Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar[1]

ZÜLFÜKAR SAYGI
Uygulamalı Matematik Enstitüsü - Orta Doğu Teknik Üniversitesi,
06531, ANKARA, saygi@metu.edu.tr

SEZEN YEŞİL
Telekomünikasyon Kurumu, Bilgi Teknolojileri Dairesi
Yeşilırmak Sok. No:16 Demirtepe/ANKARA, syesil@tk.gov.tr

ÖZET : Açık Anahtar Altyapısı üzerinden sunulmakta olan e-imza, sahip olduğu kimlik doğrulama, bütünlük ve inkar edilemezlik özellikleri ile sanal ortamda gittikçe artan oranlarda ihtiyaç duyulan güvenlik ve hukuki açıdan geçerlilik ihtiyaçlarına cevap veren bir teknoloji olduğundan e-ticaret ve e-devletin başarıyla uygulanmasında önemli etkenlerden birisidir. E-imzanın kullanımının yaygınlaşması, elektronik imzaya karşı duyulan güvenin tesis edilerek toplumda kabul edilmesine de bağlıdır ve elektronik imzanın güvenliği, ele alınması gereken hususlar arasındadır. Bu nedenle elektronik imza güvenliğinde önemli olan algoritma ve parametrelerle ilgili bir araştırma yapılması gündeme gelmiştir. TÜBİTAK tarafından başlatılan "Kamu Kurumları Araştırma Projelerini Destekleme Programı" çerçevesinde, elektronik imzanın temelini teşkil eden kriptografik algoritmalar konusunda, Telekomünikasyon Kurumu ve ODTÜ-Uygulamalı Matematik Enstitüsü Kriptografi Bölümü işbirliği ile bir proje başlatılmıştır. Bu makalenin amacı, Telekomünikasyon Kurumu ile ODTÜ-Uygulamalı Matematik Enstitüsü Kriptografi Bölümü tarafından yürütülmekte olan "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" başlıklı proje çerçevesinde gerçekleştirilen bilimsel çalışmalar hakkındaki bilgileri paylaşmaktır.

ANAHTAR KELİMELER: Elektronik İmza, Açık Anahtar Altyapısı, İmzalama Algoritmaları

Research, Development and Implementation of a Public Key Infrastructure

ABSTRACT : Since electronic signature, which is based on Public Key Infrastructure, with its authentication, integrity and non-repudiation properties is a technology that enables security and legal recognition needed incrasingly in cyber world, it is one of the significant factors that have influence on the successful implementation of e-commerce and e-government. The diffusion of e-signature use depends also on assuring confidence in e-signature so that society accepts it and security of electronic signature is one of the issues to be dealt with. For that reason, it appeared to start a research for the algorithms and parameters, which are very important in the field of security for electronic signatures. In the frame of "Support Programme of the Public Associations Research Projects" kamu kurumlari arastirma projelerini destekleme programi (sen cevirirsin bunu)" founded by TÜBİTAK, a project has been started by the cooperation of Telecommunication Authorithy and Cryptography Department of the Institute of Applied Mathematics-METU(Middle East Technical University) about the cryptographic algorithms which are the basic elements of electronic signature. The aim of this paper is to share information about scientific studies within the project with title "Research, Development and Implementation of a Public Key Infrastructure", which is executed by Telecommunication Authorithy of Turkey and Cryptography Department of the Institute of Applied Mathematics-METU.

KEYWORDS : Electronic Signature, Public Key Infrastructure, Electronic Signature Algorithms

[1] Proje Adı: Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar
Yürüten Kurumlar: Telekomünikasyon Kurumu ve ODTÜ-Uygulamalı Matematik Enstitüsü Kriptografi Bölümü
Destekleyen Kurum: TÜBİTAK

Giriş

Elektronik ticaret ve elektronik devlet, geçtiğimiz yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel olarak dünya genelinde giderek artan ölçüde karşımıza çıkmaya başlayan kavramlardır. E-devlet ve e-ticaret uygulamaları, kaynakların etkin kullanımı, zaman ve mekana bağımlılığın azalması, açıklık, şeffaflık, hesap verilebilirlik, katılımcılık, yüksek rekabet, hizmet kalitesi ve verimlilik artışı gibi fırsatlar sunmaları nedeniyle çok önem arz etmektedir. Bu önemin farkında olan dünya ülkeleri e-devlet ve e-ticaretin gelişimini desteklemek için hukuki ve teknik altyapının hazırlanmasına öncelik vermektedirler.

Elektronik imza, elektronik ortamda muhatapların kesin olarak tespit edilmesini sağlaması ve güvensizlik duygusunu ortadan kaldırması sebebiyle e-devlet ve e-ticaret uygulamalarının gerçekleştirilmesinde hayati öneme sahip unsurlardan birisidir [1]. Bu nedenle, elektronik imza ile ilgili hukuki düzenlemeler dünya genelinde son yıllarda yürürlüğe konulmaya başlanmıştır. Avrupa Birliği 1999 yılında çıkarmış olduğu 99/EC /93/EC sayılı Elektronik İmza Direktifi ile elektronik imzaların hukuki açıdan tanınmasına imkan sağlamıştır [2]. Ülkemizde de, Elektronik İmza Kanunu 2004 yılından bu yana yürürlüktedir.

Elektronik imzanın ülkemizde kullanımının yaygınlaşması, elektronik imzaya karşı duyulan güvenin tesis edilerek toplumca kabul edilmesine de bağlı olduğundan Telekomünikasyon Kurumumunun (TK) denetleme mekanizmasını etkili bir şekilde çalıştırması çok önem kazanmaktadır. Bu nedenle, TK'nın teknolojiyi ve son gelişmeleri yakından takip etmesine ihtiyaç vardır. Söz konusu ihtiyacın bir uzantısı olarak, elektronik imzalara ilişkin algoritma ve parametrelerle ilgili çalışma yapılması gündeme gelmiş ve haberleşmede veri güvenliğini sağlayan kripto algoritmalarının tasarlanması, kripto algoritmalarının güvenilirliği ve bu algoritmaların kullanıldığı cihazların güvenliği konularında çeşitli araştırmalar yapmakta olan ODTÜ-Uygulamalı Matematik Enstitüsü (UME) Kriptografi Bölümü ile yapılan görüşmeler neticesinde TÜBİTAK tarafından başlatılan "Kamu Kurumları Araştırma Projelerini Destekleme Programı" çerçevesinde, elektronik imzanın temelini teşkil eden kriptografi ve kriptografik algoritmalar konusunda ortak çalışmalar yapılabileceği hususunda mutabakata varılmıştır. Söz konusu TÜBİTAK programının amacı, ülkemizde bilimsel çalışmalara proje desteği vererek teşvik sağlamak ve bu sayede ulusal bilimsel düzeyimizin geliştirilmesi ve bilimin ülkemiz kalkınmasındaki rolünün arttırılması olarak ifade edilmektedir. Bu doğrultuda, TK ve ODTÜ UME tarafından "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" projesi teklifi hazırlanmış ve TÜBİTAK'ın teklifi uygun bulması üzerine proje çalışmaları başlatılmıştır.

E-imzanın Türkiye'deki Gelişimi

5070 sayılı Elektronik İmza Kanunu 23 Ocak 2004 tarihinde yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiştir. Böylece, elektronik imza ile güvenliğin yanısıra, elektronik ortamda yapılan işlemlere hukuki bir zemin sağlanarak bu alanda önemli bir eksik tamamlanmıştır.

5070 sayılı Kanun ile, ikincil düzenlemeleri hazırlama ve elektronik sertifika hizmet sağlayıcılarının (ESHS) denetlenmesi görev ve yetkisi TK'ya verilmiştir. Söz konusu Kanunun 20 nci maddesi uyarınca TK'nın ilgili tüm taraflarla yaptığı çalışmalar neticesinde hazırlanan "Sertifika Mali Sorumluluk Sigortası Yönetmeliği" 26 Ağustos 2004 tarihli ve 25565 sayılı Resmi Gazete'de ve "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 6 Ocak 2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Daha sonra, söz konusu ikincil düzenlemelerin bazı hükümlerinde görülen lüzum ve Telekomünikasyon Kurulu'nun onayı üzerine kısmi değişiklikler yapılmıştır.

Mevcut durumda, dört adet ESHS TK'ya bildirimde bulunmuş ve yapılan incelemeler sonucunda uygun bulunmalarını müteakip faaliyete başlamışlardır. Söz konusu ESHS'ler TK'nın denetimi ve gözetimi altında faaliyetlerine devam etmektedirler. 2005 ve 2006 yılı içinde kamu ve özel sektörde bazı e-imza uygulamaları başlatılmış olup 2005 yılında 1402 adet nitelikli elektronik sertifika üretilmiştir. Mevcut durumda 21 adet kamu kurumu nitelikli elektronik sertifika temin etmiş durumdadır. Kamudaki ilk e-imza uygulaması Dış Ticaret Müsteşarlığı (DTM)'nın Dahilde İşleme Rejimi (DİR) Otomasyon Projesidir. Söz konusu proje kapsamında, ihracatçı firmalara nitelikli elektronik sertifika dağıtılmıştır. DİR uygulaması 01.02.2006'dan itibaren DTM tarafından zorunlu hale getirilmiştir [3, 4]. Ayrıca, Türksat A.Ş. tarafından yürütülmekte olan ve 2007 yılı içinde başlatılması öngörülen "E-devlet Kapısı" projesi kapsamında bazı hizmetlerin e-imzalı olarak sunulması gündemdedir. Söz konusu uygulamaların önümüzdeki yıllarda e-imzanın daha çok yaygınlaşmasına katkı sağlayacağı değerlendirilmektedir.

Genel Kavramlar

Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (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. Bu tanımda kullanılan "bilgi" sözcüğü, herhangi bir elektronik ortamda (elektronik, optik veya bunlarla sınırlı olmamak üzere, EDI (elektronik veri transferi), elektronik posta, telgraf, teleks veya telekopi de dahil olmak üzere benzer her türlü araçla) yaratılan, iletilen ya da depolanan ve daha sonra yeniden kullanılabilir şekilde geri çağrılabilen her türlü bilgiyi içermektedir. Elektronik imza her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir. Sayısal imza elektronik imzanın özel bir çeşidi olup, asimetrik şifreleme adı verilen teknik kullanılarak yaratılan bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühür olarak tanımlanabilir [5]. Bu çalışmada kullanılan "elektronik imza" kavramı 5070 sayılı Kanunda geçen haliyle "güvenli elektronik imza"dır. Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur ve münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır [6].

5070 sayılı Kanunda belirtilen hükümler ve kullanılan terminoloji dikkate alındığında ilgili şartların günümüzde "Açık Anahtar Altyapısı" (AAA) ile sağlanabileceği görülmektedir. AAA, sayısal imzanın dayandığı teknoloji olan açık anahtar şifrelemesinden (asimetrik şifreleme) doğmuştur. Açık anahtarla şifrelenen bir veri, sadece bu anahtarın gizli olanı kullanılarak deşifre edilebilir. Gizli anahtar kişiye özeldir ve sadece o kişi tarafından bilinir ve kullanılır. Bu anahtar çiftinin diğeri olan açık anahtar ise farklı şekillerde kullanıcılara duyurabilir. Duyuru işlemi, bir web sitesinden ya da e-posta ile yapılabilir. Gizli anahtarların, güvenliği yüksek ortamlarda üretilmesi ve korunmaları gereklidir. Bunun için akıllı kart gibi donanımlar kullanılır. Bir AAA, tipik olarak kök sertifika otoritesi, alt sertifika otoritesi, kayıt otoritesi, elektronik sertifikalar, güvenlik politikaları, güvenen taraf gibi bileşenlerden oluşur. Sertifika otoriteleri, gizli anahtarlara karşılık gelen açık anahtarların kişinin kimlik bilgileriyle ilişkilendirildiği elektronik sertifikaları üretir ve yayınlar. AAA kullanılarak oluşturulan bir elektronik imzanın kimden geldiğinin belirlenmesi, imzalanmış metnin elektronik ortamdaki doğruluğunun ve bütünlüğünün sağlanması, atılan imzanın imza sahibi tarafından inkar edilememesi sağlanmış olur [5, 7].

AAA terminolojisine göre, 5070 sayılı Kanunda geçen, imza doğrulama verisi açık anahtara, imza oluşturma verisi gizli anahtara, sertifika otoritesi ise ESHS'ye karşılık gelmektedir. İmza doğrulama verisi "elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler", imza oluşturma verisi ise "imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler" olarak tanımlanmaktadır [6].

Şifreleme, güvenli olmayan kanallar üzerinden haberleşmede veya verilerin güvenli olmayan ortamlarda saklanmasında kullanılan ve matematiksel fonksiyonlardan oluşan teknikler ve uygulamalar bütünüdür. Kullanılan teknikler ile oluşturulan şifreli veri, farklı bir forma dönüştürülerek anlaşılmaz hale getirilir. Şifrelemede; güvenlik düzeyi, işlevsellik, işlem metodları, performans ve kolay uygulanabilirlik gibi değerlendirme kriterleri önem arz etmektedir. Şifreleme ve şifre çözmede kullanılan, genelde rastgele bitlerden oluşan veri kümesine anahtar denir. Şifrelemede anahtar seçimi ve uzunluğu güvenlik açısından önemli bir rol oynamaktadır. Ayrıca gizli tutulması gereken bir anahtarın korunması da şifreli verilerin çözülememesi için kritik bir öneme sahiptir.

Elektronik imzanın teknik altyapısında yer alan bileşenlerden birisi olan, özetleme algoritmaları, girdi olarak kullanılan herhangi bir uzunluktaki veriyi işleyerek sabit uzunlukta bir özet değeri üreten tek yönlü algoritmalardır. Özetleme algoritmalarının en önemli özellikleri, birbirinden çok az farklı girdiler için dahi tamamen ayrı çıktılar üreterek çakışmaları önleyebilmeleridir. Özet değerinden girdi verilerine ulaşmak neredeyse imkansızdır. Özet değerleri, veri bütünlüğünün bozulup bozulmadığının kontrolü için kullanılmaktadır. En bilinen özetleme algoritmaları olarak SHA-1 (Secure Hash Algorithm-1 – Güvenli Özet Algoritması-1), RIPEMD-160 (RACE Integrity Primitives Evaluation-160 – RACE Bütünlük Asli Değerlendirme Mesaj Özeti-160) ve MD5 (Message Digest 5 – Mesaj Özeti 5) sayılabilir.

Bileşenlerden bir diğeri olan, imzalama algoritmaları, girdi verilerini ve imza atacak kişinin gizli anahtarını kullanarak asimetrik şifreleme yapan algoritmalardır. Esas olarak asimetrik şifreleme için geliştirilmiş bu algoritmalar, tam eşlemeli olduklarından dolayı şifreleme ve şifre çözme işlemlerinin rolleri karşılıklı olarak değiştirilerek sayısal imzalama için de kullanılmaktadır. İmzalama algoritmalarından bazıları RSA, DSA ve EDSA'dir.

RSA Algoritması

Açık anahtar sistemleri fikri ortaya atıldıktan sonra, 1978 yılında R. Rivest, A. Shamir ve L. Adleman tarafından tasarlanmış olan RSA algoritması [11], asimetrik şifrelemenin ve dolayısıyla elektronik imzanın temellerini oluşturan uygulamalardan birisidir. RSA, temel olarak büyük sayıların çarpanlara ayrılması problemi üzerine

yapılandırılmıştır. RSA kullanılarak anahtar çifti üretme, imzalama ve imza doğrulama aşamaları aşağıda verilmiştir:

Anahtar çifti üretme:

1) $Z_n = \{0, 1, 2, 3, \ldots, n - 1\}$ olmak üzere, asal ve birbirinden farklı p ve q sayıları seçilir ve $n = p \,.\, q$ hesaplanır,
2) $\Phi = (p - 1) \,.\, (q - 1)$ değeri hesaplanır,
3) $2 < e < \Phi$ ve $OBEB^2(\Phi, e) = 1$ olacak şekilde bir e tamsayısı seçilir,
4) $e \,.\, d \equiv 1 \pmod{\Phi}$ sağlayacak d değeri hesaplanır.
5) Özel anahtar: (n,d) ve açık anahtar: (n, e)'dir.

İmzalama:

1) M mesaj uzayı ve $m \in M$ olmak üzere bir m mesajı seçilir,
2) $t \in [0, n - 1]$ ve tamsayı olmak üzere $t = R(m)$ hesaplanır,
3) $s \equiv t^d \bmod n$ değeri hesaplanır,
4) s, m mesajının imzalanmış halidir.

İmza doğrulama:

1) İmzalayan kişinin açık anahtarı (n, e) öğrenilir,
2) $t \equiv s^e \bmod n$ hesaplanır,
3) $t \in M_R$ olduğu doğrulanır,
4) $m = R^{-1}(t)$ işleminden m'ye ulaşılır.

RSA algoritması üzerine yapılan saldırılardan en önemlisi, elde edilen açık anahtar kullanılarak gizli anahtara ulaşılmaya çalışılmasıdır. Saldırgan, n katsayısının çarpanları olan p ve q değerlerini hesaplamaya çalışır. Eğer bu değerler bulunursa özel anahtara ulaşılabilir. Buradaki en zor kısım n sayısını çarpanlarına ayırma işlemidir. Ancak n değerinin yeterince büyük olmaması veya p, q çiftinin ve ayrıca e değerinin iyi seçilmemesi durumlarında RSA'nın güvenli olduğu söylenemez.

DSA Algoritması

DSA, 1991 yılında NIST tarafından Elektronik İmza Standardı (DSS – Digital Signature Standard) olarak federal uygulamalarda kullanılmak üzere oluşturulmuştur [12]. DSA, ElGamal algoritmasının farklı bir versiyonu olup ayrık(kesikli) logaritma problemini temel almaktadır. İmzalama işleminde, özetleme algoritması olarak SHA-1 kullanılması gerekmektedir.

DSA ilk versiyonlarında anahtar uzunluğu en fazla 512 bit uzunluğunda olacak şekilde tasarlanmıştır. Ancak 2001 yılında yapılan değişiklikle p asal sayısının değerinin 2^{1023} ile 2^{1024} arasında yani 1024 bit uzunluğunda olmasına karar verilmiştir. DSA kullanılarak anahtar çifti üretme, imzalama ve imza doğrulama aşamaları aşağıda verilmiştir:

Anahtar çifti üretme:

1) $2^{1023} < p < 2^{1024}$ olacak şekilde p asal sayısı seçilir
2) $(p - 1)$'in asal böleni ve $2^{159} < q < 2^{160}$ olmak üzere q asal sayısı seçilir
3) $1 < h < p - 1$ ve $h^{(p-1)/q} \bmod p > 1$ olmak üzere h seçilir,
4) $g = h^{(p-1)/q} \bmod p$ hesaplanır.
5) $0 < x < q$ olmak üzere rastgele bir x tamsayısı seçilir,
6) $y = g^x \bmod p$ hesaplanır,
7) Açık anahtar (p, q, g, y), özel anahtar (x)'dir.

İmzalama:

1) M mesaj uzayı ve $m \in M$ olmak üzere bir m mesajı seçilir,
2) $m' = SHA\text{-}1\,(m)$ hesaplanır,
3) $0 < k < q$ olmak üzere k tamsayısı seçilir.
4) $r = (g^k \bmod p) \bmod q$ hesaplanır,
5) $s = (k^{-1}(m' + x \,.\, r)) \bmod q$ hesaplanır,
6) (r, s), m mesajının imzalanmış halidir.

İmza Doğrulama:

1) İmzalayan kişinin açık anahtarı (p, q, g, y) öğrenilir ve
2) $0 < r < q$ ve $0 < s < q$ olduğu doğrulanır,
3) $m' = SHA\text{-}1\,(m)$ hesaplanır,
4) $w = s^{-1} \bmod q$ hesaplanır,
5) $u = (w \,.\, m') \bmod q$ ve $v = (r \,.\, w) \bmod q$ hesaplanır,
6) $v = ((g^u y^v) \bmod p) \bmod q$ hesaplanır,
7) $v = r$ ise imza doğrulanmış olur.

İmzalamada hesaplanan s ve r değerinin 0'dan farklı olması gerekmektedir. Tersi bir durumda s^{-1} hesaplanamayacağından dolayı imza doğrulanamaz. Bu durumun oluşması ihtimali $(½)^{160}$ gibi oldukça küçük bir değer olsa da s ve r'nin sıfırdan farklı olup olmadığı kontrol edilmelidir.

DSA'nın, imza oluşturma performansı oldukça iyidir. Bazı hesaplamaların imzalama öncesinde yapılması dolayısıyla RSA ile karşılaştırıldığında avantajlı durumdadır. Ancak aynı durum imza doğrulama için geçerli değildir. RSA'da, imza doğrulama işlemleri daha çabuk bir şekilde gerçekleştirilebilmektedir. Verilerin bir kez imzalanıp birçok kez doğrulandığı göz önünde bulundurulursa RSA'nın bir adım önde olduğu düşünülebilir. Ancak bu durum ihtiyaçlar ve kullanılacak uygulamalar doğrultusunda değişebilir.

[2] OBEB: Ortak Bölenlerin En Büyüğü

Eliptik Eğri Algoritmaları

Eliptik eğriler, matematikcilerin 150 yıldır üzerinde çalıştığı bir konu olup bunların kriptografiye uygulanması 1985 yılında Neal Koblitz ve Victor Miller tarafından gerçekleştirilmiştir.

Eliptik eğriler, yaygın olarak kullanılan (RSA, DSA gibi) açık anahtar sistemlerinin benzeridir. Kriptografik güvenliği ayrık logaritma problemine dayanmakta olup en önemli özelliği, RSA ve DSA'nın sağladığı güvenliği daha kısa parametrelerle sağlamasıdır. Parametreler küçüldükçe yapılan işlemlerin süresi de azalmaktadır. Böylece, imzalama ve imza doğrulama daha hızlı bir şekilde gerçekleştirilmektedir. Eliptik eğri imzalama algoritmaları, kullanıldıkları varyasyonun (RSA, DSA, ElGamal gibi) güvenlik özelliklerini taşımaktadır. Burada seçilen eliptik eğriler ve kullanılan parametrelerin iyi bir şekilde seçilmesi güvenlik açısından önemlidir.

Eliptik eğri DSA (EDSA – Elliptic Curve DSA), DSA'nın eliptik eğri kullanılarak meydana getirilmiş bir benzeridir. 1992 yılında hazırlanmış ve 1999 yılında ANSI (American National Standards Institute – Amerika Ulusal Standartlar Enstitüsü) , daha sonra ise IEEE (Institute of Electrical and Electronics Engineers – Elektrik ve Elektronik Mühendisleri Enstitüsü) ve ISO (International Organization for Standardization – Uluslararası Standardizasyon Teşkilatı) tarafından standart olarak kabul edilmiştir.

EDSA'da kullanılan eliptik eğri algoritmaları ya büyük p asal tek sayıları ile elde edilen sonlu alanlar (Z_p) ya da 2 nin kuvvetleri ile elde edilen sonlu alanlar ($GF(2^m)$) üzerine uygulanır. Girdi olarak kullanılan veriler, SHA-1 ile özetlendikten sonra 160 bit olarak işlenir. EDSA'ya ilişkin parametreler ve açıklamaları aşağıda yer almaktadır:

1) q; p veya 2^m için alan uzunluğunu belirtir,
2) $a, b \in Z_p$ veya $a, b \in GF(2^m)$ olmak üzere a ve b sayıları aşağıdaki eliptik eğri eşitliklerini tanımlayacak şekilde seçilmiş parametreleri belirtir,

Z_p ve $p > 3$ için $E: y^2 = x^3 + ax + b$
$GF(2^m)$ ve $q = 2^m$ için $E: y^2 + xy = x^3 + ax^2 + b$

3) $G = (x_G, y_G)$ şeklinde E üzerinde bir G noktasını belirtir.

EDSA ile anahtar üretme, imzalama ve imza doğrulama aşamaları aşağıda verilmiştir [8]:

Anahtar üretme:

1) $1 \le d \le n-1$ olacak şekilde bir d sayısı seçilir,
2) $Q = (x_Q, y_Q) = dP$ olmak üzere Q noktası belirlenir,
3) Açık anahtar: (Q), özel anahtar (d)'dir.

İmzalama:

1) $m' = SHA\text{-}1\ (m)$ hesaplanır,
2) $1 \le k \le n-1$ olacak şekilde k sayısı seçilir,
3) $(x_1, y_1) = k.G$ şeklinde eliptik eğri üzerinde nokta hesaplanır,
4) x_1 tamsayı değerine çevrilerek x_1' hesaplanır,
5) $r = x_1' \bmod n$ hesaplanır. $r = 0$ ise ikinci adıma dönülür,
6) $s = k^{-1}(m' + d.r) \bmod n$ hesaplanır. $s = 0$ ise ikinci adıma dönülür,
7) m mesajı için imza (r, s) çiftidir.

İmza Doğrulama:

1) $1 \le r \le n-1$ ve $1 \le s \le n-1$ olduğu doğrulanır,
2) $m' = SHA\text{-}1\ (m)$ hesaplanır,
3) $c = s^{-1} \bmod n$ hesaplanır,
4) $u_1 = m'.c \bmod n$ ve $u_2 = r.c \bmod n$ hesaplanır,
5) $(x_1, y_1) = u_1G + u_2Q$ noktası bulunur,
6) x_1 tamsayı değerine çevrilerek x_1' hesaplanır,
7) $v = x_1' \bmod n$ değeri bulunur,
8) $v = r$ ise mesaj doğrulanmış olur.

TK tarafından hazırlanan ve yayımlanan, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Tebliğ)'in "Algoritmalar ve Parametreler" başlıklı 6. maddesinde imza oluşturma ve doğrulama verileri ile özetleme algoritmaları için uyulması gereken asgari şartlar şu şekilde belirlenmiştir:

a) İmza sahibinin imza oluşturma ve doğrulama verileri
   i. RSA için en az 1024 bit veya
   ii. DSA için en az 1024 bit veya
   iii. EDSA için en az 163 bit

b) ESHS'nin imza oluşturma ve doğrulama verileri
   i. RSA için en az 2048 bit veya
   ii. DSA için en az 2048 bit veya
   iii. EDSA için en az 256 bit

c) Özetleme algoritması
   i. RIPEMD – 160 veya
   ii. SHA – 1 veya
   iii. SHA-224 veya
   iv. SHA-256 veya
   v. WHIRLPOOL.

Proje ile İlgili Bilgiler

TK, imza oluşturma araçları, ESHS güvenliği, imzalama algoritmaları gibi elektronik imzanın güvenliği ile ilgili hususlarda güvenliğin sağlanması için 5070 sayılı Kanundaki denetim ve gözetim görevleri çerçevesinde çalışmalarını yürütmektedir. Bununla birlikte, ODTÜ UME Kriptografi Bölümü ile yapılan görüşmeler neticesinde, elektronik imza güvenliğinde, büyük öneme sahip olan hususlardan

biri olan algoritma ve parametrelerle ilgili olarak bir çalışma yapılması gündeme gelmiş ve TÜBİTAK tarafından başlatılan "Kamu Kurumları Araştırma Projelerini Destekleme Programı" çerçevesinde, elektronik imzanın temelini teşkil eden kriptografi ve kriptografik algoritmalar konusunda ortak çalışmalar yapılabileceği hususunda mutabakata varılmıştır. Bu doğrultuda, TK ve ODTÜ UME tarafından "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" projesi teklifi hazırlanmış ve 25/05/2005 tarihinde TÜBİTAK'a onay için sunulmuştur.

Ayrıca TK ile ODTÜ arasında, bilgi ve iletişim teknolojileri sektöründe bilgi güvenliği ve e-imza gibi e-devlet uygulamalarının başarıyla gerçekleşmesi için büyük öneme sahip hususlar başta olmak üzere daha geniş bir çerçevede işbirliği yapılması hususunda da mutabakata varılmıştır. Söz konusu hususlar dikkate alınarak hazırlanan işbirliği protokolü 01/03/2006 tarihinde ODTÜ Rektörlüğü ile TK Başkanlığı tarafından imzalanmış ve yürürlüğe girmiştir.

Onay için başvurulan tarihten yaklaşık 1 yıl sonra, TÜBİTAK'ın 08/06/2006 tarihli yazısı ile "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" konulu proje önerisinin taraflarınca değerlendirilerek desteklenmesine karar verildiği belirtilmiş ve 01/07/2006 tarihinden itibaren de proje çalışmaları resmen başlatılmıştır. 2 yıllık bir süresi olan projenin bitiş tarihi ise 01/07/2008 olarak belirlenmiştir.

Projenin amaçları; elektronik imzada kullanılan RSA, DSA ve EDSA gibi algoritmalardaki gelişmeleri yakından takip ederek bunlarla üretilen anahtarların güvenilirliklerini test edecek ve sınıflandırabilecek araçların, yazılımların geliştirilmesi ve açık anahtar altyapıları konusunda bir referans sistem oluşturulması, böylece TK'nın denetleme görevini daha etkin şekilde yerine getirmesine yardımcı olacak araçların geliştirilmesidir.

Belirtilen amaçlar doğrultusunda yürütülmekte olan bu projenin aşamaları aşağıdaki gibi özetlenebilir:

1. Elektronik imza ve uygulamaları konusunda literatür devamlı takip edilmekte, uygulamada kabul gören kriptolojik esasları incelemek, var olan açık kodlu yazılımlar ve örnek uygulamaları inceleyerek bir kütüphane oluşturmak.
2. Elektronik imza uygulamalarında kullanılan RSA, DSA ve EDSA algoritmalarının uygulama yazılımları tarafından kullanılabilecek modüller halinde uyarlama yapmak ve yazılım kodları geliştirmek.
3. Geliştirilen yazılım modüllerince üretilen anahtarları test edebilecek ve sınıflandırabilecek test algoritmaları ve ilgili yazılım modüllerini sistematik bir yapı içinde geliştirmek.
4. Geliştirilen RSA, DSA ve EDSA yazılım modüllerini kullanarak ODTÜ UME bünyesinde kurulacak referans sistemin sistem yazılımını geliştirmek ve donanımla entegrasyonunu sağlamak.
5. Sistemin kullanımında deneyim sahibi olmak ve sistemin demonstrasyonu amacıyla Enstitü bünyesinde bir pilot uygulama yapmak.
6. Sistem yazılımına tasarım fazında kazandırılacak özellikler yardımıyla, zaman içerisinde gözlenecek teknolojik gelişmelere göre tasarlanacak yeni ve değişik algoritmaların ve tekniklerin denenmesine imkan veren, aynı zamanda e-imzayı ilgilendiren her konuda araştırma ve eğitim çalışmalarının da yapılabildiği bir platform özelliği kazandırmak.

Sonuç

Elektronik imzanın ülkemizde kullanımının yaygınlaşması, elektronik imzaya karşı duyulan güvenin tesis edilerek toplumda kabul edilmesine de bağlıdır. Bu nedenle, bir çok faktörle ilişkili olan elektronik imza güvenliğinin sağlanması için çeşitli çalışmalar yürütülmektedir. Bu çalışmalardan birisi olarak, "Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar" konulu proje TK ve ODTÜ UME işbirliği ile gerçekleştirilmektedir. Söz konusu proje, TÜBİTAK'ın "Kamu Kurumları Araştırma Projelerini Destekleme Programı" çerçevesinde desteklenmektedir. 2 yıllık bir süresi olan projenin başlangıç tarihi Temmuz 2006 olarak belirlenmiştir.

Proje ile, elektronik imzada kullanılan algoritmalardaki gelişmeleri yakından takip ederek bunlarla üretilen anahtarların güvenilirliklerini test edecek ve sınıflandırabilecek araçların, yazılımların geliştirilmesi ve açık anahtar altyapıları konusunda bir referans sistem oluşturulması sağlanmış olacaktır. Elektronik imza güvenliğine katkıda bulunacak olan söz konusu proje ile, e-dönüşüm projelerinin başarısı da dolaylı yoldan etkilenmiş olacaktır.

Proje sürecinde ortaya çıkan teknik bilgi birikimi ve araçlar düzenlenecek seminer ve konferanslarda kamu ve özel sektör ile paylaşılacaktır. 2006 Aralık ayında düzenlenen Ulusal Kriptoloji Sempozyumu [9] ve Ulusal Elektronik İmza Sempozyumu [10] bunlara örnek olarak verilebilir.

Teşekkür

Bu çalışmada emeği geçen tüm proje ekibine teşekkürlerimizi sunarız.

Kaynaklar

[1] İlter, K., Türkiye'de Bilgi Toplumu'na Geçiş Sürecinde Telekomünikasyon Kurumu'nun Rolü, Önemi ve Yapılması Gereken Düzenlemeler, Telekomünikasyon Kurumu Uzmanlık Tezi, 2005

[2] Dumortier, J. , Kelm, S., Nilsson, H., Skouma, G., Eecke, P.V., "Legal and Market Aspects of Electronic Signatures", Study for European Commission, icri, Katholieke Universiteit Leuven, 2003

[3] Telekomünikasyon Kurumu 2005 Yılı Faaliyet Raporu, 2006

[4]TÜBİTAK, UEKAE-Kamu Sertifikasyon Merkezi, http://www.kamusm.gov.tr/net/bilgiler/kurumsal/kurumsalmusteriler.jsp, 06.09.2006

[5] İnalöz A., Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Telekomünikasyon Kurumu Uzmanlık Tezi, 2003

[6] 5070 Sayılı Elektronik İmza Kanunu

[7] Sağıroğlu, Ş., Alkan, M., Her Yönüyle Elektronik İmza (E-İmza), Grafiker Yayınları, ISBN:975-6355-23-9, Ankara, 2005

[8] Sarıkaya, K.S., Elektronik İmza Güvenliği ve Güvenlik Standartları Çerçevesinde Düzenleyici Yaklaşımlar, Telekomünikasyon Kurumu Uzmanlık Tezi, 2005

[9] http://www.iam.metu.edu.tr/sempozyum

[10] http://www.eimza.org.tr/

[11] R. Rivest, A. Shamir ve L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February 1978

[12] FIPS PUB 186, Digital Signature Standard, Federal Information Processing Standards Publications 186, U.S. Department of Commerce, National Institute of Standards and Technology (NIST), National Technical Information Service, Springfield, Virginia, 1994. http://www.itl.nist.gov/fipspubs/fip186.htm