

# **TÜRKİYE'DE ELEKTRONİK İMZA UYGULAMASI**

**Mesut ORTA**  
**Hakim**  
**Adalet Bakanlığı**  
**Bilgi İşlem Dairesi Başkanlığı**  
**Başkan Yardımcısı**

## İÇİNDEKİLER

KISALTMALAR .....	2
TABLO VE ŞEKİLLERİN LİSTESİ .....	2
<b>GİRİŞ</b> .....	<b>3</b>
<b>1. ELEKTRONİK İMZA</b> .....	<b>5</b>
<b>2. TÜRKİYE'DE E-İMZANIN HUKUKİ ALTYAPISI</b> .....	<b>5</b>
<b>3. ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILAR</b> .....	<b>6</b>
3.1. Başbakanlık Genelgesi İle Öngörülen Sertifikasyon Modeli .....	6
3.2. Telekomünikasyon Kurumu .....	9
3.3. Kamu Sertifikasyon Merkezi: UEKAE .....	9
3.4. ESHS'nin Kurulum Süreci .....	10
3.5. ESHS'nin Yükümlülükleri ve Hukuki Sorumluluğu .....	11
3.6. ESHS'nin Denetimi .....	12
<b>4. ELEKTRONİK SERTİFİKALAR</b> .....	<b>12</b>
4.1. Nitelikli Elektronik Sertifikalar .....	13
4.2. Sertifikaların Oluşturulması Yayımlanması .....	14
4.3. Sertifikaların Yenilenmesi ve İptali .....	15
4.4. Yabancı Elektronik Sertifikalar .....	15
4.5. Bilgilerin Korunması .....	16
4.6. Pazar ve Fiyat Oluşumu .....	16
<b>5. KABUL EDİLEN STANDARLAR</b> .....	<b>16</b>
<b>6. ALTYAPI</b> .....	<b>17</b>
6.1. İletişim Altyapısı .....	18
6.2. Bilgisayar Sahipliği .....	18
6.3. İnternet Kullanımı .....	19
<b>7. TANITIM VE BİLİNÇLENDİRME ÇALIŞMALARI</b> .....	<b>21</b>
<b>8. SORUNLAR VE ÇÖZÜM YOLLARI</b> .....	<b>22</b>
8.1. Yaygınlaştırma Problemi .....	22
8.2. Sertifikaların Güvenilirliği .....	23
8.3. Sonuç ve Değerlendirme .....	23
<b>KAYNAKÇA</b> .....	<b>24</b>
<b>DİĞER KAYNAKLAR</b> .....	<b>24</b>

## KISALTMALAR

A.g.e	: Adı geçen eser
A.g.m	: Adı geçen makale
AAA	: Açık Anahtar Altyapısı
EAL	: (Evaluation Assurance Level): Değerlendirme Garanti Düzeyi
EİK	: Elektronik İmza Kanunu
ESHS	: Elektronik Sertifika Hizmet Sağlayıcı
Md.	: Madde
PIN	: Personal Identification Number, veri erişim kodu
TK	: Telekomünikasyon Kurumu
UEKAE	: Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü
Yön	: Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik

## TABLO VE ŞEKİLLER LİSTESİ

Şekil	: Başbakanlık Genelgesi İle Kabul Edilen Altyapı Modeli .....	8
Tablo-1	: Dünyadan Türkiye'nin Görünümü .....	18
Tablo-2	: Gelir Dağılımı ve Bilgisayar Sahipliği .....	19
Tablo-3	: İnternet Kullanım Sıralaması .....	20
Tablo-4	: 100 Kişi Başına Düşen İnternet Kullanıcı Sayısı .....	20
Tablo-5	: ESHS ve Nitelikli Elektronik Sertifika Sayısı .....	21

## GİRİŞ

İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işaretir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır<sup>1</sup>.

İmza, genel olarak, bir belgenin doğruluğunu gösterme niyetiyle yapılan her türlü işaret olarak tanımlanabilir. İmza çok eski çağlardan beri değişik şekillerde kullanılmıştır. Örneğin Roma Hukukunda, bir sözleşmenin oluşturulabilmesi için, sözleşme yapan kişilerin mühür yüzüklerini balmumuna basarak metni mühürlemeleri gerekiyordu. Orta çağ boyunca Avrupa'da, belgeler, topraktan yapılmış mühürlerle mühürlenerek doğrulukları/güvenilirlikleri ispat edilmiştir. Daha sonraları, taraflar, el yazısı ile atılmış imzaları, sözleşmenin geçerliliğini ispat vasıtası olarak kullanmaya başlamışlardır<sup>2</sup>.

Borçlar Kanunu'nun 14'üncü maddesine göre imza, üzerine borç alan kimsenin el yazısıyla olmak zorundadır. İmza, kural olarak metnin altına atılmalıdır. Çıktılar, ilâveler varsa, bunlar da imzalanmalıdır. Aksi halde bunlar geçerli olmayacaktır.

2525 Sayılı Soyadı Kanunu'nun 2. maddesine göre imza ad ve soyad yazılmak

suretiyle atılır. Ancak, uygulamada farklı şekiller veya ismin ve soyismin ilk harfleri kullanılarak imza atılmaktadır. Kağıt üzerine atılan imza, uygulamada elektronik imza karşısında "ıslak imza" olarak nitelendirilmektedir.

İnternet kullanımı günümüzde çok yaygınlaşmış, günlük yaşamın ayrılmaz bir parçası haline gelmiştir. Sağlıktan adalete, kütüphanelerden alışveriş merkezlerine, bankacılık işlemlerine kadar pek çok bilgiyi ve hizmeti içinde barındıran internet, kullanıldıkça bir takım gereksinimler ortaya çıkmaktadır. İnternet üzerinde yapılan işlemlerde, özellikle elektronik ticaret uygulamalarında güvenlik ve kimlik tespiti, en çok ihtiyaç duyulan şeylerin başında gelmektedir. Öyle ki en kolay cinsiyet değiştirme internet üzerinde yapılmaktadır. Zaman içinde elektronik ortamda kimlik tespitinin güvenli bir şekilde tespitini sağlamak, diğer taraftan el yazısı ile imza yerine geçebilecek kadar güvenilir bir mekanizma kullanarak belgenin değiştirilmediğinin garanti edilmesi (bütünlük kontrolü) arayışlarına gidilmiştir. Böylece internet üzerinden yollanan bilgilerin güvenilirliğinin sağlanması, bilgilerin, güvenli ve değişmeden aynı zamanda hukuki koruma sağlayıcı nitelik kazanarak yerine ulaşması gibi amaçlarla teknik çalışmalara başlanılmıştır.

Elektronik imza altyapısı, bize, kimlik tespiti, bütünlük kontrolü ve inkâr edi-

<sup>1</sup> Reed, Chris, 'What is a Signature?', The Journal of Information, Law and Technology (JILT).2003/3, <http://elj.warwick.ac.uk/jilt/00-3/reed.html/>

<sup>2</sup> Lupton W. Everett, The Digital Signature: Your Identity by the Numbers, 6 RICH. J.L. & TECH. 10 (Fall 1999) <http://www.richmond.edu/jolt/v6i2/note2.html>

lemezlik gibi ıslak imza ile sağlanan fonksiyonların elektronik ortamda temin edilmesi için geliştirilen bir yöntemdir. Elektronik imzanın yakın bir zamanda günlük yaşamımıza gireceği ve yaşamın ayrılmaz bir parçası olacağı konusunda yalnız uzmanlar değil; pekçok kişi görüş birliği içindedir. Çünkü, güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün değildir. Bu gereksinim, yalnızca şirketler, kurum veya kuruluşlar için değil, aksine elektronik ortamda hukuken bağlayıcı işlemler yapmak isteyen herkes bakımından söz konusudur.

Ülkemizde elektronik imzanın kullanımı için gerekli yasal çalışmalar, ilk kez 29 Haziran 2001 tarihinde Hazine Dış Ticaret Müsteşarlığı koordinasyonunda oluşturulan Hukuk Alt Çalışma Grubu tarafından başlatılmıştır<sup>3</sup>. Adalet Bakanlığı, 14 Ocak 2002 tarihli yazısı yeni bir çalışma komisyonu kurarak kısa sürede "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" taslağını hazırlamış, söz konusu tasarı taslağı, 10 Eylül 2002 tarihli yazı ile kurumların görüşüne sunulmuş ve 19 Şubat 2003 tarihinde Başbakanlığa gönderilmiştir.

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmî Gazete'de yayımlanmıştır. İkincil düzen-

leme çalışmaları Telekomünikasyon Kurumuna verildiğinden Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır.

Elektronik imza kullanımında en önemli aktörlerin başında elektronik imza hizmet sağlayıcıları (ESHS) gelmektedir. Elektronik sertifika hizmet sağlayıcısı olmak için şimdiye kadar biri kamu, ikisi özel olmak üzere üç kurum faaliyete geçmek üzere Telekomünikasyon Kurumu'na bildirimde bulunmuş ve lisanslarını almıştır. Dolayısıyla elektronik imza kullanımı için gerekli elektronik sertifikalar bu kurumlardan sağlanabilmektedir. Diğer taraftan ilk elektronik imza, 18 Temmuz 2005 tarihinde kullanılmıştır<sup>4</sup>.

Bu çalışmada, Ülkemizde elektronik imzanın kullanımı konusunda gelinen aşamayı mevzuat ve teknik altyapı açılarından ele alacağız. Elektronik imzanın teknik altyapısı çalışma kapsamı dışında tutulmuştur. Ancak elektronik imza kullanımında asli unsur denilebilecek elektronik sertifika, elektronik sertifika sağlayıcıları, Türkiye'de öngörülen sertifikasyon modeli, Telekomünikasyon Kurumu, Kamu Sertifikasyon Merkezi, elektronik imzanın uygulamaya konması için aşılması gereken problemler ve çözüm yolları tartışılmıştır.

<sup>3</sup> Çamurdan, Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme, 2003, [http://dergi.tbd.org.tr/yazarlar/26052003/cigdem\\_camurdan.htm](http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm)

<sup>4</sup> www.tk.gov.tr (20.08.2005)

## 1. ELEKTRONİK İMZA

Elektronik imza bir üst kavramdır. Her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir<sup>5</sup>. Ancak "sayısal imza"<sup>6</sup> kavramı yerine kullanımına rastlamak da mümkündür<sup>7</sup>. Genel olarak elektronik imza kavramı, çok genel bir tanım olup; kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları da içermektedir.

Başka bir tanıma göre elektronik imza, ıslak imzanın fonksiyonlarını da kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır<sup>8</sup>.

13 Aralık 1999 tarihli Avrupa Birliği Direktifinde elektronik imza, doğrulama yöntemi olarak hizmet veren ve başka bir elektronik veriye eklenmiş veya mantıksal olarak ilişkilendirilmiş elektronik biçimindeki veri olarak tanımlanmıştır.

Elektronik imza ile sayısal imza aynı şey değildir. Sayısal imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır<sup>9</sup>. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

## 2. TÜRKİYE'DE E-İMZANIN HUKUKİ ALTYAPISI

Elektronik imzanın kullanımı konusunda halihazırda geçerli bulunan mevzuat şunlardır:

a) 5070 Sayılı Elektronik İmza Kanunu (23 Ocak 2004)

b) Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik (6 Ocak 2005 R.G. 25692)

c) Kamu Sertifikasyon Merkezi Oluşturulması Hakkında Genelge

d) Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26 Ağustos 2004 R.G. 25565)

e) Sertifika Mali Sorumluluk Sigortası Tarife Ve Talimatı (27.01.2005 R.G.25709)

f) Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005, R.G. 25709)

<sup>5</sup> Alkan, İnalöz, (Telekom Reg.), 2004, s.111.

<sup>6</sup> Sayısal imza yerine dijital imza kavramı da kullanılmaktadır.

<sup>7</sup> www.turkpoint.com/e-yasam/sayisal-imza.asp (01.12.2003)

<sup>8</sup> Arkan, Saadet., "Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım", Ankara 1999, s.151.

<sup>9</sup> Keser Berber, "İmzalıyorum O Halde Varım" s.503

g) *Elektronik İmza İle İlgili Süreçlere Ve Teknik Kriterlere İlişkin Tebliğ (06 Ocak 2005, ve R.G.25692)*

h) *Elektronik İmza İle İlgili Süreçlere Ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ.*

### 3. ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILAR

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 kişileridir (md. 8). Tanımda da anlaşılacağı üzere sertifika otoritesi olma konusunda herhangi bir sınırlama getirilmemiştir.

Elektronik ortamda, elektronik sertifikada yer alan kimlik bilgilerinin doğruluğunu, bu bilgilerin güncel şekilde kalmasını, sertifikaların yaşam döngülerinin sürdürülmesini sağlayan yegâne kurum ESHS'dir. Bu nedenle, ESHS, elektronik imza altyapısında çok önemli bir unsurdur. Sertifika hizmet sağlayıcıları açık anahtar altyapısının temel yapıtaşı olup; elektronik ödemeleri yapan ya da gönderen veya diğer temasları gerçekleştiren tarafların kimliklerini onaylayan noter benzeri kuruluşlardır<sup>10</sup>.

Elektronik imza sahibi olmak isteyen kişiler, elektronik sertifika hizmeti sağlayan kuruma kimlik bilgileriyle

başvuruda bulunur<sup>11</sup>. Bu başvuruya göre, kanunda belirtilen unsurların yer aldığı elektronik sertifika düzenlenerek kurumun özel anahtarı ile imzalanır<sup>12</sup>. Oluşturulan elektronik sertifika, kişinin bizzat kendisine teslim edilir.

Elektronik sertifika sağlayıcıları Telekomünikasyon Kurumu tarafından yetkilendirilmektedir. Kamu kurum ve kuruluşlarının elektronik sertifika ihtiyacı, 2004/21 sayılı Başbakanlık Genelgesi gereği Kamu Sertifikasyon Merkezi tarafından karşılanacaktır.

#### 3.1. Başbakanlık Genelgesi İle Öngörülen Sertifikasyon Modeli

5070 sayılı Elektronik İmza Kanunu'na göre isteyen herkes, şartları taşıyorsa ESHS olabilmektedir. Bu konuda herhangi bir sınırlandırma yapılmamıştır. Aksine kamu kurum ve kuruluşlarına sertifika sağlayıcı olma yolu açılmış, Kanunun 21'inci maddesi ile kamu kurum ve kuruluşlarına uygulanmayacak hükümler getirilmiştir. Anılan maddeye göre Kanunun 8'inci maddesinin dört ve beşinci fıkraları ile 15 ve 19'uncu maddelerinin elektronik sertifika hizmeti sağlayan kamu kurum ve kuruluşları hakkında uygulanmayacağı hüküm altına alınmıştır. Söz konusu hükümlere göre sertifika hizmeti sağlayan kamu kurum ve kuruluşları denetimden muaf olacak, Kurum tarafından belirlenen ücret üst ve alt sınırlarına uymak zorunda

<sup>10</sup> İnalöz, Ayşe, a.g.e, s.36.

<sup>11</sup> Açık anahtar elektronik sertifika hizmet sağlayıcılara ait mekânlarda da gerçekleştirilebilir.

<sup>12</sup> Topaloğlu, 2001, s.123; Altınışık, 2003, s.85; Keser Berber, (Dijital), 2004, s.5.

olmayacak, kendilerine idarî para cezası verilemeyecek ve faaliyetine son vermek mümkün olmayacaktır.

Telekomünikasyon Kurumu tarafından, elektronik imzaya ilişkin yapının oluşturulmasında ve denetiminde etkin rol oynayabilmek için piyasanın sağlıklı kurulması ve işleyişinin temin edilmesi gibi amaçlarla kamunun koordinasyonuna ilişkin olarak kamuda elektronik imza altyapısı kurmaya yönelik faaliyetlerin tek elden koordine edilmesi önerisi hazırlanarak E-Dönüşüm Türkiye İcra Kurulu'na sunulmuş, öneri, bazı bölümleri dışında 10 Haziran 2004 tarihinde yapılan E-Dönüşüm Türkiye VI. İcra Kurulu Toplantısında benimsenmiştir. E-Dönüşüm İcra Kurulu Kararı doğrultusunda 2004/21 sayılı Başbakanlık Genelgesi hazırlanmış, 06.09.2004 tarih ve 25575 sayılı Resmî Gazete'de yayımlanmıştır.

Başbakanlık Genelgesi ile Kamu Sertifikasyon Merkezi oluşturulmasında Telekomünikasyon Kurumu tarafından şu gerekçeler ileri sürülmüştür<sup>13</sup>.

- *Elektronik İmza Kanununun 21'inci maddesi ile kamu kurum ve kuruluşlarının Telekomünikasyon Kurumunun belirleyeceği ücret alt ve üst sınırlarına uyma yükümlülüğünden muaf tutulmasının sonucunda kamu yatırımlarının özel sektörü dışlama etkisi yaratacağı,*
- *Kamu kurum ve kuruluşlarının elektronik ortama geçişte kendi problemlerini çözmek üzere özel*

*çözüm arama yoluna gitmeleri ve bu çalışmaların kamu kuruluşları arasında koordinasyondan yoksun şekilde yürütülmesinin Türkiye için büyük problemleri beraberinde getireceği,*

- *Bağımsız ürünler seçilmesi halinde kurumlararası iletişimde uyum sorunuyla karşılaşılacağı,*
- *Kamu kurum ve kuruluşlarının bu işleri yapabilmek için mükerrer yatırımlara giderek gereksiz işgücü ve kaynak sarfiyatı yapmış olacağı.*

Başbakanlık Genelgesi ile bütün kamu kurum ve kuruluşlarının, kurumsal 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 kurulması öngörülmüştür. Söz konusu yapının gözden geçirilmesi ve uygunluğunun izlenmesi görev ve sorumluluğu Telekomünikasyon Kurumu'na verilmiştir.

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. Böylelikle kurumsal sertifikaların tek merkezden sağlanması, kamu sertifikasyon yapısının kurulması sonucu bütün kamunun

<sup>13</sup> 22.03.2005 Tarihinde Telekomünikasyon Kurumunda Yapılan Elektronik İmza Bilgilendirme Toplantısı, www.tk.gov.tr

güveneceği bir Kök ESHS'nin kurulması öngörülmüştür.

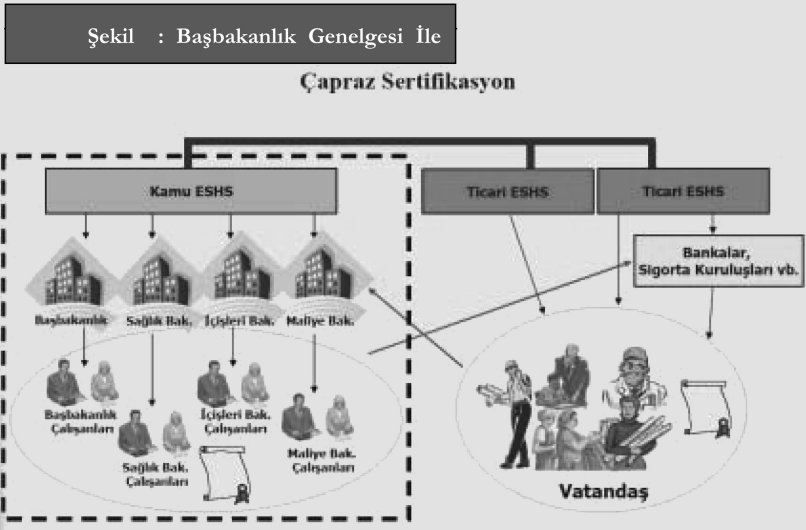
Tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifika yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulması ve sertifika yaşam çevriminin yönetilmesini sağlayacak kamu sertifikasyon yapısının kurulması ve işletilmesi görev ve sorumluluğu Türkiye Bilimsel ve Teknik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü'ne (UEKAE) verilmiştir.

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 kurula- cak kök sertifika hizmet sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet Sağlayıcısı sistemlerini kendi bünyele-

rinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları kurumsal sertifikalarını, Kamu Sertifikasyon Merkezinden temin edeceklerdir.

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.

Yukarıda belirtilen istisnalar dışındaki tüm kamu kurum ve kuruluşları, sertifika ihtiyaçlarını karşılamak amacıyla sertifika hizmet sağlayıcısı olmak üzere kendi bünyelerinde hiçbir surette yeni yatırım yapmayacaklar, bu konuda başlatılmış ve sürdürülmekte olan ihale çalışmaları ile henüz sözleşmeye bağlanmamış olan tüm ihaleler derhal iptal edilecektir. Böylece bütün ihalelerin iptal edilmesi, halihazırda kullanılan sistemlerin en kısa sürede bu yapıya uygun hale getirilmesi öngörülmüştür.





Sözleşmeye bağlanmış olanlardan, tek taraflı fesih hakkı bulunan sözleşmeler derhal feshedilecek, hâlihazırda kullanılmakta olan sistemler ise Telekomünikasyon Kurumunun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

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.

Başbakanlık genelgesi ile ortaya konulan sertifikasyon alt yapısı Şekilde gösterilmiştir. Buna göre, Kamu Sertifika Merkezi, kamu kurum ve kuruluşlarının elektronik sertifika ihtiyacını karşılayacak, kamu çalışanları dışındaki kişilere sertifika veremeyecektir. Kamu çalışanları, kurumsal sertifikalarını kamu dışı bireysel işlemlerinde de kullanabilecektir. İstenilirse ticari ESHS kök sertifikasını Kamu Sertifika Merkezinden alabilecektir.

### **3.2. Telekomünikasyon Kurumu**

ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuathükümlerine uygunluğunun incelenmesi, muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan bütün çalışmalar Telekomünikasyon Kurumu'na verilmiştir.

Telekomünikasyon Kurumu, ikincil mevzuat çalışmalarına başlamış ve öngörülen süreden önce Yönetmeliği hazırlamıştır<sup>14</sup>. Yapılan düzenlemeler çerçevesinde sertifika hizmet sağlayıcılarının yetkilendirilmesi ve denetlenmesi Kurum tarafından yerine getirilecektir.

Kanun, sertifika otoritelerinin yetkilendirilmesi ve denetlenmesi görevini Telekomünikasyon Kurumu'na vermiştir (EİK. md.15). Sertifika otoriteleri, Kurum'a yapacakları bildirimden başlamak üzere iki ay sonra faaliyete başlayabilirler (EİK. md.8). Bu düzenleme 99/93/EC sayılı AB Direktifi ile paralellik sağlamaktadır.

### **3.3. Kamu Sertifikasyon Merkezi: UEKAE**

Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri ESHS olabilirler.

Ancak, kamu kurum ve kuruluşlarının ESHS olmaları 06.09.2004 Tarihli Başbakanlık Genelgesi ile sınırlandırılmıştır.

Kamu Sertifikasyon Merkezi Oluşturulması Hakkında 2004/21 Sayılı Genelge'de, Elektronik İmza Kanunu ve yapılan ikincil düzenlemeler, kamu kurum ve kuruluşlarının kendi aralarında yapacakları iletişimin yanı sıra, vatandaşlar ve iş âlemi ile arasındaki iletişimin niteliğini, güvenilirliğini, etkinliğini ve hızını da büyük oranda ve olumlu yönde etkileyeceği belirtilmektedir.

<sup>14</sup> Telekom Dünyası, Aralık 2004, s.56

Söz konusu Başbakanlık Genelgesinde, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaya çalıştıklarının gözlemlendiği, bu münferit çalışmaların, bir yandan sistemin kendi işleyişi içerisinde karmaşaya yol açabileceği, diğer yandan da mükerrerliklere ve dolayısıyla emek ve kaynak israfına neden olacağı tespiti yapılmıştır.

Elektronik imza uygulamaları kapsamında; kamu kurum ve kuruluşlarının elektronik ortamlarda yürütecekleri iş ve işlemlerde uyumlu, birlikte işler ve güvenilir bir yapıda çalışmasını sağlamak amacıyla, 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 kararlaştırılmış, bütün kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının karşılanması amacıyla Kamu Sertifika Otoritesi kurulmuştur.

Kamu çalışanları, kurumsal sertifikalarını kamu dışı bireysel işlemlerinde de kullanabilecektir. Kamu Sertifika Dileyen gerçek ve tüzel kişilerin kuracakları Sertifika Hizmet Sağlayıcılarına da kök sertifika hizmeti verebilecektir

Kamu Sertifikasyon Yapısının kurulması ve işletilmesi görev ve sorumluluğu Türkiye Bilimsel ve Teknik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Elektronik ve Kriptoloji Araştırma Ensti-

tüsü Müdürlüğü'ne (UEKAE) verilmiştir. Yapının işleyiş ve denetim sorumluluğu Telekomünikasyon Kurumuna verilmiştir.

Elektronik sertifika hizmet sağlayıcısı, Elektronik İmza Kanunu veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı, kusursuzluğunu ispat ederse tazminat ödemek zorunda değildir (md. 13/2).

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.

### 3.4. ESHS'nın Kurulum Süreci

Elektronik Sertifika Hizmet Sağlayıcısı olmak için, kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini içeren dilekçeyi ve Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik Ek-1'inde yer alan bilgi ve belgeleri eksiksiz olarak Kuruma ibraz etmek suretiyle bildirimde bulunurlar.

Kurum, bu başvuru üzerine derhal yapılan bildirimini inceler ve iki ay içinde sonuçlandırır (Yön. md. 7/I). Kurum tarafından herhangi bir eksiklik tespit edilmezse elektronik sertifika hizmet sağlayıcı faaliyetine başlayabilir. Eksiklik tespit olunursa eksikliklerin tamamlanması için ESHS'na 1 ayı geçmemek üzere süre verilir. Bu zaman zarfında faaliyete başlanamaz.

Eksiklikler süresinde giderildiğinde, buna ilişkin bilgi ve belgeler Kuruma sunulur. Eksikliklerin giderilmesi, bildirimden başlayarak iki ayın dolmasından önce ise elektronik hizmet sağlayıcı yine de faaliyete başlayamaz. İki aylık süre Kanunda "Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer" denilerek emredici bir hüküm olarak düzenlenmiştir.

Eksiklikler, verilen bu bir aylık sürede giderilmezse Kurum ESHS'nın faaliyetine son verir (EİK. md. 8/III). Bu karar, ilgili ESHS'na 7201 sayılı Tebligat Kanunu'na göre tebliğ edilir. Kurumun faaliyete son verme kararına karşı tebliğden başlayarak en geç 7 gün içerisinde yetkili idare mahkemesine itiraz edebilir. İtiraz, Kurum tarafından verilen faaliyete son verme kararının yerine getirilmesini durdurmaz. İtiraz üzerine verilen kararlara karşı ilgili Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir (EİK. md. 19/II). ESHS'nın faaliyetlerinin devamı sırasında bildirimde belirttiği hususları kaybetmeleri hâlinde de kapatmaya ilişkin hükümler uygulanır (EİK. md. 8/IV).

ESHS, faaliyete geçtikten sonra, bildirimde belirttiği hususlarda herhangi bir değişiklik meydana gelmesi halinde, söz konusu değişiklikleri yedi gün içinde Kuruma bildirmesi gerekmektedir (Yön. md.8).

ESHS olmak herhangi bir izne tâbi değildir. Kuruma yapılacak bildirimden iki ay sonra faaliyete başlanabilir. Avrupa Birliği Direktifi md. 3/1'e göre hizmet sağlayıcılarının kurulması herhangi bir izne bağlanamaz hükmüyle paralel bir düzenleme yapılmıştır.

### **3.5. ESHS'nın Yükümlülükleri ve Hukuki Sorumluluğu**

ESHS'nın yükümlülükleri Elektronik İmza Kanununda maddeler halinde sayılmıştır.

Elektronik sertifika hizmet sağlayıcısı, imza oluşturma verisinin korunmasından ve bununla bağlantılı olarak, kötüye kullanılmasından, kaybindan, şifrenin başkalarına açıklanmasından, değiştirilmesinden ve yetkisiz kullanımından asla sorumlu değildir.

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 istih-

dam 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. Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır (EİK. md. 13).

### 3.6. ESHS'nin Denetimi

Avrupa Birliğinin 3/3 maddesine göre, "her üye devlet, ülkelerinde kurulmuş kamuya nitelikli sertifika veren sertifikasyon hizmeti sunucularını denetlemek amacıyla uygun bir sistem kurulmasını temin edecektir." hükmü Elektronik İmza Kanununun 15'inci maddesinde karşılanmıştır.

Denetim işlemini Telekomünikasyon Kurumu yerine getirir. Denetimini gerek gördüğü zamanlarda yapabileceği gibi şikâyet üzerine de yapabilir. Ancak yönetmeliğe göre denetimin en az iki yılda bir yapılması gerekmektedir (Yön. md. 22).

Denetim görevlileri denetimleri sırasında gerekli gördükleri her türlü defteri, belgeyi ve kayıtları istemeye, incelemeye ve bunların asıl ve örneklerini alma yetkisine sahiptir. Bunun yanı sıra denetim görevlileri, ESHS'na ait binaları ve eklentilerine girebilir, inceleme yapabilir, yazılı veya sözlü bilgi isteyebilir, her türlü işlem ve hesapları denetleyebilirler. ESHS, gizlilik ve sır saklama gibi gerekçeleriyle süre- rek denetim yükümlülüklerinden imtina

edemezler. ESHS denetim elemanlarınca talep edilen bilgi ve belgeleri vermezse yirmi bin YTL idarî para cezasına çarptırılacaktır (EİK. md. 18/e).

Bütün bu işlemlerin yapılması sırasında denetim görevlileri gerekli özeni göstermek durumundadırlar. Aynı zamanda tarafsız davranmaları, dürüstlük ve tarafsızlığı etkileyebilecek herhangi bir müdahaleye imkân vermemekle yükümlüdürler (Yön. md. 23).

Denetim sonunda hazırlanan denetim raporu en geç otuz gün içinde Telekomünikasyon Kurulu'na sunulur. Denetim sırasında, ESHS'nin faaliyetini olumsuz yönde etkileyebilecek derecede önem arz eden hususların tespit edilmesi halinde denetim faaliyetinin sonuçlanmasını beklemeksizin söz konusu hususları Telekomünikasyon Kuruluna sunar. Sertifika sağlayıcısının faaliyetine tesir edecek derecede olumsuz durumlar, bu sağlayıcıdan alınmış bütün sertifika sahiplerini, dolayısıyla kamuyu ilgilendirmektedir. Bu nedenle hazırlanan rapor Kurul tarafından öncelikli olarak gündeme alınır; Kurul, raporları değerlendirerek ihlal edilen herhangi bir durum varsa mevzuatın öngördüğü yaptırım ve cezaların uygulanmasına kararını verir (Yön. md.28).

## 4. ELEKTRONİK SERTİFİKALAR

Elektronik ortamda ihtiyaç duyulan güven sorunu elektronik sertifikalarla çözüme kavuşturulmaya çalışılmıştır. Buna göre sertifika sağlayıcılar sertifikadaki kişinin gerçekten o şahıs olup olmadığını tescil ederler. Yani açık

anahtar ve kimlik bilgilerini sertifikaya yerleştirip kendi özel anahtarlarını kullanarak tasdik ederler.

Elektronik sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarının elektronik ortamdaki karşılığıdır denilebilir. Elektronik sertifikalar sertifika otoriteleri tarafından düzenlenir<sup>15</sup>. Elektronik sertifika, kullanıcı adıyla onun açık anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik dokümandır<sup>16</sup>. Diğer bir deyişle elektronik sertifika imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder<sup>17</sup>. Elektronik sertifika, kişilerin veya kuruluşların bilgilerinin elektronik ortamda güvenli bir şekilde iletilmesini sağlamaktadır.

Elektronik sertifika imza sahibinin imza doğrulama verisini yani açık anahtarını ve kimlik bilgilerini birbirine bağlayan elektronik kayıt olarak da tanımlanabilir.

Elektronik sertifikalar sertifika otoriteleri tarafından hazırlanır. Bir elektronik sertifika almak için, bir sertifika otoritesinin sayfasını ziyaret edip sertifika isteğinde bulunmak gerekir. Bizden gerekli kimlik belirleyici bilgileri sunmamız beklenir.

Kök sertifika, sertifika hizmet sağlayıcısının kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyadır<sup>18</sup>. Kök kimliği

diğer sertifikalardan ayıran tek özellik, üzerinde kendi imzasını taşıyor olmasıdır. Kök sertifika, elektronik sertifika hizmet sağlayıcısının sertifikasıdır. Kullanıcılar Internet üzerinden kök sertifikayı bilgisayarlarına yüklerlerken aynı zamanda bu sertifika sağlayıcısının güvenli olduğunu kabul etmiş sayılırlar. Sertifika ile birlikte gelen açık anahtar, sertifika kurumunun kimliğini doğrulamakta kullanılırlar. Zira elektronik sertifikalar sertifika otoritelerinin özel anahtarları ile imzalanırlar. Doğrulama gerçekleştirilerek sertifikanın o hizmet sağlayıcısı tarafından onaylanmış, gerçek bir sertifika olduğu teyit edilmiş olur.

#### 4.1. Nitelikli Elektronik Sertifikalar

ESHS tarafından oluşturulacak elektronik sertifikada öncelikle "nitelikli elektronik sertifika" olduğuna dair bir ibare, elektronik sertifika hizmet sağlayıcının kimlik bilgileri ve kurulduğu ülke adının bulunması gerekir. ESHS gerçek kişi olabileceği gibi tüzel kişi de olabilir.

Kanun'un 9'uncu maddesinde sayılan unsurlar nitelikli elektronik sertifikada bulunması zorunlu unsurlardır. Bu unsurlardan birinin olmaması halinde sertifika "nitelikli elektronik sertifika" olarak kabul edilemez. Kanun, elektronik imza için nitelikli elektronik sertifika aramaktadır (EİK, md. 4-c).

<sup>15</sup> Erzincan, Özgür Deniz, "Sayısal İmza Hayatımıza Nasıl Girecek?", BİMY'11, Antalya, 2003,s.14.

<sup>16</sup> Ergun, Ömer, "Dijital İmza – İnternet Hukuku", <http://www.law.ankara.edu.tr/yazi.php?yad=856> (03.02.2005)

<sup>17</sup> İnalöz, Ayşe, 2003, s.156.

<sup>18</sup> Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, 10–12 Mayıs 2002, Ankara, [http://www.taek.gov.tr/taek/bet/pdf/hukuk\\_cg\\_raporu.pdf](http://www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf)

#### 4.2. Sertifikaların Oluşturulması Yayımlanması

Elektronik sertifika talep üzerine oluşturulur. ESHS, nitelikli elektronik sertifika başvurusundan sonra sertifikayı oluşturur ve sertifika sahibine teslim eder. Sertifikanın geçerlilik süresi sözleşmeyle belirlenir (Yön. md. 10). Sertifika, teslim edilmeden önce sertifika talep edene elektronik imza kullanımına ilişkin aydınlatma yükümlülüğünün yerine getirilmesi (EİK. md. 10 e-f) ve sigortalandıktan sonra teslim edilmesi gerekmektedir (EİK. md. 13/son).

Başvuru şahsi başvuru olabileceği gibi kurumsal başvuru da olabilir. Yönetmelikte kurumsal başvuru, bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusudur denilmektedir (Yön. md. 4).

ESHS, sertifikanın tanziminden sonra bir sertifikanın içerdiği bilgilerin doğruluğunu kontrol etmek zorunda değildir. Ancak sertifika çalınmış veya kötüye kullanılmış ise gereğini yapmak durumundadır. ESHS'nin Kanunda belirtilen sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir şekilde tespit etmesi işlevi, sertifikanın tesliminden öncedir. Tespit işlemini belgelere göre yapamıyorsa sertifika oluşturulması gerekmektedir. Sertifikanın oluşturulup tesliminden sonra meydana gelecek değişiklikler ESHS'nin elektronik sertifikadaki bilgiler yönünden kendisini sorumluluk altına sokmaz. Ancak sertifika sahibinin bilgilerinde meydana gelen değişiklikleri biliyorsa veya bilmesi gerekiyorsa sertifikaya güvenerek işlem

yapan üçüncü kişilere karşı sorumlu olacaktır (EİK. md. 13/2).

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür (EİK. md. 13/son). Bu amaçla Telekomünikasyon Kurumunca hazırlanan, "Sertifika Mali Sorumluluk Sigortası Yönetmeliği", 26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazete'de yayımlanmıştır. Söz konusu yönetmelikte sertifika mali sorumluluk sigortası, elektronik sertifika hizmet sağlayıcısının, Elektronik İmza Kanunundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigorta olarak tanımlanmıştır.

Elektronik sertifikalar üçüncü kişiler tarafından erişilebilir halde tutulmalıdır. Bunu sağlamak amacıyla ESHS sertifikaları yayımlamak durumundadır. Yönetmeliğin 11'inci maddesine göre ESHS, sertifika sahibinin onayını almak kaydıyla nitelikli elektronik sertifikayı kamuya açık bir dizinde yayımlamak ve dizin hizmetinin kesintisiz olarak verilmesini sağlamak zorundadır.

Nitelikli elektronik sertifikalar, geçerlilik süresinin sona ermesinden önce sertifikaya sahibinin veya sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda ESHS tarafından yenilenirler. ESHS, nitelikli elektronik sertifikayı, sertifika sahibine ait bilgilerin geçerliliğini doğrularak yeniler (Yön. md. 12). Sertifikada yer alan bilgilerin değişmesi halinde de yenilenmesi gerekir.

#### **4.3. Sertifikaların Yenilenmesi ve İptali**

Elektronik sertifika hizmet sağlayıcılarının elektronik sertifika sahibinin fiil ehliyetinin sınırlanması, iflâsı, gaipliği veya ölmesi hâlinde elektronik sertifikayı iptal etmesi yetki ve yükümlülüğü düzenlenmiş, böylelikle yapılacak hukukî işlemden iyi niyetli üçüncü kişilerin zarar görmemesi amaçlanmıştır.

Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez (EİK. md. 11/son). İptal işlemi geçmişe yürütülemeyeceği gibi, geçmiş bir tarihte iptal edilmesi de mümkün değildir. Zira sertifika kullanılmış veya sertifikaya güvenilerek işlem tesis edilmiş olabilir.

Yönetmeliğin 13'üncü maddesine göre 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 sağlamak durumundadır. ESHS nitelikli elektronik sertifika sahibini söz konusu durum hakkında bilgilendirmesi zorunludur. Kurumsal başvurularda başvuru sahibinin de bilgilendirilmesi öngörülmüştür.

#### **4.4. Yabancı Elektronik Sertifikalar**

Yabancı elektronik sertifikaların Türkiye'de geçerli olabilmesi için gerekli koşullar, Elektronik İmza Kanunu'nun 14'üncü maddesinde belirlenmiştir. Buna göre yabancı elektronik sertifikaların geçerlilikleri ve hukukî sonuç doğurabilmeleri, milletlerarası anlaş-

maların varlığına veya yerli bir elektronik sertifika hizmet sağlayıcısı tarafından garanti edilmesine bağlıdır. Söz konusu sertifikaların ait olduğu ülkede o ülkenin mevzuatına göre faaliyette bulunuyor olması da gereklidir. Bu suretle yabancı sertifikaya ait sorumluluklar yerli ESHS tarafından üstlenilmiş olmaktadır.

Her iki durumda da yabancı elektronik sertifikalar Türkiye'de geçerli nitelikli elektronik sertifika ile aynı hukuki statüye sahip olacaklardır. Burada gözden kaçırılmaması gereken önemli bir konu, Türkiye'deki elektronik sertifika hizmet sağlayıcı tarafından garanti edilen yabancı sertifikaların kendi ülkelerinde nitelikli olup olmadıklarına bakılmaksızın, 5070 Sayılı Kanunda tanımlanan nitelikli elektronik sertifikalar ile aynı hukuki etki ve sonuçlara sahip olacağı hususudur. Ancak bu durum yerinde bir düzenleme yapılarak Yönetmelik ile açıklığa kavuşturulmuş bulunmaktadır. Söz konusu yabancı elektronik sertifikanın, Kanunda ve Yönetmelikte yer alan nitelikli elektronik sertifikanın teknik şartlarını taşıması yerli bir ESHS tarafından kabul edilmesi için bir şart olarak ileri sürülmüştür.

Yapılan düzenleme ile hem ESHS'ları hem de sertifika kullanıcılarını koruyucu bir özellik taşımaktadır. Bu haliyle ileride doğacak zararların veya ihtilafların önceden öngörülerek tedbirinin alınması sevindirici bir konudur.

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik gereği yabancı elektronik sertifikaların hukuki sonuçları ve kabul edilmesine ilişkin şartlar milletlerarası

anlaşmalarla belirlenecektir (EİK. md. 14, Yön. md. 32/1).

Yabancı ESHS'na ait bilgiler Kurum'un internet sayfasında yayımlanacaktır. Kabul edilen yabancı elektronik sertifikaların kullanılması sonucunda doğacak her türlü zarardan sertifikaları kabul eden Türkiye'deki ESHS da sorumludur (Yön. md. 32/son).

Gerek Kanunla gerek Yönetmelikle yapılan düzenlemeler sonucu uluslararası sertifikaların kullanım imkânı sağlanmış olmaktadır. Aynı zamanda yapılan bu düzenleme, 30 Ocak 2001 tarihinde yayınlanan Birleşmiş Milletler UNCITRAL Elektronik İmza Yasa Model Taslağı'nın 12'inci maddesinde bahsedilen yabancı sertifikaların tanınmasına ilişkin düzenleme ile de paralellik arz etmektedir<sup>19</sup>.

#### 4.5. Bilgilerin Korunması

Elektronik sertifika sağlayıcı, elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler dışında hiçbir bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez.

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

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 (EİK.m.12).

#### 4.6. Pazar ve Fiyat Oluşumu

Elektronik sertifika hizmet sağlayıcılar yetkilendirmelerini yeni almış bulunmaktadır. Dolayısıyla piyasa fiyatının oluşumu beklenmektedir. Kurum ve kuruluşlar sertifika talebinde aceleci davranmayarak beklemeyi tercih etmektedirler.

Diğer taraftan güvenli imza oluşturma ve doğrulama araçlarının seçimi konusunda kafalarda bir takım şüpheler bulunmaktadır. Kamu Sertifikasyon Kurumu akıllı kart kullanımı konusunda bir takım çalışmalar yapmaktadır. Bilindiği üzere, akıllı kartlar ayrıca bir kart okuyucu gerektirmektedirler. Kamu Sertifika Merkezinin kamu kurum ve kuruluşlarına artıları ve eksileriyle bir takım önerilerde bulunması takdirle karşılanmaktadır.

#### 5. KABUL EDİLEN STANDARLAR

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ 6 Ocak 2005 tarih ve 25565 sayılı Resmi Gazete'de yayınlanmıştır.

Elektronik imza güvenliğinden bahsedildiğinde, ESHS güvenliği, algoritma güvenliği ve imza oluşturma/doğrulama araçlarının güvenliği sözkonusudur.

Elektronik İmza Kanunu'nun 8'inci maddesinde belirtildiği üzere ESHS; güvenli ürün ve sistemleri kullanmakla, hizmeti güvenilir bir biçimde yürütmekle ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almakla yükümlüdür. Bunun detayı tebliğde

<sup>19</sup> İnalöz, Ayşe, 2003, s.59.



açıklanmış olup ESHS, işleyişinin bütün aşamalarında;

- a) ETSI TS 101 456 ve
- b) CWA 14167-1

standartlarına uymakla yükümlüdür.

Bunun yanısıra ESHS, Sertifika İlkeleri (Sİ) ile Sertifika Uygulama Esasları'nı (SUE) IETF RFC 3647 standardına uygun olarak hazırlaması gerekmektedir.

Tebliğin 9'uncu maddesinde, ESHS'nin güvenlik kriterlerine ilişkin olarak uymak zorunda oldukları standartları gösterilmiştir. Bunlar:

- a) CWA 14167-1,
- b) ETSI TS 101 456 ve
- c) TS ISO/IEC 17799 veya ISO/IEC 17799 satandartlarıdır.

Tebliğin 10'uncu maddesinde ise ESHS, zaman damgası ve hizmetlerine ilişkin olarak;

- a) CWA 14167-1 ve
- b) ETSI TS 101 861,

standartlarına uyacakları hüküm altına alınmıştır. Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanmaları gerekmektedir.

Elektronik imzada kullanılan algoritma ve parametreler imza 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

c) *Özetleme algoritması (hash) olarak;*

- i. RIPEMD-160 veya
- ii. SHA-1, kullanılır.

## 6. ALTYAPI

Elektronik imzanın uygulama alanı bulabilmesi için altyapı çalışmalarının tamamlanmış olması gerekmektedir. Kastımız sadece fiziki altyapı, yani iletişim altyapısı ile bilgisayar kullanım oranı değil, aynı zamanda internet kullanımı, kolay ve ucuz erişim, elektronik ticaret kullanım oranı, kamu ve tüzel kişiliğe sahip kurumların hizmetlerini elektronik ortamdan sunması ve bunun talep görmesidir.

Altyapı ve internet kullanımı konusunda aşağıda verilen talodan<sup>20</sup> da anlaşılacağı üzere son yıllarda yapılan çalışmalar memnuniyet verici olsa da diğer gelişmiş ülkelerle karşılaştırıldığında helen arada uçurum olduğu söylenebilir.

<sup>20</sup> Tablo e-dönüşüm yol haritası, Dünya, Türkiye adlı kitaptan alınmıştır.

**Tablo-1: Dünyadan Türkiye'nin Görünümü**

	Değer	Kaynak	Yıl	Sıralama
Nüfus	73,197,200	internetworldstats.com	2003	
İnternet Kullanıcı Sayısı	2,500,000	nationmaster.com	2002	36/162
	4,900,000	internetworldstats.com	2003	
Kişisel Bilgisayar Sayısı	2,500,000	nationmaster.com	2000	
	2,700,000	Birleşmiş Milletler	2001	
İnternet Ana Bilgisayarı	1,100,000	nationmaster.com	2003	64/119
ISP Sayısı	50	nationmaster.com	2001	19/28
20 saat internet kullanımının ortalama maliyeti	11,20\$		2001	
e-Devlet Projesi Sayısı	200	Brown Üniversitesi	2003	
e-Devlet Olgunluk Düzeyi	56/190	Birleşmiş Milletler	2002	56/190
	83/196	Brown Üniversitesi	2001	83/196
	51/178	nationmaster.com	2003	51/178
e-Devlet Performansı	6/198	Brown Üniversitesi	2003	

## 6.1. İletişim Altyapısı

İnternet erişimin yaygın ve ucuz olması en büyük beklenti olarak görülmektedir. Bunun yanı sıra kapasite, kesintisizlik de aranmaktadır. İletişim altyapısında henüz Telekom tekelinin bazı alanlarda kalkmadığı, fiyatların ise istenen seviyelere gelmediği, dolayısıyla internet kullanımının istenilen düzeylere gelemediği söylenebilir.

Son zamanlarda yapılan kampanyalarla ADSL abone sayısının artırılması hedeflenmektedir. 2005 yılı sonunda ADSL abone sayısının 2,2 milyona ulaşması beklenilmektedir<sup>21</sup>. 2004 yılı sonunda 454.061 olan Türk Telekom

ADSL abone sayısı 9 Eylül 2005 günü 1.000.000'a ulaşmıştır<sup>22</sup>.

## 6.2. Bilgisayar Sahipliği

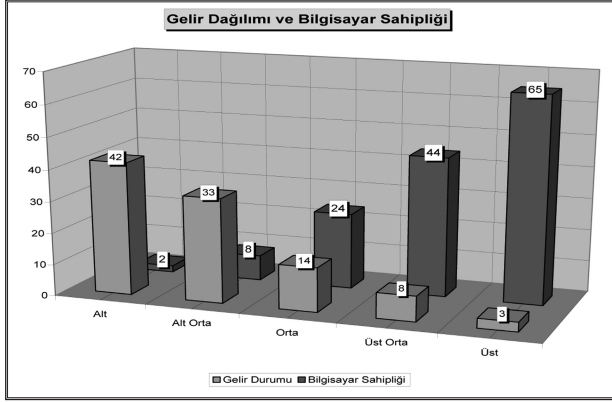
Elektronik imzanın yaygınlaşmasında bilgisayar sahipliği oranı büyük önem taşımaktadır. Gerek kamunun gerekse özel teşebbüsün sundukları hizmetleri bilgisayar ortamından arz etmeleri, talepte bulunacak vatandaşların da taleplerini internet ortamından yapabilmeleri gerekmektedir. Bunun için kamunun bilişim alanına öncelik vermesi, e-devlet çalışmalarını hızlandırması, yapılan çalışmalarını etkin bir şekilde denetlemesi, mükerrer yatırımlara izin vermemesi, kurumlararası entegrasyona gereken

<sup>21</sup> www.turkinternet.com (30.09.2005)

<sup>22</sup> www.ulastirma.gov.tr (25.09.2005)

**Tablo-2: Gelir Dağılımı ve Bilgisayar Sahipliği<sup>23</sup>**

Gruplar	Alt	Alt Orta	Orta	Üst Orta	Üst
Gelir Durumu (%)	42	33	14	8	3
Bilgisayar Sahipliği (%)	2	8	24	44	65



değerin verilmesi, bunlar için gerekli ödeneği ayırması büyük önem arz etmektedir.

Diğer taraftan kamunun internet üzerinden sunulan hizmetler için kolay erişim platformları oluşturması (kiosklar), alım gücünün düşük olduğu göz önünde bulundurularak bilgisayar sahipliği oranını arttırmak için gerekli desteğin sağlanması yerinde olacaktır.

Bilgisayar teknolojilerindeki hızlı gelişim ve değişim, bilgisayar okur-yazarlığının, bir kerede tamamlanabilecek bir eğitim aşaması olmadığını ve bunun yaşam boyu sürdürülmesi gerektiğini göstermektedir.

Aşağıda gelir dağılımı ve bilgisayar sahipliğine ilişkin tablo verilmiştir. Tabloya göre gelir dağılımında en alt seviyede bulunan büyük bir çoğunluğun çok az miktarda bilgisayar sahibi oldukları, toplam nüfusun yüzde 3'ünü oluşturan üst gelir seviyesine sahip kesimin toplam bilgisayar sahipliği oranının yarısından fazlasına sahip oldukları görülmektedir. Sonuç olarak gelir durumu arttıkça bilgisayar sahipliği oranı ortmaktadır.

### 6.3. İnternet Kullanımı

İnternet Türkiye'de ilk kez 1993 yılında kullanılmaya başlandı<sup>24</sup>. Türkiye'de 2000 yılı sonunda 2 milyon olduğu hesapla-

<sup>23</sup> Özçivelek, Rukiye, E-Devlet Kavramı Üzerine Bir Sorgulama, www.tubitak.gov.tr

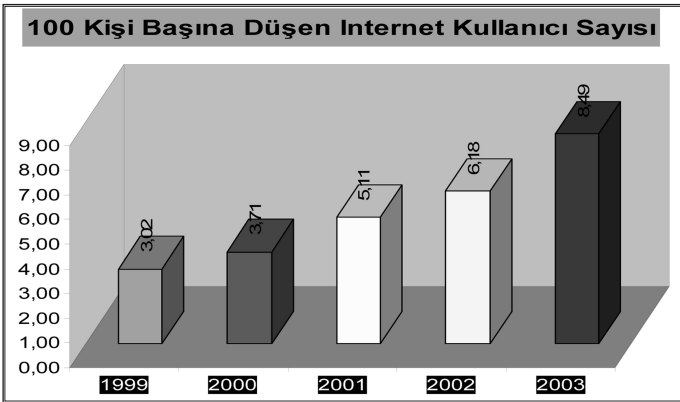
<sup>24</sup> <http://www.ivhp.net> (26.9.2005)

nan internet kullanıcısı sayısı, son 4,5 yılda yüzde 263,5 ile, yüzde 160 olan dünya ortalamasının hayli üzerinde artarak 7 milyon 270 bine ulaştı. Buna

rağmen Türkiye'de internet kullananların oranı, toplam nüfus dikkate alındığında, yüzde 13,9 olan dünya ortalamasının altında kalarak yüzde 9,9 oldu<sup>25</sup>. Aşağıda

Tablo-3: İnternet Kullanım Sıralaması		
Ülke	İnternet kullanıcısı (milyon kişi)	Nüfusa oranı (%)
1. ABD	202.9	68.5
2. Çin	103.0	7,9
3. Japonya	78.0	60.9
4. Almanya	47.1	57.0
5. Hindistan	39.2	3,6
6. İngiltere	35.8	59.8
7. Güney Kore	31.6	63.3
8. İtalya	28,6	48.8
...		
24. Türkiye	7,3	9,9

Tablo-4: 100 Kişi Başına Düşen İnternet Kullanıcı Sayısı					
Yıllar	1999	2000	2001	2002	2003
%	3,02	3,71	5,11	6,18	8,49



<sup>25</sup> "internetworldstats"ın araştırma şirketi ACNielsen'in yayımladığı verilere göredir.

tabloda da görüldüğü üzere, 7 milyon 270 bin internet kullanıcısı olduğu hesaplanan Türkiye, bu rakamlarla internet kullanımında dünya sıralamasında 24'üncü sırada yer almaktadır<sup>26</sup>.

Devlet İstatistik Enstitüsü (DİE) tarafından yayımlanan aşağıdaki tabloda ise, yıllara göre 100 kişi başına düşen internet kullanıcı sayısı görülmektedir<sup>27</sup>. Tablodan, 1999 yılından 2003 yılına gelindiğinde kullanıcı sayısının yaklaşık 3 kat arttığı anlaşılmaktadır.

## 7. TANITIM VE BİLİNÇLENDİRME ÇALIŞMALARI

Ülkemizde elektronik imza konusunda mevzuat çalışmaları tamamlanmış; uygulamaya geçmek için çalışmalar başlatılmıştır. Çalışmalarını tamamlamış bulunan diğer ülkelere bakıldığında elektronik imzanın istenilen düzeyde kullanımının sağlanamadığı görülmektedir. Bunun sebepleri ne olursa olsun yaygınlaştırmanın çok kolay olmadığı

söylenbilir. Aşağıdaki Tablo-3'ten de anlaşılacağı üzere ilk düzenlemesini 1997 yılında yapan Almanya'da toplam 23 adet akredite elektronik sertifika sağlayıcı ve 25 bin adet nitelikli elektronik sertifika bulunmaktadır. İtalya'da 1998 yılından bu yana 14 adet akredite elektronik sertifika sağlayıcı ve 1 milyon elektronik sertifika, 2000 yılında uygulamaya geçen Avusturya'da 2 akredite sertifika sağlayıcı ve 10 bin adet nitelikli elektronik sertifika, Estonya'da 1 akredite sertifika sağlayıcısı ve 200 bin nitelikli elektronik sertifikaya ulaşıldığı anlaşılmaktadır. Bu rakamlara bakarak elektronik sertifika talebinin nüfusa oranla çok düşük olduğu söylenebilir.

Ülkemizde aynı tablo ile karşılaşılması için gereken tedbirler bir an önce alınmalı, alt yapı oluşturulurken kullanıma özendirilecek unsurlar dikkate alınmalıdır. Öncelik kamu ve bankacılık sektörü olarak belirlenerek, bu alanlarda eğitim ve bilinçlendirme çalışmaları yapılmalıdır.

Tablo-5: ESHS ve Nitelikli Elektronik Sertifika Sayısı			
Ülkeler	Akredite Elektronik Sertifika Hizmet Sağlayıcı Sayısı	Nitelikli Elektronik Sertifika Sayısı	Uygulamaya Başlama Tarihi
Almanya	23	25.000	1997
Avusturya	2	10.000	2000
İtalya	14	1.000.000	1998
Estonya	1	200.000	2000

Kaynak: icri-Leuven, 2004

<sup>26</sup> www.milliyet.com.tr (26.9.2005)

<sup>27</sup> www.die.gov.tr (27.09.2005)

Bu konuda en büyük görev denetleme ve düzenleme görevi kendisine verilen Telekomünikasyon Kurumu'na düşmektedir. Elektronik sertifika sağlayıcıları Telekomünikasyon Kurumu'na bildirim ile elektronik sertifika hizmet sağlayıcısı olarak devreye gireceklerdir. Bu kuruluşlar, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan gerçek veya tüzel kişiler olacaktır. Hizmet sağlayıcıları, Telekomünikasyon Kurumu'na yapacağı bildirimde, hizmetin gerektirdiği nitelikte personel istihdam edeceğini, güvenli ürün ve sistemi kullanacağını, hizmeti güvenilir biçimde yürüteceğini ve sertifikaların taklit ve tahrifini önleyici her türlü önlemi alacağını güvencesi verecektir.

Elektronik imzanın yaygınlaşması için kamuda kullanımının sağlanması şart görünmektedir. 2004/21 sayılı genelge kamuda elektronik imza kullanımında ortaya çıkabilecek pek çok problemi çözmüş bulunmaktadır.

## **8. SORUNLAR VE ÇÖZÜM YOLLARI**

Ülkemizin elektronik imza mevzuatı açısından pek çok ülkeden ileri düzenlemelere sahip olduğu söylenebilir. Özellikle 2004/21 sayılı Başbakanlık Genelgesiyle ortaya konulan altyapı modeli, uygulamada çıkabilecek sorunları en aza indirmiş, mükerrer yatırımları önlemiş, sertifikasyon açısından kurum ve kuruluşların aynı çatı altında toplanması sağlanmıştır. Ancak, 5070 sayılı Elektronik İmza Kanunu'nda kamu kurum ve kuruluşlarının denetimden muaf tutulma-

ları, kapatılmamaları ve sertifikalar için belirlenecek ücret alt ve üst sınırlarına uymak zorunda olmamaları Genelge ile ortaya konulan altyapı modelini zorunlu kılmışsa da bunun Genelge ile yapılması yerinde değildir.

Ülkelerin elektronik imza konusunda işbirliği yaparak ortak düzenlemeler ya da uluslararası sözleşmeler yapmaları sistemin sağlıklı işleyişi açısından zorunlu görünmektedir. Zira, elektronik imza uygulamaları ülke sınırlarını aşan bir nitelik arz etmektedir.

Elektronik imzanın yaygınlaşmasında devlet öncü rol oynamalıdır. Elektronik İmza Kanununun hayata geçirilmesi ile birlikte devlet hizmetlerinde ve kurumların iş yapma yöntemlerinde büyük değişimlerin yaşanması kaçınılmaz hale gelecektir. Bu nedenle gelişmelerin zamanında farkına varılarak kamu kurum ve kuruluşları, iş süreçlerini gözden geçirmeli, e-devlet kurumu olmanın gereklerini yerine getirmelidirler.

### **8.1. Yaygınlaştırma Problemi**

Uygulamanın yaygınlaştırılması pek çok ülkede görüldüğü üzere kolay olmamaktadır. Bu nedenle, önce konuya ilişkin olarak, gerek kamu, gerekse özel sektörün bilgilendirilmesi gerekmektedir. Öte yandan, elektronik imza uygulamasının pilot seçilen bir kamu kurumunda uygulamaya konulması, değerlendirilmesi, sonuçlarına göre hareket edilmesi yerinde olacaktır. Bu konuda Adalet Bakanlığı tarafından yürütülen UYAP, pilot proje olarak seçilebilir.

Elektronik imza kullanımının önündeki engellerden birisi kullanım zorluğu ve teknolojinin karmaşıklığıdır. Standartlar henüz tam oturmamıştır. Diğer taraftan elektronik sertifika hizmet sağlayıcısı olma maliyetleri oldukça yüksek olup, sertifika pazarı gelişim sürecindedir.

Sertifika dağıtımı, iptal ve yenileme işlemlerinin güçlüğü, uygulama ve standart sorunları, kullanıcı ve işletme maliyetinin yüksek olması, e-imza sahibi olacak vatandaşların sistemin işleyişi hakkında bilgi sahibi olması gerekliliği gibi konuların sertifika yönetimini ve elektronik imzanın yaygınlaşmasını zorlaştıran unsurlar arasındadır<sup>28</sup>.

### 8.2. Sertifikaların Güvenilirliği

Elektronik sertifika hizmet sağlayıcılarının dağıttığı elektronik sertifikalarda yer alan bilgiler doğru kabul edilmektedir. Ancak bu konuda karşılaşılabilecek yanlış kimlik bilgileri sisteme olan güveni büyük ölçüde zedeleyecektir. Bu nedenle ESHS, sıkı bir şekilde denetlenmeli, gerekirse sorumlulukları yeniden gözden geçirilmelidir. Bu konuda denetleme ve düzenleme görevi Telekomünikasyon Kurumuna ait olduğundan Kurumun teknik bilgi düzeyi yüksek yeterince uzman personeli bulunmalıdır.

### 8.3. Sonuç ve Değerlendirme

Sonuç olarak, elektronik imzanın kullanılmaya başlaması ve yaygınlaşması, kuşkusuz kâğıt ve kalem ikilisinin orta-

dan kalkması sonucunu doğurmayacaktır. Elektronik imza kullanımı, elektronik ortamda güvenli iletişim ve işlemler için günümüzde vazgeçilmez yöntem olarak görülmekle birlikte isteyen herkes el yazısı ile de işlemlerini yapabileceklerdir. Bir başka deyişle fotoğrafa karşın nasıl günümüzde nasıl resim yapılmaya devam ediliyorsa, elektronik haberleşme ve sayısal imzanın yanı sıra kâğıt dokümanlar, el yazıları ve el yazısı ile atılan imza da var olmaya devam edecektir.

Bilişim yatırımlarına ağırlık verilmesi, bilişim alanında yeterli donanımına sahip insan kaynaklarının oluşturulması gerekiyor. Özellikle kamu kurum ve kuruluşlarında bilgisayar okuryazarlığının teşvik edilmesi gerekmektedir. Bilgisayar okuryazarlığının artırılması gerekir. Vatandaş ile iletişimin ve etkileşimin güçlendirilmesi gerekir.

Elektronik imzanın uygulamaya konmasında pilot birim ve pilot proje seçilmesi, uygulama sonuçlarına göre diğer kurumların harekete geçirilmesinde büyük yararlar bulunduğu kanaatindeyim.

Elektronik imza kullanımının yaygınlaştırılması amacıyla internet üzerinden yapılacak satışlar özendirilmeli, elektronik ortamdan yapılacak sözleşmeler yaşamımıza pek çok kolaylıklar getireceğinden internet üzerinden yapılacak işlemlere muafiyetler tanınmalıdır. Örneğin verginin elektronik ortamdan yatırılması halinde indirimi olması, elektronik

<sup>28</sup> Tüfekçi, Tolga, [http://www.bilten.metu.edu.tr/Web\\_2002\\_v1/common/yayinlar/Elektronik\\_imza\\_nicin\\_yayginlasamiyor-doc.pdf](http://www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/Elektronik_imza_nicin_yayginlasamiyor-doc.pdf), (21.06.2005)

ortamdan yapılacak başvurulara öncelik tanınması gibi. Devlet bu durumda daha az personel istihdam edeceği gibi personelinin performansını takip edebilecek, bina, ulaşım, yakıt gibi giderleri de azalacaktır. Diğer taraftan devlet, elektronik devlete geçmeyi kolaylaştırmak için işlemlerini elektronik ortamdan yapan personelini teşvik etmeli, gerekirse ödüllendirmelidir.

Türkiye’de elektronik imza konusunda yapılan yasal düzenlemeler yeterli olmakla birlikte uygulamaya geçiş konusunda bir planın olmayışı büyük bir eksikliklerdir. Elektronik imzanın kullanılması, kamudaki dönüşümün, yeniden yapılanmanın, verimliliği sağlamanın ve e-devlet olmanın bir fırsatı olarak görülüp iyi değerlendirilmelidir.

## KAYNAKÇA

ALKAN, Mustafa, İNALÖZ, Ayşe, (2004), “Telekomünikasyon Regülasyonları ve Elektronik İmzanın Elektronik Ticaret Üzerindeki Etkileri”, TBD 21. Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara

ALTINIŞIK, Ulvi, (2003), “Elektronik Sözleşmeler”, Ankara.

ARIKAN, Ayşe Saadet, (1999), “Dünyada ve Türkiye’de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım”, 1999, Ankara.

ARIFOĞLU, Ali, e-Dönüşüm Yol Haritası, Dünya, Türkiye, 2004

ÇAMURDAN, Çiğdem, “Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme”, [http://dergi.tbd.org.tr/yazarlar/26052003/cigdem\\_camurdan.htm](http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm) (13.11.2004).

ERGUN, Ömer, (2004), “Dijital İmza – İnternet Hukuku”, <http://www.law.ankara.edu.tr/ya-zi.php?yad=856> (03.02.2005)

ERZİNCAN, Özgür Deniz, (2003), “Sayısal İmza Hayatımıza Nasıl Girecek?”, BİMY’11, Antalya.

İNALÖZ, Ayşe, (2003), “Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi”, Uzmanlık Tezi, Aralık 2003, Ankara.

KESER BERBER, Leyla, (2000), “İmzalıyorum O Halde Varım”, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri, TBB Dergisi, 2000/2, s.503–556.

KESER BERBER, Leyla, (2004), “Dijital İmza”, Bilişim Teknolojisi Hukuku Gündemi 2003–2004, İstanbul Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi yayını, İstanbul. (Dijital).

LUPTON, W. Everett, “The Digital Signature: Your Identity by the Numbers”, 6 RICH. J.L. & TECH. 10 (Fall 1999) <http://www.richmond.edu/jolt/v6i2/note2.html> (12.11.2004).

REED, Chris, “What is a Signature?”, The Journal of Information, Law and Technology (JILT).2003/3, <http://elj.warwick.ac.uk/jilt/00-3/reed.html/>

ÖZCİVELEK, Rukiye, E-Devlet Kavramı Üzerine Bir Sorgulama, [www.tubitak.gov.tr](http://www.tubitak.gov.tr)

TÜFEKÇİ, Tolga, “Elektronik İmza Niçin Yaygınlaşmıyor?”, TÜBİTAK, [http://www.bilten.metu.edu.tr/Web\\_2002\\_v1/common/yayinlar/Elektronik\\_imza\\_nicin\\_yayginlasmiyor-doc.pdf](http://www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/Elektronik_imza_nicin_yayginlasmiyor-doc.pdf)

TOPALOĞLU, Mustafa, (2001), “Dijital İmza”, PC Life, Şubat 2001.

## DİĞER KAYNAKLAR

TELEKOM DÜNYASI Dergisi, Aralık 2004.

Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, [http://www.taek.gov.tr/taek/bet/pdf/hukuk\\_cg\\_raporu.pdf](http://www.taek.gov.tr/taek/bet/pdf/hukuk_cg_raporu.pdf)

<http://www.ivhp.net>

[www.die.gov.tr](http://www.die.gov.tr)

[www.milliyet.com.tr](http://www.milliyet.com.tr)

[www.tk.gov.tr](http://www.tk.gov.tr)

[www.turkinternet.com](http://www.turkinternet.com)

[www.turkpoint.com/e-yasam/sayisal imza.asp](http://www.turkpoint.com/e-yasam/sayisal_imza.asp)

[www.ulastirma.gov.tr](http://www.ulastirma.gov.tr)