ÜNİTE 4

ELEKTRONİK İMZA VE
ELEKTRONİK İMZA KANUNU

Arş. Gör. Mustafa Can DAĞLI

ANAHTAR KAVRAMLAR

Sözleşmelerde şekil
İmza
Dijital imza
Hash değeri
Elektronik sertifika hizmet sağlayıcısı

ÖĞRENME HEDEFLERİ

1. Sözleşmelerde şekil konusunu öğrenmek.
2. Elektronik imza ve dijital imzanın ne olduğunu, farklarının ne olduğunu öğrenmek.
3. Dijital imzanın teknik yapısını öğrenmek.
4. Güvenli elektronik imzaya bağlanan hukuki sonuçların ne olduğunu öğrenmek.
5. Elektronik sertifika hizmet sağlayıcısının rolünü, nasıl faaliyete başladığını, temel yükümlülüklerinin ne olduğunu öğrenmek.

DÖRDÜNCÜ BÖLÜM

GİRİŞ

Sözleşmelerde şekil, genel olarak tarafları düşünmeye sevk etmesi, sözleşmeye açıklık ve kesinlik sağlaması, ispat ve güvenlik sağlaması, sözleşmenin yorumunu kolaylaştırması açısından faydalı görülmektedir. Ancak hukuki işlemlerin büyük çoğunluğunun, özellikle geçerlilik şartı olarak şekle bağlı olması birçok hukuki işlemin geçersizlik yaptırımıyla karşılaşmasına yol açacaktır. Bir diğer yandan, elektronik ortamda yer alan verilere dayanan hukuki işlemlerin, yapıları gereği ağır şekil koşullarına uyması mümkün değildir. Bu hukuki işlemlerin, özellikle internet üzerinden akdedilen sözleşmelerin katı şekil koşullarına tabi tutulması halinde geçersizlik yaptırımıyla karşılaşma riski doğmaktadır. Bu sebeple ülkemizde ve diğer ülkelerde güvenli elektronik imza düzenlemeleri yapılmış ve güvenli elektronik imzaya belirli hukuki sonuçlar bağlanmıştır.

İmza, kişileri birbirinden ayırmayı, kişinin kimliğini tespit etmeyi mümkün kılar. Kişi, metni imzalayarak irade beyanını ortaya koyar. Böylece, kişinin metinde yer alan hukuki sonucu benimsediği kabul edilir. Elektronik belgelerin metin ve el yazısı unsurlarını içermemesi bu belgelerin nasıl imzalanacağı sorununu doğurmuştur. Bu soruna çözüm olarak dijital imza (güvenli elektronik imza) bulunmuştur. Güvenli elektronik imza da kişinin kimliğini tespit etmeyi mümkün kılar ve elektronik belgenin imzalayan tarafından yazıldığını (bağlayıcı olduğunu), belgenin değişikliğe uğramadığını ve belgenin varlığını doğrulamayı sağlar. Güvenli elektronik imzanın, geleneksel imza ile benzer fonksiyonları yerine getirmesi nedeniyle, güvenli elektronik imzaya önemli hukuki sonuçlar bağlanmıştır.

Bu bölümde genel olarak şekil kavramı, el ile atılan imza, el ile atılan imzaya bağlanan hukuki sonuçlar, elektronik imza, dijital imza, dijital imzanın teknik yapısı, güvenli elektronik imzaya bağlanan hukuki sonuçlar ve elektronik imza ile ilgili belirli düzenlemeler incelenecektir.

Sözleşme Nedir

Borç kavramı doktrinde, dar anlamda borç ve geniş anlamda borç olmak üzere ikiye ayrılarak incelenmektedir. Dar anlamda borç *"alacaklının borçludan istemeye yetkili olduğu, borçlunun da yerine getirmek zorunda olduğu tek bir edimi, yani bir tek alacak veya borcu..."* ifade edecek biçimde tanımlanmaktadır. Geniş anlamda borç ise alacaklı ve borçlu arasında farklı borçlar doğurabilen ve bu borçların bütününü oluşturan hukuki ilişki ya da borç ilişkisi olarak tanımlanmaktadır.

Borç ilişkileri hukuki işlemden veya doğrudan kanundan kaynaklanabilir. İşte sözleşmeler de borç ilişkisi kuran hukuki işlemlerdir. 6098 sayılı Türk Borçlar Kanunu'nun (RG. 04.02.2011, S. 27836, TBK) 1. maddesinin 1. fıkrasında, sözleşmelerin tarafların karşılıklı ve birbirine uygun irade açıklamalarıyla kurulduğu belirtilmiştir. Bir başka ifadeyle sözleşme, karşılıklı ve birbirine uygun irade açıklamalarıyla kurulan hukuki ilişkidir.

Sözleşmelerde Şekil

İradenin dış dünyaya söz, yazı, işaret gibi bir biçimde aktarılması şekil olarak adlandırılır. Her hukuki işlem ve her irade beyanı belirli bir şekilde yapılır. Örneğin, bir sözleşmenin imzalanması sözleşmenin şekli ile ilgili bir husustur.

Hukuk sistemimizde kural olarak şekil özgürlüğü geçerlidir. Bu kural TBK m. 12/1'de *"Sözleşmelerin geçerliliği, kanunda aksi öngörülmedikçe, hiçbir şekle bağlı değildir."* şeklinde düzenlenmiştir. Şekle bağlı olmamak ile kastedilen sözleşmelerin belirli bir şekilde yapılmasının zorunlu olmadığı, yani şekil özgürlüğüdür.

DİKKAT EDELİM

Bunlara Dikkat Edelim: Sözleşmelerde şekil amaca göre, geçerlilik şekli ve ispat şekli olmak üzere ikiye ayrılmaktadır. Geçerlilik şekli, tarafların şekil şartına uymamaları halinde hukuki işlemin geçersiz olduğu şekildir. Bir hukuki işlemin ispatı için aranan şekil ise ispat şeklidir.

Geçerlilik Şekli

TBK m. 12/2'ye göre *"Kanunda sözleşmeler için öngörülen şekil, kural olarak geçerlilik şeklidir. Öngörülen şekle uyulmaksızın kurulan sözleşmeler hüküm doğurmaz."* Söz konusu düzenlemeye göre bir sözleşme, kanun ile belirli bir şekle tabi tutulmuş ise bu şekil geçerlilik şekli olacak ve bu şekle uyulmaması halinde sözleşme hüküm doğurmayacak, yani geçersiz olacaktır. Kanunda düzenlenen şekil şartı yasal şekil ya da kanuni şekil olarak da adlandırılmaktadır.

Şekil, geçerlilik koşulu olarak yalnızca kanunda öngörülmemektedir. Taraflar kendi özgür iradeleri doğrultusunda kanunda şekle bağlanmamış bir sözleşmeyi belirli bir şekilde yapmak üzere anlaşabilirler. Bu durumda iradi şekil söz konusu olmaktadır. İradi şekilde, tarafların kanunda şekle bağlanmamış bir sözleşmeyi belirli bir şekilde yapmak üzere anlaşmaları halinde, belirlenen şekilde yapılmayan sözleşme tarafları bağlamaz (TBK m. 17/1). Ancak, taraflar geçerlilik koşulu yerine ispat koşulu olarak da iradi şekil kararlaştırabilirler. Taraflar, herhangi bir belirleme yapmaksızın yalnızca yazılı şekil kararlaştırırlarsa, yasal yazılı şekle, yani adi yazılı şekle ilişkin hükümler uygulanacaktır (TBK m. 17/2).

Tekrar etmek gerekir ki geçerlilik şekline uyulmamasının yaptırımı sözleşmenin geçersiz olmasıdır.

İspat Şekli

Daha önce belirtildiği gibi ispat şekli bir hukuki işlemin varlığının ispatı için gerekli olan şekildir. Mahkemede görülmekte olan bir davada ispat ise taraf taleplerinin dayandığı olay ve olguların doğru olup olmadığını konusunda hâkimi ikna etme faaliyeti olarak tanımlanmaktadır. İspat şekli kanundan veya taraf iradelerinden kaynaklı olabilir. Taraflar kendi özgür iradeleri doğrultusunda belirli bir ispat şekli belirleyebilirler. Bu durumda da iradi şekil söz konusu olur. İspat, medeni usul hukuku ile ilgili bir konu olduğu için ispata ilişkin kurallar 6100 sayılı Hukuk Muhakemeleri Kanunu'nda (RG. 04.02.2011, S. 27836, HMK) düzenlenmiştir.

HMK'da ispat şekli ile ilgili iki ana kural bulunmaktadır. Birinci kurala göre, HMK'da senetle ispat zorunluluğu başlığı ile düzenlenen m. 200/1 uyarınca, yapıldıkları tarihte miktar veya değeri belirli bir tutarı aşan hukuki işlemler kural olarak yalnızca senet ile ispat edilebilir. Burada senetle ispat zorunluluğu ile kastedilen kesin delille ispat zorunluluğudur. Bu hüküm, bahsedilen hukuki işlemlerde yazılı şekli zorunlu tutmaktadır. Ancak bu kuralın istisnaları bulunmaktadır. İkinci kural ise, HMK m. 201 gereğince; senet ile ileri sürülen her çeşit iddiaya karşı ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemlerin tanıkla ispatının yasak olmasıdır. Bir diğer ifadeyle senede karşı ancak senetle veya diğer kesin delillerle ispat mümkündür. Bu kuralın da belirli istisnaları bulunmaktadır.

İspat şekline uyulmamasının sonucu hukuki işlemin varlığının veya doğruluğunun ispat edilmemiş olmasıdır. İspat şekline uyulmaması sözleşmenin geçersiz olmasına neden olmaz. Geçerli olarak kurulan ancak ispatlanamayan bir hak veya hukuki işlem gerçekten var olsa bile mahkeme tarafından dikkate alınmayacaktır. Bu nedenle ispat şekli son derece önemlidir.

Şeklin Türleri

Şekil, yapılış biçimine göre; "sözlü şekil", "adi yazılı şekil", "nitelikli yazılı şekil" ve "resmi şekil" olarak dörde ayrılarak incelenmektedir.

Sözlü şekil, tarafların iradelerini sözlü olarak dış dünyaya aktarmalarıdır. Şekil özgürlüğü gereği kural olarak, sözleşmeler -kanunda veya taraflarca yapılan sözleşmede aksi kararlaştırılmadıkça- sözlü şekil ile geçerli biçimde kurulabilmektedir.

Adi yazılı şekil, beyan sahibinin, şekle bağlı irade beyanının içeriğini yazıyla belgeleyip imzalanması şeklinde tanımlanmaktadır. Adi yazılı şeklin metin ve imza olmak üzere iki unsuru bulunmaktadır. Adi yazılı şekilde yalnızca imzanın el yazısı ile olması gerekir. Metin, el yazısı, daktilo, yazıcı vb. araçlarla

oluşturulan, beyanda bulunan kişinin iradesinin yer aldığı somut belgedir. İmza ise belirli bir kişinin belgeyi yazdığını veya onayladığını belirlemek için kullanılan işarettir.

Nitelikli yazılı şekil, adi yazılı şekle göre ilave unsurların yer aldığı şekil türüdür. Örneğin, 4721 sayılı Türk Medeni Kanunu'nun (RG. 08.12.2001, S. 24607, TMK) 538. maddesinin birinci fıkrası uyarınca el yazılı vasiyetname nitelikli yazılı şekle tabi tutulmuştur. Hüküm; *"El yazılı vasiyetnamenin yapıldığı yıl, ay ve gün gösterilerek başından sonuna kadar miras bırakanın el yazısıyla yazılmış ve imzalanmış olması zorunludur."* şeklinde düzenlenmiştir. Görüldüğü üzere, adi yazılı şekilde metnin nasıl yazıldığı önem arz etmezken, el yazılı vasiyetnamede (nitelikli yazılı şekil) metnin başından sonuna kadar belirli unsurlarla birlikte el yazısıyla yazılmış olması şartı aranmıştır. Benzer şekilde, kefalet sözleşmesi de TBK m. 583/1'deki *"Kefalet sözleşmesi, yazılı şekilde yapılmadıkça ve kefilin sorumlu olacağı azamî miktar ile kefalet tarihi belirtilmedikçe geçerli olmaz. Kefilin, sorumlu olduğu azamî miktarı, kefalet tarihini ve müteselsil kefil olması durumunda, bu sıfatla veya bu anlama gelen herhangi bir ifadeyle yükümlülük altına girdiğini kefalet sözleşmesinde kendi el yazısıyla belirtmesi şarttır."* hükmüyle nitelikli yazılı şekle tabi tutulmuştur.

Resmi şekil, bazı hukuki işlemlerin resmi makamların huzurunda ve katılımıyla yapılmasıdır. Resmi şekilde, hukuki işlem veya sözleşme kanunda düzenlenen usul ve esaslara uyularak resmi senet düzenleme yetkisi bulunan kişi tarafından yapılır. Resmi senet düzenlemeye yetkili makamlar genel olarak, sulh hakimliği, noter ve tapu sicil müdürlükleridir. Örneğin, TBK m. 237/1 hükmü *"Taşınmaz satışının geçerli olabilmesi için, sözleşmenin resmî şekilde düzenlenmesi şarttır."* şeklinde düzenlenmiştir. Bu hüküm uyarınca, taşınmaz satışının geçerlilik koşulu resmi şekle bağlanmıştır.

İmza Nedir?

Daha önce belirtildiği üzere imza, bir kişinin bir belgeyi yazdığını veya onayladığını belirlemek için kullanılan işarettir. İmza, kişinin kimliğini tespit etmeye, onu diğer kişilerden ayırmaya yarar. İmza, genellikle ad ve soyadı içerecek biçimde atılır. 2525 sayılı Soyadı Kanunu (RG. 02.07.1934, S. 2741) m. 2'ye göre imzada, öz adın önde, soy adının sonda kullanılacağı belirtilmiştir. Ancak, bu hüküm emredici olmayıp, bir işaret veya başka sözcüklerden oluşan yazılar da imza olarak kabul edilebilecektir. Keza imzanın kısaltılmış hali olan paraflar da imza olarak nitelendirilmektedir. İmzanın her zaman aynı şekilde atılması şart değildir.

TBK m. 14/1 hükmü *"Yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunması zorunludur."* şeklinde düzenlenmiştir. Bu hüküm uyarınca, bir sözleşme ile borç altına giren tarafın sözleşmede imzasının bulunması gerekmektedir. İki tarafa borç yükleyen sözleşmelerde, her iki taraf da borç altına girdiği için iki tarafın da imzasının bulunması gerekmektedir.

Genel kural TBK m. 15/1 gereğince, borç altına giren kişinin el yazısı ile imza atması zorunluluğudur. Bu hükümler birlikte değerlendirildiğinde, adi yazılı şekle bağlı bir sözleşmede, borç altına giren kişinin el yazısı ile atılmış imzasının bulunması zorunludur.

TBK m. 14/2; *"Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer."* hükmünü ihtiva etmektedir. Bu maddede sayılan araçlar adi yazılı şekil şartını yerine getirmektedir. Ancak, bunun için TBK dışındaki bir kanunda bu hükmün aksine bir düzenlemenin yer almaması gerekmektedir.

Güvenli elektronik imza ile gönderilip saklanılan metinler konumuz açısından önem arz etmek-

tedir. Kanun, güvenli elektronik imza ile gönderilip saklanan metinlerin adi yazılı şekil şartını yerine getirdiğini kabul etmiştir.

İmza ile ilgili genel kuralın el yazısı ile imza atmak olduğunu belirtmiştik. Bu kuralın TBK m. 15 ve 16'da öngörülmüş üç istisnası bulunmaktadır. Bu istisnalar; bir araçla imza atmak, görme engellilerin imzası ve imza atamayanların imza yerine geçen işaretler kullanması olarak sayılabilir.

Bir araçla imza atmak ancak örf ve adetçe kabul edilen hallerde ve özellikle çok sayıda çıkarılan kıymetli evrakın imzalanmasında geçerli kabul edilmiştir (TBK m. 15/2). Ancak 6102 sayılı Türk Ticaret Kanunu'nun (RG. 14.02.2011, S. 27846, TTK) 756. maddesinin ikinci fıkrası ve 780. maddesi uyarınca bono, poliçe ve çeklerde imzaların el ile atılması zorunludur. Bu senetlerde herhangi bir mekanik araç (örneğin, damga) ile atılacak imza kullanılamaz.

Görme engellilerin imzası ile ilgili TTK m. 15/3'te *"Görme engellilerin talepleri halinde imzalarında şahit aranır. Aksi takdirde görme engellilerin imzalarını el yazısı ile atmaları yeterlidir."* düzenlemesi yer almaktadır. Ayrıca, 1512 sayılı Noterlik Kanunu (RG. 18.01.1972, S. 14090, NK) m. 73 uyarınca noterin; ilgilinin işitme, konuşma veya görme engelli olduğunu anlaması halinde ilgilinin isteğine bağlı olarak işlemlerin iki tanık huzurunda gerçekleştirileceği hüküm altına alınmıştır.

Herhangi bir sebeple imza atamayan kişiler (örneğin, okuma yazma bilmeyenler, sağlık durumları nedeniyle imza atamayanlar) ise, TBK m. 16/1 uyarınca, imza yerine usulünce onaylı parmak izi, el ile yapılmış bir işaret veya mühür kullanabileceklerdir. Ancak, bu hüküm kambiyo senetleri için uygulanmamaktadır (TBK m. 16/2). Söz konusu parmak izini, el işaretini veya mührü onaylamaya yetkili makam noterdir. Keza NK m. 75'te *"İlgililerle tanık, tercüman ve bilirkişi imza atamadıkları ve imza yerine geçen bir el işareti kullanmadıkları takdirde, varsa mühür, yoksa sol elinin baş parmağı, bu da yoksa diğer parmaklarından biri bastırılır ve hangi parmağın bastırıldığı yazılır."* hükmü yer almaktadır.

İmzaya Bağlanan Hukuki Sonuçlar

Bir kişi, metne imza atarak irade beyanını açıklar. İmza aracılığıyla hukuki işlemi gerçekleştiren kişinin kimliğinin tespit edilmesi sağlanır ve metinde yer alan ifadelerin imzalayan tarafından kabul edildiği varsayılır. Bir diğer ifadeyle, bir kişi metne imza attığında, kişinin metinde yer alan hukuki sonucu kabul ettiği anlaşılır.

HATIRLATMA

Daha önce belirtildiği üzere, TBK m. 14/1 uyarınca, borç altına giren kişinin sözleşmeyi imzalaması ile yazılı şekil şartı yerine getirilmiş olur. Bir diğer ifadeyle imza, geçerlilik koşulu olarak şekle bağlı bir sözleşmede, geçerlilik koşulunu yerine getirmeyi sağlayan bir unsurdur.
Yazılı şekilde yapılması öngörülen bir sözleşme imzalanmadan sözleşme geçerli olmaz.

HMK m. 199 hükmü; *"Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir."* düzenlemesi ile "belge" kavramının kapsamına nelerin gireceğini belirtmiştir.

Medeni usul hukukunda "belge" ile "senet" kavramları birbirlerinden farklıdır. Senet, hâkimi bağlayıcı nitelikte olan kesin deliller arasında yer almakta iken, belge kesin deliller arasında sayılmamıştır. Senet, onu düzenleyen kişinin imzasını taşımalıdır. Belgede ise böyle bir zorunluluk yoktur. Hatta belgenin onu düzenleyen kişinin imzasını içermesi halinde ortada bir senet söz konusu olabilecektir. Kesin delillerin dayanak teşkil ettiği bir iddiayı hâkim doğru kabul etmek zorundadır. Sonuç olarak imza, diğer unsurlarıyla birlikte bir belgenin hukuken senet olarak değerlendirilebilmesini mümkün kılmaktadır. Bu da ispat açısından önemli sonuçlar doğurmaktadır.

HMK m. 205/1; *"Mahkeme huzurunda ikrar olunan veya mahkemece inkâr edenden sadır olduğu kabul edilen adi senetler, aksi ispat edilmedikçe kesin delil sayılırlar."* düzenlemesi ile adi senetlerin aksi ispat edilmedikçe kesin delil olarak nitelendirileceğini hükme bağlamıştır. Adi senet, resmi makamların katılımı olmaksızın düzenlenen senettir.

Elektronik İmza Kanunu

5070 sayılı Elektronik İmza Kanunu (RG. 23.01.2004, S. 25355, EİK) Avrupa Birliği'nin 1999/93 sayılı Yönergesine uygun olarak düzenlenerek 15.01.2004 tarihinde kabul edilmiş ve 23.07.2004 tarihinde yürürlüğe girmiştir. Kanun ile elektronik imzanın hukuki, teknik yönleri ve kullanım esasları düzenlenmiştir. EİK'ya dayanarak hazırlanan, elektronik imzanın hukuki ve teknik yönleri ile uygulamasına ilişkin usul ve esasları düzenleyen Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (RG. 06.01.2005, S. 25692) 06.01.2005 tarihinde yürürlüğe girmiştir.

Elektronik İmza Nedir?

"Elektronik imza" denilince akla "dijital imza" gelse de iki kavramı karıştırmamak gerekir. Elektronik imza, dijital imzayı da kapsamına alan, elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavram olarak değerlendirilmektedir. Elektronik imza yöntemlerine örnek olarak; biyometrik imza (parmak izi, retina taraması gibi), PIN (Personal Identification Number), dijital ortama aktarılmış el yazısı ve dijital imza verilebilir.

EİK m. 3/1/b'de elektronik imza; *"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi"* ifade edecek biçimde düzenlenmiştir.

Dijital İmza Nedir?

Dijital imza, özel bir algoritma (hash fonksiyonu) kullanılarak oluşturulan ve gönderenin özel anahtarı ile şifrelenen bir ileti/mesaj özetidir. Dijital imza mesaja eklenerek alıcıya gönderilir. Alıcı, kendisine iletilen mesajdan yeniden bir mesaj özeti çıkarır ve gönderenin açık anahtarı ile dijital imza şifresini çözerek elde ettiği özet ile kendi hesapladığı özeti karşılaştırır. Böylece gönderilen mesaj ile kendisine ulaşan mesajın aynı olduğu, değişikliğe uğramadığı (veri bütünlüğü), ilgili kişi tarafından gönderildiği (kimlik doğrulama) ve mesajın gönderildiği (gönderildiğini inkâr edememe-bağlayıcılık) doğrulanmış olur.

Dijital imzanın oluşturulması için kriptografi (şifreleme) kullanılır. Kriptografi, anlaşılabilir durumda bulunan verilerin anlaşılamayacak hale dönüştürülmesinde kullanılan matematik yöntemlerinin bütünüdür.

Şifreli mesaj anlamsız bir hale geldiği için, bu mesajı anlamlı bir hale dönüştürmek için şifrenin çözülmesi gerekir. Şifrenin çözülmesi için ise anahtar gereklidir. Şifreleme için birçok teknik bulunmakla birlikte, en sık kullanılan şifreleme yöntemleri; simetrik şifreleme yöntemi ve asimetrik şifreleme yöntemidir.

Simetrik şifreleme yönetimde tek şifre (anahtar) hem mesajın şifrelenmesi hem de mesajın çözülmesinde kullanılır. Dolayısıyla, gönderici ve alıcı aynı anahtarı kullanır. Bunun için gönderici ve alıcının anahtarı bilmesi gerekir. İletinin güvenli bir biçimde gönderilebilmesi anahtarın gizliliğine bağlı olduğu için, simetrik şifreleme yöntemi yalnızca birbirine güvenen taraflarca kullanılması halinde ve internet ortamı dışarısında bir ortamda paylaşılması halinde güvenli bir biçimde kullanılabilecektir.

Asimetrik şifreleme yönteminde ise biri gizli (özel) ve biri açık(genel) olmak üzere iki anahtar bulunmaktadır. Gizli anahtara yalnızca kullanıcı erişebilir ve güvenlik gereği bu anahtarın kimse ile paylaşılmaması gerekir. Açık anahtar ise herkese açıktır ve güvenilir üçüncü kişiler tarafından ilan edilir. Dijital imzanın şifrelenmesi için asimetrik şifreleme yöntemi kullanılmaktadır.

Dijital İmzanın Teknik Yapısı

Asimetrik şifreleme yöntemi sayesinde mesajı gönderenin kimliği tespit edilebilecektir. Mesajın, özet fonksiyonu (hash) kullanılarak üretilen özet değeri (hash değeri) sayesinde ise mesajda herhangi bir değişiklik yapılmadığı tespit edilebilecektir.

Yukarıda bahsedildiği üzere, dijital imza asimetrik şifreleme yöntemi kullanılarak oluşturulur. Asimetrik şifreleme yönteminde açık ve gizli olmak üzere iki anahtar bulunur. Bu anahtarlar elektronik sertifika hizmet sağlayıcılar (ESHS) tarafından üretilir ve bir sertifika ile temsil edilirler. Bu sertifikada anahtar sahiplerinin kimlik bilgileri yer alır. Böylece dijital imzanın kimlik doğrulama fonksiyonu yerine getirilir.

Dijital imzanın taklit edilmesi zordur. Zira asimetrik şifreleme yönteminde kullanılan anahtar çifti uzun ve karmaşık bir yapıdadır. Ancak bu uzun şifrelerin kırılarak taklit edilmesi imkânsız değildir. Bu sebeple dijital imzanın tamamen güvenilir olduğu düşünülmemelidir.

Dijital imza ile imzalanmış mesajın alıcısı, imzanın dayandığı sertifikayı sağlayan sertifika hizmet sağlayıcısının sunucusunda sertifika bilgilerine ulaşabilir ve böylelikle göndericinin kimliğini tespit edebilir. Ayrıca göndericinin açık anahtarı da sertifika hizmet sağlayıcısının sunucusunda yayımlanacağı için, alıcı, mesajın göndericiden gelip gelmediğini kontrol edebilir.

Dijital imzada güvenlik sorunu gizli anahtarın saklanmasıyla ilgilidir. Zira gizli anahtara sahip olan kişi herkesin ulaşabildiği açık anahtara erişerek mesajın içeriğine ulaşabilecektir. Gizli anahtar dijital imzanın oluşturulmasına, açık anahtar dijital imzanın doğrulanmasına imkân vermektedir.

Gizli anahtar kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir. Gizli anahtar yalnızca kullanıcıya tahsis edildiği için bu chip kartın yetkisiz kişilerin eline geçmemesi için kullanıcının gerekli özen ve tedbiri göstermesi gerekir.

EK BİLGİ

Kullanıcı, chip kartını okuyucuya yerleştirip bilgisayara bağladıktan sonra, PIN şifresini girip imzala butonuna tıklayarak elektronik belgeyi dijital imza ile imzalamaktadır. Teknik yapısı anlatılan tüm süreç bilgisayar yazılımları vasıtasıyla otomatik olarak gerçekleştirilmektedir.

Uygulamada chip kartın güvenliğini sağlamak adına PIN (Personal Identification Number-Kişisel Kimlik Numarası) kullanılmaktadır. PIN, genellikle dört veya sekiz haneden oluşan, bir cihazı kullanacak kullanıcıyı doğrulamak için şifre olarak kullanılan sayı dizisidir. Chip kartın şifresi olarak PIN'lerin kullanımı, dört veya sekiz hanelik bir şifrenin zayıf güvenlik önlemi sağlaması nedeniyle doktrinde eleştirilmektedir.

Hash Fonksiyonu (Hash Function-Özet Fonksiyonu)

Asimetrik şifreleme yönteminde sertifikaya bağlanan anahtarlar kimlik doğrulama işlevini yerine getirmektedir. Ancak gönderilen mesajda değişiklik yapılıp yapılmadığı yalnızca bu yöntem kullanılarak anlaşılamaz. Alıcıya ulaşan mesajın gönderici tarafından gönderilen orijinal mesaj olup olmadığını tespit etmek amacıyla hash fonksiyonu geliştirilmiştir. Hash fonksiyonu, mesajı belirli bir uzunlukta özet değerine (hash value) dönüştürür. Bu özet değeri mesajı gönderen kişi tarafından mesaja eklenir ve mesajı alan alıcı mesaja tekrar aynı hash fonksiyonunu uygulayarak elde ettiği özet değeri ile gönderici tarafından gönderilen özet değerini karşılaştırır. Mesajda herhangi bir değişiklik yapılması halinde hash değeri de değişeceği için karşılaştırma sonucunda mesajda bir değişiklik yapılıp yapılmadığı anlaşılır.

DİKKAT EDELİM

Burada dikkat edilmesi gereken nokta şifrelemenin asıl mesaja değil, asıl mesajın hash değeri üzerine yapılması ve mesaja eklenerek alıcıya gönderilmesidir.

EK BİLGİ

Günümüzde en yaygın kullanılan hash fonksiyonları 128 bit boyutta hash değeri üreten MD5 (Message-Digest algorithm 5) ve 224, 256, 384 veya 512 bit boyutlarında hash değeri üreten SHA-3'tür. (Secure Hash Algorithm 3). MD5 hash fonksiyonu çeşitli saldırılara maruz kalarak güvenilirliği sarsılmış olsa da günümüzde yaygın olarak kullanılmaktadır.

Konuyu bir örnekle açıklayalım. A'nın B'ye dijital imzalı bir mesaj göndermek istediğini varsayalım. A'nın göndermek istediği mesaj *"B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim."* olsun. Öncelikle, A bu mesaja hash fonksiyonu uygulayacak ve bir sonuç elde edecektir. Sonucun "2e779edc849e4a9c9838dd7e02548838" olduğunu varsayalım. Daha sonra A, bu hash değerini mesaja ekleyecek ve kendi gizli anahtarını hash değerine uygulayacaktır. Bu durumda "2e779edc849e4a9c9838dd7e02548838" hash değeri şifreli olarak (genellikle hash değerine göre çok daha uzun bir şifre olacaktır) mesajın altında yer alacaktır. İşte burada yer alan şifreli hash değeri A'nın dijital imzasıdır. Mesaj bu haliyle B'ye gönderilecektir.

Mesaj kendisine iletilen B, öncelikle *"B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim."* mesajına hash fonksiyonunu uygulayacak ve "2e779edc849e4a9c9838dd7e02548838" hash değerini bulacaktır. Daha sonra A'nın gizli anahtarı yalnızca A'nın açık anahtarı kullanılarak çözülebileceği için B, A'nın açık anahtarını şifreli hash değerine uygulayacak ve "2e779edc849e4a9c9838dd7e02548838" değerini görebilecektir. İki hash değeri de aynı olduğu için gönderilen mesaj ile iletilen mesajda bir değişiklik yapılmadığı doğrulanmış olacaktır. Zira mesajda yapılacak en ufak değişiklik hash değerinin farklı hesaplanmasına yol açacaktır. Ayrıca şifreli hash değeri A'nın açık anahtarı ile çözülebildiği için mesajın A tarafından gönderildiği aksi ispat edilinceye kadar kesin olacaktır.

Örneği görsel olarak açıklayacak olursak, A'nın B'ye dijital imzalı olarak gönderdiği mesaj;

B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim.

A

04.10.2022

MIIBOwIBAAJBAI3pJFuPgjWya2uM1yuh4mKICmpjiVbYCnWoDOS0SNwROHuvmw6K5F
6q4hL1Fm2GDLgPVwoE3UIqkaTzjJqYxjECAwEAAQJACil4zgmvxFKbeJ8kRV6ZTH77Z/Tq
v8pGrXg0PChg00lYb3JnPEuQfgQrcu7Mfwd3XqqubyO8NOA+1Fa8Vlv9NQIhAO3AbqqnaIq
SQtSh/VBiHAlmjdOnbdWrZQswHR5DVsNPAiEAmM2JV+Y+ul+nTem6ABguQnqwF8Tg7N
ORxiNdWWODfn8CIQCmnmqwTFx2aKRPcisd73PonqecgkT2LoTEv3ZYpCak/wIgY6Xugm8
5yyskHTBmRzd9u4btHaMcF/XlY/SeJPQ7xZsCIQDqHEU7Cscp/2m9d423nVkiJEiSiqAGqQ4
wJ48ceHS1GQ== **(A'nın gizli anahtarı)**

2e779edc849e4a9c9838dd7e02548838 **(B'nin, A'nın gönderdiği mesaja *hash* fonksiyonu uygulayarak hesapladığı *hash* değeri)**

B öncelikle *"B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim."* mesajına hash fonksiyonu uygulayarak "2e779edc849e4a9c9838dd7e02548838" hash değerini elde eder.

Daha sonra B, elektronik sertifika hizmet sağlayıcıdan edindiği A'nın açık anahtarını

(MFw wwDQYJKoZIhvcNAQEBBQADSwAwSAJBAI3pJFuPgjWya2uM1yuh4mKICmpjiVbYCnWoDOS0SNwROHuvmw6K5F6q4hL1Fm2GDLgPVwoE3UIqkaTzjJqYxjECAwEAAQ==) A'nın gizli anahtarına uygular ve aşağıdaki sonucu elde eder. Bu noktada, şifreli hash değeri A'nın açık anahtarı ile çözü-

B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim.

A

04.10.2022

2e779edc849e4a9c9838dd7e02548838 **(imzalı hash değeri)**

lebildiği için mesajın A tarafından gönderildiği aksi ispat edilinceye kadar kesinleşmiş olur.

1. 2e779edc849e4a9c9838dd7e02548838 (B'nin hesapladığı hash değeri)
2. 2e779edc849e4a9c9838dd7e02548838 (imzalı hash değeri)

Son olarak B iki hash değerini karşılaştırır ve mesajın orijinal mesaj olup olmadığını (mesajda değişiklik yapılmadığını) doğrular.

İki değer de aynı olduğu için mesajın A tarafından gönderilen orijinal mesaj olduğu doğrulanmış oldu.

HATIRLATMA

Yukarıda belirtilen teknik işlemlerin tümü bilgisayar tarafından belirli yazılımlar vasıtasıyla otomatik olarak gerçekleşmektedir. Dolayısıyla uzun bir sıralama ile anlatılan güvenli elektronik imzanın oluşturulması ve doğrulanması işlemleri saniyeler içerisinde tamamlanmaktadır.

Zaman Damgası

Hukuki işlemlerin ne zaman gerçekleştirildiği önemlidir. Bir sözleşmenin kurulmasıyla tarafların hak ve borçları doğacak, buna bağlı olarak ifa zamanı belirlenebilecek, süre sınırının olduğu hukuki işlemlerde sürenin bitmesi hak kayıplarına yol açacaktır. Bu gibi sebeplerle irade beyanlarının ne zaman gerçekleştirildiğini belirlemek gerekir.

Elektronik ortamdaki verilerle oluşturulan belgelerde, belgenin oluşturulma zamanına çok basit bir biçimde, bilgisayarın tarih ve saat ayarlarının değiştirilmesi ile müdahale edilebildiği için hukuki işlemin yapılma anını bu şekilde belirlemek güvenli değildir. Zaman damgası, elektronik ortamda yapılan irade beyanlarının yapılma anını belirlemek ihtiyacını güvenilir bir biçimde karşılamak üzere geliştirilmiştir.

EİK m. 3/1 h bendinde zaman damgası; *"Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı ... ifade eder."* şeklinde tanımlanmıştır.

Zaman damgası elektronik sertifika hizmet sağlayıcısı (ESHS) tarafından elektronik imzayla doğrulanan kayıt sistemidir. Gönderici, mesajını önce ESHS'ye ulaştırır ve ESHS, göndericinin dijital imzasına, mesajın kendisine ulaşma zamanını gösteren bir damga ekler ve elektronik imzasıyla imzalar. Böylece, göndericinin mesajına ESHS tarafından eklenen zaman damgası sayesinde, mesajın gönderilme zamanı güvenli bir biçimde tespit edilebilir. Ayrıca mesajın gönderilme zamanına ESHS tarafından tutulan kayıtlardan da ulaşılabilir.

Güvenli Elektronik İmza Nedir

Güvenli elektronik imza;

"a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,"

elektronik imza olarak tanımlanmıştır.

Bir elektronik imzanın güvenli elektronik imza sayılması için; münhasıran imza sahibine bağlı olması, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulması, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlaması ve imzalanmış elektronik veride sonradan herhangi bir değişikliğin yapılmamış olması gerekir. Aksi takdirde güvenli elektronik imzaya bağlanan hukuki sonuçlar uygulama alanı bulmayacaktır. Güvenli elektronik imzada kullanılan gizli anahtar, kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir.

EİK kapsamında düzenlenen güvenli elektronik imza, Avrupa Birliği'nin 1999/93 sayılı Yönergesi'nde düzenlenen gelişmiş elektronik imza ile paraleldir.

EİK'da güvenli elektronik imza ile kast edilen elektronik imza türü dijital imzadır.

Münhasıran İmza Sahibine Bağlı Olma Unsuru

Kimlik doğrulaması işlevinin yerine getirilmesi, elektronik imzanın münhasıran imza sahibine bağlı olması ile mümkündür. Yukarıda yaptığımız açıklamalarda el yazısı ile atılan imza için kişinin kimliğini tespit etmeyi ve onu diğer kişilerden ayırmayı sağladığını belirtmiştik. Aynı durum güvenli elektronik imza için de geçerlidir. El yazısı ile atılan imza, el yazısının özgün ve karakteristik olması nedeniyle kimlik tespitini sağlarken, güvenli elektronik imzada kimlik tespiti, güvenli elektronik imza oluşturma aracının sadece imza sahibinin tasarrufunda bulunmasıyla, güvenli elektronik imzanın münhasıran imza sahibine bağlı olmasıyla ve güvenli elektronik imzanın nitelikli elektronik sertifikaya bağlı olmasıyla sağlanmaktadır.

Sadece İmza Sahibinin Tasarrufunda Bulunan Güvenli Elektronik İmza Oluşturma Aracı ile Oluşturulma Unsuru

EİK m. 6'da güvenli elektronik imza oluşturma araçları;

"a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini," sağlayan imza oluşturma araçları olarak tanımlanmıştır.

O halde, güvenli elektronik imzadan bahsedebilmek için, güvenli elektronik imzanın, yukarıda sayılan şartları taşıyan bir güvenli elektronik imza oluşturma aracı ile oluşturulması gerekmektedir. Bu şartları taşıyan elektronik imza oluşturma aracı EİK'ya göre güvenli kabul edilmiştir.

Daha önce belirtildiği üzere, güvenli elektronik imzada kullanılan gizli anahtar, kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir. Bu chip kart güvenli elektronik imza aracında yer almaktadır. Uygulamada güvenli elektronik imza oluşturma aracı genellikle; chip kart ve kart okuyucu USB parçalarından oluşmaktadır. Bu donanımlar bilgisayara bağlandıktan sonra bir yazılım vasıtasıyla imzalama işlemi tamamlanmaktadır.

Nitelikli Elektronik Sertifikaya Dayanarak İmza Sahibinin Kimliğinin Tespitini Sağlama Unsuru

EİK m. 3/1.1 bendinde elektronik sertifika, "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı" ifade edecek biçimde tanımlanmıştır.

EİK m. 9'da, nitelikli elektronik sertifikada bulunması gereken unsurlar aşağıdaki şekilde sayılmıştır:

"Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının, bulunması zorunludur."

Görüldüğü üzere, kimlik doğrulama işlevinin önemli bir parçası olan nitelikli elektronik sertifikada imza sahibinin teşhis edilebileceği kimlik bilgileri yer almaktadır.

EİK m. 9/1, d bendinde yer alan imza doğrulama verisi EİK m. 3/1/f'ye göre *"Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri"* ifade etmektedir. İmza sahibinin açık anahtarı bu kapsamdadır.

Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihi de ESHS'ler tarafından sertifikaya işlenir.

İmzalanmış Elektronik Veride Sonradan Herhangi Bir Değişiklik Yapılıp Yapılmadığının Tespitini Sağlama Unsuru

İmzalanış elektronik veride herhangi bir değişiklik yapılıp yapılmadığı hash fonksiyonu ile sağlanmaktadır. Bu konu, yukarıda ayrıntılı olarak açıklandığı için tekrarlanmayacaktır.

Güvenli Elektronik İmzaya Bağlanan Hukuki Sonuçlar

Daha önce belirtildiği üzere, kanunda aksine hüküm bulunmadığı takdirde, TBK m. 14/2 uyarınca güvenli elektronik imza ile gönderilip saklanabilen metinler yazılı şekil yerine geçer.

Gerek EİK m. 5/1, gerek TBK m. 15/1. fıkrasında güvenli elektronik imzanın el ile atılan imza ile aynı hukuki sonucu doğurduğunu hüküm altına almıştır. Ancak, bu kural her hukuki işlem için geçerli değildir. EİK m. 5/2'de bu kuralın istisnaları *"Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları ve Türkiye'de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez."* şeklinde düzenlenmiştir.

Böylece, güvenli elektronik imza ile resmi şekle veya özel bir merasime tabi olmayan hukuki işlemler ve teminat sözleşmeleri hariç (yalnızca banka teminat mektupları ve Türkiye'de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri güvenli elektronik imza ile yapılabilir), adi yazılı şekilde yapılabilen tüm sözleşmeler yapılabilir. Nitelikli yazılı şekilde sözleşme metninin de el yazısı ile yazılması arandığı için; nitelikli yazılı şekil şartının bulunduğu sözleşmelerde güvenli elektronik imza kullanılamayacaktır.

Örneğin, kanunla resmi şekle tabi tutulan taşınmaz satışı; kanunun özel bir merasime tabi tuttuğu evlilik; kanunun nitelikli yazılı şekle tabi tuttuğu el yazılı vasiyetname ve kefalet sözleşmesi, banka teminat mektupları ve Türkiye'de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri dışındaki diğer teminat sözleşmeleri geçerlilik şekline uygun olmadığı için güvenli elektronik imza ile gerçekleştirilemez.

Hatırlamak gerekir ki, kanun koyucu HMK'nın 199. maddesinde *"...fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları..."* belge olarak nitelendirmiştir.

Medeni usul hukukunda kesin deliller; ikrar, kesin hüküm, senet ve yemin olarak sayılmış olup, bu deliller hâkimi bağlayıcı niteliktedir. Hâkim, kesin delillerin dayandığı bir iddiayı doğru kabul etmek zorunda olup, bu konuda hâkimin takdir yetkisi bulunmamaktadır. Kanunda düzenlenen takdiri deliller ise; tanık, bilirkişi, keşif ve uzman görüşüdür. Hâkim bu delillere dayanan iddiaların doğru olup olmadığını takdir yetkisine dayanarak değerlendirebilir.

Yukarıda da belirtildiği gibi senetler kesin deliller arasında yer almaktadır. HMK m. 205/2 hükmü; *"Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir."* şeklinde düzenlenmiştir. Hükme göre, usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik verilerin aksi ispat edilinceye kadar kesin delil olarak nitelendirileceği kabul edilmiştir.

HMK m. 205/3, güvenli elektronik imzanın teyit edilmesi ile ilgili; *"Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler."* düzenlemesini içermektedir. Re'sen inceleme, hâkimin belgenin elektronik imza ile oluşturulup oluşturulmadığını kendiliğinden araştırması anlamına gelmektedir.

Güvenli elektronik imzalı veriye dayanarak mahkemeden bir talepte bulunulması halinde, karşı taraf bu verinin doğruluğunu veya varlığını inkâr edebilir. Bu durumda HMK'nın *"Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur."* şeklindeki 210. maddesi uygulanır. Hükme göre hâkim, tarafları ve gerekirse bilirkişiyi dinleyerek verinin doğruluğu hakkında bir karara varacaktır.

HATIRLATMA

Hatırlamak gerekir ki, burada anlatılan hukuki sonuçlar her elektronik imza için geçerli olmayacaktır. Burada bahsedilen hukuki sonuçlar yalnızca güvenli elektronik imza için geçerlidir.

Elektronik Sertifika Hizmet Sağlayıcısı

Dijital imzanın, güvenli elektronik imza olarak değerlendirilebilmesi için nitelikli elektronik sertifikaya dayanarak imza sahibinin kimlik tespitini sağlaması gerektiğini belirtmiştik (EİK m. 4/1/c). Bunun altında yatan sebep, açık anahtar ve gizli anahtar oluşturma algoritmaları ve yöntemlerinin tek başına güvenli olmamasıdır. Bu algoritmalar ve yöntemlerin kötü niyetli bir kişi tarafından bilinmesi ve imzada kullanılmak üzere sahte bir kimliğe bağlı bir çift dijital imza anahtarı üretilmesi mümkündür. Bu nedenle dijital imza açık anahtarının güvenilir bir üçüncü kişi tarafından onaylanarak belirli bir kişiye tahsis edilmesine ihtiyaç duyulmuştur. Güvenilir üçüncü kişi *(Trust Center)*, sertifika makamı *(Certification Authority)* veya onay makamı olarak da adlandırılmaktadır. Türk hukukunda bu makam ESHS'dir. ESHS'lerin yayımladığı sertifikalarda yer alan bilgilerin doğru olduğu kabul edilmektedir . Ayrıca, zaman damgası hizmetini de ESHS sunmaktadır.

Dijital imzada kullanılan asimetrik şifreleme yöntemi kapsamında açık ve gizli anahtarları (şifreleri) ESHS hazırlar. Hazırlanan her anahtar, her bir kullanıcı için ayrı olarak oluşturulmaktadır. Dijital imza kullanıcısı ESHS'ye başvurarak, kimlik bilgilerini iletir, bunun üzerine ESHS, açık anahtarı kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Gizli anahtar ise kullanıcı dışında kimseye verilmez. Kullanıcı, alıcıya dijital imzalı bir mesaj gönderdiğinde alıcı, ESHS'nin listesinden kullanıcının açık anahtarına ulaşabilir ve şifreli mesajı çözerek, okunur hale getirebilir.

Elektronik Sertifika Hizmet Sağlayıcısının Faaliyete Başlaması

ESHS olarak faaliyete başlayabilme şartları EİK m. 8'de düzenlenmiştir. Hükme göre ESHS faaliyete başlamak için herhangi bir izin almak zorunda değildir.

EİK m. 8/1; *"Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer."* şeklinde düzenlenmiştir. Görüldüğü üzere, bu hükme göre gerçek veya tüzel kişiler herhangi bir izne tabi olmaksızın ESHS olabilecektir. Burada düzenlenen usul bildirim usulü olarak adlandırılmaktadır. Ancak bahsi geçen maddenin devam eden fıkralarına ve Elektronik İmza Yönetmeliği'ne birlikte bakıldığında, burada aslında bildirim usulünün değil izin usulünün düzenlendiği anlaşılacaktır. Bu hususa ilerleyen paragraflarda ayrıntılı olarak değinilecektir.

ESHS'nin faaliyete başlayabilmesi için Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) bildirimde bulunması gerekmektedir. Bu bildirimde belirli şartların sağlanması gerekmektedir.

EİK m. 8/2'de bu şartlar;

"a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak" olarak sayılmıştır. BTK, ESHS'nin bu şartları yerine getirip getirmediğini re'sen inceler. Şartlardan birinin eksik olması veya yerine getirilmediği tespit edilirse, bu eksiklerin giderilmesi için hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verilir, bu süre içinde hizmet sağlayıcısının faaliyetleri durdurulur (EİK m. 8/3). Bu süre içerisinde de eksikler giderilmezse, BTK, ESHS'nin faaliyetlerine son verir (EİK m. 8/3).

ESHS faaliyetlerine devam ederken, yukarıdaki paragrafta sayılan şartları (EİK m. 8/2'de yer alan şartlar) kaybederse yine yukarıdaki paragrafta anlatılan, önce süre verilmesiyle başlayan usul (EİK m. 8/3) uygulanır.

EİK m. 20'de yer alan *"Bu Kanunun uygulanmasına ilişkin usul ve esaslar, ilgili kurum ve kuruluşların görüşü alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir."* hükmü gereğince, EİK m. 8/2'de yer alan şartlar, Elektronik İmza Yönetmeliği ile somutlaştırılmıştır. Yönetmelik Ek-1'de bildirimde sunulacak bilgi ve belgeler düzenlenmiştir.

Elektronik İmza Yönetmeliği m. 7/1'de; *"Kurum, yapılan bildirimi derhal incelemeye alır ve incelemeyi iki (2) ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki (2) ay sonra faaliyete geçer."* hükmü düzenlenmiştir. BTK'nın bildirimi re'sen incelemesi, iki ay içerisinde kararını açıklaması, bildirim şartlarını yerine getirmeyen hizmet sağlayıcıların faaliyetinin durdurulması birlikte değerlendirildiğinde "bildirim" adı altında geçen usulün aslında izin usulü olduğu anlaşılmaktadır. BTK'nın ESHS'lerin faaliyetine son verme yetkisi de bu görüşü destekler niteliktedir.

Elektronik Sertifika Hizmet Sağlayıcısının Temel Yükümlülükleri

ESHS'lerin temel yükümlülükleri EİK m. 10'da düzenlenmiştir. Ancak, ESHS'lerin yükümlülükleri bu maddede sayılanlar ile sınırlı değildir. ESHS'lerin EİK'da düzenlenen diğer maddelere ve genel hükümlere göre de yükümlülükleri bulunmaktadır. Biz, bu konu kapsamında en önemli ve bilinmesi gereken yükümlülüklere değinmekle yetineceğiz.

EİK m. 10/1' de düzenlenen ESHS'nin önemli yükümlülükleri;

"b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre veya Türkiye Cumhuriyeti kimlik kartı vasıtasıyla uzaktan güvenilir bir biçimde tespit etmek

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamak

e) Kanunlarda öngörülen sınırlamalar saklı kalmak üzere sertifikanın kullanımına ilişkin özellikler, uyuşmazlıkların çözüm yolları ile ilgili şartlar ve güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında talep eden kişiyi sertifikanın tesliminden önce bilgilendirmek

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini bilgilendirmek

g) Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamak

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmek" olarak sayılabilir.

Güvenli elektronik imzanın en önemli fonksiyonlarından biri olan kimlik tespiti, daha önce de belirtildiği üzere, ESHS'lerce çıkarılan nitelikli sertifikalar ile sağlanmaktadır. ESHS, açık anahtarı kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Böylece imza sahibinin kimliği tespit edilebilir.

Güvenli elektronik imzaya bağlanan hukuki sonuçlardan en önemlisi olan güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiye sertifika tesliminden önce bilgi vermek de ESHS'nin yükümlülükleri arasındadır.

ESHS, sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini bilgilendirmek ile yükümlüdür. Bu bilgilendirmeyi yaptıktan sonra imza oluşturma verisini başkasına kullandırmak imza sahibinin sorumluluğuna tabi olacaktır. Uyuşmazlık halinde ESHS, bilgilendirme yaptığını ispatlamakla yükümlüdür. Aksi takdirde meydana gelen zararlardan sorumlu olacaktır. Keza ESHS'nin hukuki sorumluluğunun düzenlendiği EİK m. 13'te *"Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz."* hükmü yer almaktadır.

ESHS, verdiği hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla yükümlüdür. Ayrıca faaliyetine son vereceğini en az üç ay önce BTK'ya ve sertifika sahibine bildirmekle yükümlüdür.

Son olarak, EİK m. 10/2'de *"Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz."* hükmü yer almaktadır. Bu hüküm gereğince, ESHS'nin ürettiği imza oluşturma verisi yalnızca imza sahibine tahsis edilecek, gizliliği korunacaktır. ESHS kendisi dahi bu veriyi kopyalayamayacak veya bu veriyi saklayamayacaktır.

BÖLÜM ÖZETİ

Elektronik belgeler el ile imzalanamamakta olup imzanın taranarak belgeye eklenmesi güvenlik ihlalleri nedeniyle mümkün değildir. Taranmış imzanın, imzalayan tarafından elektronik belgeye eklendiğini ispatlamak çok zordur. Taranmış imza, kolaylıkla kötü niyetli üçüncü kişilerin eline geçebilir ve imza kopyalanarak taklit edilebilir. Bilgisayarda üretilen belgelerin tarih, saat, yazar bilgileri kolaylıkla değiştirilebilmektedir. Bu sebeplerle elektronik ortamda yer alan verilere dayanan hukuki işlemlerin yazılı şekle uygun yapılamaması sorunu doğmuştur. Bu sorun, elektronik imza düzenlemeleri ile dijital imza ya da Elektronik İmza Kanunu'nda yer alan güvenli elektronik imzanın kullanılmasıyla çözülmüştür.

Gerek Elektronik İmza Kanunu gerekse Türk Borçlar Kanunu güvenli elektronik imzanın el ile atılan imza ile aynı hukuki sonucu doğurduğunu hüküm altına almıştır. Burada güvenli elektronik imza ile kastedilen, kanundaki şartları taşıyan dijital imzadır. Ancak, bu hukuki sonuç yalnızca Elektronik İmza Kanunu madde 4'te tanımlanan güvenli elektronik imza için geçerlidir. Burada sayılan şartları taşımayan veriler, Hukuk Muhakemeleri Kanunu madde 199 gereğince belge olarak kabul edilebilmektedir.

Güvenli elektronik imzaya bağlanan hukuki sonuçlardan bir diğeri ispata ilişkin olmak üzere usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik verilerin, aksi ispat edilinceye kadar kesin delil olarak nitelendirileceğidir. Elektronik imza denilince akla dijital imza gelse de elektronik imza dijital imzayı da kapsamına alan elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavramdır. Elektronik imza yöntemlerine örnek olarak; biyometrik imza (parmak izi, retina taraması gibi), PIN, dijital ortama aktarılmış el yazısı ve dijital imza verilebilir.

Dijital imzanın teknik yapısı temel olarak; asimetrik şifreleme yöntemine, hash fonksiyonuna ve zaman damgasına dayanmaktadır. Asimetrik şifreleme yönteminde kullanılan gizli ve açık anahtarlar elektronik sertifika hizmet sağlayıcıları tarafından üretilir ve bir sertifika ile temsil edilirler. Bu sertifikada anahtar sahiplerinin kimlik bilgileri yer alır. Böylece dijital imzanın kimlik doğrulama fonksiyonu yerine getirilir. Hash fonksiyonu ile mesajda herhangi bir değişiklik yapılmadığı doğrulanır.

Zaman damgası ile güvenli elektronik imzalı belgenin ne zaman oluşturulduğu ve gönderildiği tespit edilir. Zaman damgası hizmeti, elektronik sertifika oluşturulması elektronik sertifika hizmeti sağlayıcıların görevleri arasındadır. Elektronik sertifika hizmeti sağlayıcılar, açık anahtarı kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Gizli anahtar ise kullanıcı dışında kimseye verilmez. Böylece imza sahibinin kimliği tespit edilebilir. Güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiye sertifika tesliminden önce bilgi vermek de Elektronik sertifika hizmeti sağlayıcıların yükümlülükleri arasındadır. Elektronik sertifika hizmeti sağlayıcılar, sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda sertifika sahibini bilgilendirmek ile yükümlüdür.

GÖZDEN GEÇİRELİM

1. Sözleşmelerde geçerlilik şekline uyulmamasının yaptırımı ..... iken ispat şekline uyulmamasının yaptırımı ..... .

2. Adi yazılı şekle bağlı bir sözleşmede kural olarak, borç altına giren kişinin ..... bulunması zorunludur.

3. Senet, hâkimi bağlayıcı nitelikte olan ..... arasında yer almaktadır.

4. ..... dijital imzayı da kapsamına alan, elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavram olarak değerlendirilmektedir.

5. ..... özel bir algoritma (hash fonksiyonu) kullanılarak oluşturulan ve göndere-nin özel anahtarı ile şifrelenen bir ileti/mesaj özetidir.

6. Dijital imzanın şifrelenmesi için ..... kullanılmaktadır.

7. Gerek EİK m. 5/1, gerek TBK m. 15/1 güvenli elektronik imzanın ..... hüküm altına almıştır.

8. Güvenli elektronik imza ile ..... ve teminat sözleşmeleri hariç (yalnızca banka teminat mektupları ve Türkiye'de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri güvenli elektronik imza ile yapılabilir), ... yapılabilen tüm sözleşmeler yapılabilir.

9. Usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik veriler; aksi ispat edilinceye kadar ..... olarak değerlendirilecektir.

10. Dijital imza açık anahtarının güvenilir bir üçüncü kişi tarafından onaylanarak belirli bir kişiye tahsis edilmesine ihtiyaç duyulmuştur. Güvenilir üçüncü kişi (Trust Center), sertifika makamı (Certification Authority) veya onay makamı olarak da adlandırılmaktadır. Türk hukukunda bu makam .....'dır.

CEVAP ANAHTARI

1. sözleşmenin geçersiz olması / sözleşmenin varlığının veya doğruluğunun ispat edilmemiş olmasıdır.	6. asimetrik şifreleme yöntemi
2. El yazısı ile atılmış imzasının	7. el ile atılan imza ile aynı hukuki sonucu doğurduğunu
3. kesin deliller	8. resmi şekle veya özel bir merasime tabi olmayan hukuki işlemler/ adi yazılı şekilde
4. Elektronik imza	9. kesin delil
5. Dijital imza	10. Elektronik sertifika hizmet sağlayıcısı (ESHS)

SÖZLÜK

Algoritma: Bir sorunun çözümü veya cevabını bulmak üzere sınırlı sayıda adımlardan oluşan sistematik yöntem.

Anahtar: Bilişimde şifre yazmak ve çözmek için kararlaştırılmış olan yol.

Bit: Bilgisayarda veri depolama ve aktarımında en küçük birimdir. Bir byte 8 bitten oluşur.

Biyometrik imza: İmza sahibinin biyometrik verilerini kullanarak ve genellikle bu verilerin imzalanan belgeye çözülemez biçimde bağlanmasıyla oluşturulan imzalama yöntemi.

Chip kart: Akıllı kart veya tümleşik devre kartı olarak da adlandırılan, entegre devreler içeren, herhangi bir mikroçip boyutunda karttır.

Delil: Bir vakıanın ispatı için başvurulan araç veya araçlar.

Dijital: Sayısal.

Hukuki işlem: Bir ya da daha çok kişinin hukuk düzeninin öngördüğü sınırlar içerisinde, hukuki sonuç veya sonuçlar doğurmaya yönelik irade açıklaması.

Hukuki sonuç: Hukuk düzeninin hukuki olaylara bağladığı sonuç. Hukuki sonuca bağlı olarak bir hak veya hukuki ilişki kurulur, değiştirilir veya ortadan kaldırılır.

İrade beyanı: Hukuki bir sonuca yönelik işlem iradesini dış dünyaya açıklamak.

Paraf: Yalnız adın veya ad ve soyadın baş harfleriyle atılan kısa imza.

Sunucu: Bilgisayar biliminde sunucu, istemci adı verilen başka programlar veya cihazlar için işlevsellik sağlayan belirli bilgisayar donanım ve yazılımlarının (bilgisayar programlarının) bileşimidir.

USB: Dış donanımların bilgisayar ile bağlantı kurabilmesini sağlayan bağlantı aparatı.

Üçüncü kişi: Bir sözleşmenin, davanın veya icra takibinin taraflarının dışında olan kişi.

Veri: Ölçüm, deney, gözlem gibi araştırma yöntemleri vasıtasıyla elde edilen ham olgu veya gözlemler.

Yürürlüğe girmek: Bir kanun, yönetmelik vb. düzenlemenin, kararın uygulanır duruma gelmesi.

KAYNAKÇA

Antalya, Gökhan: Borçlar Hukuku Genel Hükümler, 2. Bası, C. V/1,1, Seçkin Yayıncılık, Ankara 2019.

Arslan, Ramazan/Yılmaz, Ejder/Taşpınar Ayvaz, Sema/Hanağası, Emel: Medenî Usul Hukuku, 4. Bası, Yetkin Yayıncılık, Ankara 2018.

Eren, Fikret: Borçlar Hukuku Genel Hükümler, 26. Bası, Yetkin Yayıncılık, Ankara 2021.

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

Greenleaf, Grahan/Clarke, Roger: "Privacy Implications of Digital Signatures", 1997, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263663), (E.T.: 04.10.2022).

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

Kılıçoğlu, Ahmet M.: Borçlar Hukuku, 25. Bası, Turhan Yayınevi, Ankara 2021.

Menezes, Alfred J./Oorschot, Paul C. Van/Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, 1997.

Orta, Mesut: Elektronik İmza ve Uygulaması, Seçkin Yayıncılık, Ankara 2005.

Sağlam, İpek: Elektronik Sözleşmeler, Legal Yayıncılık, İstanbul 2007.

Sarıakçalı, Turgay: İnternet Üzerinden Akdedilen Sözleşmeler, 2. Bası, Seçkin Yayıncılık, Ankara 2021.

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

Topaloğlu, Mustafa: Bilişim Hukuku, Karahan Kitabevi, Adana 2005.