Elektronik İmza Seviyeleri

Levels of Electronic Signature

Merve Melis ŞİMŞEK
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
melis.balkaya@tubitak.gov.tr

Tuğba ÖZCAN
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
tugba.ozcan@tubitak.gov.tr

Tamer ERGUN
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
tamer.ergun@tubitak.gov.tr

Vural ÇELİK
TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi
vural.celik@tubitak.gov.tr

Bilgi Yönetimi Dergisi
Cilt: 2 Sayı: 2 Yıl: 2019
https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 06.11. 2019
Kabul tarihi: 09.12. 2019
Yayınlanma tarihi: 31.12. 2019

Article Info

Date submitted: 06.11. 2019
Date accepted: 09.12. 2019
Date published: 31.12. 2019

Anahtar sözcükler

Elektronik imza nitelikli elektronik imza, gelişmiş elektronik imza, biyometrik imza

Keywords

Electronic signature, qualified electronic signature, advanced electronic signature, biometric signature

DOI numarası

10.33721/by.642860

ORCID

0000-0001-9737-302X (1)
0000-0002-9015-2790 (2)
0000-0002-7118-5191 (3)
0000-0003-3319-8829 (4)

Öz

Ülkemizde nitelikli elektronik imzanın kullanımına 5 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile başlanmıştır. 5070 sayılı Kanun, Avrupa Birliği (AB) 1999/93/EC Direktifini model alarak güven hizmetleri kapsamını elektronik imza ve zaman damgası ile sınırlı tutmaktadır. 2014 yılında ise günümüz gereksinimlerini karşılamak için elektronik kimlik tanımlama ve güven hizmetleriyle ilgili bir AB tüzüğü olan Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü (eIDAS) yayımlanarak güven hizmetleri çeşitlendirilmiştir. AB 1999/93/EC Direktifi yerine geçen eIDAS; basit, gelişmiş ve nitelikli olmak üzere birbiri üzerine yapılanan üç farklı elektronik imza türü tanımlamaktadır.

eIDAS'da tanımlanan farklı seviyedeki elektronik imza türlerinin AB üyesi ülkelerde elektronik işlemlerde kullanımına bakıldığında, imza türü seçiminin, işlemin gerektirdiği güvenlik ihtiyacına uygun seviyede yapıldığı görülmektedir. Bazı ülkelerde tüketici kredisine başvurmak ya da kira sözleşmesi imzalamak gibi ticari işlemler için nitelikli elektronik imza gerekirken; bankacılık, sigortacılık, telekomünikasyon alanlarında bazı işlemlerde gelişmiş elektronik imza kullanımının yeterli olduğu, üniversitelerde öğrenci işleri işlemlerinde ise genellikle basit elektronik imzanın kullanıldığı görülmektedir. Ülkemize bakıldığındaysa, elektronik işlemlerde güvenlik kriterlerinin belirlenmemesi sebebiyle neredeyse tüm işlemlerde Elektronik İmza Kanunu'na göre ıslak imzayla eşdeğer kabul edilen nitelikli elektronik imzanın kullanıldığı görülmesine karşın son zamanlarda farklı yaklaşımlar da ortaya çıkmıştır. Bu yaklaşımlar içinde en popüleri biyometrik imzadır. Biyometrik imza, ülkemizde GSM operatörleri ve bazı bankalar tarafından kullanım kolaylığı sağlaması nedeniyle ıslak imza gerektirmeyen işlemlerde tercih edilmektedir.

Bu çalışmada, eIDAS elektronik imza seviyeleri incelenerek popüler örnek olan biyometrik imzanın belirtilen imza çeşitlerinden hangisine girdiği üzerinde durulacak; ülkemizde elektronik imza türlerinin kullanımı için yasal çerçevenin çizilmesi ve ortak çalışabilirliğin sağlanabilmesi amacıyla elektronik imzanın sınıflandırılması gerekliliğine dikkat çekilecektir.

Abstract

The use of a qualified electronic signature in Turkey started with the Electronic Signature Law No. 5070 dated January 5, 2004. Law No. 5070 restricts the scope of trust services to electronic signatures and timestamps by taking the European Union (EU) Directive 1999/93/EC as a model. In 2014, trust services were varied to meet today's requirements with the Regulation on Electronic Identification and Trust Services (eIDAS). It repeals EU Directive 1999/93/EC and defines three different types of electronic signatures, which are basic, advanced and qualified.

In EU member countries, the type of eIDAS electronic signature is selected in accordance with the security required by the transaction. Some of the countries require the use of qualified electronic signatures for commercial transactions, such as applying for consumer loans or signing a lease. Similarly, in the banking, insurance, telecommunication fields, the use of advanced electronic signature is sufficient while basic electronic signatures are generally used in transactions requiring less security, such as student affairs in universities. On the other hand, in Turkey, it is seen that the qualified electronic signature is used in almost all transactions due to the lack of security criteria in electronic transactions. But recently there are different approaches. The most popular of these approaches is the biometric signature. A biometric signature is preferred by GSM operators and some banks in our country for transactions that do not require a wet-ink signature because it provides ease of use.

In this study, the eIDAS electronic signature levels will be examined and the biometric signature, which is a popular example, will be discussed. It is emphasized that the necessity of drawing the legal framework for the use of electronic signature types and the classification of electronic signature in order to provide interoperability.

1. Giriş

İmzanın sözlük anlamı "Bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret"tir (TDK, 2019). Islak imza ise "Kişinin kâğıt üzerine kalemle attığı imza" olarak tanımlanmaktadır (TDK, 2019). Türkiye'de resmi kurumlarla yürütülen işlemler başta olmak üzere günlük hayatta karşımıza çıkabilecek, neredeyse başvuru gerektiren her türlü işlemde ıslak imza kullanılmaktadır. Islak imzanın kullanıldığı alanlar aşağıdaki gibi özetlenebilir:

- Kamu kurumları ya da özel kuruluşlarla yapılan sözleşmeler, şartnameler, mutabakatlar, yazışmalar
- Talep ya da itiraz bildiren dilekçeler
- Tüm bankacılık işlemleri
- Mali belgeler, faturalar, raporlar
- Üniversite öğrenci işleri, personel işlemleri
- Operatör hat siparişi, teklif, onay gönderimleri (E-Güven, 2013).

Kısacası, imzacının kanıtlanmasını gerektirsin ya da gerektirmesin kişiyle ilişkilendirilen her türlü belgede ıslak imzanın kullanım alışkanlığı olarak zorunlu tutulduğu söylenebilir. 2004 yılında yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu ile birlikte ıslak imzaya alternatif olarak aynı yasal geçerliliğe sahip güvenli elektronik imza hayatımıza girmiştir. Kanunda (2004) e-imza, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmıştır (md.3/b). E-imzanın ıslak imzayla kanuni açıdan aynı hükmü taşıması için güvenli elektronik imza olarak oluşturulması gerekmektedir. Bunun için gerekli koşullar Kanunda (2004) aşağıdaki şekilde belirtilmiştir:

- Münhasıran imza sahibine bağlı olmalıdır.
- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmalıdır.
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamalıdır.
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamalıdır (md.4).

Bilindiği üzere 5070 sayılı Kanun, AB 1999/93/EC Direktifini temel almakta ve bu direktifte tanımlanan elektronik imza tanımı ile Kanundaki güvenli elektronik imza tanımı örtüşmektedir. Kanun neticesinde ülkemizde birçok kurum ve kuruluş iş süreçlerini elektronik ortama taşımış, başta e-devlet uygulamaları olmak üzere kamu projeleri, bankacılık işlemleri gibi pek çok alanda güvenli elektronik imza kullanımı yaygınlaşmıştır.

Avrupa Birliği (AB) üyesi ülkeler arasında elektronik ticaretin geliştirilmesini hedefleyen 1999/93/EC Direktifi, genel bir elektronik imza tanımı sunarak AB bünyesinde temel bir çatı çizmiş ancak üye ülkelerin kendi içinde yasal düzenlemeler yapmasını beklemiştir. Bu durum, her ülkenin elektronik imzanın hukuki ve teknik yönlerini kendi iç yasalarıyla belirlemesi gerektiği anlamına gelmektedir. Sonuç olarak uygulamada bir takım farklılıklar doğmuş ve 1999/93/EC Direktifinde yapılan bazı tanımlamaların ihtiyaca tam olarak cevap verememesi üzerine 2014 yılında eIDAS tüzüğü oluşturularak, 1999/93/EC Direktifinin yerini almıştır. eIDAS tüzüğünün ülkemizde henüz bir karşılığı bulunmamaktadır.

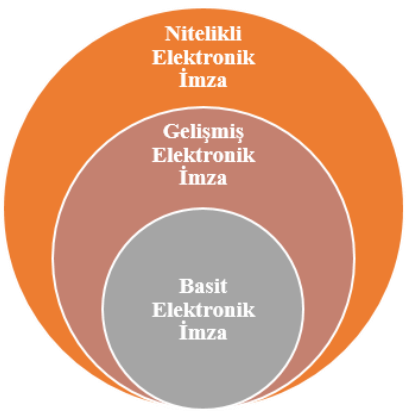
Ancak son zamanlarda kullanım kolaylığı sağlaması sebebiyle alternatif elektronik imza yaklaşımları görülmektedir. Bu çalışmada, ilk olarak eIDAS tüzüğünde tanımlanan elektronik imza seviyelerine değinilmiştir. Sonrasında bir elektronik imza alternatifi olarak karşımıza çıkan biyometrik imza incelenerek alternatif çözümlere yaklaşım üzerinde durulmuştur. Çalışmanın amacı, yaygınlaşan alternatif elektronik imza çözümlerinde ortak çalışabilirliğin sağlanabilmesi için elektronik işlemlerin güvenlik seviyelerinin belirlenmesinin ve farklı elektronik imza türlerinin kullanımı konusunda yasal düzenleme yapılmasının gerekliliğini vurgulamaktır.

2. eIDAS ve Elektronik İmza Seviyeleri

1999/93/EC Direktifi, AB üye ülkelerindeki elektronik imza çözümleri arasında birlikte çalışabilirliği sağlayamamış ve parçalanmış bir pazara yol açmıştır. Bu direktif, elektronik imzanın yasal etkilerini belirtse de herhangi bir AB üyesi ülkede oluşturulan elektronik imzanın diğer AB üyesi ülkede tanınacağını garanti altına almamıştır. Sonuç olarak, elektronik imzaların ve diğer güven hizmetlerinin kullanımını artırmak ve AB genelinde dijital tek bir pazarın oluşturulmasına katkıda bulunmak için 2014 yılında eIDAS tüzüğü kabul edilmiştir (eIDAS, 2014). O zamandan beri, eIDAS tüzüğü tüm AB üye ülkeleri için elektronik kimlikleri ve imzaları kabul etmek için tutarlı bir yasal çerçeve sağlayan standartlaştırılmış tek düzenlemedir. Böylelikle her ülkenin kendi içinde yasal bir düzenleme yapmaksızın tüzüğe göre hareket edebilmesi amaçlanmıştır.

5070 sayılı Kanun tarafından temel alınan 1999/93/EC Direktifinde güven hizmetleri elektronik imza ve zaman damgası ile sınırlıyken; eIDAS ile güven hizmetleri çeşitlendirilmiştir. Tüzüğün 26. maddesinde belirtildiği üzere teknolojik değişimin hızı nedeniyle, eIDAS'da inovasyona açık bir yaklaşım benimsenmiştir (eIDAS, 2014). Bir sonraki maddede "Bu tüzük teknolojiden bağımsız olmalıdır. Verdiği yasal etkiler, bu tüzüğün gerekliliklerinin yerine getirilmesi şartıyla herhangi bir teknik yolla sağlanmalıdır." ifadesi ile 26. madde desteklenmektedir (eIDAS, 2014). Sonrasında yürürlüğe giren Komisyon Uygulama Kararları ile güven hizmetlerine dair teknik detaylar genişletilmiştir. Örneğin; 2015/1506 sayılı Komisyon Uygulama Kararı ile gelişmiş elektronik imza ve formatları ile ilgili temel gereksinimler ayrıca belirlenmiş; hali hazırda geçerli olan Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute – ETSI) standartlarına referans verilmiştir (Commission Implementing Decision, 2015).

Elektronik imza türlerinin geniş bir tanımını sağlayan eIDAS tüzüğünde basit; gelişmiş ve nitelikli elektronik imza olmak üzere birbiri üzerine kurulan üç seviye imza tanımlanmıştır (Şekil 1). İmza seviyelerine dair detaylar alt başlıklarda açıklanmıştır.



Şekil 1. eIDAS Elektronik İmza Seviyeleri

2.1. Basit Elektronik İmza

eIDAS kapsamında tanımlanan basit elektronik imza, elektronik formlardaki diğer verilere ekli veya mantıksal olarak bağlı olan ve bir imzacı tarafından imzalamak amacıyla kullanılan elektronik formdaki verilerdir. Başka bir deyişle bir imzalayanın belgeye kabul veya onayının kanıtı olarak sunulabilecek elektronik biçimdir. Bu tanım, AB üyesi ülkelerde tüm elektronik imza türleri için geniş bir yasal kabul sağlamıştır. eIDAS'a (2014) göre basit elektronik imzanın sağlaması gereken koşullar aşağıda listelenmiştir:

- İmzalanan veri elektronik biçimde olmalıdır.
- İmza değeri elektronik veriye eklenmeli veya mantıksal olarak ilişkilendirmelidir.
- İmza değeri elektronik biçimde olmalıdır (böl.3 md.10).

eIDAS tüzüğünde basit elektronik imzaya ilişkin bu kriterler ötesinde bir açıklama bulunmamaktadır. Bu durumda basit elektronik imzanın yoruma ve teknolojik yeniliklere açık bırakıldığı söylenebilir. Örneğin, kağıt üzerine atılan ıslak imzanın taranmak suretiyle elektronik ortama aktarılarak elektronik belge içerisine eklenmesi, "Kabul ediyorum" butonuna tıklanması, PIN kodları, e-posta sonuna eklenen imzalar gibi belgenin içeriğini onaylama niyetini alan elektronik yöntemler basit elektronik imza olarak kabul edilebilir. Örneklerden anlaşılacağı üzere basit elektronik imza oluşturmak bir e-postanın altına ad-soyad yazmak kadar kolaydır.

eIDAS'a göre, elektronik imzaların sadece elektronik biçimde olması veya nitelikli elektronik imzanın gerekliliklerini karşılamaması sebebiyle yasal olarak kabulü reddedilemez (eIDAS, 2014, böl.25 md.1). Ancak bu, ıslak imza ile aynı yasal statüye sahip olduğu anlamına gelmez.

2.2. Gelişmiş Elektronik İmza

Gelişmiş elektronik imza, basit elektronik imzaya göre imzalayanın kimliğinin daha ayrıntılı doğrulanmasını gerektirir ve karşılaması gereken özel gereksinimler dolayısıyla daha yüksek düzeyde güvenlik sağlar (Kamu SM Beyaz Bülten, 2019). Basit elektronik imzaya ek olarak gelişmiş elektronik imzanın sağlaması gereken koşullar aşağıda listelenmiştir:

- İmza ile imzacı arasında eşsiz bir bağ olması zorunludur.
- İmzalayanı belirleme yeteneğine sahip olmalıdır.
- İmzacının kendi kontrolündeki imza oluşturma verileri kullanılarak oluşturulmalıdır.
- Veri değişikliklerini tespit edecek şekilde ilgili olduğu veriye bağlı olmalıdır (eIDAS, 2014, böl.26).

eIDAS'da yapılan bu tanım teknolojik olarak tarafsız bir şekilde formüle edilmiş olsa da, 2015/1506 sayılı Komisyon Uygulama Kararı ile CAdES, XAdES ve PAdES tipinde ve B (Temel), T (Zaman damgalı) veya LT (Uzun dönem doğrulama sağlayan) formatındaki imzaların kabulü zorunlu kılınmıştır (Commission Implementing Decision, 2015). Dolayısıyla bu seviyede çoğunlukla açık anahtar altyapısına dayanan elektronik imzalar kullanılmaktadır. Açık anahtar altyapısının kullanıldığı elektronik imzalama sistemlerinde, imza; imzalanan verinin özet değerini içeren ve imzacının özel anahtarı kullanılarak oluşturulan elektronik bir dosya formatı olarak karşımıza çıkar. İmza doğrulama ise imzacının açık anahtarı ile yapılır. Açık anahtarın imzacıya ait olduğu imzacıya ait kimlik bilgilerini içeren imzacıyla ilişkilendirilmiş elektronik sertifika ile kanıtlanır (Kamu SM Temel Kavramlar Sözlüğü, 2011) .

Gelişmiş elektronik imzanın, eIDAS'a göre yasal etkileri sağlamış olduğu özelliklerin kanıt oluşturabilecek yetkinlikte olması sebebiyle, basit elektronik imzadan üstün olsa da ıslak imzaya eşdeğer olabilecek düzeyde değildir. Bu özellikleri kanıt olarak kabul etmek ise adli makamların inisiyatifindedir.

2.3. Nitelikli Elektronik İmza

Nitelikli elektronik imza, eIDAS'a göre AB üye ülkelerinde özel bir yasal statüye sahip olan ve ıslak imzanın yasal karşılığı olan tek elektronik imza türüdür (eIDAS, 2014, böl.25 md.2). Gelişmiş elektronik imzanın sağlaması gereken tüm koşullara ek olarak imzacı sertifikasının akredite bir ESHS tarafından verilmesini ve nitelikli elektronik imza oluşturma aracı içerisinde tutulmasını zorunlu kılar.

Elektronik sertifikalar, kişinin elektronik ortamda kimliğini ispatlaması için kullanılan elektronik dosyalardır (Kamu SM Temel Kavramlar Sözlüğü, 2019). Elektronik sertifika, sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşır ve taşıdığı açık anahtar bilgisinin belirtilen kişiye ait olduğunu temin eder. Nitelikli elektronik imzanın oluşturulması için kullanılan nitelikli elektronik sertifikanın sağlaması gereken koşullar eIDAS Ek 1'de ayrıntılı olarak açıklanmıştır (eIDAS, 2014, ek 1).

İmzacıya ait nitelikli elektronik sertifika ve onunla kriptografik olarak ilişkili özel anahtar, elektronik imza oluşturma aracı içerisinde tutulur. Bu aracın güvenli olarak nitelendirilebilmesi için sağlaması gereken koşullar eIDAS Ek 2'de ayrıntılı olarak açıklanmıştır (eIDAS, 2014, ek 2).

Bu doğrultuda, 5070 sayılı Kanunda işaret edilen ve yasal olarak ıslak imzayla eşdeğer kabul edilen güvenli elektronik imzanın nitelikli elektronik imzaya karşılık geldiği görülmektedir. Kanunun "Güvenli Elektronik İmza ve Sertifika Hizmetleri" bölümünün 4. maddesinde belirtilen koşullar neticesinde, güvenli elektronik imza; tekillik, inkar edilemezlik, kimlik doğrulama ve veri bütünlüğü sağlar ve nitelikli elektronik sertifika (NES) ile oluşturulması zorunludur (Kanun, 2004).

3. Elektronik İmza Alternatifleri ve Biyometrik İmza

Teknolojideki değişiklikler ve gelişmelerle birlikte tüm dünyada alternatif elektronik imza çözümleri doğmuştur. eIDAS'a göre tüm elektronik imza türleri ulusal yasalarla belirli bir iş süreci için kısıtlama getirilmediği sürece mahkemede tarafların anlaşmasının kanıtı olarak kabul edilebilir (eIDAS, 2014, md.22). Belirli bir iş sürecinin ıslak imza, nitelikli elektronik imza veya gelişmiş elektronik imza kullanımıyla sınırlı olması durumu ülkenin medeni veya ticari hukukunda belirtilen usule ilişkin yükümlülükler çerçevesinde tanımlanmaktadır.

2016 yılında Akıllı Bilgi Yönetimi Derneği (The Association for Intelligent Information Management – AIIM) tarafından Avrupa'daki e-imzalarla ilgili yapılan bir araştırmada AB üyesi ülkelerin belirli süreçler çerçevesinde benimsediği gelişmiş elektronik imza kullanımına değinilmiştir. İtalya'da 2013 yılında "Gelişmiş Elektronik İmza için Teknik Düzenlemeler Kararnamesi"nin yayımlanmasıyla birlikte özellikle el yazısına dayalı gelişmiş biyometrik imzalar bazı alanlarda kullanılmaya başlanmıştır (AIIM, 2016). Benzer şekilde İspanya ve Slovakya'da tablet üzerine atılan biyometrik imzalar özellikle finans sektöründe yaygınlaşmıştır (AIIM, 2016).

Bazı ülkelerde ise yalnızca birkaç ticari işlem nitelikli elektronik imzalar uygulanırsa yasal olarak geçerli kabul edilmektedir. Bir tüketici kredisine başvurmak ya da bir kira sözleşmesi imzalamak Almanya, İsviçre ve Avusturya'da bu kısıtlamaya tabidir. Elektronik imzalamadan hariç tutulan bazı işlemler de bulunmaktadır. Almanya kanunları uyarınca iş akdinin feshi, evlilik, miras sözleşmeleri, borcun onaylanmasına ilişkin belgeler, ömür boyu tazminat taahhüdü, kefalet sözleşmesi bu sınıfa girmektedir (AIIM, 2016).

Bu kullanımlar göz önünde bulundurulduğunda ülkelerde eIDAS'da ıslak imzayla eş değer hükme sahip olmasa da yasal olarak geçerli sayılan basit ve gelişmiş elektronik imza türlerinin kullanımı için ek düzenlemeler getirildiği görülmektedir.

Ülkemizde ise elektronik imzayla ilgili 5070 sayılı Kanun haricinde yasal düzenleme bulunmamaktadır. Elektronik İmza Kanununda da, 1999/93/EC Direktifini temel alması sebebiyle eIDAS'da tanımlanan elektronik imza seviyelerinin karşılığı bulunmamaktadır. Ancak gelişen teknoloji doğrultusunda ülkemizde yasal bir karşılığı bulunmamasına rağmen bir takım elektronik imza alternatiflerinin var olduğu söylenebilir. Alternatiflere örnek olarak; elektronik ortamdaki sözleşmelerin "Onaylıyorum." butonuna tıklanarak kabul edilmesi, telefona mesaj olarak gelen onay koduyla kimlik doğrulanması veya onay alınması, özel kalemler aracılığıyla ıslak imzaya benzer şekilde tablet veya imza pedi üzerine atılan biyometrik imzalar verilebilir.

Bu alternatiflerden hem AB üyesi ülkelerde hem de ülkemizde son zamanlarda popülerleşen ve kullanım kolaylığı ile dikkat çeken biyometrik imzaya alt bölümlerde değinilmiştir.

3.1. Biyometrik İmza

Biyometrik imza, imza sahiplerinin belirli biyometrik verilerini kullanarak imzalarını özel bir tablet/ped üzerinde oluşturmaları ve genellikle bu verilerin imzalanan belgeye çözülemez biçimde bağlanmasıyla elde edilir (Kamu SM Beyaz Bülten, 2019). Burada bahsi geçen biyometrik veriler; ıslak imza ve el yazısı analizinde (grafoloji) de kullanılan imzanın kalem ile atılması sırasında ortaya çıkan imzacıyı ayırt etmeye yarayacak eğim, basınç, ivme ve hız gibi özelliklerdir (Kamu SM Beyaz Bülten, 2019). Biyometrik imza çözümlerinin uygulanması için imzacının biyometrik verilerini yakalayabilecek kabiliyete sahip özel bir cihaza bağlantı olması gereklidir. Bu cihazlar hem statik verileri (imzanın resmi gibi) hem de dinamik verileri (hızlanma, hız, eğim açısı, basınç vb.) yakalayabilir ve kaydedebilir. Sonuç olarak, hem statik hem de dinamik veriler elektronik belgede saklanır.

3.1.1. Biyometrik İmzanın Oluşturulması

Biyometrik imza çözümleri belirli bir standart çerçevesinde tanımlanmadığından farklı kurgusal özelliklere sahiptir. İmzalayan kişi elektronik bir cihaz üzerinde özel bir kalem kullanarak ıslak imzaya benzer şekilde imzalama işlemini gerçekleştirir. Bu aşamada, özel bir imza pedi/tableti üzerine özel imza kalemi kullanılarak oluşturulan el yazısı imzasından imzacıya ait biyometrik veriler elde edilir.

Kimi uygulamalar belge ile elektronik veri arasındaki bağlantıyı gösteren bir kanıt oluşturmak için belgenin özet değeri ile imzacıya ait biyometrik verileri birlikte şifreleyerek saklarken (Banca Finnat, 2019, s.21) ; kimi uygulamalar şifrelemeden önce zaman damgası bilgisi de ekleyerek imza zamanının tespit edilebilmesine olanak sağlar (Intel, 2019, s.8). Buradaki zaman damgası güvenilir bir üçüncü taraftan alınabilir veya uygulama tarafından sağlanabilir. Bazı yaklaşımlarda bunlara ek olarak biyometrik veri, imzanın resmi, imzalanan belgenin özeti, belgenin kendisi, imzacıya ait kimlik bilgileri gibi ayırt edici özellikler en son paket haline getirilir; kurum veya kuruluşa ait elektronik sertifika ile imzalanarak koruma altına alınır. Bu sertifikanın güvenilir taraftan alınması tercihe bağlıdır.

3.1.2. Biyometrik İmzanın Doğrulanması

İmza oluşturma tarafında farklı yaklaşımlar olduğu gibi imzanın doğrulanmasında da farklı yöntemler bulunmaktadır. Bazı uygulamalar kişiye ait biyometrik verileri kaydedip imza oluşturma sırasında karşılaştırma yöntemiyle anlık doğrulama gerçekleştirmektedir. Bu yöntem biyometrik sensör tarafından toplanan verilerin depolanan önceki verilerle karşılaştırılmasına dayanır. Tanımlama sürecinde ise biyometrik sensör tarafından toplanan veriler, veri tabanında bulunan çeşitli müşterilerin biyometrik verileriyle karşılaştırılmaktadır (Banca Finnat, 2019, s.15).

Sistem, bir müşterinin biyometrik örneğini özel bir yazılım kullanarak, daha önce elektronik belge imzalama aşamasında saklanan verilerle karşılaştırılabilir durumda tutar. Karşılaştırma sonucu, daha önce kaydedilen ve kullanıcıyla ilişkilendirilmiş benzersiz bir tanımlama koduyla indekslenen kişinin biyometrik verileri arasındaki eşleştirme puanına dayanarak doğru veya yanlış olacaktır. Bir diğer yaklaşımda ise anlık doğrulama yapılmaksızın yalnızca ihtilaf durumunda belgenin imzası dava sırasında toplanacak imzalarla karşılaştırılır.

3.2. Biyometrik ve Nitelikli Elektronik İmza Karşılaştırması

Biyometrik imzanın oluşturulması ve doğrulanmasındaki farklı yaklaşımlar göz önünde bulundurulduğunda en iyi yeteneklere ve güvenlik düzeyine sahip cihaz ile oluşturulmuş biyometrik imzanın ancak gelişmiş elektronik imzaya karşılık gelebileceği görülmektedir. Bu durumda dahi biyometrik imza, ıslak imza ile eşdeğer olan nitelikli elektronik imza gereksinimlerini nitelikli elektronik imzanın tanımı gereği karşılamaz. Nitelikli elektronik imza ile biyometrik imzanın sahip olduğu özellikler alt bölümlerde karşılaştırmalı olarak incelenmiştir.

3.2.1. Islak İmzaya Denklik

5070 sayılı Kanuna göre ıslak imza ile eşdeğer olan tek elektronik imza türü nitelikli elektronik imzadır. eIDAS tüzüğüne göre biyometrik imza yasal olarak geçerli olmasına rağmen ıslak imzayla denk sayılmamaktadır.

3.2.2. Veri Bütünlüğü

Nitelikli elektronik imza, açık anahtarlı kriptografiye dayandığı için imzalı veride yapılacak herhangi bir değişiklik imzanın bozulmasına sebep olur. Nitelikli elektronik imza içerisinde imzalanan belgenin özet değeri yer almaktadır. Bu sayede imzanın imzalanan belgeyle ilişkisi koruma altına alınır. Bazı biyometrik imza uygulamaları imzalanan belgenin özet değeriyle biyometrik veriyi şifreleyerek paket halinde tutma kabiliyetine sahiptir. Ancak bu kabiliyetten yoksun uygulamalar için biyometrik imzanın oluşturulduğu cihazda imzacıya gösterilen belgenin imzalandığı garanti edilemez. Ayrıca şifreleme yapılmadığında imzalı veri üzerinde sonradan değişiklik yapılabilir.

3.2.3. İmza Oluşturma Güvenliği

Açık anahtarlı kriptografide kullanılan özel anahtar sadece sahibi tarafından kullanılabilir. Herkesin erişimine ve kullanımına açık olan açık anahtarla matematiksel bağlantısı vardır. İmza doğrulama verisiyle (açık anahtar) matematiksel olarak ilişkilendirilmiş imza oluşturma verisi (özel anahtar), güvenli elektronik imza oluşturma aracı içerisinde tutulmaktadır (Kanun 2004, md.6) . Özel anahtara yalnızca imzacı tarafından PIN ile giriş yaparak erişilmektedir. Biyometrik imzada ise kişilere ait "özel anahtar" niteliğinde olan biyometrik veriler imza tableti/pedi tarafından imzacının tanınması veya imzanın doğrulanması amacıyla kaydedilmektedir. Bu durum imza oluşturma verisini güvenlik zafiyetlerine karşı açık hale getirmektedir.

3.2.4. İmza Doğrulama Güvenliği

Nitelikli elektronik imzanın doğrulaması anlık olarak yapılmaktadır. İmza doğrulama verilerine nitelikli elektronik imza içerisinden veya ESHS aracılığıyla erişilebilir. Biyometrik imzada ise anlık ve itilaf durumunda doğrulama olmak üzere iki farklı yaklaşım söz konusudur. İtilaf olması durumunda imzacının imzasıyla mevcut imzanın kıyaslanması yordamıyla imza doğrulama yapılabilir. Bazı uygulamalar ise imzacının biyometrik verilerini önceden alarak sistemlerinde saklar. Böylelikle aynı kullanıcının farklı zamanlarda oluşturduğu imzaları her defasında önceki örneklerle kıyaslayarak imzacı ile imza arasında eşleştirme sağlar ve oluşturulan imzaları anlık doğrulayabilir. Ancak imza oluşturma verisinin güvenliğinin tehlikeye girmesi durumunda biyometrik imzanın imzacıyla olan bağlantısı da riske girecektir.

3.2.5. Ortak Çalışabilirlik

Nitelikli elektronik imza formatları uluslararası standartlar ile belirlenmektedir. ETSI'ye bağlı hizmet veren Elektronik İmza Altyapıları Birimi (Electronic Signatures and Infrastructures - ESI) Avrupa Birliği üye ülkeler kapsamında elektronik imza standartlarını belirlemektedir. Bu standartlarda farklı kullanım alanlarının ihtiyacını karşılayacak imza tipleri belirlenmiştir. Ülkemizde de elektronik imza standardı olarak ETSI tarafından hazırlanan CMS tabanlı CAdES, XML'e özgü XAdES ve PDF'e gömülü imza oluşturmaya imkan veren PAdES imza standartları kullanılmaktadır (Telekomünikasyon Kurulu Kararı, 2006). Uluslararası standartlarda imzanın uzun dönemli korunması için arşivleme mekanizmaları dahi tanımlanmaktadır. Böylece ortak çalışabilirlik mümkündür, bir standarda göre atılan imza o standardı temel alan her yerde doğrulanabilir. Buna karşın; biyometrik imzanın oluşturulmasıyla ilgili herhangi bir standart bulunmamaktadır. Biyometrik verilerin yakalanmasıyla ilgili uluslararası standartlar mevcut olsa da imza oluşturma esnasında kullanılan cihaza bağlı olarak biyometrik verinin doğrulanmasında farklılıklar oluşabilir. İmzanın uzun dönemli korunması da garanti edilemez.

3.2.6. Kullanım Kolaylığı

Nitelikli elektronik imza oluşturma işlemi öncesinde imzacının nitelikli bir ESHS'den nitelikli elektronik sertifika temin etmesi gerekmektedir. Ayrıca imza oluşturma işlemi için güvenli elektronik imza oluşturma aracı kullanımı zorunludur. Bu durum imzacı için hem sertifika ve imza oluşturma cihazı alımı sırasında ek maliyet anlamına gelmekte hem de bu cihazların ortam bağımlılığı aksaklıklara sebebiyet verebilmektedir.

Biyometrik imza oluşturma işlemi ıslak imzaya benzer şekilde gerçekleştirildiğinden kullanım kolaylığı sağlamaktadır. Tablet veya imza pedi gibi biyometrik verileri yakalama kabiliyetine sahip cihaz kurum/kuruluş tarafından temin edilir ve kullanıcı ıslak imzaya benzer şekilde hiçbir ek maliyet gerektirmeden imzalama işlemi gerçekleştirilebilmektedir.

3.2.7. Diğer Durumlar

Nitelikli elektronik imza değeri, imzalanan her belge için eşsizdir. İmzalanan belge içerisinden elde edilen imza değerinin başka bir belgeye iliştirilerek kullanılması söz konusu değildir. Biyometrik veri ele geçirildiği durumda herhangi bir belgeye iliştirilerek tekrar kullanılabilmesi mümkündür.

Nitelikli elektronik imza oluşturulduğu andan itibaren kriptografik olarak korunduğu için aktarım sırasında ek güvenlik önlemi gerekmemektedir. Kullanılan imza tabletinin kabiliyetine göre oluşturulan biyometrik imzanın başka bir ortama aktarılması gerekebilir. İmzanın aktarımı sırasında biyometrik verinin ek güvenlik önlemleriyle korunması gerekmektedir.

3. Sonuç ve Öneriler

Çalışma kapsamında eIDAS tüzüğünde tanımlanan elektronik imza seviyelerine değinilmiş; bu seviyelerin AB üyesi ülkelerde kullanım alanları incelenmiştir. Ülkemizde yasal olarak karşılığı bulunmamasına rağmen farklı seviyedeki elektronik imza kullanımının yaygınlaştığına dikkat çekilmiştir. Biyometrik imza örneğinden yola çıkılarak elektronik imza alternatiflerinin seviyesinin belirlenebileceği üzerinde durulmuştur.

Ülkemizde, telekomünikasyon, sağlık, bilişim ve finans sektöründeki iş süreçlerinin büyük çoğunluğu hangi imza türünün kullanılabileceği konusunda herhangi bir kısıtlamaya tabi değildir. Çoğu durumda belgeye olan güven seviyesinin seçimini yapmak kuruluşun kendi görevidir. Hem ıslak imzanın hem güvenli elektronik imzanın gerçekleştirilen işlemin seviyesine bakılmaksızın yer edinmiş bir alışkanlık olduğu görülmektedir. Bu durumun gerekliliği sorgulanmalı; alternatif elektronik imza yaklaşımlarının yaygınlaşması da göz önünde bulundurularak işlem seviyesine göre kullanılan imza türünün sınıflandırılabilmesinin önü açılmalıdır. Yapılacak işlemin seviyesine göre imza seviyesi belirlemek; her kurumun kendi özelinde, kurumun hizmet verdiği sektörün otoritelerince ya da en üst düzeyde kanun ve yönetmeliklerle belirlenebilir. Elektronik imzalamanın odağı yalnızca ıslak imzanın yerini almak gibi düşünülmemeli ve mümkün olan iş akışlarında dahil edilmelidir. Elektronik imzaların neden, nasıl ve ne zaman kullanılması gerektiğine ve bu girişimi desteklemek için hangi teknolojilerin kullanılacağına dair kurallar belirlenmelidir. Alternatif elektronik imza türlerinin kullanımına izin verilirken, ortak çalışabilirliği sağlamak adına, ilgili imza türünün uluslararası otoritelerce onaylanmış standarda sahip olmasına da dikkat edilmelidir.

Kaynakça

2006/DK-77/353 sayılı Telekomünikasyon Kurulu Kararı. (2006).

5070 sayılı Elektronik İmza Kanunu. (2004). *Resmi Gazete*, Sayı:25355, 23 Ocak 2004.

Banca Finnat. (2016). Advanced Electronic Signature Solution Graphometric Signature on Bank Forms. Erişim Adresi: https://www.bancafinnat.it/assets/documenti/pdf/advanced_electronic_signature_bfe.pdf

Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 Laying Down Specifications Relating to Formats of Advanced Electronic Signatures and Advanced Seals To Be Recognised by Public Sector Bodies Pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 tf the European Parliament and of the Council On Electronic Identification And Trust Services For Electronic Transactions in the Internal Market. (2015).

E-Güven. (2013). E-İmza Kullanım Alışkanlıkları Araştırması. Erişim Adresi: http://e-guven.com/Documents/EGUVEN_Eimza_Kullanim_Aliskanliklari_Arastirmasi.pdf

Intel. (2019). Biometric Signature Solution Guide for Financial Sector. Erişim Adresi: https://www.intel.com/content/dam/www/public/us/en/documents/case-studies/biometric-signature-for-financial-sector-solution-brief.pdf

Kamu Sertifikasyon Merkezi (Kamu SM). (2019). Biyometrik İmza ve Nitelikli Elektronik İmza Karşılaştırması Beyaz Bülteni. Erişim Adresi: http://www.kamusm.gov.tr/dosyalar/beyazbulten/Biyometrik_Imza_ve_Nitelikli_Elektronik_Imza_Karsilastirmasi_Whitepaper.pdf

Kamu SM. (2011). Temel Kavramlar Sözlüğü. Erişim Adresi: http://www.kamusm.gov.tr/dokumanlar/belgeler/kitaplar/temel_kavramlar.jsp

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market And Repealing Directive 1999/93/EC (eIDAS). (2014).

The Association for Intelligent Information Management (AIIM). (2016). E-Signatures in Europe: Understanding the legal requirements for proof of intent. Erişim Adresi: https://www.project-consult.de/files/AIIM_eSignatures_2016.pdf

Türk Dil Kurumu Sözlükleri. (2019). Erişim Adresi: https://sozluk.gov.tr/