e-Arşiv ve Uzun Dönemli Doğrulama

e-Archive and Long Term Validation

İlk Yazar
Dr. Tamer ERGUN, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi, tamer.ergun@tubitak.gov.tr

İkinci Yazar
Dr. Vural ÇELİK, TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi, vural.celik@tubitak.gov.tr

Öz

5070 sayılı elektronik imza kanununun ve ilgili mevzuatın ülkemize getirdiği düzenlemeler sayesinde, elektronik ortamda özel merasime tabi olmayan belgelerin yasal olarak imzalanması mümkün hale gelmiştir. Bu doğrultuda kurumlar ve kişiler süreçlerini ve işlemlerini elektronik ortamdan yapmaya başlamışlardır. Elektronik ortamda atılan imzaların günlük hayatta kullanılmaya başlanması ile elektronik imzanın elektronik ortamda doğrulanması ve saklanması da fiziksel evraktan farklı olarak karşımıza çıkmaktadır.

Elektronik imzanın ilk doğrulanması ve sonraki yıllar için hukuksal kanıt oluşturacak şekilde saklanması ve doğrulanması, elektronik imzanın geleceği için büyük önem arz etmektedir. Elektronik imzanın uzun dönemde tekrardan doğrulanması için yapılması gereken faaliyet ise elektronik imzanın arşivlenmesi olarak adlandırılmaktadır. Ülkemizde elektronik imza standardı olarak ETSI (European Telecommunications Standards Institute) tarafından hazırlanan CAdES, XAdES ve PAdES imza standartları kullanılmaktadır. Elektronik imzanın arşivlenmesi de yine bu standartlarda belirtilen yöntemlere göre yapılmaktadır.

Anahtar sözcükler: *Elektronik arşiv, elektronik imza, ETSI, e-BEYAS*

Abstract

Through the electonic signature law no.5070 and the regulations arised by the law, it is legally possible to sign a document electronically with the exception of ones which have to be signed with a special ceremony as a mandatory requirement. From this point of view, natural and legal persons began to organize their processes and procedures electronically. Since the usage of electronic signature is increasing in our daily life, long term validation and preservation of an electronic signature is crucial and an additional process apart from its physical counterpart.

Initial and subsequent verification of electronic signature as a proof of legal evidence is an important step for long term validation and preservation of electronic signature. Protection method for long term validation is known as archiving electronic signature. In our country, the electronic signature standards of ETSI, CAdES, XAdES and PAdES are used and in those standards, the specific methods for archiving a signature is described in detail.

Keywords: *Electronic archive, electronic signature, ETSI, e-BEYAS*

Giriş

Kurumların e-devlet yapılanmasına dahil olabilmesi için süreçlerini elektronik ortama taşımaları gerekmektedir. Bunun ilk adımlarından biri de kurumsal belgelerin, mevzuat ve standartlara uygun biçimde elektronik ortama taşınması ve bu ortamda etkin biçimde yönetilmesidir. Kurumlarda belgelerin elektronik ortamda yönetilmesi, elektronik belge yönetim sistemleri (EBYS) tarafından sağlanmaktadır. EBYS sistemlerinin kullanılmasının yanında, tam bir e-dönüşümün sağlanabilmesi için geçmişte oluşturulmuş belgelerin dijitalleştirilmesi ve e-arşiv önem kazanmıştır.

E-Dönüşüm, e-devlet, e-kurum ve benzeri yapılanmaların kurumsal süreçlere ve vatandaşlara pozitif etkilerinin yanında, elektronik ortamda yürütülecek bu süreçlerin güvenlik tarafının da dikkate alınması çok önemlidir. Elektronik belgelerin oluşturularak ilgili makama gönderilmesi veya kurum içi dolaştırılması aşamalarında, belgenin bütünlüğünün korunması, değiştirilmeye karşı korunmasının sağlanması gerekmektedir. Bunun yanında belgeyi oluşturan kişinin veya makamın, belgenin elektronik ortamda kontrolü esnasında kimliğinin doğrulanabilmesi de olmazsa olmazlar arasındadır. Elektronik ortamdaki bu gereksinimler elektronik imza sayesinde sağlanabilmektedir. Buradan anlayacağımız üzere, elektronik imza e-dönüşümün, e-devletin, kısaca elektronik ortamda yürütülen tüm projelerin merkezinde bulunmaktadır.

Bu çalışmamızda, e-belgelerin elektronik arşivlenme sürecinde, elektronik imzanın yolculuğundan, imzaların arşivlenmesi ve uzun dönemli doğrulanabilmesi için neler yapılması gerektiğinden bahsedeceğiz. Bunların yanında, ülkemizde imza formatlarını kullanmakta olduğumuz ETSI imza standartlarından ve yaygın kullanılan imza tiplerinden bahsederek imzanın uzun dönemli doğrulama için arşivlenme gerekliliğine vurgu yapacağız.

Elektronik İmza Mekanizması

Elektronik imza temelde matematiksel metotlar üzerine kurulmuş bir yapıdır. 5070 sayılı e-imza kanununda (Kanun, 2004) tanımı "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" şeklinde yapılmaktadır. Tanımda dikkat edilmesi gereken nokta elektronik imzanın, imzalanacak elektronik veriyle mantıksal bağlantısı bulunmasıdır. Normal hayatta attığımız imzalarda, her türlü belgeye aynı imzayı atarız ve dolayısıyla imza ile belgenin bir bağlantısı bulunmamaktadır, fakat elektronik imzada kişinin atmış olduğu her imza, belgeye bağlı olarak değişmektedir. Bunun sebebi kişinin imzasının, belgeye bağlı matematiksel bir fonksiyon olmasıdır ve bu fonksiyon kendi içerisinde kriptografik öğeler barındırmaktadır.

Kriptografik Algoritmalar

Elektronik imza mekanizması içerisinde bulunan kriptografik algoritmalar; özet algoritmaları ve açık anahtarlı şifreleme algoritmalarıdır. Özet algoritmaları yine bir matematiksel fonksiyon olmakla birlikte, girdisinin izi şeklinde çıktılar üretmektedir. Girdi ve çıktı arasında bağ kuran bu fonksiyon sayesinde kanundaki tanımda belirtilen elektronik imzanın, elektronik veriyle bağlantısı oluşmaktadır.

Elektronik imzada özet algoritmaları dışında kullanılan diğer bir kriptografik öğe ise açık anahtarlı şifreleme sistemleridir. Bu sistemde her imzacı için tekil olarak üretilmiş anahtar çiftleri kullanılmaktadır. Anahtar çiftlerinin kişiye veya kuruma özel üretilmesi, benzerinin olmaması sebebiyle, imzacı imzaladığı belgeyi inkar edemez. Açık anahtarlı sistemlerde, tekil olarak üretilmiş anahtar çiftinin bir kişiye veya kuruma zimmet edilmesi önem taşımaktadır. Bu sayede imzalama için kullanılmış anahtarın kime ait olduğu tespit edilir ve imza üzerinden kimlik doğrulama yapılabilir ki yukarıda belirttiğimiz gibi imzalı bir belgenin kim tarafından imzalandığının tespit edilmesi önemli bir husustur. Açık anahtar altyapısı adı verilen, açık anahtarlı şifreleme sistemlerinin idame ettirildiği

yapıda, anahtar çiftinin bir kişi ya da kuruma zimmetlenmesi işlemine anahtarın sertifikalanması adı verilmektedir. Sertifikalama işlemini ise o ülkedeki üst kurul tarafından akredite edilmiş Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) yapmaktadır.

Elektronik Sertifika

Elektronik sertifikanın 5070 sayılı elektronik imza kanunundaki tanımı "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt" şeklinde yapılmaktadır. Bu tanımdan anlaşılacağı üzere sertifikanın varlık sebebi, imzalama için kullanılan ve yukarıda anlatılan anahtar çiftinin kime ait olduğunu ve dolayısıyla imzayı kimin attığını belirlemektir. Genel itibarıyla kullanım alanlarına bakıldığına farklı birçok çeşit sertifikanın olduğu görülmektedir. Bu sertifikalara örnek olarak internet güvenliğinde kullanılan "SSL/TLS" sertifikalarını, işletim sistemlerine veya uygulamalara giriş yapmak için kullanılan "Log in" sertifikalarını, yazılımsal kodların bütünlüğünü sağlamak için kullanılan "kod imzalama" sertifikalarını verebiliriz fakat e-dönüşüm itibariyle, 5070 sayılı kanunda tanımı yapılan, kurum personelinin elektronik imza için kullandığı ve "elle atılan imza ile aynı hukuki sonucu doğuran" sertifikaya Nitelikli Elektronik Sertifika (NES) adı verilmektedir.

Sertifika, imzayı oluşturacak kişinin tespiti ve sertifikada belirtilen anahtar çifti kullanım yetkisinin yine sertifikada belirtilen kişide olduğunu ispatlamak sebebiyle kullanıldığından imzalama ve sonrasında imza doğrulama aşamalarında mutlaka kontrol edilmesi gereken önemli bir unsurdur. Örnek teşkil etmesi açısından sertifika, kredi kartına benzetilebilir. Nasıl kredi kartının ödeme aşamasında iptal olma durumu, süresinin dolma durumu ve daha birçok farklı kontrol yapılıyorsa, sertifika için de aynı kontrollerin yapılması gerekmektedir.

İmzanın uzun dönemli doğrulanması, sertifikanın iptal bilgilerinin, imza tarihi üzerinden uzun dönem geçse dahi temini ve imza doğrulanmasında kullanılabilmesiyle mümkündür. Sertifika ile ilgili iptal bilgileri sertifikayı üreten makam tarafından oluşturulmaktadır.

ETSI Elektronik İmza Formatları

ETSI'ye bağlı hizmet veren Elektronik İmza Altyapıları Birimi (Electronic Signatures and Infrastructures - ESI) Avrupa Birliği üye ülkeler kapsamında elektronik imza standartlarını belirlemektedir. Ülkemizde de ETSI'nin elektronik imza standartlarına (CAdES, 2013), (XAdES, 2009), (PAdES, 2012) uyulmaktadır. Bu standartlarda farklı kullanım alanlarının ihtiyacını karşılayacak imza tipleri belirlenmiştir. Bu bölümde, belirtilen imza tiplerinden en yaygın kullanılanların temel özelliklerinden bahsedeceğiz ve bu tipleri tanıdıktan sonra temel amacımız olan, imzanın arşivlenmesi gerekliliğine değineceğiz.

BES – Basit Elektronik İmza

BES imza ETSI standartlarına göre atılabilecek en temel imza tipidir. İleri seviye imza tipleri, temelinde BES imza üzerine kurulu olduğu için geçiş maksatlı kullanılmaktadır. Basit denmesinin en önemli sebebi imza içerisinde imzalama tarihinin bulunmamasıdır. Bu sebeple yukarıda bahsedilen sertifika doğrulama işlemi göz önüne alındığında, sertifikası geçerli iken imza atan bir kişi, sertifikası iptal olduktan veya süresi dolduktan sonra BES imzayı doğrulamaya çalıştığında, imzalama zamanı belirsiz olduğu için doğrulama yapamayacaktır ve dolayısıyla uzun dönemli doğrulama için uygun imza tipi değildir.

EST – Zaman Damgalı Elektronik İmza

EST imza temelde BES imza üzerine kurulmaktadır. BES imzadan farkı ise imzanın atıldığı tarihi güvenilir olarak belirten imza zaman damgasına sahip olmasıdır. Bu sayede BES imzada belirtilen, sertifika süresi dolduktan veya sertifika iptal olduktan sonra doğrulanamayan imza senaryosu ortadan kalkmaktadır. İmzanın doğrulanması, imza içerisinde barındırılan zaman damgasındaki tarih esas alınarak yapılmaktadır. EST imza BES imzaya kıyasla daha ileri ve güvenilir bir imza tipidir fakat yine de uzun dönemli doğrulama için uygun değildir. Uygun olmama sebebi ise, uzun dönemli doğrulama için gerekli olan sertifika doğrulama verilerinin EST imza içerisinde olmaması ve sertifikayı üreten makam tarafından uzun dönemli saklama ve hizmet verme garantisinin olmamasıdır. Yani bugün atılmış EST imzayı 10 yıl sonra doğrulamaya çalıştığımızda, imzacı sertifikasının doğrulama verilerini bulamama riski yüksek olduğu için uzun dönemli doğrulamaya uygun değildir.

ESXL – Uzun Dönemli Elektronik İmza

ESXL imza temelde EST imzayı içerisinde barındıran ileri imza tipidir. EST imzanın sertifika doğrulama verilerini içerisinde barındırmaması sebebiyle uzun dönemli doğrulama için uygun olmadığını belirtmiştik. ESXL imza bu zafiyeti ortadan kaldırmak adına EST imzadan farklı olarak sertifika doğrulama verilerini paket yapısı içerisinde barındırmaktadır ve bu sebeple bugün atılmış ESXL imza, aradan uzun süreler geçse dahi içerisinde gerekli tüm doğrulama verilerini barındırdığı için doğrulaması yapılabilir hale gelir. Doğrulama yapmak için sertifikayı üreten makama bağımlılık ortadan kalkar.

Elektronik İmzanın Arşivlenmesi

ESA – Arşiv Elektronik İmza

ESA adı verilen arşiv imza temelde ESXL imza tipi üzerine kurulmuştur. ESXL imza yukarıda belirttiğimiz üzere içerisinde sertifika doğrulama verilerini barındırmaktadır ve uzun dönemli doğrulama için tavsiye edilen imza tipidir.

Elektronik imza teknolojisine duyulan güven, imza paketleri içerisinde kullanılan her türlü doğrulama verisinin güvenilir bir makam tarafından imzalanmasına ve imzalamada kullanılan kriptografik algoritmaların var olan ataklara karşı dayanıklılığına bağlıdır. Elektronik imza adı üzerinde elektronik ortamda gerçekleştiğinden, bilgisayarların hesaplama kabiliyetleri kriptografik atakların gücünde belirleyici olmaktadır. Dolayısıyla bugün atılmış ve uzun dönemli doğrulama için gerekli verileri içerisinde barındıran ESXL tipindeki bir imza, içerisinde kullanılan kriptografik algoritmaların ömrü dolmaya yaklaştığında ataklara karşı açık hale gelir. Bu da şu anlama gelmektedir, kriptografik atak yapmaya yeteneği ve donanımı olan art niyetli kişiler, imzalanan belgenin içeriğini değiştirebilir, imzacı sertifikasını imza tarihinde geçerli veya geçersiz hale getirebilir, yani kontrolü tamamıyla eline alabilir. Arşiv imzanın gerekliliği tam da burada ön plana çıkmaktadır. ESXL imzanın arşivlenmesi aslında imzanın daha güçlü bir algoritma kullanılarak zarflanması, koruma altına alınması anlamına gelmektedir.

Elektronik belge yönetiminde dijitalleştirme ve e-Belgelerin arşivlenmesi önem arz etmektedir. Elektronik imza ile ilgili verdiğimiz bilgiler ışığında, e-belgenin arşivlenmesi aşamasında içeriğindeki elektronik imzanın da arşivlenmesinin çok önemli olduğu ve göz ardı edilmemesi gerektiği görülmektedir. TÜBİTAK Kamu Sertifikasyon Merkezi, 2006/13

sayılı Başbakanlık Genelgesi (Genelge, 2006) gereğince kamu kurumlarının, genel itibariyle EBYS sistemlerine entegre ettikleri elektronik imza uygulamalarının ilgili uluslar arası standartlara uygunluğunu test etmektedir. Bu kapsamda kurumlara ESXL imza tipinde imza oluşturmaları zorunlu tutulmaktadır ve uzun dönemli doğrulama için uygulamalarının arşivleme özelliğinin olması konusunda da bilgilendirilmektedir.

Kaynakça

5070 sayılı Elektronik İmza Kanunu (2004).

ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) (2013).

ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES) (2009).

ETSI TS 103 172, Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile (2012).

2006 / 13 sayılı Başbakanlık Genelgesi (2006).