BİR SANAL NOTER UYGULAMASININ GEREKTİRDİKLERİ

Dursun Akçeşme
Bilgisayar Mühendisliği Bölümü
Yıldız Teknik Üniversitesi, İstanbul
dursunakcesme@hotmail.com

A. Coşkun Sönmez
Bilgisayar Mühendisliği Bölümü
Yıldız Teknik Üniversitesi, İstanbul
acsonmez@ce.yildiz.edu.tr

ABSTRACT

Together the improving internet technology, the processes that in every respect of our lives, are realised in virtual environment under the name of e-process; thus the question whether the public notary services can be realised securly in a virtual environment or not has arised. In this study; how public notary services can be realised by using the present technological infrastructure with in the consideration of juidical regulations is explained and how secure these services can be implemented is mentioned. As a result of this study, it is decided that a big part of public notary services can be transfered into virtual environment in a secure and juidical way via today's techonology.

Key words: Digital Notarization, Digital Signature, Public Key Infrastructure, Public Key, Private Key, Digital Certificate.

1. GİRİŞ

Günümüz dünyasında müthiş bir ivmeyle gelişen internet teknolojisi kullanılarak, yer ve zaman kavramının önemi olmadan, elektronik posta ile başlayan süreç; internet bankacılığı, finans sektöründe yapılan işlemler ve elektronik ticaret ile doruğa ulaşmıştır. Son yıllarda sıkça duyduğumuz e-devlet kavramı da bu zincirin son halkasıdır. E-devlet kavramı ile birlikte kamunun sunmuş olduğu hizmetleri kanunlar ve yönetmelikler çerçevesinde, bilgi güvenliği sağlanmış vaziyette elektronik ortama taşınması amaçlanmıştır. Bununla beraber, kamu hizmetleriyle sürekli etkileşim halinde olan noterlik hizmetlerinin de sanal ortamda, bilgi güvenliği sağlanmış vaziyette sunulması ihtiyacı doğmuştur [1].

Tüm bu gelişmeler ile birlikte bilgi güvenliği riski de aynı hızla artmıştır. Bu konuda bilgi güvenliğini sağlamaya yönelik yapılan çalışmalarda, en öndeki kurumlar olan bankalar internet bankacılığı işlemleri için, ilk olarak, kullanıcı şifre ile ilişkilendirilerek, şifre koruması yapılmıştır, fakat sahtekârlıkların olması, şifre koruması ile birlikte ek olarak elektronik sertifika kullanılmıştır ve son olarak OTP (One Time Password) kullanılmaktadır. Ama görülüyor ki tüm bu adımlar tam anlamıyla güvenliği sağlayamamakta ve hukuki mevzuata uygunluğu tartışılmaktadır, oysaki hayatımıza yeni yeni giren dijital imza, mevcut teknoloji şartlarına göre mutlak bir güvenlik sağlamaktadır. Bunun yanında dijital imza, hukuki olarak güvence altına alınarak, ıslak imza ile bazı istisnalar (emlak alım-satım, vasiyetname, evlenme vb.) dışında eş konumdadır [5].

Noterlik hizmetlerinin sanal ortama taşınmasında, tüm noterlik uygulamalarının taşınması hukuki mevzuattan ve yapılacak işin niteliğinde dolayı söz konusu olamayacağı bir gerçektir [6]. Fakat noterlerin onaylama faaliyetlerinin birçoğu hukuki mevzuata uygun bir şekilde sanal ortama taşınabilir.

Noterlik hizmetlerinin sanal ortamda hizmet verilebilmesinin hukuki dayanağı, 2004 yılında kabul edilen 5070 sayılı Elektronik imza kanunudur [5]. Bu kanunla birlikte, noterlik hizmetlerinin sanal ortamda gerçeklenmesinin önü açılmıştır.

2. DİJİTAL İMZA

5070 sayılı Elektronik İmza Kanunu'nda yer alan tanımda elektronik imza; "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar "[5] şeklinde tanımlanmıştır.

Başka bir ifadeyle elektronik imza; elektronik veriye eklenen, mesaj alıcısının ve göndericisinin kimliğinin doğrulamasını ve gönderilen elektronik verinin bütünlüğünü sağlayan ve dijital sertifikalarla birlikte inkâr edilemeyen bir kriptografik dönüşümdür. Elektronik imza mevcut teknoloji koşullarında mutlak güvenlik sağlayan asimetrik kriptografi yöntemini kullanır. Kriptografik dönüşümlerde, elektronik imza RSA, DSA ve ECDSA vb. algoritmaları kullanır [17].

Elektronik imza çok geniş bir kavram olup, kişilerin göz retinası, parmak izi gibi biyometrik özellikleri

de elektronik imzanın içinde kalır, bu sebeple elektronik veri tanımlaması yerine dijital imza demek daha doğru bir tanımlama olur. 5070 sayılı Elektronik İmza Kanunu'da esasında dijital imza'yı tanımlamaktadır. [7].

Noterlik hizmetleri düşünüldüğünde hukuki geçerliliğin sağlanması için iki koşul yerine gelmek zorundadır, bu koşullar dijital imza teknolojisinde de var olan;

- Kimlik doğrulama ve onaylama
- İnkâr Edilemezlik

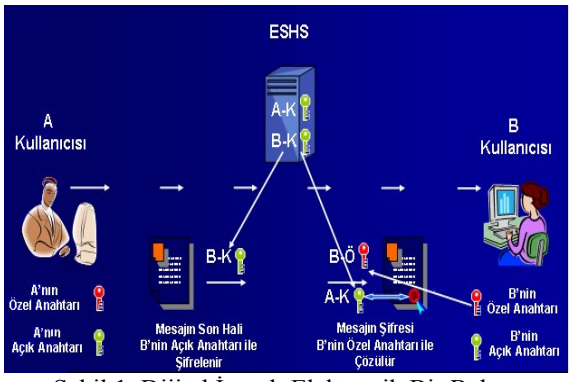
Dijital imza teknolojisi kullanılarak, elektronik veriyi imzalayan kişinin kimliği, elektronik sertifikalar yardımıyla açık olarak tespit edilebilmektedir. Bununla birlikte ESHS (Elektronik Sertifika Hizmet Sağlayıcısı)'larda her işlem için kayıt oluşturulduğundan inkâr edilememeyi sağlamaktadır, tüm bu yapı, hukuki mevzuatta da düzenlenmiştir. Başka bir ifadeyle, hukuki olarak gerekli zemin hazır konumdadır [9]. Dijital imza ile birlikte elektronik dokümanlarımızın,

- Veri Bütünlüğü'de sağlanmış olur.

Oysaki Islak imza'lı belgelerde tahrifat yapılma tehlikesi her zaman vardır.

2.1. Dijital İmza Güvenlik Altyapısı

Dijital imza Açık Anahtarlı Altyapı (AAA) Teknolojisi üzerine kurulmuştur [12]. Bu sistem asimetrik algoritmalar (RSA, DSA vb.) kullanarak güvenliği sağlamaktadır. Dijital imza teknolojisinde kullanılan güvenlik altyapısı, asimetrik algoritmaların çalışma biçimini gizlemeye dayalı bir yapıda değildir, çünkü güvenliği sağlayan algoritma olmayıp, algoritmayı kullanarak oluşturulan anahtarlardır, bu yapı, Kerckhoff prensibine göre "sadece anahtar gizli olmalıdır" şeklinde standartlaşmıştır. [18]. AAA teknolojisinde, asimetrik algoritmalar kullanıcıya iki anahtar tanımlar, bu anahtarlar Açık Anahtar (Public Key) ve Gizli anahtar (Private Key)'dir. Açık anahtar gizli olmayan herkesin erişebileceği bir anahtardır. Gizli anahtar ise sadece dijital imzanın sahibinin bildiği anahtardır. Kişinin dijital imzası Gizli Anahtardır. Açık anahtar ise dijital imza ile imzalanmış elektronik verinin, Alıcı tarafında ihtiyaç duyacağı anahtardır. Alıcı kendisine gelen dijital imza ile imzalanmış bu elektronik veriyi ilgili kişi tarafından gönderilip gönderilmediğini ve veri bütünlüğünün bozulup bozulmadığını doğrulamak için, gönderen kişinin dijital imza(Gizli Anahtar)'sının eşi olan Açık anahtarı kullanmak zorundadır. Açık anahtarı kullanarak hukuki geçerliliği olan veriye ulaşır, bu doğrulama için alıcı, kişinin Açık Anahtarını nitelikli elektronik sertifika kullanarak elde eder. Bu sertifikaları 5070 sayılı Elektronik imza Kanununda belirtilen kurallara göre yurtiçinde hizmet veren ESHS tarafından verilir [5]. ESHS'lar kullanıcı kimliği ile kullanıcının Açık anahtarı arasında ilişki kuran ve dijital imzanın inkâr edilememesini sağlamaktadır.



Şekil 1. Dijital İmzalı Elektronik Bir Belge Oluşturulma Aşamaları [8]

Şekil 1. de görüldüğü gibi A kullanıcısı elektronik bir veriyi dijital imzasını ekleyerek güvenli bir şekilde B kullanıcısına göndermektedir [8].

Her iki kullanıcı da Elektronik Sertifika Hizmet Sağlayıcıdan nitelikli elektronik sertifika almıştır. A kullanıcısı ilk olarak göndermek istediği elektronik verinin hash algoritmasını (SHA-1, MD5) kullanarak bir özetini çıkartır, bu işlemin sebebi dosya boyutu ne olursa olsun sabit uzunlukta eşsiz bir verinin elde edilerek şifreleme yapılmasıdır. Oluşturulan bu veriden ana metne ulaşmak mümkün değildir. Bir sonraki adımda hash algoritması ile oluşturulan özet metin A kullanıcısının Gizli anahtarı ile şifrelenir ve son olarak ESHS' dan B'nin açık anahtarı da elektronik veriye eklenerek, elektronik veriye mantıksal bağı olan elektronik imza oluşturulmuştur. Oluşturulan bu mesaj sadece B kullanıcısının gizli anahtarı ile açılabilir. Gönderilmeye hazır olan bu mesaj B kullanıcısına ulaştığında B kullanıcısı kendi özel anahtarını kullanarak mesajı açar. Bir sonraki aşamada B kullanıcısı ESHS' dan A kullanıcısının açık anahtarını talep eder ve mesajın özetine ulaşır ve doğrulama bu noktada yapılır, A noktasında oluşturulan özet değeri ile B noktasında oluşturulmuş olan özet değeri aynı ise elektronik veri güvenli bir şekilde B kullanıcısına ulaştırılmış olur. Burada elektronik verinin gizliliği, bütünlüğü ve inkâr edilememesi sağlanmış ve hukuki olarak güvence altına alınmıştır.

Yukarıdaki dijital imzalı bir elektronik belgenin oluşturulma aşamalarından anlaşılacağı üzere, dijital imza imzalanacak elektronik veriye göre farklılık gösterir, içerik matematiksel fonksiyonlardan geçilerek eşsiz bir elektronik imza elde edilmesi sağlanır. Islak imzada olduğu gibi bir kişinin tek imzası olmayıp, tek bir gizli anahtarı vardır.

Dijital imzaya temel oluşturan Açık anahtar Altyapısı elektronik mevcut teknoloji koşullarında daha öncede değinildiği gibi mevcut teknolojiler içerisinde mutlak güvenlik sağlamaktadır.(Tablo 1)

	Kimlik Kanıtlama	Gizlilik	Bütünlük	İnkâr Edememe
Antivirüs			✔	
Firewall	✔	✔		
Erişim Denetimi	✔	✔		
Şifreleme		✔		
Açık Anahtar Altyapısı	✔	✔	✔	✔

Tablo 1. Elektronik Emniyet Yöntemlerinin Karşılaştırılması [17]

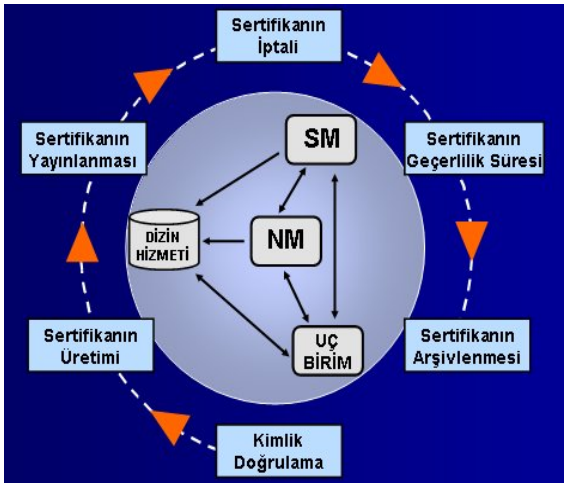
Elektronik Sertifika Hizmet Sağlayıcıları, Açık Anahtarlı Altyapının en önemli bileşenlerinden biridir, genel olarak görevi nitelikli elektronik sertifika vermektir. Nitelikli elektronik sertifikalar kişinin kimlik bilgisi ile açık anahtarının birbirine bağlayan elektronik kayıtlardır. Daha genel bir ifadeyle sanal ortamda bizim kimlik kartlarımızdır. Bu sertifikalar Uluslar arası Telekom Birliği standartlarına göre X.509 standardında olmalıdır [9]. Temel olarak bir elektronik sertifika içinde;

- Sertifika Seri Numarası
- Sertifika Sahibinin Kimlik Bilgileri (TC kimlik No, Adı, Soyadı, e-mail adresi)
- Sertifika geçerlilik başlangıç tarihi
- Sertifika geçerlilik sonlanma tarihi
- Sertifikanın kullanım amacı
- Kullanılacak Algoritmalar
- Sertifika sahibinin açık anahtar bilgisi
- Yayınlayan ESHS

Bilgileri bulunur. Bu sertifika yayınlayan ESHS tarafından gizli anahtarı kullanılarak imzalanır böylece geçersiz, sahte sertifikaların yayınlamasının önüne geçilmiş olur.

Türkiye'de nitelikli elektronik sertifika hizmeti sağlayan dört kurum vardır [3]. Bunların kendi aralarında olan trafiği çapraz sorgu şeklindedir [9]. Örneğin A ESHS'den alınan dijital imza ile B ESHS'den alınan dijital imzanın aynı elektronik belgeyi imzalaması durumunda ESHS'lar kendi aralarında çapraz sorgu yaparak ESHS'ların açık anahtarları güvenli bir şekilde paylaşması sağlanır. Uluslar arası ESHS'larda bu durum devletlerarası hukuki düzenlemeler ile sağlanabilmektedir.

Açık Anahtarlı altyapıda oluşturulan sertifikaların yaşam döngüsü aşağıdaki şekildedir;



Şekil 2. Sertifika Yaşam Döngüsü [8]

Şekil 2'de görüldüğü gibi Nitelikli elektronik sertifika kimlik doğrulaması ile başlar bu safhada kişi nüfus cüzdanı pasaport vb. kimlik ile bizzat ESHS kurumuna giderek adına sertifika talebinde bulunur [4]. Bu talebin sonucunda ilgili kişi yasal mevzuata haykırı bir durumu yok ise adına geçerlilik süresi belirlenen eşsiz bir nitelikli elektronik sertifika üretilir, hiçbir zaman güvenliği sağlamak için, süresiz sertifika üretimi yapılmaz. Üretilen sertifika işlemler tamamlandıktan sonra yayınlanır, kişinin talebi olmadığı müddetçe geçerlilik süresi boyunca geçerliliğini korur, sürenin sonunda geçerliliğini yitirir, aynı şekilde geçerliliğini yitiren sertifikanın yayınlama işlemi ESHS tarafından yapılır, geçerliliğini yitiren sertifika arşivlenerek, sertifikanın yaşam döngüsü tamamlanmış olur [8].

2.2.Dijital İmza Donanımları

Dijital imza teknolojisinde gizli anahtarı depo edebilmek için mevcut'ta iki farklı çözüm vardır [17]. Gizli anahtar verisi, yalnızca bir kere

yazılabilen ve kopyalanamayan akıllı kartlarda, ya da usb dongle'larda tutulur.

Bu donanımları kullanmak istediğinizde ek bir güvenlik olarak pin koruması vardır. Pin bilgisi geçildikten sonra gizli anahtarı üretme verisine ulaşılarak gizli anahtar üretilir. Akıllı karta verilen bir komutla, gizli anahtar karmaşık matematiksel fonksiyonlar sonucunda üretilir.

Dijital imza donanımının geçerliliğini doğrulayan ESHS'un yayınlamış olduğu Açık anahtardır. Kayıp olması yâda elden çıkması durumunda, ESHS ile bağlantı kurularak kolaylıkla geçersiz kılınabilir.

Şekil 3. Dijital İmza Donanımları [17]

3. DİJİTAL İMZA İLE NOTERLİK İŞLEMLERİ

Daha öncede değinildiği gibi tüm noterlik işlemlerini hukuki mevzuat ve işin niteliğinden dolayı tümüyle sanal ortamda gerçekleştirmek mümkün değildir. Dijital imza ile noterlik hizmetlerinin onaylama işlemleri güvenli bir şekilde, hukuki mevzuata uygun şekilde gerçekleştirilebilir.

Sanal Ortamda verilebilecek noter hizmetleri dört başlık altında toplanabilir [6];

- Elektronik tarih damgası vurma
- Kendisine gönderilen dokümanlardaki elektronik imza ve tarihi onaylamak
- Elektronik dokümanların saklanması ve istendiğinde belgelenmesi
- Tebligat işlemleri

3.1.Elektronik tarih damgası vurma

Noterlerin görevlerinden biri de bir belgedeki tarih ve imzanın doğrulanması yoluyla o belgenin hukuki bağlayıcılığını sağlamak vardır. Bu göreve istinaden elektronik bir belgenin dijital olarak imzalanması ve sanal noterlik hizmetini veren web sunucusuna gönderilmesi durumunda, ilgili noter bu elektronik belgeyi kendi dijital imzasını koyması halinde bu belgenin hukuki geçerliliği sağlanmış olur.

Bu şekil bir işlemin hukuki geçerliliğini açıklamak istersek; Dijital imza ile yapılan sözleşmelerin, işlemlerin hukuki olarak, adi senet statüsündedir. Adi senet, resmi bir makam veya memurun katılımı olmaksızın, bizzat hukuki ilişkilerin taraflarınca düzenlenen senet olarak tanımlanabilir. Hukuk Usulü Muhakemeleri kanununda adi senetlerin ispat gücü; "Bir adi senet, senet altında imza tarafından ikrar edilirse kesin delil teşkil eder" şeklinde tanımlanmıştır. Aksi bir durumda inkâr edilmesi halinde ESHS kurumundan ilgili doğrulamanın yapılması ile gerçek açığa kavuşur, bu doğrulama ıslak imza ile mukayese edildiğinde hukuk sistemine çok şey katacağı açıktır.

3.2. Kendisine gönderilen dokümanlardaki elektronik imza ve tarihi onaylamak

Noterler tarafından hukuki işlemlerin altındaki imzaların onaylanması Noterlik Kanununun 90. maddesinde düzenlenmiştir. Buna göre hukuki işlem altındaki imzanın onaylanması imzayı atan kişiye ait olduğunun bir şerhle belirlenmesi şeklinde yapılacaktır. Elektronik ortamda hazırlanan bir elektronik evrak altındaki imzanın onaylanma ihtiyacı duyulduğunda, sanal noter hizmeti veren web sunucusuna gönderildiğinde, dijital imzası ile ilgili kişinin açık anahtarı kullanılarak karşıdaki kişinin kimliği çözülür, bu işlem ile noter tarafından doğrulama sağlanmış olur ve kayıt altına alınır.

3.3.Elektronik dokümanların saklanması ve istendiğinde belgelenmesi

Noterlerin görevlerinden bir tanesi de, noterlikçe yapılan her işlemin bir kopyasının noterlik tarafından saklanılmasıdır. Talep edildiğinde bu belgenin örneklerinin verilmesi gereklidir. Hukuki olarak orijinali ile aynı geçerliliğe sahiptir. Dijital imza ile imzalanarak kendisine gönderilen elektronik dokümanın, sanal noter web sunucusu gönderildikten sonra, açık anahtar yardımıyla kişinin kimliği saptanır ve ilgili elektronik doküman kişinin kimliği işe ilişkilendirilerek saklanır. Bu noktada noterlerin görevini kısmen yapan ESHS ile ayrımı ortaya çıkmaktadır, çünkü ESHS'lar yalnızca işlemle ilgili elektronik imzanın bir kopyasını tutarken Noterler ilgili elektronik dokumanı tutmakla görevlidirler.

3.4.Tebligat işlemleri

Noterlerin görevlerinden biride kendisine getirilen belgeleri ilgili kişiye posta aracılığıyla tebliğ etmektir. İhbarname ve ihtarname işlemleri noterlerin yoğun olarak yaptığı işlemlerdendir. Sanal ortamda tebligat işlemleri için, noterlerin kullanmış olduğu ve noter kanununda da belirlenmiş olan metin, sanal ortama aktarılıp ve harici bilgileri dışarıdan kullanıcının girmesi şeklinde ve son olarak ilgili kişinin dijital imzası ile tebligat işlemi, tebligatı yapan tarafında tamamlanır. Bir sonraki adımda sanal ortamdan gelen tebligat talebi sanal noter olarak hizmet veren web sunucusu aracılığıyla hizmeti veren noterin ortamına gelir. İlk olarak dijital imza ile imzalanmış olan elektronik verinin üzerindeki imzadan ilgili kişinin kim olduğunu belirlemek için ESHS' ten kişinin açık anahtarı ile ilişkilendirilmiş kimlik doğrulaması yapılır. Doğrulama gerçeklendikten sonra ilgili tebligat klasik noter işlemine tabi tutulur. Son aşamada tebligat yapıldıktan sonra, noter ilgili elektronik belge üzerine kendi dijital imzasını koyarak ilgili elektronik veriyi tebligat talebinde bulunan kişiye göndererek tebligat işleminin yapıldığını kişiye bildirir.

SONUÇLAR

Noter hizmetlerinde görülüyor ki onaylama işlemlerinin birçoğunda kimlik tanımlaması yapıldığı takdirde, ilgili belgenin içeriğinin önemi olmadan noter ilgili belgeyi kayıt altına almaktadır. Burada önem arz eden işlemi talep eden kişinin kimlik tanımlamasının yapılmasıdır.

Dijital imza ile mutlak kimlik tanımlaması yapılabilmekte olduğundan, internet ortamında oluşturulacak bir web uygulamasından, elektronik olarak gelen verinin mutlak doğruluğu kanıtlanabilecek ve inkâr edilmesi söz konusu olmayacaktır. Ayrıca sanal noter uygulamasının, 5070 sayılı Elektronik İmza Kanunu ile hukuki dayanağı olduğundan dolayı onaylama faaliyetleri içeren noter hizmetleri hiçbir şüpheye neden olmadan sanal ortamda mevcut teknoloji ile gerçeklenebilir.

KAYNAKLAR

[1] Turan Orhan, Noterlik İşlemleri ve Elektronik, 2001.
[2] http://www.e-imza.gen.tr, Mart 2008.
[3] http://www.tk.gov.tr, Mart 2008.
[4] Keser Leyla, İstanbul Bilgi Üniversitesi, e-imza & e-Türkiye, Temmuz 2004.
[5] http://mevzuat.basbakanlik.gov.tr, E-imza Kanunu, Mart 2008.
[6] http://turk.internet.com, Kamu Yönetimi ve Hukuk Ekseninde E-noterlik, Mart 2008.
[7] http://turk.internet.com, Elektronik İmza Kanunu ve Dijital İmza, Mart 2008.
[8] Serhat Özeren, TEDER, Bilgi Güvenliği, Temmuz 2004
[9] Türkiye Bilişim Derneği, Nitelikli Sertifikasyon Altyapısı ve Yetkilendirme, Mayıs 2005 Antalya.
[10] http://enoter_hukuk.tripod.com/dijitalimza.htm, Mart 2008.
[11] Çelikyılmaz Sertaç, Türkiye'de Kurumlar İçin e-Güven Altyapısı e-İmza, Aralık 2005.
[12] Beceni Yasin, Elektronik İmza ve Uygulamalar, Ocak 2006.
[13] http://www.uekae.tubitak.gov.tr, Mart 2008.
[14] http://www.pki.iam.metu.edu.tr, Kriptografi Bölümü, Açık Anahtar Altyapısı Araştırma, Geliştirme ve Uygulamalar, Mart 2008.
[15] Eralp Özgür, Bilişim ve Hukuk Sempozyumu, Ocak 2006.
[16] Sağıroğlu Şeref, Elektronik İmza, Gazi Üniversitesi, Nisan 2006
[17] http://www.e-imza.biz.tr, Mart 2008
[18] Demir İlke, ODTU Bilgisayar Topluluğu, e-bergi/Nisan 2007
[19] Yavuz Alper, Digital Notary, YTÜ Computer Department Final Year Project, 2006