ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICISI

Dr. Mine ERTURGUT*

GİRİŞ

Bilgisayar ve elektronik alanda yaşanan gelişmeler, internetin de hayatımıza girmesiyle birlikte, kişilerin elektronik ortamda neredeyse günlük hayatlarının bir parçası olarak, çeşitli işlemler yapmalarına yol açmıştır. Belgelerin elektronik ortamda saklanması, elektronik ortamda veri aktarımı ve elektronik ticaretin gelişimi, güvenlik sorunlarını da beraberinde getirmiştir. Elektronik ortamda işlem yapan kişinin gerçek kimliğinin tespiti ve elektronik olarak iletilmiş verilerin veya mesajların herhangi bir şekilde üçüncü kişilerin eline geçerek içeriğinin değiştirilip değiştirilmemiş olduğunun saptanması bu sorunların başında gelmektedir.

Elektronik imza, elektronik ortamda yapılan işlemlerde güvenliğin sağlanması bakımından bir çare olarak ortaya çıkmıştır. Ancak matematiksel işlemlerle üretilen elektronik imza, tek başına güvenilir biçimde kişilerin kimliğinin tespiti veya veri bütünlüğünün sağlanması bakımından yeterli gelmemektedir. Bu sebeple güvenilir üçüncü kişilere ihtiyaç duyulmuş ve çeşitli ülkelerde yapılan yasal düzenlemelerde de sertifika hizmet sağlayıcı bu görevi üstlenmiştir.

Elektronik ortamda yapılan işlemlerde kimlik tespiti, sertifika hizmet sağlayıcıları tarafından sağlanmaya çalışılmıştır.

Çalışmamızda, sertifika hizmet sağlayıcıları, genel bir bakış açısından, özellikle Elektronik İmza Kanunu hükümleri çerçevesinde ve mümkün olduğunca diğer ülkelerin yasal düzenlemeleri ile karşılaştırma yapılarak değerlendirilecektir. Bu anlamda sertifika hizmet sağlayıcısının fonksiyonu, işleteni, faaliyetleri ve faaliyete başlaması konusunda bilgiler verilmeye

* DEÜ Hukuk Fakültesi Medeni Usul ve İcra-İflas Hukuku Anabilim Dalı

Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt : 6, Sayı : 2, 2004, s.97-130

çalışılacak, ancak sertifika hizmet sağlayıcılarının sorumluluğu konusuna değinilmeyecektir.

I. GENEL OLARAK

Özellikle elektronik ticaret alanında faaliyette bulunan şirketler ve çoğu kurum internet üzerinde gerçek ve yasal bir şirket olduklarını kanıtlamak için sertifika kullanmaktadır. Bundan başka, internet bankacılığı veya internet üzerinden yapılan alışveriş gibi kişilerin gerçek kimliklerinin ve verilerin gizliliğinin önemli olduğu işlemlerde şifre kullanımı ve bunun yanında elektronik sertifikanın da kullanılması, güvenliğin arttırılması bakımından önemli olduğundan elektronik sertifikanın kullanım alanı artmaktadır[1].

Genel olarak elektronik sertifika hizmet sağlayıcısı (Elektronik İmza Kanununda kullanılan terim), Trust Center (güven kurumu), onay kurumu, sertifikasyon kurumu (1997 tarihli Alman İmza Kanununda kullanılan terim, Zertifizierungsstelle), sertifikasyon hizmetleri sunucusu (13 Aralık 1999 tarihli 1999/93/AT sayılı "Elektronik İmzalar İçin Topluluk Çerçevesi" Avrupa Birliği Direktifinde, 2001 tarihli Alman İmza Kanununda (SigG)[2] ve Avusturya İmza Kanununda kullanılan terim, Zertifizierungsdiensteanbieter; aynı şekilde İsviçre'deki Elektronik Sertifikasyon Hizmetleri Yönetmeliğinde ve İsviçre Elektronik İmza Federal Kanun Tasarında kullanılan terim, Anbieterin von Zertifizierungsdiensten), belgelendirme mercii[3], e-kimlik

---

1 Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Raportör: Avniye Tansuğ, Şubat 2002, s. 5.

2 Alman Elektronik İmza Kanunu 22 Mayıs 2001 tarihli Kanun ile daha önceki "sertifikasyon kurumu" ifadesini "sertifikasyon hizmet (sunucusu) sağlayıcısı" olarak değiştirmiştir.

3 **Arıkan,** A. Saadet, Elektronik Ticaret, Hukuk ve Noterler, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 23; **Arıkan,** A. Saadet, Modern İletişim Araçları ve Özel Hukuk, in:Hukuk Kurultayı 2000, Ankara 2000, s. 307 vd. Ayrıca sertifika (onay) kurumu şeklindeki kullanım için bkz. **Arıkan**-Kurultay, s. 320.

hizmet sağlayıcısı[4], onay hizmeti sağlayıcı (onay kurumu)[5], (dijital) sertifika servis sağlayıcı[6] gibi isimler altında anılmaktadır[7].

Dijital sertifikalar (dijital kimlikler), ehliyet, pasaport gibi kimlik kartlarının elektronik ortamdaki benzerleri olarak tanımlanabilir. Dijital sertifika, kişilerin kimliğini, elektronik bilgiyi imzalamak ve şifrelemek için kullanılan bir çift elektronik anahtara bağlar. Bu şekilde ticari ve kişisel işlemlerin, iletişim ağları üzerinde güvenli bir şekilde gerçekleştirmesi mümkün hale gelmektedir[8]. Sertifikanın en önemli fonksiyonu kimlik belirlemedir.

---

4 http://e-kimlik.bilten.metu.edu.tr/net/teknik/ehs.jsp

5 **Acır**, Birsen, Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, Sermaye Piyasası Kurulu, Yeterlilik Etüdü, Ankara 2000, s. 34, 37.

6 **Yaltı,** Billur, E-İmza ve E-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-I, Vergi Sorunları, Nisan 2001, S. 151, s. 130; **Yaltı,** Billur, Elektronik Ticarette Vergilendirme, İstanbul 2003, s. 248.

7 Burada Avrupa Birliği Düzenlemeleri ve diğer ülke kanunları ile Elektronik İmza Kanunu arasındaki terim farklılığına değinmek gerekir. Diğer yasal düzenlemelerde "*sertifikasyon* hizmetleri sunucusu" terimi tercih edildiği halde, Elektronik İmza Kanununda "*sertifika* hizmet sağlayıcısı" terimi tercih edilmiştir. Kuşkusuz, bu terimin kullanılması sebebiyle sertifika hizmet sağlayıcısının, sadece elektronik imzalarda kullanılacak sertifika düzenleyeceği anlamı çıkmamaktadır. Sertifika, sertifikasyon hizmeti sonucunda imza sahibi kişilere verilen kimliktir. Sertifikasyon, yapılan iş; sertifika, yapılan işin sonucudur. Sağlayıcının sertifika verebilmek için sertifikasyon hizmetlerini sunması gerekmektedir. Bu hizmetlere bloke listesi ve sertifika listesi de dahildir. Bu sebeple terim farklılığının, sertifika hizmet sağlayıcısının işlevini farklılaştırmadığı belirtilmelidir. Kaldı ki, sertifika hizmet sağlayıcısının yasal tanımında, yer alan "elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan" (EİK m.8/I) ifadesi bu konudaki tereddütleri gidermektedir. Biz de çalışmamızda kanuni terimi kullanacağız.

8 http://www.globalsign.com.tr/support/general/about_dig_cer.htm?anc=di_ce. Dijital imza ve şifreleme (kriptografi) birbirine karıştırılmamalıdır, her ikisi farklı amaçlara hizmet eder. Bir e-mailin imzalanması, imza sahibinin kendi e-kimliğini gönderdiği e-maile ekleyerek e-mailin kendisi tarafından gönderildiği ve başka kişilerce içeriğinin değiştirilmediği konusunda garanti vermesidir. İmzalamak, mesajın onaylandığı anlamına gelir, fakat bu mesajın içeriğinin başkaları tarafından görülmesini engelleyemez. Mesajın başkaları tarafından görülmesini engellemek için mesajın şifrelenmesi gerekir (http://e-kimlik.bilten.metu.edu.tr/net/sorular/guvenli_e-posta.jsp). Şifreleme konusunda bkz. **Sözer,** Bülent, Elektronik Sözleşmeler, İstanbul 2002, s. 123-126; **Keser Berber**, Leyla, Şekil ve Dijital İmza, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 84 vd.; **Keser Berber**, Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital

Elektronik imza, kişilerin biyometrik özelliklerine dayalı (ses, göz retinası taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın elektronik ortama aktarılmış hali veya çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavram olarak karşımıza çıkmaktadır[9]. Biz de çalışmamızda üst başlık olarak elektronik imza kavramını esas alarak açıklamalarda bulunacağız. Ancak günümüzde en çok kullanılan yöntem dijital imza olduğu için açıklamalarımız daha çok dijital imzaya ilişkin olacaktır.

Elektronik imza, *"teknolojik tarafsızlık"* kavramına dayanmaktadır. Bu anlamda yasal düzenleme yapan ülkelerin, *elektronik imza* kavramını tercih etmelerinin nedeni, dijital imza yanında diğer yöntemleri de kabul edecek şekilde, hukukun teknolojik gelişmeye uygunluğunun sağlanmasıdır. Böylece ileride geliştirilecek elektronik imza yöntemleri de kimlik belirleme ve mesajın bütünlüğü gibi, imzadan beklenen fonksiyonları yerine getirdikleri takdirde, yasal düzenlemelere uyum sağlayacaklardır. Bu nedenle, elektronik imza kavramı, bir kişinin elektronik bir belgeyi imzalamada kullanacağı tüm yöntemleri kapsamaktadır[10].

İmza, Ankara 2002, s. 144 vd.; **Miccoli,** Mario, Teknolojik Açıdan Elektronik Ticaret (Çev. Günal, Nadi), in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 207 vd.

9 **Pütmann,** F.Frank/**Sander**, Matti, Internationale Signaturgesetze im Vergleich, in: **Hoeren** Thomas/**Schüngel** Martin, Rechtsfragen der digitalen Signatur, Berlin 1999, s. 387; **Pekcanıtez,** Hakan, Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslar arası İnternet Hukuku Sempozyumu, İzmir 2002, s. 395; **Yaltı,** Vergi Sorunları, S. 151, s. 129; **Yaltı,** s. 247, dn.44; **Arıkan,** s. 23; **Arıkan**-Kurultay, s. 312; **Altınışık,** Ulvi, Elektronik Sözleşmeler, Ankara 2003, s. 78-79; **Sevimli**, Ahmet, Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası, Prof. Dr. Hayri Domaniç'e 80. Yaş günü Armağanı, C.II, İstanbul 2001, s. 1029; **Acır**, s. 22 vd. Elektronik imza ile dijital imza sık sık aynı anlamda kullanılmakla beraber ikisi arasında fark vardır. Dijital imza bir elektronik imza çeşididir. Dolayısıyla dijital imza, bir üst kavram olan elektronik imza başlığı altında bulunur. Dijital imza esas olarak açık anahtar altyapısına (public key ınfrastructure- PKI) dayanır. Elektronik imza ise PKI modeli de dahil, diğer teknolojileri de içeren bir anlama sahiptir (**Pütmann**/**Sander**, s. 387). Elektronik imza, *"elektronik ortamda yaratılan kimlik bilgisi"* kavramını ifade etmektedir (**Yaltı,** Vergi Sorunları, S. 151, s. 128).

10 **Altınışık,** s. 78, özellilke dn.61 ve s. 79; **Yaltı,** Vergi Sorunları, S. 151, s. 133.

Elektronik imzaların üretilmesinde değişik yöntemler kullanılabilir. Ancak elektronik imzaların tümü, 0 ve 1 sayılarından oluşan seriler halinde ifade edildiği için dijitaldir[11].

Dijital imza[12], elektronik şekilde gönderilen verinin bütünlüğünü, başka bir deyişle gönderildikten sonra değiştirilip değiştirilmediğini ve en önemlisi,

---

11 **Altınışık**, s. 79 ve s. 79, dn.63.

12 Dijital imza ya da sayısal imza, elektronik ortamdaki yazışmalara eklenmek suretiyle, imza sahibi olan yazıyı gönderenin kimliğini ve gönderilen yazının bütünlüğünün korunduğunu doğrulayan bölümdür. Sayısal imza, yazının içeriğine (metin) ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle üretildiği için, sayısal imzanın doğrulanmasında, imzayı atanın açık anahtarı kullanılmaktadır (http://www.e-ticaret.gov.tr/e_kutuphane/sozluk.htm). Ayrıca bkz. **Pekcanıtez,** s. 395; **Acır**, s. 26 vd. Dijital imza, "dijital bir veri üzerinde sahibinin gizli anahtarı ile şifreleme yöntemiyle yaratılan bir mühürdür" (**Arıkan**, s. 23). "Dijital imzanın amacı, kimliği belirlenebilir bir kişinin, mevcut bir belgenin görüldüğünü ve imza edildiğini ispat edilebilir şekilde garanti etmektedir." (**Keser Berber**-Şekil ve Dijital İmza, s. 73; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 137). Aynı şekilde bkz. "Dijital imza, metnin belgenin yazarı tarafından düzenlendiğini belirtmek kadar, başkası tarafından bozulmadığını da göstermek amacını güder ve dolayısıyla da esasında metnin tamamı dijital imzaya dönüşmüş olur." (**Sözer,** s. 127). "Dijital imza, göndericinin özel anahtarıyla şifrelediği mesaj özetidir." (**Altınışık,** s. 84; aynı şekilde bkz. **Sözer,** s. 128). "Dijital imza, elle atılmış bir imzanın bilgisayardan bir grafik programı kullanılarak ekrana yansıtılması anlamına gelmez. Bu tamamen şifreleme metodu ile gerçekleştirilen bir tanıtma yöntemidir." (**Sözer,** s. 127).

Dijital imzanın işleyişi kısaca şöyledir: Dijital imza yaratmak için, imzalayan, mesajın (gönderilecek metnin) kısaltılmış mesaj özetini (öz-hash) yaratır ve mesaj özetini şifrelemek için kendi özel anahtarını kullanır. Böylece mesaj özeti şifrelenir ve bu şifrelenmiş öz dijital imzadır. Gönderen, metne (mesaja) ekleyerek dijital imzayı da alıcıya gönderir. Alıcı, gelen mesajdan mesaj özetini (öz-hash) tekrar yaratır ve gönderenin açık anahtarını gelen mesajdaki şifrelenmiş özü deşifre etmede kullanır. Sonuçta alıcının mesajdan çıkardığı öz (metin özeti) ile dijital imzanın deşifre edilmesi sonucu elde edilen öz karşılaştırıldığında, her ikisi de aynı ise ilk sonuç olarak, dijital imza gönderenin özel anahtarı kullanılarak yaratılmıştır, bu şekilde gönderen mesajı imzalamadığını iddia edemez; ikinci sonuç, mesaj değiştirilmemiştir ve bu mesajın doğruluğu onaylanmıştır. Mesaj herhangi bir şekilde değişirse, değişmiş mesajın özeti de değişik olur. Dijital imza, mesaj için ve onu yaratan özel anahtar için tek olduğundan değiştirildiği takdirde bunun fark edilmemesi mümkün değildir. (http://www.globalsign.com.tr/support/general/about_dig_sig.htm?anc=di_si_what). Dijital imzanın işleyişi konusunda ayrıntılı bilgi için bkz. **Melullis,** Klaus-J, Zum Regelungsbedarf bei der elektronischen Willenserklearung, Monatsschrift für Deutsches Recht (MDR) 1994/2, s. 110-111; **Schreiber** Lutz, Digitale Signaturen im Rechtsverkehr, Hamburg 1999, s. 6-8; **Mertes,** Paul/**Zeuner**, Volker, Digitale Signatur und Signaturgesetz, in: **Hoeren** Thomas/

sertifika hizmet sağlayıcısı tarafından gerçekleştirilen sertifikasyon işlemi sayesinde, gönderilen verinin gerçekten o kişi tarafından gönderilip gönderilmediğini, yani kimlik tespitini mümkün kılmaktadır. Bu anlamda, verinin değiştirilmesinin engellenmesi değil, verinin değiştirilip değiştirilmediğinin saptanması dijital imza ile mümkün olmaktadır; bu sebeple dijital imza bir doğrulama aracı olarak karşımıza çıkmaktadır. Sertifikasyon ise kimlik belirleme aracıdır.

Elektronik belgeler hakkında en önemli iki sorun olan gönderilen verinin bütünlüğünün korunması ve gönderen kişinin kimliğinin tespiti, dijital imza sayesinde çözümlenmektedir. Ancak, dijital imzanın bu avantajlarına rağmen, bu imza usulü güvenilir bir kurumun katılımı olmaksızın gerçekleştirildiği takdirde dijital imzaya yüklenen fonksiyonlar anlamını yitirmektedir[13]. Bu anlamda, dijital imzaya güvenmek için ve hukuki etkiler doğurmasını sağlamak üzere, sertifika hizmet sağlayıcıları bir şart olarak karşımıza çıkmaktadır. Dijital imzalı belgelere, daha geniş anlamıyla elektronik imzalı belgelere hukuken geçerlilik tanınması, sertifika hizmet sağlayıcılarının bu prosedüre katılmaları sayesinde olmaktadır. Zira, Elektronik İmza Kanununda, elektronik imzalı belgelerin borçlar hukuku anlamında elle atılan imzaya eşdeğer kabul edilmesi ve usul hukuku anlamında bu belgelere senet niteliğinin verilmesi, imzanın, güvenli elektronik imza niteliğinde olması şartına bağlanmıştır (EİK m.5, m.22, m.23).Güvenli elektronik imzanın bir şartı da nitelikli sertifikaya dayanmasıdır (EİK m.4). Dolayısıyla sertifika hizmet sağlayıcıları, elektronik belgelere hukuki anlamda geçerlilik tanınırken olmazsa olmaz bir koşul olarak karşımıza çıkmaktadır. Ayrıca, hukuki güvenliğin sağlanması, veri güvenliğinin sağlanmasına bağlıdır.

Sieber Ulrich (Hrsg.), Handbuch Multimedia-Recht, München 2002, Teil 13.3, s. 11-12; **Yaltı,** Vergi Sorunları, S. 151, s. 129-130; **Yaltı,** s. 247-248; **Şenocak,** Zarife, Dijital İmza ve Dijital İmzanın Borçlar kanunun Hükümleri Açısından Ele Alınması, AÜHFD C.50 S. 2 2001, s. 98-105; **Keser Berber**, Leyla, "İmzalıyorum O Halde Varım" Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri, TBBD 2000/2, s. 514-516; **Keser Berber**, Şekil ve Dijital İmza, s. 74 vd.; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 138 vd.; **Altınışık,** s. 81-84, 91-92; **Sözer,** s. 127-128. Ayrıca bkz. **Orta,** Mesut, Ulusal Yargı Ağı Projesinde Elektronik İmza, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 166.

13 **Mertes**, Paul, Digitale Signatur-Wertlos ohne Trust Center, in: **Glade**, Albert/**Reimer,** Helmut/**Struif,** Bruno (Hrsg.), Digitale Signatur & Sicherheitssensitive Anwendungen, Braunshweig/Wiesbaden 1995, s. 155-156.

Sertifika hizmeti olmaksızın, şifre kullanımı (bu anlamda PGP[14] kullanımı) sadece matematiksel güvenliği sağlamakta, ancak bunun dışında veri güvenliği (kimlik doğrulama ve gönderilen verinin sonradan değiştirilip değiştirilmediği) gündeme gelmemektedir[15].

Elektronik sertifika hizmet sağlayıcısının, sadece dijital imzanın altyapısı içinde bir kurum olarak düzenlendiği şeklindeki düşüncenin[16] kabul edilmesi, Elektronik İmza Kanunu ve diğer ülke hukukları değerlendirildiğinde mümkün gözükmemektedir. Elektronik İmza Kanununda ve birçok ülkede, elektronik imza teriminin seçilmesi tesadüf değildir[17]. Elektronik imza, bildiğimiz üzere bir üst başlıktır ve altında dijital imza (sayısal imza), biyometrik imza, bilgisayar ekranında kalemle atılan imza çeşitleri de dahil olmak üzere elektronik ortamda imza sahibinin kimliğinin tespitine imkan veren çeşitli yöntemleri ifade eder. Zira, Kanunda elektronik imza, *"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* şeklinde tanımlanmıştır. Günümüzde en yaygın şekilde kullanılan dijital imzanın, yakın

---

[14] PGP (Pretty Good Privacy), bir mesaj şifreleme ve sayısal imzalama programıdır. PGP aynı zamanda açık ve gizli anahtarlarla ilgili işlemleri de yapabilmektedir. PGP Phil Zimmerman tarafından oluşturulmuş bir yazılımdır. Dosya bazında işlem yapan bir şifreleme ve sayısal imzalama programıdır. Elektronik posta gönderme özelliği yoktur. Sadece elektronik posta olarak gönderilebilir halde dosyalar yaratmaktadır.

[15] **Mertes,** s. 159.

[16] **Arıkan,** s. 23. Ayrıca bkz. **Altınışık,** s. 84. Bu düşünce doğru olmakla birlikte, elektronik imza üst başlığı da dikkate alınarak düşünülmesi gerekir kanaatindeyiz.

[17] Zira Kanunun gerekçesinde, elektronik imza kavramının seçilmesini kapsayıcı bir üst kavram olması sebebiyle tercih edildiği ve bu terimin kullanılması sonucu, ABD ve Fransa gibi ülkeler ve Avrupa Birliği düzenlemelerinde kullanılan temel kavramlara uyum sağlandığı belirtilmiştir (Bkz. genel gerekçe).

Amerika Küresel ve Ulusal Ticarette Elektronik İmza Kanunu'nda belirtildiği üzere, *elektronik imza terimi (Bölüm 106), "bir şahıs tarafından kaydı imzalamak amacıyla uygulanan ya da kabul edilen sözleşmeye ya da başka bir kayda iliştirilen ya da mantıksal bağ kurulan elektronik bir ses, sembol ya da yöntem anlamına gelir."* Görüldüğü üzere, burada elle atılan imzanın fonksiyonlarını da üstlenecek herhangi bir elektronik ses, sembol ya da yöntem elektronik imza olarak kabul edilmiştir. İmzanın fonksiyonları, kanundaki tanımdan da anlaşılacağı üzere asıl olarak iki tanedir. Birincisi, irade beyanının tespiti (kaydı imzalama amacı irade beyanıdır ve bu anlamda kimliğin tespitini de kapsar), ikincisi ise veri bütünlüğünün korunmasıdır (kayda iliştirilen ya da mantıksal bağlantı kurulabilen ifadesiyle). Görüldüğü gibi, Amerika'da elektronik imza geniş şekilde düzenlenmiştir.

gelecekte teknolojik gelişmelere bağlı olarak, farklı tekniklerle yeni versiyonlarının kullanılacağı ve yaygınlaşacağı kaçınılmazdır. Sertifika hizmet sağlayıcıları günümüzde sayısal imza teknolojisini kullanarak imza anahtarları üretmekte ve kişinin kimliğini tespit etmektedir. Aynı şekilde diğer elektronik imza tekniklerinin de kullanılarak bu elektronik imzaların kişilere özgülenmesi ve bu özgülenmenin yine sertifika hizmet sağlayıcısının görevi çerçevesinde güvenli bir şekilde kimlik tespiti yapılarak sertifika ile belgelenmesi mümkündür.

Sertifika hizmet sağlayıcısına duyulan ihtiyacın temel sebebi, imza sahibi kişinin kimliğini tespit etmek ve bu şekilde elektronik işlemlerde güvenilirliği sağlamaktır. Sertifika hizmet sağlayıcısının temel fonksiyonu imza anahtarı üretmek değildir; çünkü kişi kendi bilgisayarında imza anahtarını üretebilir ve sadece sertifikasyon amacıyla sertifika hizmet sağlayıcısına başvurur. Sertifika hizmet sağlayıcısı kimlik denetimini yaptıktan sonra imza anahtarının kişiye özgülendiğini ifade etmek amacıyla sertifika hazırlar ve bu kişinin kimliğinin işleme katılan üçüncü kişilerce kontrolünü sağlamak için liste hizmeti sunar. Bu anlamda sadece sayısal imzanın değil, diğer imza çeşitlerinin de sertifikasyon sayesinde bir kişiye özgülenmesi mümkün olabilecektir. Kanun koyucunun sadece dijital imzayı kabul etmek suretiyle günümüz tekniğiyle kendini sınırlamayarak gelecekteki gelişmelere de uygun olacak şekilde başarılı bir düzenleme yaptığını söylemek mümkündür. Teknolojinin hızlı gelişimine, kanunların geç kalmaksızın, derhal uyum sağlaması çoğu zaman mümkün olmadığı için, bu yolun tercih edilmesinin yerinde olduğu söylenmelidir.

II. SERTİFİKA HİZMET SAĞLAYICISININ FONKSİYONU

Elektronik yolla belge gönderilirken taraflarca üç esasın varlığı aranır. Birincisi gizlilik (mesajın başkaları tarafından okunmamasının sağlanması), ikincisi mesajın bütünlüğü (başkası tarafından değiştirilmemiş olması) ve son olarak güvenlik (karşıdaki kişinin kimliği konusunda güvenlik)[18].

Gizliliğin sağlanması, çeşitli şifreleme yöntemlerinin kullanılması ile mümkündür. Bunun yanında, mesajın veri bütünlüğünün korunması ise kullanılan elektronik imza tekniği ile ilgilidir. Bu sebeple mesaj metninin şifrelenmesi yoluyla elde edilecek gizlilik ile elektronik imza usulünün

---

[18] **Miccoli,** s. 206. Benzer şekilde bkz. **Yaltı,** Vergi Sorunları, S. 151, s. 128-129.

uygulanması sonucu elde edilecek mesaj metninin değiştirilmemiş olması birbirinden farklı konulardır. Güvenlik konusuna gelince, sertifika hizmet sağlayıcıları olmazsa, imza sahibi kişinin kimliğinin tespiti ve bunun ispatı mümkün olmaz. Bu sebeple asıl olarak güvenlik konusunda, güvenilir üçüncü kişi anlamında, sertifika hizmet sağlayıcılarına ihtiyaç duyulmaktadır.

Elektronik ticaret işlemlerinde tarafların kimliğinin tespitinde en etkili yol, mevcut gelişmelere göre dijital sertifikalardır. Kimliklerin belirlenmesi ve kimliğin doğruluğunun onaylanması, vergilendirmenin sağlıklı olarak gerçekleştirilebilmesini, hukuki ilişkilerin güvenli biçimde kurulmasını sağlayacağı gibi, özellikle internette tüketicilerin korunmasını da gerçekleştirecektir[19].

1. Sertifika Hizmeti

Sertifika, kimlik tespitini mümkün kılmak için elektronik imza ile yaratılmış bir araçtır. Bir kereye mahsus olmak üzere, bir anahtar çifti, sertifika işlemi sayesinde bir gerçek kişiye özgülenir. Sertifika ile özgüleme belgelendirilir. Özgüleme, imza anahtarı sahibinin kimliğinin tespitine; anahtar çiftinin verilmesine; gizli anahtarın kişiselleştirilmesine ve gizli anahtar ile veri taşıyıcılarının güvenli aktarımına dayanır. Bu özgüleme, Alman İmza Kanunu § 10 ve İmza Yönetmeliği § 13'e göre belgelendirilir. Sertifika hizmet sağlayıcısı, organizasyonla ilgili tedbirler aracılığıyla el yazısı ile imzadaki biyometrik niteliklere yaklaşır biçimde kimlik belirleme fonksiyonunu sağlar. Sertifika hizmet sağlayıcısı bununla elektronik hukuki işlemlerin zorunlu şartı olarak karşımıza çıkmaktadır[20].

Sertifika, dijital bir kimliktir[21], daha açık ifadeyle günlük hayatta kullandığımız kimlik kartlarının elektronik ortamdaki karşılığıdır. Sertifika, kişinin kimlik bilgileri ile bilgileri şifrelemek ve şifrelenen bilgileri çözmek için kullanılan bir çift elektronik anahtarı birbirine bağlayan bir elektronik

---

19 **Yaltı,** s. 246-247.

20 **Rossnagel** Alexander, Recht der Multimedia Dienste, München 2001, 5 SigG § 2, s. 2.18.

21 **Schmidl**, Michael, Die elektronische Signatur, CR 7/2002, s. 512; Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Raportör: Avniye Tansuğ, Şubat 2002, s. 4; **Altınışık,** s. 85. Başka bir deyişle, dijital kimlik, kimliğin sayısal ispatıdır (http://e-kimlik.bilten.metu.edu.tr/net/teknik/ekimlik.jsp) Ayrıca bkz. **Orta,** s. 165.

kayıttır[22]. Nitekim Elektronik İmza Kanununda da "*elektronik sertifika, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt*" olarak tanımlanmıştır (m.3/ı).

Sertifika hizmet sağlayıcısı, güvenlik alt yapısının kilit noktasıdır[23]. Bu anlamıyla sağlayıcının ana görevi, gerçek kişilerin kimliğinin güvenli şekilde tespit edilmesidir[24]. Sertifika hizmet sağlayıcısının tanımsal görevi, "sertifika vermek"tir. Alman İmza Kanununda, sertifika hizmet sağlayıcısı, nitelikli sertifika veya nitelikli zaman damgası düzenleyen gerçek veya tüzel kişi olarak tanımlanmıştır (§ 2 N.8 SigG). Alman İmza Kanunu güvenlik altyapısı çerçevesinde hizmet sağlayıcıların sadece bir çeşidini tanımaktadır ve güvenlik alt yapısının diğer fonksiyonlarına bağımsız fonksiyon taşıyıcı olarak tanımda yer verilmemektedir. Ancak tanım maddesi, diğer maddelerle birlikte değerlendirildiğinde, sertifika hizmet sağlayıcısının, kanun tarafından, güvenlik alt yapısının bütün diğer gerekli fonksiyonlarından da yükümlü bir hizmet sağlayıcısı olarak düzenlendiği görülecektir. Bununla sertifika hizmet sağlayıcısının görevi, sadece tanımsal görevi olan sertifika vermek değil, aynı zamanda kimlik kontrolü, anahtarın kişiselleştirilmesi, liste hizmeti ve bloke hizmeti, zaman damgası hizmeti vermektir. Buna göre, imza anahtarının düzenlenmesi ve bununla bağlantılı bütün işlemlerin belgelenmesini kapsayan bir usul de tespit edilir[25]. İsviçre'de 12 Nisan 2000 tarihli Elektronik Sertifikasyon Hizmetleri Hakkında Yönetmeliğe göre (m.2), sertifikasyon hizmetleri sunucusu, elektronik ortamdaki veriler çerçevesinde verileri tasdik eden ve bu amaçla elektronik sertifika düzenleyen kurumlar olarak belirtilmiştir. Görüldüğü üzere, İsviçre'de de tanımsal unsur, verilerin tasdiki ve elektronik sertifika düzenlenmesidir. İsviçre'de 2001 tarihli Elektronik

---

22 Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Raportör: Avniye Tansuğ, Şubat 2002, s. 4. Başka bir tanıma göre, "sertifika, kullanıcı ismi ile onun genel şifre anahtarını ihtiva eden ve özel şifre anahtarının kulanıcıya ait olduğunu doğrulayan elektronik dokümandır" (**Göç Gürbüz**, Diğdem, Elektronik Ticarette Hukuki Yapı ve Yasal Düzenlemeler, Mükellefin Dergisi, 2000/95, s. 19).

23 **Rossnagel**, 5 SigG § 2, s. 2.18; **Mertes**/**Zeuner**, Teil 13.3, s. 16. Başka bir ifadeyle hizmet sağlayıcılar, elektronik oratamdaki ticari ve ticari olmayan işlemlerin güvenliğinin "*belkemiği*"ni oluşturmaktadırlar (**Yaltı,** Vergi Sorunları, S. 151, s. 130; **Yaltı,** s. 248).

24 **Schmidl,** CR 7/2002, s. 512. Kimlik tespiti için resmi belgelerin kullanılması gerekir. Nitekim Kanunda da sağlayıcının sertifika verdiği kişilerin kimliğinin resmi belgelere göre güvenilir biçimde tespit edilmesi yükümlülükleri arasında sayılmıştır (EİK m.10/b).

25 **Rossnagel,** 5 SigG § 2, s. 2.18-2.19.

İmza Kanunu Tasarısında da aynı unsurlara rastlanmaktadır (m.3). Ayrıca sunucuların diğer görevleri, Yönetmeliğin ve Tasarının çeşitli maddelerinde düzenlenmiştir. Buna karşılık Avusturya İmza Kanununa göre, sertifikasyon hizmet sağlayıcısı, sertifika düzenleyen veya diğer imza ve sertifika hizmetlerini sağlayan gerçek veya tüzel kişi veya diğer hak ehliyetine sahip müesseselerdir (Avusturya İmza Kanunu § 2 N.10) . Görüldüğü gibi, Alman Hukukunda yasal tanımda yer almayan hususlar, Avusturya'da yasal tanımsal öğeler olarak karşımıza çıkmaktadır. 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Birliği Direktifinde de ("Elektronik İmzalar İçin Topluluk Çerçevesi"), sertifikasyon hizmet sağlayıcısı, sertifika üreten veya elektronik imzayla bağlantılı diğer hizmetleri sunan bir kurum veya gerçek ya da tüzel kişi olarak tanımlanmıştır (m.2/11). Aynı şekilde Elektronik İmza Kanununda da sertifika hizmet sağlayıcısının, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya tüzel kişileri olduğu belirtilmiştir (EİK m.8). Bu anlamda sağlayıcının işlevleri, hukukumuzda tanım düzenlemesinde yer almaktadır.

Dijital imza için gizli ve açık anahtardan oluşan bir anahtar çifti ve açık anahtarın verildiği ve bu anahtara isteyen herkes tarafından ulaşılmasını sağlayacak, kimlik tespitini de dijital bir kimlik belgesi ile yapacak bir sağlayıcı gereklidir[26].

Sertifika, kişinin kimlik denetimine imkan verdiği için içeriğinin buna uygun olması gerekir. Nitelikli elektronik sertifikada bulunması gerekenler Kanunda şöyle belirtilmiştir (EİK m.9):

a. Sertifikanın nitelikli sertifika olduğuna dair bir ibare,
b. Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı,
c. İmza sahibinin teşhis edilebileceği kimlik bilgileri,
d. Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi,
e. Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihi,

---

26 **Arıkan,** s. 24. Açık anahtarın onu oluşturan kişiye ait olup olmadığının kontrolü, anahtar çifti kullanılmadan önce sertifika hizmet sağlayıcı tarafından yapılacak kimlik tespiti sayesinde mümkün olmaktadır (**Miccoli,** s. 211). Asimetrik şifreleme yöntemini kullanarak herkes herhangi bir isim altında anahtar çiftlerini üretebilir. Bu anahtarı üreten kişinin gerçekten o kişi olup olmadığının tespiti için bağımsız bir sertifika hizmet sağlayıcısına gerek duyulmaktadır (**Yaltı,** Vergi Sorunları, S. 151, s. 130).

f. Sertifikanın seri numarası,

g. Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi,

h. Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgileri,

ı. Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgiler,

j. Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan gevenli elektronik imzası.

Nitelikli sertifika yukarıda sayılan bilgileri içerecektir. Gerçekte imza "sadece" güvenli bir imzadır, ne bundan daha az, ne de bundan daha çok bir şey sunar. Örneğin, imzalayanın doğum tarihi üçüncü kişiler tarafından denetlenemez. Aynı şekilde, üçüncü kişi, imza sahibinin yerleşim yeri veya doğum tarihini bilemeyecek durumdadır. Bu bilgiler, müşteri bilgileri arasında yer alır. Bu bilgiler, bazı işlemlerde gerekli değildir. Ancak birçok alanda da elektronik imza, imzalayanın kimliğine güveni ve sözleşmenin karşı tarafının, alıcının veya başvuru sahibinin gerçekten o kişi olduğuna güveni sağlar[27]. Diğer yandan elektronik imzanın, gerekirse bir yargılamada, sertifika almak için başvurduğu sırada sunmuş olduğu belgeler sayesinde sertifika sahibinin kimliğinin denetimini mümkün kılacağı açıktır[28].

Sertifika hizmet sağlayıcısının faaliyeti ile "*belgenin geldiği yer*" konusunda bir garanti sağlanmış olur[29].

Farklı imza standartlarının yaratılmasıyla zorunlu olarak sertifikalar bakımından da farklı standartlar ortaya çıkmıştır. Bu durum ikiye ayrılarak incelenebilir. İlk olarak *(basit) elektronik imza* tanımı (EİK, m.3/b; § 2 N.1 SigG) çerçevesinde herhangi bir imza anahtarına gerek olmaksızın, yani bir *sertifika mevcut olmaksızın* imza anahtarı sahibi kişiye açık bir şekilde özgüleme görevi üstlenmiş olan (basit) elektronik imza karşımıza çıkmaktadır. Buna karşılık ikinci olarak *gelişmiş* (§ 2 N.2 SigG) *ve nitelikli* (§ 2 N.3 SigG) *(Elektronik İmza Kanununun 4. maddesinin ifadesiyle güvenli) elektronik imza*da her defasında bir *sertifika* düşünülebilir ve kanunen

---

27 **Meinel** Cristoph/**Gollan** Lutz, Der elektronische Personalausweis?, JurPC Web-Dok 223/2002, Abs.10.

28 **Meinel**/**Gollan**, JurPC Web-Dok 223/2002, Abs.10.

29 **Miccoli,** s. 213.

gereklidir[30]. Esasen Alman İmza Kanununa göre belirtilen bu görüşe Hukuk sistemimiz bakımından da katılmak mümkündür. Hukukumuzda Elektronik İmza Kanununa göre, elektronik imza tanımında, elektronik imzanın sertifikaya dayanması gerekliliği düzenlenmemiştir (EİK m.3/b). Elektronik imza, "*başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*"yi ifade eder. Buna karşılık, güvenli elektronik imzanın ise nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğini tespit edilebilir kılması gerekir (EİK m.4/c). Bu anlamda basit elektronik imzanın sertifikaya dayanması gerekli değildir; ancak güvenli elektronik imzanın sertifikaya dayanması kanunen zorunludur sonucuna varmak gereklidir.

Alman İmza Kanununa göre, sertifika, imza kontrol anahtarının (yani Elektronik İmza Kanunumuza göre imza doğrulama verisi) bir kişi için düzenlendiğini ve bu kişinin kimliğini onaylayan elektronik belgedir (§ 2 N.6 SigG). Nitelikli sertifikanın tanımında ise bu sertifikanın, sertifika hizmet sağlayıcısı tarafından düzenleneceği bir unsur olarak yer almaktadır (§ 2 N.7 SigG). Kanuni tanımdan yola çıkılarak basit sertifikalarda böyle bir kanuni sınırlamanın formüle edilmemesine karşılık; nitelikli sertifikanın sadece sertifika hizmet sağlayıcısı tarafından düzenleneceği sonucuna varılmaktadır[31].

Elektronik İmza Kanununda, tanımlar bölümünde nitelikli sertifikanın tanımı yapılmamakla beraber, nitelikli elektronik sertifikanın düzenlendiği 9. maddeden Türk Hukuku bakımından da aynı sonuca varmak mümkündür. Zira, nitelikli elektronik sertifikada bulunması gereken hususlar düzenlenirken, sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı (EİK m.9/b) ve sertifika hizmet sağlayıcısının sertifikada yer alan bilgilerini doğrulayan güvenli elektronik imzası (EİK m.9/j) da sayılmıştır. Bu düzenleme, nitelikli elektronik sertifikanın, ancak sertifika hizmet sağlayıcıları tarafından düzenlenmesi gerektiğini açıkça belirtmektedir.

Kanunda sertifika hizmet sağlayıcısının tanımında, Alman İmza Kanunundaki tanımdan farklı olarak[32], imza bakımından herhangi bir açıklık getirilmemiştir. Buna karşılık, sertifika hizmet sağlayıcısının elektronik

---

30 **Schmidl,** CR 7/2002, s. 513.

31 **Schmidl,** CR 7/2002, s. 513.

32 Alman İmza Kanununa göre, nitelikli sertifika ve nitelikli zaman damgası üreten gerçek veya tüzel kişiler sağlayıcı olarak tanımlanmıştır (§ 2 N.8 SigG).

sertifika ile ilgili hizmetleri sağlayacağı 8. maddede belirtilmiştir. Kanunda (basit) sertifikanın tanımında (EİK m.3/ı), sertifika hizmet sağlayıcısı kavramına yer verilmediği halde, sağlayıcının tanımında (m.8), sertifika vermek görevi sayıldığı için her türlü sertifikanın *mutlaka*, sağlayıcılar tarafından verileceği sonucuna varılabilir. Kuşkusuz hizmet sağlayıcılar, nitelikli sertifika dışında kalan sertifikalarla ilgili hizmetleri de yürütebileceklerdir. Buna karşılık, başka bir düşünüş tarzıyla kanunun böyle bir *sınırlama amacını hedeflemediği*, sertifika hizmet sağlayıcısı dışında kalan gerçek ve tüzel kişilerin verdiği sertifikaların da elektronik sertifika niteliğinde olabileceği kabul edilebilir. Başka bir deyişle imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydın (elektronik sertifika) mutlaka kanunda belirtilen niteliklere sahip sertifika hizmet sağlayıcısı tarafından düzenlenmesi şart değildir. Sertifikalar teknik altyapıya sahip her gerçek ve tüzel kişi tarafından üretilebilir. Ancak yukarıdaki paragrafta da belirtildiği gibi, her iki düşünce tarzında da kabul edilmesi gereken, güvenli elektronik imzanın unsurlarından olan nitelikli sertifikanın, kanunun aradığı şartları haiz sertifika hizmet sağlayıcıları tarafından verilmesi gerektiğidir.

Kanımızca, kanun tarafından amaçlanan husus, elektronik sertifikanın, bir sertifika hizmet sağlayıcısı tarafından verilmesidir. Bu sebeple nitelikli sertifika ve diğer sertifikaların mutlaka, sertifika hizmet sağlayıcıları tarafından verilmesi gerekir. Çünkü ancak, kanundaki şartları taşıyan sağlayıcılar, hukuki işlemlerdeki kimlik belirleme ve doğrulama hususundaki güvensizlik problemine çözüm oluşturabilirler. Bu sonuca varılmasına bir başka gerekçe olarak Elektronik İmza Kanununda yer alan "elektronik sertifikalarda sahtekarlık" suçuna ilişkin düzenleme gösterilebilir. Nitekim Elektronik İmza Kanununun 17. maddesine göre, "*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.*" Bu düzenlemeden de açıkça anlaşılacağı gibi, Kanun tarafından, elektronik sertifikaların, mutlaka yetkili kişi veya kurumlarca verilmesi hedeflenmektedir; aksine davranış cezai sorumluluğu gerektirecektir. Elektronik sertifika konusunda yetki ise Kanuna göre kurulmuş ve faaliyette bulunan sertifika hizmet sağlayıcılarına aittir.

(Basit) Sertifika ve nitelikli sertifika şeklindeki ayırım, kanundaki tanımlardan kaynaklanmaktadır. (Basit) Sertifika, sadece imza sahibinin imza doğrulama verisiyle, kimlik bilgilerini birbirine bağlayan elektronik kayıt şeklinde tanımlanmışken; nitelikli elektronik sertifikada, sertifika hizmet sağlayıcısı, nitelikli sertifikanın unsuru olarak onunla iç içe geçmiştir. Bu sayede güvenli elektronik imza, el yazısıyla imza ile hukuken eşdeğer sayılacaktır[33]. Nitekim Alman İmza Kanununda da bu sebeple yalnızca nitelikli elektronik sertifikanın verilmesi düzenlenmiştir[34].

2. Güvenli Şekilde Kimlik Tespiti

El yazısı ile imzanın, sonuçlandırma işlevi, kimliği tespit işlevi, gerçeklik işlevi, uyarı işlevi, devamlılık işlevi ve ispat işlevi vardır[35]. Ancak imzaya yüklenmiş en önemli iki görevin, kişinin kimliğinin belirlenmesi ve irade beyanının tespiti olduğu söylenebilir. İmza, altına atıldığı metnin, imza sahibinin iradesine uygun olduğunu ifade eder[36]. El yazısıyla imza, sahibinin kimliğini tespit eder niteliktedir; çünkü kişinin el yazısının karakteristik özellikleri, kimliği tespite imkan verecek niteliktedir[37].

Elektronik imzalı belgeler, sonuçlandırma ve kimliği tespit işlevlerini yerine getirmektedirler[38]. Sertifika hizmet sağlayıcısının önemi, kimliğin

---

33 **Schmidl,** CR 7/2002, s. 513.

34 **Schmidl,** CR 7/2002, s. 513.

35 İmzanın işlevleri konusunda ayrıntılı bilgi için bkz. **Schreiber,** s. 13; **Köhler,** Helmut, Die Problematik automatisierter Rechtvorgaenge, insbesondere von Willenserklaerungen, AcP 182 (1982), s. 148; **Mertes**/**Zeuner**, Teil 13.3, s. 12-13; **Fritzsche,** Jörg/**Malzer,** M.Hans, Ausgewaehlte zivilrechtliche Probleme elektronisch signierter Willenserklaerungen, DnotZ 1995, s. 18-19; **Hohenegg,** Christoph/**Tauschek,** Stephan, Rechtliche Problematik digitaler Signaturverfahren, BB 1997, s. 1547; **Pekcanıtez**, s. 407; **Şenocak**, s. 125; **Keser Berber**, Şekil ve Dijital İmza, s. 126-127; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 193-194; **Arıkan**-Kurultay, s. 311; **Acır**, s. 24 vd.

36 Bu, imzanın sonuçlandırma işlevidir. Nitekim imzanın almanca karşılığı "Unterschrift" (kelimelerin ayrı ayrı anlamlarıyla "alt yazı") kelimesi bunu tam anlamıyla karşılamaktadır. Bu anlamda, bir metnin yanına (Nebenschrift) veya üst tarafına atılmış imzalarda (Oberschrift) söz konusu metnin tamamının kişinin iradesine uygun olduğu sonucu çıkarılamayacaktır.

37 **Bafra,** Jale, El Yazısı ve İmza İncelemesi Alanında Karşılaşılan Güçlükler, Standardizasyon ve Güvenilirlik, İBD 1997/3, s. 530.

38 **Pekcanıtez**, s. 407; **Şenocak**, s. 125-126. El yazısıyla imzanın diğer işlevlerini de yerine getirdiğine dair bkz. **Mertes**/**Zeuner**, Teil 13.3, s. 13; **Keser Berber**, Şekil ve Dijital

tespiti bakımından ortaya çıkmaktadır. Zira kendisine elektronik imzalı bir metin gönderilen kişi, bu imzanın bir kişiye özgülenmiş olduğunu, açık anahtar vasıtasıyla tespit edebilecektir. Elektronik sertifikaya dayanan bu şekildeki özgülenme, gönderilen kişi tarafından kişinin kimliğini tespit etmeye yarayacaktır. Kimliği tespit işlevi, kişinin elektronik sertifikası sayesinde gerçekleşmektedir. Bu durumda, sertifika hizmet sağlayıcısının en önemli fonksiyonunun, elektronik imza sahibinin kimliğini tespit etmek olduğu söylenmelidir. Böylece, el yazısı ile imzanın sağladığı kimliği tespit işlevi elektronik imza ile de sağlanmış olacaktır.

Herkes, bir program aracılığıyla dijital imzanın anahtar çiftini üretebileceğinden, imza sahibinin *"gerçek"* kimliğinin tespiti, güvenilir bir üçüncü kişi (sertifika hizmet sağlayıcı) tarafından önceden tespit edilmesi sayesinde mümkün olabilecektir. Bu anlamda gerçek kimliğin tespiti, sertifika hizmeti olmaksızın gerçekleşemez[39]. Sadece anahtar sisteminin kullanılması açık anahtarın imza sahibi kişiye ait olduğu konusunda bir tahmini içerir[40]. Bazı kişilerin, başka isimlerle anahtar üretebilmesi ve bu imzayı kullanabilmesi riski her zaman bulunmaktadır. Çift anahtar sisteminde imzalayanın kimliğiyle imza arasında bağlantı kurma özelliği yoktur. Bu riski ortadan kaldırmanın çaresi, açık anahtarın gerçekten o kişiye ait olup olmadığını tespit eden bir kurumun varlığıdır[41].

Sahte bir kimlik gösterilerek, sertifika hizmet sağlayıcısından sertifika alınması durumuyla karşılaşılabilir. Bu sebeple sağlayıcının kimlik tespitini yaparken dikkatli olması, kimlik tespitinin resmi belgelere dayandırılması gerekir[42]. Almanya'da bu husus 16 Kasım 2001 tarihli Elektronik İmza Yönetmeliğinde düzenlenmiştir (§ 3 SigV). Buna göre, kimlik belgesi veya pasaport ile kimlik tespiti yapılacaktır. Avusturya'da ise İmza Kanununa göre, kimlik tespiti için resmi resimli kimlik belgesi gereklidir (§ 8 SigG). Aynı şekilde bu durum Elektronik İmza Kanununda da sağlayıcının yükümlülükleri

---

İmza, s. 128-131; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 195-197; **Acır**, s. 28; **Altınışık,** s. 93. Ayrıca, elektronik imzanın elle atılan imzaya hukuki denkliği konusundaki yaklaşımlar için bkz. **Acır**, s. 28.

39 **Şenocak,** s. 126, dn.87; **Keser Berber**, Şekil ve Dijital İmza, s. 97; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 153-154.

40 **Göç Gürbüz**, s. 19.

41 **Altınışık,** s. 84-85; **Göç Gürbüz**, s. 19.

42 **Şenocak,** s. 126.

arasında sayılmıştır (EİK m.10/b). Sertifika hizmet sağlayıcısı, nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre, güvenilir bir biçimde tespit etmekle yükümlüdür.

III. SERTİFİKA HİZMET SAĞLAYICISININ İŞLETENİ

Alman Hukukunda, sertifika hizmet sağlayıcısının ilk tanımsal özelliği, sertifika hizmet sağlayıcısının gerçek ya da tüzel kişi olmasıdır[43]. Ancak, sertifika hizmet sağlayıcısı kavramının, ilk tanımsal özelliği (niteliği) itibariyle yanlış anlaşılmaya müsait olduğu belirtilmiştir. Tanım, sertifika hizmet sağlayıcısının "bir kişi" olduğundan söz etmektedir. Sertifika hizmet sağlayıcısı gerçek kişi değildir. Ne doğar, ne ölür ve gerçek kişinin sahip olacağı haklara sahip olamaz -üyelik ve vatandaşlık gibi-; hukuki işlemlerle uğraşamaz -boşanma veya vasiyetname tanzimi gibi-[44]. Sertifika hizmet sağlayıcısı, aynı zamanda tüzel kişi de değildir. Çünkü sertifika hizmet sağlayıcısı gerekli hukuki bağımsızlığa ve hukuki işlem ehliyetine sahip değildir. 1997 tarihli Alman İmza Kanunu, izin sistemini öngörmüş olduğundan § 4 Abs.2 de izin taleplerinde başvuru sahibi, *başvuru sahibi* olarak adlandırılmıştır. Bu gerçek ya da tüzel kişidir, bununla beraber sertifika hizmet sağlayıcısı, işletenle aynı değildir; aksine başvuran onun işletmesidir. Dolayısıyla onun işleteni başvuruda bulunur. Bu başvuru, sertifika hizmet sağlayıcısının başvurusu değildir. İşleten iflas edebilir, konkordato teklif edebilir; sertifika hizmet sağlayıcısı iflas etmez, konkordato teklif edemez[45]. 2001 tarihli Alman İmza Kanunu ile Avrupa Birliği Direktifine uygun olarak izin sisteminden vazgeçildiğinden artık bir izin talebine gerek yoktur. Bu sebeple artık kanunda başvuru sahibi ifadesi bulunmamakla birlikte, *sertifika hizmeti işletmesinden* (der Betrieb eines Zertifizierungsdienstes) bahsedilmektedir (§ 4 Abs.1 SigG). Sertifika hizmeti işletmesi, sertifika hizmet sağlayıcı olarak görev yapmaktadır. Buna göre, işleten, gerçek kişi olabileceği gibi, tüzel kişi de olabilir.

Bu sebeple Alman Hukukunda, sertifika hizmet sağlayıcısı tanımında yer alan gerçek ya da tüzel kişinin, sertifika hizmet sağlayıcısının işleteni olabileceği sonucuna varılmıştır. S*ertifika hizmet sağlayıcısı, bir gerçek ya da*

---

43 **Rossnagel,** 5 SigG § 2, s. 2.19.

44 **Rossnagel**, 5 SigG § 2, s. 2.19.

45 **Rossnagel**, 5 SigG § 2, s. 2.19.

tüzel kişi tarafından işletilen ve sertifika hizmeti sunan bir organizasyondur[46]. Buna göre Alman İmza Kanunundaki tanımda istenilenin hatalı formüle edilmesi söz konusu olmuştur[47].

Alman İmza Kanununda işleten, gerçek ya da tüzel kişi olarak adlandırılmaktadır[48]. Kişi toplulukları (tüzel kişiliği olmayan-cemiyet, birlik) işleten olarak belirtilmemiştir. Ancak kanun koyucu tüzel kişiliği olmayan kişi topluluklarını olası işleten olarak kanuni tanım dışında bırakmak istememiştir[49]. Tüzel kişiliği olmayan kişi topluluklarını da gerçek kişiler kapsamında görmek mümkündür. Zira bu topluluklar birden çok gerçek kişiden oluşmaktadır[50]. Bu durumda işleten, tüzel kişiliği olmayan adi ortaklık[51] olabileceği gibi, tüzel kişiliğe sahip şahıs şirketlerinden kollektif şirket, komandit şirket ve sermaye şirketlerinden limited şirket ve anonim şirket olabilir[52].

Elektronik İmza Kanunumuzda, sertifika hizmet sağlayıcısının kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri olabileceği düzenlenmiştir (EİK m.8/I). Ayrıca kamu kurum ve kuruluşları da sertifika hizmet sağlayıcısı olabileceklerdir. Bu anlamda Kanundaki işleten kavramının, Alman Kanunundan daha geniş ele alındığı söylenmelidir. Kanunda, işleten olarak kamu kurum ve kuruluşlarının belirtilmesi, gerçek ve tüzel kişiler yanında, kurumu (Stelle) kabul eden (Avrupa Birliği Direktifi) veya diğer hak ehliyetine sahip müesseseleri (sonstige rechtsfaehige Einrichtung) kabul eden (Avusturya Kanunu) düzenlemeler gibi daha geniş bir yaklaşımın benimsendiği şeklinde yorumlanabilir.

1 Haziran 2002 tarihi itibariyle Almanya'da onbeş akredite edilmiş sertifika hizmet sağlayıcısı ve bir akredite edilmiş zaman damgası sağlayıcısı bulunmaktadır. Bunlardan altısı herkese hizmet vermekte, geri kalanları ise

---

46 **Rossnagel**, 5 SigG § 2, s. 2.19-2.20.

47 **Rossnagel**, 5 SigG § 2, s. 2.20.

48 **Rossnagel**, 5 SigG § 2, s. 2.20; **Bister** Jörg/**Rath** Marco, Gesellschaftsrechtliche Fragen bei der Gründung einer Zertifizierungsstelle, in:**Hoeren** Thomas/**Schüngel** Martin, Rechtsfragen der digitalen Signatur, Berlin 1999, s. 96.

49 **Rossnagel**, 5 SigG § 2, s. 2.20.

50 **Rossnagel**, 5 SigG § 2, s. 2.20.

51 Adi ortaklığın sertifika hizmet sağlayıcısı için en uygun kuruluş şekli olduğu konusunda bkz. **Bister**/**Rath**, s. 123.

52 Bu konuda ayrıntılı açıklamalar için bkz. **Bister**/**Rath,** s. 98 vd.

sadece belli meslek gruplarına hizmet vermektedir[53]. 21 Kasım 2002 tarihi itibariyle bu sayı yirmiüçe ulaşmıştır[54]. Avusturya'da ise Mart 2003 tarihi itibariyle beş adet sertifika hizmet sağlayıcısı aktiftir[55].

Sertifika hizmet sağlayıcısı, bir kamu kurumu veya özel hukuk kişisi olabileceği gibi aynı hizmeti veren birden fazla sağlayıcı da olabilir. Dünyadaki genel eğilim, sağlayıcıların özel hukuk kişileri olması ve birden fazla olması ve fakat bunun yanında sağlayıcıları akredite eden veya lisans veren bir kurumun da varlığıdır[56]. Elektronik İmza Kanununda ise akreditasyon sistemi benimsenmemiştir.

Noterlerin de sertifika hizmet sağlayıcısı olarak görev yapmaları düşünülebilir. Nitekim Amerikan Barolar Birliği tarafından yapılan öneride sanal noterin, hem noterlik işlemlerini yapabilmesi, hem de sertifika hizmet sağlayıcısı fonksiyonunu üstlenebilmesi ileri sürülmüştür[57].

IV. SERTİFİKA HİZMET SAĞLAYICISININ FAALİYETİ

1. Genel Olarak

Sertifika hizmet sağlayıcısının ikinci tanımsal özelliği gerçek kişilere açık anahtar düzenlemesinin tasdik edilmesi (belgeleme)dir[58]. 2001 tarihli Alman İmza Kanununa göre bu konuda biraz daha farklı bir açıklama yapılabilir. Bu kanuna göre, sertifika hizmet sağlayıcısının ikinci tanımsal özelliği *nitelikli sertifika veya nitelikli zaman damgası* düzenlemektir. 1997 tarihli Alman İmza Kanununda tanımda yer alan hususlar, artık Kanunda çeşitli hükümlerde düzenlenmiştir. İmza sahibinin gerçek kişi olması

---

53 **Meinel/Gollan**, JurPC Web-Dok 223/2002, Abs.5-6; Ekim 2001 tarihine kadar akredite edilmiş sertifika hizmet sağlayıcıları bakımından bu sayı 13 idi.

54 http://www.regtp.de/tech_reg_tele/start/in_06-02-04-00-00_m/index.html#an2002

55 http://www.internet4jurists.at/intern25.htm

56 **Arıkan,** s. 24. Sertifika hizmet sağlayıcılarının birden fazla olması halinde, bunlar arasında hiyerarşik bir yapılanma olup olmaması ülkelerin tercihindedir (**Altınışık,** s. 85).

57 **Arıkan,** s. 46. Sertifika hizmet sağlayıcısı faaliyetinin, şu anda yapılan noterlik hizmeti ile aynı olmaması sebebiyle elektronik noterlik ve noterin yapabileceği sertifika hizmet sağlayıcısı fonksiyonları birbirine karıştırılmamalıdır (Bu konuda bkz. **Turan,** Orhan, Noterlik işlemler ve Elektronik, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 187 vd.; **Arıkan**, s. 43 vd.).

58 Bu özellik, 1997 tarihli Alman İmza Kanununa göre bir tanımsal özellik olarak karşımıza çıkmaktadır. (**Rossnagel**, 5 SigG § 2, s. 2.21).

gerektiği, imza sahibinin tanımında (§ 2 N.9 SigG); belgeleme ise sertifika ve nitelikli sertifika tanımlarında (§ 2 N.6-7 SigG) belirtilmiştir. Sağlayıcıyı, diğer gerçek veya tüzel kişi müteşebislerin faaliyetinden ayıran özel faaliyeti, nitelikli sertifika ve nitelikli zaman damgası üretilmesidir. Kanunda, "belgelemek" kelimesi, kelime anlamıyla kullanılmamıştır. Burada belgelemekten anlaşılması gereken "tasdik etmek"tir. Her şeyden önce elektronik hukuki işlemler karşısında, sertifika düzenleyicisi tarafından, anahtar düzenlemesinin tasdiki söz konusudur. Sertifika hizmet sağlayıcısı, bir sertifika sayesinde, kontrol edildikten sonra dijital imzalanmış bilgi aracılığıyla anahtar düzenlemesini tasdik eder[59]. Sertifikanın özelliği "dijital tasdik"tir. Bu tasdik, biri şekli, diğeri içeriksel olmak üzere iki özellik arzetmektedir. Birincisi bu tasdik, dijital imzalanmış olmalıdır, ikinci olarak belli bir içeriğe sahip olmalıdır[60]. Sertifikanın fonksiyonu, kim tarafından imzalandığının tespiti, imza sahibinin kimliğinin kontrol edilmesi, gönderilen verinin bütünlüğünün korunmuş olduğunun tespitidir (bununla bağlantılı olarak irade açıklamasıyla bağlılığın temin edilmiş olması)[61].

Sertifika hizmet sağlayıcısı, sadece gerçek kişiler için tasdik faaliyetinde bulunabilir, diğer sertifika hizmet sağlayıcısının sertifikalarını imzalamak amacıyla kullandıkları açık anahtarları tasdik edemez. Daha çok, bütün sertifika hizmet sağlayıcıları, eşit ölçüde kök sertifika[62] kurumunun sertifikası üzerinde tasarruf ederler. Bu düzenleme ile Alman İmza Kanunu, farklılaşmış sertifikasyon hiyerarşisi sayesinde özel güvenlik altyapıları kurulabilmesine engel olmaktadır[63].

---

59 **Rossnagel**, 5 SigG § 2, s. 2.21.

60 **Rossnagel**, 5 SigG § 2, s. 2.24.

61 **Rossnagel**, 5 SigG § 2, s. 2.25; **Meinel**/**Gollan**, JurPC Web-Dok 223/2002, Abs.8.

62 Kök sertifika, sertifika hizmet sağlayıcısının kendi dijital sertifikasıdır. Kök sertifika açık anahtar ile sertifika hizmet sağlayıcısının birbirine bağlı olduğunu kanıtlar. Kullanıcılar sertifika kurumunun kök sertifikasını internet üzerinden bilgisayarlarına yükleyerek sertifika hizmet sağlayıcısının güvenilirliğini kabul eder. Bu sertifikanın açık anahtarı sertifika hizmet sağlayıcısının kimliğini doğrulamak için kullanılır. Ona bağlı özel anahtar ile de sertifika hizmet sağlayıcısı hazırlanan bütün sertifikaları imzalar. Böylece sertifika hizmet sağlayıcısının verdiği sertifikaların doğruluğunun kontrol edilebilmesi sağlanır. (Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Raportör: Avniye Tansuğ, Şubat 2002, s. 4; **Altınışık,** s. 85; http://www.globalsign.com.tr/support/general/about_dig_cer.htm?anc=di_ce).

63 **Rossnagel,** 5 SigG § 2, s. 2.21. Sertifika hizmet sağlayıcısının dijital imzası başka bir sertifika kurumu tarafından doğrulanabilir, bu ikinci sağlayıcının hiyerarşik olarak daha üstte olması gerekmez (**Altınışık,** s. 85).

Sadece gerçek kişiler için açık anahtar düzenlemesinin tasdiki kök sertifika hizmet sağlayıcıları için de geçerlidir[64].

Sertifika hizmet sağlayıcılarının üç önemli özelliğe sahip olmaları gerekir. Birincisi güvenlik protokolleri ve standartları, güvenli iletişim ve kriptoloji gibi *teknoloji*leri uyguluyor olmalıdır. İkincisi, sağlayıcıların *altyapı* bakımından gizlilik yetenekleri olmalı, müşteri desteği hizmetlerini verebilmelidir. Son olarak hizmet sağlayıcısının *yasal altyapısı* ve internette güvenilir üçüncü kurum olma modeli, kapsamlı dokümanlar şeklinde yayınlanmalıdır[65]. Sistemin, kendisine yüklenen görevleri yerine getirebilmesi, sadece teknik altyapı ve güvenliğe bağlı değildir. Bunun yanında, sertifika hizmet sağlayıcılarının güvenilir olması diğer bir faktördür. Eğer, hizmet sağlayıcıların gerekli gizliliği kırılırsa, bu sistemin elektronik hukuki ilişkilere faydası çok az olacaktır[66]. Sertifika hizmet sağlayıcısı, imza usulünde kullanılan teknik güvenliğin yanı sıra, buna ilave olarak, organizasyon anlamında güvenliği ve yeterliliği bünyesinde birleştirmelidir[67].

2. Faaliyetin Aşamaları

Dijital imzadan beklenen avantajların korunması için genel olarak dört aşamanın gerçekleştirilmesi gerekir[68].

a. Anahtar Üretilmesi

Dijital imza usulü için kapalı (Elektronik İmza Kanununda imza oluşturma verisi) ve açık anahtar (Elektronik İmza Kanununda imza doğrulama verisi) olmak üzere iki anahtara ihtiyaç vardır. Bu anahtarların üretilmesi sırasında gerekli özenin gösterilmesi şarttır. Kapalı anahtar, diğer ifadeyle gizli anahtar bu sistemin bir parçasıdır. Anahtarların tek olarak üretilmesi ve çoğaltılmaya karşı korunması gerekir. Sertifika hizmet sağlayıcısı, bunu sağlamak için gerekli yapısal önlemleri alabilir. Bu sebeple anahtarların güvenli yerlerde üretilmesi ve güvenli donanımların kullanılması

---

64 **Rossnagel**, 5 SigG § 2, s. 2.22.

65 http://e-kimlik.bilten.metu.edu.tr/net/teknik/ehs.jsp

66 **Melullis,** MDR 1994/2, s. 111.

67 **Mertes,** s. 156.

68 **Mertes,** s. 156.

zorunludur[69]. Anahtar çiftinin mutlaka sertifika hizmet sağlayıcıları tarafından üretilmesi zorunlu değildir; kişiler tarafından bilgisayar aracılığıyla şifreleme programıyla da üretilebilir[70]. Günümüzde en çok kullanılan şifreleme programı PGP (pretty good privacy) dir.

b. Kişiselleştirme

İkinci adım olarak, güvenli şekilde üretilen anahtar çiftinin, bir kullanıcıya özgülenmesi gerekir. Bu özgüleme için öncelikle kullanıcının kimliğinin sertifika hizmet sağlayıcısı tarafından tespit edilmesi gerekir. Bu tespit, sadece kimlik belgesinin ibrazı suretiyle ve genel bir kontrol şeklinde gerçekleşmemelidir. Çünkü, kimlik bilgilerinde evlenme, adres değiştirme şeklinde değişiklikler ve bu sayede tahrifat imkanı olabilir. Bu sebeple sertifika hizmet sağlayıcısının bu görevinin, güvenilir şekilde kimliğin tepsitinin gerekmesi ve verilerin korunması sebebi de dahil olmak üzere sadece resmi başvuru makamları tarafından verilen belgelerle sağlanması gerekir[71].

c. Sertifikasyon

Üçüncü adım olarak, anahtar çifti ve kullanıcının kimliği, teklik ilkesi çerçevesinde birbirine bağlandığı takdirde, bu bağlantının, sürekli şekilde olması ve taklit ve tahrifata karşı elektronik olarak "*mühürlenmesi*" gerekir. Bu mühürleme işlemi, sertifika hizmet sağlayıcısı tarafından, anahtar çiftinin, kullanıcının kimliğinin ve bunların birbirine bağlantısının bulunduğu şekilde, sertifika hizmet sağlayıcısının gizli anahtarı ile dijital olarak imzalanması[72] sonucu gerçekleştirilir. Bu mühürleme işlemi *"sertifika"* olarak adlandırılır. Sertifika sayesinde, sertifika hizmet sağlayıcısının açık anahtarı ile dijital olarak imzalanmış ileti, bütünlük ve kimlik doğrulama açısından kontrol edilebilir. Bu durumda bu işlemlere katılan kişiler, sertifika hizmet sağlayıcısınca düzenlenmiş ve sertifika verilmiş verilerin, herhangi biri tarafından,

---

69 **Mertes,** s. 156-157.

70 **Şenocak,** s. 99; **Keser Berber**, s. 531.

71 **Mertes,** s. 157.

72 Sertifika hizmet sağlayıcılarının da kendilerine ait açık ve gizli anahtarları bulunmaktadır, böylece sertifika verebilmektedirler. Nitekim, nitelikli sertifikada bulunması gereken unsurlardan biri de sertifika hizmet sağlayıcısının sertifikada yer alan bilgilerini doğrulayan güvenli elektronik imzasıdır (EİK m.9/j).

fark edilmeksizin değiştirilmeyeceğine her zaman güveneceklerdir[73]. Bu güvenin sebebi, sertifika hizmet sağlayıcısının açık anahtarına olan güvendir. Sertifika, sağlayıcının imzasıyla mühürlendiğinden, bunun sonucunda, sağlayıcı olan üçüncü kişinin, imza sahibinin bilgilerini güvenilir şekilde tespit ettiği ortaya çıkmaktadır.

Sertifika hizmet sağlayıcılarının kendilerine ait bir veya birden fazla anahtar çiftleri bulunabilir. Sağlayıcının gizli anahtarının yetkili kişiler dışında kimsenin ulaşamayacağı ve kullanamayacağı şekilde saklanması gerekmektedir. Gizli anahtarın bilgisayarın sabit diskinde şifrelenmek suretiyle saklanması tercih edilebileceği gibi, saklamak için akıllı kartlar da kullanılabilir. Her sertifika hizmet sağlayıcısının bir kök kimliği vardır ve sağlayıcılar kök kimliklerini kamuya açarak liste hizmeti çerçevesinde ("directory services") herkesin ulaşabileceği yerlerde tutmalıdır[74]. Bunun sonucunda, bir sertifikanın verildiği hizmet sağlayıcısının kimliği kontrol edilebilecektir.

Sertifikasyon için kullanılan anahtarın üretilmesi bakımından da, anahtarın üretilmesi için gerekli koşulların yerine getirilmesi gerekir[75].

d. Liste Hizmetinin Verilmesi

Son adım olarak, bütün geçerli ve bloke edilmiş sertifikalar için liste hizmetinin verilmesi gerekir. Liste hizmeti, dikkat ve özen gösteren bir denetime ihtiyaç gösterir. Bu sistemin her zaman güvenli olması ve güvenli kalması gerekir. Örneğin, 24 saat bloke hizmeti verilmesi gereklidir. Kayıp anahtar araçlarının ya da bu şekildeki anahtar araçlarının kötüye kullanılma tehlikesinin mümkün olduğunca çabuk bloke edilmemesi ve bu durumun katılımcılarca bilinememesi halinde sistemde eksiklik olduğu söylenebilir[76].

Bloke listesi, sertifika numaralarını, bloke tarihini ve geçici bloke sebebini içerir. Bununla beraber, nitelikli sertifikanın geçerliliğinin de sertifika listesinde belirtilmesi gerekir, çünkü bloke listesi tek başına sertifikanın geçerlilik denetimi için yeterli değildir[77].

---

73 **Mertes,** s. 158.

74 http://e-kimlik.bilten.metu.edu.tr/net/teknik/ehs.jsp

75 **Mertes,** s. 158.

76 **Mertes,** s. 158.

77 **Brandner**, Ralf/**Pordesch**, Ulrich/**Rossnagel**, Alexander/**Schachermayer**, Joachim, Langzeitsicherung qualifizierter elektronischen Signaturen, DuD 26 (2002) 2, s. 100.

Bloke listesine alternatif olarak belirli sertifikalar bakımından online sertifika statü sorgulaması söz konusudur. OCSP (Online Certificate Status Protokol) üzerinden liste hizmetine online soru sorularak sertifikanın mevcudiyeti ve bir veya birden fazla sertifikanın geçerliliği konusunda bilgi edinilebilir. Bloke listesi ile OCSP üzerinden alınan cevap arasındaki farklılık, OCSP cevabında blokenin yanında mevcut olmayan sertifikaları da "*bilinmeyen*" olarak göstermesidir. OSCP cevapları elektronik olarak imzalanır ve böylece cevabın doğruluğu kontrol edilebilir ayrıca sürekli olarak saklanabilir[78].

V. SERTİFİKA HİZMET SAĞLAYICISININ DİĞER FAALİYETLERİ VE YÜKÜMLÜLÜKLERİ

Dijital imza usulünün bütün sistemi için yeterli güvenliğin sağlanması bakımından sertifika hizmet sağlayıcısı tarafından diğer hizmetlerin de sunulması gereklidir[79]. Asıl hizmeti ile birlikte bu yükümlü olunan hizmetler kısaca şunlardır:

- Sertifika hizmet sağlayıcısının gerek sertifika hizmet sağlayıcısı tarafından ve gerekse başvuru sahibinin kendisi tarafından üretilmiş olsun, anahtarın belirtilen uygun teknik bileşenler kullanılarak ve güvenli şekilde üretildiği konusunda tam bir kanaate sahip olması;
- Sertifika hizmet sağlayıcısının, başvuru sahibini güvenlik tedbirleri ve üretilen dijital imza hakkında bilgilendirmesi;
- Sertifika hizmet sağlayıcısının onun tarafından üretilmiş anahtar ve kişisel bilgilerin yetkili katılımcılara kişisel olarak iletilmesi;
- Talep üzerine dijital veriye zaman damgası eklemesi.

Kanunda sertifika hizmet sağlayıcısının elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayacağı belirtilmiştir (EİK m.8/I). Ayrıca, sağlayıcıların yükümlülükleri arasında da yukarıda

---

78 **Brandner**/**Pordesch**/**Rossnagel**/**Schachermayer**, DuD 26 (2002) 2, s. 100.

79 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Birliği Direktifi ("Elektronik İmzalar İçin Topluluk Çerçevesi") Ek II'de sertifika hizmet sağlayıcıları ile ilgili şartlarda bu hususlar ayrıntılı şekilde belirtilmiştir. Ayrıca bkz. **Rossnagel**, 5 SigG § 2, s. 2.22-2.23; **Bister**/**Rath** s. 96; **Keser Berber,** s. 529; **Keser Berber**, Şekil ve Dijital İmza, s. 98; **Keser Berber**-Elektronik Para ve Dijital İmza, s. 155; **Altınışık,** s. 86-87; **Göç Gürbüz**, s. 20.

belirtilen yükümlülükler sayılmış, bunlara ek olarak sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak (EİK m.8/II,c); hizmetin gerektirdiği nitelikte personel istihdam etmek (EİK m.10/I,a); sertifikanın kullanımına ilişkin özelliklerin ve güvenli elektronik imzanın elle atılan imzaya eşdeğer olduğunu imza sahibine bildirmek (EİK m.10/I,e); imza oluşturma verisini başkasına kullandırmaması konusunda imza sahibini uyarmak ve bilgilendirmek (EİK m.10/I,f); yaptığı hizmetlere ilişkin tüm kayıtları Yönetmelikte belirlenen süreyle saklamak (EİK m.10/I,g); üretilen imza oluşturma verisinin bir kopyasını almamak veya bu veriyi saklamamak (EİK m.10/II) gibi yükümlülükleri bulunmaktadır.

VI. SERTİFİKA HİZMET SAĞLAYICISININ FAALİYETE BAŞLAMASI

Elektronik İmza Kanununa göre, sertifika hizmet sağlayıcısı Telekomünikasyon Kurumuna yapacağı bildirimden iki ay sonra faaliyete geçer (EİK m.8/I). Hizmet sağlayıcı bu bildirimde, güvenli ürün ve sistemleri kullanmak (EİK m.8/II,a), hizmeti güvenilir bir biçimde yürütmek (EİK m.8/II,b), sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak (EİK m.8/II,c) ile ilgili şartları sağladığını ayrıntılı bir şekilde göstermelidir.

Kurum, sertifika hizmet sağlayıcısının 8. maddenin II. fıkrasında belirtilen ve güvenlikle ilgili olan şartların yerine getirilmediğini veya eksikliğini tespit ederse sertifika hizmet sağlayıcısına bir ayı geçmemek üzere eksikliğin giderilmesi için süre verir ve bu sürede sağlayıcının faaliyetlerini durdurur. Sürenin sonunda eksiklikler giderilmemişse sertifika hizmet sağlayıcısının faaliyetine son verilir (EİK m.8/III). Bu hükmün sertifika hizmet sağlayıcının faaliyetinin devamı sırasında uygulanması gerektiği gibi, sağlayıcının en başta faaliyete geçmek üzere Kuruma bildirimde bulunması zamanında da uygulanacağı açıktır. Bu durumda sertifika hizmet sağlayıcısının yaptığı bildirimde, eksiklik olduğu tespit edilirse, bildirimden itibaren henüz iki ay dolmamış olsa bile, eksikliklerin yerine getirilmesi için sağlayıcıya Kurum tarafından süre verilecektir. Ancak bu halde, henüz faaliyete geçmemiş bir sertifika hizmet sağlayıcısı söz konusu olduğu için faaliyetinin durdurulması da söz konusu olmayacaktır. Zira faaliyetin durdurulması için öncelikle geçerli bir şekilde faaliyete başlanmış olması gerekir.

Kanuna göre, sertifika hizmet sağlayıcıları faaliyetlerinin devamı süresince de 8. maddedeki şartları yerine getirmek zorundadırlar (EİK m.8/IV).

Bu sebeple sağlayıcılar her zaman Kurumun denetimine tâbi olacaklar ve şartlarda bir eksiklik tespit edilmesi halinde Kurumca süre verilmesi ve bu süre içinde faaliyetin durdurulması söz konusu olacaktır.

Alman İmza Kanunu (SigG) § 2 N.8'e göre, sertifika hizmet sağlayıcısı (Zertifizierungsdiensteanbieter), nitelikli sertifika veya nitelikli zaman damgası düzenleyen gerçek veya tüzel kişidir. Alman İmza Kanununa göre, 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Birliği Direktifine ("Elektronik İmzalar İçin Topluluk Çerçevesi") uygun olarak bir sertifika hizmet sağlayıcısı idari bir usule tâbi olmadan ve işletme için bir izin almaksızın sertifika hizmeti sunabilir. Sertifika hizmeti işletmesi, esasen izne tâbi değildir; bununla beraber en geç hizmete başlamasıyla beraber durumun yetkili makama (Almanya'da yetkili makam, (RegTP) Regulierungsbehörde für Telekommunikation und Post) bildirilmesi zorunludur. 1997 tarihli önceki Kanunda "izin" olarak belirtilen kavram, 2001 tarihli Kanun ile "ihtiyari akreditasyon" olarak değiştirilmiştir (§ 25 SigG). Bununla yeni Alman İmza Kanununa göre, ihtiyari akreditasyon tanımı altında yetkili makamdan, sertifika hizmet işletmesi için izin verilmesi anlaşılır. İzin ise özel hak ve yükümlülüklere bağlı hizmet için verilir. Akreditasyon, eğer sertifika hizmet sağlayıcısı, nitelikli sertifikaya dayanan nitelikli imza için İmza Kanununda belirtilen teknik ve kurumsal güvenliği sağladığını ispatlarsa yetkili makam tarafından verilir (§ 15 SigG). Bunun için kapsamlı araştırma yapılmış olmalıdır[80].

Alman İmza Kanununa göre sertifika hizmet sağlayıcıları ikiye ayrılır[81]:

1. Hiçbir usule tâbi olmayan sadece yetkili makama bildirilen sertifika hizmet sağlayıcısı
2. Yetkili makam tarafından akredite edilmiş sertifika hizmet sağlayıcısı

---

80 www.sit.fraunhofer.de/smartcard-ws/WS_02/Beitrag_Wohlmacher.pdf+zertifizierungsdiensteanbieter&hl=tr&ie=UTF-8

81 Sertifika hizmet sağlayıcısına göre elektronik imzalar üç sınıfa ayrılabilir. Buna göre III. sınıf imzalar, akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilen imzalardır. II.sınıf imzalar ise sadece yetkili makama bildirilmiş olan sertifika hizmet sağlayıcılarının vermiş oldukları imzalardır. I. sınıf imzalar ise akredite edilmemiş sertifika hizmet sağlayıcılarının vermiş oldukları veya yetkili makama bildirilmemiş sertifika hizmet sağlayıcılarının verdiği imzalar ya da kişilerin kendilerinin ürettikleri imzalardır (**Geis**, İvo, Die elektronische Signatur als Bestandteil rechtssicheren Geschaeftsverkehrs, in: **Geis**, İvo (Hrsg.), Die digitale Signatur- eine Sicherheitstechnik für die Informationsgesellschaft, Eschborn, 2000, s. 168-169).

Her iki halde de sağlayıcı, Alman İmza Kanunu § 12'ye göre, kanuni yükümlülükleri sebebiyle ortaya çıkacak zararların karşılanması amacıyla istenen teminatı yatırmalı, uygun branş bilgisini ispat etmeli ve uygun güvenlik tasarısı (Sicherheitskonzept) sunmalıdır. Yetkili makamdan akreditasyon almak isteyen sertifika hizmet sağlayıcısının, bunun için tanınmış bağımsız bir kontrol ve onay kurumundan, teknik ve kurumsal güvenliğinin ve kanuni hükümlere riayetinin, kapsamlı olarak kontrol edilmesi ve onaylanması gerekir. Güvenlik kontrolü, sertifika hizmeti işletmesinin yazılı güvenlik tasarısını ve bu güvenlik tasarısının pratikte gerçekleşip gerçekleşmediğinin kontrolünü de kapsar[82]. Yetkili makam, sertifika hizmet sağlayıcısının, İmza kanununun gerektirdiği şartları ileride de sağlayıp sağlamadığı konusunda denetim tedbirlerini yürütür (§ 15 SigG).

Alman Hukukunda, bir sertifika hizmet sağlayıcısı, akredite edilmeyi amaçlamıyor, aksine sadece işletmeye başladığını bildirmekle yetiniyorsa güvenlik tasarısının nasıl gerçekleştirileceği konusunda yetkili makama (Reg TP) tam bir açıklama sunmalıdır. Sertifika hizmet sağlayıcısının, bu güvenlik tasarısına dayanarak İmza Kanununa göre talep edilen ve sertifika hizmet sağlayıcısı tarafından iddia edilen güvenliğe ulaşıp ulaşılmadığı yetkili makam tarafından denetim tedbirleri çerçevesinde belirlenir[83].

Alman İmza Kanununda, sertifika hizmet sağlayıcısının en geç işletmeye başlamasıyla birlikte yetkili makama bildirimde bulunacağı düzenlenmiştir (§ 4 Abs.3 SigG; aynı şekilde Avusturya İmza Kanunu § 6 Abs.2 SigG). Bu bildirimde gerekli yeterliliğe ve branş bilgisine sahip olduğunu, teminatı yatırdığını ve bu Kanun ve Yönetmelikte belirtilen bütün koşulları yerine getirdiğini belirtmelidir (§ 4 Abs.2-3 SigG; aynı şekilde Avusturya İmza Kanunu § 6 Abs.2-3 SigG). Bunun dışında gereken koşulları işletmenin devamı süresince taşımayı garanti etmelidir (§ 4 Abs. 4 SigG; aynı şekilde Avusturya İmza Kanunu § 6 Abs.4 SigG).

Elektronik ticaretin yaygınlaşması bakımından, aynı ülkede veya farklı ülkelerde bulunan elektronik sertifika hizmet sağlayıcıları arasındaki iletişimin de sağlanması gereklidir. Böylece herhangi bir ülkedeki sağlayıcının

---

82 www.sit.fraunhofer.de/smartcard-ws/WS_02/Beitrag_Wohlmacher.pdf+zertifizierungsdiensteanbieter&hl=tr&ie=UTF-8

83 www.sit.fraunhofer.de/smartcard-ws/WS_02/Beitrag_Wohlmacher.pdf+zertifizierungsdiensteanbieter&hl=tr&ie=UTF-8

sertifika sahiplerinin, başka bir sağlayıcının sertifika sahipleri ile ayrıca başka bir ülkenin sertifika sahipleri arasında güvenli iletişim yapılabilecektir[84].

VII. GÜVENLİ İMZA OLUŞTURMA ARAÇLARININ NİTELİK (UYGUNLUK) DEĞERLENDİRMESİNİ YAPAN KURUMLAR

İmza oluşturma aracı, elektronik imza oluşturmak üzere, imza oluşturma verisini[85] kullanan "*yazılım veya donanım aracı"*nı ifade eder (EİK m.3/e; Avrupa Birliği Direktifi, Art.2/5; Alman İmza Kanunu, § 2 N.10). Elektronik imzaya tanınan hukuki sonucun doğması için elektronik imzanın güvenli elektronik imzanın şartlarını taşıması gerekir (EİK m.5). Güvenli elektronik imzanın şartlarından birisi de güvenli elektronik imza oluşturma aracı ile oluşturulmasıdır (EİK m.4/b).

Güvenli elektronik imza oluşturma araçları (EİK m.6; Avrupa Birliği Direktifi, Ek III; Alman İmza Kanunu § 17) :

- Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
- Ürettiği elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
- İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan imza oluşturma araçlarıdır.

Sertifika hizmet sağlayıcısının, sertifika verirken imza oluşturma araçlarının belirtilen uygun teknik bileşenler kullanılarak ve güvenli şekilde üretildiği konusunda tam bir kanaate sahip olması gerekir (Alman İmza Kanunu, § 5 N.6). Çünkü imza oluşturma araçlarının mutlaka sertifika hizmet sağlayıcısı tarafından üretilmesi gerekli değildir.

---

84 **Miccoli,** s. 222-223.

85 İmza oluşturma verisi, imza sahibine ait olan imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri ifade eder (EİK m.3/d).

Sertifika hizmet sağlayıcısı tarafından üretilen elektronik imzalarda da yukarıda belirtilen şartların gerçekleşmesi gerektiği gibi, imza sahibi tarafından üretilmiş olan imzalar bakımından da aynı şartların sağlanması gerekmektedir.

Avrupa Birliği Direktifinden anlaşıldığına göre, sertifika hizmet sağlayıcılarından başka, imza oluşturma araçlarının nitelik (uygunluk) değerlendirmesini yapan kurumların da mevcut olması mümkündür. Bu durumda, sertifika hizmet sağlayıcılarının, kendileri tarafından üretilmemiş olan imzalara olan güvenin sağlanması bakımından bu değerlendirme gerekli olacaktır. Bu kurumlar, kimlik tespiti konusunda yetkili olmayacaklar, sadece güvenli elektronik imza oluşturma araçlarının nitelik (uygunluk) değerlendirmesi konusunda faaliyet göstereceklerdir. Sertifika hizmet sağlayıcılarının ise bu anlamda hem sertifika hizmeti sunması, hem de güvenli elektronik imza oluşturma araçlarını değerlendirmesi mümkündür; bu halde ise uygunluk değerlendirmesinin ayrıca yapılmasına gerek olmağı sonucuna varılabilir. Görüldüğü üzere uygunluk değerlendirmesi yapan bu kurumlar sertifika hizmet sağlayıcılardan farklıdırlar.

13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Birliği Direktifinin 3. maddesinin 4. fıkrasında güvenli imza oluşturma araçlarının Ek III'te belirtilen kurallara uygunluğunun, üye devletler tarafından, yetkili özel veya kamu nitelikli kurumlar aracılığıyla belirleneceği düzenlenmiştir. Komisyon, 9. maddede öngörülen usule uygun olarak, üye devletlerin bir kurumu belirlemekte kullanacağı kriterleri tespit eder. Bu kurumlar tarafından Ek III'te belirlenen şartlara uygunluk konusunda yapılan bir saptama, tüm üye devletler tarafından tanınacaktır. Bu kriterleri belirleyen 6 Kasım 2000 tarihli, 2000/709/EG sayılı bir Komisyon Kararı mevcuttur. Bu kararın amacı, üye ülkelerin, güvenli elektronik imza oluşturma araçlarının nitelik (uygunluk) değerlendirmesini yapacak yetkili kurumların belirlenmesi sırasında dikkat edilmesi gerekli kriterlerin belirlenmesidir (Karar m.1). Bu karar çalışan personel, kurumun faaliyeti ve gerekli güvenliğin sağlanması bakımından bir takım kurallar koymaktadır. Bu karar, bütün üye ülkelere yöneltilmiştir (Karar m.12) Kısaca bu kriterleri şu şekilde belirtmek mümkündür:

- 1999/93/AT Direktifinin III no'lu ekinde belirtilen şartlar ile güvenli elektronik imza oluşturma araçlarının nitelik değerlendirmesi dışında başka faaliyetlerde bulunan ve organizasyonun bir parçası olan

belirlenmiş kurum, bu organizasyon içinde açıkça tanınmış olmalıdır. Değişik faaliyetleri açıkça ayırt edilebilir olmalıdır (Karar m.2).

- Kurum ve personeli, onların bağımsız karar verme iktidarını ve kendilerine verilen (onlara yüklenmiş) görevlerin yürütülmesi sırasındaki dokunulmazlıklarını etkileyebilecek nitelikte, başka bir meslek icra edemezler. Özellikle kurum, katılımcı taraflardan bağımsız olmalıdır. Bu sebeple Kurumda, işletme müdürü ve nitelik değerlendirmesi için yetkili personel ne güvenli elektronik imza oluşturma aracını geliştirenler (Entwickler), bu aracın üreticileri, teslimatçıları (Lieferant) veya bunu kuranlar ne de kamuya sertifika düzenleyen sertifika hizmet sağlayıcıları veya tarafların tam yetkili temsilcileri olamaz (Karar m.3/I).
- Bundan başka, Kurum ve personeli bağımsız olmalıdır, ne doğrudan güvenli elektronik imza oluşturma araçlarının geliştirilmesi, yapımı, pazarlaması veya bakım/muhafazasına katılabilirler ne de burada belirtilen tarafları temsil edebilirler. Bu durum üretici ve kurum arasında teknik bilgi alışverişini kapsamaz (Karar m.3/II).
- Kurum ve personeli, 1999/93/AT Direktifinin III no'lu ekinde belirtilen şartlarda güvenli elektronik imza oluşturma araçları konusundaki anlaşma ile belirlenen yüksek derecede mesleki dürüstlük, güvenilirlik ve yeterli teknik bilgiye sahip olmalıdır (Karar m.4).
- Kurum, şeffaf bir nitelik değerlendirmesi uygulaması ve bu uygulama ile bağlantılı kapsamlı belgeleme hizmeti verir. Taraflar Kurumun hizmetlerine girebilmelidirler. Kurumun çalışma metodları ayırımcı olamaz (Karar m.5).
- Kurum, kurum için belirlenmiş, görevlerinin yürütülmesinde (tasfiyesinde) teknik ve idari ölçüler çerçevesinde usulüne uygun ve gecikmeksizin görevini yürütmek için gerekli personel ve gerekli donanıma sahip olmalıdır (Karar m.6).
- Nitelik değerlendirmesi için görevli personelin aşağıda belirtilen şartları tamamlaması gerekir:
  - Özellikle elektronik imza teknolojisi ve bununla bağlantılı güvenli bilgi teknolojisi alanında temel alansal ve mesleki eğitim;

- Bu tür değerlendirmelerin yürütülmesi için yeterli tecrübe ve nitelik değerlendirmeleriyle bağlantılı şartlarda yeterli bilgi. (Karar m.7).

- Personelin bağımsızlığı temin edilmiş olmalıdır. Ücret, ne yürütülen nitelik değerlendirmelerinin sayısına ne de nitelik değerlendirmelerinin sonuçlarına bağlı olmalıdır (Karar m.8).
- Kurum, faaliyeti çerçevesinde üstlendiği sorumluluğun karşılanması için gerekli tedbirleri almalıdır. Örneğin yeterli bir sigortanın yapılması gibi (Karar m.9).
- Kurum, bilgilerin gizliliğinin temini için, 1999/93/AT Direktifi çerçevesinde üstlenilen görevlerin gerçekleştirilmesinde veya Direktife uyum sağlamak için tek tek ülkelerin çıkardığı hukuki düzenlemelerde belirtilen, uygun tedbirleri alır (Karar m.10).
- Nitelik değerlendirmesinin bir bölümünün yürütülmesi ile bir başka kuruluş görevlendirilirse Kurum, bu tarafın ilgili hizmetlerin gerçekleştirilmesine ilişkin olarak ehil olduğunu garanti edebilir ve ispatlayabilir. Tayin edilen Kurum, bu tür anlaşmalarla yürütülen çalışmalar çerçevesinde sınırsız sorumluluk taşır. Son karar konusunda külfet belirlenen kuruma aittir (Karar m.11).

SONUÇ

Elektronik hukuki işlemlerde güven unsuru olarak karşımıza çıkan, işlem yapan kişilerin kimlik tespitini mümkün kılmak üzere elektronik sertifika hizmet sağlayıcısı, elektronik imza altyapısı içinde bu görevi üstlenmiştir.

Sertifika hizmet sağlayıcısı, imza sahibi kişinin kimliğini güvenli şekilde tespit ederek, bu kimlik ile -gerek kendisi tarafından üretilmiş ve gerekse imza sahibi tarafından üretilmiş olsun- elektronik imzanın anahtar çiftini, teklik ilkesi çerçevesinde birbirine bağlar. Bu bağlantının, sürekli şekilde taklit ve tahrifata karşı elektronik olarak korunması için sertifika hizmet sağlayıcısının kendi elektronik imzasıyla "*mühürlenmesi*" gerekir. Bu durumda sağlayıcının en önemli fonksiyonu olan sertifikasyon gerçekleştirilmiş olur.

Sertifika hizmet sağlayıcısının işleteni gerçek kişi olabileceği gibi, tüzel kişi veya kamu kurum veya kuruluşu da olabilir (EİK m.8). Sertifika hizmet sağlayıcısı, sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlar. Bu anlamda sertifika hizmet sağlayıcısının elektronik imzanın güvenli

işleyişini gerçekleştirebilmek için gerekli önlemleri alması, bunun yanında her zaman ulaşılabilir liste hizmeti ve bloke hizmeti vermesi de gereklidir. Ayrıca sağlayıcı, imza sahiplerini elektronik imzanın kullanımı, saklanması konusunda almaları gereken güvenlik önlemleri konusunda uyarmak ve elektronik imzanın gerekli koşulları taşıması halinde, hukuki işlemlerde elle atılan imzaya eşdeğer olduğunu belirtmekle yükümlüdür.

Hukuki işlemlerde geçerli olarak kullanılacak güvenli elektronik imzanın nitelikli elektronik sertifikaya dayanması zorunludur. Nitelikli elektronik sertifika ise sadece Kanuna göre kurulmuş ve faaliyette bulunan sertifika hizmet sağlayıcısı tarafından verilebilir.

Sertifika hizmet sağlayıcısının faaliyetine başlaması için Kanunda da belirtildiği şekilde ve Avrupa Birliği Direktifine uygun olarak herhangi bir kurumdan izin alınmasına gerek yoktur. Bu konuda bildirim sisteminin geçerli olduğu söylenmelidir. Sertifika hizmet sağlayıcısı, Telekomünikasyon Kurumuna yapacağı bildirimden iki ay sonra faaliyete geçer (EİK m.8/I). Bildirimde, güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir biçimde yürütmek ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri sağladığını ayrıntılı şekilde gösterir. Aynı şekilde, sertifika hizmet sağlayıcıları faaliyetlerinin devamı sırasında da bu şartları taşımalıdır.

Sertifika hizmet sağlayıcısının asıl görevi *sertifikasyon*dur. Bundan başka sertifika hizmet sağlayıcılarından farklı olarak, görevleri sadece imza oluşturma araçlarının nitelik (uygunluk) değerlendirmesi olan kurumlar da mevcuttur. Avrupa Birliği Direktifinde belirtildiği üzere, bütün üye ülkelerin uyacağı şekilde, sertifika hizmet sağlayıcılarından başka, imza oluşturma araçlarının nitelik (uygunluk) değerlendirmesini yapan kurumların mevcudiyeti halinde, sertifika hizmet sağlayıcılarının, kendileri tarafından üretilmemiş olan imzalara olan güvenin sağlanması bakımından bu değerlendirme gerekli olacaktır. Sertifika hizmet sağlayıcılarının sertifika hizmeti sunması yanında, güvenli elektronik imza oluşturma araçlarını değerlendirmesi mümkün olmalıdır, bu halde ise uygunluk değerlendirmesinin başka bir kurum tarafından ayrıca yapılmasına gerek olmağı sonucuna varılabilir.

K a y n a k ç a

Acır, Birsen, Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, Sermaye Piyasası Kurulu, Yeterlilik Etüdü, Ankara 2000.

Altınışık, Ulvi, Elektronik Sözleşmeler, Ankara 2003.

Arıkan, A. Saadet, Elektronik Ticaret, Hukuk ve Noterler, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 13-52.

Arıkan, A. Saadet, Modern İletişim Araçları ve Özel Hukuk, in:Hukuk Kurultayı 2000, Ankara 2000, s. 307-333. (Kısaltma: Kurultay)

Bafra, Jale, El Yazısı ve İmza İncelemesi Alanında Karşılaşılan Güçlükler, Standardizasyon ve Güvenilirlik, İBD 1997/3, s. 529-538.

Bister, Jörg/**Rath,** Marco, Gesellschaftsrechtliche Fragen bei der Gründung einer Zertifizierungsstelle, in:Hoeren Thomas/Schüngel Martin, Rechtsfragen der digitalen Signatur, Berlin 1999, s. 93-126.

Brandner, Ralf/**Pordesch**, Ulrich/**Rossnagel**, Alexander/**Schachermayer**, Joachim, Langzeitsicherung qualifizierter elektronischen Signaturen, DuD 26 (2002) 2, s. 97-103.

Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Raportör: Avniye Tansuğ, Şubat 2002.

Fritzsche, Jörg/ **Malzer,** M.Hans, Ausgewaehlte zivilrechtliche Probleme elektronisch signierter Willenserklaerungen, DnotZ 1995, s. 3-25.

Geis, İvo, Die elektronische Signatur als Bestandteil rechtssicheren Geschaeftsverkehrs, in: **Geis**, İvo (Hrsg.), Die digitale Signatur- eine Sicherheitstechnik für die Informationsgesellschaft, Eschborn, 2000, s. 155-169.

Göç Gürbüz, Diğdem, Elektronik Ticarette Hukuki Yapı ve Yasal Düzenlemeler, Mükellefin Dergisi, 2000/95, s. 13-22.

Hohenegg, Christoph/**Tauschek,** Stephan, Rechtliche Problematik digitaler Signaturverfahren, BB 1997, s. 1541-1548.

Keser Berber, Leyla, "İmzalıyorum O Halde Varım" Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri, TBBD 2000/2, s. 503-556.

Keser Berber, Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Ankara 2002. (Kısaltma: Elektronik Para ve Dijital İmza)

Keser Berber, Leyla, Şekil ve Dijital İmza, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 53-157.(Kısaltma: Şekil ve Dijital İmza)

Köhler, Helmut, Die Problematik automatisierter Rechtvorgaenge, insbesondere von Willenserklaerungen, AcP 182 (1982), s. 126-171.

Meinel Cristoph/**Gollan** Lutz, Der elektronische Personalausweis?, JurPC Web-Dok 223/2002.

Melullis, Klaus-J, Zum Regelungsbedarf bei der elektronischen Willenserklearung, Monatsschrift für Deutsches Recht (MDR) 1994/2, s. 109-114.

Mertes, Paul, Digitale Signatur-Wertlos ohne Trust Center, in: **Glade**, Albert/**Reimer,** Helmut/**Struif,** Bruno (Hrsg.), Digitale Signatur & Sicherheitssensitive Anwendungen, Braunshweig/Wiesbaden 1995, s. 153-162.

Mertes, Paul/**Zeuner**, Volker, Digitale Signatur und Signaturgesetz, in:**Hoeren** Thomas/**Sieber** Ulrich (Hrsg.), Handbuch Multimedia-Recht, München 2002, Teil 13.3.

Miccoli, Mario, Teknolojik Açıdan Elektronik Ticaret (Çev. Günal, Nadi), in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 205-223.

Orta, Mesut, Ulusal Yargı Ağı Projesinde Elektronik İmza, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 159-174.

Pekcanıtez, Hakan, Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslar arası İnternet Hukuku Sempozyumu, İzmir 2002, s. 389-427.

Pütmann, F.Frank/**Sander**, Matti, Internationale Signaturgesetze im Vergleich, in:**Hoeren** Thomas/**Schüngel** Martin, Rechtsfragen der digitalen Signatur, Berlin 1999, s. 385-425.

Rossnagel Alexander, Recht der Multimedia Dienste, München 2001.

Schmidl, Michael, Die elektronische Signatur, CR 7/2002, s. 508-517.

Schreiber, Lutz, Digitale Signaturen im Rechtsverkehr, Hamburg 1999.

Sevimli, Ahmet, Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası, Prof. Dr. Hayri Domaniç'e 80. Yaş günü Armağanı, C.II, İstanbul 2001, s. 1023-1041.

Sözer, Bülent, Elektronik Sözleşmeler, İstanbul 2002.

Şenocak, Zarife, Dijital İmza ve Dijital İmzanın Borçlar kanunun Hükümleri Açısından Ele Alınması, AÜHFD C.50 S.2 2001, s. 97-135.

Turan, Orhan, Noterlik işlemler ve Elektronik, in: Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s. 187-203.

Yaltı, Billur, E-İmza ve E-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-I, Vergi Sorunları, Nisan 2001, S.151, s. 127-135.

Yaltı, Billur, Elektronik Ticarette Vergilendirme, İstanbul 2003.