

“İMZALIYORUM O HALDE VARIM” DİJİTAL İMZA, DİJİTAL İMZA HAKKINDAKİ YASAL DÜZENLEMELER, DİJİTAL İMZALI ELEKTRONİK BELGELERİN HUKUKİ DEĞERİ

Yrd. Doç. Dr. Leyla Keser BERBER (*)

GİRİŞ

Dijital imza, el yazısı ile atılan imzanın sahip olduğu özellikleri, elektronik belgeler alanında sağlamaya çalışan bir yöntemdir. Şifreleme yöntemleri sayesinde, elektronik olarak imzalanan bir belgenin, sadece elektronik imzanın sahibi olan kimse tarafından düzenlendiği tespit edilebilmektedir. Dijital imzanın taklit edilmesi çok zordur ve ayrıca dijital imzanın kaynağı da (yani kimin tarafından atıldığı) şüpheye yer bırakmayacak bir şekilde ispatlanabilmektedir (1). Ancak dikkat edilecek olursa, bu konuda kesin ifadeler kullanmaktan sürekli kaçınmaktayız. Çünkü; günümüzde bir çok şirketin web sayfalarının taklit edildiği, Hacker'ların kol gezdiği bir internet ortamında, dijital imzanın % 100'e yakın bir garanti temin edeceğini düşünmek, kanımca sanal bir beklenti olacaktır.

Bu açıklamalar ışığında, dijital imzaya ilişkin olarak bilgi ağı üzerinde çözmemiz gereken dört sorun vardır:

(*) İstanbul Bilgi Üniversitesi Hukuk Fakültesi Medeni Usul Hukuku ve İcra İflas Hukuku Öğretim Üyesi

(1) " Sicherheit-Die elektronische Unterschrift ", <http://www.hypowelt.de/info/unterschrift.htm>, s. 1.

- GERÇEKLİK
- ORJİNALLİK
- GÜVENİLİRLİK
- DİJİTAL İMZANIN KAYNAĞINA İTİRAZ EDİLEMESİ(2)

Hukuken bağlayıcı olan her işlemde olduğu gibi, Elektronik Ticaret (e-Commerce) için de, internet üzerinden yapılan irade beyanlarının ispatlanabilmesi çok büyük bir önem taşımaktadır (3). Sözleşmenin kuruluş aşamasında olduğu kadar sözleşmenin ifası aşamasında da, normal hukuk yaşantımızda alışık olmadığımız sorunların ispatlanması gerekecektir (4). Örneğin; bugün internet üzerinden yapılan sözleşmelerin ifasında ödeme vasıtası olarak artık sadece, çek, kredi kartları, havale vs. değil, "**Dijital (veya Elektronik) Para**" (5) da kullanılmaktadır.

-
- (2) " Elektronische Unterschrift?", Recht im Internet, <http://www.mbnet-key.ch/sgnrecht4.htm>, s. 1.
 - (3) Bizer, Johann/Fox, Dirk; " Digital Signierte Zukunft ". Datenschutz und Datensicherheit (DuD) 1997, s. 66.
 - (4) Elektronik sözleşmeler hakkında bkz. Özsunay, Ergun: " ELEKTRONİK SÖZLEŞMELER - AB Hukuku ile Avusturya ve Alman Hukuklarındaki Gelişmelerin Işığında Türk Hukukuna İlişkin Çözümler - ". AB'de, Bazı Üye Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları - Elektronik Sözleşmeler -" konulu Konferans'da sunulan Tebliğ, 12 Mayıs 2000, İstanbul (henüz yayımlanmamıştır).
 - (5) **Dijital Para** ile, diğer elektronik ödeme vasıtalarının (çek, kredi kartları, EFT (Elektronik Fon Transferi)) aksine, dijital olarak sembolize edilmiş bir ödeme aracının (paranın) üçüncü bir kişinin (örneğin; bir Bankanın) araya girmesine gerek olmadan, bir kişiden diğerine transfer edilmesi kastedilmektedir (Beutelspracher, s. 155 vd.; Grämlich, Ludwig; " Elektronisches Geld " im Recht. Datenschutz und Datensicherheit (DuS) 1997, s. 383-389; Schneier, s. 165 vd.; Petersen, Holger; Anonymes elektronisches Geld. Der Einfluss der blinden Signatur. Datenschutz und Datensicherheit (DuD) 1997, s. 403-410; Knorr, Michael/Schlaeger, Uwe; Datenschutz bei elektronischem Geld. Ist das Bezahlen im Internet Anonym?. Datenschutz und Datensicherheit (DuD) 1997, s. 396-402; Herreiner, Dorothea K.; Die volkswirtschaftliche Bedeutung elektronisches Geldes. Datenschutz und Datensicherheit (DuD) 1997, s. 390-395). Sistemin bu şekilde işlemesi, internette ger

Bu çalışmada, sadece bilgisayar uzmanlarının değil, aynı zamanda hukukçuların da dikkatini çeken dijital imza konusu gerek teknik gerekse hukuki açıdan açıklanmaya çalışılmıştır. Konuya açıklık getirmesi bakımından güncel dijital imza programlarına kısaca değinilmiş; daha sonra ise dijital imzalı elektronik belgelerin olası bir uyuşmazlıkta delil olarak değeri tartışılmıştır.

I. GENEL BİLGİ

Bilgi ve İletişim teknolojisi alanında son yıllarda yaşanan baş döndürücü gelişme, sadece cesur beklentileri gerçekleştirmekle kalmamış, bilakis yeni olanaklara da geniş bir kapı açmıştır. Örneğin bu olanaklardan internet, hemen hemen herkes tarafından kullanılmakla birlikte, bir çok kişi, internet ile hangi alanlarda ne gibi imkanlara sahip olabileceklerini tahmin edememektedir.

çek bir ticari alt yapının oluşturulması bakımından önemli bir özelliktir (*Petersen*; s. 403). Dijital paranın sanal ortamda kullanılabilmesi için, bazı şartları yerine getirmesi gerekmektedir. Para bilgisayar ağı üzerinden transfer edilebilmeli, kopyalanamamalı ve sonra tekrar kullanılabilmelidir. Ödeme yapmak için merkezi bir ağı bağlantının mevcut olmaması gerekir. Bunun yanı sıra, dijital paranın kullanımının yaygınlaştırabilmesi için; kullanışı kolay, her yere yerleştirilebilir, hesaplı, sağlam bir sistem kurulması da önemlidir. **ELEKTRONİK PARA BORSASI** olarak adlandırılan ve uygulama alanını bilgisayar ağlarının dışında, günlük yaşamda da bulması gereken sistem ise; müşterileri tarafından benimsenmek için, normal peşin para karşısında, kullanıcılarına daha fazla avantajlar sağlamak zorundadır. Bunlar arasında; Kayıp toleransları, ödemelerin makbuza bağlanması, ödemelerin iptal edilmesi; farklı para birimleri arasında para değişiminin yapılması örnek olarak sayılabilir (*Petersen*, s. 403- 404). Bu taleplerin çoğunu veya tamamını yerine getirebilecek ve bu suretle prensip olarak uygulamadaki değişimi ile uyuşabilecek son derece karmaşık şifreleme protokolleri mevcuttur (*Petersen*, s. 403, 406 vd.; *Schneier*, s. 174; Şifreleme protokolleri, ilk bakışta bir bilgisayar ağı içinde kesinlikle çözülemeyeceğini düşündüğümüz bir çok problemin çözümünde kullanılabilir. Bu tür protokollere birkaç örnek verecek olursak; bir sırrın birden çok kimse arasında paylaşılması, eş zamanlı sözleşme imzalanması, eş zamanlı gizli bilgi alış veriş, yerel seçimlerin güvenli bir şekilde gerçekleştirilmesi (örneğin; Costa Rica'da 2002 yılı ulusal seçimleri internet üzerinden yapılacaktır, <http://www.intern.de/97/22/29.shtml>) gibi.

Henüz birkaç yıl öncesine kadar network çalışmaları, dışarıya kapalı sistemlerle yapılmaktaydı. Çünkü; ya doğrudan doğruya ya da network işletmesindeki telefon ağı sayesinde gizli dinleme mümkündü. Fakat zaman içinde uzak mesafelere bir işlem ağı ile bağlanmak ve işini evden halletmek artık sorun olmamaya başlamıştır. Ancak bu durum güvenlik açısından yeni bakış açılarının doğmasına yol açmıştır.

Örneğin; bilgisayar vasıtasıyla haberleştiğimiz kişinin, gerçekten o kişi olup olmadığından nasıl emin olabiliriz? Veya herkesin kullandığı iletişim ağını kullanarak gönderdiğimiz bir mesajın, bu işlem sırasında, yani alıcıya giden yolda başkaları tarafından okunmadığına ve değiştirilmediğine nasıl inanabiliriz (6)? İşte bu her iki husus, güvenlik altyapısına yönelik olan yeni taleplerin sadece küçük bir bölümünü oluşturmaktadır.

Bu talepler sayesinde, güvenli haberleşmeye duyulan büyük bir gereksinim ortaya çıkmıştır. Söz konusu güvenlik gereksinimi kriptografi (şifreleme) ve dijital imza ile sağlanmaya çalışılmaktadır. Kavram olarak kriptografi, okunabilir durumdaki bir bilginin, kimsenin okuyamayacağı bir bilgi haline dönüştürülmesidir. Bu süreçte bilgi, ilgili alıcı kimse dışında, hiç kimsenin okuyamayacağı veya değiştiremeyeceği bir şekilde kodlanmaktadır (şifreleme). Şifreleme veya mesajı deşifre etmek için, bir algoritmaya (matematiksel bir formüle) ve bir anahtara ihtiyaç vardır. Anahtar, dijital imzanın ya da şifreli mesajın oluşturulması için yazıya eklenmiş basit bir sayıdır (7). Kriptoloji veya şifreleme bilimi, matematiğin

(6) <http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>, Das aktuelle Thema: Die elektronische Unterschrift, Informationsbrief 2/97, s. 1.

(7) Bauer, Friedrich L.; Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie, 1. Auflage, Berlin 1995; Beutelspracher, Albert; Kryptologie, 5. Auflage, Braunschweig/Wiesbaden 1996 (İnternet adresi: <http://www.uni-giessen.de>; Bizer, Johann; Rechtliche Bedeutung der Kryptographie. Datenschutz und Datensicherheit (DuD) 1997, s. 203-208; http://www.global-sign.com.tr/195.207.49/generel/en/faqsg_body.htm.

alt dallarından biridir (8). Kriptografi, belgelerin muhatapları dışındaki kimseler tarafından okunmasını engellemekte; dijital imza ise, birbiri ile haberleşen tarafların kimliklerini ispat etmeye yaramaktadır. Bunlardan özellikle dijital imza, son zamanlarda hukukçuların da dikkatini çekmiştir. Dijital imza konusunda Matematik ve Data İşleme Şirketi (GMD) tarafından, " *Elektronik İmza Prosedürü Hakkında Mevcut Durum* " başlıklı bir çalışma (9); Federal Noterler Odası tarafından, TeleTrust Deutschland işbirliği ile düzenlenen " *Elektronik Hukuki İlişkiler* " konulu bir Forum (10) gerçekleştirilmiştir. Gerçekte sadece dijital bir kaşeden ibaret olan dijital imza, açık bilgi ağlarında mesajların güvenilir bir şekilde transferini sağlamak şeklinde büyük bir olanak yaratmıştır (11). Bunun dışında şifrelenen bir mesajın ilave olarak bir de dijital imza ile imzalanması, mesajın doğruluğunu da garanti etmektedir (12). Diğer bir ifade ile, dijital imzanın;

- **Amacı:**

- ➔ Kimliği belirlenebilir bir kişinin

- ➔ Mevcut bir Belgenin

görüldüğünü ve imza edildiğini, ispat edilebilir şekilde garanti etmektedir.

- **Gerektirdiği Hususlar:** Gerçeklik ve orijinallliği gerektirir.

Dijital imzanın sahip olması gereken diğer unsurlar, aşağıda Dijital İmza Kanununun yardımıyla açıklanacaktır (13).

(8) Schneier, Bruce; *Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in Computer*. Almanca tercümesinin 1. Basısı, Bonn 1996; Telesec: Kryptokontrolle, 9 August 1996, <http://www.telesec.de/recht3.htm>.

(9) GMD-Veröffentlichung, St. Augustin 1992.

(10) Elektronischer Rechtsverkehr, Digitale Signaturverfahren und Rahmenbedingungen, Bundesnotarkammer (Hrsg.), Köln 1995.

(11) "Die elektronische Unterschrift", Net Investor, 1998/1, s. 15 vd.

(12) <http://www.ec-guide.com/technologien/16-1-5-2-Signatur.asp>.

(13) Bkz. aşağıda s. 5.

Dijital imza kullanımında, Kimlik Tespit Etme olarak adlandırılan durum için, smartcard (akıllı kart) ve pin gereklidir. Ancak, pin – pin enflasyonu, kullanıcıların doğum tarihi ve benzeri kişisel bilgilerin talep edilmesi şeklindeki operasyonel zayıflıklar yüzünden, kullanıcının kimliğinin kesin bir şekilde tespit edilebildiğinden bahsetmek güçtür. Dijital imza ile ilgili bir çok çalışmada ise bu konudan şimdiye kadar ya hiç bahsedilmemiş veya bu konu unutulmuştur (14).

Aşağıda önce, Alman Parlamentosu tarafından, dijital imzanın hukuki açıdan bağlayıcılığının esası olarak 11.6.1997 yılında kabul edilen, *Bilgi ve İletişim Hizmetlerinin Çerçeve Şartlarının Düzenlenmesi Hakkındaki Kanunun* (15), 3. Paragrafında düzenlenen *Dijital İmza Kanunu* (16) incelenecektir. Bu kanundan başka, Almanya'da ayrıca 8.10.1997 tarihli bir de *Dijital İmza Yönetmeliği* yürürlüktedir (17). Avrupa Topluluğu Telekomünikasyon Bakanlığı Kurulu da 30 Kasım 1999 tarihinde, Topluluğa üye ülkelerde Elektronik İmzanın Kabulünü gerçekleştirmeyi hedefleyen yeni bir Yönergeyi oy birliği ile kabul etmiştir. Bu Elektronik İmza Yönergesi, Avrupa Topluluğu çerçevesinde elektronik ticaretin gelişmesi bakımından çok önemli bir adımdır. Geçmişte sadece el yazısı ile atılan imza uluslararası alanda kabul görmekte ve hukuki sonuç doğurmaktaydı. Söz konusu Yönerge, aynı zamanda bu kuralı elektronik imzaların da kabul edilmesi şeklinde genişletmiştir. Yine bu Yönerge ile birlikte, Avrupa'da elektronik ticaretin hızlı bir

-
- (14) <http://www.provet.org/bib/mmge/er-gb.htm>; Kimlik Tespit Etme olarak adlandırdığımız bu işlemin amacı, bir kişinin gerçekten o kişi olduğunun gerekirse parmak izi, retina tarama yöntemi veya ses tahlilleri yardımıyla tartışmaya yer bırakmayacak şekilde tespit edilmesidir (<file://A:\a4.htm>).
- (15) Bilgi ve İletişim Hizmetleri Kanunu (Informations- und Kommunikationsdienste-Gesetz-IuKDG, 13. 7.1997 (<http://www.iid.de/rahmen/iukdgbt.html>), s. 1-16.
- (16) Signaturgesetz-SigG (<http://www.iid.de/rahmen/iukdgbt.html>), s. 5-10; ayrıca bkz. <http://www.ec-guide.com>.
- (17) Verordnung zur digitalen Signatur (Signaturverordnung-SigV). [File://A:\Internet-Recht.htm](file://A:\Internet-Recht.htm), s. 1-11.

şekilde gelişimi konusunda önemli bir engel kaldırılmış olmaktadır. Çünkü; garanti ve güven olmadan, ticari tekliflerin ve para işlemlerinin internet üzerinden yapılması düşünülemez. Yönerge, her konuyu detaylı bir şekilde düzenlememektedir. Aksine, elektronik imza işlemleri ve güvenlik standartları konusunda alınması gerekli asgari tedbirleri belirlemektedir (18). Avusturya'da 1.1.2000 tarihinde yürürlüğe giren Kanunla, bu Yönerge Avusturya Hukukunda somutlaştırılmıştır (19). Amerika'da ise, internette yapılan işlemlerde atılan imza, doğurduğu sonuçlar bakımından, bir kağıt üzerine atılmış el yazısı imza ile eşdeğerdir. Bu sonuç, Birleşik Devletler Temsilciler Meclisinin, elektronik imzayı hukuken kabul eden bir kararında yer almaktadır. Ancak Kanunun yürürlüğe girmesi, Senatonun ve Başkanın onayını gerektirmektedir (20). Amerika Birleşik Devletlerinde ayrıca, dijital imza ile ilgili olarak, federal düzeyde olmasa da, eyalet bazında yasal düzenlemelere rastlamak mümkündür. Bunlardan birisi New York eyaletinin 5 Ağustos 1999 tarihinde kabul ettiği " *State Technology Law* "dur. Bu kanunun 57/A Bölümünün, 1. Maddesi dijital imza ile ilgili hükümler içermektedir (21). Diğeri ise; California ve Pennsylvania'da yürürlüğe giren; Arizona, Minnesota, Nebraska, Ohio, Oklahoma, Maryland, Virginia ve Vermont'da ise henüz askıda olan, Temmuz 1999 tarihli " *Uniform Electronic Transactions Act* "tir (22). Dijital imza konusunda yasal düzenlemeye sahip olan diğer

(18) EU-Richtlinie (1999/93/EG), <http://www.europa-eu.int>.

(19) "EU: Gemeinsame Elektronische Unterschrift beschlossen (Ab 1. Januar in Österreich gesetzlich geregelt)", http://e2i.e2i.at/AA/1p19991130elektronische_unterschriften.htm, s. 1.

(20) "USA: Rechtliche Anerkennung für elektronische Unterschrift", http://www.beck.de/rsw/zeitschr/njw/Archiv/Heft49_99/Wochenpiegel/wosp15.htm, s. 1-2.

(21) <http://www.mbc.com/ecommerce.html>; Tanenbaum, William A.; "State Electronic Signatures and Records Act, Enabling Regulations Have Taken Effect", LEXIS-NEXIS Academic Universe-Dokument, <file://C:\WINDOWS\TEMP\digitalsignatures art.htm>, s. 1-11.

(22) Boss, Amelia H.; Tearing Down Paper Barriers, Uniform Electronic Act Sets New Contract Rules, LEXIS-NEXIS Academic Universe-Dokument, <file://C:\WINDOWS\TEMP\digitalsignaturesart2.htm>, s. 1-5.

ülkeler ise ülkeler ise şunlardır: Arjantin (13 Kasım 1999) (23), Kanada (1 Mayıs 2000) (24), İsrail (5 Mart 2000) (25-26).

II. DİJİTAL İMZA KANUNU- SigG ve BU KANUNA GÖRE DİJİTAL İMZANIN TEKNİK ŞARTLARI

Dijital İmza Kanunu, 13.7.1997 tarihinde, *Bilgi ve İletişim Hizmetleri Kanununun* 3. Maddesinde, Alman Parlamentosu tarafından Kanun olarak kabul edilmiştir (27). Dünyadaki birkaç devletten biri olarak Almanya, bu Kanun ile, dijital imzanın uygulanması için çok önemli yasal bir dayanak yaratmıştır (28). Aşağıda kısaca Dijital İmza Kanununun düzenlediği konulara yer verilmiştir:

- a) **Kanun Yapma Yetkisi**, Federal Devlete aittir. Böylece Almanya'nın her yerinde aynı garanti koşulları ve talepleri söz konusu olacaktır (Alman Anayasası md. 74/f.1, b. 11).
- b) **Kanunun Amacı**, dijital imza için çerçeve şartları tespit etmektir (SigG md. 1/f.1). Şekle ilişkin hükümlerde veya ispat hukukunda değişiklikler yapılmamış, özellikle dijital imza yasal şekil ile (BGB md. 126) mukayese edilmemiştir.
- c) **Onay Makamları**: Dijital İmza Kanunu "*Onay Makamı*" olarak adlandırdığı kurumların çalışması hakkında gerekli olan başlıca koşulları düzenlemiştir. Dijital İmza Kanunu md. 2/f.2'ye göre; bu kurumlar dijital imza sahibi olmak isteyen kişilerin açık kontrol şifrelerini onaylayan ve bunun için de SigG md. 4'e göre bir Lisans'a (ruhsata) sahip olan kuruluşlardır. Onay makamlarının bu kontrol şifreleri, SigG md. 4/f.5'e göre yet-

(23) Bkz. <http://www.mille.com.ar/>.

(24) Bkz. <http://aix1.uottowa.ca>.

(25) Bkz. http://www.law.co.il/computer-law/digsig_1stdraft.doc.

(26) Hepsini için bkz. Legal InfoSoc News Kiosk (LINK), May/June 2000, s. 3-4.

(27) Dijital İmza Kanunu, 1.8.1997 tarihinde yürürlüğe girmiştir (<http://www.iid.de/rahmen/iukdg.html>).

(28) Rossnagel, Alexander; Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung. Datenschutz und Datensicherheit (DuD) 1997, s. 75-81.

kili makamlar tarafından onaylanacaktır. Burada iki aşamalı bir onaylama hiyerarşisi göze çarpmaktadır. Bütün onay kurumlarının şifrelerinin yetkili makamlar tarafından tasdik edilmesiyle birlikte, merkezi bir güvenlik rizikosunu yaratılmış olmaktadır. Çünkü; yetkili makamların şifreleri herhangi bir şekilde elde edilirse, bütün onaylama hiyerarşisi ve böylece tüm elektronik hukuki ilişkiler tehlikeye girmiş olacaktır. Ancak bunun yanı sıra, mevcut düzenleme onay makamlarının bağımsızlıklarını ilan etmelerini ve böylece çok tabakalı bir onay hiyerarşisi kurmalarına engel olmaktadır. Fakat bunun amaca uygun olup olmadığı şüphelidir (29).

d) **Lisans Zorunluluğu:** SigG md. 4' göre, bir onay makamının işletilebilmesi için lisansa gerek vardır. Talep sahibi, bir onay makamının işletilebilmesi için gerekli güvenilirliğe ve orada çalışacak gerekli tecrübeli personele sahipse ve ayrıca iş yerinin ön kontrolü sırasında, Dijital İmza Kanununa göre teknik ve düzenleyici güvenlik koşullarını yerine getirmişse; yetkili makam tarafından lisans talep etme şeklinde bir hakka sahiptir (SigG md. 4/f.4).

e) **Onay makamının Vazifleri:** Dijital İmza Kanunu ve bu Kanunun 16. Maddesine istinaden Alman Hükümeti tarafından 22.10.1997 tarihinde kabul edilen ve Dijital İmza Kanununun 19. Maddesine göre, 1.11.1997 tarihinde yürürlüğe giren, Dijital İmza Kanunu Yönetmeliği (SigV); onay makamlarına bir dizi vazife yüklemiştir: Onay makamı, sertifika talebinde bulunan kimsenin, kimlik kontrolü yaparak, gerçekten o şahıs olup olmadığını tespit etmek zorundadır (SigG md. 5/f. 1; SigV md. 3/f. 1). Talep sahibi kimse için bir çift şifre hazırlar ve bu şifreleri o kişi adına tahsis eder (SigV md. 5). Bu şifrelerin bizzat talepte bulunan kişiye verilmesi zorunludur (SigV md. 6). Ek olarak temsil yetkisi veya meslek dolayısıyla kullanım izni vs. hakkında da açıklamaların yer alacağı, bir kontrol şifresi sertifikası

(29) Rossnagel, s. 75, 78 vd.

düzenler (SigG md. 1/c. 2) ve talep sahibini güvenlik sorunları hakkında aydınlatır (SigG md. 6; SigV md. 4). Bunun yanı sıra onay makamı, her zaman ulaşılabilir bir blokaj servis hizmeti de sunmak zorundadır (SigG md. 8; SigV md. 9).

- f) **Güvenlik ve Kontroller:** SigG md. 5/f.4; md. 5/f.5 ve SigV md. 10; md. 11 vd. hükümleri; düzenleyici, kişisel ve teknik güvenliğin nasıl sağlanması gerektiğine ilişkin düzenlemeler içermektedir. Bu hükümler arasında, onay makamının özel (gizli) imza şifresini bloke etmesi yasağına ilişkin olan SigG md. 5/f.4, c.3 özel önem taşımaktadır. Çünkü; bu şifreyi kim kullanıyorsa, dijital imza taşıyan ilgili belgenin, teorik olarak o şifrenin yetkili sahibi tarafından imzalandığı kabul edilmektedir. Bu hüküm aslında, dijital imzaya olan güveni ağır bir şekilde sarsacak niteliktedir. Onay makamının, güvenlik koşullarını yerine getirirken alması gereken tedbirler, bir güvenlik taslağı şeklinde ifade edilebilir (SigG md. 4/f.3, c.3; SigV md. 12): Bu taslağın lisans verme işlemi sırasında ve bu andan itibaren iki yıl süre ile takip edilmesi gerekir. Ayrıca yetkili makamın, onay makamını kontrol etmek amacıyla araştırma yapmak, inceleme yapmak ve bilgi sormak hakkı mevcuttur. Yetkili makam, onay makamına karşı icra edilmek üzere bir dizi tedbir alabilir, lisansını geri alabilir (SigG md. 13). Ayrıca yetkili makam, SigG md. 12/f.3'e göre; herhangi bir şüpheli durum söz konusu olmasa bile, kontrol yapma hakkına sahiptir. SigG md. 13/f.2, gerçi yetkili makamın, kontrol sırasında onay makamının yazılı belgelerine bakabileceğini ve bunları alabileceğini düzenlemektedir. Ancak bu hükümde, dataların toplandığı yerlerin ve teknik donanımların da incelenmesi konusunda kontrol makamına yetki verilmesi ya unutulmuştur veya gözden kaçırılmıştır. Geniş kapsamlı bir kontrolün yapılması, bu yetki olmadan hemen hemen mümkün gözükmemektedir (30).

(30), Rossnagel, s. 75, 80.

g) **Sorumluluk Sorunu:** Dijital İmza Kanunu, herhangi bir sorumluluk kuralı içermemekte ve bu sorunun cevabını, sorumlulukla ilgili genel kurallara bırakmaktadır.(31). Buna göre; onay makamı, şifre sahibine karşı; BGB md. 278'e göre, çalışanlarının ve diğer ifa yardımcılarının kusurlarından ve onay sözleşmesinin pozitif ihlalden doğan zararlardan, kurtuluş beyyinesi ileri sürme hakkı olmadan sorumludur (kusursuz sorumluluk). Şifre sahibi ise sadece yükümlülüğün ihlal edildiğini ve bunun da sonuç olarak zarara sebebiyet verdiğini ispat edecektir (32). Onay makamı, üçüncü kişilere karşı, sadece kendi çalışanlarından birinin kasten yaptığı işlemlerden dolayı, maddi zarar ödemekle sorumludur (BGB md. 831; md. 826; md. 823/f.2; StGB md. 263) (33). Ancak burada dikkat edilecek olursa, çalışanların ihmale dayanan davranışlarının veya üçüncü kişinin eylemlerinin, şifre sahibinden başka bir şahsa verebileceği maddi zararlar konusunda bir hüküm boşluğu söz konusudur (34).

Dijital İmza Kanunu 16 maddeden oluşmaktadır. Madde 7 hükmüne göre, imza şifresi sertifikası olarak adlandırılan sertifika, aşağıdaki şu bilgileri içermelidir:

- Dijital imza anahtarı sahibinin adını,
- Koordine edilen (bağlanılan) aleni (açık) dijital imza anahtarını,
- Algoritmanın adını (örneğin; RSA) (35)
- Sertifikanın sıra numarasını,
- Sertifikanın başlangıç ve geçerliliğinin sona erme süresini,

(31) Rossnagel, s. 75,79; Engel-Flehsig, Stefan/Maennel, Fritjof A./Tettenborn, Alexander; Das neue Informations-und Kommunikationsdienste-Gesetz. Neue Juristische Wochenschrift (NJW) 1997, s. 2981-2992.

(32) Timm, Birte; Signaturgesetz und Haftungsrecht. Datenschutz und Datensicherheit (DuD) 1997, s. 525-528.

(33) Timm, s. 525, 526 vd.

(34) Engel-Flehsig/Maennel/Tettenborn, s. 2981, 2989; Timm,s. 525, 527.

(35) Bkz.aşa.s. 11.

- Onay makamının adını,
- Kullanım ile ilgili belirli sınırlamalar varsa, bunlar hakkındaki açıklamaları.

III. DİJİTAL İMZA PROSEDÜRÜ

Bir belgeyi elektronik olarak imzalayabilmek için, kullanıcıların, bir Onay Makamının veya - daha sık kullanılan İngilizce karşılığı ile "*Trust Center'in*" hizmeti yanında teknik bir alt yapıya da sahip olması gerekir. Kullanıcının bir bilgisayarı ve kendine ait **Software'inin** (YAZILIM ?) olması gerekir. Kullanıcının ayrıca bilgisayar üzerinden yapacağı işlemlerde kullanacağı bir de şifresinin olması gerekir. Bu şifre, aşağıda tekrar değineceğimiz üzere, ya yazılım (software) programları vasıtasıyla veya akıllı kart (SmartCards) olarak da adlandırılan Chip kartlar kullanılarak elde edilebilir. Chip Kartların çalınması veya kaybedilmesi durumunda, eğer kullanıcı bu durumu fark ederse, aynen kredi kartları uygulamasında olduğu gibi, Chip Kart Dağıtım Merkezine yapılacak bildirim ile, kart derhal bloke edilecektir (36).

Dijital imza, bir datanın üçüncü kişiler tarafından görülüp değiştirilmesi tehlikesini önlemeye yaramaktadır. Bu tür mesajı yüklemek, okumak ve değiştirebilmek, sadece şifre ve giriş kodunu (Password) kullanmak hakkına sahip olan kimseye aittir. Eğer şifre ve giriş kodu sahibi, bir başka kimseye gönderdiği mesajı okuma yetkisi vermek isterse, bu kişiye anahtar kelimeyi bildirmek zorundadır. Bu olanak, şifre sahibinin bir çok katılımcı ile elektronik yoldan haberleşmek istemesi durumunda pratik olmayacaktır. Çünkü; herkesin bütün mesajları, öğrenmesi istenmeyeceği için, şifre sahibinin haberleşmek istediği her bir kişi ile farklı anahtar kelimeler kararlaştırması ve haberleştiği kişi ile aralarında kararlaştırdıkları bu şifreye göre mesajı şifrelemesi ve karşı tarafın da bu şifreye göre mesajı deşifre etmesi gerekecektir. Bu durumun di-

(36) "Faelschungssicherer unterschreiben", Fracht und Materialfluss, Mai 1999, s. 43 vd.

ger bir sakıncası da şudur: Mesajı deşifre edebilecek olan bir okuyucu, bu mesajı değiştirebilir de (37). Ve bu manipulasyon olanakları, hukuki ilişkilere ve iş ilişkilerine zarar verebilir (38). İşte burada dijital imza gündeme gelmektedir. Dijital imza, elektronik belgenin şifrelenmesini mümkün kılmaktadır, değiştirilmesini önlemektedir ve ayrıca birden çok kişi ile, mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek olmadan, elektronik yoldan haberleşmeyi kolaylaştırmaktadır. Teknik olarak dijital imza, bir çift şifreden oluşmaktadır. Söz konusu şifreler, haberleşmek isteyen taraflara (biri göndericiye, diğeri ise alıcıya) ait olacaktır. Bu bir çift şifre, elektronik belgeleri, mesajları imzalamak için kullanılacak olan ve sadece imza atacak olan kişide kalacak bir "gizli şifre"den; ayrıca imzanın tetkiki için kullanılacak ve haberleşmek isteyen kişiye kullanması için verilecek olan bir "açık şifre"den oluşmaktadır (39). Sistemin güvenilir bir şekilde işlemesi, her iki anahtarın uzunluğuna ve özel (gizli) şifrenin kullanıcı tarafından iyi saklanmasına bağlıdır. İmzalama aşamasında söz konusu olan karmaşık matematik işlemlere rağmen, prosedür kullanıcı için oldukça kolaydır. kullanıcı chip kartını, gizli şifresi ile birlikte sürücüye soktukten sonra, sadece "imzala" komutuna mause ile dokunması yeterli olmaktadır. bundan sonraki bütün işlemleri bilgisayar halletmektedir (40). Bir mesaj dijital imza ile tasdik edilirse, bu mesajın artık başkaları tarafından değiştirilmesi güç olacaktır. Değiştirilmesi imkansız değildir, sadece bu tür değişiklikleri yapmak güç olacaktır (41).

(37) "Digitale Unterschrift besiegelt Vertraege", Welt am Sonntag, 1999/1, s. 65 vd.

(38) " Chancen und Risiken des Faktors Information – Auswirkungen auf Politik, Gesellschaft, Wirtschaft und Militaer. Forum der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik, Bonn-Bad Godesberg, 19-20 Növmber 1997, Kompendium.

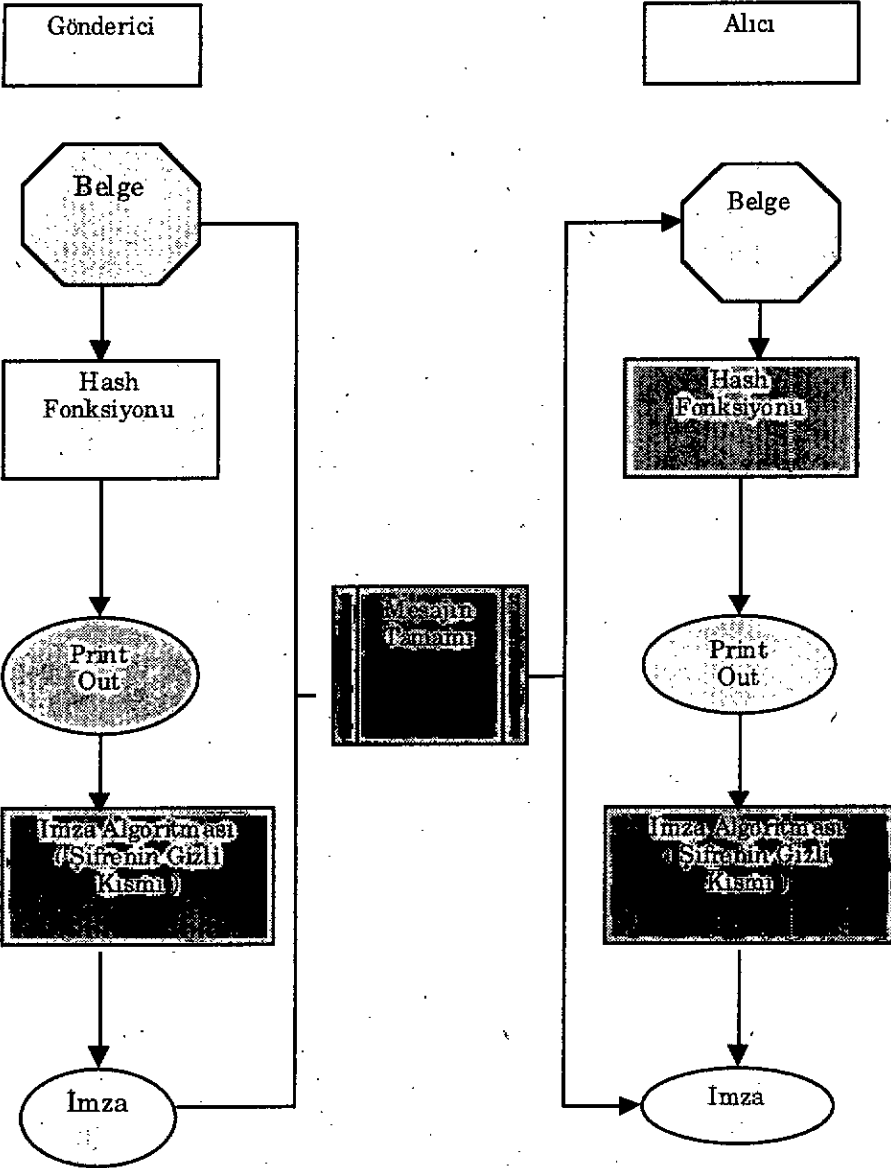
(39) <http://www.dzsh.de/aktuell/inbrief/97-02/unter.htm>, s. 1; Her bir şifre 1024 Bit uzunluktadır.

(40) "Elektronische Unterschrift Kommt (Sicherheit im Internet für rund 150 Mark) (Digitale Signatur soll Hackern ab 1999 das Handwerk legen)", <http://www.rhein-zeitung.de/op/98/04/27/topnews/esign.html>, s. 1-2.

(41) Siehe auch "Loch im Datennetz", Focus 1998/3, s. 158.

Dijital imzanın işleyiş şekli aşağıdaki gibi şematize edilebilir:

TABLO 1



Dijital İmza Kanununda ve Tüzüğünde, kimlik tespiti aracı olarak PIN'in (42) ön plana çıkarılmış olması eleştirilmektedir. Ancak, Kanun koyucu teknik alandaki ilerlemeye yaptığı atıf ile birlikte, şüphesiz biyometrik özelliklerin de kullanılmasına izin vermiştir (43).

Dijital imza teknik, elektronik ve şifreleme yöntemlerinin yanı sıra, kimlik tespiti için kullanıcının şifreye zilyetliğini ve kullanıcının tanınabilmesini de gerektirmektedir. Zilyetlik, bir Chip Kartı ile sağlanır. Tanınabilme ise, bir pin ile tespit edilir. Ancak kanaatimizce, hiç bir fert bir pin kodu ile teşhis edilemez. pin kodu sadece Chip Kartının tespit edilmesine yarayabilir. Bundan başka bir fonksiyonunun da olmaması gerekir.

Dijital imzanın sonuç olarak el yazısı imza ile eş değerli olması arzu edildiği ve bunun ötesinde taklit edilme riskine karşı da güvenli olması gerektiği için, normal bir imzanın taşıdığı bütün şartları, dijital imza da taşımak zorundadır. Ancak, yeri gelmişken hemen belirtmek gerekir ki; dijital imzanın hukuken el yazısı imza ile bir tutulması aşağıda da tekrar belirteceğimiz üzere bugün için mümkün değildir (44).

Bu yüzden dijital imza, el yazısı ile imzanın ve elektronik belge de normal bir belgenin işlevini yerine getirmek zorundadır.

Bu işlevler aşağıdaki şekilde belirlenebilir:

♦.....Gerçeklik İşlevi - İmza, imzalanan belgenin, imza eden kişi tarafından görüldüğünü ve onun tarafından kabul edildiğini teyit eder.

♦.....Kimlik Tespit Etme İşlevi - İmza sayesinde birbiri ile haberleşen kişilerin kimliği, şüpheyi yer vermeyecek şekilde tespit edilebilir.

(42) "Personen-Identifikations-Nummer," Kişi Tanımlama Numarası".

(43) Bkz. aşağıda s. 23 vd.; Leicher Trendforum : "Biometrische Identifikationssysteme", München 1997/11 (Vortrag von Dr. Bocksläff).

(44) Bkz. aşağıda s. 23 vd.

•.....Sonuçlandırma İşlevi - İmza, metnin içerik olarak doğru ve tam olduğunu açıklar.

•.....Uyarı İşlevi - İmzanın gerekliliği sayesinde, imza atan kişi için, hukuken önemli bir durum yaratıldığı açığa kavuşmuş olur (45).

Yukarıda saydığımız bu dört işlevi yerine getiren bir imza, delil gücü kazanır. Yani yazılı belge hükmünde sayılır. Alman hukuk düzeninde ise, yazılı belgeler en güçlü delildir (46).

Normal bir belgenin ispat gücü kazanabilmesi için şüphesiz, hemen her zaman, yer ve tarih bilgileri de gereklidir. Bu yüzden dijital imza da, normal bir belgenin tarihine karşılık olmak üzere bir zaman kaşesine (47) ihtiyaç göstermektedir.

Yukarıda açıklanan tüm fonksiyonlar ve zaman kaşesi vasıtasıyla elektronik irade beyanı, normal bir beyanı gibi sonuçlar doğurur. Ancak hukuki bir uyumsuzluk durumunda, İmza Kanununa göre dijital imzayı kabul etmek veya etmemek her zaman hakimnin takdirindedir (48).

Bundan sonraki bölümde dijital imzanın bazı esaslarına değinilecek ve daha sonra ise birkaç uygulama örneği verilecektir.

IV. ŞİFRELEMENİN ESASLARI (KRİPTOGRAFİ)

Şifrelemenin temel amacı, herkesin okuyabileceği bir açık metinden, şifreleme yoluyla sadece istenilen bir veya birkaç kişinin okuyabileceği gizli bir metin yaratmaktır. Alıcı bu şifrelenmiş metni daha sonra ilk şekline çevirecek, yani deşifre edecektir. Şöyle ki:

(45) Bkz. Köhntopp, Christian; Beweiskraft von PGP-Signaturen, <http://www.koehntopp.de>.

(46) Alman Usul Kanunu (ZPO) § 415-444.

(47) Echtheits-Zertifikat, Computer Technik, 1998, s. 113.

(48) Bkz.aşa.s. 29 vd.

(Açık Metin) - Şifreleme - (Gizli Metin)

(Gizli Metin) - Şifreleme - (Açık Metin) (49)

Günümüzde kullanılan şifreleme yöntemlerinde farklı matematiksel metotlardan hareket edilmektedir. Başlıca yöntemler arasında;

- **Data Encryption Standard (DES):** 1977 tarihli olan bu yöntem, IBM'in 1970'li yıllarda geliştirdiği algoritmaya dayanmaktadır (50).
- **International Data Encryption Algorithm (IDEA):** 1991 tarihli bir yöntemdir. Henüz çok yeni tarihli olmasına rağmen, bir çok analizde kullanılmıştır ve en emin algoritmalarından biri olarak kabul edilmektedir (51).
- **RSA:** 1978 yılında Rivest, Shamir ve Adleman tarafından hazırlanan bu algoritma, Diffie ve Hellmann'ın 1976 tarihli algoritmalarına dayanmaktadır.
- **ElGamal ve DSA:** Diffie ve Hellmann'ın fikirlerinin çatısını oluşturduğu ve 1985 yılında Taher ElGamal tarafından geliştirilen şema, aynı zamanda asimetrik bir algoritmadır (52).

Bugün kullanılan diğer yöntemler arasında; faktör analizi, gizli saklı logaritma ve eliptik eğriler sayılabilir (53). Güncel yöntemler arasında yer alan ve aşağıda ayrıntılı olarak değinilecek olan Simetrik ve Asimetrik şifreleme yöntemlerinde ise, parametrik metotlar ailesi söz konusudur. Seçilen parametre, şifre olarak da adlandırılır ve bu şifrenin birbiri ile haberleşen kişiler tarafından ta-

(49) Fachverband Informationstechnik, FVIT, 1998, s. 11; Beutelspracher, s.11; Bauer, s. 26; Schneier, s. 1.

(50) DES hakkında ayrıntılı olarak bkz. Schneier, s. 309 vd.

(51) IDEA hakkında ayrıntılı olarak bkz. Schneier, s. 370 vd.

(52) Beutelspracher, s. 141 vd.; Schneier, s. 543 vd.

(53) Bkz. Koenigsmann, J; Elliptische Kurven, <http://www.uni-konstanz.de/koenigsmann001.htm>, s. 1-2; Seiler, Wolfgang K.; Elliptische Kurven, <file:///A:/elkurven.htm>, s. 1-2.

mamen veya kısmen gizli tutulması gerekir. Şifrenin yetkili olmayan kişiler tarafından, bilgisayar yardımıyla kolayca bulunması için, parametrenin veya şifrenin yeteri kadar büyük olması gerekir. Modern şifreleme yöntemlerine; **Güvenilirlik** (Belgenin içeriği sadece bu konuda yetkili olan kimseler tarafından okunabilmelidir), **Orijinallik** (Belgenin içeriği düzenleyen kimse fark etmeden değiştirilememelidir), **Gerçeklik** (Belgeyi düzenleyen kişinin, yani belgenin sahibinin kim olduğu tespit edilebilmelidir. Başka hiç kimse kendisini, belgeyi düzenleyen kişi olarak tanıtamamalıdır), **Bağlayıcılık** (Belgeyi düzenleyen kişi, bu belgeyi düzenlemediği yolunda itirazda bulunamamalıdır) ve bazı durumlarda **Anonimlik** (Bununla mesajın içeriğinin güvenilirliği değil, aksine haberleşme şeklinin güvenilirliği kastedilmektedir (54)) sağlanması yönünde talepler yöneltilmektedir.

Dijital imza hizmeti sunan kuruluşlar ve kullanıcılar, işlemlerinde hangi yöntemi kullanacaklarını serbestçe kararlaştırabilirler. Dijital İmza Kanunu, bu konuda herhangi bir yöntem öngörmediği gibi, herhangi bir yöntemi de yasaklamamaktadır. Ancak yine de kullanılacak yöntemin Dijital İmza Kanununun hükümleri ile çelişmemesi ve Onay Makamının taleplerine ve teknik koşullara uygun bulunması gerekir (55).

V. SİMETRİK VE ASİMETRİK ŞİFRELEME YÖNTEMLERİ, GİZLİ (ÖZEL) VE AÇIK ŞİFRE

Şifreli haberleşme yapılmadan önce, bir veya bir çok şifrenin hazırlanmış olması gerekir. Şifrenin hazırlanması ise farklı tarz ve şekillerde söz konusu olabilir. Örneğin ya yazılım (software) programları vasıtasıyla veya akıllı kart (Smart Card) olarak da adlandırılan Chip Kart'lar kullanılarak şifre elde edilebilir.

(54) Beutelspracher, s. 149.

(55) <http://www.ec-guide.com>.

A. SİMETRİK ŞİFRELEME YÖNTEMİ

Simetrik şifreleme yönteminde; şifreleme ve deşifre işlemi için, aynı şifre kullanılır. Örneğin; A ile B arasında haberleşmenin güvenli bir biçimde gerçekleşebilmesi için, şifrenin sadece birbiri ile haberleşen taraflarca bilinmesi, bunun dışındaki kimselere karşı ise mutlak bir şekilde saklı tutulması gerekir (56). Bir haberleşmeye ikiden çok kimse katılıyorsa, bu durumda tüm katılanlar şifreyi öğrenmiş olacaklardır. Bu durum ise, birbiri ile haberleşen tarafların, yetkili olmayan bir kimse tarafından şu ya da bu şekilde şifrenin öğrenilemeyeceğine inanarak nasıl haberleşecekleri sorununun ortaya çıkarmaktadır (57).

Bu konuda bir çok olasılık söz konusu olabilir:

- *Elektronik olmayan yoldan şifre değişimi:*

Taraflar, haberleşme işlemine başlamadan önce örneğin; posta yoluyla şifreyi birbirlerine gönderebilirler. Ancak bu olasılık, haberleşmek isteyen tarafların birbirini tanıması şartıyla kullanılabilir.

- *Örnek bir şifre ile elektronik yoldan şifre değişimi:*

Haberin şifreleneceği şifre, gönderilmek istenen mesaj ile birlikte, örnek bir şifre yardımıyla şifrelenmektedir. Şüphesiz bu örnek şifrenin de, haberleşmeden önce taraflar arasında değişiminin yapılması gerekir. Bu yöntem de, haberleşen tarafların birbirlerini önceden tanımalarını gerektirmektedir.

(56) Bauer, s. 154; Beutelspracher, s. 10; Gerling, Rainer W.; Verschlüsselungsverfahren. Eine Kurzübersicht. Datenschutz und Datensicherheit (DuD) 1997, s. 197-202; Grimm, Rüdiger; Kryptoverfahren und Zertifizierungsinstanzen. Datenschutz und Datensicherheit (DuD) 1996, s. 27-36; Huhn, Michaela/Pfitzmann, Andreas; Krypto(de)regulierung. Datenschutz-Nachrichten (DANA) 1996, Heft 6, s. 4-13 (İnternet adresi: http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/lit/abstr96.html#HuPf2_96); Ohst, Daniel; Vertrauliche Kommunikation, 9.Mai.1996, <http://www2.rz.hu-berlin.de>.

(57) Schmidt, Jens-Uwe/Ungerer, Bert; Al dente. IX 1997, Heft 4, s. 128-131 (İnternet adresi: <http://www.heise.de/ix/artikel/1997/04/128/artikel.shtml>).

- *Hybrid yöntemi ile şifre değişimi:* Hem simetrik hem de asimetrik şifreleme yönteminde kullanılabilen (58) bu yöntemle göre; asıl mesaj, tesadüfen yaratılan bir şifre ile şifrelenir. Bu şifre, toplantı şifresi (Session Key) olarak da adlandırılır. Daha sonra bu mesaj, alıcının açık şifresi (Publik Key) yardımıyla şifrelenir. Alıcı, sadece kendisi tarafından bilinen gizli şifresi (Privat Key) yardımıyla, mesajın toplantı şifresini açar ve bu şifre yardımıyla mesajı deşifre edebilir.

TABLO 2

Yöntem	Şifreleme Uzunluğu	Lisans (Ruhsat) Sınırlamaları
Simetrik Şifreleme Yöntemi.		
DES	56 Bit	Lisans (Ruhsat) gerekli değil
3DES	112 veya 168 Bit	Lisans gerekli değil
RC2	Değişken (variable)	Lisans zorunlu (RSADSI)
RC4	Değişken	Lisans zorunlu (RSADSI)
RC5	Değişken	Lisans zorunlu (RSADSI)
IDPA	128 Bit	Ticari amaçlı kullanım için lisans zorunluluğu (Ascom AG)
SAFER	64 veya 128 Bit	Cylink için geliştirilmiştir. Lisans sorunu henüz cevaplanmamıştır.
SEAL	160 Bit	Lisans zorunluluğu (IBM)

Yukarıda Tablo 2'de bazı şifreleme algoritmalarına yer verilmiştir (59).

- (58) Beutelspracher, s. 136 vd.; Gerling, s. 197, 199; Grimm, s. 27, 30; Huhn/Pfitzmann, s. 4, 6; Schmidt/Ungerer, s. 128, 131; Schneier, s. 38 vd.
 (59) Fachverband Informationstechnik, FVIT 1998, s. 14.

B. ASİMETRİK ŞİFRELEME YÖNTEMİ

Birbiri ile haberleşen iki kişi arasındaki, asimetrik şifreleme yöntemi şöyle açıklanabilir (60): Burada haberleşen her bir taraf, biri açık, diğeri ise gizli veya özel olmak üzere, yöndeş bir çift şifreye sahiptir. Bu durumda örneğin; A, B'ye bir mesaj yollamak isterse, bu mesajı şifrelemek için, B'nin aleni olarak ulaşılabilen açık şifresini kullanacaktır. B, şifreli mesajı aldıktan sonra, mesajı deşifre etmek için kendi gizli şifresini kullanacaktır. Tam tersi durum, yani bu sefer B'nin, A'ya mesaj yollaması da aynı şekilde gerçekleşecektir (61). Buna göre, asimetrik şifreleme yönteminde önemli olan herkesin kendi açık şifresini aleni olarak ulaşılabilir kılmasıdır (62).

TABLO 3

Yöntem	Şifreleme Uzunluğu	Lisans Sınırlamaları
Asimetrik Şifreleme Yöntemi		
RSA	Asgari 768 (1024) Bit	Amerika'da lisans zorunluluğu var.
DSA (özellikle Diffie-Hellman)	Asgari 768 (1024) Bit	Lisans zorunluluğu yok.
Elipitik KURVEN	Asgari 128 Bit	Lisans zorunluluğu yok.

Tablo 3'de bugün sık olarak kullanılan asimetrik şifreleme yöntemleri açıklanmıştır (63).

(60) Fachverband Informationstechnik, FVIT 1998, s. 14.

(61) Bauer, s. 154 vd.; Beutelspracher, s. 114; Gerling, s. 197, 198; Grimm, s. 27, 29 vd.; Schneier, s. 5.

(62) Bauer, s. 155; Beutelspracher, s. 115 vd.; Grimm, s. 28; Huhn/Pfitzmann, s. 4, 6; Schmidt/Ungerer, s. 128,130.

(63) Fachverband Informationstechnik, FVIT 1998, s. 15.

Burada en büyük problem şüphesiz açık şifrenin uyumudur (koordinasyonudur). Bu yüzden, belirli bir açık şifrenin belirli bir kişiye % 100 ait olduğunun garanti edilmesi gerekir. Bu problemle Onay Makamı veya Trustcenter veya Certification Authorities adlandırılan kurumlar uğraşmaktadır. Bu konuya aşağıda ayrıntılı olarak değinilecektir.

VI. ÖZ DEĞERİ (HASHWERT)

Bilgisayar terminolojisinde "Hash (= Öz) (64) "; yazılan bir mesajın, kısaltılmış şeklidir. Dijital İmza, bilginin doğruluğunu korumaktadır. Teknik açıdan dijital imza, imzalanmış belgenin özünü (Hash) içerir. İçerikte yapılacak herhangi bir değişiklik dijital Hash'ı geçersiz kılacaktır.

TABLO 4

Yöntem	Şifreleme Uzunluğu	Lisans Sınırlamaları
Hash Fonksiyonları		
MD5	128 Bit	Lisans zorunluluğu yok
SHA 1	160 Bit	Lisans zorunluluğu yok
HIPE-MD	128 veya 160 Bit	Lisans zorunluluğu yok

Tablo 4, geçerli Hash fonksiyonlarının bir listesini göstermektedir (65). Kavram olarak Hash, göndermek istediğimiz mesaj bakımından bir " çarpaz toplam " oluşturma yöntemidir (66).

Hash fonksiyonları, dijital imzanın hazırlanması için son derece önemlidir. Yukarıda değinildiği gibi, asimetrik şifreleme yöntemi

(64) Konu ile ilgili eserlerde Hash kavramı, ilgili dildeki karşılığı yerine, aynen kullanılmıştır. Bu nedenle biz de, çalışmamızda terminolojik tartışmaya meydan vermemek için, Hash kelimesini aynen kullanmayı tercih ediyoruz.

(65) Fachverband Informationstechnik, FVIT 1998, s. 16.

(66) <file://A:\hashhandkeys.htm>, s. 3.

minde birbiri ile haberleşen her bir taraf, biri açık diğeri ise gizli olmak üzere iki şifreye sahiptir (67). Hazırladığı mesajı imza etmek isteyen kimse, mesajının hash değerini hesaplamak için, bir hash fonksiyonu kullanacaktır. Bu şekilde hash değeri, gizli şifre ile şifrelenmiş olacaktır. Bir belgenin hash değeri belli olduğu için, alıcı bunu mesajı gönderenin açık şifresi yardımıyla tespit edebilir. Alıcı hash fonksiyonunu bu defa deşifre edilen mesaja da uygulayabilir ve her iki değeri birbiri ile karşılaştırabilir. Her iki değer birbirine uyuyorsa, alıcı, bu belgenin göndericinin orijinal belgesi olduğundan ve mesajın sonradan değiştirilmediğinden emin olabilir. Mesaj sonradan değiştirilmiş olsaydı, bu durumda elde edilen hash değerleri birbirinden farklı olacaktı.

Bugün en çok tanınan ve en yaygın olarak kullanılan hash algoritması, MD (Message Digest)'dir. MD kendi içinde üç farklı versiyona sahiptir:

MD2 (artık güvenli bir yöntem değildir)

MD4 (artık güvenli bir yöntem değildir)

MD5 (bazı güvenlik problemleri olduğu bilinmekle birlikte kullanılan bir yöntemdir).

Bir dijital imza, şüphesiz farklı yollarla da hazırlanabilir. Gönderici, orijinal belgeyi kendi gizli şifresi ile şifreler ve bu belgeyi alıcıya hem şifreli hem de şifresiz olarak gönderir. Alıcı, şifreli belgeyi deşifre etmek için, göndericinin açık şifresini kullanır ve bundan sonra her iki belgeyi birbiri ile karşılaştırabilir. Her ikisi de birbirine uyuyorsa, belge, orijinal olarak kabul edilebilir.

VII. ZAMAN KAŞESİ

Elektronik bir belgenin ispat gücünü güçlendirmek için, diğer koşulların yanı sıra belgenin hazırlandığı düzenlendiği zamanın

(67) Bkz. yuk. s. 13.

şüpheyi yer bırakmayacak bir şekilde tespit edilmesi gerekir. Bu yüzden şifreleme ve kimlik teşhis etmenin yanı sıra, zaman kaşesi fonksiyonu da önemli bir role sahiptir. Günlük yaşamdaki bir çok işlemlerde, örneğin; hisse senedi ve döviz işlemlerinde tam zamanın açıkça tespit edilmesi gerekir.

Elektronik belgelerden çok fazla şey beklenmektedir. Bir kere bu belgeler normal belgelerin tüm görevlerini yerine getirmelidirler ve ayrıca bu belgeler taklit edilme riski ve esneklik konusunda daha güvenilir yeni bir standarda ulaşmak zorundadırlar (68).

Her zaman güncel, üzerinde oynama yapılmamış ve değiştirilmemiş zaman bilgileri elde etmek, şu an hiç de öyle kolay değildir. Normal bilgisayarlarda ve işletme sistemlerinde, tarih ve saat ayarı, fazla bir zahmete gerek olmadan, kolaylıkla değiştirilebilmektedir. Normal belgelerdeki gibi, elektronik belgelerde de, tarih ve saatin doğru bir şekilde tespit edilmesi gerektiğinden, bunu başarmak için güvenli bir yöntem ihtiyacı vardır. Onay makamları, özellikle Trust Center'lar, talep üzerine dijital tarihleri, bir zaman kaşesi ile birlikte bildirmeye mecburdurlar.

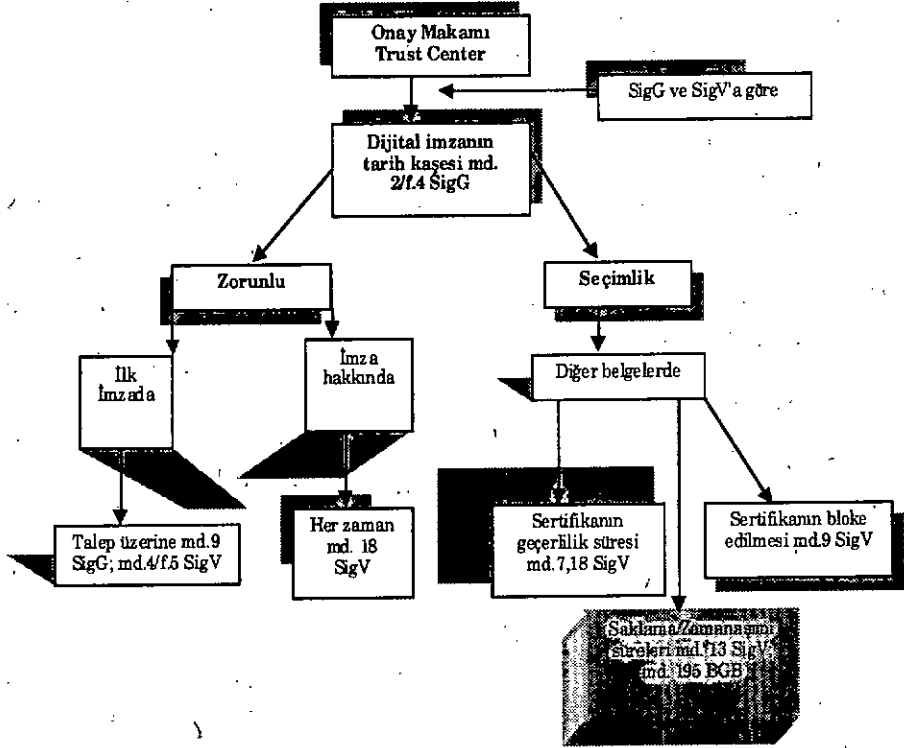
Gerçek tarihin bilinmesi son derece büyük önem taşıdığı için, Federal Güvenlik ve Bilgi Teknikleri Bakanlığı (BSI), "Güvenlik Kutusu (Sicherheitsbox)" olarak adlandırılan bir vasıtayı önermiştir. Bu güvenlik kutusu, çok sıkı güvence altına alınmıştır ve imzalayanlar arasındaki bütün önemli işlemler, bu kutu içinde gerçekleşmektedir. Burada, söz konusu güvenlik kutusunun ayrıntılı olarak açıklanmasına yer verilmemiştir (69).

Aşağıda Dijital İmza Kanunu ve Dijital İmza Yönetmeliğine göre, dijital imzanın zaman kaşesi taşımasına ilişkin durum şematize edilmiştir:

(68) Echtheits-Zertifikat, CT, 1998, s. 113.

(69) Echtheits-Zertifikat, CT 1998, s. 114.

TABLO 5



VIII. ONAY MAKAMI (TRUSTCENTER-CERTIFICATION AUTHORITIES)

Daha önce simetrik şifreleme yöntemi (70) anlatılırken değinildiği üzere, bu yöntemde birbiri ile haberleşen her iki taraf, şifreleme ve deşifre için aynı şifreyi kullanmaktadır. Sadece iki kişi gizli bir bilgiyi paylaşıyorsa, simetrik şifreleme yöntemi herhangi bir sorun yaratmayacaktır. Diğer bir ifade ile, kullanıcı sayısının az olduğu durumlarda bu prensiple yetinmek mümkündür. Ancak kullanıcı sayısı artarsa, özellikle birçok kimseye haberleşmeye katılma imkanı verilirse, hiyerarşik bir alt yapı olmaksızın bunun üs-

(70) Bkz. yuk: s. 12.

tesinden gelinemeyecektir. İşte bu aşamada onay makamları veya Trustcenter, özellikle Certification Authorities gündeme gelmektedir. Dijital İmza Kanunu "*Onay Makamından*" bahsetmektedir (SigG md. 2).

Bir kimsenin dijital imzasının geçerliliği, bu kişinin açık şifresinin bir Trust Center tarafından, dijital bir imza ile tasdik edilmesi suretiyle olur (71). Bu kapsamda olmak üzere, şifreleri kullanacak olan kişi hakkındaki bilgiler, Trust Center'ın gizli şifresi ile şifrelenecek olan sertifikanın düzenlendiği tarih ve geçerlilik süresi de önem taşımaktadır. Sertifikanın hazırlanması genel olarak şu şekilde gerçekleşir: İmza şifresi sertifikası sahibi olmak isteyen bir kişi, Trust Center'a veya yetkili diğer bir kuruma, kimlik bildiriminde bulunur. Trust Center bunun üzerine, ilgili şahıs tarafından imza için kullanılacak olan bir çift şifre hazırlar, açık şifreyi sertifikalar ve bunu kullanıcının ismi ile birlikte bir "*şifre listesinde*" yayımlar.

Dijital imzalı bir mesajı alan kişi ise, Trust Center'ın Şifre Listesinden göndericinin açık şifresini bulabilir. Bu şifre ile, dijital imzayı çözer ve yine bu açık şifre yardımıyla metni okunabilir hale getirebilir. Bu açıklamalar bile, bir Trust Center'a ne kadar büyük güvenlik ve garanti taleplerinin yönelttiğini ortaya koymaktadır. Trust Center'ın gizli şifresi hiç bir koşulda kullanıcıdan başka kimseye verilmeyecektir. Hazırlanan her şifrenin, her kullanıcı için ayrı olması; yani bir şifrenin sadece bir tane yapılmış olması gerekir. Dijital İmza Kanunu bu yüzden, Trust Center'ların işletilmesini bu konuda lisans verildikten sonra geçerli olarak kabul etmektedir (SigG md. 4) (72).

Bir Trustcenter'ın vazifleri kapsamında olmak üzere şunlar sayılabilir (73):

(71) <http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>, s. 2.

(72) <http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>, s. 2-3.

(73) Fachverband Informationstechnik, FVIT 1998, s. 19.

- Katılımcıların kaydedilmesi
- Şifre hazırlanması
- Chipkart'ların (Smart Card = Akıllı Kart) kişiselleştirilmesi
- Şifrenin haberleşen taraflar arasında koordine edilmesi)
- Rehber Hizmetleri (Katılımcıların Listesi)

Kapatma (Blokaj) Servisi (Katılımcıların ayrılması, şifrenin süresinin dolması vs. durumlarında).

Bir Sertifikanın içeriğinde hangi hususların yer alacağı konusuna daha önce değinmiştik (74). Burada ise bu unsurlar tekrar sayılacaktır:

- Sertifikalandırmanın versiyon numarası
(Örneğin; v3)
Seri numarası
- Sertifikanın şifrlenmesi usulünün tespit edilmesi (seçilmesi)
(Örneğin; RSA/MD5)
- Tanzim eden kişinin açık bir şekilde adı (Örneğin; c = almanya, o = FVIT)
- Geçerlilik süresi (Örneğin; Başlangıç: 1.11.1997, Bitiş: 31.12.1999)
- Sertifika sahibinin açık bir şekilde adı (Örneğin; cn = muster-mann)

Trust Center'lar, belirli bir açık şifrenin sadece belli bir kişiye ait olduğunu gösteren bir sertifikanın düzenlenmesi suretiyle,

(74) Bkz. yuk. s. 7.

elektronik yoldan da onay verebilirler. Şüphesiz herkes kendini kendini Trust Center olarak tanıtamaz. Trust center'ın açık şifresinin de aynı zamanda ya aynı alanda hizmet veren başka bir Trust Center tarafından veya daha üst bir makam tarafından tasdik edilmiş olması gerekir. Federal Almanya'da en üst makam, sertifikaları talep üzerine tanzim eden Düzenleme Makamı'dır. Şimdiye kadar yaklaşık 30 işletme, bu makama, Trust Center kurmak amacıyla talepte bulunmuştur. Dijital İmza Kanununa göre; Trust Center açmak isteyen kimse, bu yönde bir talepte bulunmak zorundadır (SigG md. 2). 1999 yılı, Mart ayında kabul edilen Avrupa Topluluğu Dijital İmza Yönergesi'ne (75) göre; bu yönde bir talepe gerek yoktur. Federal Almanya Devleti de Avrupa Topluluk Hukukuna tabi olduğu için, yakın bir tarihte Trust Center açmak için artık talepte bulunmaya gerek kalmayacaktır. Şüphesiz Düzenleme Makamı habersiz kontrolleri bizzat yapabilecektir.

Hiyerarşi de en üst konumda yer alan Düzenleme Makamından yola çıkılacak olursa, sayıları ne kadar çok olursa olsun Trust Center'lar birbiri ile bağlantılı olabileceklerdir (76).

Bir kimse birden çok Trust Center'a kayıt yaptırmışsa, ilk önce Trust Center'lar bunun doğruluğunu kontrol etmek için, aralarında haberleşirler. Bu durum Güven Zincirleri adı verilen ilişkinin doğmasına sebep olmaktadır. Bu prosedür yukarıda değinilen hiyerarşik sistemden daha karmaşıktır. Eğer dünyadaki farklı ülkelerin "ana kurum" olarak da adlandırılan en üst makamları karşılıklı olarak birbirlerini tanır ve yetkilerini tasdik ederlerse, bu durumda artık uluslararası haberleşme bir sorun olarak karşımıza çıkmayacaktır. Bu yüzden zaten standardize edilmiş bir usule göre yürüyen X 500 (77), ve "Directory Services" adıyla özetlenebilecek olan uluslararası yöntemler mevcuttur.

(75) Bkz. <http://www.europa.eu.int>.

(76) Fachverband Informationstechnik, FVIT 1998, s. 21.

(77) X 500, Rehberlik hizmeti için hazırlanan uluslararası normlar.

Bu konuda ilk Alman İşletmesi olarak, Alman Telekom Şirketi, Telesec adını verdiği yavru şirketi, bir Trust Center olarak hizmete sokmuştur. Telesec'i yakın bir tarihte şüphesiz yeni Trust Center'lar izleyecektir.

Bir mesajı veya tarihi imzalamak için kullanıcı, kendisini tanıtabilmek için, sadece kendisi tarafından bilinen giriş kodunu yazmalıdır. Giriş kodu yoluyla sağlanan bu güvenlik, yetkili olmayan kişilerin, kullanıcının bilgisayarında, kullanıcının gizli şifresi yardımıyla farklı bir imza yaratmasını engellemektedir. Yazılım programlarında sisteme girebilmek için giriş kodunun yazılması zorunludur. Donanım (Hardware) esaslı Chip Kartlı özellikle Smart Kartlı kullanımlarda ise; Chip Kart, pin vasıtasıyla gizli bir şifre ile korunmaktadır. Her iki durumda da kullanıcı, giriş kodunun, özellikle pin'in en iyi bir şekilde saklanmasıyla sorumludur. Alman Medeni Kanununda (BGB) yapılması öngörülen zorlayıcı tedbirlerin, kullanıcıları 6 haneli pin kodlarının güvenli bir şekilde saklanması konusunda motive edip edemeyeceği ise henüz belli değildir (78).

IX. UYGULAMA OLANAKLARI

Dijital imzanın özelliklerini ve yapısını açıkladıktan sonra, aşağıda bir kaç kullanım olanaklarına yer verilecektir:

A. BİR ŞİFRELEME YÖNTEMİ OLARAK: PGP (Pretty Good Privacy)

PGP (Pretty Good Privacy) (79), her türlü elektronik belgenin ve postanın (e-Mail) şifrelenmesinde kullanılan bir yöntemdir. Ayrıca PGP ile belgeleri dijital imza ile imzalamak da mümkündür. PGP son derece yaygın ve şu an Kriptografinin standardı (normu)

(78) Baltus/Woop, <http://www.edvgt.jura.uni-sb.de/Tagung99/ak99/authentifikation.htm>, s. 2.

(79) Versiyon 6.0.2, Amerika kaynaklı bir yazılım (Shareware) programıdır. Ayrıntılı olarak bkz. <http://www.pgp.com>.

olarak kullanılan bir yöntemdir. Gerçek kişiler ve kamuya yararlı kuruluşlar için bu program ücretsizdir. PGP, RSA'nın açık şifre yöntemini kullanmaktadır. PGP, birbirlerini kişisel olarak belki de hiç görmemiş olan kişiler arasında, başkaları tarafından dinlenilmesi mümkün olmayan güvenli bir haberleşme sağlamaktadır (80).

► Şifre Yapımı

► Açık şifrenin Keyserver olarak adlandırılan yere gönderilmesi

► Trust Center'a kişisel bilgilerin (kimlik bilgileri) bildirilmesi

► Açık şifrenin tasdik edilmesinden sonra, Onay verilen kişinin TrustCenter tarafından imzalanmış açık anahtarını alması.

B. HBCI 2.1 (*Home Banking Computer Interface*) (81)

Eylerinden bilgisayar yardımıyla banka işlemlerini halleden kimseler, PIN/TAN (82) usulünü tanımaktadır. Bu yöntemde kişi kendisini PIN ile tanıtmakta ve her bir işlem için sadece bir defa geçerli olan bir TAN kullanmaktadır. Buna rağmen bu yöntemin uygulama alanı son derece sınırlıdır. Çünkü; hesap soruşturmaları ve münferit havale gibi işlemlerin yapılması çok defa bu yöntemle mümkün olmamaktadır. Üstelik bu yöntemi kullanabilmek için, kişi, her zaman bir bilgisayara bağlı olmaktadır.

HBCI 2.1 standardı bu yüzden, daha işlevsel ve ayrıca ister bir bilgisayar ister mobil telefon olsun mümkün olduğu ölçüde her türlü Donanım (Hardware) ile kişilere, banka işlemlerini yapabilme

(80) <http://www.helmbold.de/pgp>, s. 1.

(81) HBCI (Home Banking Computer Interface): Sparkasse (Sparkasse, Almanya'nın büyük Bankalarından biridir) Organizasyonlarının Danışma Merkezlerinden birisidir. Merkezi Kredi Kurulunda organize edilen Alman Kredi Ekonomisi Birlikleri ile bağlantılı olarak, Banka ve müşterileri arasındaki elektronik işlemlerin (Homebanking) güvenli olarak yapılabilmesi için geliştirilen normlar.

(82) PIN: Persönliche Identifikationsnummer, Kişi Tanımlama Numarası.
TAN: Transaktionsnummer, İşlem Numarası.

olanağını sunduğu için daha esnek olarak tanımlanmaktadır. HBCI, bir bilgisayar programı değildir, aksine müşteri ve banka arasındaki bir birleşme noktası ve doğrudan bankacılık için yeni müşterek bir dildir. HBCI, Almanya'daki bütün kredi kurumlarıyla ortak bir çalışma içindedir ve gelecekte müşteri - özellikle müşterinin yazılım programı - ve bankanın bilgi işlem merkezi arasındaki diyalogu düzenleyecektir. Bu Almanya için çok büyük bir adımdır. Çünkü; şimdiye kadar her bankanın kendine ait bir müşteri yazılım programı vardı ve bu kapsamdaki her bir fonksiyon en ince ayrıntılarına kadar düzenleniyordu. Yeni gelişmeler ve düzenlemelere istinaden dijital formlarda değişiklik yapılması gerektiğinde yazılım programı müşteri için kullanılamaz hale geliyordu. Ancak HBCI ile artık bu duruma bir son verilmiştir. Çünkü; her bankanın anlayacağı bir dildir. Yazılım programlarındaki değişiklikleri artık bankaların bilgi işlem merkezlerinden kolayca izlemek mümkündür (83). HBCI ile işlem güvenliği garanti edilmiş olmaktadır, yani verilen talimatın durumu online olarak kontrol edilebilmektedir. Bu özellik PIN/TAN yönteminde mevcut değildir. PIN/TAN yönteminde sadece sonradan hesap ekstresi üzerinden bir kontrol imkanı söz konusudur.

HBCI 2.1'de iki farklı güvenlik yöntemi kullanılmaktadır. Bunlardan ilki, simetrik şifreleme yönteminin kullanıldığı MAC (Message Authentication Code) Yöntemidir. Bu yöntemde Triple-DES/3DES (BKZ. TABLO 3) kullanılır. Bu yöntemin gizli şifresi bir ZKA (84) -Chip Karta kaydedilir (Hardware Çözümü). Diğeri ise, RSA yöntemi. Bu yöntemde ise şifre ya diskete veya diske kopyalanır (Software Çözümü).

Dijital İmza Kanununa göre, Hardware çözümünün kullanılması zorunlu olduğu için, RSA yöntemi Dijital İmza Kanununa uygun değildir. Kanundaki bu handikap nedeniyle piyasalarda gerçekten büyük bir hareketlenme başlamıştır. Çünkü; bütün teşekküllerin amacı standardize ortak bir RSA- Chip Kartı kullanmaktır.

(83) Was ist HBCI? Der Standard der Zukunft, <http://www.hypovereinsbank.de/?Category=/Online.../Infos&Page=WasistHBC>, s. 1.

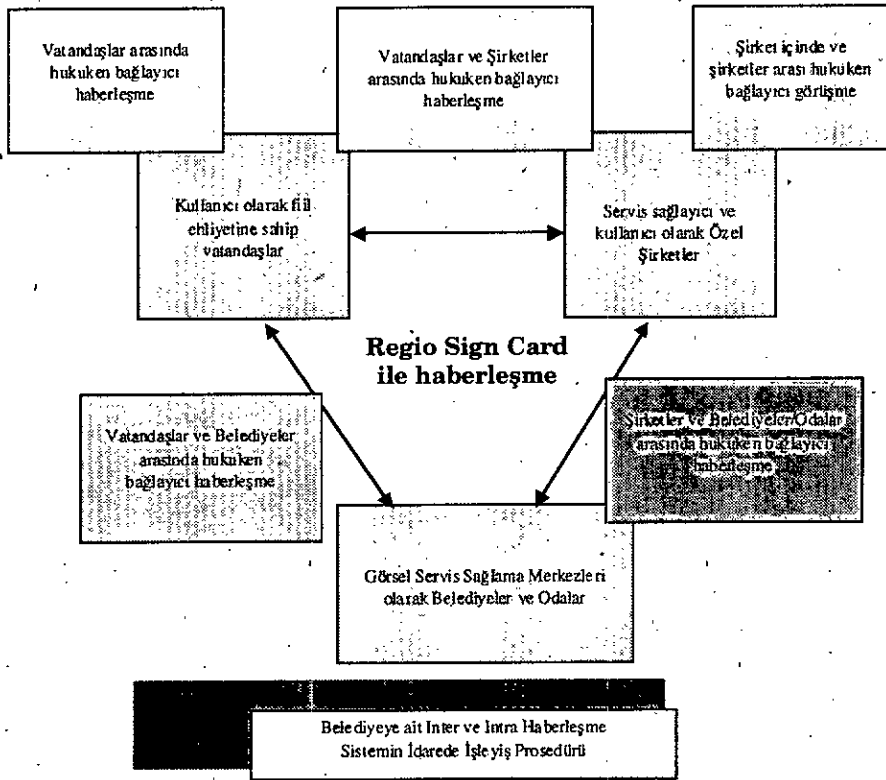
(84) ZKA: Zentraler Kreditausschuss (Merkezi Kredi Komisyonu).

ZKA tarafından kabul edilen ancak henüz yayımlanmayan HB-CI 3.0 Standardının ise mutlaka Dijital İmza Kanununa uygun olması gerekir (85).

C. DİĞER UYGULAMA OLANAKLARI

Alman Hükümeti, bilgi teknolojisi alanındaki olası gelişmeleri ve özellikle bu konudaki çözüm ilkelerini belirlemek için, Staedte-wettbewerb MEDIA@Komm ile birlikte bir rekabet ortamı yaratmıştır. Nürnberg-Führt-Erlangen-Schwabach-Bayreuth, bu rekabette ilk sıralarda yer almışlardır. "RegioSignCard" adlı bu proje-

TABLO 6

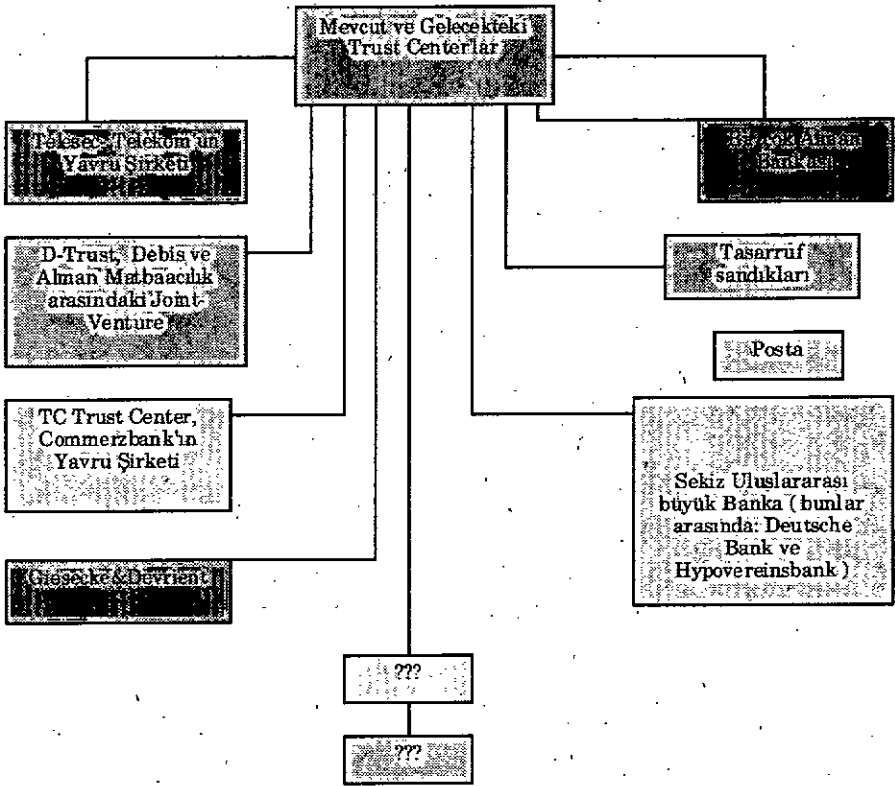


(85) Bu konuda daha ayrıntılı bilgi için bkz. <http://www.hbci-zka.de> veya <http://www.sixsigma.de>.

de; vatandaşlar, işletmeler ve belediyeler arasında gerçekleşen farklı haberleşme olanakları aşağıda açıklanmıştır:

Daha önce değinildiği üzere; Telekom yavru şirketi Telesec ile birlikte kabul edilen ilk Trust Center'dır. Şüphesiz Düzenleme Makamının önünde, bu yönde yapılmış bir çok talep mevcuttur. Aşağıda TABLO 7'de yakın zamanda hangi şirketlerin çalışmalarını Trust Center olarak devam ettireceklerini göstermektedir.

TABLO 7.



X. DİJİTAL İMZANIN ELEŞTİRİLMESİ

İnsan vücudu üzerinde yapılan, teşhis yöntemleri kullanılmadan (örneğin; parmak izi, retina taraması, ses tahlili gibi), dijital imzaya güven konusunda aceleci davranmamak gerekir. Çünkü;

burada sadece bir kaç uzmanın değil, aksine milyonlarca insanın güveni söz konusudur.

El yazısı ile atılan imza, belli durumların dışında hiç bir zaman istemsiz olarak atılmaz ve yine belli durumların dışında kişiler imza atmaya zorlanamazlar. El yazısı ile atılan imzanın tartışmasız diğer bir üstünlüğü de; kişileri aceleci davranmaktan, düşüncesizce hareket etmekten korumasıdır.

Şu an için dijital imzaya yeni ve çekici bir konu olduğu için, yoğun bir ilgi mevcut ise de, zaman içerisinde görülecektir ki, el yazısı ile imza modern multi medya çağına da damgasını vuracaktır. El yazısı imza, alışılmıştan yeniye uzanan köprü işlevi görmeye, internet çağında bile, **"İMZALIYORUM, O HALDE VARIM"** ilkesi geçerli olmaya devam edecektir.

Dijital imza başkalarına devredilebileceği gibi, başları tarafından algoritması çözülebilir; bir çok kişi ve bilgisayar tarafından paralel olarak kullanılabilir ve hatta çalınabilir de. Fakat el yazısı ile imza da bu durumların hiç birisi söz konusu olmamaktadır (86).

El yazısı imzaya ilişkin hiç bir açıklama, dijital imza doğrultusunda bir çağrışım yapmamaktadır. Diğer bir deyimle Chip Kart ve PIN ile atılacak dijital bir imzaya cevaz vermemektedir. Sonuç olarak imzanın el yazısını veya kişinin yazısını ihtiva etmesi gerekir, yoksa bilgisayar klavyesinde tuşlanan pin kodunu değil (87).

Chip Kart ve PIN ile kullanıcıların gerçek kimliği tespit edilmeyeceği için, dijital imza sadece dijital bir kaşe hükmünde olabilir.

Elektronik kaşeler de dahil olmak üzere, tüm kaşeler kolayca elden ele geçebilir. Bu zayıflık daha eski zamanlarda keşfedilmiş ve ortaçağda el yazısı ile imza, mühürlerin yerine geçmiştir (88). El

(86) Köhntopp, <http://www.koehntopp.de>, s. 2 vd.

(87) Baltus/Woop, <http://www.edvgt.jura.uni-sb.de/Tagung99/ak99/authentifikation.htm>, s. 4.

(88) Baltus/Woop, <http://www.edvgt.jura.uni-sb.de/Tagung99/ak99/authentifikation.htm>, s. 5.

yazısı ile atılan imzanın kolayca taklit edilebileceği yolundaki gerekçeler konusunda, bu konunun uzmanları tamamen farklı görüştedirler ve bu görüşlerini araştırmalarında ve doktrinde çok açık ve şüpheyeye yer bırakmayacak şekilde ispat etmişlerdir: **EL YAZISI İLE İMZA TAKLİT EDİLEMEZ!**

XI. PIN'in OPERASYONEL ZAYIFLIĞI: İNSAN FAKTÖRÜ

Pin veya kod numarası ile gerçek bir kimlik tespiti yapılması gerektiği gibi, aynı zamanda bunun ispat edilmesi de gerekir. Hatta gerekirse bir mahkeme kararı ile! Pin'in Chip Kartı üzerine şifrelenmesi en büyük teknik tehlikelere karşı güvenli olabilse dahi, insan faktörünün unutulmaması gerekir. Burada inkar edilemez bir şekilde Pin'in zayıflığı söz konusudur. Bir çok uzman kişi sadece işin teknik ve şifreleme yönleri ile uğraşırken, insan faktörünü dikkate almamaktadırlar.

XII. EL YAZISI İLE İMZANIN ÜSTÜN ÖZELLİKLERİ

- İmza, yegane aktif biyometrik özelliktir
- Belli durumlar dışında, kişiler hiç bir zaman istemeden imza atmaya zorlanamazlar
- Bir irade beyanı göstergesidir
- Asırlardan beri kabul gören bir araçtır
- Uyarı fonksiyonu mevcuttur
- Aynı zamanda hem kağıt üzerinde ve hem de bilgisayar ortamında kullanılabilir. Ancak, el yazısı ile imzanın bilgisayarda hazırlanan metinlerin altına atılması, kişinin el yazısı ile imzasını taşıyan bir sayfanın tarayıcıdan (Scanner) geçirilerek, bilgisayara kaydedilmesi ile gerçekleşmektedir. Bu şekilde kaydedilen imza, kişinin yaptığı yazışmalarda ilgili metnin altına eklenmektedir. ancak el yazısı ile imzanın bu şekilde kullanılması önemli bir sakıncası mevcuttur. el yazısı ile imza sahibinin bilgisayar aracılığıyla haberleştiği ve kendi imzasını taşıyan metinleri gönderdiği kişiler bu imzayı kopyalayarak, imza

sahibi aleyhinde olacak bir çok işlemde kullanabilirler. aynı şekilde birbiri ile haberleşen kişiler dışındaki tamamen yabancı üçüncü kişiler de, sanal ortamda gönderilen metinleri, elde ederek imza sahibinin imzasını kopyalayıp, başka işlemlerde kullanabilirler. Bu yüzden tarayıcıdan geçirilmiş el yazısı ile imzaların, sanal işlemlerde kullanılması konusunda son derece dikkatli olmak veya en iyisi hiç kullanmamak gerekir.

Bir sözleşmenin, bir makbuzun, Avukatın mahkemeye sunduğu bir dilekçenin, taahhütlü bir mektubun ve benzeri bir çok işlemlerin, bir Pin ile tasdik edilmiş olması, bunların ispat güçleri bakımından bir çok sorunuda beraberinde getirecektir. Mahkeme önünde Yazılı Delil esastır ve el yazısı ile imza geçmişte olduğu gibi gelecekte de ilk planda tercih edilmektedir.

Bir davada Alman Yüksek Mahkemesi'nin (BGH) 11. Dairesi şöyle bir tespitte bulunmuştur: " Bir yazı dizisinin prensip olarak, hukuki işlem ehliyetine sahip bir kimse tarafından el yazısı imzalanmasının gerekli olması, tüm Üst Mahkemelerinin süreklilik arz eden içtihatlarına uygundur... " (89).

XIII. ELEKTRONİK BELGELER VE DİJİTAL İMZA İLE İLGİLİ OLARAK ÖNERİLEN BGB § 126a

Alman Hukukunda, Dijital İmza Kanunu ve Yönetmeliği ile yasal bir temele kavuşan dijital imzalı elektronik belgeler hakkında, Alman Medeni Kanununda (BGB) herhangi bir hüküm yoktur. Bu hüküm boşluğunu doldurmak amacıyla, BGB'nin "Kanuni şekil'e" ilişkin olan § 126 hükmüne, yeni bir madde eklenmesi yönünde teklifler yapılmaktadır.

Bu konuda Federal Alman Noterler Odasının değiştirilmiş öneri metni (90) şu şekildedir:

(89) <http://urteile.kanzlei.de>.

(90) <http://www.fitug.de/archiv/presse/para126a.htm>.

BGB § 126a

1. Kanunen elektronik şekil öngörölmüşse, beyanın sahibi hazırladığı metne kendi ismini eklemeli ve hem metni hem de kendi ismini elektronik olarak imzalamalıdır (elektronik imza). Elektronik imzanın, güvenli olarak bilinen bir yöntem içinde, beyandan ve imza sahibinden bağımsız olarak yapılması hazırlanması gerekir. Elektronik imzanın, belgeyi düzenleyen kişinin kimliğinin tespit edilebileceği ve imzanın kontrol edilebileceği, geçerli bir kurum tarafından verilmesi gerekir.
2. Federal Alman İç İşleri Bakanlığı, yetkili iktisadi kuruluşları dinledikten sonra, Adalet Bakanlığı ve Maliye Bakanlığı ile istişare ederek hazırlayacağı yönetmelik ile,
 - I. Elektronik imzanın hazırlanması için gerekli olan teknik alt yapı ve yöntem için gerekli olan güvenlik koşullarını,
 - II. Fıkra 1, cümle 4'te anılan Kurumları ve bu kurumların görev ve yükümlölüklerini,
 - III. Fıkra 2, bend I'e göre tespit edilecek olan güvenlik koşullarını ve bend II'de anılan kurumlarını belirleyecek Federal bir merciyi

belirleyecek ve fıkra 2, cümle 2 anlamında elektronik imzanın hazırlanması yöntemini açıklayacaktır.

Taklit edilmeyi önlemeye yarayan elektro-mekanik teknik ve bir imzanın veya bir giriş kodunun dijitalleştirilmesi ve bunların dijital bir belge ayrılmaz bağılıkları, uluslararası teknolojinin bugün ulaştığı bir noktadır. Bu durum ise, imza bakımından BGB'de herhangi bir değişikliğin yapılmasını kanımızca gerektirmemektedir. Tam aksine; vatandaşların modern iletişime olan güvenleri, klasik imza ile önemli ölçüde güçlenmiş olacaktır. Belgelerin mühürlenmesi yöntemine geri dönölmesi, bu durumu bilgisayar teknikleri daha iyi bir yöntem olarak gösterse bile, ortaçağa geri adım atmak olacaktır. Elektronik medya için, Pin vasıtasıyla el yazısı ile imzanın belgelere eklenmesi de gereksiz bir işlemdir. Bu yüzden Al-

manya'da bir Banka, kredi kartı için hazırladığı bir reklamda şu sloganı kullanmaktadır: Die "Meine Unterschrift ist Geld wert"-Karte.

XIV. ALMAN HUKUKUNDA ELEKTRONİK BELGELERİN DELİL DEĞERİ (İSPAT HUKUKU)

Bilgisayar Hukuku veya Elektronik Data İşleme (EDV) alanına ilgi duyan hukukçular için, Alman ispat hukuku sistemi, elektronik belgelerin delil olarak niteliğini, yazılı belgeler için geçerli olan kurallara değil de, ilk görünüş ispatı ile ilgili kurallara tabi kıldığı için, çağa ayak uyduramayan bir yapıdadır. Bu konuda, elektronik belgelere belli şartlar altında yazılı delil niteliğini bahsetmesi (91) veya en azından bu belgeleri Alman Usul Kanunu (ZPO) md. 416'da kabul edilen kurala göre değerlendirmesi yönünde Kanun koyucuya tavsiyelerde bulunmaktadır (92). Elektronik belgelerin

- (91) **Seidel-Signaturverfahren** (Signaturverfahren und elektronische Dokumente. Rechtliche Bewertung und Regelungsvorschläge), Bestandaufnahme über die elektronischen Signaturverfahren (Veröffentlichung der Gesellschaft für Mathematik und Datenverarbeitung-GMD), St. Augustin 1992, s. 80 vd.; **Seidel-Zertifizierung** (Zertifizierung rechtsverbindlicher und urkundensicherer Dokumentverarbeitung), Bundesnotarkammer (Hrsg.), Elektronischer Rechtsverkehr, Digitale Signaturverfahren und Rahmenbedingungen, Köln 1995, s. 89, 94; **Seidel-Dokumentenschutz**, (Dokumentenschutz im elektronischen Rechtsverkehr), CR 1993, Teil I, s. 409 vd.; Teil II, s. 484 vd.; Geiss, Zivilprozessrechtliche Aspekte des elektronischen Dokumentenmanagements, CR 1993, s. 653, 656; Bergmann/Streitz, Beweisführung durch EDV-gestützte Dokumentation, CR 1994, s. 77, 79.
- (92) Bu konuda örneğin; Ekonomik İdare Hakkındaki Çalışma Grubunun (AWV), "Elektronik Kaydetme Sistemi Esasına Dayalı Belge Yönetiminin Usul Hukuku Açısından Durumu" isimli proje gruplarında Alman Usul Kanununa 416a şeklinde yeni bir maddenin eklenmesi ve içeriğinin şu şekilde olması tavsiye edilmektedir: "Bilgisayara kaydedilen belgeler ve bu belgelerin içerikleri; teknolojinin mevcut durumuna göre uygulanacak yöntem, kayıtlı bilginin gerçekliğini ve belgeyi düzenleyen kişinin teşhisini sağlamaya elverişli ise ve bu teknikler ve düzenleyici tedbirler vasıtasıyla taklit edilmeye karşı korumalı bir düşünce açıklaması söz konusu ise; bu düşünce açıklaması söz konusu ise, bilgisayarda kayıtlı olan bu belgeler ve içerikleri ZPO md. 416 anlamındaki özel yazılı belgelerle eş değerli olacaktır", (AWV-Schrift, 06 531, Eschborn 1993, s. 17 vd.).

İlk Görünüş İspatı (93) delilinin alternatifi olarak değerlendirilmesi, yeterli olarak görülmemektedir. Hatta, eğer Kanun Koyucu arzu edilen tarzda çalışmazsa, Almanya'nın ekonomik durumunun bu yüzden tehlikeye düşeceği bile belirtilmektedir (94). Ve Kilian (95) bunu, yani devlet mahkemelerindeki yargılamanın ispat hukukuna ilişkin kurallarının elverişsizliğini, Alman EDI- Çerçeve sözleşmelerinde Tahkim Klotu kabul edilmesinin bir nedeni olarak göstermektedir.

XV. ALMAN İSPAT HUKUKUNDA ELEKTRONİK BELGELER

Alman ispat hukukunda elektronik belgeler için, öncelikle (her şeyden önce) ilk görünüş ispatının veya yazılı delilin alternatifini teşkil etme durumu söz konusudur. İlk görünüş ispatı, diğer delillerin tüm unsurlarını tam olarak taşımayan bütün belgeler bakımından bir "*torba delil*" niteliğinde olduğu için, yazılı delilin analiz edilmesi ve buradan elde edilen verilerin İlk Görünüş İspatı ile ilgili kurallarla karşılaştırılması, soruna açıklık getirmesi bakımından (elektronik belgeler bakımından hangi delile ait ispat kurallarının uygulanacağını belirleme bakımından) önem taşımaktadır.

(93) İlk Görünüş İspatı hakkında bkz. Baumbach/Lauterbach/Albers/Hartmann-ZIVILPROSESSORDNUNG, 52. Auflage, München 1994, § 415, Rdnr. 3; Rosenberg/Schwab/Gottwald-ZIVILPROZESSRECHT, 15. Auflage, München 1993, s. 697 vd.

(94) Seidel-Dokumentenschutz, s. 170, "...Burada gerçekten elektronik iletişimin delil olarak değerinin tespiti ve bu tespitin hukuki bağlayıcılığı söz konusudur. Hukuki durum şüpheli olduğu için, bir pipette sıkışmış kalmış milyarlık yatırımlar mevcuttur. Bu konu üzerinde yoğun bir şekilde düşünmemiz gerekir ve "Almanya'nın ekonomik durumu" baz olarak alındığında, gerçekten hukuki bir düzenlemeye ihtiyacımız olduğu kanaatindeyim".

(95) Kilian, Zweck und Inhalt des deutschen EDI-Rahmenvertrages, CR 1994, s. 657, 660.

XVI. ALMAN HUKUKUNDA ÖZEL YAZILI BELGELERİN DELİL DEĞERİ

Alman Hukukunda özel yazılı belgelerin (Privaturkunde) ispat hukukundaki durumları şöyle özetlenebilir:

- Alman Usul Kanunu md. 439, 440 gereğince gerçekliğin ispatı, delillerin serbestçe değerlendirilmesi ilkesine tabidir. Eğer belgedeki imzanın ilgili kişiye ait olduğu tartışmasız ise ve imzanın doğruluğu ispat edilebiliyorsa, burada yazılı belgenin gerçekliği lehinde çürütülebilir bir karine mevcuttur.
- Eğer belge imzalanmışsa veya noter vasıtasıyla tasdik edilen bir el işareti ile imzalanmışsa; bu nitelikteki gerçek yazılı belgeler için, Alman Usul Kanunu md. 416'daki ispat kuralı geçerlidir. İçerik olarak doğru olan ancak, yukarıdaki şekilde imzalanmamış olan yazılı belgeler için herhangi bir ispat kuralı yoktur. Bunlar delillerin serbestçe değerlendirilmesi ilkesine tabidirler.
- İçerik olarak doğru olan ve Alman Usul Kanunu md. 416 anlamında imzalanmış olan belge, herhangi bir irade açıklaması içermiyorsa, bu ispat kuralı işe yaramayacaktır. Çünkü; belgenin gerçekliğinin tespiti konusunda mahkemenin kanaatini sağlamlaştırmak için beyanın yapıldığının ispat edilmesi gerekir. İrade açıklamasının gerçeklik değeri ise, hemen her zaman serbest takdire göre belirlenir.
- İçerik olarak doğru olan ve Alman Usul Kanunu md. 416 anlamında imzalanmış olan bir yazılı belge, bir irade beyanını ihtiva ediyorsa, bu durumda md. 416'daki ispat kuralına istinaden, irade beyanında bulunmak şeklindeki maddi hukuki vakıa, aksi iddia edilemez, yani çürütülemez bir şekilde tespit edilmiş olacaktır. Yazılı belge, bu belgeyi düzenleyen kişinin iradesi istemi olmaksızın gündeme gelemeyeceği için, beyanda bulunma vakıası dışında kalan hukuki sonuçların ise, her zaman ispat edilmesi gerekecektir.

XVII. ELEKTRONİK BELGELER BAKIMINDAN ÇIKARILAN SONUÇLAR

Elektronik belgeleri de lege lata veya de lege ferenda yazılı belge ile eş tutarsak, az önce sözünü ettiğimiz kurallardan elektronik belgeler bakımından hangi sonuçları elde edebiliriz? Sorumuzun yanıtı ne yazık ki: "Çok az" olacaktır.

- Elektronik belgelerin gerçekliğinin ispatı delillerin serbestçe değerlendirilmesi ilkesine tabidir. Olsa olsa (belki) elektronik imza taşıyan belgeler bakımından Alman Usul Kanunu md. 440/f.2'ye uygun olarak, eğer elektronik imza ispat edilebilir derecede doğru ise, belgenin gerçekliği doğruluğu lehinde bir karene geçerli olabilir.
- Elektronik imzada Alman Usul Kanunu md. 416'nın imza unsuru için aradığı şartlara benzer bir durum görülmek istenseydi, bu durumda md. 416'daki ispat kuralı sadece elektronik bir belgede yer alan irade beyanları için gündeme gelebilecekti. Elektronik imza, maddi hukuka ilişkin irade beyanında bulunma vakiasının, usul hukuku açısından söz konusu olabilecek şüphelerini ortadan kaldırmakla beraber, yine de elektronik belgenin gündeme getirilmesinin (uyuşmazlıkta kullanılmasının) irade beyanında bulunma vakiası açısından söz konusu olabilecek hukuki sonuçlarının tartışılması ve mahkemenin kanaatinin çürütülmesi gibi konuları açık bırakmaktadır.
- Bilgi açıklamaları bakımından ise, beyanda bulunma vakiası, zaten gerçekliğin ispatı ile birlikte, yani ispat kuralının araya girmesinden önce, yapılmıştır.
- Bilgi açıklamalarının içeriği esasen delillerin serbestçe değerlendirilmesi ilkesine tabidir.

XVIII. ELEKTRONİK YALAN

Elektronik belgenin güvenilirliği bakımından söz konusu olabilecek bu tehlike, bizzat belgeyi düzenleyen kişiden kaynaklanabilir. Elektronik belgelerde de, yazılı belgelerdeki yalan veya yazılı

şekle tabi belgelerdeki hata gibi sorunlar oldukça sık ortaya çıkmaktadır. Ancak yazılı belgelerdeki yalan beyanlar veya hata iddiaları belli şartlar altında keşfedilebildiği veya özel analiz metotları sayesinde tespit edilebildiği halde, elektronik belgelerde sonradan yapılan değişiklikler ise prensip olarak arkasında hiç bir iz bırakmadan yapılabilmektedir. Bu nedenle, yazılı belgeler delillerin serbestçe değerlendirilmesi faaliyeti çerçevesinde elektronik belgelere nazaran, daha fazla kesinlik temin edeceklerdir. Basit bir örnekle açıklamak gerekirse:

Eğer bir kişinin bilgisayarına yazdığı bir mesaj, mahkemede görülen bir davada delil olarak kullanılacaksa, bu belgenin mahkemeye ibraz edilecek nüshasında içerik olarak bazı değişiklikler yapılabilir. Belge lehine olan kimse, içerik olarak kendi elindeki nüshadan farklı bir belge verildiğini iddia etse bile, bu değişiklik mahkeme veya bilirkişi tarafından ispat edilemez. Bu durum, bilgisayarın hafızasındaki bilgilerin kontrol edilmesi yoluyla da tespit edilemez. Bilgisayarın çalışma sistemi bilgileri kaydetme anını, tarih ve saat olarak dakikası dakikasına hafızasına kaydetmesine rağmen, bu veri yine de gerçek kaydetme zamanını göstermesi bakımından güvenilir değildir. Çünkü; bilgisayarın sistem ayarını değiştirmek ve bilgilerin kaydedildiği an olarak, gerçek kaydedilme zamanı ile hiç ilgisi olmayan, tamamen başka bir tarih elde etmek için, küçük bir el hareketi yeterlidir. Hiç kimse elektronik kaydetme sisteminde yapılan bu işlemi fark edemez.

XIX. YETKİLİ OLMAYAN ÜÇÜNCÜ KİŞİLERİN SİSTEMLERE MÜDAHALELERİ

Tehlike, elektronik belgenin düzenlenmesi ile yakından uzaktan ilgisi olmayan üçüncü kişiler tarafından da yaratılabilir. Üçüncü kişiler belgenin bulunduğu bilgisayara bizzat veya network'e bağlı kullanıcılarda ağ üzerinden bilgisayara girip belgede değişiklikler yapabilirler. Üçüncü kişiler tarafından yapılan bu tür sahteciliklerin ve müdahalelerin önüne geçmek ve elektronik belgenin güvenilirliğini artırmak için, çok sıkı tedbirler alınması gerekir. Örneğin; bilgisayara girişin, giriş kodu korumalı olması, bireysel kullanıcılarda ve network'e bağlı kullanıcılarda özel önem taşıyan dosyala-

rın bilgisayar hafızasında değil de, bir diskette, yine özel dosyaların şifreleme yöntemleri yardımıyla şifrlenmesi, verilerin elektronik imza vasıtasıyla korunması, bütün girdilerin ve programların kayda geçirilmesi gibi.

XX. ELEKTRONİK BELGELERİN DELİL DEĞERİ HAKKINDAKİ SONUÇLAR

Elektronik belgelerin gerçekliğinin ve orijinalliğinin dijital imza ile sağlanması ve bunun yöntemleri hakkındaki yukarıdaki açıklamalara göre, elektronik belgelerin Alman İspat Hukukundaki ispat gücü hakkında şu sonuçlar çıkarılabilir:

- Alman Usul Hukuku, elektronik belgeler ile delil ikame edilmesi konusunda herhangi bir sınırlama içermemektedir. Elektronik belgeler geçerli ispat vasıtalarıdır. Bu belgeler ya ilk görünüş ispatı veya bilirkişi delili kapsamında değerlendirilmektedir. Mahkemenin, elektronik belgenin görsel içeriği hakkında bizzat bilgi sahibi olmak istediği durumlarda, ilk görünüş ispatından bahsedilmektedir. Elektronik belgenin görselleştirilmesi veya gerçekliği veya orijinalliğinin kontrolü için uygulanması gereken yöntem, özel bilgi ve yetenekleri gerektiriyorsa, bu durumda ise bilirkişi delili söz konusu olmaktadır.
- Elektronik belgelerin, gerçekliği, değiştirilemezliği ve güvenilirliğine yönelik önemli sorular, her halükarda delillerin serbestçe değerlendirilmesi ilkesine tabidir.

XXI. TÜRK İSPAT HUKUKU BAKIMINDAN DİJİTAL İMZALI ELEKTRONİK BELGELERİN DELİL OLARAK DEĞERİ

Öncelikle şu hususu belirtmemiz gerekir ki; dijital imza her sözleşme tipinde kullanılamayacaktır. Noterler veya resmi memurlar tarafından düzenlenmesi gereken sözleşmeler (evlenme, gayrimenkul mülkiyetinin nakli vs.) hariç olmak üzere, diğer sözleşme tiplerinde dijital imza son derece günceldir.

Türk İspat Hukuku sisteminde, Kanuni Delil sistemi mevcuttur. Bu sisteme göre hakim, Hukuk Usulü Muhakemeleri Kanununda (HUMK) sayılan ve Kesin Delil olarak da adlandırılan, ikrar (HUMK md. 236), kesin hüküm (HUMK md. 237), senet (HUMK md. 286 vd.) ve yemin (HUMK md. 377 vd.) delillerinden biri ile ispat edilen bir vakıayı, doğru olarak kabul etmek zorundadır. Yani hakim, bu delillerle bağlıdır ve bu delilleri takdir yetkisi yoktur (96).

Hukuk Usulü Muhakemeleri Kanunumuz, kesin deliller kategorisi yanında, ayrıca Takdiri Delilleri de düzenlemektedir. Takdiri deliller ile hakim, kesin delillerin aksine bağlı değildir. Bu delillerle ispatlanan bir vakıanın doğru olup olmadığını serbestçe takdir eder. Bunlar; tanık (HUMK md. 245 vd.), bilirkişi (HUMK md. 275 vd.), keşif (HUMK md. 363 vd.) ve özel hüküm sebepleridir (HUMK md. 367) (97).

Hukuk Usulü Muhakemeleri Kanununun mevcut bu yapısına göre, bir vakıanın veya hukuki işlemin elektronik bir belge ile ispatlanmasına herhangi bir yasal engel yoktur. Elektronik belgelerin, daha doğrusu dijital imza taşıyan elektronik belgelerin (98), Kanunda sayılan hangi delil türüne gireceği konusunda ise, aşağıdaki şu kriterlerin dikkate alınması gerekecektir: Hukuk Usulü Muhakemeleri Kanunu md. 288/f.1'e göre; bir hakkın doğumu, düşürülmesi, devri, değiştirilmesi, yenilenmesi, ertelenmesi, ikrar ve itfası amacıyla yapılan hukuki işlemlerin, yapıldıkları zamanki miktar veya değeri kırk milyon lirayı (99) geçtiği takdirde senetle ispat olunması gerekir. Senetle (veya kesin delille) ispat zorunluluğu olarak adlandırılan bu kurala göre; yapıldıkları zamanki miktar veya değeri 40 milyon lirayı geçen hukuki işlemlerin kanunda

(96) Kuru, s. 1398.

(97) Kuru, s. 1399.

(98) Önemle belirtmemiz gerekir ki; dijital imza, noter aracılığıyla veya resmi memur tarafından yapılması gereken belirli sözleşme tipleri hariç, son derece yaygın bir kullanım alanına sahiptir.

(99) 4146 sayılı Kanun ile HUMK'a eklenen Ek. md. 3.

sayılan istisnalar saklı kalmak koşuluya (100), kesin delillerden biri ile ispatlanması zorunludur. Bu hukuki işlemler, kural olarak tanıkla ispat edilemez. Senetle (veya kesin delille) ispat zorunluluğu hakkındaki ikinci ana kural ise, senede karşı senetle ispat zorunluluğudur. Bu kurala göre; senede bağlı olan her çeşit iddiaya karşı savunma olarak ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemler, kırk milyon liradan az miktara ilişkin olsa bile, anıkla ispat olunamaz. Ancak senetle (veya kesin delille) ispat edilebilir. Hukuk Usulü Muhakemeleri Kanununda bu ikinci ana kuralın da istisnalarına yer verilmiştir (101). İşte ispat hukuku sistemimize hakim olan bu her iki ana kural çerçevesinde; elektronik ortamda yapılan ve miktar veya değeri 40 milyon lirayı geçen bir hukuki işlemin ispatı için, altında borçlunun dijital imzasını taşıyan elektronik bir belge mahkemeye ibraz edilirse, acaba hakim, bu belgeyi adi senet (HUMK md. 299/f.1; md. 314) olarak kabul edebilecek midir? Bu sorunun ve aşağıdaki diğer soruların cevaplanabilmesi, Ülkemizde de dijital imza konusunda yasal bir düzenleme yapılmasına ve bu düzenleme çerçevesinde ilgililere dijital imza verecek olan Onay Kurumlarının veya Trust Center'ların kurulmasına bağlıdır. Diğer bir ifade ile, gerek ulusal (örneğin; Türk vatandaşı olan kişiler – gerçek ve/veya tüzel kişiler – arasında sanal ortamda yapılan hukuki ilişkiler) gerekse uluslararası (örneğin; bir Türk vatandaşı ile yabancı bir ülke vatandaşı veya tüzel kişisi arasında sanal ortamda yapılan hukuki ilişkiler) nitelik taşıyan dijital imzalı elektronik belgelerin delil değeri, öncelikle Kanun koyucunun bu konuda yasal bir düzenleme yapmasını gerektirmektedir (102). Ülkemizde bu konuda yasal bir düzenleme mevcut olduğunu farz et-

(100) Bu istisnalar: HUMK md. 287/f. 2; md. 289; md. 292; md. 293; md. 294.

(101) Bkz. HUMK md. 287/f. 2; md. 289; 292; md. 293/f. 3, 5; md. 294

(102) Sanal ortamda gerçekleştirilen hukuki ilişkiler daha çok uluslararası nitelik taşıdığı ve son derece sık kullanıldığı için, günümüzde bir çok dünya devleti tarafından sadece ulusal boyutta yasal düzenlemeler, gelecekte bir çok ülkeyi birden ilgilendiren uluslararası bir hukuki sorun olarak karşımıza çıkacak ve Kanun koyucuların dijital imza konusunda çok taraflı uluslararası sözleşmelere imza atmaları sonucunu doğuracaktır.

sek bile, az önceki sorunun cevabı : "*Hayır*" olacaktır. Çünkü; yukarıdaki açıklamalarımızda da belirttiğimiz gibi; dijital imza, imza sahibini hiç bir şekilde karakterize etmemekte ve algoritmasının üçüncü kişiler tarafından çözülebilmesi tehlikesini bünyesinde taşımaktadır. Bu nedenle de el yazısı imza ile bir tutulması mümkün değildir (103). Dijital imzalı elektronik belgeler, adi senet delili kapsamında altlanamadığına göre, acaba Kanunumuzda yer alan hangi delil veya deliller kategorisinde yer alacaktır? Hakim, hukuki bir işlemin ispatı için kendisine ibraz edilen dijital imzalı bir elektronik belgeyi ya yazılı delil başlangıcı (HUMK md. 292) olarak veya özel hüküm sebebi (HUMK md. 367) olarak kabul edebilecektir. Ancak bilgisayarda hazırlanan bir elektronik belgede, borçlunun parafının veya el yazısı ile yaptığı bir takım çıkıntıların mevcut olması gerektiği ileri sürülebilir. Daha önceki açıklamalarımızda belirttiğimiz gibi, dijital imza da borçlunun bir tür parafıdır. İleride Ülkemizde sorun yasal bir çözüme kavuştuğunda, dijital imza sahibi olmak için Kanun koyucunun belirleyeceği, izlenmesi gereken prosedüre göre hareket edilmiş ve dijital imza vermeye yetkili olacak bir kurumdan (Onay Kurumu, Trust Center) imza yetkisi alınmışsa; elektronik belge altında yer alan dijital imzayı, borçlunun parafı olarak kabul etmemek için herhangi bir sebep olmayacaktır. Çünkü; hakim, eğer kendisi bu konuda özel ve teknik bilgiye sahip değilse, bilirkişi yardımıyla dijital imzanın alındığı kurumdan, elektronik belge altındaki dijital imzanın gerçekten o kişiye ait olup olmadığını tespit ettirebilecektir. Ancak; eğer dijital imza, borçlunun parafı olarak kabul edilmek istenmiyorsa, bu durumda Türk İspat Hukukunun "*Torba Delili*" olarak da adlandırabileceğimiz Özel Hüküm Sebebi olarak kabul edilmesi gerekir. O halde dijital imzalı elektronik belgeler, Türk Hukukunda Takdiri Delil niteliğindedir. Ayrıca hakim, elektronik belgelerin görsel içeriği hakkında, özel ve teknik bilgisinin yeterli olduğu durumlarda bizzat değerlendirme yapacak (ilk görünüş ispatı); konu hakkında özel ve teknik bilgiye sahip olmadığı durumlarda ise, bil-

(103) Bkz. yuk. s. 23.

gisayar uzmanı bilirkişilere müracaat ederek, edineceği kanaate göre bir karar verecektir (bilirkişi delili).

Hukuk Usulü Muhakemeleri Kanunumuz, md. 287/f. 2 ve md. 289'da; senetle ispat zorunluluğuna ilişkin her iki ana kuralın istisnalarından biri olan "*delil sözleşmesi*" kurumunu düzenlemiştir. Bu hükümler incelendiğinde, Kanunda iki çeşit delil sözleşmesi düzenlendiğini görüyoruz. Bunlar: Münhasır ve münhasır olmayan delil sözleşmesidir. Münhasır delil sözleşmesinde, uyuşmazlığın tarafları, uyuşmazlık doğduktan sonra veya daha uyuşmazlık doğmadan önce, bir vakıanın veya hukuki işlemin, sadece belli bir delil ile ispat edilebileceği konusunda aralarında bir anlaşma yapmaktadırlar. Bunun sonucu olarak, taraflar, o vakıayı veya hukuki işlemi, sadece aralarında kararlaştırdıkları delil ile ispat edebilirler (örneğin; aslında tanıkla ispatı mümkün olan bir hukuki işlemin sadece senetle ispat edilebileceğini kararlaştırmışlarsa, o hukuki işlem sadece senetle ispatlanabilir). Başka bir delil ile ispat edemezler (md. 287/f. 2). Münhasır olmayan delil sözleşmesinde ise, taraflar, kendilerini ispat konusunda belli delil veya delillerle sınırlamak yerine, bir vakıanın veya hukuki işlemin başka bir delil ile de ispat edilebileceğini kararlaştırabilirler (örneğin; taraflar, aslında senetle ispatı mümkün olan bir hukuki işlemin, tanıkla da ispat edilebileceğini kararlaştırabilirler). İşte Usul Kanunumuzda yer alan münhasır ve münhasır olmayan delil sözleşmesi kurumlarını taraflar, ileride dijital imzalı elektronik belgeler bakımından da yapabileceklerdir. Örneğin; dijital imzalı elektronik belgede yapılan hukuki işlemin miktar veya değeri 40 milyon TL.'yi geçtiği için senetle ispat edilmesi gerekirken, taraflar bu işlemin takdiri delillerle ispat edilebileceğini münhasır veya münhasır olmayan delil sözleşmesi ile kararlaştırabileceklerdir.

Sanal sözleşmenin tarafları, aralarındaki sözleşmede, "*Bu sözleşmeden doğacak uyuşmazlıkların çözümünde ...tahkime gidilecektir...*" şeklinde, tahkim klotlarına da yer verebilirler. Yani elektronik ortamda yapılan hukuki işlemlerden doğacak uyuşmazlıklarda mahkemeler değil, hakemler de yetkili kılınabilir. Yine taraflar, tahkim ve mahkeme dışında, "*Alternatif Yargı Yolları – Alternative*

Dispute Settlement – " olarak adlandırdığımız yollara da müracaat edebilirler. Bunlardan en yaygın olarak kullanılanı Mediation'dır (104).

Dijital imzalı elektronik belgeler bakımından, ispat yükü ile ilgili Medeni Kanun md. 6'daki genel kuralın da irdelenmesi gerekmektedir. Medeni Kanun md. 6'ya göre; Kanun hilafını emretmedikçe, iki taraftan her biri iddiasını ispata mecburdur. Diğer bir ifade ile; bir vakıadan kendi lehine haklar çıkaran taraf o vakıayı ispat etmelidir (105). Elektronik belgelerde ise, belgeyi dijital olarak imzaladığı iddia edilen kişi, yani dijital imzanın sahibi, bu belgeyi dijital olarak imzalamadığını ispat etmelidir. Görüldüğü gibi burada ispat yükü yer değiştirmiş ve dijital imza sahibinin durumu ağırlaştırılmıştır. Ancak ispat yükünün bu şekilde, iddia eden kimseden, dijital imza sahibine geçmesi ve imza sahibinin ispatla yükümlü kılınması haksız bir sonuç değildir. Çünkü; dijital imzanın haberleşme işleminin tarafları dışında, üçüncü kişilere karşı gizliliğinin sağlanması hem onay kurumunun hem de dijital imza sahibinin vazifesidir. Özellikle imza sahibinin, şifresini saklı tutmak konusunda bir özen borcu vardır. Bu yükümlülüğüne aykırı davranan ve şifresinin üçüncü kişiler tarafından öğrenilmesine sebep olan dijital imza sahibi, bu davranışının sonuçlarına katlanmalıdır. İspat yükü bu şekilde yer değiştirmezse; yani karşı taraf, imzanın dijital imza sahibi tarafından atıldığını ispatla yükümlü kılınırsa, bu durum hem söz konusu vakianın ispat edilmemesi hem de sanal ortamda artık işlem yapılamaması sonucunu doğurur. Çünkü; internette ticaret yapan hiç bir firma, zaten kişisel olarak tanıma olanağına sahip olmadığı bir kimse ile akdettiği sözleşmede yer alan imzanın, aslında o kişi tarafından atılmadığını ispatla yükümlü olmak istemeyecektir.

(104) Ayrıntılı olarak bkz. <http://www.mediation.com>.

(105) Kuru, s. 1358.

SONUÇ

Dijital imza; elektronik ticaret alanında ilişkileri kolaylaştırma, hızlandırma ve elektronik belgeleri yasallaştırma gibi cazip özelliklere sahiptir. Ancak, dijital imzanın ve elektronik ilişkilerin güvenilirliğini sağlamaya ve artırmaya yönelik bilgisayar programları bu konuda ne kadar iddialı olurlarsa olsunlar, kanımca "*insan faktörü*" yüzünden, bu iddialarında yüzde yüz haklı oldukları söylenemeyecektir. Ne kadar çözülmesi zor ve karmaşık bir matematik şifreye dayanırsa dayansın, sanal ortamda yapılan işlemlerin, işlemin tarafları dışındaki üçüncü kişiler tarafından kesinlikle görülemeyeceğini, elektronik belgelerin başkaları tarafından değiştirilemeyeceğini iddia etmek mümkün değildir. Ancak gelişen teknoloji ve uluslararası ticari ve ekonomik ilişkilerin "*e-Ticaret*" sloganı ile internette yoğunlaşması, hemen her ülkeyi bu değişimde ve pazarda yer alma konusunda zorlamaktadır. Aksi halde, uluslararası ilişkilerde yaşanan hıza ve teknolojiye ayak uyduramama yüzünden kaynaklanan, geçmişte örneklerini oldukça sık olarak yaşadığımız sorunlar tekrar gündeme gelecektir. Bu tablo karşısında Ülkemizde de yakın bir tarihte, dijital imza prosedürü ve dijital imzalı elektronik belgeler konusunda yasal düzenlemeler yapılması kaçınılmaz bir hale gelecektir. Çünkü; bu konuda bir yasa boşluğu mevcut olmasına rağmen, bir çok Türk vatandaşı internet üzerinden yerli veya yabancı şirketlerle bağlantı kurarak sanal sözleşmeler yapmakta ve ürün siparişleri vermektedirler. İşlemin her iki tarafı açısından da "*her şeyin yolunda gideceği umularak*" yapılan bu sözleşmelerden doğabilecek uyuşmazlıkların nasıl çözümleneceği, ispat kurallarının sanal işlemlerde nasıl uygulanacağı gibi noktalar, Türk Kanun koyucusunu bu konuda tavır alması için bekleyen sorulardır.

YARARLANILAN KAYNAKLAR

Baltus/Woop, <http://www.edvgt.jura.uni-sb.de/Tagung99/ak99/authentifikation.htm>, s. 2.

Bauer, Friedrich L.; Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie, 1. Auflage, Berlin 1995.

Baumbach/Lauterbach/Albers/Hartmann- ZIVILPROZESSORDNUNG, 52. Auflage, München 1994, § 415, Rdnr. 3; Rosenberg/Schwab/Gottwald-**ZIVILPROZESSRECHT**, 15. Auflage, München 1993, s. 697 vd.

Bergmann/Streitz, Beweisführung durch EDV-gestützte Dokumentation, CR 1994, s. 77, 79.

Beutelspracher, Albert; Kryptologie, 5. Auflage, Braunschweig/Wiesbaden 1996 (Internet adresi: <http://www.uni-giessen.de>);

Bizer, Johann; Rechtliche Bedeutung der Kryptographie. Datenschutz und Datensicherheit (DuD) 1997, s. 203- 208.

Bizer, Johann/Fox, Dirk; "Digital Signierte Zukunft". Datenschutz und Datensicherheit (DuD) 1997, s. 66.

Boss, Amelia H.; Tearing Down Paper Barriers, Uniform Electronic Transactins Act Sets New Contract Rules, LEXIS-NEXIS Academic Universe-Documment, file://C:\WINDOWS\TEMP\digitalsignaturesart2.htm., s. 1-5.

Engel-Flehsig, Stefan/Maennel, Fritjof A./Tettenborn, Alexander; Das neue Informations-und Kommunikationsdienste-Gesetz. Neue Juristische Wochenschrift (NJW) 1997, s. 2981-2992.

Gramlich, Ludwig; "Elektronische s Geld" im Recht. Datenschutz und Datensicherheit (DuS) 1997, s. 383-389;

Geiss, Zivilprozessrechtliche Aspekte des elektronischen Dokumentenmanagements, CR 1993, s. 653, 656;

Gerling, Rainer W.; Verschlüsselungsverfahren. Eine Kurzübersicht. Datenschutz und Datensicherheit (DuD) 1997, s. 197-202;

Grimm, Rüdiger; Kryptoverfahren und Zertifizierungsinstanzen. Datenschutz und Datensicherheit (DuD) 1996, s. 27-36;

Herreiner, Dorothea K.; Die volkswirtschaftliche Bedeutung elektronisches Geldes. Datenschutz und Datensicherheit (DuD) 1997, s. 390-395)

Huhn, Michaela/Pfitzmann, Andreas; Krypto(de)regulierung. Datenschutz-Nachrichten (DANA) 1996, Heft 6, s. 4-13 (Internet adresi: http://www.informatik.uni-hildesheim.de/FB4/Projekte/sire-ne/lit/abstr96.html#HuPf2_96);

Kilian, Wolfgang; Zweck und Inhalt des deutschen EDI-Rahmenvertrages, CR 1994, s. 657, 660.

Knorr, Michael/Schlaeger, Uwe; Datenschutz bei elektronischem Geld. Ist das Bezahlen im Internet Anonym?. Datenschutz und Datensicherheit (DuD) 1997, s. 396-402;

Köhntopp, Kristian; Beweiskraft von PGP-Signaturen, <http://www.koehn-topp.de>.

Königsmann, J.; Elliptische Kurven, <file:///A:/koenigsmann001.htm>.

Kuru, Baki; Hukuk Muhakemeleri Usulü, 5. Baskı, Cilt. 2, İstanbul 1990.

Ohst, Daniel; Vertrauliche Kommunikation, 9.Mai.1996, <http://www2.rz.hu-berlin.de>.

Özsunay, Ergun; Elektronik Sözleşmeler (AB Hukuku İle Avusturya ve Alman Hukuklarındaki Gelişmelerin Işığında Türk Hukukuna İlişkin Çözümler), AB'de, BAZI ÜYE DEVLETLERDE VE TÜRKİYE'DE ELEKTRONİK TİCARETİN HUKUKSAL SORUNLARI – ELEKTRONİK SÖZLEŞMELER – KONULU SEMİNER, 12 MAYIS 2000, İSTANBUL.

Petersen, Holger; Anonymes elektronisches Geld. Der Einfluss der blinden Signatur. Datenschutz und Datensicherheit (DuD) 1997, s. 403-410;

Rosenberg/Schwab/Gottwald-ZİVİLPROZESSRECHT, 15. Auflage, München 1993, s. 697 vd.

Rossmagel, Alexander; Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung. Datenschutz und Datensicherheit (DuD) 1997, s. 75-81.

Schmidt, Jens-Uwe/Ungerer, Bert; Al dente. IX 1997, Heft 4, s. 128-131 (İnernet adresi: <http://www.heise.de/ix/artikel/1997/04/128/artikel.shtml>).

Schneier, Bruce; Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in Computer. Almanca tercümesinin 1. Basısı, Bonn 1996; Telesec: Kryptokontroverse, 9 August 1996,

Seidel, Signaturverfahren und elektronische Dokumente. Rechtliche Bewertung und Regelungsvorschläge), Bestandaufnahme über die elektronischen Signaturverfahren (Veröffentlichung der Gesellschaft für Mathematik und Datenverarbeitung-GMD), St. Augustin 1992, s. 80 vd. (**Signaturverfahren**);

- Zertifizierung rechtsverbindlicher und urkundensicherer Dokumentverarbeitung, Bundesnotarkammer (Hrsg.), Elektronischer Rechtsverkehr,

Digitale Signaturverfahren und Rahmenbedingungen, Köln 1995, s. 89, 94 (Zertifizierung);

- Dokumentenschutz im elektronischen Rechtsverkehr, CR 1993, Teil I, s. 409 vd.; Teil II, s. 484 vd. (**Dokumentenschutz**);

Seiler, Wolfgang K.; Elliptische Kurven, <file:///A:/elkurven.htm>.

Tanenbaum, William A.; State Electronic Signatures and Records Act, Enabling Regulations Have Taken Effect, LEXIS-NEXIS Academic Universe-Dokument, <file:///C:/WINDOWS/TEMP/digitalsignaturesart.htm>, s. 1-11.

Timm, Birte; Signaturgesetz und Haftungsrecht. Datenschutz und Datensicherheit (DuD) 1997, s. 525-528.

LINKLER

<http://www.hypowelt.de/info/unterschrift.htm>
<http://www.mbnetkey.ch/sgnrecht4.htm>
<http://www.intern.de/97/22/29.shtml>
<http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>
<http://www.mille.com.ar/>
<http://aix1.uottawa.ca>
http://www.law.co.il/computer-law/digsig_1stdraft.doc
http://www.globalsign.com.tr/195.207.49/general/en/fagsg_body.htm
<http://www.telesec.de/recht3.htm>
<http://www.helmbold.de/pgp>
<http://www.ec-guide.com/technologien/16-1-5-2-Signatur.asp>
<http://nestroy.wi.uni-essen.de/L.v/ibis2/folien/07-10.html>
<http://www.provet.org/bib/mmge/er-gb.htm>
<http://www.iid.de/rahmen/iukdgbt.html>
<http://www.iid.de/rahmen/iukdgbt.html>
<http://www.ec-guide.com>
<File://A:\Internet-Recht.htm>
<http://www.europa-eu.int>
http://e2i.e2i.at/AA/1p19991130elektronische_unterschriften.htm
http://www.beck.de/rsw/zeitschr/njw/Archiv/Heft49_99/Wochenspiegel/wosp15.htm
<http://www.iid.de/rahmen/iukdg.html>
<http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>
<http://www.ec-guide.com>
<http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>
<http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm>
<http://www.mbc.com/ecommerce.htm>
<http://www.europa.eu.int>
<http://urteil.kanzlei.de>
<http://www.hbci-zka.de>
<http://www.sixsigma.de>

BİLİMSEL YAZILAR

"Faelschungssicherer unterschreiben", Fracht und Materialfluss, Mai 1999, s. 43 vd.

"Digitale Unterschrift besiegelt Vertraege", Welt am Sonntag, 1999/1, s. 65 vd.

"Chancen und Risiken des Faktors Information – Auswirkungen auf Politik, Gesellschaft, Wirtschaft und Militaer". Forum der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik, Bonn-Bad Godesberg, 19-20 November 1997, Kompendium.

"Elektronische Unterschrift Kommt (Sicherheit im Internet für rund 150 Mark) (Digitale Signatur soll Hackern ab 1999 das Handwerk legen)", <http://www.rhein-zeitung.de/on/98/04/27/topnews/esign.html>, s. 1-2.

"Loch im Datennetz", Focus 1998/3, s. 158.

Leicher Trendforum : "Biometrische Identifikationssysteme", München 1997/11 (Vortrag von Dr. Bockslaff).

Echtheits-Zertifikat, Computer Technik, 1998, s. 113.

KISALTMALAR CETVELİ

AG Aktien Gesellschaft (Anonim Şirket)

Aşa aşağıda

Auflage Bası

AWV Arbeitsgemeinschaft für Wirtschaftliche

..... Verwaltung (Ekonomik İdare Çalışma Grubu)

BGB Bürgerliches Gesetzbuch (Alman Medeni Kanunu)

BGH Bundesgerichtshof (Alman Yüksek Mahkemesi)

Bkz. bakınız

CT Computer Technik (Dergi)

DANA Datenschutz-Nachrichten (Dergi)

DES Data Encryption Standard (Şifreleme Programı)

DH/DSS Diffie-Hellmann/Digitale Signatur Standard
(Dijital İmza Algoritması).

DuD Datenschutz und Datensicherheit (Dergi)

e-Commerce....	Elektronik Ticaret
EDI	Electronic Data Interchange (Elektronik Data Değişimi)
EDV.....	Elektronische Datenverarbeitung (Elektronik Data İşleme)
EFT	Elektronik Fon Transferi
EU	Europäische Union (Avrupa Topluluğu)
f.	fıkra
FVIT	Fachverband Informationstechnik (Dergi)
HBCI	Home Banking Computer Interface (Bilgisayar Programı)
Hrsg.....	Herausgeber (Editör)
HUMK.	Hukuk Usulü Muhakemeleri Kanunu
IDEA	International DataEncryption Algoritim (Şifreleme Programı)
İuKDG.....	Informations-und Kommunikationsdienstgesetz (Bilgi ve İletişim Hizmetleri Kanunu)
md.....	madde
NJW.....	Neue Juristische Wochenschrift (Dergi)
PGP	Pretty Good Privacy (Dijital imza ve mesaj şifreleme programı)
PIN	Persönliche Identifikationsnummer
RSA	Rivest, Shamir ve Adleman tarafından tasarlanan Algoritmaya verilen isimdir.
s.	sayfa
SigG.....	Signaturgesetz (Dijital İmza Kanunu)
SigV.....	Signaturverordnung (Dijital İmza Yönetmeliği)
StPO	Strafprozessordnung (Alman Ceza Usul Kanunu)
TAN.....	Transaktionsnummer (İşlem Numarası)
TL.....	Türk Lirası
vd.	ve devamı
yuk.	yukarıda
ZKA	Zentraler Kreditausschuss (Merkezi Kredi Komisyonu)
ZPO	Zivilprozessordnung (Alman Usul Kanunu)