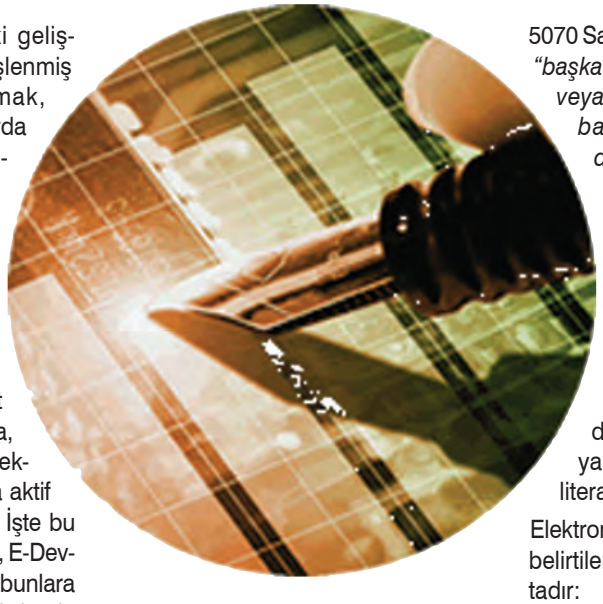
ELEKTRONİK İMZA

M. Birkan SARIFAKIOĞLU
Bilgisayar Yüksek Mühendisi-EMO Yönetim Kurulu Yedek Üyesi

Bilişim teknolojilerindeki gelişmelerin sonuçlarının, işlenmiş veriden bilgi oluşturmak, oluşturulan bilgiyi ilgili alanlarda kullanabilmek olduğu görülmektedir. Kuşkusuz finans-kapital çevreler ürettikleri mal ve hizmetleri daha rahat pazarlayabilmek için bu gelişme ihtiyacının günümüzdeki aktörleri olmuşlardır. Elektronik ortamda elde edilen bilgi ve bilginin internet ortamı üzerinden yayılmasında, kullanılmasında en az özel sektörün olduğu oranda kamu da aktif rol oynamaktadır, oynamalıdır. İşte bu noktada E-Ticaret, E-Dönüşüm, E-Devlet gibi kavramlar tartışılmaya, bunlara dayalı özel sektörde ve kamusal alanda çeşitli projeler üretilmeye başlandı. Bu tür sistemlerin amacı nihayetinde kişilere hizmet sunmaktır. Özel sektörde "mal veya hizmeti müşteriye pazarlamak", kamuda "ilgili kamu hizmetini yurttaşlara sunmak" olarak belirlenen bu eylemler kullanıcıya yöneliktir, diğer bir deyişle kişilere özeldir. Kişilere özel bu hizmetlerin elektronik ortamdaki güvenliği, doğruluğu ve gizliliğinin sağlanması gerekmektedir. E-İmza (*Elektronik İmza*) da bu ihtiyaçlardan doğmuş bir kavram olarak karşımıza çıkar.

E-İmza günlük hayatımızda her türlü süreçlerde kullandığımız geleneksel imzanın (ıslak imza) elektronik ortamda yerini almasının öngörüldüğü bir teknoloji olduğundan hukuki olarak bağlayıcı durumdadır. Ülkemizde de bilindiği gibi elektronik imza ile ilgili yapılan çalışmalar sonucunda 5070 Sayılı E-İmza Kanunu, 23 Ocak 2004 tarihinde 25355 sayılı Resmi Gazete'de yayımlandı ve 23 Ocak 2005 tarihinde de uygulanmaya başlandı. Bu teknolojinin gerekliliğini, uygulama alanlarını, yansımalarını ele alacağız ve yürürlükteki ilgili kanun üzerinde bazı değerlendirmeler yapacağız.



ELEKTRONİK İMZA NEDİR?

Bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozmadan (bilgiyi ileten tarafın oluşturduğu orjinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini, elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir seti ifade eder. Elektronik imza, günümüz teknolojisinde çeşitli şekillerde olabilmektedir. Halen kullanılan imza dosyaları, biyometri tekniği (kullanıcının parmak ya da el izi, göz retinası vb kişiye has özellikler) ile oluşturulan imzalar ve sayısal imzalar en çok bilinen ve tartışılan elektronik imza çeşitleridir.

5070 Sayılı E-İmza Kanunu'nda E-İmza *"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi"* temsil etmektedir. Bu tanımın karşılığı aslında sayısal imza olarak karşımıza çıkar. Yani bu kanunda kastedilen E-İmza kavramı günümüzde internet ortamında yaygınca kullanılan sayısal imzadan başka birşey değildir. Biz de bütünlüğü koruyabilmek için ilgili kanun ile aynı literatürü kullanacağız.

Elektronik imza, kullanıcılarına aşağıda belirtilen üç temel özelliği sağlamaktadır:

Veri Bütünlüğü: *Verinin izinsiz ya da yanlışlıkla değiştirilmesini, silinmesini ve veriye ekleme yapılmasını önlemek,*

Kimlik Doğrulama ve Onaylama: *Mesajın ve mesaj sahibinin iletiminin geçerliliğini sağlamak,*

İnkar Edilemezlik: *Bireylerin elektronik ortamda gerçekleştirdikleri işlemleri inkar etmelerini önlemek.*

BİLGİ GÜVENLİĞİ İÇİN E-İMZA YETERLİ Mİ?

Yukarıda belirttiğimiz gibi E-İmza bütünlüğü, kimlik doğrulamayı ve inkar edilememezliği sağlayabilmektedir. Fakat elektronik ortamdaki bilginin tam olarak güvenliği için bu özellikler yeterli olmamaktadır. Bilginin gizliliği de çok önemli bir parametre olarak karşımıza çıkmaktadır. Bundan dolayı Açık Anahtar Altyapısı (*AAA, Public Key Infrasturucture*) ile entegre bir E-İmza güvenlik sistemi öngürülmüştür.

AAA kullanarak E-İmza işlemi, asimetrik şifreleme algoritmaları (*RSA, DSA vs.*) kullanarak yapılan imzalama işlemlerdir. Burada yapıya göre şifreleme ve deşifreleme için açık (*Public Key*) ve özel anahtarlar (*Private Key*) kullanılır. Gönderici tarafından gönderilen bir mesaj özetleme algoritması (*SHA vs.*) ile özetlenir ve göndericinin özel anahtarı kullanılarak imzalama algoritmasından geçirilir. Elde edilen metin mesajla birlikte alıcıya iletilir. Alıcı göndericinin açık anahtarını kullanarak mesajın özetini elde eder ve özetleme algoritması ile elde ettiği mesajın özeti ile doğruluğunu sınayabilir.

AAA bileşenlerinden özel ve açık anahtarların güvenli olarak dağıtımı için Sertifika Sağlayıcıları sorumludurlar. Kişiler bu kurumlara birebir başvurarak, açık anahtar ve kimlik bilgilerinin bulunduğu Elektronik Sertifikalarına ve özel anahtarlarına sahip olurlar.

5070 SAYILI YASA'YA BAKIŞ

Yürürlükteki E-İmza Yasası'na göre, elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik kaydı ifade eden elektronik sertifikalar, kanuna uygun olarak faaliyette bulunacak Elektronik Sertifika Hizmet Sağlayıcılarından (*ESHS*) belirli bir ücret karşılığında temin edilmesi öngörülmüştür. Aynı şekilde kamusal alandaki hizmet sağlayıcı yani Kamu Sertifika Hizmet Sağlayıcısı olarak TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (*UEKAE*) belirlenmiştir.

Yine Yasa'da, elektronik imza oluşturmak üzere kullanılan yazılım veya donanımı tanımlamak için imza oluşturma araçları kavramı görülmektedir. Kanun'da güvenli elektronik imza oluşturma araçları için aşağıdaki özelliklerin sağlanması da şart koşulmuştur:

- *Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmaması.*
- *Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini sağlaması.*
- *Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesi, kullanılamaması ve elektronik imzanın sahteciliğe karşı korunması.*
- *İmzalanacak verinin imza sahibi dışında değiştirilememesi ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesi.*
- *Kullanılacak donanım/yazılımın özellikleri ve standartları Kurum tarafından yapılacak düzenlemelerle belirlenecektir.*

İlgili Yasa'da geçen düzenleyici sıfatındaki Kurum kelimesinden kasıt ise tanımlamalar kısmında Telekominikasyon Kurumu olarak belirlenmiştir.

SONUÇ

E-İmza'nın gerekliliğini ve ne olduğunu yeterince açıkladığımızı zannediyoruz. Her geçen gün elektronik ortamda daha açık bir deyişle internet ortamında kişiye özel hizmetlerin gizli ve bütün olarak verilebilmesi için E-İmza'nın önemi artmaktadır. Piyasa zaten bu teknolojiyi kullanmaya gayri resmi de olsa çok önceden başlamıştı. Çoğu zaman şu tartışmalara dahil olmuşuzdur. "Efendim kamusal alan daraltılmalıdır, vatandaşlar bürokrasinin yavaşlığından dolayı hizmet alamıyorlar, devlet küçülmelidir" vs. İşte bu noktada bizlerin yapması gerekenin bu tür E-Devlet, E-Dönüşüm uygulamaları ile bürokrasiyi yani yurttaşların kamusal alanda alacakları hizmetlerin hızlanmasını ve yaygınlaşmasını sağlamak diye düşünüyorum. Bu tür proje ve teknolojilerle demokratik merkeziyetçiliğin mümkün olduğunu, bozuk organizasyonların her birinde kamu olsun, özel olsun sorunların yaşanabileceğini, bu tür sorunların kamuya has şeyler olmadığını anlatabilmemiz gerekiyor.

E-İmza da bu tür projelerin anahtarı, bir anlamda giriş kapısı. Bu sistemi akademik, hukuki ve teknolojik olarak içselleştirmemiz, tartışmamız bizlere yararlar sağlayacaktır. Ülkemizde bu teknolojiyi kullanan gerek özel, gerekse kamusal alanda birçok proje ve firma var. Her geçen gün de artıyor. Örnek olarak güncel bir konu E-Seçim. Bildiğiniz üzere Kasım 2007'de genel seçimler var. Yine tahmin edeceğiniz gibi pusulalar, seçim listeleri, sandıklar havalarda uçuşacak. Muazzam zaman ve insan kaybı yaşanacak her zamanki gibi. ODTÜ Teknokent bünyesinde faaliyet gösteren Kale Yazılım Firması AR-GE kapsamında olarak Güvenli Uzaktan Elektronik Seçim Sistemi (GUESS) projesini geliştirmekte. Proje herhangi bir seçimin uzaktan (internet ortamından oy verme), gizli ve güvenli yapılmasını amaçlıyor. E-İmza (sayısal imza) kavramı projenin çok önemli bileşenlerinden bir tanesi, öyle ki kullanılan bir oyun, gerçek seçmen tarafından verildiği doğrulanacak ve sayım işlemlerinde kim tarafından verildiği matematiksel algoritmalar sayesinde saptanamayacak. Bu sayede hangi seçmenlerin nasıl oy kullandıkları belli olmayacak.

7-8 Aralık 2006'da ilk Ulusal Elektronik İmza Sempozyumu düzenlenecek. E-İmza'nın ulusal anlamda teknolojik, hukuki boyutlarının gözden geçirilmesi, uygulamaların değerlendirmesi, sorunların tartışılması ve her türlü fikir alışverişi için çok yararlı bir akademik ortamın olacağını sanıyoruz. Sempozyuma ilişkin detaylı bilgiyi www.eimza.org.tr adresinden edinebilirsiniz.