Bir Sanal Noter Uygulamasının Teknolojik ve Hukuki Gereksinimleri

Dursun AKÇEŞME, A.Çoşkun SÖNMEZ

Abstract— **Nowadays, internet has become an inseparable part of our lifes. Every daily activities are being modeled under the name of e-proccess and with in the acceptance of e-sign law, e-state projects took part of virtual environment. This progress has arised the question wheter the public notary services can be realised in virtual environment.**

In this study how public notary services can be realized is examined. As a result of this study, it's decided that a big part of public notary services can be implemented in virtual environment with in the consideration of technological and judicial requirements.

Keywords— **Digital Certificate, Digital Notarization, Digital Signature, Private Key, Public Key, Public Key Infrastructure.**

I. GİRİŞ

1970'lerde entegre devrelerinin icadı ile başlayan elektronikleşme süreci çok kısa sürede hayatın her alanına girmiştir. Hiç şüphe yoktur ki bu sürecin en önemli gelişmesi "internet"tir. Elektronik postayla başlayan bu süreç, internet bankacılığı ve elektronik ticaret ile doruğa ulaşmıştır. Bilişim dünyasında tüm bu gelişmeler ile birlikte sanal dünyada güvenliğin sağlanması da gitgide zorlaşmıştır.

Müthiş bir ivmeyle gelişen internet teknolojisi ile günlük hayatta yapılan işlerin birçoğu e-işlem adı altında internet ortamında modellenmiştir. Tüm bu gelişmeler beklentileri arttırmış kamu kurumlarını tek bir çatı altında birleştiren e-devlet kavramının doğmasına neden olmuştur. E-devlet projelerinde mutlak güvenliğin sağlanması gerekmektedir. Bu sebeple e-devlet projelerinde veri bütünlüğü ve veri gizliliği sağlanmalı, bunların yanında kimlik doğrulaması yapılabilmeli ve yapılan işlemlerin inkâr edilmemesi sağlanmalıdır.

Yukarıdaki bilgiler ışığında; kamu kurumları, işletmeler ve bireyler ile sürekli etkileşim halinde olan noterlere de sanal ortamda ihtiyaç duyulmuştur.

Noterlerin vermiş olduğu hizmetlerin tümünün sanal ortama taşınması hukuki mevzuattan ve yapılacak işin niteliğinden dolayı mümkün değildir[1]. Fakat noterlerin bazı hizmetlerinin sanal ortama taşınması, mevcut teknolojik koşullar ve hukuki düzenlemeler ile mümkün olabilmektedir. Bildiri içeriğinde, noterlerin sanal ortamda hizmet verebilmesi için, teknolojik gereksinimi açısından Açık Anahtar Altyapısı üzerine kurulan sayısal imza ve hukuki geçerlilik bakımından da 23 Temmuz 2004'te kabul edilen 5070 Sayılı Elektronik İmza Kanunu esas alınmıştır.

D. AKÇEŞME ve A.C. SÖNMEZ; Yıldız Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul dursun.akcesme@halkbank.com.tr, acsonmez@ce.yildiz.edu.tr

II. NOTER KURUMU

Noterler kamuya hizmet veren çok önemli kurumlardır. Toplum nazarında güven makamı olarak bilinirler. Yaptıkları her işlemde güvenliği maksimize etmeye çalışırlar. Herhangi bir noter işleminde temel olarak dört koşul yerine getirilir. Bunlar; noter işlemine konu olan belgenin içeriğinin tahrif edilemeyeceğinin(veri bütünlüğü), belgenin gizliliğinin muhafaza edileceğinin(veri gizliliği), işlemi yapan kişinin nüfus cüzdanı, ehliyet, pasaport vb. ile kimlik tespiti yapılacağının(kimlik doğrulama ve onaylama), inkâr edilmemesi için işlemi yapan kişinin ıslak imzasının alınacağının(inkâr edememe) güvence altına alınmasıdır. Tüm bu koşullar noterlerin yapmış olduğu her işlemde yerine getirilir. Görülüyor ki, bir Sanal Noter Uygulamasının gerçekleştirilebilmesi için yukarıda verilen,

- Veri Bütünlüğü
- Veri Gizliliği
- Kimlik Doğrulama ve Onaylama
- İnkâr Edememe

koşullarının sağlanması gerekmektedir. Aksi halde, Sanal Noter Uygulamasından söz edilemez.

Teknolojik olarak, Açık Anahtar Altyapısı üzerine kurulan sayısal imza ile veri gizliliği dışında, veri bütünlüğü, inkâr edememe, kimlik doğrulama ve onaylama sağlanabilmektedir[2]. Veri gizliliği için aşağıda verilen modelde görüleceği gibi kriptolojik yöntemlerden yararlanılmaktadır.

Hukuki açıdan, 5070 Sayılı Elektronik İmza Kanunu, nitelikli elektronik sertifika kullanılarak yapılan işlemleri hukuki olarak geçerli kılmaktadır.

III. TEKNOLOJİK GEREKSİNİMLER

A. Açık Anahtar Altyapısı(AAA)

Sanal Noter teknolojik altyapısı, Açık Anahtar Altyapısı üzerine kurulu olan sayısal imza ile sağlanmaktadır. Açık Anahtar Altyapısı'nın temel görevi; elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar ve cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır[2]. Bu altyapı içerisinde gizlilik, bütünlük, inkâr edememe, kimlik doğrulama ve onaylama işlevleri sağlanarak sanal ortam güvenli hale getirilir.

AAA kriptoloji bilimi üzerine kurulmuş bir yapıdır. Kriptoloji bilimi günümüzde anahtar tabanlı şifreleme üzerine yoğunlaşmıştır. Anahtar tabanlı şifreleme iki çeşittir. Bunlar simetrik ve asimetrik şifrelemedir.

Simetrik şifreleme ve asimetrik şifreleme yöntemleri algoritma bağımsız şifreleme yöntemleridir. Algoritma bağımlı şifreleme yöntemleri günümüzde tercih edilmemektedir. Bunun sebebi, algoritmanın deşifre olması durumunda tüm sistemin güvenliğinin tehlikeye girmesidir.

En eski şifreleme yöntemlerinden olan Sezar Şifreleme algoritma bağımlı şifrelemeye en güzel örnektir. Sezar Şifreleme, her karakteri kendisinden sonra gelen üçüncü karakteri alarak şifreler, deşifre etmek için de şifrelenmiş verinin her karakterinin kendisinden önce gelen üçüncü karakteri alarak metni deşifre eder[2].

Matematiksel olarak;

E(M) = (M+3) mod 29 = C D(C) = (C–3) mod 29 = M

E = Şifreleme işlemi D = Deşifre İşlemi
M = Şifrelenecek Metin C = Şifrelenmiş Metin
C = Şifrelenmiş Metin M = Deşifre Edilmiş Metin

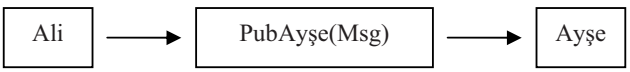
şeklinde ifade edilir. Fonksiyonda oluşan verinin 29 mod alınma sebebi alfabemizde 29 harf bulunmasıdır[2]. Bu şekilde bir şifreleme yapan sistemin algoritması mutlak suretle gizli kalmalıdır. Algoritmanın deşifresi tüm sistemi tehlikeye sokar.

Simetrik şifreleme yöntemlerinde metni şifreleme ve deşifre etmek için bir gizli anahtar kullanılır. Kullanılan bu anahtarı şifreli haberleşmek isteyen her iki tarafta bilmelidir. Sistemin güvenliği gizli anahtarın büyüklüğü ile doğru orantılıdır. Simetrik şifreleme yönteminde, IBM tarafından geliştirilmiş olan DES(Data Encryption Standart) algoritması standart olarak kabul edilmektedir.

Asimetrik şifreleme yönteminde ise, veriyi şifrelemek ve deşifre etmek için farklı anahtarlar kullanılmaktadır. Bu iki anahtar üretilirken aralarında matematiksel bir bağ kurularak üretilir. Bu anahtarlar açık anahtar(public key) ve gizli anahtar(private key) olarak isimlendirilir. Bir anahtarın şifrelediği metni ancak ikizi olan diğer anahtar deşifre edebilir. Burada, açık anahtar herkes tarafından bilinen anahtardır. Gizli anahtar ise sadece sahibi tarafından bilinen ve gizli tutulması gereken anahtardır. Asimetrik şifrelemede, kullanılan algoritmanın bilinmesinin simetrik şifrelemede olduğu gibi hiçbir önemi yoktur.

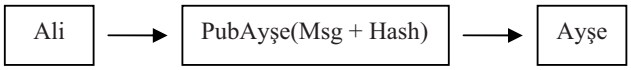
AAA asimetrik şifreleme yöntemini kullanmaktadır. AAA da şifreli haberleşmek isteyen her bireyin açık ve gizli anahtarı vardır. Bu iki anahtarın nasıl kullanıldığını açıklayalım. Ali Ayşe ile AAA ile haberleşmek istemektedir. Her ikisi de birbirlerinin açık anahtarlarına erişebilmektedirler. Aşama aşama AAA'nın işlevlerini görelim.

Ali Ayşe'ye gizliliği sağlanmış bir mesaj göndermek istediğinde; Ali göndereceği mesajı Ayşe'nin açık anahtarı ile şifreleyerek Ayşe'ye gönderir. Gönderim esnasında mesaja erişilse dahi şifrelenmiş olduğundan mesaj anlaşılamaz. Şifrelenmiş mesajı alan Ayşe kendi gizli anahtarı ile şifreli mesajı deşifre eder ve mesaja ulaşır. Bu örnekte anlaşıldığı üzere AAA ile gizlilik sağlanmış olur (Şekil 1).



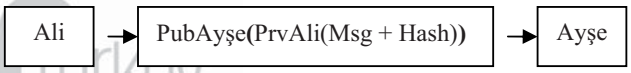
Şekil 1. AAA Gizlilik İşlevi

Ali Ayşe'ye gizliliği ve veri bütünlüğü sağlanmış mesaj göndermek istediğinde; Ali Ayşe'ye mesajı göndermeden önce hash algoritması (MD5, SHA–1, SHA–2 vb.) ile mesajın özetini çıkartır. Bu algoritma mesajın uzunluğu ne olursa olsun sabit uzunlukta ve mesajı ifade eden eşsiz bir özetini çıkartır. Bu özetten mesajı elde etmek mümkün değildir. Mesajın özeti çıkartıldıktan sonra, mesaj ve mesajın özeti Ayşe'nin açık anahtarı ile şifrelenir. Ayşe'ye şifrelenmiş mesaj gönderilir. Şifrelenmiş mesajı alan Ayşe kendi gizli anahtarı ile şifreli mesajı deşifre eder ve mesaja ulaşır. Daha sonra hash algoritması ile mesajın özetini elde eder, kendi elde etmiş olduğu değer ile gelen mesaj özetini karşılaştırır. Her iki özet de aynı ise Ayşe mesajın yolda değişmediğini anlar. Bu örnekte AAA ile gizlilikle beraber veri bütünlüğü de sağlanmış olur(Şekil 2).



Şekil 2. AAA Veri Bütünlüğü İşlevi

Ali Ayşe'ye gizliliği ve bütünlüğü sağlanmış, kimlik doğrulama ve onaylama yapılabilen ve inkâr edilemeyen bir mesaj göndermek istediğinde; Ali Ayşe'ye mesajı göndermeden önce hash algoritması ile mesajın özetini çıkartır. Mesaj ve özetini kendi gizli anahtarı ile şifreler, daha sonra şifreli mesajı Ayşe'nin açık anahtarı ile şifreler. Son şifrelenmiş mesajı Ayşe'ye gönderir. Şifrelenmiş mesajı alan Ayşe önce kendi gizli anahtarı ile mesajı deşifre eder. Veri gizliliği bu aşamada sağlanmış olur. Daha sonra Ali'nin açık anahtarı ile şifrelenmiş ikinci mesajı deşifre eder. Eğer Ali'nin açık anahtarı bu şifreli mesajı deşifre ederse AAA ile kimlik doğrulama ve onaylama sağlanmış olur. Bununla beraber bu şifreli mesajı sadece Ali'nin gizli anahtarı oluşturabileceğinden AAA ile inkâr edememe sağlanmış olur. Sonraki aşamada da özet değer ile hash algoritma sonucu karşılaştırılarak veri bütünlüğü de sağlanmış olur(Şekil 3).



Şekil 3. AAA Kimlik Doğrulama ve İnkâr Edememe İşlevi

B. Sayısal İmza

Sayısal İmza, Sanal Noter Uygulamasının en önemli bileşenidir. Başlangıçta belirtildiği üzere, noter kurumunda yapılan her işlemde yerine getirilen veri bütünlüğü, inkâr edememe, kimlik doğrulama ve onaylama sayısal imza ile yerine getirilir. Fakat sayısal imza haberleşmede gizliliği sağlamaz[2]. Bunun sebebi AAA'da haberleşmede gönderilecek mesaj şifrelenirken, sayısal imza yapısında sadece mesajın hash algoritmasından elde edilen özeti şifrelenir. Bu şifrelenmiş özet de sayısal imzayı oluşturur.

Sayısal İmza 5070 Sayılı Elektronik İmza Kanunu'ndaki tanımıyla; "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar" şeklindedir[3].

AAA'da haberleşmek isteyen her birey ve kurumun açık ve gizli anahtarı vardır. Sayısal imza'da AAA üzerine kurulmuş bir yapı olduğundan, sayısal imza ile haberleşmek isteyen her

bireyin açık anahtarını içeren elektronik sertifikası ve gizli anahtarını muhafaza eden token ya da akıllı kartı vardır. Elektronik sertifikalar sahibinin sanal kimlik kartlarıdır. Bu sanal kimlik kartlarının yönetimini sağlayan bir yapı daha vardır. Bu yapıda Elektronik Sertifika Hizmet Sağlayıcısıdır(ESHS).

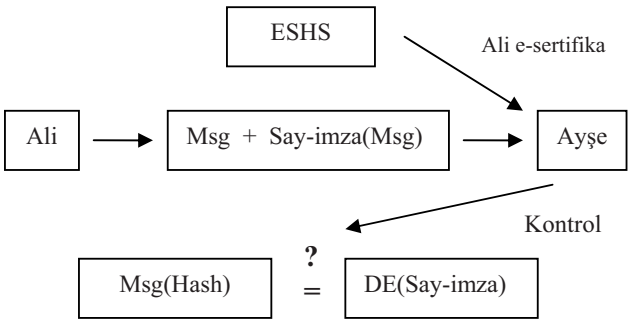
Ali Ayşe'yle sayısal imza kullanarak haberleşmek istediğinde ilk olarak hash algoritmasını kullanarak göndereceği mesaj özetini çıkartır. Ondan sonra içinde gizli anahtarı bulunan usb token ya da akıllı kartı ile mesajın özetini şifreler ve mesajla birlikte Ayşe'ye gönderir. Mesajı alan Ayşe ESHS'dan içinde Ali'nin açık anahtarı bulunan elektronik sertifikasını alır. Daha sonra buradaki açık anahtar ile sayısal imzayı deşifre eder. Mesajı da hash algoritmasından geçirerek mesajın özetine ulaşır. Deşifre ettiği sayısal imza ile özet aynı ise bu mesajı Ali'nin imzaladığını anlar(Şekil 4). Bu senaryo da elektronik sertifikalar, inkâr edilememeyi, kimlik doğrulama ve onaylamayı sağlamaktadır. Görülüyor ki ESHS'lardan alınan bilgi esas kabul edilmiştir. Bu kabul 5070 Sayılı Elektronik İmza Kanunu ile güvence altına alınmıştır.

C. Elektronik Sertifikalar

Elektronik sertifikalar, kişinin kimlik bilgisi ile kişinin açık anahtarını birbirine bağlayan elektronik kayıtlardır. Elektronik sertifikaların görevi kişinin kimliğini doğrulamak, inkâr edilememeyi sağlamaktır. 5070 Sayılı Kanun ile elektronik sertifikalar kayıtlı bir ESHS tarafından verilirse nitelikli elektronik sertifika(NES) olarak tanımlanırlar. Bu sertifikalar tektir, başka bir kişiye bağlı olamaz, yalnızca bağlı olduğu kimliği ifade eder.

Nitelikli elektronik sertifikalar Uluslararası Telekom Birliği standartlarına göre X.509 standardında tanımlanırlar[4]. Standart bir nitelikli elektronik sertifika örneği şekil 5'te görülmektedir.

Nitelikli elektronik sertifikaların bir ömrü vardır. Bu sürenin sonunda sertifika yenilenir veya iptal edilir. Hiçbir zaman hiçbir ESHS tarafından, süresiz nitelikli elektronik sertifika üretimi yapılamaz. Bu sertifikaların üst sınırı ülkemizde Telekomünikasyon Kurumu tarafından belirlenir. Bu sürenin sonunda yenilenmelidirler. Nitelikli elektronik sertifika sahibi, gizli anahtarını içeren donanımını kaybetmesi ya da benzer bir durumda nitelikli elektronik sertifikası iptal edilir. Sertifikalar geçersiz olsa bile, sertifikanın geçerli olduğu dönemlerde yapmış olduğu işlemlerde gelecekte ihtilaf oluşması ihtimaline karşı, sertifikayı üreten ESHS tarafından geçersiz olmasından sonra bile arşivlenirler.



Şekil 4. Sayısal İmza ile Haberleşme

Sertifika Seri No	**59014325431**
Sertifika Sahibinin Kimlik Bilgileri	**Dursun Akçeşme**
Sertifika Geçerlilik Başlangıç Tarihi	**10 Şubat 2008 14.00**
Sertifika Geçerlilik Bitiş Tarihi	**10Eylül 2009 14.00**
Sertifikanın Kullanım Amacı	**Test Kullanımı**
Kullanılacak Algoritma	**Sha1RSA**
Sertifika Sahibinin Açık anahtar Bilgisi	**65 94 73 58 59 ef 8e 6f 1e 95 22 a7 c9 67 2e a5 d4 ee 2c 1c**
Yayınlayan ESHS	**XXXX Kurumu**
ESHS Sayısal İmzası	**4t 4a 31 e8 9y 3d fa 3e 0a b7 dd 70 71 c7 51 7c 45 83 4f 11**

Şekil 5. Nitelikli Elektronik Sertifika

D. Elektronik Sertifika Hizmet Sağlayıcı(ESHS)

ESHS'lar bireylere veya kurumlara nitelikli elektronik sertifika veren ve vermiş oldukları sertifikaların yönetim işini üstlenen güven makamlarıdır. ESHS'lar temel olarak kayıt makamı, sertifika makamı ve kök sertifikadan oluşur. Kayıt makamı bireyin başvuru yaptığı, nitelikli elektronik sertifika taleplerinin alındığı ve ilgili kişinin kimlik doğrulamasının yapıldığı makamdır. Sertifika makamı ise eşsiz bir sertifika tanımlamasının yapıldığı ve tanımlanan sertifikayı kendi sayısal imzası ile imzalayarak yayınlayan makamdır. ESHS'ların temel görevleri;

- Nitelikli Sertifika Üretimi
- Zaman Damgası Hizmeti
- Nitelikli Elektronik Sertifikaları bir dizinde yayınlama (Örnek olarak LDAP dizini)
- SIL(CRL)(Sertifika İptal Listesi) yayınlama
- ÇİSDUP(OCSP)(Çevrim İçi Sertifika Durum Protokolü) hizmeti
- Sertifika Mali Sorumluluk Sigortası Yaptırma
- Kanunda belirtilen Sertifika ilkeleri(Sİ) ve Sertifika Uygulama Esaslarına göre hizmet verme

- Tüm bu hizmetlerini sürekli kılmak

Ülkemizde olduğu gibi bir ülkede nitelikli elektronik sertifika veren birden fazla kurum olabilir. Bu durumda sertifika makamlarının hepsi kök sertifika'ya bağlı olur. Her sertifika makamının elektronik sertifikasını da kök sertifika imzalar. Sertifika makamları kendi aralarında çapraz sertifikasyon yaparak iletişim kurarlar.

ESHS'ların hizmetlerinden en önemlilerinden biride iptal veya bir sebepten dolayı geçersiz kılınan sertifikaların yayınlandığı SIL listelerini belirli aralıklarla yayınlamaktır. ESHS, yayınladığı listeyi kendi sayısal imzasıyla imzalar. Sertifikanın geçerliliği kontrol edildiğinde, ESHS'ın yayınladığından emin olmak için sayısal imzalar mutlaka kök sertifikaya ulaşıncaya kadar doğrulanmalıdır. Geçersiz kılınan sertifikaları anlık öğrenmek için ise OCSP hizmetinden yararlanılır, anlık olarak sertifikanın durumu hakkında sayısal imza ile imzalanmış şekilde sertifikanın geçerliliği hakkında bilgi verir. SIL listesinde olduğu gibi bu işlemde de kök sertifikaya ulaşıncaya kadar doğrulama yapılmalıdır.

E. Sayısal İmza Donanımları

Sayısal imzayı oluşturabilmek için kişinin gizli anahtarının bir donanımda tutulması gereklidir. AAA tabanlı uygulamalarda, gizli anahtar bilgisi, bir kere yazılabilen ve donanımın içerisinden çıkartılamayan akıllı kartlar veya usb token'larda tutulurlar. Bu donanımların güvenlik seviyesi minimum EAL–4 uluslararası standardında olmalıdır.

Her iki donanım da PIN(şifre) bilgisi ile korunur. İşlem yapılmak istendiğinde sadece sahibinin bildiği PIN bilgisi girilerek işlem yapılır. Aksi halde işlem yapılması mümkün değildir. PIN bilgisi girildikten sonra gizli anahtar verisi karmaşık matematiksel fonksiyonlardan geçerek üretilir.

F. Bir Sanal Noter Uygulamasında Gizliliğin Sağlanması

Bir Sanal Noter Uygulamasında olması gereken veri bütünlüğü, kimlik doğrulama ve onaylama, inkâr edememe koşulları yukarıda ki bilgiler de görüldüğü gibi sayısal imza kullanılarak yerine getirilebilir. Gizlilik koşulu için kriptolojik yöntemlerden yararlanılır. Kriptolojik bir yöntem olan SSL(Secure Socket Layer) bu koşulu yerine getirir.

SSL çalışma prensibi; A kişisi B kişisine mesaj göndermek istediğinde sadece B kişisinin sahibi olduğu gizli bir anahtarın eşi olan açık anahtarla mesajı şifreler, dolayısıyla sadece şifrelenmiş mesajı B kişisinin sahibi olduğu gizli anahtar açabileceğinden mesaja erişilse bile deşifre edilemez. Bu kriptolojik yöntem ile gizlilik sağlanmış olur. Sonuçta SSL ve sayısal imza kullanılarak, sanal ortamda bir noter işlemi için gerekli tüm koşullar yerine getirilmiş olur.

IV. SAYISAL İMZA İLE YAPILABİLECEK NOTERLİK İŞLEMLERİ

Daha öncede değinildiği gibi bir noterin tüm işlevlerini sanal ortama taşımak mümkün değildir. 5070 Sayılı Elektronik İmza Kanunu'nda yer alan "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli Elektronik İmza ile gerçekleştirilemez." [3] ifadesine göre noterlerin yapmış olduğu işlemlerin bazıları sayısal imza kullanılarak yapılamaz.

Şekil 6. Sayısal İmza Donanımları

Fakat, yapılacak hukuki düzenlemeler(yönetmelik, tebliğ, genelge vb) ile, sayısal imza kullanılarak sanal ortamda aşağıdaki noter işlemleri hukuki normlara uygun, teknolojik olarak her türlü bilgi güvenliği sağlanmış olarak yapılabilir.

- Elektronik zaman damgası vurma
- Kendisine gönderilen elektronik belgelerdeki Elektronik İmza ve tarihi onaylamak
- Elektronik belgelerin saklanması ve istendiğinde belgelenmesi
- Özel Kanununda hükmü bulunmayan defterleri onaylamak
- Tebligat İşlemleri

A. Elektronik Zaman Damgası Vurma

Noterlik Kanunu'nun 60. Maddesi 4. bendi "Bu kanuna uygun olarak dışarıda yazılıp getirilen kâğıtların üzerindeki imza, mühür veya herhangi bir işareti veya tarihi onaylamak"[5] kanununa göre, noterler bir belge üzerinde herhangi bir işareti, tarihi, imzayı onaylayıp tarih atarak hukuki geçerliliğini sağlarlar. Sayısal imza kullanılarak imzalanmış bir elektronik belge notere ulaştığında kişinin elektronik sertifikasıyla kimlik doğrulama yapılabilir. Bu işlemde noter belgenin içeriği ile ilgilenmeyip sadece kimlik doğrulamasını yapmaktadır. Bu sonuç esas alınarak işlemin sanal ortamda modellenebileceğini söyleyebiliriz, kurulacak bir otomasyon ile onaylama işlemi yapılıp, sonuç olumlu ise noter kendi sayısal imzası ile elektronik belgeyi onaylar. Hali hazırda ülkemizde bu konuda hizmet veren bir kurum mevcuttur.

B. Kendisine Gönderilen Elektronik Belgelerdeki Elektronik İmza ve Tarihi Onaylamak

Noterlik Kanunu'nun 90. Maddesi "Hukuki işlemlerin altındaki imzanın onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır"[5]. 91. Maddesi "Onaylama, imzanın noter huzurunda atılması veya kendisine ait olduğunun ilgili tarafından kabulü ile kabildir" şeklindedir[5]. Bu maddelere göre noter bir belgedeki imza ve tarihi kendi huzurunda ve kendisine ait olduğunun kabul edilmesi durumunda bir şerhle

belgelendirmektedir. Sayısal imza ile imzalanmış bir elektronik belgede kimlik doğrulama yapılabildiğinden noter sanal ortamda gerekli doğrulama mekanizması ile bu hizmeti verebilir.

C. Elektronik Belgelerin Saklanması ve İstendiğinde Belgelenmesi

Noterler yapmış oldukları işlemleri 2000'li yıllardan itibaren kâğıt üzerinde tutmanın yanında elektronik olarak kayıt altına almaktadırlar. Noterlik Kanunu'nun 94. Maddesi "Noterler tarafından yapılan işlemlerin örnekleri, ancak ilgililerine, kanuni mümessil veya vekillerine yahut da mirasçılarına verilir."[5] şeklindedir. Bu kanuna göre birey ya da kurum kendisiyle ilgili bir belgeyi noterden elektronik olarak talep edebilir. Bu durumda sanal ortamda kişi sayısal imzası ile başvuruda bulunup, kimlik doğrulaması yapılarak kanunda öngörüldüğü gibi noter işlemi ile ilgili ise noter işlem örneklerini, noterin sayısal imzası ile imzalanmış olarak sanal ortamda alabilir.

D. Özel Kanununda Hükmü Bulunmayan Defterleri Onaylamak

Günümüzde ticari olsun olmasın hemen hemen tüm defterler elektronik ortamlarda tutulmaktadır. Fakat dijital olmayan bir kopyası, kanun gereği tahrifatı önlemek ve kayıt altına almak için belirli aralıklarla noterlere onaylatılır.

Noterlik Kanunu'nun 107. Maddesi "Özel kanununda hüküm bulunmayan hallerde defter onaylaması, defterin baş ve son sayfasına kaç sayfadan ibaret olduğu yazılmak ve her sayfası numaralanıp mühürlenmek suretiyle yapılır." şeklindedir[5]. Bu kanuna göre; noterler sanal ortamda kurulacak bir otomasyon ile kendisine ulaştırılan özel kanunda hükmü bulunmayan defterleri, kendi sayısal imzası ile onaylayıp, kayıt altına alabilir.

E. Tebligat İşlemleri

Noterlerin en yoğun olarak yaptığı işlemlerden biri de kendisine gelen belgeleri ilgili kişiye tebliğ etmektir. Noterlik Kanunu'nun 106. Maddesi "Her türlü hukuki işlemlere ait ihtarname ve ihbarname:

I. İstemde bulunan ve diğer tarafın ad ve soyadları ile açık adreslerini,
II. İhtar ve ihbar konusunu,
III. İstemde bulunanın imzasını,
IV. Tebliğ şerhini, noterin imza ve mührünü ve tarihi (Yazı ve rakam ile),

kapsar. İhtarname ve ihbarnameler ilgili tarafından yazılıp tebliğ için notere getirebileceği gibi, notere de yazdırılabilir."[5] şeklindedir. Bu işlem kurulacak bir otomasyon ile bireyin yâda kurumun internet üzerinden açık adres bilgilerini, ihtar ve ihbar konusunu elektronik belgeye girip sayısal imzası ile tebligat notere ulaştırılır. Gerekli kimlik doğrulaması yapıldıktan sonra tebligat ilgili kişiye klasik noter hizmetlerinde olduğu gibi ulaştırılır.

Fakat burada ihtar eden kişinin tebligat üzerinde ıslak imzası olmaması, hukuki normlara göre geçersiz gözükse de, diğer yandan ıslak imzayla eş olan sayısal imzasının noter tarafından doğrulanmış olması hukuki geçerliliğini sağlamaktadır. Bu ve benzeri durumlar da oluşabilecek yorum farklılıklarından dolayı Sanal Noter Uygulaması için Noterlik Kanunu ve diğer ilişkili kanunlarda çeşitli düzenlemeler yapılmalıdır.

V. Hukuki Gereksinimler

Noter işlemlerinde teknolojik altyapı kullanılarak, normal bir noterin sağlamış olduğu tüm güvenlik sağlanmış olsa da hukuki mevzuat tam anlamıyla noterlik işlemleri yapmaya uygun değildir.

5070 Sayılı Elektronik İmza Kanunu kabul edilerek, sayısal imza ile ıslak imza belirli kısıtlamalar dışında eş kılınmıştır. Fakat kurumların yapmış olduğu işlemlere sayısal imzayı entegre edecek düzenlemeler yapılmamıştır. Oysaki kurumların birçoğunun noterlerde olduğu gibi(Noterlik Kanunu) kendi iş yapısına uygun kanunları vardır. Bu nedenle hukuki anlamdaki temel gereksinim, sayısal imzayı kurumların iş yapısına uyarlamaktır.

Sayısal imza ile yapılan sözleşmeler ve işlemler hukuki olarak, adi senet statüsündedir. Adi senet, "resmi bir makam veya memurun katılımı olmaksızın, bizzat hukuki ilişkilerin taraflarınca düzenlenen senetlerdir"[17]. Hukuk Usulü Muhakemeleri kanununda adi senetlerin ispat gücü; "Bir adi senet, senet altında imza tarafından ikrar edilirse kesin delil teşkil eder"[17] şeklinde tanımlanmıştır. Bu ifadelere göre, sayısal imza ile işlem yapan taraflardan birinin noter olması, yapılan işlemin hukuki tanımıyla çelişmektedir. Çünkü artık taraflardan biri resmi bir makamdır. Bu durumda yapılan işlem adi senet statüsünde mi değerlendirilecektir? Burada üzerinde durulması gereken konu, sayısal imza ile yapılan işlemlerinin neden adi senet olarak tanımlandığıdır. Bunun sebebi, işlem taraflarından kaynaklanan güven zafiyeti mi, yoksa teknolojik altyapıya olan güven zafiyetimidir? İşlem taraflarına olan güven zafiyeti var ise bu işlemi bir noter sayısal imza ile yapması veya koordine edip işleme sayısal imzasını koyması durumunda bu işlemi hukuki olarak hangi statüde değerlendirilecektir. Diğer yandan teknolojik altyapıya olan güven zafiyeti mi, işlemi hukuki olarak adi senet şeklinde tanımlamıştır. Sebep bu ise, sayısal imza ile yapılan işlemler, tarafların dışında üçüncü bir kurum olan ESHS tarafından teyit edilmektedir, bu sebeple adi senet tanımlamasının sayısal imza işlemleri ile ne kadar örtüştüğü değerlendirilmelidir.

Türkiye'de hizmet veren ESHS'ların Elektronik İmza Kanunu'na göre "Sertifika Mali Sorumluluk Sigortası" yaptırması gereklidir. Bu sigorta ESHS'ın, Elektronik İmza Kanunu'ndan doğan yükümlülüklerini yerine getirmemesi durumunda, nitelikli elektronik sertifika sahibi kişi veya kuruluşların ve üçüncü şahısların uğrayacağı zararlara ilişkin sorumluluğu, sözleşmede belirlenen zorunlu sigorta limitlerine kadar teminat altına alır[6]. Bu sigorta, sigortalıya karşı yapılan talepler sonucundaki yasal giderler için de teminat verir.

Sertifika Mali Sorumluluk Sigortası olay başına 10.000 (On bin YTL) ve Sözleşme süresince 1.000.000(Bir Milyon YTL) teminat tutarlarını vermektedir[7]. Diğer sigorta işlemleri ile mukayese edildiğinde teminat tutarları oldukça düşüktür,

birey ve kurumlara güven vermemektedir. Sadece noter işlemleri için değil tüm işlemlerde bu teminat tutarları daha yukarı çekilmeli, toplumun sayısal imzayı kullanması teşvik edilmelidir.

Daha önce belirtildiği gibi, sayısal imza uygulamalarında işlemi yapan elektronik sertifikaların geçerli olup olmadığının doğrulanma süreci çok önemlidir. Doğrulama sürecinde SIL listeleri veya OCSP sorgusu kullanılabilir. OCSP anlık olarak elektronik sertifikanın geçerliliğini bize verdiği için, noter uygulamaların da mutlaka her işlem için OCSP kullanılmalıdır. OCSP sorgusundan dönen ESHS'ın sayısal imzasını koyduğu sonuca göre işlem yapılmamalı, dönen sonuçtaki sayısal imza kök sertifikanın doğrulanmasına kadar devam edilmelidir. Bu sebeple Noter uygulamaları için yapılacak yazılımlar mutlaka CWA 14167–1 standardında olmalı ve ek olarak OCSP sorgu şartı yönetmelik ve kanunlarla düzenlenmelidir.

Hukuki anlamda düzenleme gereken diğer bir konuda, sanal ortamda gerçeklenecek bir Sanal Noter Uygulamasının ne şekilde ücret tahsil edeceğidir. Noterlik Kanunu'na göre noterlik hizmetleri, peşin olarak noterde tahsil edilir. Bu durum da hukuki olarak düzenlenmelidir. Ücretlendirme için kontör sistemi ya da sanal poslar kullanılabilir.

VI. SONUÇLAR

Ülkemizin ilk sayısal imza uygulamalarından olan UYAP ile başlayan süreç, Sanayi Bakanlığı, Başbakanlık Dış Ticaret Müsteşarlığı ve Türk Patent Enstitüsü'nün uygulamaları ile devam etmiştir.

Bu projelerden bir sonraki adım Sanal Noter Uygulaması olmalıdır. Günümüzde bankacılık işlemlerini kâğıt üstünde yürütebiliriz demek, ne kadar imkânsız ise, artan iş yüküyle beraber gelecekte noter işlemlerini kâğıt üstünde yürütürüz demek o kadar imkânsızdır. Sanal ortamda e-ticaret hacmi arttıkça, e-sözleşme, e-fatura, e-devlet vb. uygulamalar arttıkça, Sanal Noter ihtiyacı daha da belirginleşecektir. Bu sebeple sanal ortamda noterin işlevlerini, gerekli güvenlik sağlanarak modellenmesi zorunluluk haline gelmiştir.

Yapılan çalışmada noterlerin, sanal ortamda bazı hizmetlerinin hiçbir kuşkuya neden olmadan AAA teknolojisi üzerine kurulmuş sayısal imza ile gerçeklenebileceği aşikârdır.

5070 Sayılı Elektronik İmza Kanunu ile beraber kurum kanunlarında yapılacak hukuki düzenlemeler, Sanal Noter Uygulamasının hukuki dayanağını oluşturur. Bu koşullar altında Sanal Noter Uygulaması hayata geçirilebilir.

KAYNAKLAR

[1] http://turk.internet.com, Kamu Yönetimi ve Hukuk Ekseninde E-noterlik, Kasım 2008.
[2] Sağıroğlu, Ş., Alkan, M., Her Yönüyle Elektronik İmza (E-İmza), Grafiker Yayınları, ISBN:975-6355-23-9, Ankara, 2005
[3] http://mevzuat.basbakanlik.gov.tr, 5070 Sayılı Elektronik İmza Kanunu, Kasım 2008.
[4] Türkiye Bilişim Derneği, Nitelikli Sertifikasyon Altyapısı ve Yetkilendirme, Kasım 2008 Antalya.
[5] http://www.noterlerbirligi.org.tr/nkanunu.htm, 1512 Nolu Noterlik Kanunu, Kasım 2008.
[6] http://www.tk.gov.tr/eimza/eimza_mevzuat.htm, Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları, Kasım 2008.
[7] http://www.tk.gov.tr/eimza/eimza_mevzuat.htm, Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı, Kasım 2008.
[8] http://www.k-binder.be, Introduction to PKI - Public Key Infrastructure, Kasım 2008.
[9] http://www.comms.scitech.susx.ac.uk,, Understanding Public Key Infrastructure (PKI), Kasım 2008.
[10] Keser Leyla, İstanbul Bilgi Üniversitesi, e-imza & e-Türkiye, Temmuz 2004.
[11] http://turk.internet.com, Elektronik İmza Kanunu ve Dijital İmza, Mart 2008.
[12] http://www.pki.iam.metu.edu.tr, Kriptografi Bölümü, Açık Anahtar Altyapısı Araştırma, Geliştirme ve Uygulamalar, Mart 2008.
[13] Akçeşme Dursun, Sönmez Çoşkun, Bir Sanal Noterin Altyapısının Gerektirdikleri, Ağ ve Bilgi Güvenliği Sempozyumu, Mayıs 2008
[14] Yavuz Alper, Digital Notary, Lisans Tezi, 2006
[15] Demir İlke, ODTU Bilgisayar Topluluğu, e-bergi/Nisan 2007
[16] [11] Çelikyılmaz Sertaç, Türkiye'de Kurumlar İçin e-Güven Altyapısı e-İmza, Aralık 2005.
[17] http://turk.internet.com, e-imza ve Adi Senetler, Kasım 2008.
[18] Beceni Yasin, Elektronik İmza ve Uygulamalar, Ocak 2006.