

Dijital İmzanın Hukuksal Açıdan İncelenmesi

Rüya ŞAMLI

Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi, İstanbul
e-posta: rsamli@istanbul.edu.tr

Özetçe

İmza, en genel tanımıyla bir kişinin, bir yazının, bir belgenin altına, bu yazıyı yazdığını veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işaretler olarak tanımlanabilir. Bir insan yaşamı boyunca pek çok imza atmaktadır. Resmî evraklardan sınavlara kadar pek çok yerde binlerce kez kullanılan imza kişi için büyük bir önem arz etmektedir. Özellikle hukuksal işlemlerde imza atmak çok önemli sonuçlar doğuran bir işlemdir. Günümüzde artık pek çok işlemin dijital ortamlar ve internetten yapılabilmesi sonucunda, kimlik doğrulamayı sağlayan imza işleminin dijital otama da taşınması gerekmiştir. Bu çalışmada bu amaçla ortaya çıkan elektronik imza kavramı, bu kavramın bir çeşidi olan dijital imza ve bu kavramın uluslararası çerçevede ve Türk hukuku açısından durumu incelenmiştir.

1. Giriş

Günümüzde, kağıtla yapılan pek çok işlemi artık dijital dünyada da yapmak mümkündür. Bankacılık işlemleri, pasaport başvuruları, sigorta işlemleri, otobüs, tren, uçak, sinema, tiyatro bileti rezervasyon ve satın alma işlemleri, vergi, fatura ödeme işlemleri, sınav başvuruları, öğrencilerin ders seçimlerini gerçekleştirmeleri, kimlik no, vergi no gibi bilgilerin öğrenilmesi bu işlemlerden bazılarıdır. İnternet üzerinden yapılan işlemlerde kimlik doğrulama işlemi genelde bir kullanıcı adı ve şifre kullanılarak gerçekleştirilmektedir. Ancak bu doğrulama işlemi, kolay kırılabilme riskinden dolayı kimlik bilgisinin hayatı önem taşıdığı uygulamalar için çok uygun bir işlem olarak kabul edilmez. Bu sebeple dijital imza kavramı ortaya çıkmıştır.

2. Dijital İmza

Dijital imza kavramını anlayabilmek için öncelikle elektronik imza kavramı hakkında bilgi sahibi olmak yarar vardır. Elektronik imza ya da diğer şekliyle e-imza, "elektronik ortamda kişinin kendi olduğunu kanıtlama tekniğidir" şeklinde tanımlanabilir. Kişinin doğruluğu kağıt ortamında el imzası, mühür vb ile kanıtlanırken, elektronik ortamda da e-imza ile kanıtlanmaktadır [1]. E-imza ile kavramı çok geniş bir kavramdır. Kişilerin göz retinası, parmak izi gibi biyolojik özelliklerinin kullanıldığı biyometrik güvenlik yöntemleri veya kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, bunlara örnek olarak gösterilebilir. Dijital imza ise elektronik imzanın günlük hayatta kullanılan imzalarda olduğu gibi, elektronik ortamda gönderilen bilginin veya e-mail'in kime ait olduğunu

göstermek için kullanılan bir çeşiddir [2]. Asimetrik şifreleme tekniğine dayanan, içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilen bir imza şeklidir.

Dijital imzaların oluşturulmasında ve doğrulanmasında dijital sertifikalar kullanılır. Herhangi bir veriyi dijital olarak imzalayabilmesi için bir kişinin kendine has bir dijital sertifikası bulunmalıdır.

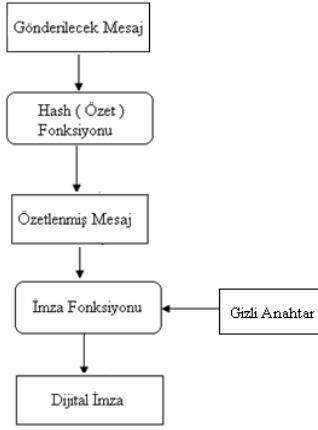
2.1. Dijital İmzanın Özellikleri

- Dijital imza bir kullanıcı, sunucu ya da host'tan gönderilen bilgilerin kesinlikle o kuruma veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eder.
- Dijital imza, veri akışı sırasında bilgilerin içeriğini korur, bir başka kişinin eline geçmesini ya da değiştirilmesini engeller, bilginin sadece alıcıya gittiğini ve sadece alıcı tarafından okunacağını garanti eder.
- Dijital imza, veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkan tanır. İmzalanmış bir dokümanı yollayan kişi onu yolladığını; alıcı da aldığını inkar edemez [3].

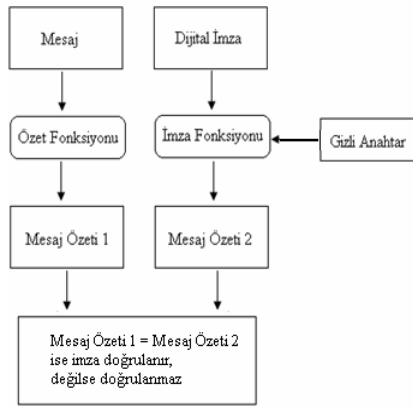
2.2. Bir Dijital İmza Nasıl Oluşturulur ve Doğrulunur?

Dijital imza, gönderilecek mesaj üzerinde değil, mesajın özeti üzerinde işlem yaparak oluşturulur. Gönderilecek mesaj özgün bir biçimde kısaltılarak (özet fonksiyonundan geçirilerek) mesajın yeni bir versiyonu elde edilir, buna "hash" adı verilir. Bu özetten mesajın tamamına erişmek mümkün değildir, diğer bir deyişle hash fonksiyonu geri dönüşümsüz bir fonksiyondur. Ardından gizli anahtar kullanılarak bu özet kodlanır. Bu kodlanmış hash, dijital imza olarak kullanılır. Dijital imza mesaja eklenir ve mesaja birlikte alıcıya gider. Dijital imzayı oluşturan bu adımlar Şekil 1'de gösterilmektedir.

Alıcı mesajı, şifrelenmiş özeti yollayan kişinin açık anahtarını kullanarak çözer. Bu iki hash aynı ise bu mesajın gönderen kişiye ait olduğu ve mesajın değişmeden geldiği onaylanmış olur. Mesaj iletilirken bir şekilde değişirse özeti ilk mesajdan farklı olacağından değiştiği anlaşılacaktır. Buna göre dijital imzanın mesaja ve mesajı gönderen kişinin gizli anahtarına özgü olduğu açıkça görünmektedir. Bir dijital imzanın nasıl doğrulandığı Şekil 2'de gösterilmektedir.



Şekil 1: Dijital imza oluşturulması



Şekil 2 : Dijital imzanın doğrulanması

3. Dijital İmza İle İlgili Hukuksal Düzenlemeler

Dijital imza elektronik dünyada pek çok işlemi gerçekleştirmesi ile kullanıcılara kolaylıklar sağlamaktadır. Ancak imzanın kullanıldığı tüm durumlarda olduğu gibi dijital imzanın kullanıldığı yerlerde de kişilerin ve kurumların güvenliği açısından bazı hukuksal düzenlemeler yapmak gereklidir. Dijital imza ile ilgili Türkiye'deki ve uluslararası arenadaki durum şu şekilde incelenebilir:

3.1 Dijital İmza İle İlgili Uluslararası Düzenlemeler

Özellikle 1996 yılından beri bir çok ülkede dijital imzanın hukukî düzenlemeleri ile ilgili çalışmalar yapılmıştır. Çoğu ülkenin dijital imza düzenlemelerinde UNCITRAL (United Nations Commission on International Trade Law) [4] model yasaları ve Avrupa Birliği direktifleri rol oynamıştır. Bu model kanun, iki tespitten ötürü oluşturulmuştur. Bu tespitlerden birincisi, modern iletişim araçlarının arttığı, diğeri ise hukuken önem arz eden bilgilerin elektronik olarak iletilmesinin, hukukî engeller ve belirsizlikler yüzünden sorun teşkil etmesidir [5]. Bazı ülkelerin dijital imza ve daha genel olarak elektronik imza ile ilgili sahip oldukları hukuksal düzenlemeler aşağıdaki gibidir:

3.1.1. Amerika Birleşik Devletleri (ABD)

EPIC (Elektronik Privacy Information Center – Elektronik Gizli Bilgi Merkezi) tarafından belirtildiğine göre, ABD'de dijital imza için bir standart oluşturulması ve hukuksal düzenlemeler gerçekleştirilmesi, 1994 yılında, NIST (National Institute of Standards and Technology – Ulusal Standart ve Teknoloji Enstitüsü) tarafından oluşturulan bir kriptografik standart olan DSS

(Digital Signature Standart – Dijital İmza Standartı) ile birlikte başlamıştır [6]. ABD'de dijital imza ilgili en önemli gelişme S.761 numaralı ve içeriğinde "Bir imza, bir sözleşme veya herhangi bir işleme ait bir kayıt, elektronik formda ise, bir sözleşme yapılırken, bir elektronik imza veya elektronik kayıt kullanılmış ise, sadece elektrondur diye, bunların hukuken hüküm taşımadığı, yürürlüğü olmayacağı veya uygulanma kabiliyeti bulunmadığı hiçbir biçimde ileri sürülemez." maddesinin bulunduğu yasanın 2000 senesinde kabul edilmesidir [7,8]. Buradaki en ilginç durum ise, dönemin ABD başkanı Bill Clinton'ın dijital imza kanununun, bir dijital imza ile imzalanmış olmasıdır.

3.1.2. Avrupa Birliği Ülkeleri – Almanya

SigG olarak ifade edilen Alman Dijital İmza Kanunu 2001 yılından beri yürürlüktedir. Genel hükümler, sertifika hizmeti sunan kuruluşlar, ihtiyarî akreditasyon, teknik güvenlik, denetim ve sonuç hükümleri başlıklarını inceleyen kanunun dijital imza ile ilgili tanımı şu şekildedir: "Elektronik imza diğer elektronik datalara eklenebilen veya bu datalarla mantıksal olarak bağlantılı olan ve kullanıcıyı tanımaya yarayan elektronik formdaki datalardır" [9].

3.1.3. Avrupa Birliği Ülkeleri – Fransa

Fransa'da 2000 tarihli ve 2000-230 sayılı kanunla elektronik imza Medenî Kanununun 1316-4 üncü maddesinde yer almış olup, bu maddenin uygulanması amacıyla 2001 tarihli ve 2001-272 sayılı kararname ile elektronik imza hakkında bir düzenleme yapılarak yürürlüğe konulmuştur [10]. Fransa'da, mahkemelerin, e-imza ile imzalanmış olan ticarî sözleşmelerin geçerliliğini sorgulamakta serbest olması nedeniyle e-imza kullanım istenilen boyutlarda değildir [11].

3.1.4. Avrupa Birliği Ülkeleri – İspanya

Dijital imza ile ilgili yetki ve sorumluluğu Telekomünikasyon ve Bilgi Güvenliği Bakanlığı'na bırakan e-imza kanunu İspanya'da 2003 yılında yürürlüğe girmiştir. Konu ile ilgili oldukça kapsamlı bir kanuna sahip olmasına rağmen, İspanya e-imzanın yaygın olarak kullanıldığı ülkeler içerisine girememiştir [12].

3.1.5. Avrupa Birliği Ülkeleri – Avusturya

2000 senesinden itibaren Federal Elektronik İmza Kanunu geçerlidir [13]. Bu ülkenin kanununa göre, güvenli elektronik imza ile elektronik imza iki ayrı kavramlar olarak kabul edilmiş ve kullanım alanları, yetkileri, sahip olabilecek kişiler ayrı ayrı kanun içerisinde incelenmiştir [14].

3.1.6. Avrupa Birliği Ülkeleri – Finlandiya

Elektronik imza ve daha sonrasında mobil imza kullanımının en yüksek olduğu ülkelerden biri olan Finlandiya'da konu

ile ilgili çalışmalar 1998 yılında başlamış, 2000 senesinde ise İdarî Elektronik Hizmet/ler Yasası ismi ile kabul edilerek uygulanmaya başlanmıştır [15]. Bu kanunda, kullanılan algoritma ve parametrelere ilişkin belirgin kriterler bulunmamaktadır. Ancak e-ımkaya ilişkin olarak kullanılan algoritmanın kırıldığının tespit edilmesi durumunda, kullanılan tüm sertifikaların iptal edileceği belirtilmektedir [16].

3.1.7. Japonya

Elektronik imzalar ve sertifika hizmetleri hakkındaki yasa, 24 Mayıs 2000'de kabul edilip, 1 Nisan 2001'de yürürlüğe girmiştir [17].

3.1.8. Kanada

Tüm elektronik işlemleri kapsayan ve 10 Nisan 2001'de yürürlüğe giren bir Elektronik İşlemler Yasası'na sahiptir [17].

3.1.9. Hong Kong

7 Nisan 2000'de yürürlüğe giren Elektronik İşlemler Yönetmeliği mevcuttur [18].

Bunların yanı sıra, Arjantin, Brezilya, Singapur, Hindistan, Rusya, Çin, Tayvan, İsrail ve Avustralya'da da dijital imza kanunlaşmıştır [19]. Pek çok ülkede ise kanunlaşma için halen çalışmalar yapılmaktadır.

3.2. Türk Ticaret Hukuku Açısından Dijital İmza

Elektronik imza ile ilgili çalışmalar Türkiye'de 2001 yılında Dış Ticaret Müsteşarlığı'nda başlamış 2002'de Adalet Bakanlığı bünyesinde yapılan çalışmalarla devam etmiş, 2004 yılında da bugünkü şeklini alarak 5070 sayılı Elektronik İmza Kanunu olarak kabul edilerek resmî gazetede yayınlanmıştır. Bu kanunda elektronik imza tanımı "Başka bir elektronik veriye eklenen veya elektronik veriyle matkusal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar." şeklinde yapılmıştır [20]. Söz konusu kanunda sırasıyla amaç, kapsam ve tanımlar, güvenli elektronik imza ve sertifika hizmetleri, denetim ve ceza hükümleri ve diğer bazı hükümler yer almaktadır [21]. 5070 sayılı kanun geneli itibarı ile AB'nin 99/93/EC sayılı "Elektronik İmzalarla İlgili Konsey - Komisyon Direktifi" ile uyumludur [22]. Bu kanunla beraber diğer bazı kanunlarda da değişiklikler yapılması gerekmiştir. Örneğin Borçlar Kanunu'nun 14'üncü maddesi uyarınca "İmza, üzerine borç alan kimsenin el yazısı olmak lazımdır." şeklindeki ifadeye, Elektronik İmza Kanunu'ndan sonra bu kanunun 22. maddesi ile söz konusu yasa maddesine "Güvenli elektronik imza elle atılan imza ile aynı ispat gücüne haizdir." şeklinde bir yapılan ekleme yapılmıştır [23].

Ülkemizde dijital sertifika verme işlemi ise aracı kurumlar tarafından 2005 yılında başlamıştır. Kronolojik sıraya göre "Elektronik Bilgi Güvenliği A.Ş. (E-Güven); TÜBİTAK - UEKAE [24]; TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. [25]; EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (e-Tugra) [26]" kurumları bu hizmeti veren kuruluşlar olarak karşımıza çıkmaktadır.

4. Sonuçlar

Temeli zaman, emek ve maliyet tasarrufuna dayanan teknolojik gelişmeler eski zamanlarda insanlara birer lüks gibi görünse de günümüzde artık birer ihtiyaç haline gelmiştir. Teknolojik gelişim dendiğinde pek çok insanın aklına gelen makineler, robotlar, manuel olarak yapılabilecek pek çok işlemi gerçekleştirebilen araçlardır. Donanımsal olarak bu yaklaşım doğru olmakla beraber işin bir de yazılımsal kısmı vardır ki buradaki en önemli araç tabii ki su götürmez bir şekilde internettir. İlk çıktığı zamanlarda sadece askerî amaçlar için ve kısıtlı imkanlarla kullanılabilen internet bir süre sonra insanların eğlence için, yazışma için, bilgi paylaşımı için, mailleşme için sıklıkla kullandığı bir araç haline gelmiştir. Ancak internetteki esas gelişme, insanların zaman, emek ve para harcayarak gerçekleştirecekleri işlemleri bilgisayar başından, yerlerinden kalkmadan, buldukları herhangi bir ortamdan yapabilecek duruma gelmesiyle gerçekleşmiştir. Günümüzde bundan birkaç sene önce aklımıza dahi gelmeyen uygulamaları internet bağlantısı ile gerçekleştirebilmekteyiz. Bunların arasında her türlü bankacılık işlemi, para transferleri, vergi numarası gibi bilgilerin öğrenimi, sınavlara online başvurular, faturaların, vergilerin ödenmesi, noter işlemleri, pasaport başvuruları, herhangi bir organizasyon ya da toplu taşıma aracı için bilet satın alımı gibi işlemler sayılabilir. Büyük rahatlık sağlayan bu işlemler elbette ki tamamen sorunsuz değildir. En büyük sorun bu işlemleri yapan kişinin, yaptığı beyan edilen kişi olup olmadığına nasıl karar verileceğidir. Kağıt üzerindeki işlemlerde bu kısım oldukça kolaydır. Islak imza olarak tabir edilen, kişinin kendisine ait imzası, mührü, pul, sair vs ile kişi kendi kimliğini doğrulayabilmektedir. Ancak sayılan bu işlemleri dijital ortamda yapmak mümkün değildir. İnternette yapılan işlemlerdeki sorunları yok edebilmek için yaklaşık 15 yıldır elektronik imza ve dijital imza kavramları ortaya çıkmıştır.

İmzanın dijital dünyadaki karşılığı olan dijital imza, çeşitli matematiksel algoritmalar sayesinde işlemi yapan kişinin, yaptığı beyan edilen kişi olup olmadığını gösterebilmektedir. Bu çalışmada dijital imzanın ne olduğundan, özelliklerinden ve imzalamayı nasıl yapıldığından bahsedildikten sonra dünya üzerindeki çeşitli ülkelerin ve Türkiye'nin hukukunun dijital imzaya nasıl baktığı incelenmiştir. Bazı ülkelerin bu konuya daha büyük önem verdiği ve dijital imza ile ilgili birer yasa sahibi olduğu, bazı ülkelerin yalnızca çalışma yapma düzeyinde olduğu ancak hatırı sayılır sayıdaki ülkenin dijital imzanın farkında olduğu görülmüştür. Türkiye'nin de bir dijital imza kanunu vardır ve günümüzde sorunsuz bir şekilde uygulanmaktadır. Bu konuda genel bir değerlendirme yapılacak olursa, dünyanın dev gücü olarak bilinen ülkelerin bile 2000li yılların başında dijital imza kanunu çıkardıkları bir ortamda Türkiye'nin onlardan yalnızca birkaç sene sonra çalışmalara başlaması ve kanunlaşması, ayıca da sahip olduğumuz dijital imza kanununun, AB'nin Elektronik İmzalarla İlgili Konsey - Komisyon Direktifi ile uyumlu olması, dijital imza sahibi olabilmek için gerekli olan dijital sertifika hizmetini veren pek çok kuruluşun bulunması, TÜBİTAK'ın bu konuda çalışmalar yapması ülkemiz için sevindirici gelişmelerdir. Bu ve bunun gibi teknolojik gelişmeler ile Türkiye sahip olmayı amaçladığı değerlere her geçen gün birer adım daha yaklaşmaktadır.

5. Kaynakça

- [1] Büyükbahçeci, M., “*Dijital Sertifikalar ve Dijital İmzalar*”, e-imza & e-Türkiye Sempozyumu, Ankara / 15.07.2004.
- [2] Orta, M., “*Elektronik İmza ve Uygulaması*”, Seçkin Yayınları, Ankara, 2005.
- [3] E-İMZA (Kavramlar, Hukuki Boyut ve Uygulamalar), Yüksel SAMAST - TÜRKTRUST A.Ş. BT Vizyon - İstanbul Toplantısı / 03.05.2005.
- [4] <http://www.uncitral.org/uncitral/en/index.html>
- [5] *Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması*, Yard. Doç. Dr. Zarife Şenocak, 2001.
- [6] <http://epic.org/crypto/dss/>
- [7] <http://www.house.gov/commerce/>
- [8] <http://www.thomas.loc/>
- [9] bthukuku.bilgi.edu.tr/documents/alman_imza_kanunu.doc
- [10] <http://turk.internet.com/haber/yazigoster.php3?yazid=9480>
- [11] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business practices, Country Report France, 2006.
- [12] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business practices, Country Report Spain, 2006.
- [13] <http://www.a-sit.at/Englisch/documents.htm>
- [14] Özenç, K, Avrupa Birliği’nde Elektronik İmza, Ulusal Elektronik İmza Sempozyumu, Ankara 7-8 Aralık 2006, s. 172-176.
- [15] <http://www.om.fi/2838.htm>
- [16] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business practices, Country Report Finland, 2006.
- [17] İnci Demirel, Hukuk Elektronik Yaşam ve Ticaretin Hizmetinde veya Siber Uzayda Hukukun Yükselişi
- [18] http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=469
- [19] Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Avniye Tansuğ, Şubat 2002
- [20] <http://www.mevzuat.basbakanlik.gov.tr>, 5070 Sayılı Elektronik İmza Kanunu, Kasım 2008.
- [21] <http://www.tbmm.gov.tr/kanunlar/k5070.html>
- [22] <http://www.hukuki.net/hukuk/index.php?article=2724&type=print-article>, Emrah Yavuzcan
- [23] <http://www.mevzuat.adalet.gov.tr/html/407.html>, Borçlar Kanunu, Ocak 2009
- [24] <http://www.uekae.tubitak.gov.tr>, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, UEKAE, TÜBİTAK.
- [25] <http://www.turktrust.com.tr/>
- [26] <http://www.e-tugra.com.tr/>, EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.