



Bilgi Yönetimi Dergisi

Cilt: 7 Sayı: 1 Yıl: 2024

<https://dergipark.org.tr/tr/pub/by>



Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 25.04.2024

Kabul tarihi: 21.05.2024

Yayınlanma tarihi: 30.06.2024

Article Info

Date submitted: 25.04.2024

Date accepted: 21.05.2024

Date published: 30.06.2024

Anahtar Sözcükler

*Elektronik İmza Standartları,
Dijital Dönüşüm, Avrupa
Birliği*

Keywords

*Electronic Signature
Standards, Digital
Transformation, European
Union*

DOI numarası

10.33721/by.1473545

ORCID

0000-0002-8353-6075 (1)

0000-0002-9015-2790 (2)

0000-0003-0755-1289 (3)

0009-0005-8091-6346 (4)

0009-0005-9062-3758 (5)



Elektronik İmza Standartlarındaki Güncellemeler ve Türkiye'deki Mevcut Durum

*Enhancements in Electronic Signature Standards and the
Current Situation in Türkiye*

Meltem SEYİRT

TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi,
meltem.seyirt@tubitak.gov.tr

Tuğba ÖZCAN

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

Bergen KARABULUT

TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi,
bergen.karabulut@tubitak.gov.tr

Süleyman Mete DOĞAN

TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi,
mete.dogan@tubitak.gov.tr

Emame AKMAN HARMANCI

TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi,
emame.harmanci@tubitak.gov.tr

Öz

Gelişen teknoloji, işlemlerin dijital ortamda gerçekleştirilmesini artırarak elektronik imza kullanımını yaygınlaştırmıştır. Elektronik imza kullanımının, etkinliğinin ve ortak çalışabilirliğinin sağlanması adına birbiri ile konuşabilen sistemlerin oluşturulması gerekliliği kaçınılmazdır. Sistemler arasındaki etkileşimi sağlayabilmek ve ortak bir dil oluşturabilmek için de ortak standartların benimsenmesi gerekmektedir. Uyumu sağlamak amacıyla başvuru standartlar teknolojik gelişmelerden etkilenmekte ve mevcut ihtiyaçların karşılanması için değişime uğramaktadır. Bu sebeple, elektronik imza kullanımının getirilerinden tam anlamıyla yararlanabilmek için güncel standartların yakından takip edilmesi ve bu standartlara uyum sağlanması gerekmektedir. Türkiye'de yaşanan dijital dönüşüm sürecinde elektronik imza kritik bir rol üstlenmektedir. Bu nedenle, elektronik imza teknolojisi alanındaki değişim ve gelişmelerin izlenmesi gün geçtikçe daha fazla önem kazanmaktadır. Bu bağlamda, Türkiye'de kullanımda olan standartların güncellenmesi, güvenilirliğin ve küresel düzeyde uyumluluğun sağlanması için stratejik bir adım olarak değerlendirilmelidir. Bu çalışma, elektronik imza standartlarının gelişiminin incelenerek yapılan güncellemelerin belirlenmesi amacıyla gerçekleştirilmiştir. İnceleme kapsamında, öncelikle elektronik imza standartlarının gelişimi değerlendirilmiştir. Bu gelişim sonucunda ortaya çıkan güncel standartlar ile Türkiye'de kullanımda olan standartlar arasındaki farklar belirlenmiştir. Buna ek olarak, Türkiye'de elektronik imza ile ilgili mevzuat ve mevzuat destekli elektronik imza kullanım alanları ele alınmıştır. Elektronik imzanın Türkiye'deki mevcut kullanım alanlarında güncel elektronik imza standartlarına uyumluluğun sağlanması için bir dizi geçiş adımı belirlenerek entegrasyon süreci için genel bir çerçeve sunulmuştur. Yapılan çalışma, elektronik imza standartlarında gerçekleştirilen güncellemeleri ele alması yönüyle, gelecekte Türkiye'de güncel standartlara uyumluluk sürecinin şekillenmesine önemli katkı sağlayacak niteliktedir.

Abstract

The advancement of technology has increasingly facilitated the conduct of transactions in digital environments, thus popularizing the use of electronic signatures. It is inevitable to establish systems that can communicate with each other to ensure the effectiveness and interoperability of electronic signature usage. Adopting common standards is necessary to facilitate interaction between systems and to establish a common language. Standards applied to ensure compatibility are influenced by technological advancements and undergo changes to meet current needs. Therefore, to fully benefit from the advantages of electronic signature usage, it is necessary to closely monitor current standards and ensure compliance with them. In the digital transformation process in Türkiye, electronic signatures play a critical role. Consequently, monitoring changes and developments in electronic signature technology in Türkiye is becoming increasingly important day by day. In this context, updating the standards in use in Türkiye should be considered a strategic step to ensure trustworthiness and global compatibility. This study aims to examine the development of electronic signature standards and determine the enhancements made. Within the scope of the study, firstly, the development of electronic signature standards was evaluated. The differences between the current standards resulting from this evolution and the standards in use in Türkiye were identified. In addition, the legislation related to electronic signatures in Türkiye and the areas of use supported by legislation were discussed. A series of transition steps were determined to ensure compliance with current electronic signature standards in the existing usage areas of electronic signatures in Türkiye and a general framework for the integration process was presented. The study, by addressing the enhancements in electronic signature standards, is expected to make a significant contribution to shaping the compliance process with current standards in Türkiye in the future.

1. Giriş

1999 yılında Avrupa Birliği (AB), elektronik imzalara ilişkin ilk çerçeveyi sağlayan 1999/93/EC sayılı Elektronik İmza Direktifini yayımladı. Avrupa Birliği (AB) iç pazarının düzgün işleyişini sağlamak amacıyla elektronik imzalara ve belirli sertifika hizmetlerine yönelik yasal bir çerçeve oluşturan bu direktif, elektronik imzaların kullanımını kolaylaştırmayı ve yasal olarak tanınmasına katkıda bulunmayı amaçlamıştır (European Parliament and Council, 1999). Ancak bu direktif, elektronik işlemler için kapsamlı bir sınır ötesi ve sektörler arası çerçeve sunmadan elektronik imzayı ele almıştır (European Parliament and Council, 2014). Kapsamının sınırlı olması ve yalnızca bir direktif niteliğinde olması, her AB Üye Devletinin bu direktifi ulusal hukukuna farklı şekillerde aktarmasına imkân tanımıştır (ENISA, 2023). Direktifin getirdiği uyumlaştırma yeterli olmamış ve farklı AB Üyesi Devletlerdeki elektronik imza çözümleri arasında birlikte çalışabilirlik eksikliğine ve sonuç olarak parçalanmış bir pazara yol açmıştır (Adobe, 2016).

AB dijital pazarı için büyük bir gelişme, “eIDAS Tüzüğü (eIDAS Regulation)” olarak bilinen (Federal Office for Information Security, 2023) 910/2014 (AB) tüzüğünün yayımlanması ile olmuştur. eIDAS Tüzüğü, 17 Eylül 2014 tarihinde yürürlüğe girmiş olup aynı zamanda Elektronik İmza Direktifinin yürürlükten kaldırıldığı 1 Temmuz 2016 tarihinde tam olarak uygulanabilir hâle gelmiştir (European Parliament and Council, 2014). Bu tüzük, tüm üye devletlerde doğrudan uygulanabilir olmasının yanı sıra yalnızca elektronik imzaları değil, geniş bir dijital imza yelpazesini kapsamaktadır (ENISA, 2023). Bu tüzük ile güven hizmetleri; elektronik imza, elektronik mühür, elektronik zaman damgaları, elektronik kayıtlı teslimat hizmetleri ve web sitesi kimlik doğrulamasını destekleyen güven hizmetleri şeklinde genişletilmiştir. Bu tür hizmetlere güvenen veya bunları sağlayan tüm taraflar için ortak bir yasal çerçeve sağladığı için eIDAS tüzüğü dijital tek pazar oluşturmada ileriye doğru atılmış büyük bir adımı temsil etmektedir (ENISA, 2016).

Avrupa Komisyonu, eIDAS Tüzüğü'nün zayıf yönlerini gidermek amacıyla Haziran 2021'de eIDAS Tüzüğü'nün revizyonuna yönelik bir teklif yayımlamıştır. eIDAS 2.0 olarak da bilinen bu teklif (European Parliament and Council, 2021), mevcut düzenleyici çerçevenin eksikliklerini gidermeyi ve faydalarını özel sektördeki daha geniş bir kullanım alanına genişletmeyi amaçlamaktadır. Mevcut eIDAS çerçevesi üye devletlerin gönüllü iş birliğine dayanırken, yeni teklif her üye devletin bir dijital kimlik çözümü sunmasını ve bilgilendirmesini gerektirmektedir (Busch, 2022). eIDAS 2.0'daki temel değişiklikler elektronik kimlik tanımlamayla ilgilidir. Güven hizmetlerine ilişkin olarak, elektronik kimlik belirlemeyle ilgili yalnızca bazı ek hizmetler eklenmiş ve bazı mantıksal boşluklar kapatılmıştır (Schwalm, 2023).

Avrupa Birliği mevzuat düzenlemelerinin sunduğu çerçeve ve referans alınan standartlar, elektronik imza konseptini daha detaylı anlamak için bir zemin oluşturmuştur. Bu temel üzerine inşa edilen elektronik imza kavramı, elektronik formdaki diğer verilere eklenen veya bunlarla mantıksal olarak ilişkilendirilen ve imza sahibi tarafından imzalamak için kullanılan elektronik formdaki veriler olarak tanımlanmaktadır (European Parliament and Council, 2014a). eIDAS Tüzüğü farklı güven seviyelerinde üç tür elektronik imza ayırımı yapmaktadır: (basit) elektronik imza, gelişmiş elektronik imza ve nitelikli elektronik imza (Niestadt, 2022). Elektronik imzaların Avrupa'nın herhangi bir yerinde oluşturulabilmesi ve doğrulanabilmesini sağlamak için eIDAS Tüzüğü, 2015/1506/EU sayılı uygulama kararı (European Parliament and Council, 2015) aracılığıyla bir dizi temel profil tanımlamıştır (European Commission, 2023). Bu uygulama kararı ile gelişmiş elektronik imzaya veya nitelikli sertifikaya dayalı gelişmiş elektronik imzaya ihtiyaç duyan üye devletler için en yaygın imza formatları olarak belirlenen CMS, XML ve PDF gelişmiş elektronik imzanın tanınması zorunlu kılınmış ve bu imzaların uyması gereken Avrupa Telekomünikasyon Standartlar Komitesi (European Telecommunications Standards Institute, ETSI) Teknik Özellikleri (Technical Specification, TS) belirlenmiştir (European Parliament and Council, 2014b).

Avrupa yasal çerçevesi, Avrupa standart kuruluşlarının hem kamu hem de özel sektörün ihtiyaçlarını karşılarken, küresel standartlarla (mevcut olduklarında) birlikte çalışabilirliği mümkün olduğu kadar korumaları için sürekli bir zorunluluk oluşturmaktadır. Elektronik İmza Direktifinin yürürlüğe girmesinden bu yana, dijital imzalara ve ilgili güven hizmetlerine ilişkin standartlar, ETSI Teknik Komitesi "Elektronik İmzalar ve Altyapılar" (ETSI Technical Committee "Electronic Signatures and Infrastructures", ETSI TC ESI) tarafından geliştirilmektedir (ENISA, 2019). ETSI, Elektronik İmzalar ve Altyapılar Teknik Komitesi, dijital imza formatlarının ve bunların oluşturulması ve doğrulanmasına ilişkin prosedür ve politikaları koordine etmektedir (Niestadt, 2022). ETSI teknik özellikleri, belgenin teknik gereklilikler içerdiği ve hızlı bir şekilde kullanıma hazır olmasının önemli olduğu durumlarda kullanılırken Avrupa standartları belgenin Avrupa'ya özgü ihtiyaçları karşılaması amaçlandığı ve ulusal standartlara aktarılması gerektiğinde kullanılmaktadır (ETSI, 2020). Ayrıca Avrupa Standartları, teknik özelliklere kıyasla genellikle daha uzun sürede onaylanmaktadır (ETSI, 2013a). ETSI gelişmiş elektronik imza için teknik özellikleri yayımlamasından birkaç yıl sonra, eIDAS tüzüğü gerekliliklerine dayanarak bir dizi Avrupa Standardı (European Standards, ENs) yayımlamıştır (ENISA, 2019). Bu standartlarda CADES (CMS Advanced Electronic Signature)/XAdES (XML Advanced Electronic Signature)/PADES (PDF Advanced Electronic Signature)/ASiC ETSI Plugtests™ (ETSI Plugtests Interop Events, 2024) etkinlikleri sırasında paydaşlardan alınan geri bildirimlerde belirtilen konular da göz önünde bulundurulmuştur. Standartların birlikte çalışabilirliği ve güvenliği sağlarken, maliyetleri azaltma ve şirketlerin değer zincirine ve ticarete entegrasyonunu kolaylaştırma gibi yararları (European Commission, 2024) dikkate alındığında ETSI tarafından eIDAS Tüzüğü temel alınarak geliştirilen Avrupa Standartlarının oldukça önem taşıdığı görülmektedir.

Bu çalışmada; CMS, XML ve PDF tabanlı gelişmiş elektronik imzalar özelinde ETSI standartlarında yapılan güncellemeler ele alınmaktadır. Her bir imza türü için eIDAS kapsamında tanımlanan standartlara ve bu standartların güncellenme durumlarına değinilmektedir. İlgili standartlarda güncellenen kısımlar ve değişen özelliklere dair incelemeler yapılarak, Türkiye'deki elektronik imza mevzuatı çerçevesinde kullanılan elektronik imza standartları ve güncel elektronik imza standartları karşılaştırmalı olarak incelenmiştir. Bu çalışma ile yaygın kullanılan gelişmiş elektronik imza türleri için kullanılan standartların eIDAS kapsamında güncellenmesi ve Türkiye'ye yansımaları hakkında genel bir bakış sağlanmaktadır.

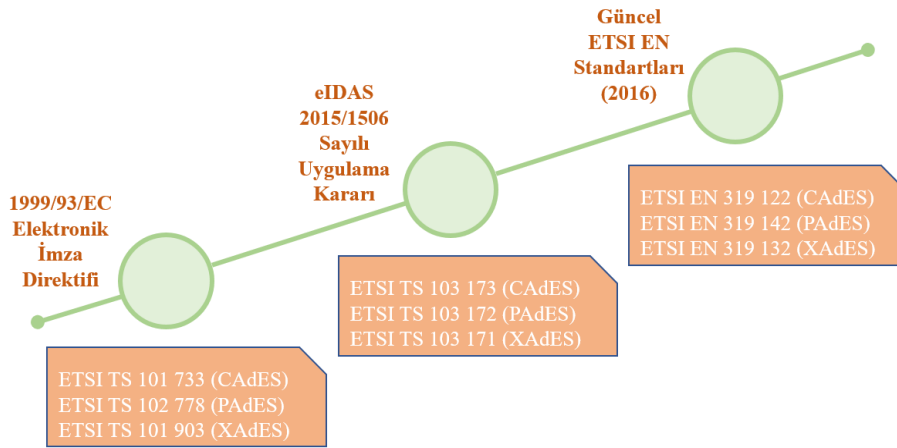
2. Elektronik İmza Standartlarının Gelişimi

Elektronik imzanın hukuki düzenlemelerle ve yasalarla garanti altına alınması, belgelerin dijital ortamda kullanımına geçişi önemli ölçüde kolaylaştıran bir gelişmedir. Yasal çerçevesi oluşturulan elektronik imzanın kullanımında istenen başarının yakalanması için büyük ölçüde birlikte çalışabilirliği sağlayacak ortak bir formatın üretilmesi ve kullanıcılar tarafından kabul edilmesi gerekliliği de aşıkardır. Bu doğrultuda elektronik imzanın uygulamaya konulması ve kullanımının yaygınlaştırılması sürecinde dünyada ve ülkemizde başlatılan faaliyetler ile ya mevzuatlarda düzenleme yapılmış ya da yeni bazı yasal düzenlemelere gidilmiştir (Biçkin, 2006).

Elektronik imza alanında 1999/93/EC sayılı Elektronik İmza Direktifi ile atılan temel çerçeve, 2014 eIDAS Tüzüğü ile oldukça genişletilerek elektronik güven hizmetleri çeşitlendirilmiş ve dijital tek pazar oluşturma yönünde önemli gelişmeler sağlanmıştır. eIDAS Tüzüğü'nün eksikliklerin giderilmesi için de günümüzde eIDAS 2.0 başlığında çalışmaların devam ettiği görülmektedir. Belirtilen gelişim sürecinde elektronik imza için kullanılan standartlar da çeşitli geliştirmelere ve güncellemelere uğramıştır. Yaygın kullanılan elektronik imza türleri için standartların değişim/gelişim sürecinin dönüm noktaları Şekil 1'de verilmiştir. Elektronik İmza Direktifinin yürürlüğe girmesi ile başlayan bu süreçte dijital imzalar ve ilgili güven hizmetlerine ilişkin standartlarda yapılan değişiklik ve iyileştirmeler ETSI TC ESI tarafından gerçekleştirilmektedir.

Şekil 1

Elektronik İmza Standartlarının Gelişimi



2.1. Elektronik İmza Direktifi ve İlk ETSI Teknik Özellikler Serisi

1999 yılında yayımlanan Elektronik İmza Direktifinin (1999/93/EC) kabul edilmesine paralel olarak elektronik imza tabanlı çözümlerin kullanımını ve birlikte çalışabilirliğini kolaylaştırmak amacıyla, Avrupa Elektronik İmza Standardizasyon Girişimi (Electronic Exchange of Social Security Information, EESSI), elektronik imza ürünleri ve hizmetleri için bir dizi standart geliştirme amacıyla Avrupa standardizasyon kuruluşları olan Avrupa Standartlar Komitesi (European Committee for Standardization, CEN) ve ETSI'yi koordine etmek üzere kurulmuştur (ETSI, 2016). Elektronik imza ürünleri için genel kabul görmüş standartlara ilişkin 2003/511/EC sayılı Komisyon Kararı (European Parliament and Council, 2003), EESSI'nin sonuçlarını takiben komisyon tarafından kabul edilmiştir. Bu karar, direktifin 3. maddesinin 5. fıkrasına uygun olarak elektronik imza ürünleri için "genel kabul görmüş standartlar" yayımlayarak elektronik imza kullanımını teşvik etmeyi amaçlamıştır. Bu kapsamda XML, CMS ve PDF tabanlı elektronik imzalar için CAeS, XAdES ve PAeS gelişmiş elektronik imza formatlarının tanımlandığı ETSI standartları kabul edilmiştir (ENISA, 2019) (Tablo 1).

Tablo 1

İlk ETSI Teknik Özellikler Serisi

İmza Tipi	Standart
CMS Gelişmiş Elektronik İmzalar (CAeS)	ETSI TS 101 733 (ETSI, 2013b)
XML Gelişmiş Elektronik İmzalar (XAeS)	ETSI TS 101 903 (ETSI, 2010)
PDF Gelişmiş Elektronik İmza (PAeS)	ETSI TS 101 778 (ETSI, 2009a)

Tablo 1’de belirtilen standartlarda, CMS, XML ve PDF tabanlı gelişmiş elektronik imzaların tanımları sunulmuştur:

- CMS Gelişmiş Elektronik İmzalar (CAAdES): IETF RFC 5652 "Kriptografik Mesaj Sözdizimi (Cryptographic Message Syntax, CMS)" üzerine inşa edilen CAAdES imza yapısı, özellikleri ve formatlarını belirler.
- XML Gelişmiş Elektronik İmzalar (XAdES): "XML İmza Sözdizimi ve İşleme (XMLDSig)" üzerine inşa edilen XAdES imza yapısı, özellikleri ve formatlarını belirler.
- PDF Gelişmiş Elektronik İmza (PAdES): PDF tabanlı olarak oluşturulan ve imzanın ayrı bir veri olarak oluşturulması yerine PDF dosyasının içerisine gömülmesine izin veren PAdES imza yapısı, özellikleri ve formatlarını belirler.

2.2. 2015/1506 Uygulama Kararı ve İkinci Teknik Özellikler Serisi

Elektronik İmza Direktifi ile birlikte geliştirilen ilk imza standartlarında; her imza formatı için tanımlanan çok sayıda farklı imza biçimi ve seviyesi bulunmakta, tanımlanan imza seviyelerine ilişkin asgari gereksinimler net olarak belirtilmemektedir. Bu sebeple, imzaların oluşturulması, doğrulanması ve uzun dönemli saklanması gibi işlemlerde farklı yorumlamalara sebep olan ve ortak çalışabilirliği olumsuz yönde etkileyen çeşitli teknik zorlukların ortaya çıktığı görülmüştür (ENISA, 2019).

eIDAS Tüzüğü ile ilgili yapılan çalışmalar kapsamında direktif ile kabul edilen standartlarda tespit edilen sorunlar yeniden değerlendirilerek yine ETSI tarafından yaygın olarak kullanılan imzalar için ikinci teknik özellikler serisi yayımlanmıştır. 2015/1506 sayılı uygulama kararı (European Parliament and Council, 2015) ile kabul edilen yeni imza standartlarında bir önceki standartlarda bulunmayan bir dizi imzalı ve imzasız özellik tanımlanarak imza içeriğindeki değişikliklere paralel şekilde temel imza profilleri tanımlanmıştır. Yayımlanan standartlar Tablo 2’de belirtilmiştir.

Tablo 2

İkinci ETSI Teknik Özellikler Serisi

İmza Tipi	Standart
CMS Gelişmiş Elektronik İmzalar (CAAdES)	ETSI TS 103 173 (ETSI, 2012a)
XML Gelişmiş Elektronik İmzalar (XAdES)	ETSI TS 103 171 (ETSI, 2012b)
PDF Gelişmiş Elektronik İmza (PAdES)	ETSI TS 103 172 (ETSI, 2013c)

2.3. Güncel Avrupa Standartları Serisi

2015/1506 sayılı uygulama kararının yayımlanmasından sonra ETSI ESI, birtakım güncellemeler, paydaşlar tarafından yapılan derin incelemeler ve açık şekilde gerçekleştirilen birlikte çalışabilirlik testlerinden sonra gelişmiş elektronik imza standartları ailesini tanımlayan ve Avrupa Birliği üye ülkelerinin ulusal standardizasyon kuruluşları tarafından onaylanan bir dizi Avrupa Standardı (EN) yayımlamıştır (Ibarz, 2020). Yayımlanan güncel standartlar hâlen yürürlükte olan 2015/1506 sayılı uygulama kararında atıfta bulunulan elektronik imza standartlarının olası güncellemesi durumunda, eIDAS Tüzüğü gereksinimlerini yerine getirmek amacıyla oluşturulmuştur (ENISA, 2019).

Oluşturulan Avrupa Standartları (ETSI ENs) imza standardı serisi;

- Belirli bir sözdizimindeki (ASN.1, XML, PDF Sözlüğü) imzalı ve imzasız özellikleri,
- İlgili özelliklerin imza yapısına eklenmesine yönelik mekanizmaları,
- Standartlarda belirlenen temel imza seviyelerinde ihtiyaç duyulan imza özelliklerinin bileşimini içermektedir.

Yapılan güncellemelerle birlikte Tablo 3’te belirtilen standartlar oluşturulmuştur.

Tablo 3*Güncel Avrupa Standartları*

İmza Tipi	Standart
CMS Gelişmiş Elektronik İmzalar (CAAdES)	ETSI EN 319 122 Part 1: CAAdES Baseline Signatures (ETSI, 2023) ETSI EN 319 122 Part 2: Extended CAAdES Signatures (ETSI, 2021)
XML Gelişmiş Elektronik İmzalar (XAdES)	ETSI EN 319 132 Part 1: XAdES Baseline Signatures (ETSI, 2016b) ETSI EN 319 132 Part 2: Extended XAdES Signatures (ETSI, 2016c)
PDF Gelişmiş Elektronik İmzalar (PAdES)	ETSI EN 319 142 Part 1: PAdES Baseline Signatures (ETSI, 2022) ETSI EN 319 142 Part 2: Additional PAdES Signatures Profiles (ETSI, 2016d)

Yeni imza standartlarında her bir imza formatı iki ayrı kısımda detaylandırılmıştır. Standartların ilk bölümü, ilgili imza formatının temel yapıtaşlarını içeren imza profillerini, imza özelliklerine ilişkin sözdizimleri ve imzanın uzun vadede korunmasını sağlamak için ihtiyaç duyulan gereksinimleri içeren dört imza seviyesini tanımlamaktadır. Bu seviyeler, birbiri üzerine kurulu olup, imza formatının temel yapısal özelliklerini belirlemektedir. İkinci bölüm ise ETSI TS imza standartlarında atıfta bulunulan imza seviyelerini ve gereksinimlerini yeniden düzenlenmiş bir formda içermektedir. Bu yaklaşım, ilk bölümde yer alan imza formatlarına ek olarak yeni formatları tanımlama imkânı sağlarken, daha fazla esneklik ve isteğe bağlılık sunmaktadır (ENISA, 2019).

3. Güncel ve Geçmiş İmza Standartları Arasındaki Farklar

ETSI tarafından 2016 Nisan ayında yayımlanan Avrupa standartları, standartların oluşturulması sürecinde kamuya açık bir inceleme ve test (eSignature Validation Plugtests, b.t.) imkânı sunarak teknik kusurların ortadan kaldırılmasına yardımcı olduğundan önceki teknik özellikler serilerinden daha yüksek bir kararlılığa ve belge hiyerarşisinde daha yüksek bir değere sahiptir. Bu hâliyle ilgili standartlarla çakışan başka hiçbir ulusal standardın geliştirilemeyeceğini ve kabul edilemeyeceğini garanti eder (ENISA, 2019).

Güncel Avrupa Standartları; önceki standartlarda belirlenmiş olan imza özelliklerinin yerine geçecek yeni özelliklerin belirlenmesi, daha önce sunulmayan yeni özelliklerin tanımlanması, önceki standartlarda tanımlı bazı özelliklerin kullanımdan kaldırılması, mevcuttaki bazı imza özelliklerinin kullanım durumlarına açıklık getirilmesi ve yeni imza seviyelerinin tanımlanması gibi temel farklılıklar sunmaktadır.

Bu bölümün alt başlıklarında, 1999/93/EC sayılı Elektronik İmza Direktifi ile uygulamaya konulan ve 2015/1506 sayılı eIDAS Uygulama Kararı'na kadar yürürlükte kalan ilk ETSI Teknik Özellikler serisi ile Avrupa elektronik imza standardizasyon çerçevesi kapsamında oluşturulan güncel ETSI Avrupa Standartları arasındaki temel farklılıklara değinilmiştir.

3.1. Yeni İmza Özelliklerinin Tanımlanması

Güncel Avrupa Standartlarında, önceki standartlarda yer alan bazı imza özelliklerinin yerine geçen veya önceki standartlarda bulunmayan yeni imza özelliklerinin tanımlanması sağlanmıştır. İlgili standartlar incelendiğinde her bir temel imza formatında yapılan değişikliğin farklılık gösterdiği görülmektedir. Örneğin; yeni standartlarla birlikte CAAdES ve XAdES imza formatında bulunan ve imzacı sertifikasının değiştirilmelere karşı korunmasını sağlayan signing-certificate özelliği içerisindeki IssuerSerial alanının kullanımının önerilmediği görülmektedir. Benzer şekilde CAAdES ve PAdES imza formatında bulunan ve imzacı tarafından taahhüt edilen durumları içeren signer-attributes imza özelliği yerine iddia edilen taahhütlerden daha kesin durumların imzaya eklenebilmesini sağlayan signedAssertions alanını içeren yeni signer-attributes-v2 imza özelliği tanımlanmıştır (ETSI, 2023; ETSI, 2022). İmza türlerine göre yeni tanımlanan özelliklere ilişkin durumlar Tablo 4'te listelenmiştir.

Tablo 4*Güncel Standartlarda Tanımlı Yeni İmza Özellikleri*

İmza Formatı	ETSI TS 101 733 / ETSI TS 103 173	ETSI EN 319 122-1/2	
	ETSI TS 101 778 / ETSI TS 103 172	ETSI EN 319 142-1/2	
	ETSI TS 101 903 / ETSI TS 103 171	ETSI EN 319 132-1/2	
CAeS	signer-attributes	signer-attributes-v2	
PAeS	--	signature-policy-store	
	ats-hash-index	ats-hash-index-v3	
CAeS	SigPolicyQualifierInfo in signature-policy-identifier	SigPolicyQualifierInfo in signature-policy-identifier (SPDocSpecification)	
	sigPolicyHash in signature-policy-identifier	sigPolicyHash in signature-policy-identifier (zero-hash-value)	
	--	cms-algorithm-protection	
	signing-certificate-v2	signing-certificate-v2	
	xades:SigningCertificate	xades:SigningCertificateV2	
XAdES	xades:CompleteCertificateRefs	xadesv141:CompleteCertificateRefsV2	
	xades:AttributeCertificateRefs	xadesv141:AttributeCertificateRefsV2	
	xades:SigAndRefsTimeStamp	xadesv141:SigAndRefsTimeStampV2	
	xades:RefsOnlyTimeStamp	xadesv141:RefsOnlyTimeStampV2	
	xades:SignatureProductionPlace	xades:SignatureProductionPlaceV2	
	SignerRole	SignerRolev2	
	--	xadesv141:SignaturePolicyStore	
	--	xadesv141:RenewedDigests	

3.2. Kullanımdan Kaldırılan İmza Özellikleri

Güncellenen standartlar ile birlikte tanımlanan yeni özelliklerin kullanıma alınmasıyla eski standartlarda yer alan birtakım imza özelliklerinin kullanımına son verilmiştir. Bunların dışında kalan ve kullanımına son verilen diğer imza özellikleri aşağıda belirtilmiştir:

- signing-certificate-v2 imza özelliğine alternatif olan other-signing-certificate özelliği, signing-certificate-v2 yapısının daha basit olması sebebiyle kullanımdan kaldırılmıştır (ENISA, 2019).
- archive-time-stamp (ATSv2) imza özelliği kullanımındaki avantajlar sebebiyle archive-time-stamp (ATSv3) versiyonu ile değiştirilmiş ve kullanımına son verilmiştir (Ibarz, 2020). Doğrulama verilerinin uzun vadeli kullanımı ve bütünlüğünün sağlanması amacıyla kullanıma alınan bu özellik ile doğrulama verileri imzalı dosya içindeki “SignedData.certificates” ve “Signed-Data.crls” alanlarına eklenmektedir. Bu alanların kullanımı uzun dönemli imza oluştururken, ATSV2 yapılandırmasının aksine imzacı sertifikalarına ait doğrulama verilerinin tekrarlı bir şekilde imzalı dosyalara eklenmesini önlemektedir (ETSI, 2023). Bu nedenle, güncel standartlara uyumlu olarak oluşturulan versiyon 3 arşiv imzalı dosyalar (ESAv3) imzalı dosyalar, v2 arşiv imzalı dosyalara (ESAv2) kıyasla boyut avantajı sağlamaktadır.
- archive-time-stamp özelliğine alternatif olan long-term-validation özelliğinin kullanımı güncel standartlar ile birlikte kaldırılmıştır. Yerine archive-time-stamp (ATSv3) özelliğinin kullanılabilmesi belirtilmiştir.
- İmzaya güvenilir zaman bilgisinin eklenmesi noktasında zaman damgası özelliğine alternatif olan time-mark özelliğinin kullanımına da son verilmiştir.

3.3. Kullanım Durumları Açıklığa Kavuşturulan İmza Özellikleri

Önceki standartlarda zaman içerisinde fark edilen ve bazı imza özelliklerinin hangi durumlarda ve ne şekilde kullanılabilmesine ilişkin tanımlamaların yeterince anlaşılır olmaması sebebiyle güncel standartlarda bu özelliklerin sözdizimleri, anlambilimleri (semantics) ve kodlama tipleri (encoding) ile ilgili durumlar açıklığa kavuşturulmuştur.

Kullanım durumlarına açıklık getirilen özelliklere bakıldığında çoğunlukla her üç imza formatı için de ortak şekilde sertifika doğrulama verileri (Sertifikalar, Sertifika İptal Listesi (SİL) dosyaları, Çevrimiçi Sertifika Durum Protokolü (Online Certificate Status Protokol, OCSP) Yanıtları ve bu verilere ilişkin referans değerleri) içeren imza özellikleri olduğu görülmektedir (ENISA, 2019). Bunun yanında PAdES imza formatında yer alan ve genellikle imzacıyı ve imzalama sebebini niteleyen bilgilerin yer aldığı Filter, Location, Name, ContentInfo, Reason ve commitment-type-indication özelliklerinin kullanım durumlarına da açıklık getirilmiştir.

3.4. Yeni İmza Seviyelerinin Tanımlanması

Güncel standartlarla birlikte gelen yeniliklerden biri de teknik özelliklerde (ETSI TSs) belirtilen imza seviyelerinin revize edilerek yeni imza seviyelerinin tanımlanmasıdır. Avrupa Standartları (ETSI ENs) ile gelen imza setinde dört yeni imza seviyesi tanımlanarak seviyelere ilişkin açıklamalar ve imza seviyelerine uygunluk için asgari gereksinimler belirlenmiştir (Tablo 5) (Ibarz, 2020; ETSI, 2016b; ETSI, 2022). Bu sayede elektronik imza uygulamalarında farklı yorumlamaların önüne geçerek elektronik imza formatlarının ortak bir temele oturtulması ve ortak çalışabilirliğin artırılması hedeflenmiştir (ENISA, 2019).

Tablo 5

Güncel Standartlarda Tanımlı Yeni İmza Seviyeleri

	CAdES (ETSI EN 319 122-1)	PAdES (ETSI EN 319 142-1)	XAdES (ETSI EN 319 132-1)
B-B-Level	İmzalı ve bazı imzasız özellikler dahil edilerek oluşturulan en alt seviye imzadır. İmzanın geçerliliği, imzacı sertifikası geçersiz hale geldiğinde (iptal, geçerlilik süresinin dolması vb. durumlarda) sona erer.		
B-T-Level	İmzanın oluşturulduğu zamanın kayıt altına alınabilmesi amacıyla <i>B-B-Level</i> bir imza üzerine imza zaman damgası özelliği eklenmesi ile oluşan imza seviyesidir.		
B-LT-Level	B-T-Level bir imza üzerine uzun dönem doğrulama verilerinin eklenmesiyle oluşturulan imza seviyesidir. Eklenen doğrulama verileri ile sertifika ömürlerinin dolmasından sonra da imzanın doğrulanabilmesi sağlanır.		
B-LTA-Level	B-LT-Level bir imza üzerine arşiv zaman damgası eklenmesiyle elde edilen imza seviyesidir. Arşiv zaman damgası ile doğrulama verilerinin uzun dönemli erişilebilirliği yanında bütünlüğünü de korumayı amaçlar.		

Her seviyede, imza bileşenlerinin hangi durumlarda kullanılacağı veya kullanılmayacağı açık bir şekilde tanımlanmıştır. Bu güncelleme kullanıcıların ve uygulama geliştiricilerinin hangi imza seviyesi için hangi özellikleri dahil etmesi gerektiği konusunda netlik sağlamak amacıyla gerçekleştirilmiştir.

4. Türkiye’de Elektronik İmza

Elektronik imza konusunda Türkiye’deki temel yasal düzenleme, 5 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu’dur. Bu kanun ve kanuna bağlı ikincil mevzuatın getirdiği düzenlemeler ile, özel merasime tabi olmayan belgelerin yasal olarak imzalanması mümkün hâle gelmiştir (Ergun ve Çelik, 2015). 5070 Sayılı Elektronik İmza Kanunu’nda, güvenli elektronik imzanın sahip olması gereken özellikler tanımlanmış ve yasal çerçeve çizilmiştir. Elektronik imzanın ıslak imza ile eşdeğerliği de garanti altına alınmıştır (Elektronik İmza Kanunu, 2004).

6 Ocak 2005 tarihinde yayımlanan ve Elektronik İmza Kanunu'nun uygulanmasına ilişkin önemli detayları içeren “Elektronik İmza Kanunu’nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönet-

melik” Türkiye’de elektronik imza uygulamalarının teknik ve idari yönlerini düzenlemektedir. Bu yönetmelik, elektronik imza hizmeti sunacak olan sağlayıcıların yetkilendirilmesi, sertifika politikalarının belirlenmesi, sertifikaların yayınlanması ve geri çağırılması gibi konularda detaylı kurallar getirmektedir (Elektronik İmza Kanunu’nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2005).

Elektronik İmza Kanunu’nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik’te elektronik imza formatlarına özgü herhangi bir düzenleme bulunmaması sebebiyle söz konusu yönetmeliğin 35. maddesi gereğince Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 1 Haziran 2006 tarih ve 2006/DK-77/353 sayılı Telekomünikasyon Kurulu Kararı yayımlanmıştır. Bu karar ile CAAdES ve XAdES formatındaki güvenli elektronik imzaların ETSI TS 101 733 ve ETSI TS 101 903 standartlarına uygun olarak oluşturulması tavsiye edilmiştir (BTK, 2006). İleriki yıllarda ülkemizde kullanılan elektronik imza uygulamalarında ortaya çıkan PDF temelli imza oluşturma ihtiyacı üzerine BTK’nın 02/07/2012 tarih ve 2012/DK-15/299 sayılı Kararı yayımlanarak güvenli elektronik imza formatları arasında PAdES de dahil edilmiş ve PAdES’in ETSI TS 102 778 standardına uygun olarak oluşturulması tavsiye edilmiştir (BTK, 2012a).

Farklı sistemlerde, farklı standartları temel alan imza formatları tercih edilerek oluşturulan elektronik imzalar sebebiyle sistemler arasında birlikte çalışabilirliğin sağlanması konusunda sorunlar ortaya çıkmaktadır. Ortak standartların belirlenmesi adına BTK tarafından Elektronik İmza Kullanım Profilleri Rehberi yayımlanmıştır (BTK, 2012b). Bu rehberde imza formatları tanımlanmış ve CAAdES için ETSI TS 101 733 (ETSI, 2013b), XAdES için ETSI TS 101 903 (ETSI, 2010), PAdES için ise ETSI TS 102 778-3 (ETSI, 2009b) ve ETSI TS 102 778-5 (ETSI, 2009c) dokümanlarında tanımlanan “Explicit Policy Electronic Signatures (EPES)” formatı temel alınmıştır. Mevcut durumda Elektronik İmza Kullanım Profilleri Rehberi, Türkiye’de geçerliliğini korumaktadır.

E-devlet ve e-dönüşüm kavramları, teknolojik ilerlemenin kamu yönetimine entegre edilmesi yoluyla kamu hizmetlerinin performansını, kalitesini ve şeffaflığını artırmak adına kritik unsurlardır. Elektronik imza da bu dönüşüm sürecinin önemli bir bileşeni olarak öne çıkmaktadır (Güler, 2011). Özellikle Elektronik İmza Kanunu’nun 2004 yılında yürürlüğe girmesi ve bunu takip eden diğer hukuki düzenlemeler, elektronik imza kullanımını hem kamuda hem de özel sektörde giderek yaygınlaştırmıştır (Özgül, 2021).

Elektronik imza ile ilgili kullanımın yaygınlaşması sayesinde kurumsal belgelerin dijital ortamda güvenli bir şekilde imzalanması mümkün hâle gelmiş ve elektronik belge yönetim sistemleri (EBYS) oluşturulmuştur. EBYS’ler, kurumlar arasında ortak çalışabilirliği sağlayarak, değişen teknolojiye uyum sağlama konusunda önemli ilerlemeler kaydetmiştir (Kayalı vd., 2021). EBYS’lerin kurum içerisindeki belge yönetim süreçlerini elektronik ortama taşımasıyla beraber kurumlar arasında iletilecek resmi yazışmalar ile bunların üst verilerini ve elektronik imzalarını taşıyacak bir paket yapısı oluşturulması ihtiyacı gündeme gelmiştir. Bu ihtiyaç doğrultusunda, kamu kurum ve kuruluşları arasındaki resmi yazışmaların elektronik ortamda güvenli bir şekilde yapılmasını sağlamak amacıyla e-Yazışma Projesi (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023) oluşturulmuştur.

E-Yazışma Projesi, kurumların elektronik belge yönetim sistemlerinin işleyişini mümkün olduğunca az etkileyecek şekilde, kurumlar arasında iletilecek resmi yazıyı taşıyan paketin (e-Yazışma Paketi) gönderici kurumda oluşturulması ve alıcı kurumda alınıp açılması işlemlerine odaklanmaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023). E-Yazışma Projesi çalışmaları Ağustos 2019 tarihi itibarıyla Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığınca yürütülmeye başlanmış ve 28 Ağustos 2020 tarihinde güncel EYP 2.0 Teknik Rehberi (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020) yayımlanmıştır. Elektronik belgelerin e-Yazışma Teknik Rehberi’ne uygun olarak hazırlanma esasları “Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkındaki Yönetmelik” (Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkındaki Yönetmelik, 2020) ile belirlenerek elektronik belgelerin güvenliği ve standartları daha net bir şekilde vurgulanmıştır (Kayalı vd., 2021).

İlgili rehberde EBYS entegrasyon çalışmalarına ilişkin genel bilgiler, EYP 2.0 paket yapısı, imzalama ve şifreleme mekanizmaları gibi teknik hususlar detaylı şekilde anlatılmaktadır. E-Yazışma Paketi’nde yer alan imza bileşenlerinin BTK’nın Elektronik İmza Kullanım Profilleri Rehberi’nde (BTK, 2012b) yer alan uzun dönemli imza profiline sahip P4 CAAdES-X Long formatında olması, mühür bileşeninin ise P4 CAAdES-Arşiv formatında olması gerekmektedir (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020).

Kamu ve özel sektördeki tüm sağlık hizmetlerinde kullanılmak üzere, Sağlık Bakanlığı kontrolünde ortak bir e-reçete uygulamasına geçilmesi gerektiğine dair 5 Mart 2018 tarihli genelge (Türkiye İlaç ve Tıbbi Cihaz Kurumu, 2018) yayımlanmıştır. Hekimlerin, genelgede verilen 1 Nisan 2018 tarihi itibarıyla e-reçete sistemini kullanarak ve e-imza prosedürü ile imzalama yaparak reçete oluşturması gerektiği belirtilmektedir. E-Reçete uygulamasında XAdES imza formatı kullanılmaktadır (Sosyal Güvenlik Kurumu, 2023).

Türkiye’de hayata geçirilen bu teknolojik gelişmeler tüm sektörleri etkilediği gibi muhasebe uygulamalarında da e-dönüşüm ihtiyacı doğmuştur. Muhasebe sektörünün de dijital dönüşüme dahil edilmesi, hata ve hileyi en aza indirmek, vergi kayıplarını önlemek, aktif bir denetim ve kontrol sistemini hayata geçirmek adına önem arz etmektedir. E-dönüşüm kapsamında Türkiye’de kullanılmakta olan e-fatura, e-arşiv fatura, e-defter ve e-irsaliye gibi kavramlar ve bunların elektronik imza prosedürleri ile kullanılabilmesi uygulamalar geliştirilmiştir (Akyüz, 2020). E-dönüşüm kapsamında muhasebe ile alakalı işlemler için kullanılan uygulamalarda XAdES imza formatı kullanılmaktadır (Gelir İdaresi Başkanlığı, 2018).

Elektronik imza gerçekte olduğu gibi dijital dünyada da bir kimliğe sahip olabilmemizi sağlamaktadır. Söz konusu kimliğe sahip olarak çeşitli elektronik işlemlerin yapılması mümkün olmaktadır. Elektronik imzanın gündelik yaşama katacağı değişikliklerden en önemlisi de tüm dünya ülkelerindeki yasal düzenlemelerin elektronik imzaya attığı hukuki değerle alakalıdır. Islak imza ile aynı yasal sonuçları doğurması ve ülkeleri, "kâğıtsız dünya" idealine yaklaştırması söz konusudur (Güler, 2011). E-Devlet hizmetlerinin yaygınlaşması kaynak ve zaman israfını azaltarak verimliliği artıracak, ekonomik iyileşme sağlayacak ve Türkiye’yi refah seviyesi yüksek bir toplum olma hedefine yaklaştıracaktır (Naralan, 2010).

Türkiye’de e-dönüşüm başlı başına kapsamlı bir oluşumdur. Bu nedenle hem ulusal hem uluslararası mecralarda konunun gündeme getirilmesi, dönüşümün doğru anlaşılması ve aktarılması isabetli olacaktır (Tektüfekçi, 2017). Türkiye’de hâlihazırda kamu ve özel sektör olmak üzere birçok alanda elektronik imza uygulamalarının kullanıldığı sistemler mevcuttur. Bu sistemler aracılığıyla dijital dönüşümün her alana yayılmasının başlıca hedefi, kurumlar arası birlikte çalışabilirliği sağlamak ve gelişen teknoloji ile beraber gelen yenilikleri yakalayabilmektir.

5. Bulgular

İçerisinde çok sayıda ülkenin yer aldığı Avrupa Birliği, 1999/93/EC sayılı Elektronik İmza Direktifi ile başlayarak günümüzde eIDAS 2.0’a kadar uzanan elektronik imza gelişim sürecinde, elektronik imza mevzuatı ve buna paralel olarak elektronik imza standartlarında çeşitli geliştirme ve iyileştirmeler içeren güncellemeler yapmıştır. Bu güncellemelerin temel hedefleri şunlardır;

- AB iç pazarında tespit edilen problemleri gidererek ihtiyaca yönelik değişiklikler ortaya koymak,
- AB üyesi herhangi bir ülkede oluşturulan bir elektronik imzanın diğer Avrupa ülkelerinde doğrulanabilmesini sağlayarak birlikte çalışabilirliği mümkün olduğu kadar korumak ve kolaylaştırmak,
- İmzanın uzun vadede korunmasını sağlamak,
- Elektronik imzaların oluşturulması ve doğrulanması noktasındaki belirsizlikleri gidermek,
- Elektronik imza kullanımının güvenliği, bütünlüğü ve kabul edilebilirliği hususlarında iyileştirmeler yaparak elektronik iletişimdeki güveni artırmak.

Avrupa Birliğinde bu kazanımların sağlanması noktasında gelişmiş elektronik imza formatlarının kullanımını desteklemekte ve güncel ETSI EN standartlarına uyum teşvik edilmektedir. Ancak hâlen yürürlükte olan 2015/1506 sayılı uygulama kararında ETSI TS imza standartlarına referans verilmektedir. Nisan 2016’da ETSI tarafından oluşturulan Avrupa Standartları (ETSI ENs), standartlar hiyerarşisinde önemli bir istikrar sağlamakta ve bir değer temsil etmektedir. CMS, XML ve PDF tabanlı elektronik imza ve mühür formatlarıyla ilişkili olarak oluşturulan ETSI EN’ler, birlikte çalışabilirliği artırırken, tespit edilen teknik kusurları gidermektedir. Ayrıca, güncel standartta desteklenen zaman damgası özelliği sebebiyle CMS tabanlı imzalarda uzun dönemli imza oluşturma aşamasında boyut avantajı sağlamaktadır. Böylece, belgelerin daha hızlı ve verimli şekilde işlenmesi mümkün hâle gelmektedir. Bu

doğrultuda, ETSI EN imza standartlarını referans alarak, kullanılan imza yazılımlarının güncellenmesi ve uygulamaların geçiş sürecine izin verecek şekilde revize edilmesi Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından tavsiye edilmektedir (ENISA, 2023).

Türkiye’de ıslak imza ile aynı yasal geçerliliğe sahip olan elektronik imza; e-fatura, e-reçete ve elektronik yazışma paketi gibi çeşitli alanlarda oldukça yaygın şekilde kullanılmaktadır. Bununla birlikte, mevcutta Türkiye’de sürdürülen dijital dönüşüm çalışmaları ile elektronik imzanın önemi giderek artmaktadır. Dolayısıyla elektronik imza oluşturulmasında kullanılan standartlar da oldukça önem kazanmıştır. Bu doğrultuda, Avrupa Birliğinde elektronik imza standartlarının yakından takibi ve ilgili güncellemelerin analiz edilerek Türkiye’de elektronik imza mevzuatına kazandırılması önemlidir. Türkiye’de 1999/93/EC sayılı Elektronik İmza Direktifine uygun olarak benimsenen elektronik imza standartları, Avrupa Birliği içerisinde zamanla eIDAS düzenlemeleriyle güncellenmiş ve uygulanmaya başlamasına karşın Türkiye’de henüz eIDAS’ın getirdiği güncel standartlara uyum bulunmamaktadır. Avrupa Birliği ile sağlanacak olan dijital ticaretin ve iletişimin güvenliği ve etkinliğini sağlamak adına elektronik imza ve güven hizmetleri kapsamında Avrupa Birliği ve Türkiye arasındaki ortak altyapının sağlanması önemli bir ihtiyaçtır.

Türkiye’de güncel standartlara entegrasyon süreci, elektronik imza sistemlerinin güncel teknolojilere uyum sağlaması ve ilerlemesi için bir dizi adımı içermektedir.

- i. Türkiye’de yürürlükte olan elektronik imza mevzuatı ve ikincil düzenlemelerin güncel standartları referans alacak şekilde düzenlenmesi, sektördeki paydaşlar için önemli bir tetikleme olacaktır.
- ii. Elektronik imza yazılım kütüphanesi (API) sağlayan geliştiricilerin, güncel standartlara uyum sağlamak adına yazılım güncellemelerini sağlamaları gerekmektedir.
- iii. Eski standartlarla oluşturulan imzalı dosyaların, güncel standartlara uygun oluşturulan dosyalarla birlikte çalışabilirliğinin sağlanması da kritik bir adımdır. Bu, geçmişte oluşturulan verilerin ve dosyaların güncel teknolojilerle uyumlu hâle getirilmesi ve kullanılabilirliğini sürdürmesi açısından önemlidir.

Tüm bu adımların bir araya gelmesiyle, elektronik imza uygulamaları hem güncel standartlara entegre olacak hem de mevcut sistemlerle uyumlu bir şekilde işlev görebileceklerdir. Bu da elektronik imza teknolojilerinin daha geniş bir kullanım ve kabul görmesine olanak tanıyacaktır.

6. Sonuç

Teknolojik gelişmelerin hız kazanmasıyla birlikte, elektronik imza gibi temel teknolojilere dayalı uygulamaların da sürekli olarak güncelliğini koruması gerekliliği ortaya çıkmaktadır. Bu bağlamda, standartlar değişen gereksinimlere cevap verecek şekilde gelişim göstermektedir. Bu gelişim çerçevesinde, 1999/93/EC sayılı Elektronik İmza Direktifinden başlayarak eIDAS 2.0’a kadar uzanan süreçte elektronik imza standartları dinamik bir yapı göstererek güncellemelere uğramıştır. Bu güncellemelerin temel hedefleri; iç pazarda tespit edilen sorunları çözmek, birlikte çalışabilirliği artırmak, elektronik imzaların uzun vadede korunmasını sağlamak, belirsizlikleri gidermek ve elektronik imza kullanımının güvenliğini ve kabul edilebilirliğini geliştirmektir.

EIDAS Tüzüğü altında Avrupa Birliği’ne uyum sağlamak ve farklı sistemler arasında birlikte çalışabilirliği elde etmek, ETSI tarafından yayımlanan güncel standartlara sıkı bir şekilde uyumu gerektirir. Bu standartlar, elektronik imza ve kimlik doğrulama sistemlerinde güvenliği, tutarlılığı ve standardizasyonu teşvik etmekte ve Avrupa Birliği genelinde bu alanda benimsenen en güncel yaklaşımları belirlemektedir. Bu bağlamda, Türkiye’deki elektronik imza kullanımı için önemli bir referans olan ETSI standartlarının yakından takip edilmesi, detaylı bir şekilde incelenmesi ve gerektiğinde ilgili tarafların katılımıyla iyileştirilmeler yapılması hem ulusal hem de uluslararası düzeyde birbiri ile uyumlu ve güvenli bir elektronik imza altyapısının sağlanması için kritik öneme sahiptir. Standartlar çerçevesinde birbiriyle uyumlu bir elektronik imza altyapısının oluşturulmasının, Türkiye ve Avrupa Birliği arasında dijital ticaretin ve iletişimin güvenliği ve etkinliğini artırarak dijital dönüşüm sürecine önemli katkılar sağlayacağı düşünülmektedir.

Bu çalışmada ETSI güncel standartları incelenerek, elektronik imza standartlarının gelişimi üzerinde durulmuştur. Türkiye'de hâli hazırda kullanımda olan elektronik imza altyapısı incelenmiş ve bu altyapının güncel standartlara uyum sağlaması sürecinde ele alınması gereken noktalar değerlendirilmiştir. Elektronik imza standartlarına uyum, ETSI'nin güncel standartlarının titizlikle incelenmesi ve ardından ülke ihtiyaçlarına uygunluğunun değerlendirilmesiyle sağlanabilir. Bu süreçte, ilgili otoritelerin ve sektör temsilcilerinin katılımı ve iş birliği önemlidir. Türkiye'nin gereksinimlerine uygun olarak yapılan değerlendirmeler, standartlarda gerekli iyileştirmelerin yapılmasına ve uluslararası alanda uyumlu bir elektronik imza çerçevesinin oluşturulmasına olanak tanıyacaktır. Bu doğrultuda bu çalışma belirtilen çerçevenin oluşturulması noktasında önemli bir kaynak sağlayacaktır. Bununla birlikte, gelişmelerin uygulamada sağlayacağı katkılar analiz edilerek Türkiye mevzuatı için uygun olanları belirleyecek yeni çalışmalara da ihtiyaç bulunmaktadır.

Etik Standartlar İle Uyumluluk

Çıkar Çatışması: Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkı Beyanı: Yazarlar makalenin eleştirel incelenmesi sürecinin Tuğba Özcan tarafından yürütüldüğünü, makalenin organizasyonu sürecinin Tuğba Özcan ve Meltem Seyirt tarafından yürütüldüğünü, diğer tüm süreçlere ise eşit oranda katkı sağladıklarını beyan ederler.

Finansal Destek: Yoktur.

Kaynakça

- Adobe. (2016). Compliance with European electronic signatures legislation. Erişim Adresi: <https://www.adobe.com/content/dam/dx-dc/en/pdfs/adobe-sign-eidas-compliance-uk.pdf>
- Akyüz, F. (2020). Yeni Tebliğler Kapsamında Meslek Mensuplarının E-Dönüşüm Algılarının İncelenmesi: Uşak İli Örneği. *Türk Turizm Araştırmaları Dergisi*. Erişim Adresi: <https://doi.org/10.26677/TR1010.2020.536>
- Biçkin, İ. (2006). Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler. *Türkiye Barolar Birliği Dergisi*, (63), 109-126.
- BTK. (2006). 2006/DK-77/353 sayılı Telekomünikasyon Kurulu Kararı. Erişim Adresi: <https://www.btk.gov.tr/uploads/pages/guvenli-elektronik-imza-formatlarına-dair-usul-ve-esaslar-5a33fef63b234.pdf>
- BTK. (2012a). 2012/DK-15/299 sayılı Bilgi Teknolojileri ve İletişim Kurulu Kararı. Erişim Adresi: <https://www.btk.gov.tr/uploads/pages/2012-07-02-tarih-2012-dk-15-299-sayili-guvenli-eimza-kurul-karari-5a33ff1a6d81d.pdf>
- BTK. (2012b). Elektronik İmza Kullanım Profilleri Rehberi, Sürüm 1.0. Erişim Adresi: <https://www.btk.gov.tr/uploads/pages/elektronik-imza-kullanim-profilleri-rehberi-5a33ff5b59f93.pdf>
- Busch, C. (2022). eIDAS 2.0: Digital Identity Services in the Platform Economy, Centre on Regulation in Europe. Erişim Adresi: https://cerre.eu/wp-content/uploads/2022/10/CERRE_Digital-Identity_Issue-Paper_FINAL-2.pdf
- Elektronik İmza Kanunu. (2004). T.C. Resmî Gazete, Sayı: 25355, Tarih: 23.01.2004. Erişim Adresi: <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5070.pdf>
- Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik. (2005). T.C. Resmî Gazete, Sayı: 25692, Tarih: 06.01.2005. Erişim Adresi: <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7224&MevzuatTur=7&MevzuatTertip=5>
- ENISA. (2016). Security Guidelines on the Appropriate Use of Qualified Electronic Registered Delivery Services. Erişim Adresi: <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures>

- ENISA. (2019). Overview of Standards Related to eIDAS. Erişim Adresi: <https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas-i>
- ENISA. (2023). Digital Identity Standards. Erişim Adresi: <https://www.enisa.europa.eu/publications/digital-identity-standards>
- Ergun, T. Çelik, V. e-Arşiv ve Uzun Dönemli Doğrulama. (2015). e-BEYAS 2015, Erişim Adresi: https://www.kamusm.gov.tr/dosyalar/bildiriler/e-Arsiv_ve_Uzun_Donemli_Dogrulama.pdf
- eSignature Validation Plugtest. (b.t.). ETSI. Erişim Adresi: <https://www.etsi.org/events/past-events/2025-esignature-validation-plugtests>
- ETSI Plugtests Interop Events. (2024). Erişim Adresi: <https://www.etsi.org/events/plugtests>
- ETSI. (2009a). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles. Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf
- ETSI. (2009b). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced- PAdES-BES and PAdES-EPES Profiles. (2009). Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.01.02_60/ts_10277803v010102p.pdf
- ETSI. (2009c). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content- Profiles for XAdES signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277805/01.01.02_60/ts_10277805v010102p.pdf
- ETSI. (2010). Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES). Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf
- ETSI. (2012a). Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile. Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103173v020101p.pdf
- ETSI. (2012b). Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile. Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
- ETSI. (2013a). A Guide to Writing World Class Standards. Erişim Adresi: <https://portal.etsi.org/portals/0/tbpages/edithelp/docs/aguidetowritingworldclassstandards.pdf>
- ETSI. (2013b). Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
- ETSI. (2013c). Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile. Erişim Adresi: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf
- ETSI. (2016a). Electronic Signatures and Infrastructures (ESI); The Framework for Standardization of Signatures: Overview. Erişim Adresi: https://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf
- ETSI. (2016b). Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 1: Building Blocks and PAdES Baseline Signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf
- ETSI. (2016c). Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 2: Additional PAdES Signatures Profiles. Erişim Adresi:

- https://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf
- ETSI. (2016d). Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures; Part 2: Extended XAdES Signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf
- ETSI. (2020). Standards, Specifications and Reports. Erişim Adresi: <https://www.etsi.org/standards/types-of-standards>
- ETSI. (2021). Electronic Signatures and Infrastructures (ESI); CAAdES Digital Signatures; Part 2: Extended CAAdES Signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.02.01_60/en_31912201v010201p.pdf
- ETSI. (2022). Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures; Part 1: Building Blocks and XAdES Baseline Signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.02.01_60/en_31913201v010201p.pdf
- ETSI. (2023). Electronic Signatures and Infrastructures (ESI); CAAdES Digital Signatures; Part 1: Building Blocks and CAAdES Baseline Signatures. Erişim Adresi: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.03.01_60/en_31912201v010301p.pdf
- European Commission. (2023). Standards and Specifications. Erişim Adresi: <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Standards+and+specifications>
- European Commission. (2024). European Standards. Erişim Adresi: https://single-market-economy.ec.europa.eu/single-market/european-standards_en
- European Parliament and Council. (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. Erişim Adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093>
- European Parliament and Council. (2003). Commission Decision of 14 July 2003 on the Publication of Reference Numbers of Generally Recognised Standards for Electronic Signature Products in Accordance with Directive 1999/93/EC of the European Parliament and of the Council. Erişim Adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003D0511>
- European Parliament and Council. (2014a). Regulation EU 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. Erişim Adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>
- European Parliament and Council. (2014b). Commission Implementing Decision (EU) 2014/148/EU, Official Journal of European Union. Erişim Adresi: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:080:0007:0009:EN:PDF>
- European Parliament and Council. (2015). Commission Implementing Decision (EU) 2015/1506, Official Journal of European Union. Erişim Adresi: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506>
- European Parliament and Council. (2021). Draft Regulation of the European Parliament and of the Council Amending Regulation (EU) no. 910/2014 Regarding the Establishment of a Framework for a European Digital Identity. EIDAS 2.0 Proposal. Erişim Adresi: https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF
- Federal Office for Information Security. (2023). Basics of Digital Signature Techniques and Trust Services, Version 2.0. Erişim Adresi:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile

- Gelir İdaresi Başkanlığı. (2018). e-Fatura Uygulaması Entegrasyon Kılavuzu. Erişim Adresi: https://www.edmbilisim.com.tr/uploads/EditorDosya/e-faturauygulamasientegrasyonkılavuzu-v1_10.pdf
- Güler, M. (2011). Türkiye'de e-İmza Alanındaki Hukuki Düzenlemeler ve Bazı Kamu Kurumlarındaki e-İmza Uygulamaları. *Sosyoekonomi*, 14(14). <https://doi.org/10.17233/se.39964>
- Ibarz, J. C. (2020). Bringing JSON signatures to ETSI AdES framework: Meet JAdES signatures. *Computer Standards & Interfaces*. Erişim Adresi: <https://www.sciencedirect.com/science/article/pii/S0920548919300960>
- Kayalı, N., Şimşek, M. U., Uysal, M. (2021). Resmî Yazışmalarda Uygulanacak Usul Ve Esaslar Hakkında Yönetmelik: Yeni Uygulamaların ve Hükümlerin Bilgi ve Belge Yönetimi Açısından Değerlendirilmesi. *Arşiv Dünyası*, 8(1), 1-13. Doi: <https://doi.org/10.53474/ad.836048>
- Naralan, A. (2010). Türkiye'de e-Hazırlık ve e-Devletleşme. *Atatürk Üniversitesi İktisadi Ve İdari Bilimler Dergisi*, 23(1), 1-17.
- Niestadt, M. (2022). AT A GLANCE Digital issues in focus: Electronic Signatures. European Parliamentary Research Service.
- Özgül, M. E. (2021). Güvenli Elektronik İmza Sahibinin Hakları ve Yükümlülükleri. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 12(2), 539-556. <https://doi.org/10.21492/inuhfd.884252>
- Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkındaki Yönetmelik. (2020). T.C. Resmî Gazete, Sayı: 31151, Tarih: 10.06.2020. Erişim Adresi: <https://www.mevzuat.gov.tr/mevzuatmetin/21.5.2646.pdf>
- Schwalm, S. (2023). The Possible Impacts of the eIDAS 2.0 Digital Identity Approach in Germany and Europe. OpenIdentitySummit.
- Sosyal Güvenlik Kurumu (2023). Medula Eczane Reçete ve Rapor Web Servisleri Kullanım Kılavuzu. Erişim Adresi: <https://medeczane.sgk.gov.tr/doktor/SaglikTesisleriReceteVeRaporWebServisleri.pdf>
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). e-Yazışma Teknik Rehberi, EYP 2.0. Erişim Adresi: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/EYP_2.0/EYP2.0_teknik-rehberi.pdf
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). E-Yazışma Projesi. Erişim Adresi: <https://cbddo.gov.tr/projeler/e-yazisma/>
- Tektüfekçi, F. (2017). E-Dönüşüm Sürecinde e-Muhasebe Uygulamaları: Türkiye Örneği. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 12(1), 79-88.
- Türkiye İlaç ve Tıbbi Cihaz Kurumu. (2018). 05/03/2018 tarihli Genelge. Erişim Adresi: https://titck.gov.tr/storage/announcement/CANONSRV_Yaz%C4%B1c%C4%B1i8-Sol_1506_001.pdf