ESHS'lerine sertifika yayınlarlar. En üstteki ESHS'nin yayınladığı sertifika, aslında iki-yanlı Çapraz-Sertifikadır.




**Şekil 21 Mutlak Hiyerarşi**

#### 7.1.3.7 Vekillendirilmiş Yol Onaylama ve Bulma

Vekillendirilmiş yol onaylama, güven kararlarını güvenilen taraftan kısmen veya tamamen kaldırmaya izin verir. Bu da, istemci tarafında, güvenilen taraf gibi davranan ve gerektiğinde güvenilen bir üçüncü-parti sunucuya sorgu gerçekleştiren bir yazılım gerektirir. Güvenilen uzak sunucuya "bu sertifikaya güvenmeli miyim?" gibi basit bir istek sorgusu gönderilebildiği gibi, daha karmaşık sorgular da gerçekleştirilebilmektedir. Bu fonksiyonu desteklemek üzere tanımlanan herhangi bir protokol, istek içerisinde farklı düzeylere izin vermelidir (Lloyd, 2001).

Bu konuyu şekillendirmek üzere İnternet Görev Gücü (IETF) tarafından çalışmalar yapılmaktadır. Çevrimiçi Sertifika Durum Protokolü'nün ikinci versiyonu (On-Line Certificate Status Protocol – OCSP) ve ilişkili yol vekillendirme ve onaylama İnternet Taslaklarında belirtilen yöntemler ile bu durum başarılabilir. Diğer bir alternatif de, Basit Sertifika Onaylama Protokolü'dür (Simple Certificate Validation Protocol – SCVP). IETF'nin bu alternatiflerden birisini benimseyeceği beklenmektedir.

Bu seçenek her ne kadar, güvenen taraf ile güvenilen taraf arasında bilginin taşınması ve işlenmesi ile ilgili karmaşıklığı azaltması açısından cazip görünse de, bu uyumu sağlamak üzere gerçekleştirilecek arka-uç altyapısı oldukça karmaşıktır.

### 7.1.4 Uluslararası Durum

Çeşitli ülkeler kendi içlerinde e-imza kullanımının yaygınlaşması ve sorunsuz işlemesi için gerekli hukuksal düzenlemeleri yeni tamamlamış durumdalar, ya da henüz üzerinde çalışıyorlar. Bu nedenle genel kabul görmüş bir uluslararası e-imza standardından söz etmek olası değil. Avrupa Birliği bünyesinde 1999 yılında Avrupa Parlamentosu tarafından yayınlanan AB Elektronik İmza Yönergesi e-imzanın uluslararası geçerliliğinin teşvik edilmesini desteklemektedir. Yönerge, bununla birlikte, özellikle e-devlet uygulamalarında ülkelerin e-imza sertifikaları için kendilerine özgü ek koşullar tanımlayabileceklerini de belirtmektedir.

# 8 Güvenlik Elektronik İmzalama Araçları

Bir elektronik imza uygulamasında, elektronik imzanın oluşturulması ve bu imzanın doğrulanmasından bahsedilebilir. Yasada Madde 6'da belirtilen elektronik imza oluşturma verisi, elektronik imzalama amacıyla kullanılan kriptografik özel anahtardır. Aynı şekilde Madde 7'de bahsedilen elektronik imza doğrulama verisi ise elektronik imzayı doğrulama amacıyla kullanılan kriptografik açık anahtardır.

5070 nolu Elektronik İmza yasasına göre, elektronik imza uygulamalarında elektronik imza üretmek için *Güvenli Elektronik İmza Oluşturma Aracı*; varolan bir elektronik imzayı doğrulamak için Güvenli *Elektronik İmza Doğrulama Aracı* kullanılır. Bu iki amaç için kullanılan cihazlara metin boyunca genel olarak "Güvenli Elektronik İmza Aracı" (GEİA) denecektir.

Yasada ve tebliğde tarif edilen şartlara uyan güvenli elektronik imza aracı olarak bugün en yaygın olarak akıllı kartlar (ing. Smartcard) ve akıllı çubuk (ing. Token) kullanılmaktadır.

## 8.1 GEİA'nın Özellikleri

Akıllı kartlar günümüzde birçok uygulama alanında karşımıza çıkmaktadır. Bir üniversitedeki tüm otomasyonu sağlamak amacıyla kullanılabileceği gibi, yemek çekleri ya da manyetik telefon kartları yerine de kullanılabilmektedir (Şekil 22). Kullandığımız cep telefonları içindeki SIM kart da bir akıllı karttır. Dünyanın en büyük üç kredi kartı üreticisi olan Europay, Mastercard ve Visa'nın ortak kararı ile dünya üzerindeki bu markaların tüm kredi kartlarının 2006 yılından itibaren birer akıllı karta dönüştürülmesi projesi de yakın zamanda gerçekleşecek en büyük akıllı kart dağıtımlarından biri olacaktır. Çubuklar da giderek yaygınlaşan ve kapasiteleri artan taşınabilir birer disk olarak günlük hayatımıza girmeye başlamıştır[1] (Şekil 23).


**Şekil 22 Akıllı Kart**

[1] 1 GB'a kadar taşınabilir çubuk bellekler mevcuttur.

**Şekil 23 Akıllı Çubuk**

Tarihsel olarak akıllı kart teknolojisinin gelişimi akıllı çubuğa göre daha eskilere dayanır. Elektronik imza amacıyla kullanılmaya başlanmadan önce, akıllı kartlar, yukarıda sayılanlara benzer birçok uygulama alanını kendilerine bulmuşlardır. Görüntü olarak aynı gibi görünse de kullanılacağı uygulamaya göre bir akıllı kartın ya da çubuğun işlevleri farklılık gösterir. Kontörlü telefon kartı olarak, elektronik imzalama aracı olarak, elektronik ödeme amaçlı olarak, kapı giriş kartı olarak veya bilgisayara kullanıcı girişi sırasında kullanılan akıllı kartlar hem fiyat olarak hem de içerdikleri fonksiyonlar açısından birbirinden farklıdır.

Aynı şekilde taşınabilir disk olarak kullanılan bir çubuk ile elektronik imza aracı olarak kullanılan çubuğun kullandığı teknolojiler birbirinden farklıdır.

## 8.2 Akıllı Kart ve Akıllı Çubuğun Birbirinden Farkı

Akıllı kartların kullanımı için bir akıllı kart okuyucuya ihtiyaç vardır. Çubuk ise artık birçok bilgisayarda bulunan USB arabirimi üzerinden bilgisayara bağlanabilir. Bunun yanında akıllı kartlar, üzerlerinden farklı uygulamalarda kullanılmak üzere birden çok elektronik devre barındırabilirler. Örneğin bilgisayara giriş için kullanılan bir akıllı kart, elektronik kapı kilitlerini açmakta da kullanılabilir (Bkz. Şekil 24).

Özellikle bankaların EMV standardına uyum nedeniyle akıllı kart verecek olmaları ve akıllı kartların işlevsel kolaylıkları nedeniyle, eğilimin daha çok akıllı kart kullanımı yönünde olacağı tahmin edilmektedir.

**Şekil 24 Akıllı Kartların Kullanımı**

## 8.3 GEİA'nın Uyması Gereken Özellikleri

Elektronik imzalama amacıyla kullanılacak akıllı kart/çubuk Güvenli Elektronik GEİA şu standartlara uygun olmalıdırlar (Tebliğ Madde 8, 11b):

- CWA 14169
- TS ISO/IEC 15408 veya ISO/IEC 15408'e göre en az EAL4+

Yasaya göre "Güvenli Elektronik İmza Doğrulama Araçları" ise şu standarda uygun olmalıdırlar:

- CWA 14171

## 8.4 GEİA nasıl kullanılır?

Bu bölümde herhangi bir elektronik imza uygulamasının GEİA ile ilgili kısımları kabaca tarif edilmiştir.

GEİA'nın bir elektronik imza uygulamasında kullanımında genel olarak beş aşamadan söz edilebilir:

- Kullanıcının uygulamayı kullanmak üzere kaydedilmesi
- Akıllı kartın kişiselleştirilmesi
- Akıllı kartın kullanıcıya ulaştırılması
- Akıllı kartın kullanımı
- Beklenmeyen durumların kotarılması

## 8.5 Kullanıcının Uygulamayı Kullanmak Üzere Kaydedilmesi

Elektronik imza uygulamasını kullanacak belli bir kullanıcı grubu vardır. Bu kullanıcı grubu örneğin, bir kamu kurumuna ait bir iç uygulamada kurumun personeli, bir kamu kurumunun vatandaşın kullanımına yönelik olarak hazırladığı bir uygulamada ise vatandaşlar olacaktır. Uygulmayı kullanacak olanlar için mutlaka bir kullanıcı kaydı oluşturularak bu kullanıcılar için en az bir elektronik imza oluşturma ve doğrulama verisi çifti (yani kullanıcının açık ve özel anahtar çifti) oluşturulmalıdır.

## 8.6 Akıllı Kart/USB Çubuk'un Kullanıcılar İçin Kişiselleştirilmesi

Kullanıcının sahip olduğu elektronik imza üretme verisi (yani kullanıcının özel anahtarı), akıllı kartının içerisinde üretilecektir. Yasaya göre bu imza üretme verisi hiçbir şekilde kopyalanamamalı, erişilememeli ve akıllı kart/usb çubuk dışına çıkmamalıdır. Akıllı karta verilen bir komutla anahtar çifti, birkaç saniye süren bir işlem ile karmaşık matematiksel fonksiyonlar sonucunda üretilir. Bu çiftin sadece açık anahtar olacak olan üyesi, akıllı kart dışına çıkarılarak, bir elektronik sertifika oluşturmakta kullanılır. Bu işlem sonucunda akıllı kartın kullanıcı için "*kriptografik olarak kişiselleştirilmesi*" sağlanmış olur.

Kullanıcıya verilecek olan kartın üzerine kullanıcıya özel bilgiler de yazılabilir. Bu işlem için kart üzerine yazma yeteneğine sahip özel yazıcılar kullanılır. İstenilen her türlü bilgi kartın her iki yüzüne de basılabilir. USB çubuklar için böyle bir

kişiselleştirme yapma şansı yoktur. Bu işleme de "*Görsel Kişiselleştirme*" denir. Bu işlemlerden sonra kart, kullanıcıya güvenli bir yolla iletilmelidir.

### 8.7 Akıllı Kartın/Çubuğun Kullanımı

Kullanıcı elektronik imzasını atmak istediği zaman akıllı kartını kullanacaktır. Elektronik imzanın atılması demek, aslında akıllı kart üzerinde bulunan bir elektronik imza fonksiyonuna, yine akıllı kartta bulunan özel anahtar ile imzalanacak dokümanın kriptografik olarak özetlenmiş halinin verilmesi ve bu fonksiyondan sonuç olarak imza bilgisinin oluşturulmasıdır. Burada en önemli nokta, imzalama işlemi kart üzerinde yapılabildiğinden, özel anahtarın kart dışına çıkması gerekmemektedir.

### 8.8 Ayrıcalıklı Durumların Kotarılması

ESHS tarafından, kullanıcının kartını kaybetmesi, kartı kullanırken ihtiyacı olan parola bilgisini unutması, çaldırması, kartın istenmeden zarar görmesi gibi durumlar için yeteri kadar ayrıntılandırılmış prosedürler oluşturulmalı ve uygulanmalıdır. Bu konuda ayrıntılı bilgiler, her ESHS'nin yayınlamakla yükümlü olduğu Sertifikasyon İlkeleri ve Sertifika Uygulama Esasları belgelerinde bulunabilir. Bu konularda ESHS tarafından açık bir nokta ve tanımlanmamış bir durum bırakılmamalıdır. Çünkü bir GEİA'nın kaybolması durumunda, bir kredi kartının kaybolmasından daha vahim sonuçlar oluşabilir.

### 8.9 Elektronik İmza Destekli Kamu Uygulamalarındaki Artışın GEİA Kullanımı Üzerinde Yaratacağı Etki

Yasaya göre, elektronik sertifikalar şahıslar için üretilebilir. Elektronik imza uygulamaları yaygınlaşmaya başladıkça, bir kişinin kullanabildiği uygulamaların sayısı zaman içinde artacaktır. Bu durumda tek bir elektronik sertifika ile birden çok uygulamaya bağlanma gerekliliği ortaya çıkacaktır. Her uygulama geliştiren kurum, kendi uygulamasını kullanacak kullanıcılar için yeni baştan elektronik sertifika üretme sürecini başlatmayacak ve kullanıcının halihazırda sahip olduğu bir elektronik sertifika varsa, bunu kullanılması sağlanacaktır. Elektronik sertifikalar, Yönetmelik'in 11. maddesinde belirtildiği gibi, kurum içi uygulamalar dışında, açık ağlar üzerinden herkes tarafından erişebilecek şekilde konumlandırılacaktır. Böylece elektronik imza doğrulama işlemi için belli bir kişinin elektronik sertifikasına her kurum ve her kişi erişebilecektir. Böylece elektronik imza, uygulamadan bağımsız olarak ancak kişiye bağımlı halde kullanılmış olacaktır.

### 8.10 GEİA'nın Teknolojisinin Eskimesi Durumu

Kriptografi çok hızlı ilerleyen bir bilimdir. Bu nedenle bugün güvenli sayılan bir algoritma veya anahtar boyu, birkaç sene sonra güvensiz görülebilir. Ayrıca Tebliğ'den de görülebileceği üzere kullanılmasına izin verilen algoritmalar ve anahtar boyları belli bir süre geçerlidir.

Elektronik imza atmalarını sağlamak üzere kullanıcılara dağıtılan GEİA'ların üzerinde kriptografik işlemleri gerçekleştirecek fonksiyonlar mevcuttur. Örneğin Tebliğ'de izin verilen algoritmalardan bir tanesinin TK tarafından 2 sene sonra değiştirildiğini varsayarsak, bu değişikliği gerçekleştirmek için tüm GEİA'ların içindeki fonksiyonları değiştirmek gereklidir. Teknolojik olarak bir GEİA'nın gerçekleştirdiği

işlemleri değiştirmek için o GEİA'yı geri alarak, istenen işlemleri gerçekleştirmeye muktedir yeni bir GEİA vermeye ihtiyaç vardır. Bu da vatandaşa ve kamu kurumlarına dağıtılan tüm akıllı kart ya da akıllı çubukların geri toplanması ve yenilerinin dağıtılması anlamına gelir. Bu eninde sonunda karşılaşılacak bir konudur. Nasıl bir kredi kartının belli bir geçerlilik süresi varsa, aynı şekilde bir GEİA'nın da geçerlilik süresi olacaktır. Bu problemi en az zarar ve iş gücü kaybı ile aşmak için, sağlam ve kusursuz dağıtım kanallarının oluşturulması beklenmektedir.

## 8.11 Ulusallık ve Dış Kaynak Bağımlılığı

Kriptografi, yüzyıllar boyu ulusların geleceklerini belirleyen önemli teknolojilerden biri olmuştur. Haberleşmenin gizliliğinin önemini kavrayan uluslar, savaş ve barış zamanlarında düşmana karşı kriptografik üstünlüklerini bir koz olarak kullanmışlardır. Aynı şekilde istihbarat açısından düşmanın algoritmasını kırmak, haberleşmesini ve bu haberleşmede geçen bilgileri ele geçirmek, başvurulan yöntemlerdir.

Henüz daha kısa sayılabilecek bir süredir elektronik imza ile tanışmış olan ülkemizde, bu konuda ulusal kaynakları kullanmamız bizi dışa bağımlılıktan kurtaracaktır. Bu konuda üniversitelerimizde ve özel sektörde çok deneyimli ve bilgili insanlar mevcuttur ve bu insanların deneyimlerinden faydalanılmalıdır. Bu teknolojilerin tamamı Türkiye'de üretilmektedir ya da talep olduğunda üretimin yapılabileceği bilgi ve hammadde mevcuttur. Daha önce bahsedildiği gibi akıllı kart ya da akıllı çubukların satın alınması, ESHS yazılımları, özel anahtar saklama teknolojileri ciddi maliyetler gerektiren yatırımlardır. Bu yatırımlarda harcanacak paranın ülke içinde kalmasını sağlamak hem ülke ekonomisine katkı sağlayacak hem de dış ülkelere bağımlılığı ortadan kaldıracaktır.

# EK-A ELEKTRONİK İMZA KANUNU

**23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete**

**Kanun No. 5070 Kabul Tarihi : 15.1.2004**

## BİRİNCİ KISIM

## Amaç, Kapsam ve Tanımlar

### Amaç

**MADDE 1.-** Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

### Kapsam

**MADDE 2.-** Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

### Tanımlar

**MADDE 3.-** Bu Kanunda geçen;

a) Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

b) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

c) İmza sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi,

d) İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri,

e) İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,

f) İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri,

g) İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını,

h) Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı,

ı) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,

j) Kurum: Telekomünikasyon Kurumunu, ifade eder.

## İKİNCİ KISIM

## Güvenli Elektronik İmza ve

## Sertifika Hizmetleri

## BİRİNCİ BÖLÜM

## Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

**Güvenli elektronik imza**

**MADDE 4.-** Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

**Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı**

**MADDE 5.-** Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

**Güvenli elektronik imza oluşturma araçları**

**MADDE 6.-** Güvenli elektronik imza oluşturma araçları;

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

Sağlayan imza oluşturma araçlarıdır.

**Güvenli elektronik imza doğrulama araçları**

**MADDE 7.-** Güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

İmza doğrulama araçlarıdır.

## İKİNCİ BÖLÜM

## Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar

**Elektronik sertifika hizmet sağlayıcısı**

**MADDE 8.-** Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak,

İle ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Kurum, yukarıdaki şartlardan birinin eksikliğini veya yerine getirilmediğini tespit ederse, bu eksikliklerin giderilmesi için, elektronik sertifika hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verir, bu süre içinde elektronik sertifika hizmet sağlayıcısının faaliyetlerini durdurur. Sürenin sonunda eksikliklerin giderilmemesi halinde elektronik sertifika hizmet sağlayıcısının faaliyetine son verir. Kurumun bu kararlarına karşı 19 uncu maddenin ikinci fıkrası hükümleri gereğince itiraz edilebilir.

Elektronik sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında bu maddede gösterilen şartları kaybetmeleri hâlinde de yukarıdaki fıkra hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcıları, Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır.

**Nitelikli elektronik sertifika**

**MADDE 9.-** Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

Bulunması zorunludur.

**Elektronik sertifika hizmet sağlayıcısının yükümlülükleri**

**MADDE 10.-** Elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle,

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle,

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla,

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik

imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

g) Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmekle,

Yükümlüdür.

Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

**Nitelikli elektronik sertifikaların iptal edilmesi**

**MADDE 11.-** Elektronik sertifika hizmet sağlayıcısı;

a) Nitelikli elektronik sertifika sahibinin talebi,

b) Sağladığı nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,

c) Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,

Durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur.

Elektronik sertifika hizmet sağlayıcısı, faaliyetine son vermesi ve vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısı tarafından kullanımının sağlanamaması durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısının faaliyetine Kurum tarafından son verilmesi halinde Kurum, faaliyetine son verilen elektronik sertifika hizmet sağlayıcısının vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısına devredilmesine karar verir ve durumu ilgililere duyurur.

Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez.

**Bilgilerin korunması**

**MADDE 12.-** Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

**Hukukî sorumluluk**

**MADDE 13.-** Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz.

Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenir.

Bu maddede öngörülen sertifika malî sorumluluk sigortası Türkiye'de ilgili branşta çalışmaya yetkili olan sigorta şirketleri tarafından yapılır. Bu sigorta şirketleri sertifika malî sorumluluk sigortasını yapmakla yükümlüdürler. Bu yükümlülüğe uymayan sigorta şirketlerine Hazine Müsteşarlığınca sekizmilyar lira idarî para cezası verilir. Bu para cezasının tahsilinde ve cezaya itiraz usulünde 18 inci madde hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür.

**Yabancı elektronik sertifikalar**

**MADDE 14.-** Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir.

Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılır. Bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki elektronik sertifika hizmet sağlayıcısı da sorumludur.

## ÜÇÜNCÜ KISIM

## Denetim ve Ceza Hükümleri

### Denetim

**MADDE 15.-** Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir.

Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

### İmza oluşturma verilerinin izinsiz kullanımı

**MADDE 16.-** Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve beşyüz milyon liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

### Elektronik sertifikalarda sahtekârlık

**MADDE 17.-** Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullananlar, fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve birmilyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

### İdarî para cezaları

**MADDE 18.-** Bu Kanunun;

a) 10 uncu maddesindeki yükümlülüklerinden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onmilyar lira,

b) 11 inci maddesindeki yükümlülüklerden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

c) 12 nci maddesi hükümlerine aykırı hareket edenler hakkında onmilyar lira,

d) 13 üncü maddesinin beş ve yedinci fıkralarındaki yükümlülükleri yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

e) 15 inci maddesi hükmüne aykırı hareket eden elektronik sertifika hizmet sağlayıcısına yirmimilyar lira,

İdarî para cezası Telekomünikasyon Kurulu tarafından verilir. Verilen para cezalarına dair kararlar ilgililere 7201 sayılı Tebligat Kanunu hükümlerine göre tebliğ edilir. Bu cezalara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, verilen cezanın yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir. Bu Kanuna göre verilen idarî para cezaları, Kurumun bildirimi üzerine 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre Maliye Bakanlığınca tahsil olunur.

**İdarî nitelikteki suçların tekrarı ve kapatma**

**MADDE 19.-** 18 inci maddedeki suçları işleyenlerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri hâlinde para cezaları iki kat olarak uygulanır, üçüncü kez işlemeleri hâlinde ise Kurum tarafından elektronik sertifika hizmet sağlayıcıları hakkında kapatma cezası verilir.

Kapatma cezası verilmesine ilişkin karar 7201 sayılı Tebligat Kanununa göre ilgililere tebliğ edilir. Bu karara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, yetkili makam tarafından verilen kapatma kararının yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir.

## DÖRDÜNCÜ KISIM

## Çeşitli Hükümler

**Yönetmelik**

**MADDE 20.-** Bu Kanunun 6, 7, 8, 10, 11 ve 14 üncü maddelerinin uygulanmasına ilişkin usul ve esaslar, Kanunun yürürlük tarihinden itibaren altı ay içinde ilgili kurum ve kuruluşların görüşleri alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir.

**Kamu kurum ve kuruluşları hakkında uygulanmayacak hükümler**

**MADDE 21.-** Bu Kanunun 8 inci maddesinin dört ve beşinci fıkraları ile 15 ve 19 uncu maddesi hükümleri, elektronik sertifika hizmet sağlama faaliyeti yerine getiren kamu kurum ve kuruluşları hakkında uygulanmaz.

**MADDE 22.-** 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir.

Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir.

**MADDE 23.-** 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmiştir.

MADDE 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır.

**MADDE 24.-** 5.4.1983 tarihli ve 2813 sayılı Telsiz Kanununun 7 nci maddesinin birinci fıkrasına aşağıdaki (m) bendi eklenmiş ve mevcut (m) bendi (n) bendi olarak teselsül ettirilmiştir.

m) Elektronik İmza Kanunu ile verilen görevleri yerine getirmek,

**Yürürlük**

**MADDE 25.-** Bu Kanun yayımı tarihinden altı ay sonra yürürlüğe girer.

**Yürütme**

**MADDE 26.-** Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

# EK-B Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

## BİRİNCİ BÖLÜM

## Genel Hükümler

**Amaç**

**Madde 1 –** Bu Yönetmeliğin amacı; elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenlemektir.

**Kapsam**

**Madde 2 –** Bu Yönetmelik; bildirim ve sertifikasyon süreçlerine, güvenli elektronik imza oluşturma ve doğrulama verileri ile araçlarına, elektronik sertifika hizmet sağlayıcısı, Kurum, nitelikli elektronik sertifika sahibi ve üçüncü kişilerin yükümlülüklerine, denetime, faaliyetin sona erme hallerine, zaman damgasına, yabancı elektronik sertifikalara, güvenliğe, teknik ve mali hususlara ilişkin usul ve esasları kapsar.

**Dayanak**

**Madde 3 –** Bu Yönetmelik 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununa dayanılarak hazırlanmıştır.

**Tanımlar**

**Madde 4 –** Bu Yönetmelikte geçen;

**Kanun:** 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununu,

**Kurul:** Telekomünikasyon Kurulunu,

**Kurum:**Telekomünikasyon Kurumunu,

**ESHS:** Elektronik Sertifika Hizmet Sağlayıcısını,

**Arşiv:** Bu Yönetmeliğin 14 üncü maddesinin ikinci fıkrasında belirtilen ve ESHS'nin saklamakla yükümlü olduğu bilgi, belge ve elektronik verileri,

**Bildirim Şartları:** Kanunun 8 inci maddesinin ikinci fıkrasında belirtilen şartları,

**Denetim:** ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan çalışmalar bütününü,

**Dizin:** Geçerli sertifikaları içinde bulunduran elektronik depoyu,

**Erişim Verisi:** Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verileri,

**İnceleme:** Kuruma yapılan bildirimin gerekli şartları sağlayıp sağlamadığını tespit etmek amacıyla yapılan çalışmalar bütününü,

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

**Kurumsal Başvuru:** Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusunu,

**Nitelikli Elektronik Sertifika:** Kanunun 9 uncu maddesinde sayılan nitelikleri

haiz elektronik sertifikayı,

**Özetleme Algoritması:** İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritmayı,

**Sertifika Özet Değeri:** Sertifikanın, özetleme algoritması ile elde edilen çıktısını,

**Sertifika İlkeleri:** ESHS'nin işleyişi ile ilgili genel kuralları içeren belgeyi,

**Sertifika Uygulama Esasları:** Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi,

**Sertifika Mali Sorumluluk Sigortası:** ESHS'nin, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortayı,

**Zaman Damgası İlkeleri:** Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgeyi,

**Zaman Damgası Uygulama Esasları:** Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi,

ifade eder.

Bu Yönetmelikte yer almayan tanımlar için Kanunda yer alan tanımlar geçerlidir.

**İlkeler**

**Madde 5 –** Bu Yönetmeliğin uygulanmasında aşağıdaki temel ilkeler göz önüne alınır;

a) Objektif nedenler aksini gerektirmedikçe, niceliksel ve niteliksel devamlılık, güvenilirlik, ayrımcı olmama, düzenlilik, verimlilik, açıklık, şeffaflık ve kaynakların etkin kullanılması,
b) Tüketici haklarının korunması,
c) Hizmet kalitesinin sağlanması,
d) Etkin ve sürdürülebilir rekabet ortamının sağlanması ve devamına yönelik uygulamaların teşvik edilmesi,
e) Uluslararası standartların dikkate alınması,
f) Elektronik imza kullanımının yaygınlaşması için yeni yatırımların ve uygulamaların özendirilmesi,
g) Elektronik sertifika sahibinin, talep ettiği hizmet ya da ürünler dışında herhangi bir hizmeti ya da ürünü satın almak zorunda bırakılmaması,
h) Bir hizmetin ya da ürünün diğer bir hizmetin ya da ürünün ücreti yoluyla desteklenmesinden veya karşılanmasından kaçınılması.

## İKİNCİ BÖLÜM

## Bildirim Süreci

**Bildirimin Yapılması**

**Madde 6 –** Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini içeren dilekçeyi ve Ek-1'de yer alan bilgi ve belgeleri eksiksiz olarak Kuruma ibraz etmek suretiyle bildirimde bulunur. ESHS yapmış olduğu bildirimde, bildirim şartlarını sağladığını ayrıntılı bir biçimde gösterir.

**Bildirimin İncelenmesi ve Sonuçları**

**Madde 7 –** Kurum, yapılan bildirimi derhal incelemeye alır ve incelemeyi iki (2) ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki (2) ay sonra faaliyete geçer.

Kurum, inceleme sonucunda bildirim şartlarından bir veya birkaçının eksikliğini veya yerine getirilmediğini tespit ederse, bu eksikliklerin giderilmesi için ESHS'ye bir (1) ayı geçmemek üzere bir süre verir. ESHS bu sürenin sonuna kadar faaliyette bulunamaz. ESHS, Kurum tarafından verilen süre içinde bildirim şartlarındaki eksiklikleri giderdiğini ispatlayan bilgi ve belgeleri Kuruma sunar. Bu şartları sağladığı Kurum tarafından tespit edilen ESHS, bildirim yaptığı tarihten itibaren iki (2) aylık sürenin tamamlanmış olması halinde faaliyete geçer. Kurum, vermiş olduğu sürenin sonuna kadar bildirim şartlarındaki eksiklikleri gidermeyen ESHS'nin ESHS olma vasfını kaybettiğine karar verir.

**Bildirimdeki Değişiklikler**

**Madde 8 –** ESHS, faaliyete geçtikten sonra, yapmış olduğu bildirimde herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri yedi (7) gün içinde Kuruma bildirir.

## ÜÇÜNCÜ BÖLÜM

## Sertifikasyon Süreci

**Nitelikli Elektronik Sertifika Başvurusu**

**Madde 9 –** ESHS, nitelikli elektronik sertifika vereceği kişilerin kimliğini; nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere göre tespit eder. Nitelikli elektronik sertifika verilecek kişi kimlik tespiti esnasında bizzat hazır bulunur.

ESHS, nitelikli elektronik sertifika verilecek kişinin kimliğinin birinci fıkra hükümlerine göre önceden tespit edilmiş olduğu hallerde veya kurumsal başvurularda kimlik tespiti için bizzat hazır bulunma şartını aramayabilir. Kurumsal başvuru sahibi, adına başvuruda bulunduğu kişilerin nitelikli elektronik sertifika taleplerini yazılı olarak belgelendirir. Nitelikli elektronik sertifika başvurusu sırasında sertifika verilecek kişiye ait kimliğin doğru ve güvenilir biçimde tespit edilmesinden ESHS sorumludur.

ESHS, nitelikli elektronik sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisinin, mesleki veya diğer kişisel bilgilerinin sertifikada yer alması durumunda, bu bilgileri resmi belgelere dayanarak eksiksiz, doğru ve güvenilir biçimde tespit eder; sertifika verilecek kişiden, sertifika vermek için gerekli olan bilgiler hariç bilgi talep edemez. ESHS, bu bilgileri nitelikli elektronik sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

**Nitelikli Elektronik Sertifikanın Oluşturulması**

**Madde 10 –** ESHS, nitelikli elektronik sertifika başvurusundan sonra sertifikayı oluşturur ve sertifika sahibine teslim eder. Nitelikli elektronik sertifikanın geçerlilik süresi sözleşmeyle belirlenir.

**Nitelikli Elektronik Sertifikanın Yayımlanması**

**Madde 11** – ESHS, sertifika sahibinin onayını almak kaydıyla nitelikli elektronik sertifikayı kamuya açık bir dizinde yayımlar. ESHS, dizin hizmetinin kesintisiz olarak verilmesini sağlar.

**Nitelikli Elektronik Sertifikanın Yenilenmesi**

**Madde 12 –** Nitelikli elektronik sertifika, geçerlilik süresinin sona ermesinden önce sertifika sahibinin veya sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda ESHS tarafından yenilenebilir. ESHS nitelikli elektronik sertifikayı, sertifika sahibine ait bilgilerin geçerliliğini doğrulayarak yeniler.

**Nitelikli Elektronik Sertifikanın İptal Edilmesi**

**Madde 13 –** Nitelikli elektronik sertifikanın iptaline ilişkin talepler; ESHS, sertifika sahibi ve sözleşme ile belirlenen kişiler tarafından yapılabilir. ESHS; bu duruma ilişkin

taleplerin yapılabilmesini, asgari olarak telefonla ve kesintisiz sağlar. ESHS nitelikli elektronik sertifika sahibini söz konusu durum hakkında bilgilendirir. Kurumsal başvurularda başvuru sahibi de bilgilendirilir.

İptal talebinin alınmasından sonra nitelikli elektronik sertifika derhal iptal edilir. İptal edilen nitelikli elektronik sertifika, geçerlilik süresi sonuna kadar iptal durum kayıtlarında yer alır. ESHS, nitelikli elektronik sertifikalara ilişkin iptal durum kaydını herhangi bir kimlik doğrulamasına gerek olmaksızın ücretsiz ve kesintisiz olarak kamu erişimine açık tutar. Kayıtların bir sonraki güncelleme zamanı söz konusu kayıtlarda açıkça gösterilir. ESHS, nitelikli elektronik sertifikayı geçmişe yönelik olarak iptal edemez.

ESHS'nin imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması ya da sertifika ilkelerinin değişmesi gibi sertifika sahibinin kusurunun bulunmadığı durumların sonucunda nitelikli elektronik sertifikaların ESHS tarafından iptal edilmesi ve yenilenmesi halinde, yenileme işlemleri için hiçbir ücret talep edilemez.

## DÖRDÜNCÜ BÖLÜM

## Yükümlülükler

### ESHS'nin Yükümlülükleri

**Madde 14 –** ESHS; nitelikli elektronik sertifika verilecek kişiyi nitelikli elektronik sertifika vermeden önce asgari olarak;

a) Kanunda öngörülen sınırlamalar saklı kalmak üzere, güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğuna,
b) İmza oluşturma verisini ve aracını başkasına kullandırmamasına,
c) Nitelikli elektronik sertifikanın kullanımı ile ilgili usul ve sınırlamaların kapsamına,
d) Nitelikli elektronik sertifikanın iptal durumuna,
e) Nitelikli elektronik sertifika sahibi ile arasında çıkacak uyuşmazlıklarda başvurulabilecek alternatif uyuşmazlık çözüm yollarına,
f) Sözleşmenin hüküm ve şartlarında meydana gelecek değişikliklere,
ilişkin yazılı olarak bilgilendirir.

ESHS;

a) Geçerlilik süresi sona eren nitelikli elektronik sertifikaları,
b) Nitelikli elektronik sertifika başvurusunda talep edilen bilgi, belge ve elektronik verileri,
c) Sertifika ilkelerini ve sertifika uygulama esaslarını,
d) Zaman damgası ilkelerini ve zaman damgası uygulama esaslarını,
e) Geçerlilik süresinin sona ermesinden itibaren kendi sertifikasını,
f) Nitelikli elektronik sertifika yönetimine ilişkin tüm işlemlere, bu işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kaydı,
en az yirmi (20) yıl süreyle saklar.

ESHS;

a) Sertifika uygulama esaslarının sertifika sahibini veya üçüncü kişileri ilgilendiren bölümlerini ve sertifika ilkelerini internet sayfasında yayımlamakla,
b) Nitelikli elektronik sertifika, zaman damgası ve elektronik imza ile ilgili hizmetlere ait ücretleri, bunları uygulamaya koyduktan sonra en geç onbeş (15) gün içinde Kuruma bildirmekle,
c) Sertifika mali sorumluluk sigortası yaptırmakla,
d) Nitelikli elektronik sertifika sahibine imza oluşturma aracı vermesi durumunda, bu aracın güvenli imza oluşturma aracı olmasını sağlamakla,
yükümlüdür.

**Nitelikli Elektronik Sertifika Sahibinin Yükümlülükleri**

**Madde 15 –** Nitelikli elektronik sertifika sahibi;

a) Nitelikli elektronik sertifika almak için gerekli tüm bilgi ve belgeleri eksiksiz ve doğru olarak sağlamakla,
b) ESHS'ye vermiş olduğu bilgilerde değişiklik meydana gelmesi halinde ESHS'yi derhal bilgilendirmekle,
c) İmza oluşturma verisini kendisi üretmesi durumunda Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenen algoritmaları ve parametreleri kullanmakla,
d) İmza oluşturma ve doğrulama verilerini sadece elektronik imza oluşturma ve doğrulama amaçlı olarak ve nitelikli elektronik sertifikanın içerdiği kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanmakla,
e) İmza oluşturma verisini başkalarına kullandırmamakla ve bu konuda gerekli tedbirleri almakla,
f) İmza oluşturma verisinin gizliliğinden veya güvenliğinden şüphe etmesi durumunda ESHS'yi derhal bilgilendirmekle,
g) Güvenli elektronik imza oluşturma aracını kullanmakla,
h) İmza oluşturma ve doğrulama verilerinin ESHS'ye ait olmayan yerlerde ve araçlarla üretilmesi durumunda gerekli güvenliği sağlamakla,
i) İmza oluşturma aracının veya erişim verisinin kaybolması, çalınması, güvenilirliğinden şüphe edilmesi durumunda ESHS'yi derhal bilgilendirmekle,
yükümlüdür.

**Üçüncü Kişilerin Yükümlülükleri**

**Madde 16 –** Üçüncü kişiler;

a) Sertifikanın "nitelikli elektronik sertifika" olup olmadığını kontrol etmekle,
b) Nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla,
c) Nitelikli elektronik sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmekle,
yükümlüdür.

**Kurumun Yükümlülükleri**

**Madde 17 –** Kurum, ESHS'lerin bildirim sürecine ve faaliyet durumuna ilişkin bilgileri internet sayfasında yayımlar.

Kurum, elektronik imzaya ilişkin yaptığı çalışmalarla ve sektörün durumuyla ilgili yıllık durum raporu hazırlar ve internet sayfasında yayımlar.

## BEŞİNCİ BÖLÜM

## Teknik Hususlar ve Güvenlik

**İmza Oluşturma ve Doğrulama Verileri**

**Madde 18 –** ESHS, kendi imza oluşturma ve doğrulama verileri ile sertifikasını Türkiye Cumhuriyeti sınırları içerisinde oluşturur ve imza oluşturma verisini hiçbir şekilde bu sınırların dışına çıkaramaz.

ESHS'ye ait imza oluşturma ve doğrulama verilerinin geçerlilik süresi on (10) yılı aşamaz.

ESHS, faaliyete geçmesini müteakip yedi (7) gün içinde; sertifikasının sertifika özet değerini ve özetleme algoritmasını kendi internet sayfasında yayımlar, ulusal yayın yapan en yüksek tirajlı üç (3) gazetede ilan vermek suretiyle kamuoyuna duyurur ve gazete ilanlarının bir örneğini Kuruma iletir.

**Güvenlik Kriterleri**

**Madde 19 –** ESHS özel hukuk tüzel kişisi ise, kurucu ortakları, tüzel kişiliği temsile yetkili yöneticileri ve istihdam ettiği veya ettirdiği personeli; gerçek kişi ise kendisi, temsile yetkili yöneticileri ve istihdam ettirdiği personeli taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya altı (6) aydan fazla hapis yahut basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş olmalıdır.

ESHS; bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam eder veya ettirir. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış olmalıdır. ESHS organizasyon şemasında istihdam ettiği veya ettirdiği tüm personelinin görev tanımını ve dağılımını belirler.

ESHS; güvenli sistem ve cihazlar kullanır, bu sistem ve cihazlar ile bunların bulunduğu bina veya alanın korunmasını sağlar.

## ALTINCI BÖLÜM

## Mali Hususlar

**Nitelikli Elektronik Sertifika, Zaman Damgası ve İlgili Hizmetlerin Ücretleri**

**Madde 20 –** Nitelikli elektronik sertifika, zaman damgası ve ilgili hizmetlere ait ESHS'lerin uymakla yükümlü olduğu ücretlerin alt ve üst sınırlarının belirlenmesine ilişkin usul ve esaslar Kurum tarafından tespit edilir.

**İdari Ücret**

**Madde 21** – Kurum ESHS'den bir önceki yıla ait net satışlarının binde dördü (% 0,4) kadar idari ücret alır. Bu ücretin tamamı Nisan ayının son iş gününe kadar Kuruma ödenir.

## YEDİNCİ BÖLÜM

## Denetim Usul ve Esasları

**Denetim**

**Madde 22 –** ESHS'nin denetimi Kurum tarafından gerek görülmesi halinde ve iki (2) yılda en az bir defa re'sen yapılır.

**Denetimde Uyulacak İlkeler**

**Madde 23 –** Denetimde aşağıdaki ilkelere uyulur;

a) Denetim faaliyeti sırasında, sonuçların değerlendirilmesinde ve denetim raporunun hazırlanmasında tarafsız olmak,

b) Dürüstlüğü ve tarafsızlığı etkileyebilecek herhangi bir müdahaleye imkan vermemek,

c) Denetim faaliyetine ilişkin çalışmaların her aşamasında gerekli özeni göstermek.

**Denetim Görevlilerinin Yetkileri**

**Madde 24 –** Denetim görevlileri;

a) Gerekli gördükleri her türlü defteri, belgeyi ve kayıtları istemeye, incelemeye ve bunların aslı ve/veya örneklerini almaya,

b) Yönetim yerleri, binalar ve eklentilerine girmeye ve bu yerlerde inceleme

yapmaya,

c) Konu ile ilgili yazılı ve/veya sözlü bilgi istemeye ve gerekli tutanakları düzenlemeye,

d) Her türlü işlem ve hesapları denetlemeye,

yetkilidir.

**Denetim Görevlilerinin Yükümlülükleri**

**Madde 25 –** Denetim görevlileri;

a) Denetime başlamadan önce denetim görevlisi olduklarına dair belge ile kendilerini tanıtmakla,

b) İlgililer tarafından kendilerine tevdi edilen defter, belge ve kayıtları işin gerektirdiği süre içinde olduğu gibi muhafaza ve işin bitiminde iade etmekle,

c) Denetim faaliyeti dolayısıyla edindikleri gizlilik niteliği taşıyan bilgileri, kanunen yetkili kılınanlardan başkasına açıklamamak ve doğrudan veya dolaylı şekilde kendi yararlarına kullanmamakla,

d) Defter, belge ve kayıtlar üzerinde incelemenin gereği olan işaretler dışında; şerh, ilave veya düzeltme yapmamakla,

e) Denetim yaptıkları yerlerde yönetim ve yürütme işlerine müdahale etmemekle,

yükümlüdürler.

**ESHS'nin Denetime İlişkin Yükümlülükleri**

**Madde 26 –** ESHS, denetim görevlilerinin yetkileri çerçevesindeki taleplerini en kısa sürede karşılamakla ve denetim görevlilerine elverişli bir çalışma ortamı sağlamakla yükümlüdür.

ESHS, gizlilik ve sır saklama gibi gerekçeler ileri sürerek denetim yükümlülüklerinden imtina edemez.

**Raporların Sunulması**

**Madde 27 –** Denetim görevlileri tarafından hazırlanan denetim raporu, denetim faaliyetinin sona ermesinden itibaren otuz (30) gün içinde Kurula sunulur.

Denetim sırasında ESHS'lerin faaliyet ve işleyişini olumsuz yönde etkileyebilecek derecede önem arz eden hususların tespit edilmesi halinde denetim görevlileri denetim faaliyetinin sonuçlanmasını beklemeksizin bu hususları içeren bir rapor hazırlayarak Kurula sunar.

**Kurul Kararı**

**Madde 28 –** Denetim raporu ve 27 nci maddenin ikinci fıkrasında belirtilen rapor Kurul tarafından öncelikli olarak gündeme alınır. Kurul, raporları değerlendirerek karar verir. Raporlarda, ilgili mevzuat hükümlerine aykırılık tespit edilmiş olması ve bu tespitin Kurul tarafından da sabit görülmesi halinde, ilgili mevzuatta öngörülen yaptırım ve cezaların uygulanmasına karar verilir.

## SEKİZİNCİ BÖLÜM

## Faaliyetin Sona Ermesi

**Kurum Tarafından Faaliyete Son Verilmesi**

**Madde 29 –** Kurum, yaptığı denetim sonucunda, ESHS'nin faaliyetinin devamı sırasında bildirim şartlarından birini veya birkaçını kaybettiğini tespit etmesi halinde ESHS'ye bu eksikliğin giderilmesi için bir (1) aya kadar süre verir ve bu süre içinde ESHS'nin faaliyetini durdurur. Kurum, vermiş olduğu sürenin sonunda eksikliğin giderilmemesi veya Kanunun 18 inci maddesindeki suçların işlendiği tarihten itibaren geriye doğru üç (3) yıl içinde üçüncü kez işlenmiş olması halinde ESHS'nin faaliyetine son verir.

Birinci fıkrada geçen faaliyete son verme hallerinden birinin gerçekleşmesi ile faaliyetine son verilen ESHS, faaliyete son verme kararının tebliği tarihinden itibaren onbeş (15) gün içinde faaliyette bulunan herhangi bir ESHS ile nitelikli elektronik sertifikaların devri konusunda anlaşabilir. Kurum, taraflar arasında anlaşma sağlanması durumunda, faaliyetine son verilen ESHS'nin oluşturduğu nitelikli elektronik sertifikaların anlaşma sağlanan ESHS'ye devredilmesine karar verir. Faaliyetine son verilen ESHS ile faaliyette bulunan herhangi bir ESHS arasında onbeş (15) gün içinde nitelikli elektronik sertifikaların devrine ilişkin anlaşma sağlanamaması durumunda Kurum, sertifikaların herhangi bir ESHS'ye devrine re'sen karar verir. Nitelikli elektronik sertifikaları devralan ESHS sertifika yenileme işlemlerini başlatır ve devir kararının tebliği tarihinden itibaren bir (1) ay içinde bu işlemleri tamamlar. Kurum, uygun görmesi halinde, bir (1) ayı geçmemek üzere ek süre verebilir.

ESHS, Kurumun faaliyete son verme kararının tebliğinden itibaren elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayamaz. Ancak, sertifika yenileme işlemleri tamamlanıncaya kadar iptal durum kaydı hizmetini devam ettirir.

Faaliyetine son verilen ESHS nitelikli elektronik sertifikaları devralan ESHS'ye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devreder ve kendi imza oluşturma verisi ile yedeklerini imha eder.

Kurum, nitelikli elektronik sertifikaları re'sen devredebileceği herhangi bir ESHS'nin bulunmaması durumunda, faaliyetine son verdiği ESHS'nin oluşturduğu nitelikli elektronik sertifikaların iptal edilmesine karar verir. Faaliyetine son verilen ESHS son iptal durum kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder, geçerlilik süresi en geç sona eren nitelikli elektronik sertifikanın geçerlilik süresi sonuna kadar iptal durum kaydı hizmetini devam ettirir ve arşivi en az yirmi (20) yıl süreyle saklar.

Kurum, nitelikli elektronik sertifikaların devrine ilişkin kararları internet sayfasında yayımlar. Faaliyetine son verilen ESHS devire ilişkin kararları nitelikli elektronik sertifika sahiplerine elektronik posta ile duyurur ve internet sayfasında yayımlar.

**ESHS'nin Faaliyetine Son Vermesi**

**Madde 30 –** ESHS faaliyetine son vereceği tarihten en az üç (3) ay önce durumu Kuruma yazılı olarak bildirir. ESHS, faaliyetine son verme kararının Kuruma bildirilmesinden itibaren nitelikli elektronik sertifika başvurusu kabul edemez ve yeni nitelikli elektronik sertifika oluşturamaz.

ESHS faaliyetine son vereceği tarihten en az üç (3) ay önce faaliyetine son verme kararını internet sayfasında yayımlar, sertifika sahiplerine elektronik posta ile bildirir ve ulusal yayın yapan en yüksek tirajlı üç (3) gazetede ilan vermek suretiyle kamuoyuna duyurur.

ESHS; faaliyetine son verme tarihine kadar geçerlilik süresi sona ermeyecek ve kullanımı faaliyette bulunan herhangi bir ESHS tarafından sağlanabilecek nitelikli elektronik sertifikaları, faaliyete son verme tarihinden bir (1) ay öncesine kadar faaliyette bulunan herhangi bir ESHS'ye devredebilir. Faaliyetine son veren ESHS devir hususunda sertifika sahiplerini elektronik posta ile bilgilendirir. Nitelikli elektronik sertifikaların devredilmesi halinde sertifikaları devralan ESHS sertifika yenileme işlemlerini başlatır ve bir (1) ay içinde bu işlemleri tamamlar. Kurum, uygun görmesi halinde, bir (1) ayı geçmemek üzere ek süre verebilir.

Nitelikli elektronik sertifikaları devreden ESHS sertifikaları devralan ESHS'ye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devreder ve kendi imza oluşturma verisi ile yedeklerini imha eder.

Faaliyetine son verme tarihinden bir (1) ay öncesine kadar nitelikli elektronik sertifikaların devredilememesi veya nitelikli elektronik sertifikaların kullanımının faaliyette

bulunan herhangi bir ESHS tarafından sağlanamaması durumunda, faaliyetine son vermek isteyen ESHS nitelikli elektronik sertifikaları faaliyete son verme tarihinde iptal eder. Faaliyetine son veren ESHS son iptal durum kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder, geçerlilik süresi en geç sona eren nitelikli elektronik sertifikanın geçerlilik süresi sonuna kadar iptal durum kaydı hizmetini devam ettirir ve arşivi en az yirmi (20) yıl süreyle saklar.

## DOKUZUNCU BÖLÜM

## Diğer Hükümler

**Zaman Damgası ve Hizmetleri**

**Madde 31 –** ESHS, zaman damgası ve hizmetlerini sağlamakla yükümlüdür. Nitelikli elektronik sertifika sahibi, bu hizmeti talep etmesi halinde alır.

**Yabancı Elektronik Sertifikaların Kabul Edilmesi**

**Madde 32 –** Yabancı elektronik sertifikaların hukuki sonuçlarına ve kabul edilmesine ilişkin şartlar milletlerarası anlaşmalarla belirlenir.

Milletlerarası anlaşma bulunmaması halinde, yabancı bir ülkede kurulu bir ESHS tarafından verilen elektronik sertifikaların Türkiye'de kurulu bir ESHS tarafından kabul edilmesi için asgari olarak;

a) Yabancı elektronik sertifikanın, Kanunda ve bu Yönetmelikte yer alan nitelikli elektronik sertifikanın teknik şartlarını taşıması,
b) Yabancı ESHS'nin kurulu bulunduğu ülkede ESHS olarak faaliyet göstermesi, gerekir.

Türkiye'de kurulu bir ESHS, kabul edeceği yabancı elektronik sertifika ile ilgili aşağıdaki belgeleri, sertifikaların kullanımına başlanmadan bir (1) ay önce Kuruma verir;

a) Elektronik sertifikalarını kabul edeceği yabancı ESHS'nin kendi sertifikasının örneği,
b) Yabancı ESHS'nin kurulu bulunduğu ülkede ESHS olduğuna dair yetkili merciden alınmış belge,
c) Yabancı elektronik sertifikanın, Kanun ve bu Yönetmelikte yer alan nitelikli elektronik sertifikanın teknik şartlarını taşıdığına dair bilgi ve belgeler.
Kurum, yabancı ESHS'ye ait bilgileri internet sayfasında yayımlar.

Kabul edilen yabancı elektronik sertifikaların kullanılması sonucunda doğacak her türlü zarardan sertifikaları kabul eden Türkiye'deki ESHS de sorumludur.

**Faaliyet Raporu**

**Madde 33 –** ESHS, Kuruma her yıl Mart ayı sonuna kadar bir önceki yıla ilişkin rapor verir. Rapor asgari aşağıdaki unsurları içerir;

a) Oluşturulan sertifika türleri ve sayıları,
b) Her bir sertifika türüne göre iptal edilen sertifika sayısı,
c) ESHS'nin geçmiş yıla ait mali durumunu gösterir bilgi ve belgeler,
d) Varsa kendisine devredilen sertifikaların durumuna ilişkin bilgiler,
e) ESHS'nin bir sonraki yıla ait pazar öngörüleri,
f) Kurum tarafından istenecek diğer bilgi ve belgeler.

**Teknik Hususlara İlişkin Tebliğ**

**Madde 34 –** Nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve

hizmetlerine ilişkin uyulması gereken teknik kriterler tebliğ ile belirlenir. Kurum gerekli görülen hallerde tebliği günceller.

**Hüküm Bulunmayan Haller**

**Madde 35 –** Elektronik imzayla ilgili bu Yönetmelikte hüküm bulunmayan haller için Kurul Kararı ile düzenleme yapılır.

**Geçici Hükümler**

**Geçici Madde –** ESHS, Kurum tarafından nitelikli elektronik sertifika, zaman damgası ve ilgili hizmetlere ait ücretlerin alt ve üst sınırları belirleninceye kadar, 5 inci maddede yer alan genel ilkeler çerçevesinde nitelikli elektronik sertifika, zaman damgası ve ilgili hizmetlere ilişkin ücretleri belirleyebilir.

**Yürürlük**

**Madde 36 –** Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

**Yürütme**

**Madde 37 –** Bu Yönetmelik hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

**Yönetmeliğe EK-1**

**Bildirimde Sunulacak Bilgi ve Belgeler**

ESHS olmak isteyen kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, yapacakları bildirimde aşağıdaki bilgi ve belgeleri Kuruma sunar:

1) **İletişim Bilgileri:** Adı/unvanı ve tüm birimlerine ait iletişim bilgileri (adres, telefon, faks, e-posta adresi, internet adresi),
2) **Şirket ile İlgili Belgeler:** Ticari şirket ise; şirketin kuruluş Ticaret Sicil Gazetesi, vergi levhası, şirketin imza sirküleri, ticaret sicil belgesi ve şirketi temsile yetkili kişi/kişilerin adli sicil kayıtları ve iletişim bilgileri,
3) **Personel:** Organizasyon şeması, istihdam ettiği kişilerin ESHS personeli olduğunu gösterir sosyal güvenlik kuruluşundan alınmış belge, istihdam ettiği ve ettirdiği tüm personelin adli sicil kayıtları ile teknik personelin özgeçmişi ve uzmanlığını ispatlayan belgeleri**,**
4) **Sertifika İlkeleri ve Sertifika Uygulama Esasları,**
5) **Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları,**
6) **Kendi Sertifikasının Örneği,**
7) **Sertifika Mali Sorumluluk Sigortası:** Sertifika mali sorumluluk sigortası için sigorta şirketi ile yaptığı sözleşmenin bir örneği,
8) **Sözleşme Örneği:** Nitelikli elektronik sertifika sahipleri ile yapacağı sözleşmenin bir örneği,
9) **Hizmet Sözleşmesi:** Hizmet alması durumunda, hizmet aldığı taraf ile imzaladığı sözleşmenin bir örneği**,**
10) **Tebliğ ile İstenilen Bilgi ve Belgeler.**

# EK-C Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

## BİRİNCİ BÖLÜM

Genel Hükümler

**Amaç**

**Madde 1 —** Bu Tebliğin amacı, elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirlemektir.

**Kapsam**

**Madde 2 —** Bu Tebliğ; nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve hizmetlerine ilişkin teknik hususları kapsar.

**Dayanak**

**Madde 3 —** Bu Tebliğ, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 34 üncü maddesine dayanılarak hazırlanmıştır.

**Tanımlar**

**Madde 4 —** Bu Tebliğde geçen;

Yönetmelik: Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliği,

BS (British Standards): İngiliz Standartlarını,

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesini,

CWA (CEN Workshop Agreement): CEN Çalıştay Kararını,

DSA (Digital Signature Algorithm): Sayısal İmza Algoritmasını,

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

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyini,

ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsünü,

ETSI SR (ETSI Special Report): ETSI Özel Raporunu,

ETSI TS (ETSI Technical Specification): ETSI Teknik Özelliklerini,

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

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

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

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliğini,

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): RACE Bütünlük Asli Mesaj Değerlendirme Özetini,

RSA: Rivest-Shamir-Adleman'ı,

SHA (Secure Hash Algorithm): Güvenli Özet Algoritmasını ifade eder.

Bu Tebliğde yer almayan tanımlar için Kanun ve Yönetmelikte yer alan tanımlar geçerlidir.

## İKİNCİ BÖLÜM

Teknik Hususlar

**ESHS'nin İşleyişi**

**Madde 5 —** ESHS işleyişinin bütün aşamalarında;

a) ETSITS 101 456 ve

b) CWA 14167-1

standartlarına uyar.

Nitelikli elektronik sertifikalar;

a) ETSITS 101 862 ve

b) ITU-TRec. X.509V.3'e

uygun olarak oluşturulur.

**Algoritmalar ve Parametreler**

**Madde 6 —** İmza oluşturma ve doğrulama verileri, aşağıda belirtilen algoritma ve parametrelere uygun olarak oluşturulur;

a) İmza sahibinin imza oluşturma ve doğrulama verileri

i. RSA için en az 1024 bit veya

ii. DSA için en az 1024 bit veya

iii. DSA Eliptik Eğrisi için en az 160 bit

b) ESHS'nin imza oluşturma ve doğrulama verileri

i. RSA için en az 2048 bit veya

ii. DSA için en az 2048 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit Özetleme algoritması olarak;

a) RIPEMD-160 veya

b) SHA-1

kullanılır.

Yukarıda belirtilen algoritmalar ve parametreler 31/12/2005 tarihine kadar geçerlidir.

Yukarıda belirtilen algoritmalara ve parametrelere bağlı kalmak şartı ile ETSI SR 002 176 raporunda belirtilen imza oluşturma ve doğrulama verilerinin oluşturulmasında kullanılan algoritma ve parametreler de geçerlidir.

**Sertifika İlkeleri ve Sertifika Uygulama Esasları**

**Madde 7 —** ESHS; sertifika ilkelerini ve sertifika uygulama esaslarını IETF RFC 3647'ye uygun olarak hazırlar.

**Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları**

**Madde 8 —** Güvenli elektronik imza oluşturma araçları CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olmalıdır.

ESHS, sağlamış olduğu güvenli elektronik imza doğrulama araçları için CWA 14171 standardına uyar ve bunu yazılı olarak taahhüt eder.

**Güvenlik Kriterleri**

**Madde 9 —** ESHS, güvenlik kriterlerine ilişkin olarak;

a) CWA 14167-1,

b) ETSITS 101 456 ve

c) TS ISO/IEC 17799 veya ISO/IEC 17799

standartlarına uyar.

**Zaman Damgası ve Hizmetleri**

**Madde 10 —** ESHS, zaman damgası ve hizmetlerine ilişkin olarak;

a) CWA 14167-1 ve

b) ETSI TS 101 861

standartlarına uyar.

Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanır.

**Belgeler**

**Madde 11 —** ESHS;

a) BS 7799-2 standardına uygunluğunu,

b) Güvenli elektronik imza oluşturma araçlarının;

i. FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

ii. CWA 14167-2'de belirtilen kriterlere uygunluğunu veya

iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya

ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu yetkili kurum veya kuruluşlardan alman belgelerle belgelendirir.

## ÜÇÜNCÜ BÖLÜM

Diğer Hükümler

**Yürürlük**

**Madde 12 —** Bu Tebliğ yayımı tarihinde yürürlüğe girer.

**Yürütme**

**Madde 13 —** Bu Tebliğ hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

# EK-D Kamu Sertifikasyon Merkezi'nin Oluşturulması Hakkında Başbakanlık Genelgesi

## Genelge

Başbakanlıktan:

Konu: Kamu Sertifikasyon Merkezi Oluşturulması.

**Genelge**
**2004/21**

23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanarak, 23 Temmuz 2004 tarihinde yürürlüğe girmiş bulunan 5070 sayılı Elektronik İmza Kanunu ile güvenli elektronik imzanın elle atılan imza ile aynı ispat gücüne sahip olduğu ve bu şekilde oluşturulan elektronik verilerin hukuken geçerli olacağı hususları düzenlenmiştir.

Kanun ile yapılan düzenlemeler, kamu kurum ve kuruluşlarının kendi aralarında yapacakları iletişimin yanı sıra, vatandaşlar ve iş alemi ile arasındaki iletişimin niteliğini, güvenilirliğini, etkinliğini ve hızını da büyük oranda ve olumlu yönde etkileyecektir. Elektronik imzanın sağlayacağı imkanlardan yararlanabilmek için, kamu çalışanları da dahil olmak üzere, vatandaşların, Kanun'da belirtilen nitelikleri haiz bir elektronik sertifika hizmet sağlayıcısından elektronik sertifika temin etmeleri yeterli olacaktır.

Diğer taraftan, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaya çalıştıkları gözlenmektedir. Bu münferit çalışmaların, bir yandan sistemin kendi işleyişi içerisinde karmaşaya yol açması, diğer yandan da mükerrerliklere ve dolayısıyla emek ve kaynak israfına neden olması kaçınılmazdır.

Yasanın yürürlüğe girmesiyle birlikte ülkemizde de giderek yaygınlaşacak olan elektronik imza uygulamaları kapsamında; kamu kurum ve kuruluşlarının elektronik ortamlarda yürütecekleri iş ve işlemlerde uyumlu, birlikte işler ve güvenilir bir yapıda çalışmasını sağlamak maksadıyla, 10 Haziran 2004 tarihinde yapılan e-Dönüşüm Türkiye İcra Kurulu VI. Toplantısı'nda alınan 6 sayılı İcra Kurulu Kararı ile kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması kararlaştırılmıştır.

Bu kapsamda, tüm kamu kurum ve kuruluşlarının, kurumsal sertifika (kamu çalışanlarınca kurum içi ve kurumlar arası işlemlerde kullanılacak sertifika) ihtiyaçlarının karşılanması amacıyla bir Kamu Sertifikasyon Yapısı oluşturulması kararlaştırılmıştır.

Söz konusu yapı içerisinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı ile buna bağlı olarak Kamu Sertifika Hizmet Sağlayıcısı kurulacaktır. Yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet Sağlayıcısı sistemlerini kendi bünyelerinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları kurumsal sertifikalarını, Kamu Sertifika Hizmet Sağlayıcısından temin edeceklerdir.

Kamu çalışanları, kurumsal sertifikalarını kamu dışı bireysel işlemlerinde de kullanabilecektir.

Kurulacak bu Kamu Sertifikasyon Yapısı içinde yer alan Kök Sertifika Hizmet Sağlayıcısı, dileyen gerçek ve tüzel kişilerin kuracakları Sertifika Hizmet Sağlayıcılarına da kök sertifika hizmeti verebilecektir.

Ulusal güvenlik gerekleri göz önünde bulundurularak, kurumsal sertifika ihtiyacının karşılanması amacıyla oluşturulacak Kamu Sertifikasyon Yapısı içinde kurulacak olan Kök Sertifika Hizmet Sağlayıcısı ve Kamu Sertifika Hizmet Sağlayıcısı milli yazılım ürünlerini kullanacaktır.

Bu kapsamda; tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulması ve sertifika yaşam çevriminin yönetilmesini sağlayacak Kamu Sertifikasyon Yapısının kurulması ve işletilmesi görev ve sorumluluğu Türkiye Bilimsel ve Teknik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü'ne (UEKAE) verilmiştir. Söz konusu yapının gözden geçirilmesi ve uygunluğunun izlenmesi görev ve sorumluluğu ise Telekomünikasyon Kurumuna verilmiştir.

Bahse konu Kamu Sertifikasyon Yapısının kurulması için TÜBİTAK-UEKAE tarafından gerekli çalışmalar derhal başlatılacaktır. Bu çerçevede; TÜBİTAK-UEKAE tarafından ihtiyaç duyulacak kaynak tahsisi ve düzenlemelere ilişkin çalışmalar ile kurulacak yapıya uyum için kamu kurum ve kuruluşları nezdinde sürdürülecek çalışmalar, DPT Müsteşarlığının koordinasyonunda yürütülecektir.

Yukarıda belirtilen istisnalar dışındaki kamu kurum ve kuruluşları, sertifika ihtiyaçlarını karşılamak amacıyla Sertifika Hizmet Sağlayıcısı olmak üzere kendi bünyelerinde hiçbir surette yeni yatırım yapmayacaklardır. Bu konuda başlatılmış ve sürdürülmekte olan ihale çalışmaları ile henüz sözleşmeye bağlanmamış olan tüm ihaleler derhal iptal edilecektir. Sözleşmeye bağlanmış olanlardan, tek taraflı fesih hakkı bulunan sözleşmeler derhal feshedilecek, halihazırda kullanılmakta olan sistemler ise Telekomünikasyon Kurumu'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

Ayrıca; henüz kullanıma geçmemiş olmakla birlikte, çalışmaları devam eden ve sözleşmeleri tek taraflı olarak fesih edilemeyen proje ya da proje bileşenlerine ilişkin karar, DPT Müsteşarlığı ve ilgili kuruluşun ortak çalışması ile sonuçlandırılacaktır.

Kamu kurum ve kuruluşları, bu Genelge çerçevesinde tek taraflı olarak feshettikleri veya tek taraflı fesih hakkı olmayan proje ya da proje bileşenleri konusunda detaylı bilgileri içerecek raporları, Genelge'nin yayımı tarihinden itibaren 15 gün içinde Devlet Planlama Teşkilatı Müsteşarlığına ileteceklerdir.

Bilgilerini ve gereğini rica ederim.

Recep Tayyip ERDOĞAN

Başbakan

# EK-E Zorunlu Sertifika Mali Sorumluluk Sigortası Tebliğ

Devlet Bakanlığından:

**Genel Şartları**

**A- SİGORTANIN KAPSAMI**

**A.1- Sigortanın Konusu**

Bu sigorta ile; ulusal veya uluslararası düzeyde nitelikli elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan Elektronik Sertifika Hizmet Sağlayıcısının (ESHS) Elektronik îmza Kanunundan doğan yükümlülüklerini yerine getirmemesi sonucu oluşan, nitelikli elektronik sertifika sahibi kişi veya kuruluşların ve üçüncü şahısların uğrayacağı zararlara ilişkin sorumluluğu, sözleşmede belirlenen zorunlu sigorta limitlerine kadar teminat altına alınmıştır.

Bu sigorta, sigortalıya karşı yapılan talepler sonucundaki yasal giderler için de teminat verir.

**A.2- Sigorta Teminatının Kapsamı**

Sertifika Mali Sorumluluk Sigortası;

**A.2.1.** ESHS'nin güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek, sertifikaların taklit ve tahrif edilmesini önlemek ile ilgili görevlerini gerektiği biçimde yerine getirmemesi,

**A.2.2.** Sertifikaların içeriğinde ESHS'den kaynaklanan yanlış bilgilerin bulunması,

**A.2.3**. Sertifikaların oluşturulması sırasında nitelikli elektronik imza sahiplerinin verdikleri bilgilerin ESHS tarafından eksik veya yanlış işlenmesi sonucu ortaya çıkan hataların bulunması,

**A.2.4.** Sertifikaların ESHS ile nitelikli elektronik imza sahipleri arasında yapılan sözleşmeye tam ve uygun olarak hazırlanmaması,

gibi ESHS'nin ve eylemlerinden sorumlu bulunduğu personelin kusurundan, ihmalinden veya gerekli özeni göstermemesinden doğan maddi zararları kapsar.

Türkiye'de faaliyette bulunan ESHS'nin sigortacının bilgisi dahilinde olan yabancı bir ülkede kurulu başka bir ESHS'ye ait kabul ettiği sertifikalardan doğan maddi zararlar da kapsam dahilindedir.

**A.3- Sigorta Sözleşmesinin Süresi**

Sözleşmenin süresi taraflar arasında serbestçe belirlenir. Poliçede başlama ve sona erme tarihlerinin gün ve saat olarak yazılması gerekir.

**A.4- Teminat Dışında Kalan Haller**

Aşağıdaki hallerden birinin veya birkaçının sonucunda doğan sorumluluğa bağlı

olarak;

**A.4.1.** Savaş, düşman hareketleri, çarpışma (savaş ilan edilmiş olsun veya olmasın), ihtilal, ayaklanma ve bunların gerektirdiği inzibati askeri hareketlerden,

**A.4.2.** Herhangi bir nükleer yakıttan veya nükleer yakıtın yanması sonucu nükleer atıklardan veya bunlara atfedilen sebeplerden meydana gelen iyonlayıcı radyasyonlar veya radyo-aktivite bulaşmaları ve bunların gerektirdiği inzibati ve askeri tedbirlerden,

**A.4.3.** Deprem, yanardağ püskürmesi, deniz depremi, sel, seylap ve su baskını, yer kayması gibi doğal afetlerden,

**A.4.4.** Kamu otoritesi tarafından yapılacak tasarruflar sonucunda oluşan ve ESHS'nin kusurundan kaynaklanmayan sorunlardan,

**A.4.5.** İletişim altyapısı ve ESHS'nin doğrudan kontrolü altında olmayan bilgi işlem altyapısında meydana gelen sorunlardan,

**A.4.6.** İmza sahibi tarafından kanun dışı amaçlar için nitelikli elektronik imzanın kullanılmasından,

**A.4.7.** Sigortacıya veya sigorta ettirene haber verildikten sonraki bir tarihte ESHS tarafından iptal edilmeyip ikinci veya daha çok miktarda hasar oluşmasına neden olan aynı nitelikli elektronik sertifika ile işlem yapılmasından,

**A.4.8.** Faaliyet konusu ile ilgili kanun, yönetmelik ve tebliğlerle belirlenen esaslar ve teknik standartlara bağlı kalınmamasından,

doğan zararlar sigorta teminatı dışındadır.

**B- ZARAR VE TAZMİNAT**

**B.l- Rizikonun Gerçekleşmesi**

ESHS'nin, sözleşme süresi içinde Kanundan kaynaklanan yükümlülüklerini yerine getirmemesi nedeniyle, sertifika sahibi veya üçüncü kişilerin sözleşme dönemi içinde veya sonrasında zarara uğraması sonucunda;

**B.1.1.** Sigortacının bilgisi dahilinde olmak koşuluyla sigortalı tarafından ödeme yapılması veya,

**B.l.2.** Zararın gerçekleştiğinin ve bu zararın ESHS'nin sorumluluğundan kaynaklandığının mahkeme tarafından karar altına alınması veya

**B.1.3.** Sigortalının tebligat üzerine davayı öğrendiği tarihte,

riziko gerçekleşmiş olur.

**B.1.2- Rizikoya İlişkin Olarak Sigorta Ettirenin ve Sigortalının Yükümlülükleri**

Sigortalı/sigorta ettiren rizikonun gerçekleşmesi halinde, aşağıdaki hususları yerine getirmekle yükümlüdür:

a) Bu sözleşmeye göre, sorumluluğunu gerektirecek bir olayı, haberdar olduğu andan itibaren beş gün içinde sigortacıya ihbar etmek,

b) Sigortalı değilmişçesine gerekli kurtarma ve koruma önlemlerini almak ve bu

amaçla
sigortacı tarafından verilecek makul talimatlara uymak,

c) Sigortacının talebi üzerine, olayın ve zararın nedeni ile hangi hal ve şartlar altında
gerçekleştiğini ve sonuçlarını tespiti, tazminat yükümlülüğü ve miktarı ile rücu hakkının kullanılmasına yararlı, elde edilmesi mümkün bilgi ve belgeleri gecikmeksizin vermek,

d) Zarardan dolayı, dava yolu ile veya başka yollarla bir tazminat talebi karşısında kaldığı veya aleyhine cezai kovuşturmaya geçildiği hallerde, durumdan sigortacıyı derhal haberdar etmek ve zarar ziyan talebine ve cezai kovuşturmaya ilişkin olarak almış olduğu ihbarname, davetiye ve benzeri tüm belgeleri derhal sigortacıya vermek,

e) Sigorta konusu ile ilgili başka sigorta sözleşmesi varsa bunları sigortacıya bildirmek.

**B.3- Tazminat ve Ödenmesi**

Rizikonun gerçekleşmesi halinde, özel durumlar hariç olmak üzere, hangi belgelerin istenileceği poliçe ekinde yer almak zorundadır. Sigortacı, talep edilen tazminat ve giderleri, hak sahibinin tazminata konu olay ve zarara ilişkin tespit tutanağını veya bilirkişi raporunu ve poliçe ekinde de yer alan diğer gerekli belgeleri eksiksiz olarak şirketin merkez veya kuruluşlarına ilettiği tarihten itibaren on iş günü içinde gerekli incelemeleri tamamlayıp sözleşmeye aykırı olmayan maddi zararlara ilişkin tazminatı öder.

**B.4- Halefiyet**

Sigortacı, ödediği tazminat tutarınca, hukuken sigortalının yerine geçer.

**C- ÇEŞİTLİ HÜKÜMLER**

**C.l- Sigorta Priminin Ödenmesi ve Sigortacının Sorumluluğunun Başlaması**

Sigortacının sorumluluğu, primin tamamının veya taksitle ödenmesi kararlaştırılmış ise ilk taksidin poliçenin tesliminde ödenmesi ile başlar. Aksi kararlaştırılmadıkça, primin tamamının veya ilk taksidin ödenmemesi halinde, poliçe teslim edilmiş olsa dahi sigortacının sorumluluğu başlamaz ve bu şart poliçeye yazılır.

Prim ödemede temerrüde düşülmesi halinde Borçlar Kanunu hükümleri uygulanır.

**C.2- Sigortalının/Sigorta Ettirenin Sözleşme Yapıldığı Sırada Beyan Yükümlülüğü**

**C.2.1.** Sigortacı sigorta sözleşmesini, sigorta ettirenin veya sigortalının beyanı ve varsa teklifname ve eklerinde yazılı sorulara verdiği cevaplara dayanarak yapar.

**C.2.2.** Sigortalının/sigorta ettirenin beyanı yanlış veya eksik ise ve bu durum, sigortacının sözleşmeyi yapmaması veya daha ağır şartlarla yapmasına neden oluyorsa, sigortacı durumu öğrendiği tarihten itibaren bir ay içinde sözleşmeden cayabilir veya sözleşmeyi yürürlükte tutarak aynı süre içinde prim farkını talep edebilir.

**C.2.3.** Sigorta ettiren, talep edilen prim farkını kabul ettiğini sekiz gün içinde bildirmediği takdirde sözleşmeden cayılmış olur. Ancak, prim farkının kabul edilmemesi nedeniyle sözleşmeden cayılması, sigortacının gerçeğe aykırı veya eksik beyanı öğrendiği

tarihten itibaren bir aylık süre içinde gerçekleşmek durumundadır.

**C.2.4** Sigortalının/sigorta ettirenin kasıtlı davrandığının anlaşılması halinde sigortacı, sözleşmeden cayabilir ve gün esasına dayanarak hesap edilen prime hak kazanır.

**C.3 Sözleşmenin Devamı Sırasındaki Beyan Yükümlülüğü**

Sözleşmenin devamı sırasında sigortacının izni olmadan rizikoya etki edici nitelikte değişiklik yapılması halinde sigorta ettiren veya sigortalı durumu sekiz gün içinde sigortacıya bildirmekle yükümlüdür.

Durumun sigortacı tarafından öğrenilmesinden sonra, değişiklik, sigortacının sözleşmeyi yapmamasını veya daha ağır şartlarla yapmasını gerektiren hallerde ise sigortacı, sekiz gün içinde sözleşmeyi fesheder veya prim farkını talep etmek suretiyle sözleşmeyi yürürlükte tutar. Sigorta ettiren, talep edilen prim farkını kabul ettiğini sekiz gün içinde bildirmediği takdirde sözleşme feshedilmiş olur.

Feshin hüküm ifade ettiği tarihe kadar geçen sürenin primi, gün esası üzerinden hesap edilir ve fazlası geri verilir.

Süresinde kullanılmayan fesih veya prim farkını talep etme hakkı düşer.

Rizikodaki değişikliği öğrenen sigortacı, sigorta hükmünün devamına razı olduğunu gösteren bir harekette bulunursa fesih ve prim talep hakkı düşer.

Değişiklik, rizikoyu hafifletici nitelikte ve daha az prim uygulamasını gerektirir hallerden ise: Sigortacı, bu değişikliğin yapıldığı tarihten sözleşmenin sona ermesine kadar geçecek süre için gün esasına göre hesap edilecek prim farkını sigorta ettirene geri verir.

Sigortacının sözleşmeyi bu değişiklere göre yapmamasını veya daha ağır şartlarla yapmasını gerektiren hallerde:

a) Sigortacı durumu öğrenmeden önce,

b) Sigortacının fesih ihbarında bulunabileceği süre içinde,

c) Fesih ihbarının hüküm ifade etmesi için geçecek süre içinde,

riziko gerçekleşirse, sigortacı, tazminatı tahakkuk ettirilen prim arasındaki orana göre öder.

**C.4. Sözleşmenin Devamı Sırasındaki Koruma Yükümlülüğü**

**C.4.1** Sigortalı, sertifikaları imzalama amacıyla kullandığı imza oluşturma verisini korumaya ilişkin bütün işlemleri, sözleşme süresi boyunca, rizikonun tutarı ve süresini de dikkate alarak, sigortalı değilmişçesine özenle yürütmekle yükümlüdür.

**C.4.2.** Sigortalı, sertifikaları imzalama amacıyla kullandığı imza oluşturma verisinin, yetkisiz kullanıma veya benzeri bir güvenlik ihlaline konu olduğunu anladığında hemen sigortacıyı haberdar etmek zorundadır.

**C.4.3.** Sigorta ettiren sigorta ettirdiği sorumluluğuna ilişkin herhangi bir güvenlik ihlalini haber alır almaz, gerekli önlemleri aldıktan sonra, sigortacıya haber vermek zorundadır.

**C-5 Sigortalının (ESHS) Değişmesi**

Aksine sözleşme yoksa sözleşme süresi içinde sigortalının değişmesi halinde sözleşme yeni sigortalı ile devam eder.

**C-6 Birden Çok Sigorta**

Sigorta ettiren ya da sigortalı başka sigorta şirketleriyle aynı rizikolara karşı aynı süreye rastlayan başka sigorta sözleşmesi yapacak olursa bunu sigortacılara derhal bildirmekle yükümlüdür.

**C.7- Tebliğ ve İhbarlar**

**C.7.1** Sigortalının/sigorta ettirenin bildirimleri, sigorta şirketinin merkezine veya sigorta sözleşmesine aracılık eden acenteye yapılır.

**C.7.2** Sigortacının bildirimleri de sigortalının/sigorta ettirenin poliçede gösterilen adresine veya bu adres değişmişse son bildirilen adresine noter eliyle veya taahhütlü mektupla yapılır.

**C.7.3** Taraflara imza karşılığı elden verilen mektup veya telgrafla yapılan bildirimler de taahhütlü mektup hükmündedir.

**C.7.4** Güvenli elektronik imza kullanılarak elektronik ortamda yapılan ve sigortalıya/sigorta ettirene ulaştığı kanıtlanabilen bildirimler de geçerli sayılır.

**C.8- Ticari ve Mesleki Sırların Saklı Tutulması**

Sigortacı ve sigortacı adına hareket edenler bu sözleşmenin yapılması dolayısıyla sigortalıya/sigorta ettirene ilişkin öğreneceği ticari, teknik ve mesleki sırların saklı tutulmamasından doğacak zararlardan sorumludurlar.

**C.9- Yetkili Mahkeme**

Sigorta sözleşmesinden doğan anlaşmazlıklar nedeniyle sigortacı aleyhine açılacak davalarda yetkili mahkeme, sigorta şirketinin merkezinin veya sigorta sözleşmesine aracılık yapan acentenin ikametgahının bulunduğu yerdeki, sigortalı/sigorta ettiren aleyhine açılacak davalarda ise davalının ikametgahının bulunduğu yerdeki ticaret davalarına bakmakla görevli mahkemedir.

**CIO- Zaman aşımı**

Sigorta sözleşmesinden doğan bütün talepler iki yılda zaman aşımına uğrar.

**C.II- Özel Şartlar**

Sigorta sözleşmesine, sigortalının / sigorta ettirenin aleyhine olmamak kaydıyla özel şartlar konulabilir.

**C.12- Yürürlük**

Bu Genel Şartlar yayımı tarihinde yürürlüğe girer.

# EK-F Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı Tebliğ

Devlet Bakanlığından:

23 Ocak 2004 tarihli ve 25355 sayılı Resmî Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ve 26 Ağustos 2004 tarihli Resmî Gazetede yayımlanan Sertifika Mali Sorumluluk Sigortası Yönetmeliğine göre yapılacak "Sertifika Mali Sorumluluk Sigortası"na aşağıdaki tarife ve talimat uygulanır.

Türkiye'de kaza branşında ruhsatı olan bütün sigorta şirketleri, Sertifika Mali Sorumluluk sigortasını yapmakla yükümlüdür.

**A. TARİFE**

Teminat tutarları, sigorta teminatı kapsamına giren olay başına, aşağıdaki şekilde belirlenmiştir:

a) Olay başına : 10.000 YTL.

b) Sözleşme süresince toplam : 1.000.000. YTL.

Sigorta primleri, sigorta şirketlerince serbestçe belirlenir.

Bu Tarife ve Talimatın yürürlüğe girmesinden sonra yapılacak sigorta sözleşmeleri, yukarıdaki teminatlar üzerinden yapılır. Ancak, sözleşme süresi içinde, Hazine Müsteşarlığının bağlı bulunduğu Bakan tarafından teminat tutarları artırıldığı takdirde, eski teminat tutarları üzerinden sigortası yapılmış ve süresi devam eden sigorta sözleşmesine Elektronik Sertifika Hizmet Sağlayıcıları, sigorta şirketlerine başvurarak yeni teminatlar üzerinden Sertifika Mali Sorumluluk Sigortası zeyilnamelerini bu Tarife ve Talimatın yürürlük tarihinden itibaren 15 gün içinde almak zorundadır. Zeyilname yapılmayan ve teminatları yeni limitlere getirilmeyen sigorta sözleşmelerinde, sigorta şirketlerinin sorumluluğu eski teminat tutarları ile sınırlıdır.

Sigorta sözleşmesine bağlı olarak sigorta ettirene yüklenmiş veya yüklenecek vergi, resim, harç ve diğer yükümlülükler sigorta ettirenden alınır.

**B. TALİMAT**

Bu sigorta, 5070 sayılı Elektronik İmza Kanunu kapsamında Elektronik Sertifika Hizmet Sağlayıcısından nitelikli elektronik sertifika, zaman damgası, elektronik imza hizmetlerinden. birini veya birkaçım alan nitelikli elektronik sertifika sahipleri ve bu sertifikalara dayanarak işlem yapan üçüncü kişileri, Sertifika Mali Sorumluluk Sigortası Genel Şartları'nın 2 nci maddesinde yer alan risklere karşı teminat altına alır.

Elektronik Sertifika Hizmet Sağlayıcısı, şirket merkezi ile internet adresindeki sayfasına sigorta sözleşmesine ait kısa bilgiler ile sigortacının adı ve açık adresini

belirten ibareleri kolaylıkla görülebilecek bir yerde bulundurmak zorundadır.

**C. YÜRÜRLÜK**

Bu Tarife ve Talimat yayımı tarihinde yürürlüğe girer.

## KAYNAKÇA

(Brink, 2001) Derek Brink ve diğerleri, "PKI Interoperability Framework", PKIforum white paper

(Entrust, 2000) "The Concept of Trust in Network Security", Entrust Security Digital Identities&Information

(Kiran, 2002) Shashi Kiran ve diğerleri, "PKI Basics-A Technical Perspective", PKIforum PKInote

(Lloyd, 2001) Steve Lloyd ve diğerleri, "CA-CA Interoperability", PKIforum white paper.

(Turnbull, 2000) Jim Turnbull, "Cross-Certification and PKI Policy Networking", Entrust Securing Digital Identities&Information

(Wilson, 2001) Stephen Wilson, "Leveraging External Accreditation to Achieve PKI Cross-Recognition", PricewaterhouseCoopers beTRUSTed

(2005) TÜBİTAK UEKAE KSM web sitesi http://www.kamusm.gov.tr

Özgür Deniz Erzincan, 15/07/2004 Telekom Dünyası, E-imza ve E-Türkiye Ankara

TK E-imza Ulusal Koordinasyon Kurulu Altyapı Çalışma Grubu İlerleme Raporu