PART 8

ZÜLAL ARSLAN

Electronic Signature and Current Advancements

Elektronik İmza ve Güncel Gelişmeler

ABSTRACT

The term of "Electronic signature" should generally be analyzed within the scope of the term "signature" and it should be clearly defined taking its technical and legal dimensions into account. Various types of electronic signatures exists. The types of electronic signatures and their legal characteristics as genuine legal institutions are defined by certain legal regulations, which contain the functions and verification of electronic signatures. Thus, electronic signature system should follow the latest developments like any other legal and technical institutions.

KEYWORDS:

Electronic signature, electronic document, security certificate, electronic evidence

ÖZET

"Elektronik imza", genel olarak "imza" kavramının tanımından başlayarak incelenmesi gereken, teknik ve hukuki boyutlarının tamamının anlaşılır ve açık bir biçimde ortaya konulması gereken önemli bir kavramdır. Elektronik imzanın pek çok türü vardır. Elektronik imza çeşitleri ve elektronik imza müessesesinin bütünü bir takım bağlayıcı hukuki kurallarla düzenlenmiştir. Bu düzenlemelerin tamamı, elektronik imzanın fonksiyonları ile birlikte oluşturulmasına ve doğrulanmasına ilişkin hususları kapsamaktadır. Nitekim her hukuki ve teknik müessesede olduğu gibi değişen ihtiyaçlara göre elektronik imza kavramı da değişimlere ve güncellemelere açık nitelik taşımaktadır.

ANAHTAR KELİMELER:

Elektronik imza, elektronik belge, güvenlik sertifikası, elektronik delil

PART 8

1. INTRODUCTION

ELECTRONIC SIGNATURE IS DEFINED IN THE LAW NUMbered 5070, titled as the Electronic Signature Law (**"ESL"**), published in the Official Gazette numbered 25355 and dated January 23rd, 2004. It is detailed in the (b) subsection of the third clause of this law as "an electronic datum which is attached to other electronic data or having a logical connection with another datum, used for the identification of the user." Yet, for better understanding, first the terms with regard to technical functions and legal validity of an electronic signature should be defined. A signature in its classic sense is a sign confirming that a written document has been written and/or verified by the signatory[1]. To determine the will of the parties that confirms the current version of a text written on a paper can be ensured by the handwritten signature. Hence, it is considered that the signatory announces his or her will by a sign that is specific to him or her[2].

Signing is a legal procedure and it is one of the most important elements one should sustain on order to ensure the validity of all kinds of documents whether it be official or private and to convey the will of the signatory. However, the 15th subsection of the Law numbered 6098, called the Turkish Code of Obligations (**"TCO"**) states that those who do not incur a debt have no obligation to sign a document. Only the party incurring a debt have the obligation to sign the document with handwriting, and the other party's statement is considered valid in any case.

There is no specific law restricting the location of the signature that should be on a document. However, the general acceptance is that the signature should be at the bottom of the document as an indication that the whole text is covered. Therefore, the signatory declares and agrees that he or she has red the text and admits all the responsibilities[3]. As a matter of fact, the signature at the end of the document implies that all the aforementioned declarations are legally binding but not the changes or additions that are subsequently made.

The Official Gazette numbered 2891 and dated December 27th, 1934 has promulgated "The Surname Regulation", the second subsection of which was amended by the Council of Ministers' decision numbered 2009/14848 and dated March 25th, 2009 states that "in the signature; there may exist the initial of first name, the two initials in

1. GİRİŞ

ELEKTRONİK İMZA, 23.01.2004 TARİH VE 25355 SAyılı Resmi Gazete'de yayınlanan 5070 Sayılı Elektronik İmza Kanunu'nun (**"EİK"**) 3. maddesinin (b) bendinde; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak tanımlanmaktadır. Ancak bu tanımın açık bir biçimde kavranabilmesi için öncelikle elektronik imzanın işlevine ve hukuki geçerliliğine konu olan kavramların tanımlanması gerekmektedir.

İmza, klasik tanımı ile bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işarete verilen isimdir[1]. Taraflarca kâğıt üzerinde onaylanan işlemlere konu bir metne mevcut hali ile yansıtılan iradenin kime ait olduğunu belirleyebilmek, el yazısı ile atılan imza sayesinde mümkün olmaktadır. Nitekim imza ile imzayı atan kişi kendisine has bir işareti kullanmak suretiyle belli bir konudaki iradesini açıklamış sayılmaktadır[2].

İmza hukuki bir işlem olup, resmi veya özel her türlü belgenin geçerlilik kazanabilmesi ve kişinin iradesini yansıtabilmesi için taşıması gereken en önemli unsurlardan biridir. Ancak 6098 Sayılı Türk Borçlar Kanunu'nun (**"TBK"**) 15. maddesi uyarınca, borç altına girmeyen kişi tarafından imza atılması zorunluluğu bulunmamaktadır. Yalnızca borç altına giren şahsın el yazısı ile imzası şart olup borç altına girmeyen diğer tarafın beyanı her halde geçerli olacaktır.

İmzanın metin üzerinde atılacağı yer hususunda bir kanun hükmü bulunmamaktadır. Ancak genel kabul, imzanın metnin tamamına şamil olması için metnin sonuna atılması yönündedir. Böylece imzayı atan kişi metni okuduğunu ve kendisine düşen tüm yükümlülükleri kabul ettiğini ikrar etmiş olacaktır[3]. Nitekim metnin sonuna atılan bir imza, metinde yazılı beyanların hukuken bağlayıcı olduğunu, sonradan yapılan değişiklik ve eklemelerin ise imza sahibi için bağlayıcı olmadığını ifade etmektedir.

27.12.1934 Tarih ve 2891 Sayılı Resmi Gazete'de yayınlanan Soyadı Nizamnamesi'nin Bakanlar Kurulu'nun 25.03.2009 Tarih ve 2009/14848 K. Sayılı Kararı uyarınca değiştirilen 2. maddesi "imzada; öz adın ilk harfi, öz ad iki tane ise her ikisinin ilk harfleri veya birinin ilk harfi

case of the first names are two or one initial and the other components of the name may be included in all." Yet, if the signature has dissimilar features to these definitions, this does not lead to the invalidity of the signature. In practice, a signature can include only first and last names as usually practiced, it does not have to include neither or it can include some signs that are not even letters as long as the identity of the signee can be defined[4].

2. ELECTRONIC SIGNATURE

It is obvious that the aforementioned statements only include paperwork applications. The main problem is to ensure the identification of online transactions and to provide a secure channel for electronically processed documents. Electronic documents often have no differences with the original copies but just the lack of handwritten signature. For this reason, it is quite easy to change the text on electronic documents and this can be untraceable. In respect of the documents with an obligation to be made in a written form, since there is no electronic counterpart of paperwork signature, their electronic application is being prevented and the usage of these documents as an evidence for substantiality has led to a legal definition of an electronic signature and elaboration of the technical details of this process[5].

2.1 Electronic Signature in General

As stated in the Article 15 of the TCO, an *authenticated electronic signature is deemed equivalent to a handwritten signature*. Accordingly, a signature is not only the trace left by ink on a paper. An electronic record or a symbol or code on data may be considered as signature as well[6].

The real persons or corporations can obtain an electronic signature through applying to the Electronic Certification Service Providers (**"ECSP"**), qualification of which concords with the ESL. A simple installation which is done in the medium of computers will suffice

ile öteki ad ve soyadının tümü yazılabilir" hükmünü içermektedir. Ancak imzanın ilgili hükümde kaleme alındığı şekilde atılmaması onun geçersizliği sonucunu doğurmayacaktır. Uygulamada da sıklıkla karşılaşıldığı üzere imza sadece isim veya soyadı kullanılarak atılabileceği gibi, imzanın kime ait olduğu belirlenebilir olduğu sürece her ikisini içermeyen ve hatta harf dışında bir takım işaretlerin kullanılması suretiyle de atılması mümkündür[4].

2. ELEKTRONİK İMZA

İmzaya ilişkin yukarıda yapılan açıklamaların kâğıt üzerindeki işlemleri kapsadığı aşikârdır. Esas sorun elektronik ortamda yapılan işlemlerde yer alan irade beyanlarında kimlik tespitinin yapılabilmesi ve söz konusu işlemlerin güvenliğinin ve güvenilirliğinin sağlanabilmesidir. Elektronik ortamda yer alan belgelerin aslı ile kopyaları arasında el yazısı ile imza eksikliği nedeniyle çoğu zaman bir farklılık bulunmamaktadır. Bu nedenle sözleşme metinlerinin değiştirilmesi çok basit bir şekilde ve fark edilmeksizin mümkün olabilmektedir. Kâğıda dayalı belgelerde bulunan el yazısıyla imza unsurunun elektronik ortamda karşılığının bulunmayışı, geçerliliği yazılı şekle tabi tutulan sözleşmelerin elektronik yolla yapılmasına ve elektronik belgelerin ispat aracı olarak kullanılmasına engel oluşturduğundan, bu engeli aşmak üzere elektronik imza kavramı yaratılarak gereken teknik altyapıyı açıklayan hukuki düzenlemeler meydana getirilmiştir[5].

2.1. Genel Olarak Elektronik İmza

TBK'nın 15. maddesi uyarınca *güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur*. Bu ifade, imzanın mutlak surette kâğıt üzerine mürekkep ile bırakılan işaret anlamına gelmediğini açıkça göstermektedir. Elektronik bir kayıt veya veri üzerindeki bir sembol ya da kod, imza olarak kabul edilebilmektedir[6].

FOOTNOTE DİPNOT

1 Türk Dil Kurumu, (20.02.2015). http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54e667fc2f94f3.39308255 .
2 Gürsel Orer, *Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu*, (Ankara: Adalet Yayınevi, 2011), 5.
3 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 13.
4 Erkut Güçlü Kahraman, "Delillerin Doğrudan Doğruyalığı İlkesinin Belgede Sahtecilik Suçlarıyla İlişkisi", *İzmir Barosu Dergisi* 78/2 (2013), 228.
5 Burcu Erbayraktar, "Elektronik İmza Ve Elektronik İmza Kanunu'na Göre Sertifika Sağlayıcının Üçüncü Kişilere Karşı Hukuki Sorumluluğu". Yüksek Lisans Tezi, İstanbul, 2011.
6 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 32.

to get an amending signature and signatures either created in an electronic environment or transferred into it. The signature has digital and biometric codes functioning as an identification method in electronic documents. The newly created signature can be used on e-Devlet (E-Government Application in Turkey) applications or any other context requiring a genuine signature[7].

2.2 Types of Electronic Signature

There are different types of electronic signatures based on their technical features in terms of security in legal transactions. According to the ESL, there are two main types of electronic signature known as "Simple Electronic Signature" and "Authenticated Electronic Signature" and based on their technical qualities, they are classifies as Simple Electronic Signature, Advanced Electronic Signature, Authenticated (Qualified) Electronic Signature and Electronic Signature given by Accredited Certification Service Providers.

Elektronik imza gerçek veya tüzel kişiler tarafından, EİK uyarınca Telekomünikasyon Kurumu'na bildirim yapmış ve Türkiye'de nitelikli elektronik sertifika vermeye yetkili Elektronik Sertifika Hizmet Sağlayıcıları'na (**"ESHS"**) yapılacak başvuru ile alınabilir. Bilgisayar ortamından yapılacak basit bir kurulum neticesinde, kişiye özel olarak üretilen ve doğrudan elektronik ortamda oluşturulan ya da fiziksel varlığı elektronik ortama aktarılabilen ve eklendiği elektronik veri üzerinde kimlik doğrulama işlevi gören sayısal ve biyometrik sembollerden oluşan elektronik imza, e-Devlet uygulamalarında veya ıslak imza gerektiren her türlü uygulamada kullanılabilmektedir[7].

2.2.Elektronik İmza Çeşitleri

Elektronik imzanın hukuki işlem güvenliğinin sağlanması bakımından taşıdığı teknik nitelikler uyarınca bazı çeşitleri bulunmaktadır. EİK uyarınca elektronik imza, "Basit Elektronik İmza" ve "Güvenli Elektronik İmza" olarak iki kategoriye ayrılmakla birlikte, taşıdığı teknik nitelikler bakımından elektronik imzanın çeşitleri; basit

2.2.1 Simple Electronic Signature

The existence of simple electronic signature only shows that the document signed is secured. A handwritten sign digitized on a computer scene or scanning a handwritten signature may be shown as examples of this type of electronic signature[8].

2.2.2 Advanced Electronic Signature

Generally, advanced electronic signature is defined as a normal electronic signature with added functionalities on the original. As for the simple electronic signature, it signifies the security of the document as well as the traceability of the signatory[9].

The ESL does not have a specific definition for advanced electronic signature. Yet, according to the Directive of European Council numbered 1999/93/CE and dated December 13th, 1999 (**"Directive"**) an advanced electronic signature shall meet the following requirements;

a. it is uniquely linked to the signatory,

b. it is capable of identifying the signatory,

c. it is created using means that the signatory can maintain under his sole control, and

d. it is linked to data which it relates in such a manner that any subsequent change of the data is detectable[10].

These features of advanced electronic signature have been adopted in the Article 4 of the ESL, as well.

2.2.3. Authenticated Electronic Signature

Authenticated Electronic Signature, as defined in the Article 4 of the ESL; (i) is only bound to the signatory as in the position of mere shareholder, (ii) is created by secure creation devices, (iii) provides identification of the signatory with the help of qualified certificate, and (iv) determines

elektronik imza, gelişmiş elektronik imza, güvenli (nitelikli) elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilmiş elektronik imza olarak incelenebilir.

2.2.1. Basit Elektronik İmza

Basit elektronik imzanın varlığı, yalnızca verinin bütünlüğünün korunduğunu göstermektedir. Basit elektronik imzaya örnek olarak, bilgisayar ekranına kalemle atılan imza veya el yazısıyla atılan imzanın tarayıcıdan geçirilmek suretiyle elektronik ortamda bulunan belgelere eklenmesi gösterilebilir[8].

2.2.2. Gelişmiş Elektronik İmza

Gelişmiş elektronik imza, genel olarak elektronik imza tanımına çeşitli unsurların eklenmesi ile tanımlanmaktadır. Gelişmiş elektronik imza, basit elektronik imzada olduğu gibi verinin bütünlüğünün korunduğunu göstermesinin yanı sıra, imzalayanın kimliğinin tespit edilmesini de sağlamaktadır[9].

EİK kapsamında gelişmiş elektronik imzaya ilişkin bir tanım bulunmamaktadır. Ancak, Avrupa Birliği ve Avrupa Konseyi'nin 13.12.1999 tarihli ve 1999/93/CE sayılı Direktifi'nde (**"Direktif"**) yer alan tanım uyarınca sadece imzalayana bağlı bulunan, imzalayanın kim olduğunu belirlemeye imkân veren, yalnızca imzalayanın kontrolü altında tutabileceği araçların kullanımı ile oluşturulan ve daha sonra verilerde yapılan tüm değişikliklerin bulunmasına imkân veren imza[10] olan gelişmiş elektronik imzanın anılan nitelikleri EİK'nın 4. maddesinde düzenlenen güvenli elektronik imzanın nitelikleri arasında sayılmıştır.

2.2.3. Güvenli Elektronik İmza

EİK'nın 4. maddesi uyarınca tanımlanan güvenli elektronik imza, (i) münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan, (ii) güvenli elekt-

FOOTNOTE DİPNOT

7 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 37.
8 Mesut Orta, "Elektronik İmza ve Kavramlar", Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı, http://www.adalet.gov.tr/duyurular/2007/nisan07/eimza/sunum/02_EKavramlar.pps.
9 Orta, "Elektronik İmza ve Kavramlar".
10 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 43.
11 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 44.
12 http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=6KTPJq0pn1nsL2hyITD2IJQB3wpx1-BwyHs3cRrPQCFZgJpcpk1Tn!-1800912348?uri=CELEX:31999L0093, (12.05.2015).

mines whether a change has been made to the document signed before.

The phenomenon on which the signature is bound only to the signatory defines the comparison of the qualified electronic signature provided by electronic certification providers and opposite to signature creation data, signature verification data contrast with documentation. These processes are necessary to match the person to the retrieved data[11].

Authenticated electronic signature corresponds to all known functions of genuine handwritten signature. Hence, as the Subsection 5 of the Directive states, all the member countries should provide it as evidence if all of the qualities of an authenticated electronic signature are satisfied[12].

ronik imza oluşturma aracı ile oluşturulan, (iii) nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, (iv) imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır.

Münhasıran imza sahibine bağlı olma durumu, elektronik sertifika sağlayıcılar tarafından sağlanan nitelikli elektronik sertifikanın ve imza oluşturma verisine karşılık imza doğrulama verisinin resmi belgelere dayandırılmak suretiyle şahıs ile eşleştirilmesini ifade etmektedir[11].

Güvenli elektronik imza, el yazısı ile atılan ıslak imzanın hukuki ve fonksiyonel anlamdaki tüm işlevlerini yerine getirmektedir. Nitekim Direktif'in 5. maddesi uyarınca üye ülkeler, güvenli elektronik imzanın niteliklerinin varlığı halinde bu imzanın el yazısı ile eşdeğerliğini ve yargılamada delil olarak kullanılmasını sağlamak durumundadırlar[12].

2.2.4. Electronic Signature Given by an Accredited Certification Service Provider

The Directive, as in the perspective of electronic certification service providers, mentions accreditation system which is not manifested in the Turkish Law System. Voluntary accreditation is the permission procedure given to a certification service provider according to certain private rights and responsibilities[13].

2.3. Electronic Signature Creation-Verification Data and Device

2.3.1 E-Signature Creation Data

As stated in the Article 3/d of the ESL, signature creation data are defined in the periphrasis of being owned solely by the signatory, unique signs to be created for the purpose of electronic signature creation. It also includes the cryptographic data like components. The creation data are owned by the creator of the signature. Being solely owned by one person, it should not be accessible by other parties. The mere responsibility of protecting the security of the signature is on the signatory[14].

2.3.2. E-Signature Verification Data

As stated in the Article 3/f of the ESL, signature verification data includes the confirming passwords to verify electronic signature and/or other components such as cryptographic open keys. Signature verification data belongs to the certificate holder. They are used to verify the signature and commuting an encrypted delivery to the signature owner. It is unique and current in the certificate as encrypted and non-obligatory to be hidden[15].

2.3.3. E-Signature Verification Device

As stated in the Article 3/f of the ESL, signature verification device is defined as the software or hardware to verify the electronic signature.

2.2.4. Akredite Edilmiş Sertifika Hizmet Sağlayıcısı Tarafından Verilmiş Elektronik İmza

Elektronik sertifika hizmet sağlayıcıları açısından Direktif uyarınca ihtiyari akreditasyon sistemi öngörülmüş olup Türk hukukunda bu hususa yer verilmemiştir. İhtiyari akreditasyon, bir sertifika hizmet sağlayıcısı için özel hak ve yükümlülüklere bağlı olarak izin verilme usulüdür[13].

2.3. Elektronik İmza Oluşturma - Doğrulama Verileri ve Araçları

2.3.1. E-İmza Oluşturma Verisi

EİK'nın 3/d maddesi uyarınca imza oluşturma verisi, imza sahibine ait olan imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir başka eşi olmayan şifreler, kriptografik gizli anahtarlar gibi verileri ifade etmektedir. İmza oluşturma verisi imza sahibine aittir. İmza sahibi ile kişi arasındaki bağı kurar. Kişiye özgü olan bu veri imza sahibi dışındaki kişilerce erişilebilir olmamalıdır. Bu hususta koruma yükümlüğü tamamen imza sahibine aittir[14].

2.3.2. E-İmza Doğrulama Verisi

EİK'nın 3/f maddesi uyarınca imza doğrulama verisi, elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri tanımlamaktadır. İmza doğrulama verisi, sertifika sahibine aittir. Sertifika sahibi tarafından atılmış elektronik imzayı doğrulamak ve sertifika sahibine şifreli mesaj göndermek için kullanılan, bir eşi olmayan, sertifikanın içinde mevcut bulunan kriptografik ve gizli tutulması gerekmeyen veridir[15].

2.3.3. E-İmza Doğrulama Aracı

EİK'nın 3/g maddesi uyarınca imza doğrulama aracı, elektronik imzayı doğrulamak amacıyla imza doğrulama

FOOTNOTE DİPNOT

13 Orta, "Elektronik İmza ve Kavramlar".
14 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 59.
15 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 59.
16 Ziya Gökalp, "PKI (Açık Anahtar Altyapısı) Nedir?" 04.06.2008, https://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/pki-acik-anahtar-altyapisi-nedir.html (22.02.2015)
17 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 61.
18 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 48.
19 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 48.

PART 8

Defined in the Article 7 the ESL, during the signature verification process, it should be ensured that;

a. the data used for verifying the signature correspond to data displayed to the verifier;

b. the signature is reliably verified and the result of that verification is correctly displayed;

c. the verifier can, as necessary, reliably establish the contents of the signed data;

d. the authenticity and validity of the certificate required at the time of signature verification are reliably verified and the result of verification and the signatory's identity are correctly displayed;

e. the use of a pseudonym is clearly indicated; and

f. any security-relevant changes can be detected.

verisini kullanan yazılım veya donanım aracını ifade etmektedir.

EİK'nun 7. maddesi uyarınca güvenli elektronik imza doğrulama araçlarının;

a. İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye göstermesi,

b. İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye göstermesi,

c. Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlaması,

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

e. İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye göstermesi,

2.3.4. Creation and Verification of Electronic Signature

In the process of creation of e-signature, the option of copying the handwritten signature to the digital medium is nonexistent. Certain tremendously complex algorithms and processes are involved and all of the maximal matter is processed by computers. Electronically created documents are encrypted with asymmetric keys to produce e-signature.

"Public Key Infrastructure" (PKI) is defined as all the promised services of e-signature given to users including person-specificity, integrity, identification and non-repudiation. This infrastructure is the most widely accepted one in regard to the verification of the e-signature process system[16].

Two keys one of which being open and the other one closed are created by the ECSP and delivered to the user. The data encrypted by the open key of the signatory can only be decrypted with the open key of the recipient of the document[17].

2.4. Functions of Electronic Signature

In order for electronic signature to replace the handwritten signature, it needs to bear the functions of (i) identification, (ii) eventuation, (iii) authenticity, (iv) monition, (v) continuity and (vi) attestation. Being said that, electronic signature can be more attributable to the aforementioned qualities with a greater precision[18].

The most significant function of electronic signature to fulfill is non-repudiation. Unless the signatory loses the control of the use of the signature, electronic signature is non-imitable[19].

The identification process in the system of electronic signature is provided by the control of the unique key of the signatory assigned as one-time by certain certification offices. This coordination is achieved by a signature key certificate and provides an identification procedure with a certain check done by the recipient who knows the open key of the owner of the signature using the open signature key certificate to verify the signature[20]. Nonetheless, the repudiation of an electronically signed data is possible according to the Article 210 of the Code of Civil Procedure numbered 6100 (**"CCP"**). If need be, after the irresolution of the issue by a judge, an expert opinion

f. İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlaması gerekmektedir.

2.3.4. Elektronik İmzanın Oluşturulması ve Doğrulanması

E-imzanın oluşturulma sürecinde ıslak imzanın elektronik ortama kopyalanması söz konusu değildir. Altyapısı oldukça karmaşık olan matematiksel bir süreç ve algoritmalar söz konusu olup bu işlemlerin tamamı bilgisayar tarafından gerçekleştirilmektedir. Elektronik ortamda oluşturulan belgeler asimetrik anahtarla şifrelenerek e-imza oluşturulmaktadır.

E-imzanın vaat ettiği kişiye özellik, bütünlük, kimlik doğrulama ve inkâr edilemezlik hizmetlerinin kullanıcılara verilmesi için gerekli hizmetlerin bütününe "Açık Anahtar Altyapısı" (**"AAA"**) denmektedir. Söz konusu altyapı e-imza sistemini doğrulamak için kurulan en yaygın altyapı niteliğini taşımaktadır[16].

AAA altyapısı ile biri açık biri kapalı olmak üzere çift anahtar ESHS tarafından oluşturularak imza sahibine teslim edilir. İmza sahibinin açık anahtarıyla şifrelenen veri, ulaştığı muhatabınca ancak açık anahtar kullanılmak suretiyle deşifre edilebilmektedir[17].

2.4.Elektronik İmzanın Fonksiyonları

Elektronik ortamda atılan bir imzanın el yazısıyla atılan ıslak imzanın yerini tutabilmesi için, (i) kimlik tespiti, (ii) sonuçlandırma, (iii) gerçeklik, (iv) uyarı, (v) devamlılık ve (vi) ispat fonksiyonlarının tamamını taşıması gerekmektedir. Nitekim elektronik imza, anılan fonksiyonları elle atılan imzadan daha kuvvetli bir biçimde sağlamaktadır[18].

Elektronik imzanın kendisinden beklenen güveni sağlaması açısından, taşıması gereken en önemli fonksiyon inkâr edilememedir. Elektronik imza sahibi imza üzerindeki kontrolünü kaybetmedikçe elektronik imzanın taklidinin yapılabilmesi mümkün değildir[19].

Elektronik imzada kimliğin tespiti, belirli onay makamları tarafından belirli bir gerçek kişiye bir defa olmak üzere tahsis edilen imza anahtarlarının, yine bu makamlar tarafından kontrol edilmesi ile yerine getirilmektedir. Bu koordinasyon bir imza anahtarı sertifikası ile yapılmakta ve anahtar sahibinin açık anahtarını bilen alıcının,

shall be searched respectively to the hearing of the repudiating party.

As stated in the ESL, if there is an issue regarding to a refund of a debt, electronic signature has a certain binding function with respect to the call of the signatory. Because of the fact that even the infinitesimal gaps in the text are encrypted with electronic signature, it has a more reinforced credibility than the handwritten signature[21].

With respect to other benefits and functions of an electronic signature, first it should be discussed that an electronic signature has the advantage of efficiency and logistics. The use of electronic signatures will add the beneficiary attributes such as speed, easiness and cheapness to processes. Data will easily be transferred and the cost of print, paper and post etc. will be minimized. The electronic signature can hardly be imitated, thus the recipient may not claim that the document has not arrived or vice versa, the sender may not allege that the document has not been sent. The content of the document is safely encrypted and cannot be changed after the document is sent, therefore neither the recipient nor the sender may repudiate the content. In addition to this, a copy of the document would be in the hands of the certificatory.

2.5. The Evidential Quality of Electronically Signed Documents in Legal Proceedings

As stated in the Article 5 of the ESL, *"authenticated electronic signature has the same juridical consequences as the handwritten signature."* Yet, *"certain jurisdiction processes and contracts of guaranty which has a specific form or special formal procedure determined by laws cannot be signed with authenticated electronic signature."*

As the aforementioned Article of the provision states, it will be adequate to say that an electronic signature has only the coverage of base written validity form. Hence the jurisdictionally imposed written forms such as such

herkes tarafından ulaşılabilen imza anahtarı sertifikasını kontrolü sayesinde, veriyi düzenleyen kişinin kimliği hakkında bilgi sahibi olabilmesini sağlamaktadır[20]. Ancak her halükarda 6100 Sayılı Hukuk Muhakemeleri Kanunu'nun (**"HMK"**) 210. maddesi uyarınca güvenli elektronik imzayla oluşturulmuş verinin inkâr edilmesi söz konusu olabilecektir. Bu durumda hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulacaktır.

EİK uyarınca, imzalanan metin kapsamında bir borç iradesi söz konusu ise elektronik imza, imzalayanın beyanıyla bağlı kalma fonksiyonunu da sağlamaktadır. Elektronik imza ile metindeki en ufak bir boşluk bile şifrelenmekte olduğundan, metindeki değişikliklerin imza sahibini bağlamama fonksiyonu elektronik imzada, el yazısı ile atılan imzaya nazaran daha kuvvetli bir hale gelmektedir[21].

Elektronik imzanın diğer faydaları ve fonksiyonlarına ilişkin ise, öncelikle elektronik imzanın verimlilik ve lojistik fonksiyonlarının söz konusu olduğunu söylemek mümkündür. E-imza sayesinde işlemler kolaylık, hız ve ucuzluk kazanacaktır. Veriler ulaşması gereken yere çabuk ulaşır ve baskı, kâğıt, posta vb. maliyetler en aza indirgenir. E-imzada taklit edilme olasılığı neredeyse tamamen ortadan kalkmakta olup, gönderici belgeyi göndermediğini alıcı ise almadığını iddia edemez. Gönderilen belge veya verinin içeriği, gönderimden sonra değiştirilemeyeceğinden, gönderici veya alıcı tarafından içerik inkar edilemez. Nitekim belgenin bir kopyası onay kurumundadır.

2.5. Elektronik İmzalı Belgelerin Yargılamada Delil Niteliği

EİK'nın 5. maddesi uyarınca *"güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur."* Ancak *"kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez."*

FOOTNOTE DİPNOT

20 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 49.
21 Orer, *Elektronik İmza ve Elektronik Sertifika...*, 50.
22 Mine Erturgut, *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi*, (Ankara: Yetkin Yayınları, 2004), 69.
23 Erturgut, *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin...*, 138.
24 Mehmet Ertan Yardım, "Güvenli Elektronik İmzanın İnkarı", www.iscturkey.org/2010/2008/2006/-pdf/bildiri/29.
25 Yardım, "Güvenli Elektronik İmzanın İnkarı".
26 Leyla Keser Berber, *İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza*, (Ankara: Yetkin Yayınları, 2002), 177.

as marriage, divorce and financial loan contracts cannot be signed with an electronic signature.

In addition, in this matter it should be noted that the evaluation of electronically signed documents with respect to bonded proof issues should be verified. In the jurisdiction system, on a specific event or act of law, the judge will decide whether it is necessary to prove this circumstance with final or discretionary proofs. In this sense, with respect to the CCP, final verdicts and oaths have the quality of final proofs, whereas the other specific acts signifying discretionary proofs such as witness, expert, investigation and other non-counted acts may refer to discretionary proofs.

Finality aspect of a muniment implies that the judge has bound by the document. The verification or authentication of a signature at the bottom of a muniment is not an issue for a judge to investigate ex officio. Qualifying of the written signature will be done by the judge through a mundane examination with eyesight[22].

In this matter, through the Article 23 of the ESL, Article 205 of the CCP states that the electronic data created by an authenticated electronic signature has the quality of

Anılan madde uyarınca, e-imzanın ancak adi yazılı geçerlilik şekline bağlı hukuksal işlemleri kapsadığını belirtmek mümkündür. Nitekim kanunların açıkça resmi yazılı şekil ile yapılmasını öngördüğü hukuki işlemlerin (örneğin; evlilik, boşanma, finansal kiralama sözleşmesi vb.) elektronik imza ile yapılabilmesi mümkün değildir.

Ayrıca bu hususta elektronik imzalı belgelerin senetle ispat kuralları bakımından da değerlendirilmesi önem arz etmektedir. Yargılamada, bir olayın veya hukuki işlemin ispatı hususunda hâkim öncelikle bu durumun kesin delil ile veya takdiri delil ile ispatlanması gerekip gerekmediğini değerlendirecektir. Bu anlamda HMK bakımından senet, yemin ve kesin hüküm kesin delil teşkil etmekte iken; tanık, bilirkişi, keşif ve kanunda sayılmayan diğer takdiri delilleri işaret eden özel hükümler takdiri delil teşkil etmektedir.

Senedin kesin delil teşkil etmesi, hâkimin senetle bağlı olmasını ifade etmektedir. Senet metninin altındaki imza hâkim tarafından gerçek kabul edilmek suretiyle senedin doğruluğu veya gerçekliği hâkim tarafından re'sen araştırılacak hususlardan değildir. Senetteki el yazılı imzanın nitelemesi hâkim tarafından gözle yapılacak basit bir inceleme neticesinde takdir edilebilecektir[22].

a muniment. The bond value and the function of final proof of these data are determined through the condition of these data created by an authenticated electronic signature. Simple electronic signed documents will not count as having the value of bond. That being said, the type of the signature of a document must be detected by judge using the commending in the Article 205/3 of the CCP ex officio. This determination is an appropriate measure to the circumstance in which parties have no objection and preventing a simple electronic signed text to have the value of final proof[23].

Alas, since a judge cannot make the distinction with regard to the type of an electronic signature used in the document with eyesight, unlike the handwritten signatures examined by the court, an expert should examine the document signed with an electronic signature.
As the Article 210 of the CCP states, *"in the event of denial*

Bu kapsamda EİK'nun 23. maddesi uyarınca, HMK'nun 205. maddesi ispat gücü bakımından güvenli elektronik imza ile oluşturulan elektronik verilerin, senet hükmünde olduğunu ifade etmektedir. Bu hüküm uyarınca elektronik belgelerin senet değeri ve kesin delil etkisi, güvenli elektronik imza ile oluşturulmuş olmaları şartına bağlıdır. Basit elektronik imzalı elektronik veriler senet niteliğini taşımayacaktır. Nitekim bir belgenin hangi tür elektronik imza ile imzalandığının tespiti, HMK 205/3 uyarınca hâkim tarafından re'sen yapılmak durumundadır. Söz konusu hüküm, tarafların itiraz etmediği bir durumda basit elektronik imzalı bir metnin kesin delil teşkil etmesinin önüne geçmek açısından isabetli bir hüküm niteliğini taşımaktadır[23].

Ancak hâkimin elektronik imzanın türüne ilişkin tespiti gözle görülecek biçimde yapamayacak olması sebebiyle, el yazısıyla imzalı senetlerden farklı olarak elektronik

of data signed with an authenticated electronic signature, if there is no verdict after the hearing of the denying party by the judge, an expert investigation will be executed." As when the previous Code of Civil Procedure numbered 1086 ("**pCCP"**) was in force, there was no evident rule when the denial of an authenticated electronic sign was handled according to the Article 308 of the pCCP[24]. The judge was in charge of the detection of the owner of the signature, possibly being the opposed party, using the protocol issued in the Article 308 of the pCCP. Hence, with the accepting of the judge being not technically equipped with the necessary information, it is stated in the doctrine that an expert should obligatorily use the expertise in the period that the pCCP was in force. Although there are certain controversial points[25], the Article 210 of the CCP has helped the hindrance of all the controversy surrounding the case and when the denial of an authenticated electronic signature, it has allowed the demand of expert opinion.

Certain acts in the law could only be executed through the use of an authenticated electronic signature. For instance, the Official Gazette dated December 20th, 2009 has promulgated the "Law of Cheques" numbered 5491. In the Article 5, subsection 8 of the Law, it is stated that the data related to cheque making and opening a cheque account are signed with an authenticated electronic signature and after that they are electronically reported via the Ministry of Justice National Judiciary Informatics System (NJIS) to the Central Bank of Turkish Republic. These reports and the bases and procedures related to the announcements done to banks are determined by the Central Bank of Turkish Republic with the confirmation by the Ministry of Justice.

3. PRACTICE AREAS OF ELECTRONIC SIGNATURE AND NEW DEVELOPMENTS

Electronic signatures, having a wide variety of practice areas, can be used in every case in which data are moved, copied and processed electronically . Articles 14 and 15 of the TCO state that an electronic signature has all the juridical qualities of paperwork signature in every written shape obligatory situation, and thus available to replace the written shapes condition. In this circumference, all acts of law obliging any written shape may be signed with an authenticated electronic signature.

Practice areas of e-signature in public sphere can be listed as; applications to Student Selection Examina-

imzalı bir belgenin yargılamada bilirkişi tarafından incelenmesi gerekecektir.

Nitekim HMK'nın 210. maddesi; *"güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur."* hükmünü içermektedir. 1086 Sayılı Hukuk Usulü Muhakemeleri Kanunu ("HUMK") yürürlükte iken bu hususta açık bir hüküm bulunmadığından, güvenli elektronik imzanın inkârı durumunda HUMK'nın 308. maddesi uyarınca imza incelemesi yapılmaktaydı[24]. Görülmekte olan dava sırasında güvenli elektronik imzanın inkârı söz konusu olduğunda hâkim HUMK'nın 308. maddesinde öngörülen prosedürü kıyasen uygulayarak güvenli elektronik imzanın aleyhine ileri sürülen kişiye ait olup olmadığını araştırmak ile yükümlü bulunmaktaydı. Nitekim söz konusu maddenin yürürlükte olduğu dönemde doktrinde hâkimin teknik bakımından kendiliğinden bu araştırmayı yapabilecek nitelikte olamayacağının kabulü ile güvenli elektronik imzaya ilişkin incelemenin mutlaka bilirkişi tarafından yapılması zorunluluğu belirtilmekteydi. Aksi yönde görüşler de olmasına rağmen[25] HMK'nun 210. maddesi ile tüm bu tartışmaların önüne geçilerek güvenli elektronik imzanın inkârı durumunda hâkimin bilirkişi incelemesini talep edebilmesinin önü açılmıştır.

Bazı hukuki işlemlerin ise kanuni bakımdan mutlak surette güvenli elektronik imza ile oluşturulması zorunlu tutulabilmektedir. Örneğin; 20.12.2009 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 5491 Sayılı Çek Kanunu'nun 5/8. maddesi uyarınca çek düzenleme ve çek hesabı açma yasağı kararına ilişkin bilgiler, güvenli elektronik imza ile imzalandıktan sonra, Adalet Bakanlığı Ulusal Yargı Ağı Bilişim Sistemi ("UYAP") aracılığıyla Türkiye Cumhuriyet Merkez Bankası'na elektronik ortamda bildirilir. Bu bildirimler ile bankalara yapılacak duyurulara ilişkin esas ve usuller, Adalet Bakanlığı'nın uygun görüşü alınarak Türkiye Cumhuriyet Merkez Bankası tarafından belirlenir.

3. ELEKTRONİK İMZANIN UYGULAMA ALANLARI VE GELİŞMELER

Oldukça geniş bir uygulama alanı söz konusu olan elektronik imzanın, bilgilerin elektronik olarak taşındığı, kopyalandığı ve işlendiği her yerde kullanılabilmesi mümkündür[26]. TBK'nın 14. ve 15. maddeleri uyarınca yazılı şekil zorunlu görülen hukuki işlemlerde, güvenli

tion, Public Personnel Selection Examination, Academic Personnel and Postgraduate Education Entrance Exam, passport etc., inter-institutional communication, social security applications, medical applications, tax payment and tax declarations and electronic votes. In moving governmental services to digital medium, the time and resources gain are aimed, especially with the project of e-Devlet. Thus, it is possible to argue that the NJIS is the most active platform for electronic signatures through courts, public prosecutor's offices, all clerks and lawyers. The improvements in e-Devlet is still ongoing.

For the use of e-signature in trade, internet banking, insurance transactions, e-contracts and e-shopping may be considered. In addition to this, in the Turkish Commercial Code numbered 6102 and dated July 1st, 2012, electronic signature and electronic data are extensively discussed. According to the Article 18/3 of the TCC, e-signature has the potency to put in default, nullify a contract or to make denunciation or warning processes. According to Articles 24, 64 and 65 of the TCC, the trade registry entries and commercial registers may be stored in an electronic medium.

Article 94 of the TCC states that the rejection period is one month and can be executed by holder of the schedule which shows the surplus determined in the current account balance with a text involving an "authenticated electronic signature". All obliged processes in accordance with the TCC can be done by commercial corporations, corporates, and real persons in an electronic medium through an authenticated electronic signature.

The Notary Act numbered 1512 (**"Notary Act"**) has an additional Article 198/A since February 12th, 2014 issued with the law numbered 6572. This addition should be examined separately. According to this Article; the processes set in the Notary Act may also be done in an electronic medium with an authenticated electronic signature. A caveat for this is that processes forced as edit and testaments of will should be executed in the presence of notary to be signed with an authenticated electronic signature.

All data and documents related to notary acts are stored and saved in the Union of Turkish Notaries Informatics System. For documents signed with an authenticated electronic signature, the seal affixing process done in handwritten signed documents is not present and it is unnecessary to prove another copy. It is also stated that a physical copy for a document containing an authenticat-

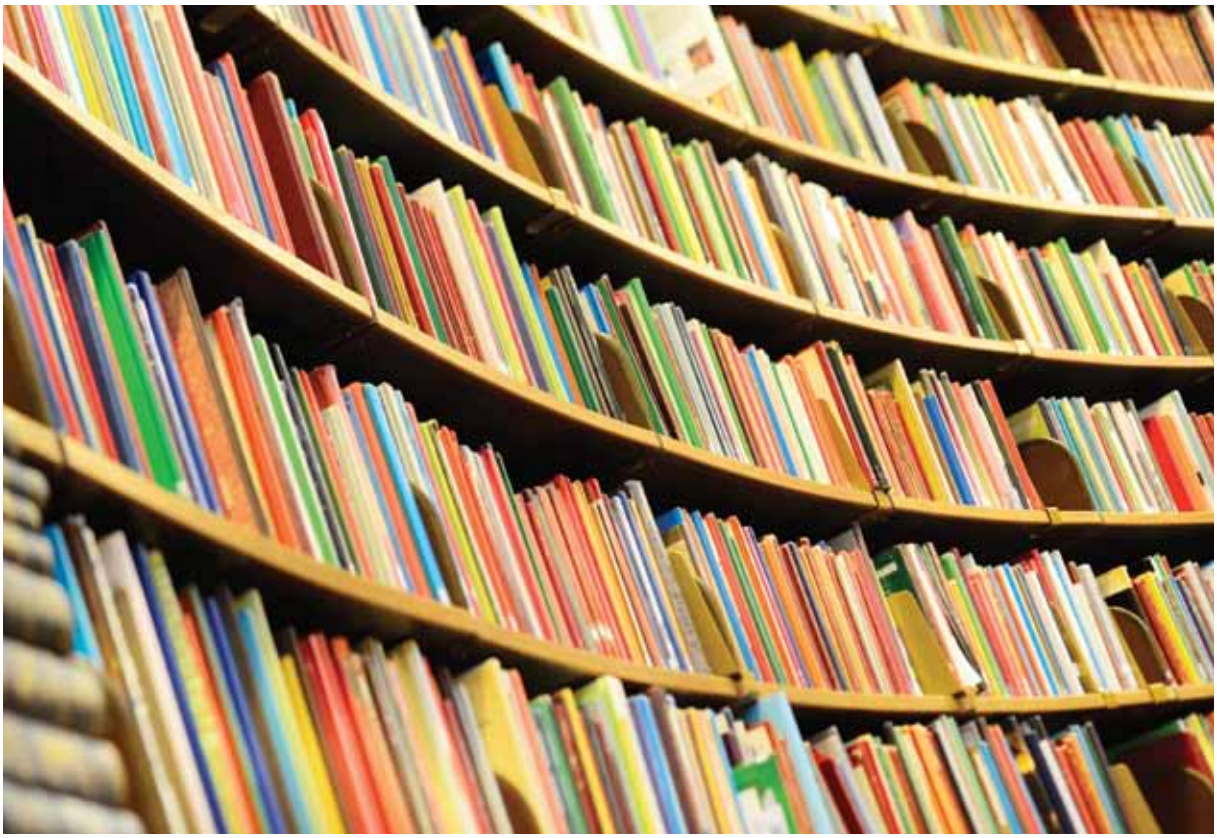
elektronik imzanın el yazısıyla imzanın bütün hukuki sonuçlarını doğurmak suretiyle bu şekilde imzalanmış belgelerde yazılı şekil şartı yerine getirilmiş sayılacaktır. Bu kapsamda yazılı şekil gerektiren her türlü hukuki işlem güvenli elektronik imza ile tamamlanabilecektir.

E-imzanın kamusal alandaki uygulama alanları; ÖSS, KPSS, ALES, pasaport vb. her türlü başvurular, devlet kurumları arası iletişim, sosyal güvenlik uygulamaları, sağlık uygulamaları vergi ödemeleri ve e-beyannameler, elektronik oy verme işlemleri olarak listelenebilir. Özellikle e-Devlet projesi kapsamında pek çok devlet hizmetinin elektronik ortama taşınması suretiyle zaman ve kaynak kazancının elde edilmesi amaçlanmaktadır. Nitekim UYAP için, e-imzanın mahkemeler, Cumhuriyet başsavcılıkları, tüm adliye kalemleri ve avukatlar tarafından aktif olarak kullanıldığı en geniş platform olduğunu belirtmek mümkündür. E-Devlet uygulamasının ise geliştirilmesi hususunda çalışmalar devam etmektedir.

E-imzanın ticari alandaki uygulamaları için ise; internet bankacılığı, sigortacılık işlemleri, e-sözleşmeler, e-sipariş alanları sayılabilir. Nitekim 01.07.2012 tarihinde yürürlüğe girmiş olan 6102 Sayılı Türk Ticaret Kanunu (**"TTK"**) uyarınca elektronik imza ve elektronik veriler geniş yer tutmaktadır. TTK'nun 18/3. maddesi uyarınca e-imza ile tacirler arası temerrüde düşürme, sözleşmeyi feshe veya sözleşmeden dönmeye yönelik ihbar ve ihtar işlemleri yapılabilmektedir. TTK'nun 24. maddesi uyarınca ticaret sicil kayıtları, 64. ve 65. maddeleri uyarınca düzenlenen ticari defterler elektronik ortamda tutulabilmektedir.

TTK'nun 94. maddesi uyarınca cari hesap bakiyesinde saptanan artan tutarı gösteren cetveli alan tarafın aldığı tarihten itibaren bir ay içinde "güvenli elektronik imza" içeren bir yazı ile itirazda bulunabileceği hüküm altına alınmıştır. TTK uyarınca zorunlu tutulan tüm işlemler, ticaret şirketleri ile gerçek ve tüzel kişi diğer tacirler tarafından elektronik ortamda güvenli elektronik imza ile yapılabilecektir.

1512 Sayılı Noterlik Kanunu'na (**"Noterlik Kanunu"**) 02.12.12.2014 tarih ve 6572 sayılı Kanun ile eklenen 198/A maddesinin ayrıca incelenmesi gerekmektedir. Bu madde uyarınca; Noterlik Kanunu'nda öngörülen işlemler, elektronik ortamda güvenli elektronik imza kullanılarak da yapılabilir. Yalnızca düzenleme şeklinde yapılması zorunlu tutulan işlemlerin ve irade beyanlarının alınmasına ilişkin işlemlerde güvenli elektronik imza



ed electronic signature is not printed unless demanded. When there is a need for a physical copy, the notary involved affixes seal to the document and sign it declaring that it is identical to the original. If the copy of the electronically signed document contradicts the handwritten signed copy, the electronically signed document stored in informatics system will be considered as the original one. Thus, the wide use of an authenticated electronic signature by notaries and increasing the security of notary embodied documents will be ensured.

4. CONCLUSION

There is no doubt that the developments in information technology race against time. As the internet gets as near as a phone, undoubtedly it plays an important role in both commercial transactions and government transactions. Hence, e-Devlet and e-commerce are constantly developed by both technical and judicial adaptations.

The E-signature justified with the Electronic Signature Law numbered 5270 is a known and spreading application. In near future, it is quite possible that e-signature

kullanılabilmesi için ilgililerin noter huzurunda olmaları gerekmektedir.

Noterler tarafından yapılan tüm işlemlere dair bilgi ve belgeler Türkiye Noterler Birliğinin Bilişim Sistemi'ne kaydedilir ve saklanır. Güvenli elektronik imza ile imzalanmış belgelerde ıslak imzalı belgeler için aranan kanunlarda belirtilen mühürleme işlemi uygulanmaz ve ayrıca suret aranmaz. Güvenli elektronik imza ile oluşturulan belgenin, talep edilmedikçe ayrıca fiziki olarak düzenlenmeyeceği de hükme bağlanmıştır. Elektronik ortamdan fiziki örnek çıkartılması gereken hâllerde belgenin aslının aynı olduğu belirtilerek noterlikçe imzalanır ve mühürlenir. Güvenli elektronik imza ile imzalanmış belgenin elle atılan imzalı suretiyle çelişmesi hâlinde noterlerin kullandığı bilişim sisteminde kayıtlı olan güvenli elektronik imzalı belge esas alınır. Böylece güvenli elektronik imzanın kullanımı Noterliklerce de yaygınlaşacak ve noter kanalıyla düzenlenen veya onaylanan belgelerin güvenilirliği artacaktır.

will be used by individuals more often. E-signature accelerates and facilitates electronic relations by tremendous amounts, thus it is significant for all citizens.

The effective use of an electronic signature will increase the efficiency of using resources recognizably. Especially in commerce, there will be copious developments on widely acclaimed base factors such as transparency, simplicity and accounting, and complete security of legal transactions will be ensured. In this matter, an electronic signature has many advantages which can be exemplified as preventing change on data and documents, secrecy, non-repudiation, integrity of data and identification. That being said, in near future it is quite possible to state that handwritten signature will be replaced completely by electronic signature. ■

4. SONUÇ

Çağımızda bilgi teknolojisinin zamanla yarışır bir biçimde hızla geliştiği yadsınamaz bir gerçektir. İnternetin bir telefon kadar uzakta olduğu bu dönem, şüphesiz ki devlet kurumları ile yapılan ve ticari hayatta yer bulan tüm işlemlerde internetin etkin bir aktör olmasında önemli rol almaktadır. Bu nedenle e-Devlet ve e-ticaret alanları hem teknik hem hukuki düzenlemeler yapılmak suretiyle sürekli olarak geliştirilmektedir.

5270 Sayılı Elektronik İmza Kanunu ile düzenlenen e-imza gün geçtikçe kullanım alanı artan ve bilinen bir uygulamadır. Yakın zamanda da kişilerin günlük hayatta da sıkça kullandığı bir uygulama olması oldukça muhtemeldir. E-imza elektronik ortamdaki ilişkileri büyük ölçüde hızlandırdığından ve kolaylaştırdığından, bilişim sektörünün yanı sıra tüm vatandaşlar için büyük önem arz etmektedir.

Elektronik imzanın etkin bir şekilde kullanımı kaynakların verimliliğini gözle görülür biçimde artıracaktır. Bununla birlikte bilhassa ticarette en önemli hususlardan biri olan şeffaflık, açıklık, hesap verilebilirlik gibi temel unsurlarda da büyük gelişmeler söz konusu olacak, hukuki işlem güvenliği tam olarak sağlanacaktır. Bu kapsamda elektronik imzanın, bilgi ve belgelerin değiştirilmesinin önlenmesi, gizlilik, inkâr edilemezlik, veri bütünlüğü ve kimlik doğrulama gibi fırsatlar doğurmakta olması gibi nedenlerle, yakın gelecekte hukuki işlemlerde ıslak imzanın yerini tamamen elektronik imzaya bırakacağını söylemek mümkündür. ■

BIBLIOGRAPHY KAYNAKÇA

Erbayraktar, Burcu. "Elektronik İmza Ve Elektronik İmza Kanunu'na Göre Sertifika Sağlayıcının Üçüncü Kişilere Karşı Hukuki Sorumluluğu". Yüksek Lisans Tezi, İstanbul, 2011

Erturgut, Mine. *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi.* Ankara: Yetkin Yayınları, 2004

Gökalp, Ziya. "PKI (Açık Anahtar Altyapısı) Nedir?" 04.06.2008, https://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/pki-acik-anahtar-altyapisi-nedir.html (22.02.2015)

Keser Berber, Leyla. "E-Sözleşme Bağlamında Digital İmza ve ETKK Yasa Taslağı Açısından Türkiye'de Durum". *İnternet ve Hukuk,* Derleyen: Yeşim Atamer. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004

Keser Berber, Leyla. "İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza", Yetkin Yayınları, Ankara, 2002

Kuru, Baki/ Arslan, Ramazan ve Yılmaz, Ejder. *Medeni Usul Hukuku Ders Kitabı,* Ankara: Yetkin Yayınları, 2014

Orer, Gürsel. *Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu.* Ankara: Adalet Yayınevi, 2011

Orta, Mesut. "Elektronik İmza ve Kavramlar". Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı. http://www.adalet.gov.tr/duyurular/2007/nisan07/eimza/sunum/02_EKavramlar.pps

Özler, İsmail. "Bilgi Güvenliği Ve Elekronik İmza Kavramları, Ekonomik Boyutlarının İncelenlemesi ve Elektronik İmza Uygulamaları". Dicle Üniversitesi Sosyal Bilimler Enstitüsü Maliye ve Ekonomi Ana Bilim Dalı Yüksek Lisans Tezi, Diyarbakır, 2007