YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SANAL NOTER

Bilgisayar Müh. Dursun AKÇEŞME

F.B.E. Bilgisayar Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof. Dr. A.Çoşkun SÖNMEZ

İSTANBUL, 2009

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SANAL NOTER

Bilgisayar Müh. Dursun AKÇEŞME

F.B.E. Bilgisayar Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof. Dr. A.Çoşkun SÖNMEZ

İSTANBUL, 2009

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

AAA	Açık Anahtar Altyapısı
APS	Acele Posta Sistemi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
B2B	Business to Business
B2C	Business to Customer
ÇİSDUP	Çevrim İçi Sertifika Durum Protokolü
DES	Data Encryption Standart
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Levels
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
HUMK	Hukuk Usulü Muhakemeleri Kanunu
IBM	International Business Machines
IETF	Internet Engineering Task Force
ISP	İnternet Service Provider
KPS	Kimlik Paylaşım Sistemi
LDAP	Lightweight Directory Access Protocol
MD5	Message-Digest algorithm 5
NCCUSL	National Conference of Commissioners on Uniform State Law
NES	Nitelikli Elektronik Sertifika
NOTOP	Noter Otomosyon Projesi
OCSP	Online Certificate Status Protocol
RFC	Request For Comments
RSA	Anahtarlı Tabanlı Şifreleme Algoritması
SHA	Secure Hash Algorithm
SIL	Sertifika İptal Listesi
Sİ	Sertifika ilkeleri
SSL	Secure Socket Layer
TAKBIS	Tapu Kadastro Bilgi Sistemi
TNB	Türkiye Noterler Birliği
USB	Universal Serial Bus
UYAP	Ulusal Yargı Ağı Projesi

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Son yıllarda teknolojik gelişmeler ile birlikte, toplumda internete erişen kişi sayısı ve erişim hızı sürekli artmaktadır. Bu gelişmeler, toplumun bilgiye ve hizmete en kolay, en ucuz ve istediği zaman erişimi için gerekli altyapıyı sağlamıştır. Bundan sonraki süreçte, günlük hayatta yaptığımız birçok işlem e-işlem başlığı altında sanal ortamda modellenmiştir. Bu gelişmeler zaman ve yer kavramını ortadan kaldırmış, işletmelerin iş ilişkilerini sanal ortamda gerçekleştirdiği modelleri (B2B, B2C) ortaya çıkarmıştır. Elektronik posta ile başlayan bu süreç E-devlet kavramı ile doruk noktasına ulaşmıştır. Kamu hizmetleri de artık sanal ortamda birer birer modellenmeye başlamıştır. Bu süreçte, dünyada ve ülkemizde sanal ortamda ıslak imza ile aynı hukuki sonucu doğuran Elektronik İmza Kanunları yasalaşmıştır. Kamu hizmetlerinin yavaş yavaş sanal ortamda modellenmesi, bir güven makamı olan noterlerin de sanal ortamda olup olamayacağının sorgulanmasına neden olmuştur.

Bu tez çalışmasında, sanal ortama uyarlanabilecek noter hizmetleri için gerekli koşullar ve yapılması gereken hukuki düzenlemeler araştırılmıştır.

Çalışmalarımın her aşamasında büyük desteğini gördüğüm, öneri ve yönlendirmeleriyle bana her konuda yardımcı olan değerli hocam Prof. Dr. A.Çoşkun SÖNMEZ'e teşekkürlerimi bir borç bilirim.

Bütün eğitim hayatım boyunca gösterdikleri sabır, hoşgörü, maddi ve manevi destekleri için değerli aileme sonsuz teşekkürlerimi sunarım.

ÖZET

Ülkemizde E-devlet kapsamında, birçok kamu kurumu bazı hizmetlerini sanal ortamda vermektedir. Bir kamu kurumu olan noterlerin ise sanal ortamda herhangi bir hizmeti verilmemektedir.

Bu çalışmada, noter hizmetlerini sanal ortamda modellemeye yönelik bir araştırma yapılmıştır. Noter hizmetlerinin analizi yapılarak sanal ortamda modellemek için gerekli koşullar belirlenmiştir. Belirlenen koşullara göre, bazı noter hizmetlerinin, mevcut teknolojik koşullar ve yapılacak hukuki düzenlemeler ile hukuki geçerliliği olacak şekilde sanal ortamda gerçeklenebileceği sonucuna varılmıştır. Bu sonuca göre; sanal ortamda noter hizmetleri için gerekli koşullar, elektronik imza ve kriptografik algoritmalar kullanılarak modellenmiştir. Noterlik kanunu temel alınarak, sanal ortamda yapılabilecek noter hizmetleri belirlenmiştir. Modelin, hukuki geçerliliği analiz edilerek, yapılması gereken hukuki düzenlemeler belirlenmiştir. Önerilen modelde, sanal ortamda yapılabilecek işlemlerden biri olan ihtarname işlemleri için prototip bir uygulama hazırlanarak, yapılan çalışma somut olarak ortaya konulmuştur.

Anahtar Kelimeler: Açık Anahtar Altyapısı, Elektronik İmza, Elektronik Sertifika, Sanal Noter.

ABSTRACT

In our country, lots of public organizations sustain some of their services within the concept of E-State. However, any of notary services as a public occupation is not served in virtual environment.

At this study, a research is done about modeling notary services in virtual environment. Notary services are analyzed and necessary conditions are determined. According to these conditions it is concluded that, some notary services can be realized in virtual environment within the existing technological structure and judicial regulations that maintaining legality. In accordance to this conclusion, necessary conditions for notary services in virtual environment are modeled by electronic sign and cryptology algorithms. Notary services which can be performed in virtual environment specified in accordance with notary laws. Judicial validity of the model is analyzed and necessary regulations are specified. In this model, a prototype implementation for official warning is prepared and the study is presented.

Keywords: Public Key Infrastructure, Electronic Signature, Electronic Certificate, Digital Notary.

1. GİRİŞ

Çağımızdaki teknolojik gelişmeler ile günlük hayatta yaptığımız birçok işlem sanal ortamda modellenmiştir. Elektronik postayla başlayan bu süreç, internet bankacılığı ve elektronik ticaret ile devam etmiştir. Son yıllarda bu atılım, elektronik ticaret ile doruğa ulaşmış ve son halka olarak E-devlet kavramını ortaya çıkarmıştır. E-devlet ile birlikte birçok kamu hizmeti sanal ortama taşınmış ve halen taşınmaya devam etmektedir. Sanal ortamda artık, birey ve işletmeler ile beraber yeni bir taraf, kamu vardır. Bu gelişmeler ile birlikte hayatımız kısmen sanal ortama taşınmıştır. Diğer yandan toplumun her işleminde güven makamı olan, noterler için bir adım atılmamıştır. Oysaki günlük hayatta kamu kurumları, bireyler ve işletmeler ile sürekli etkileşim halinde olan noterlere sanal ortamda da ihtiyaç vardır.

Sanal ortamda taraflar arasında yapılan işlemlerde kimlik doğrulamanın ve inkâr edememenin sağlandığı söylenemez. Bu konuda yargıya intikal eden birçok ihtilaf bulunmaktadır. Günlük hayatta bu ve benzeri ihtilafların oluşmaması için çözüm, noterleri işaret etmektedir. Bu ve benzeri sebepler, sanal ortamda noterlerin kısmen de olsa bulunma zorunluluğunun somut göstergesidir.

Dünyada ve ülkemizde sanal ortamda noter hizmetlerini modellemeye yönelik çeşitli çalışmalar yapılmaktadır.

Amerika Birleşik Devletleri'nde Kaliforniya ve Florida Noterlik kanunları bu konuda özel hükümler taşıyan ilk noterlik kanunlarıdır. Kaliforniya Noterlik Kanunu'nun 1633.11[*] maddesi "Elektronik Noterlik" başlığını içermektedir. Bu başlık altında noter, elektronik imza ile imzalanmış elektronik bir belgeyi onaylama gereği duyar ise bu işlem noterin elektronik imzasıyla yapılır şeklindedir [1]. Görülüyor ki sanal ortamda noter işlemlerinin yapılabilmesi 1633.11 maddede belirtildiği üzere, ancak elektronik imza ile mümkün olabilmektedir. Bu gelişmelere paralel olarak son yıllarda ülkemiz de dâhil olmak üzere, dünya genelinde birçok ülkede elektronik imzaya yönelik kanunlar yasalaşmıştır. Bu sebeple Kaliforniya kanununda belirtildiği üzere sanal noter hizmetleri elektronik imza üzerine kurulmalıdır.

---

[*] a)If a law requires that a signature be notarized, the requirement is satisfied with respect to an electronic signature if an electronic record includes, in addition to the electronic signature to be notarized, the electronic signature of a notary public together with all other information required to be included in a notarization by other applicable law.

b)In a transaction, if a law requires that a statement be signed under penalty of perjury, the requirement is satisfied with respect to an electronic signature, if an electronic record includes, in addition to the electronic signature, all of the information as to which the declaration pertains together with a declaration under penalty of perjury by the person who submits the electronic signature that the information is true and correct.

Florida Noterlik Kanunu'nun 117.20[**] maddesinde "Elektronik Noterlik" başlığı altında elektronik noterliğin ne şekilde yapılacağı açıklanmaktadır. Bu kanuna göre; "Elektronik noterlik yapmak isteyen noter, bir elektronik imza sahibi olmalıdır. İlgili bakanlığa başvuruda bulunarak gerekli izni aldıktan sonra elektronik noterlik işlemi yapabilir" şeklindedir.

Elektronik ortamda noterlik hizmetlerinin ilk örneklerinin olduğu Amerika Birleşik Devletleri'nde, Amerikan Ulusal Noterler Birliği, elektronik ortamda yapılabilecek noter işlemlerinin geleneksel noterler dışında kimseye verilmemesini ve elektronik noterlik yapacak noterin ek bir eğitimden geçirilmesi gerekliliğinin altını çizmektedir.

Amerika Birleşik Devletleri'nde Anglo-Sakson hukuk sistemini uygulanmakta olduğundan Noterlik Kurumu ülkemizde olduğundan farklıdır [1]. Noter işlemi yaptırmak istediğinizde notere ile iletişime geçerek, sizin adresinize gelmesini sağlayıp işlem yaptırabilirsiniz. Gezici noter şeklinde bir yapı mevcuttur.

Amerika Birleşik Devletleri'ndeki noterler için 1999 yılında NCCUSL'nin Birleştirilmiş Elektronik İşlemler Yasası kabul edilmiştir. Bu yasayla beraber elektronik imza 40 eyaletin noterler kanununa adapte edilmiştir. Bu yasaya dayanarak Ulusal Noterler Birliği tarafından Enjoa Projesi gerçeklenmiştir (Eralp vd., 2008). Bu projeyle beraber, noter kişinin imzasını bir elektronik cihaz üzerine attırmaktadır. Bu elektronik cihaz bir dizüstü bilgisayara bağlıdır. Bu bilgisayarda Amerikan Ulusal Noterler Birliğinin resmi noterlik defterleri tutulmaktadır. Bu cihazın kontrolü noterin parmak izi ile koruma altına alınmıştır. Bu sistemde kişinin fotoğrafının çekilerek kayıt altına alınması da mümkündür. Arizona'da bu model "Secure Electronic Signature" olarak tanımlanmaktadır (Paul, 2004). Bu modelde yapılan işlemler ABD hukuk sisteminde yasal olarak geçerli kabul edilmektedir. Enjoa Projesi ile geçilen bu sistem, elektronik noterlik olarak tanımlanmış olsa da ülkemizin hukuk sistemi ile örtüşmemektedir.

Elektronik ortamda, noterlik işlemlerini yapmaya yönelik çalışmaların yapıldığı diğer bir ülkede Japonya'dır. Japonya'da ilk adım Nisan 2000'de noterlik kanununda değişiklikler yapılarak atılmıştır. Pratik uygulamalara Ocak 2002'de başlanmıştır. İki yıllık süreçte çeşitli

---

[**] Electronic notarization

The provisions of ss. 117.01, 117.03, 117.04, 117.05(1)-(11), (13), and (14), 117.105, and 117 apply to all notarizations under this section as set forth in this section.

An electronic notarization shall include the words "Notary Public- State of Florida," the name of the notary public, exactly as commissioned, the date of expiration of the commission of the notary public, the commission number, and the notary's digital signature. Neither a rubber stamp seal nor an impression-type seal is required for an electronic notarization…

düzenlemeler yapılmıştır. Şu anda Japonya'da bazı noter işlemleri elektronik olarak yapılabilmektedir. Japonya'da elektronik imza kanunu Mayıs 2000'de kabul edilmiştir. Dikkat çekici olan, Japonya'da noterlik kanununda yapılan düzenlemenin elektronik imza kanunundan 1 ay önce yapılmış olmasıdır. (Kato, 2008).

Ülkemizde sanal ortamda noterlik faaliyetlerine yönelik Mersin Noter Odasının çeşitli çalışmaları mevcuttur. Çalışmaların ana teması, kişinin notere gitmeden önce tüm işlemlerin hazırlanarak kişinin notere yalnızca ıslak imzasını atmak için gitmesidir. Bu çalışmalar kapsamında, Mersin Noter Odası'nın internet adresinden "Çevrimiçi Noterlik İşlemleri" linki altında noterlik işlemleri gruplanarak kişinin erişimine sunulmuştur. Kişi yapmak istediği noterlik işlemini seçerek, işleme ilişkin bilgileri ve kimlik bilgilerini girerek sanal ortamda notere göndermektedir. Kişi notere gittiğinde tüm işlemler hazır olmakta ve kişi ıslak imzasını atarak noter işlemini tamamlamaktadır. Bu işlem her ne kadar efektif görünse de suiistimale çok açık bir yapıdadır. Kişinin internet üzerinden gönderdiği bilgiler kullanılarak, kati olarak kişinin kimlik doğrulaması yapılamamakta, girilen bilgilerin bütünlüğü sağlanamamakta ve işlem başvurusunun inkâr edilmesi mümkün olabilmektedir.

Ülkemizdeki diğer bir çalışmada, Türkiye Noterler Birliği sanal ortamda noterler arasında bağlantı kurmak ve arşivleme işlemlerini yapmak amacı ile NOTOP (Noter Otomasyon Projesi) projesini başlatmış ve halen sürdürmektedir [1]. Bu projede amaç E-devletin yapıtaşları olan KPS (Kimlik Paylaşım Sistemi), TAKBIS (Tapu Kadastro Bilgi Sistemi) vb. sistemler ile bütünleşen bir sistem yaratmaktır.

Dünyada ve ülkemizde yapılan çalışmalarda, noterlerin hizmetleri sanal ortamda somut olarak modellenmemiştir. Bu modellemeden kasıt, işlem taraflarının yüz yüze olmadan işlem yapabilmesidir. Böyle bir modellemenin yapılamamasının nedeni; işlemi tamamlamak için kişinin ıslak imzasının ilgili belgenin üzerinde olma zorunluluğu ve bazı işlemlerde noterin kişisel iradesine ihtiyaç duyulmasıdır. Fakat bazı noter işlemlerini yapmak için yapılan incelemede noterin kişisel iradesine gerek duyulmadığı görülmektedir. Tezin ana amacı, bu noter işlemlerini sanal ortamda ne şekilde modellenebileceğine çözüm getirmektir. Bu işlemleri sanal ortamda gerçekleyebilmenin önündeki en büyük engel ıslak imzanın ne şekilde atılacağıdır.

Biliyoruz ki; Elektronik İmza Kanunu 23 Ocak 2004 tarihinde resmi gazetede yayınlanarak yasalaşmıştır. Bu kanun ile birlikte belirli sınırlamalar dışında ıslak imza ile elektronik imza eş kılınmıştır. Bu sebeple, sanal ortamda elektronik imza kullanılarak noterin iradesini gerektirmeyen işlemler modellenebilir. Başka bir ifade ile noterlerin bazı hizmetlerinin sanal

ortama taşınması, mevcut teknolojik koşullar ve yapılacak hukuki düzenlemeler ile hukuki dayanağı olacak şekilde mümkün olabilmektedir.

2. NOTERLİK KURUMU

Noterlik Kurumu, devlet tarafından kıymetli evrakların imzalanmasına şahitlik etmek ve yeminli ifade almak üzere kurulmuş olan bir kurumdur.

2.1 Noterlik Müessesesinin Tanımı ve Önemi

Noterlik müessesesi, toplumda güven makamı olarak bilinen bir kamu kurumudur. Noterlik bir kamu hizmetidir. Noterler, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek için işlemleri belgelendirir ve kanunlarla verilen başka görevleri yaparlar.

Ülkemizde noter ve noterlik müessesesi 18.01.1972'de kabul edilen 1512 sayılı Noterlik Kanunu tarafından düzenlenmiştir [3]. Günümüze dek Noterlik Kanunu'nda çeşitli düzenlemeler yapılmıştır.

Noterlik müessesesi toplumsal huzurun garantörüdür. Her ne kadar kişilerin hakları kanunlar ile korunsa da, bir hakkın ihlali durumunda esas kabul edilen kayıtları düzenleyen kurumlar noterlerdir. Bu sebeple noterlik müessesesi dolaylı olarak hukukun kişiye sağladığı hakları kullanmasını sağlar. Kişinin haklarının ihlal edilmesi durumunda, tespit işlemi ile hukuksal mercilere karşı kişinin haklarını garanti altına alır.

Noterlik müessesesi, yukarıda belirtilen nedenlerden dolayı tarihte hemen hemen her toplumda farklı isimlerde ve farkı statülerde var olmuşlardır. Her toplumda, özde yapmış olduğu işlem birey ya da kurumlar arasında oluşabilecek anlaşamazlıkların önüne geçerek, esas kabul edilen kayıtları oluşturmaktır.

Noterlik müessesesi her asliye ve sulh mahkemesinin bulunduğu yerde mahkeme ve çevresinin yargı çevresindeki işlemleri görmek için kurulur. Yurtdışında noterlik işlemleri konsolosluklar tarafından yapılır [3].

2.2 Noterin Tanımı

Noter yukarıda ifade edildiği gibi, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek amacı ile kendisine getirilen veya kendisinin düzenlemiş olduğu belgelere resmi evrak statüsü kazandıran kamu görevlisidir.

Başka bir ifade ile noter, toplumsal sorumlulukları sebebi ile kendine özgü bir statüsü olan kamu görevlisidir.

Noter tarafından yapılan tüm işlemler Noterlik Kanunu ve Noterlik Kanunu Yönetmeliği esas alınarak yapılır. Bu kanun ve yönetmelikler ile beraber bazı noter işlemlerinde (tespit işleri,

vasiyetname işlemleri, araç satışları vb.) noterlik müessesesinin yanında noterin kişisel bilgisine deneyimine ve muhakemesine ihtiyaç duyulur. Diğer yandan bazı işlemler de (ihtarname işlemleri, defter onayı, imza mühür onayı vb.) sadece noterlik müessesesi olması yeterlidir.

2.3 Noterlerin Görevleri

Noterlerin görevleri iki başlık altında incelenebilir.

2.3.1 Noterlerin Genel Olarak Yapacakları İşler

Noterlerin genel olarak yapacağı işlemler aşağıda maddeler halinde verilmiştir (TNB, 2007).

- Yapılması kanunla başka bir makam, merci veya şahsa verilmiş olan her nevi hukuki işlemleri düzenlemek.
- Kanunlarda resmi olarak yapılmaları emredilen ve mercileri belirtilmemiş olan bütün hukuki işlemleri bu kanun hükümlerine göre yapmak.
- Gayrimenkul satış vaadi sözleşmesi yapmak.
- Bu kanuna uygun olarak dışarıda yazılıp getirilen kâğıtların üzerindeki imza, mühür veya herhangi bir işareti veya tarihi onaylamak.
- Bu kanun hükümlerine göre yapılan işlemlerin dairede kalan asıl veya örneklerinden veya getirilen kâğıtlardan örnek çıkarıp vermek.
- Belgeleri bir dilden diğer dile veya bir yazıdan başka bir yazıya çevirmek.
- Protesto, ihbarname ve ihtarname göndermek.
- Kanunen tescili gereken işlemleri tescil etmek.
- Bu ve diğer kanunlarla verilmiş sair işleri yapmak.

2.3.2 Noterlerin Özel Olarak Yapacakları İşler

Noterlerin özel olarak yapacağı işlemler maddeler halinde aşağıda verilmiştir (TNB, 2007).

- Tespit işleri: Noterler bir nesnenin veya bir yerin hal ve şeklini, kıymetini, işleme konu olan tarafların kimliklerini tespit ederler. Özel kurumların kura ve benzeri uygulamalarında hazır bulunarak durumu belgelendirirler.
- Emanet işleri: Noterler saklanmak veya birine verilmek üzere kendisine getirilen emanetleri tutanak düzenleyerek teslim alırlar.

- Defter Onaylamak: Noterler Türk Ticaret Kanunu ve diğer kanun hükümlerine göre tutulması gereken defterleri onaylarlar.
- Vasiyetname ve ölüme bağlı tasarruf işleri: Noterler açık ve kapalı olarak kendisine getirilen vasiyetnameleri saklar ve ilgili belge için tutanak düzenlerler.
- Tebligat işlemleri: Tebliği istenen her nevi kâğıt, Tebligat Kanunu hükümlerine göre muhatabına tebliğ olunur. Tebliğ tutanağı dairedeki nüshaya bağlanır. Tebliğin yapıldığı veya yapılamadığı ilgilisine verilecek nüshasına yazılıp onaylanır.

2.4 Noter İşlemlerinin Yapılış Şekli ve Gerektirdikleri

Tüm noter işlemleri Noterlik Kanunu ve yönetmelikler esas alınarak güvenlik en üst düzeyde tutularak yapılmaya çalışılır. Herhangi bir noter işleminde mutlak suretle aşağıda verilen dört koşul yerine getirilir (Akçeşme ve Sönmez, 2008).

- Bir noter işlemi yapılmak istendiğinde noter tarafından, işlemi yaptırmak isteyen kişinin kimlik doğrulaması yapılır. Kimlik doğrulaması kişinin nüfus cüzdanı, pasaport veya ehliyeti (tüm noter işlemlerinde geçerli değildir) ile yapılabilir.
- Noter işlemine konu olan belgenin hazırlanmasından sonra, kişinin kendi adına yapılan bu işlemi inkâr etmemesi için, kişinin ıslak imzası alınır.
- İlgili noter kayıtlarının içeriği noter çalışanları ya da 3. kişiler tarafından değiştirilemez. Noter ya da 3. kişiler tarafından içeriğin tahrif edilmeyeceği yasalar ile güvence altına alınmıştır. Böyle bir eylem yasal olarak suç teşkil etmektedir.
- İlgili noter kayıtlarının yalnızca noter ve işlem yapan kişi tarafından bileneceği 3. kişilere mahkeme kararları dışında verilmeyeceği yine yasalar tarafından güvence altına alınmıştır.

Bu koşullardan herhangi birinin eksik olması söz konusu değildir. Aksi takdirde işlemin hukuki geçerliliği mutlak değildir.

2.5 Noter İşlemlerine Sanal Ortamda Bakış

Sanal ortamda, bir önceki başlıkta değinilen koşulları ele alırsak; kişi ve noterin kimlik doğrulaması elektronik olarak yapılabilmeli, aynı şekilde kişinin ve noterin imzası elektronik olarak atılabilmeli, sanal ortamda taraflar arasında akan veri trafiğinin bütünlüğü bozulmamalı ve veri trafiği gizli kalmalıdır. Görülüyor ki sanal ortamda noter işleminin modellenebilmesi için;

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

koşullarının sağlanması gerekmektedir (Akçeşme ve Sönmez, 2008). Aksi halde tezin konusu olan Sanal Noter uygulamasından söz edilemez.

Açık Anahtar Altyapısı üzerine kurulan elektronik imza ile veri gizliliği dışındaki diğer üç koşul sağlanmaktadır. Veri gizliliği koşulu ise kriptolojik yöntemlerle sağlanabilmektedir.

Sanal ortamda elektronik imza ve kriptolojik yöntemler kullanılarak modellenebilecek böyle bir sistemin hukuki dayanağı 5070 sayılı Elektronik İmza Kanunu'dur. 23 Temmuz 2004 tarihinde yürürlüğe giren 5070 Sayılı Elektronik İmza Kanunu elektronik imza ile ıslak imzayı bazı sınırlamalar dışında eş kılmıştır.

Noter işlemlerindeki dört koşul sanal ortamda modellense de, noterlerin vermiş olduğu hizmetlerin tümünün sanal ortama taşınması hukuki mevzuattan ve yapılacak işin niteliğinden dolayı mümkün değildir. Fakat noterlerin bazı hizmetleri yukarıda verilen modelle ve yapılacak hukuki düzenlemeler ile mümkün olabilmektedir.

3. KRİPTOLOJİ

Sanal ortamda noter hizmetlerini üstlenecek bir model, önceki bölümde belirtildiği üzere, kimlik doğrulama yapabilmeli, inkâr edilememeli, veri bütünlüğünü ve veri gizliliğini sağlamalıdır. Tüm bu işlevleri Açık Anahtar Altyapısı sağlamaktadır. Açık Anahtar Altyapısı kriptoloji bilimi üzerine kurulmuş bir yapıdır.

3.1 Kriptoloji Bilimi

Kriptoloji bir şifre bilimidir. Her türlü metnin belirli bir sisteme göre (matematiksel temelli algoritmalar) şifrelenmesi ve şifrelenerek oluşan metinden tekrar ana metne dönülmesini sağlar (Şekil 3.1).

Kriptoloji bilimi, bilgi güvenliğini sağlamaya yönelik çalışmalar yapar. Son yıllarda teknolojik gelişmeler ile birlikte bilgi güvenliği riskinin artması ile beraber, kişiler arasındaki iletişimde kriptoloji biliminin çözümlerinden yararlanılmaktadır.

Kriptoloji bilimi Kriptografi (Şifreleme) ve Kriptoanaliz (Şifre Çözme) olmak üzere iki alt dala ayrılır (Çağlayan, 2003).

Kriptografi bilimi, matematiksel temelli algoritmalar kullanılarak bir metnin şifrelenmesi ve sonrasında kullanılan algoritmanın tersi işletilerek ana metnin elde edilmesi üzerine çalışmalar yapan bir bilimdir. Şifreleme ve şifre çözme işlemi için anahtar ya da anahtarlar kullanılabilir. Ana metnin matematiksel algoritmadan geçirilmesi veri kaybına neden olmaz.

Kriptografik bir algoritmanın başarı ölçüsü üç faktöre bağlıdır [4] .

- Güvenlik Derecesi: Bilgiyi ele geçirmeye yönelik yapılan işlem sayısını ifade eder.
- Başarım: Kriptografi algoritmanın saniyede şifrelediği bit sayısı ifade eder.
- Uygulama Başarısı: Kriptografik algoritmanın uygulanabilirlik başarısını ifade eder.

Şekil 3.1 Şifreleme ve şifre çözme işlemi

Kriptoanaliz ise matematiksel algoritmalar ile şifrelenmiş metnin, zayıf yönlerini belirlemeye yönelik çalışmalar yapan bilimdir. Kriptolojide önemi büyüktür. Kriptografik algoritmanın

güvenliğini ölçen bir bilim olarakta tanımlanabilir. Kriptoanalizde temel olarak iki yöntem vardır. Bunlardan birincisi brut force (kaba kuvvet) yöntemidir. Bu yöntemde tüm anahtar değerleri denenir. Günümüzdeki bilgisayar teknolojisindeki gelişmeler ile işlem hızı sürekli artmaktadır. Bu sebeple bu yöntemin önemi giderek artmaktadır. Bu yöntemin başarımı anahtar uzunluğu ile ters orantılıdır. İkinci yöntem ise matematiksel ifadelerle oluşturulan algoritmaya yine matematiksel yaklaşımlar ile çözüm aramaktır.

3.2 Kriptografik Yöntemler

Kriptografik yöntemler temel olarak ikiye ayrılırlar. Bunlar algoritma bağımlı kriptografik yöntemler ve anahtar tabanlı kriptografik yöntemlerdir.

Günümüzde algoritma bağımlı kriptografik yöntemler tercih edilmemektedir. Çünkü şifreleme yapan algoritmanın 3. kişiler tarafından öğrenilmesi durumunda tüm sistemin güvenliği tehlikeye girmektedir. Diğer yöntem olan anahtar tabanlı kriptografik yöntemlerde ise 3. kişiler tarafından şifreleme algoritmasının öğrenilmesi sistem güvenliğini tehlikeye sokmamaktadır. Bu yöntemde, sistemin güvenliği şifreleme algoritmasına bağlı olmayıp, anahtara bağlıdır.

Şifrelemede kullanılan anahtarın uzunluğu arttıkça, sistemin güvenliği de aynı oranda doğru orantılı olarak artar (Sağıroğlu, 2006).

3.2.1 Algoritma Bağımlı Kriptografik Yöntemler

Algoritma bağımlı kriptografik yöntemler, kriptoloji biliminin atası sayılabilecek yöntemlerdir. Fakat günümüzde hemen hemen hiç kullanılmamaktadır. Sebebi, sistem güvenliğinin şifreleme algoritmasına bağımlı olmasıdır.

Bu yöntemin kullanıldığı sistemlerde, şifreleme algoritmasını bilen bir kişinin işten ayrılması, algoritmanın 3. kişiler tarafından öğrenilmesi vb. sebeplerden dolayı sistem güvenliği sürekli tehlike altındadır. Bu nedenlerin yanında algoritmanın birden fazla sistemde kullanılamaması, her sistemde farklı bir algoritma tanımlama zorunluluğu, maliyetinin fazla olması vb. sebepler de tercih edilmemesinin diğer nedenleridir.

Algoritma bağımlı kriptografik yöntemlere verilebilecek en güzel örnek Sezar şifreleme algoritmasıdır (Sağıroğlu ve Alkan, 2005). Bu algoritmada metnin her harfi bir sayı ile ifade edilir. Şifreleme algoritmasında her harf kendisinden sonra gelen 3 karakter sonrasının sayısı ile sembolize edilerek, alfabedeki sayı kadar modu alınır. Mod işleminden sonra çıkan sayı alfabede hangi harfe karşılık geliyor ise o harf ile sembolize edilir. Matematiksel olarak ifade

edilir ise;

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

E = Şifreleme Algoritması D = Şifre Çözme Algoritması

M = Şifrelenecek Metin C = Şifrelenmiş Metin

C = Şifrelenmiş Metin M = Şifresi çözülmüş Metin

şeklindedir.

Örnek olarak YILDIZ metni Sezar Şifreleme algoritması ile şifrelendiğinde;

Alfabedeki her harfe bir sayı gelecek şekilde eşleştirme yapılır (Çizelge 3.1).

Çizelge 3.1 Sezar şifreleme algoritması referans çizelgesi

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	

Y I L D I Z	Ana metin
27 10 14 4 14 28	Rakamlarla sembolize edilmesi
1 13 17 7 17 2	Algoritmaya göre +3 eklenerek mod 29 alınması
B K O Ş O C	Şifrelenmiş metin

Örnekte görüldüğü gibi Sezar şifreleme algoritması ile YILDIZ metni BKOŞOC şeklinde şifrelenmiştir. Şifrelenen bu metnin şifresi çözülmek istenirse algoritmanın tersi işletilir.

B	K	O	Ş	O	C	Şifrelenmiş metin
1	13	17	7	17	2	Rakamlarla sembolize edilmesi
27	10	14	4	14	28	Algoritmaya göre 3 çıkartarak mod 29 alınması
Y	I	L	D	I	Z	Ana metin

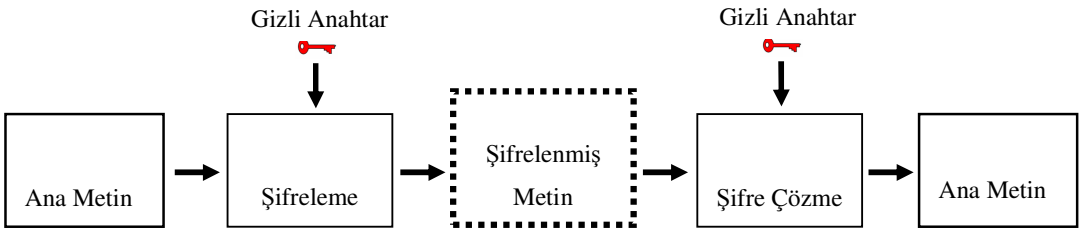
adımları uygulanarak şifrelenen metne ulaşılır.

Algoritma bağımlı kriptografik yöntemlerin tümü, Sezar Şifrelemeye benzer yöntemlerle şifreleme yaparlar.

3.2.2 Anahtar Tabanlı Kriptografik Yöntemler

Anahtar tabanlı kriptografik yöntemlerde şifreleme işlemi için anahtarlar kullanılır. Kullanılan algoritmanın bilinmesi güvenlik zafiyeti oluşturmaz. Güvenlik, kullanılan anahtarın uzunluğu ile doğru orantılıdır. Günümüzde hemen hemen tüm şifreleme sistemlerinde anahtar tabanlı kriptografik yöntemler kullanılmaktadır. Anahtar tabanlı algoritmalar Simetrik ve Asimetrik algoritmalar olmak üzere ikiye ayrılırlar.

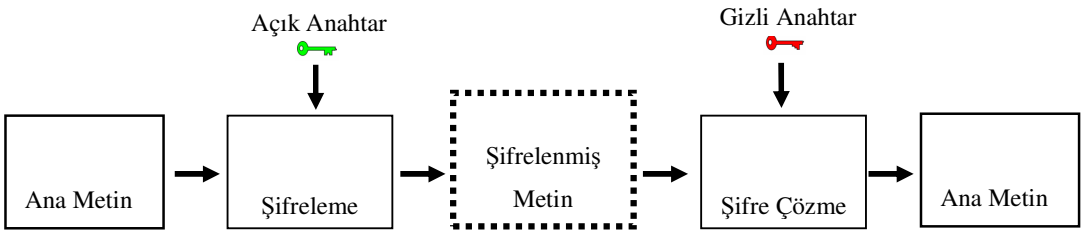
Simetrik algoritmalarda metni şifrelemek ve şifreli metni çözmek için aynı anahtar kullanılır. Kullanılan bu anahtarı, simetrik algoritma kullanarak haberleşmek isteyen her iki tarafta bilmelidir. Bu anahtar Özel Anahtar veya Gizli Anahtar olarak adlandırılır (Şekil 3.2). Günümüzde bu tür algoritmalarda kullanılacak simetrik anahtar, standart olarak en az 128 bit olarak tanımlanmaktadır. Simetrik algoritmalarda IBM'in geliştirmiş olduğu DES algoritması standart olarak kabul edilmektedir.



Şekil 3.2 Anahtar tabanlı simetrik algoritma blok şeması

Asimetrik algoritmalarda ise metni şifrelemek ve şifreli metni çözmek için farklı anahtarlar

kullanılır (Şekil 3.3). Bu anahtarlar bir çift olarak üretilirler. Bu anahtar çiftleri arasında matematiksel bir bağ vardır. Bu çiftlerden herhangi birisinin şifrelemiş olduğu metnin şifresini ancak çiftin diğer anahtarı çözebilir. Bu anahtar çiftlerinden şifreleme işlemini yapan anahtar Genel Anahtar (Public Key) veya Açık Anahtar olarak adlandırılır. Şifrelenmiş metnin şifresini çözen anahtar ise Özel Anahtar (Private Key) veya Gizli Anahtar olarak adlandırılır. Burada isimlendirme temel alınarak şifreleme işleminin yalnız açık anahtar tarafından yapılacağı anlaşılmamalıdır. İstenildiği takdirde gizli anahtar ile şifreleme yapılıp açık anahtar ile de şifre çözme işlemi yapılabilir. (Çağlayan, 2003; Sağıroğlu, 2005).



Şekil 3.3 Anahtar tabanlı asimetrik algoritma blok şeması

Asimetrik algoritmalarda en çok bilinen ve kullanılan yöntem RSA algoritmasıdır. RSA algoritması diğer yöntemlerde olduğu gibi matematiksel yöntemler üzerine inşa edilmiştir. RSA algoritmasının dışında DSA, Eliptik Eğri Sistemleri, El Gamal ve Diffie–Hellman gibi asimetrik yöntemlerde vardır. Genelde asimetrik şifreleme yapılacak ise RSA algoritması tercih edilir. Yapılan çalışmada oluşturulan örnek modelde de RSA algoritması kullanılmıştır.

RSA algoritması çarpanlara ayırma problemi üzerine kurulmuştur. Algoritmik olarak ifade edilir ise;

1. İki adet asal sayı belirlenir.

   Birinci sayı Q

   İkinci sayı P

2. Bu iki sayının çarpımı ile N sayısı oluşturulur. Bu sayı açık ve gizli anahtarda mod alma işlemi için kullanılacaktır.

   $N = Q*P$

3. Bir A sayısı oluşturulur.

$A = (Q-1)*(P-1)$

4. A sayısı ile ortak böleni bulunmayan bir E sayısı seçilir. Seçilen bu E sayısı açık anahtar ile birlikte kullanılacaktır.

5. E ile çarpılıp A ile mod alındığında 1 sonucunu veren D sayısı bulunur. D sayısı gizli anahtarda N sayısı ile birlikte üst alma işleminde kullanılacaktır.

   $(D*E) \bmod A = 1$

6. Bu işlemlerden sonra;

   Açık Anahtar = (N, E) Gizli Anahtar = (N, D) şeklinde bulunur.

7. Şifreleme işlemi için;

   $C = M^E \bmod N$ şeklinde yapılır

   C = Şifrelenmiş Metin

   M = Orijinal Metin

   E = Açık Anahtar Parametresi

   N = Açık Anahtar Parametresi

8. Şifre çözme işlemi için;

   $M = C^D \bmod N$ şeklinde yapılır.

   M = Orijinal Metin

   C = Şifrelenmiş Metin

   D = Gizli Anahtar Parametresi

   N = Gizli Anahtar Parametresi

RSA algoritması sayısal bir örnek üzerinde incelenir ise;

1. İki adet asal sayı belirlenir.

   P = 3 Q = 11

2. N sayısını hesaplanır.

   N = 3*11 = 33

3. A sayısı hesaplanır.

   A = (3-1)*(11-1) = 20

4. E sayısını seçilir.

   E = 7 olarak seçilir. (A ile ortak böleni olmayan başka bir sayıda seçilebilir.)

5. D sayısı hesaplanır.

   (D*7) mod 20 = 1

   D = 3 olarak bulunur.

6. Açık Anahtar = (33, 7) Gizli Anahtar = (33, 3) olarak hesaplanır.

7. YILDIZ metni RSA algoritması kullanılarak şifrelenir. Şifreleme işlemi için Açık Anahtar (33, 7) kullanılacaktır.

YILDIZ metni sayısal olarak sembolize edilir. (Hesaplama kolaylığı için küçük sayılar seçilmiştir.)

Y I L D I Z Ana metin

7 3 5 4 3 1 Metnin sayısal karşılığı

Şifreleme işlemi aşağıdaki şekilde yapılır.

Y harfi için $7^7 \bmod 33 = 28$

I harfi için $3^7 \bmod 33 = 9$

L harfi için $5^7 \bmod 33 = 14$

D harfi için $4^7 \bmod 33 = 16$

I harfi için $3^7 \bmod 33 = 9$

Z harfi için $1^7 \bmod 33 = 1$

YILDIZ metni 7-3-5-4-3-1 şeklinde sayısal olarak ifade edilmiştir. Yapılan şifreleme işlemi ile sayısal metin 28-9-14-16-9-1 olarak ifade edilmiştir.

8. Şifre çözme işlemi için Gizli Anahtar (33, 3) kullanılır.

28 sayısal değeri için $28^3 \bmod 33 = 7$

9 sayısal değeri için $9^3 \bmod 33 = 3$

14 sayısal değeri için $14^3 \bmod 33 = 5$

16 sayısal değeri için $16^3 \bmod 33 = 4$

9 sayısal değeri için $9^3 \bmod 33 = 3$

1 sayısal değeri için $1^3 \bmod 33 = 1$

Hesaplamaya göre 7-3-5-4-3-1 sayısal değerlerine ulaşılır. Referans alınan karakterlerin sayısal dönüşümü yapılır ise YILDIZ metnine ulaşılır.

Asimetrik algoritmalar günümüzde bilinen en güvenilir algoritmalardır. Güvenliğin tehlikeye girmesi için anahtarlar oluşturulurken belirlenen P ve Q asal sayılarının bulunması

gerekmektedir. Fakat gerçek uygulamalarda bu sayılar çok büyük seçildiği için bu sayıların bulunması neredeyse imkânsızdır.

Asimetrik algoritmalar ile simetrik algoritmaları karşılaştırdığımızda, asimetrik algoritmaların çok daha güvenli olduğunu söyleyebiliriz. Performans açısından değerlendirildiğinde ise simetrik algoritmalar, asimetrik algoritmalara göre çok daha hızlı çalışırlar. Bunun sebebi asimetrik algoritmaların işlem yükünün simetrik algoritmalara göre çok daha fazla olmasıdır.

Asimetrik algoritmalarda kullanılan anahtarın uzunluğu arttıkça performans düşmektedir. Bu konu üzerine Selçuk Üniversitesi'nde yapılan bir araştırmanın sonuçları Çizelge 3.2'de görülmektedir. Yapılan performans ölçümü Pentium IV 1.7 GHZ işlem gücüne sahip bir bilgisayarda yapılmıştır (Kodaz, 2003).

Çizelge 3.2 RSA algoritmasının performans ölçüm çizelgesi

Anahtarda Kullanılan Bit Sayısı	**Anahtar Oluşturma Süresi (saniye)**	**Şifreleme Süresi (saniye)**
64	0.021	0.011
128	0.026	0.013
256	0.083	0.015
512	0.307	0.018
1024	2.985	0.106
2048	50.432	0.766
4096	798.625	18.687

4. AÇIK ANAHTAR ALTYAPISI

Açık Anahtar Altyapısı kriptolojik algoritmaları kullanarak güvenilir bir haberleşme ortamı sağlar. AAA güvenilir haberleşmeyi sağlamak için kimlik doğrulama, inkâr edememe, veri bütünlüğü ve veri gizliliğini sağlar (Çelikyılmaz, 2005). Farklı bir ifade ile AAA'nın temel görevi; elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar ve cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır (Sağıroğlu ve Alkan, 2005).

AAA'da asimetrik algoritmalar kullanılır. Bu sebeple, haberleşen tarafların kullanmış oldukları anahtarlar farklıdır. Her bireyin açık ve gizli anahtarı vardır. Bu anahtarlar kullanılarak tarafların güvenli bir şekilde haberleşmesi sağlanmaktadır.

AAA günümüzdeki en güvenilir haberleşme şeklidir. Sistemin şifresini çözmek için tek yol anahtarları bilmektir. Anahtarları brut force* yöntemiyle tespit etmek bile yıllar almaktadır. Kurulan sistemlerde belirli aralıklarla anahtarların değiştirildiği de düşünülür ise sistem güvenliğinin tehlikeye girmesi hemen hemen imkânsızdır.

4.1 Veri Gizliliği İşlevi

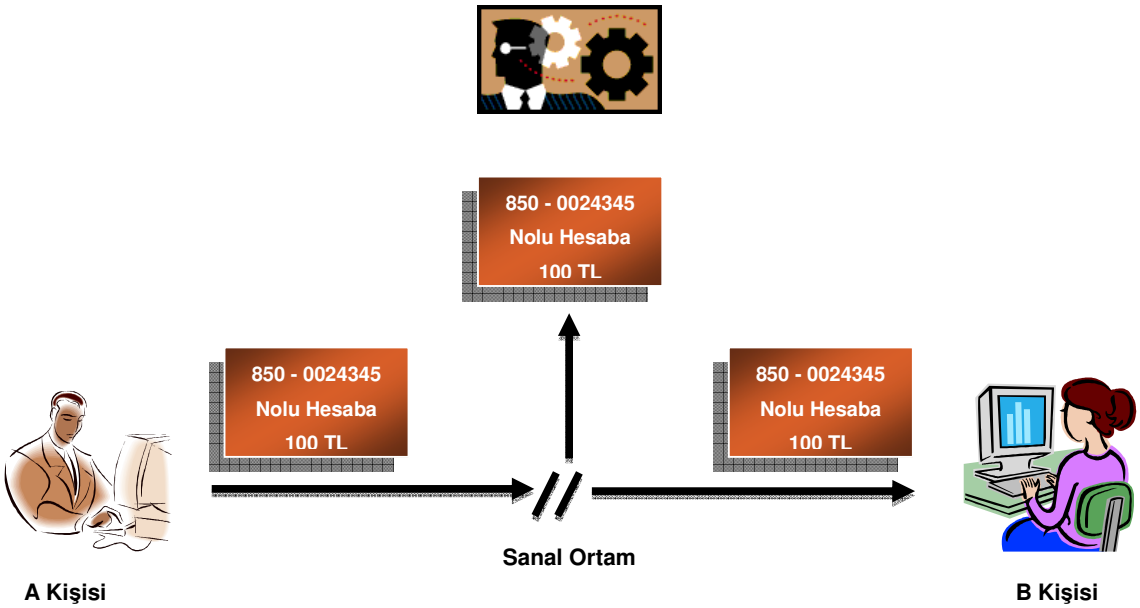
Gizlilik haberleşmenin en önemli unsurudur. Tarih boyunca gizliliği sağlamaya yönelik çok farklı çözümler kullanılmıştır. Yakın tarihimizden itibaren mühürlü zarf kullanımı gizlilik sağlamaya yönelik çözümlerden biri olmuştur. Haberleşmenin elektronik ortama taşınması ile beraber klasik yöntemlerin yerini şifreleme algoritmaları almıştır.

Veri Gizliliği işlevi, taraflar arasındaki iletişimin üçüncü kişiler tarafından bilinmesinin önüne geçilmesidir. Şekil 4.1'de görüldüğü gibi A kişisi B kişisi ile elektronik ortamda haberleşmektedir. Burada veri gizliliğini sağlamaya yönelik herhangi bir yöntem kullanılmamıştır. Bu şekil bir iletişimde 3. bir kişi A kişisinin göndermiş olduğu verinin içeriğinden haberdar olmaktadır. Burada bu durumdan A kişisi de B kişisi de habersizdir. Günümüzde, birçok elektronik haberleşme veri gizliliği sağlanmadan yapılmaktadır. Bu örnekte tek çözüm, A kişisinin göndermiş olduğu verinin şifrelenmesidir. Verinin önemine göre simetrik veya asimetrik algoritmalar kullanılmalıdır. Sürekli bir veri akışı var ise performans nedeni ile simetrik algoritmaların seçilmesi daha doğru bir çözümdür.

AAA 'da veri gizliliği de şifreleme yapılarak sağlanmaktadır. Bir sonraki adımda görüleceği üzere asimetrik algoritmalar kullanılarak veri gizliliği sağlanmaktadır.

---

* Brut Force: Olabilecek tüm şifreleri tek tek deneme yöntemidir.

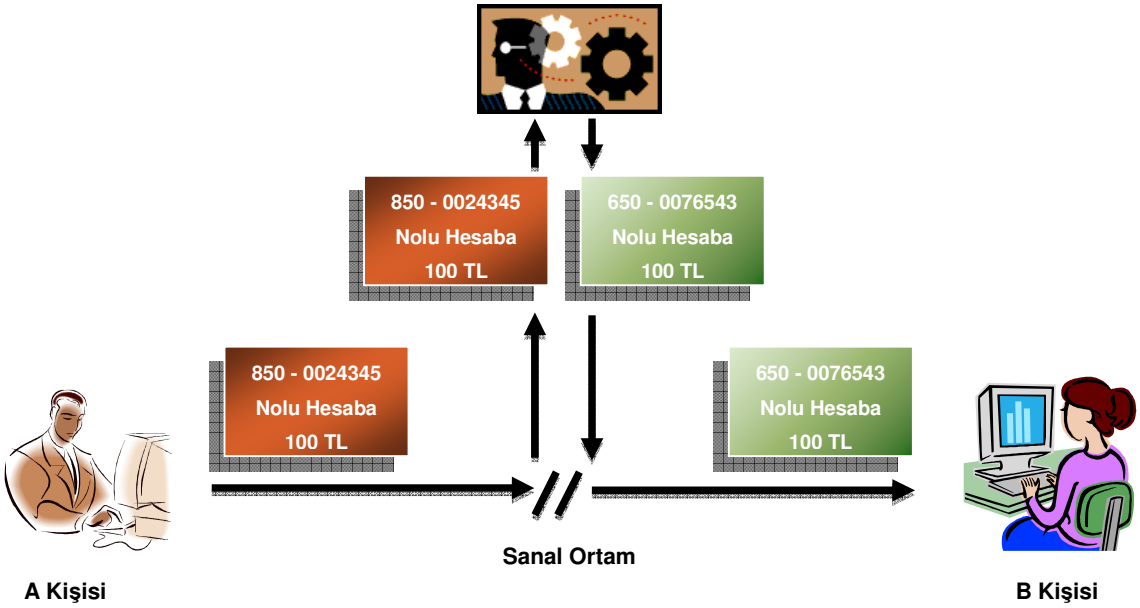


Şekil 4.1 Veri gizliliği

4.2 Veri Bütünlüğü İşlevi

Veri Bütünlüğü işlevi, taraflar arasındaki haberleşmeye konu olan verinin 3. bir kişi tarafından değiştirilmemesidir. Günlük yaşantımızda, veri bütünlüğünün tam anlamıyla sağlandığı söylenemez. Kıymetli evrakların üzerinde dahi tahrifat yapıldığı bilinmektedir.

Şekil 4.2'de A kişisi B kişisi ile elektronik ortamda haberleşmektedir. Bu haberleşmede veri bütünlüğünü sağlamaya yönelik herhangi bir yöntem kullanılmamıştır. Bu şekil bir haberleşmede araya giren 3. bir kişi A kişisinin göndermiş olduğu verinin içeriğini kendi çıkarları doğrultusunda değiştirmiştir. Başka bir ifade ile veri bütünlüğü bozulmuştur. Bu şekil bir haberleşmenin veri bütünlüğünü sağlamaya yönelik bir çözümü olmadığı için tarafların verinin bütünlüğünün bozulduğundan haberi yoktur. Karşılıklı haberleşen taraflar gelen veriyi doğru kabul ederek işlemektedir. Böyle bir haberleşme yapısı günümüz şartlarında suiistimal edilmeye çok müsaittir.



Şekil 4.2 Veri bütünlüğü

Elektronik ortamda veri bütünlüğünü sağlamak için özetleme algoritmaları kullanılmaktadır. Özetleme algoritmaları temel olarak, girdi olarak almış oldukları veriyi işleyerek, sabit uzunlukta eşsiz bir veri oluştururlar. Oluşturulan bu veri özet veya özüt olarak adlandırılır. Bu özet veriden ana veriye ulaşmak mümkün değildir.

Haberleşmede veri bütünlüğünün sağlanması için kurulan sistemde her iki tarafta da aynı özetin elde edilmesi gereklidir. Dolaylı olarak, elde edilen özüt gönderilecek verinin imzası olarakta tanımlanabilir.

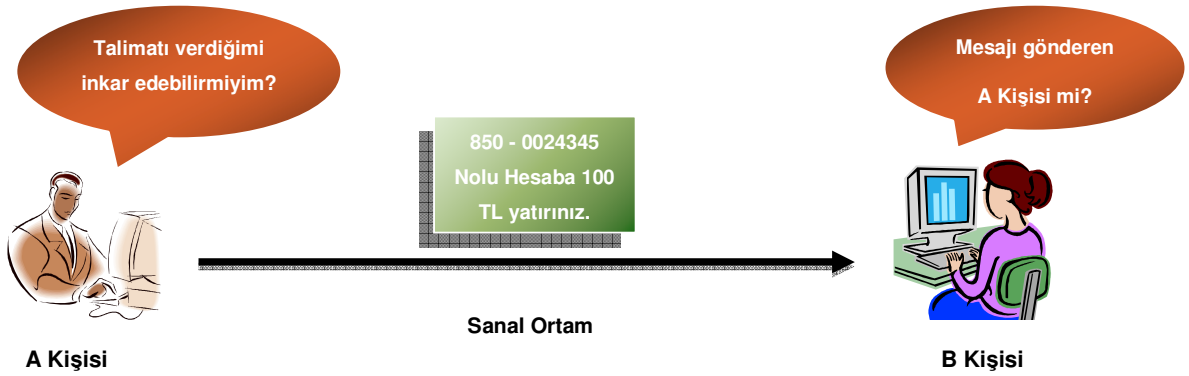
Günümüzde kullanılan birçok özetleme algoritması vardır. Bunlardan en fazla bilenenler SHA-1, SHA-2 MD5 ve RIPE-MD-160'dır. MD5 algoritması girdi olarak aldığı verinin uzunluğu ne olursa olsun 128 bit uzunluğunda bir özet çıkartır. MD5 algoritması günümüze kadar en fazla kullanılan algoritma olmasına rağmen, son yıllarda yapılan çalışmalar ile birlikte bazı zayıflıkları tespit edilmiştir. SHA-1 algoritması 160 bit uzunluğunda bir özet oluşturmaktadır. Performans olarak MD5 algoritması SHA-1 algoritmasından %25 daha performanslı çalışmaktadır. Fakat saldırılara karşı zayıflıkları sebebi ile günümüzde uygulamalarda SHA–1 algoritması kullanılmaktadır. Özetleme algoritmalarında standart olarak kabul edilen algoritma SHA-1 algoritmasıdır. Oluşturulan örnek modelde de veri bütünlüğünü sağlamak için SHA-1 algoritması kullanılmıştır.

Elektronik ortamda özetleme algoritmalarının kullanılmasının bir sebebi de dosya boyutu

büyüdükçe transfer edilecek verinin boyutunun artmasıdır. Özetleme algoritmaları ana metnin boyutu ne olursa olsun aynı uzunlukta bir veri oluşturmaktadır. Bu sebeple transfer edilecek verinin boyutu daha düşük olacağı için daha efektif bir çözüm olmaktadır.

4.3 Kimlik Doğrulama İşlevi

Kimlik Doğrulama işlevi, haberleşen tarafların karşılıklı olarak birbirlerinin kimliklerini tanımlamasıdır. Günlük hayatta bu işlem, kişinin nüfus cüzdanı, ehliyet veya pasaportu ile sağlanmaktadır. Oysaki sanal ortamda bu şekilde bir kimlik doğrulaması yapmamız mümkün değildir.



Şekil 4.3 Kimlik doğrulama ve inkar edememe

Şekil 4.3'te görüldüğü gibi A kişisi B kişisi ile haberleşmektedir. B kişisi A kişisinden gelen mesajı aldığında, mesajı gönderen kişinin A kişisi olduğunu hiçbir surette doğrulayamamaktadır. Aynı şekilde A kişisi de mesajın B kişisine gittiğini doğrulayamamaktadır.

Elektronik ortamda kimlik doğrulama işlemi için, kişinin sanal ortamdaki kimliklerini ifade eden elektronik sertifikalar kullanılmaktadır. Elektronik sertifikalara bir sonraki bölümde değinilecektir.

4.4 İnkâr Edememe İşlevi

İnkâr Edememe işlevi, haberleşen tarafların yapmış oldukları haberleşmeye ilişkin her türlü işlemi inkâr edememesidir. Günlük hayatımızda bu işlem için tek çözüm işlemi yapan kişinin

ıslak imzasının alınmasıdır. Fakat bu işlem bile bazen ihtilaflara neden olmaktadır. Kişi imzasını reddetmekte ve sonrasında doğrulama süreci için zorlu bir süreç başlamaktadır.

Şekil 4.3'te görüldüğü gibi elektronik ortamda haberleşen A kişisi mesajı gönderdiğimi inkar edebilir miyim diye düşünmektedir? Aynı şekilde mesajı alan B kişiside mesajı aldığını inkâr edebilir. Tüm bu suiistimaller elektronik ortamda yukarıdaki gibi bir haberleşmede mümkün olabilmektedir. Bu sebeple elektronik ortamda inkâr edememe sağlanmalıdır.

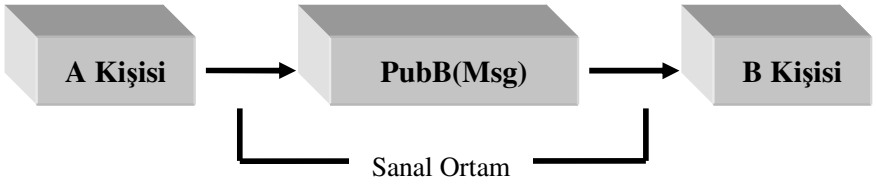
Elektronik ortamda inkâr edememe, kişinin elektronik sertifikası ile bağlı olan ve elektronik imzasını ifade eden usb dongle veya akıllı kartlar ile sağlanmaktadır.

4.5 Açık Anahtar Altyapısı Kullanan Bir Haberleşme Senaryosu

A kişisi ile B kişisinin Açık Anahtar Altyapısı kullanarak haberleşeceği bir senaryonun aşamaları aşağıdaki gibidir.

Her iki kişinin de açık ve gizli anahtarları vardır. Her iki kişide birbirlerinin açık anahtarlarına erişebilmektedir.

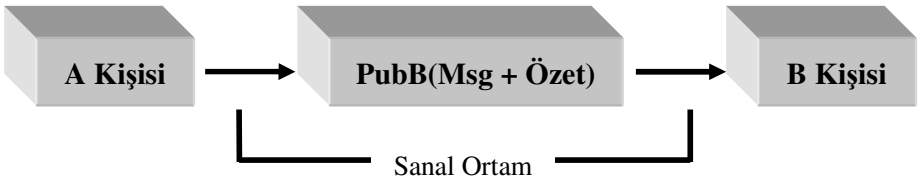
A kişisi B kişisine sanal ortamda gizliliği sağlanmış bir mesaj göndermek istediğinde, A kişisi göndereceği mesaj B kişisinin açık anahtarı ile şifrelenir. Şifrelenen bu mesaj B kişisine gönderilir (Şekil 4.4). Sanal ortamda 3. bir kişi tarafından bu mesaja erişilse dahi yalnızca B kişisinin gizli anahtarı ile şifre çözülebileceğinden 3.kişi bu mesajın içeriğine erişemez. Mesaj B kişisine ulaştıktan sonra, B kişisinin gizli anahtarı ile şifre çözülerek mesaja erişilir. Bu şekil bir haberleşmede AAA işlevlerinden olan gizlilik sağlanmış olur.



Şekil 4.4 AAA gizlilik işlevi

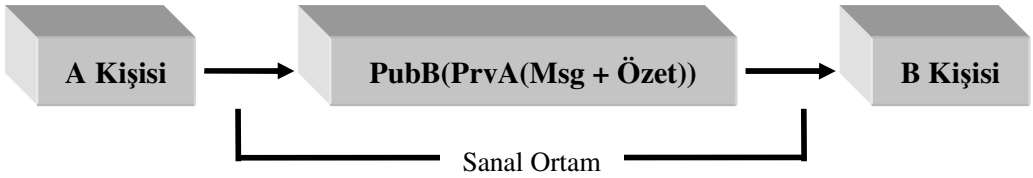
A kişisi B kişisine gizliliği ve veri bütünlüğü sağlanmış bir mesaj göndermek istediğinde, A kişisi tarafından gönderilecek mesajın özet algoritması ile özeti çıkartılır. Mesaj özeti çıkartıldıktan sonra, mesaj ve mesaj özeti B kişisinin açık anahtarı ile şifrelenir. Şifrelenen bu mesaj B kişisine gönderilir (Şekil 4.5). Sanal ortamda aktarım esnasında 3. bir kişi tarafından bu mesaja erişilse bile hiçbir şekilde içeriğine erişilemez. Mesaj B kişisine ulaştıktan sonra, B kişisinin gizli anahtarı ile şifre çözülür. Şifresi çözülen paketten mesaj ve mesaj özetine

ulaşılır. Özet algoritması kullanılarak mesajın özeti çıkartılır. Çıkartılan özet ile şifresi çözülen paketteki özet karşılaştırılır. Eğer karşılaştırılan özetler aynı ise sanal ortamda transferi esnasında hiçbir değişikliğe uğramadığı anlaşılır. Başka bir ifade ile veri bütünlüğü sağlanmış olur.



Şekil 4.5 AAA veri bütünlüğü işlevi

A kişisi B kişisine gizliliği, veri bütünlüğü, kimlik doğrulama ve inkâr edilememe işlevlerinin tümünün sağlandığı bir mesaj göndermek istediğinde, ilk olarak A kişisi tarafından mesajın özeti çıkartılır. Daha sonra, gönderilecek mesaj ve çıkartılan özet A kişisinin gizli anahtarı ile şifrelenir. Bir sonraki aşamada şifrelenen bu mesaj B kişisinin açık anahtarı ile şifrelenir (Şekil 4.6).



Şekil 4.6 AAA kimlik doğrulama ve inkar edememe işlevi

Son oluşturulan şifreli mesaj sanal ortamda transfer edilecek mesajdır. A kişisi tarafından gönderilen bu şifreli mesaj sanal ortamdan B kişisine ulaştırılır. B kişisi gelen şifreli mesajı kendi gizli anahtarı ile çözer. Bu aşamada veri gizliliği sağlanmış olur. Şifresi çözülen mesaj A kişisinin açık anahtarı ile tekrar şifresi çözülür. A kişisinin açık anahtarı bu şifreli mesajı çözer ise, bu mesajın A kişisi tarafından oluşturulduğu anlaşılır. Başka bir ifadeyle kimlik doğrulama ve inkâr edememe işlevleri sağlanmış olur. Şifresi çözülen mesajdan elde edilen mesajın özet algoritması ile özeti çıkartılır. Çıkartılan bu özet ile şifresi çözülen mesajdan çıkan özet karşılaştırılır. Eğer özetler aynı ise veri bütünlüğü işlevi de sağlanmış olur.

5. ELEKTRONİK İMZA

Elektronik imza, tez konusu olan sanal noterin en önemli bileşenidir. Noterin sanal ortamda teknolojik modellenmesi, elektronik imza üzerine kurulmuştur. Bu sebeple elektronik imza bu bölümde ayrıntılı olarak ele alınacaktır.

5.1 Elektronik İmza Kavramı

Elektronik imza, günlük hayatta elle atılan ıslak imzanın, sanal ortamda elektronik olarak modellenmiş karşılığıdır. Elektronik imza çok geniş bir kavramdır. Islak imzanın tarayıcıdan geçirilerek elektronik olarak ifade edilmesi de elektronik imza kavramı içine girer. Bunun yanında son yıllarda yapılan çalışmalar ile göz retinası, parmak izi ve kişinin fiziki özelliklerinin elektronik olarak ifade edilmesi de elektronik imza kavramı içine girmektedir.

Tezde kullanılan elektronik imza ifadesi, ülkemizde kabul edilen 5070 sayılı Elektronik İmza Kanunu'nu esas almaktadır. 5070 sayılı Elektronik İmza Kanunu'nda elektronik imza, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar." şeklindedir [5]. Kanunda yapılan tanımlamaya göre elektronik imza, tarayıcıdan geçirilerek elde edilen imza ya da göz retinasının elektronik ifadesi vb. ifadeleri kastetmemektedir. Kanunda tanımlanan elektronik imza, bir önceki bölümde ele alınan Açık Anahtar Altyapısını temel olarak işaret etmektedir. Bundan sonraki tanımlamalarda tez içeriğinde geçen elektronik imza, kanunda tanımlanan kavramı ifade etmektedir.

Elektronik imza, tıpkı ıslak imzada olduğu gibi kişinin kimliğine bağlı olan bir elektronik veridir. Islak imzada olduğu gibi kişinin tek bir elektronik imzası yoktur. Elektronik imza, imzalanacak elektronik verinin içeriğine göre değişir. Başka bir deyişle, imzalanacak elektronik veride bir karakter bile değişse elektronik imza değişir.

Elektronik imza, elektronik ortamda imzalanmış bir verinin bütünlüğünün sağlanması, elektronik veriyi imzalayan kişinin kimlik doğrulamasının yapılması ve imzalanmış elektronik verinin inkâr edilmemesini sağlar. Burada AAA' da sağlanan dördüncü işlev haberleşmede veri gizliliği, elektronik imza tarafından sağlanmaz. Bunun sebebi AAA' da haberleşmede gönderilecek veri şifrelenir iken, elektronik imzada sadece verinin özeti şifrelenir. Şifrelenmiş bu özette verinin elektronik imzasını ifade eder. Elektronik imzada gönderilecek verinin şifrelenmemesinin nedeni kanuni düzenlemelerdir.

5.2 Elektronik İmzanın Teknolojik Altyapısı

Elektronik İmza AAA üzerine kurulmuş bir yapıdır. AAA' da haberleşmek isteyen her bireyin açık ve gizli anahtarları vardır. Elektronik imza kullanılarak haberleşmek isteyen her bireyin ise açık anahtarını muhafaza eden elektronik sertifikası ve gizli anahtarını muhafaza eden USB token ya da akıllı kartı vardır.

Elektronik imza teknolojik altyapısında, elektronik sertifikaların tanımlanması, akıllı kartların üretilmesi, elektronik imzanın doğrulama süreçlerinin sağlanması ve tüm bu sistemin yönetimini sağlayan bir kurum vardır. Bu kurum Elektronik Sertifika Hizmet Sağlayıcısıdır.

5.2.1 Elektronik Sertifikalar

Elektronik sertifikalar, günlük hayatta kullanmış olduğumuz nüfus cüzdanı, ehliyet, pasaport vb. kimlik kartlarının elektronik ortamdaki karşılığıdır.

Elektronik sertifikalar, kişi için üretilen anahtar çiftlerinden açık anahtarı, kişinin kimlik bilgisine bağlayan elektronik kayıtlardır. Başka bir ifadeyle elektronik sertifikalar kişinin sanal ortamdaki kimlik kartı olarak ifade edilebilir.

Elektronik sertifikaların içeriğinde, kişinin açık anahtar bilgisi, kişinin kimlik bilgisi, sertifika teknik bilgileri ve sertifikayı yayınlayan ESHS'ın elektronik imzası bulunur (Şekil 5.1).

Elektronik sertifikaların temel görevi, kişinin sanal ortamda kimliğini belirlemek ve yapılan işlemin inkâr edilmemesini sağlamaktır.

Elektronik sertifikaların üretimi, yayınlanması, doğrulanma süreci ve sona erdirilmesi vb. tüm işlemler Elektronik Sertifika Hizmet Sağlayıcı tarafından yapılır.

5070 Sayılı Elektronik İmza Kanununda belirtildiği üzere elektronik sertifika kayıtlı bir ESHS tarafından verilir ise Nitelikli Elektronik Sertifika olarak tanımlanır. NES'ler içerik olarak eşsiz olan sertifikalardır. Bu sertifikalar yalnızca bir kişiye bağlıdır. Ülke üzerinde hizmet veren farklı bir ESHS ya da aynı ESHS'da aynı sertifika başka bir kişiye bağlı olamaz. NES'ler Uluslararası Telekom Birliği standartlarına göre X.509 standardında tanımlanırlar. Bu standart IETF tarafından RFC 2459 olarak yayınlanmıştır.

NES'lerin belirli bir kullanım süresi vardır. Bu sürenin sonunda sertifika yenilenir veya iptal edilir. Hiçbir zaman hiçbir ESHS tarafından süresiz NES tanımı yapılmaz.

Nitelikli Elektronik sertifika sahibi gizli anahtarını içeren USB token ya da akıllı kartını kaybetmesi ya da benzer bir durumda, ESHS ile iletişime geçilerek kişinin elektronik sertifikası iptal edilir.

NES'ler kullanım süresinin dolması ya da başka bir sebeple geçersiz olsa bile, ESHS tarafından arşivlenirler. Sertifikanın geçerli olduğu zaman diliminde yapılan işlemlerin doğrulanması için bu işlem gereklidir. Çünkü günlük hayatta olduğu gibi sanal ortamda da geçmiş işlemlerin geçerliliğinin sorgulanma ihtiyacı vardır.

Sertifika Seri No	**59014325431**
Sertifika Sahibinin Kimlik Bilgileri	**Dursun Akçeme**
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 Elektronik İmzası	**4t 4a 31 e8 9y 3d fa 3e 0a b7 dd 70 71 c7 51 7c 45 83 4f 11**

Şekil 5.1 Elektronik sertifika örneği

5.2.2 Elektronik Sertifika Hizmet Sağlayıcı

Elektronik Sertifika Hizmet Sağlayıcıları, kişi ya da kurumlara nitelikli elektronik sertifika tanımlayan ve tanımlamış olduğu sertifikaların yönetim işini üstlenen güven makamlarıdır. Tezin amacına uygun bir tanım verilmek istenirse; ESHS'lar sanal ortamda noter işlemlerini gerçekleyebilmek için hukuki geçerliliği olan teknolojik altyapıyı temin eden kurumlardır.

ESHS'lar özünde noterler ile aynı amaca hizmet etmektedirler. Her iki kurum da güven makamıdır. Noterlerin de ESHS'ların da kayıtları resmi makamlarca esas kabul edilir. Noterler devletin bir kurumudur. ESHS'lar ise devletin kurmuş olduğu bir kurum olabileceği gibi Bilgi Teknolojileri ve İletişim Kurumu denetiminde özel kurumlarda olabilmektedir.

ESHS'lar, sanal ortamda elektronik veriler ile işlem yapan kişinin kimliğini doğrular ve kişinin yaptığı işlemi inkâr etmemesini sağlar. Tüm bu işlemler nitelikli elektronik sertifikalar kullanılarak yapılır. Burada dikkat edilmesi gereken husus, ESHS'ların bir noter gibi işlem yapmıyor olmasıdır. ESHS'lar sadece doğrulama işlemini yapmaktadırlar, noterler gibi ihtarname, defter onayı, elektronik belgelerin arşivlenmesi vb. yapmamaktadırlar. ESHS'ların

doğrulama sürecine ilişkin yapmış olduğu elektronik kayıtlar, noter kayıtları gibi resmi makamlarca esas kabul edilir.

Ülkemizde şu anda hizmet veren dört ESHS vardır (Çizelge 5.1). 5070 Sayılı Elektronik İmza Kanunu'nun kabulü ile ilk kurulan ESHS'lardan biri TUBİTAK-UEKAE'dir. TUBITAK-UEKAE devlet desteği ile kurulan bir kamu ESHS'dır. Yapılan yasal düzenlemeler ile TUBITAK-UEKAE sadece kamu kurumu çalışanlarına nitelikli elektronik sertifika vermektedir. Vatandaşlar ve işletmeler diğer ESHS'lardan nitelikli elektronik sertifika alabilmektedirler.

Çizelge 5.1 Türkiye'deki elektronik sertifika hizmet sağlayıcıları

Elektronik Sertifika Hizmet Sağlayıcı -TÜRKİYE-	**Bildirim Tarihi**	**Faaliyete Başlama Tarihi**
Elektronik Bilgi Güvenliği A.Ş.	25.03.2005	24.06.2005
TUBİTAK-UEKAE	31.03.2005	30.06.2005
TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	13.05.2005	16.07.2005
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.	20.06.2006	01.09.2006

ESHS'lar temel olarak üç birimden oluşmaktadır. Bu birimler kayıt makamı, sertifika makamı ve kök sertifika şeklindedir.

Kayıt makamı, nitelikli elektronik sertifika almak isteyen kişi ya da kurumun muhatap olduğu makamdır. Nitelikli elektronik sertifika almak isteyen kişi kuruma geçerli bir kimlik belgesi ile bizzat başvurur. Posta ya da elektronik ortamda başvuru kabul edilmemektedir. Fakat NES yenilemelerinde NES'in kullanım süresi bitmeden elektronik olarak başvuru da kabul edilmektedir. Kişinin kimlik doğrulaması yapıldıktan sonra, kişi ya da kurumu temsil eden kişiye NES sözleşmesi imzalatılarak başvurusu alınır.

Sertifika makamı ise, kayıt makamından gelen bilgilere göre kişi ya da kuruma NES verilmesinde hukuki bir engel yok ise kişinin kimliğine bağlı NES'i tanımlayıp yayınlayan birimdir. Bu makamda ilk olarak kayıt makamından gelen bilgilere göre eşsiz bir anahtar çifti üretilerek, açık anahtar verisi kişinin nitelikli elektronik sertifikasına konulur. Bu sertifika kişinin kimlik bilgisi ile bağlanır. Artık hukuki geçerliliği olan bu kayıt, kişinin sanal ortamda

kimliğini ifade etmektedir. Anahtarın diğer çifti olan gizli anahtar ise kişinin elektronik imza oluşturma aracı olan USB dongle ya da akıllı kartın içine konur. Tüm bu işlemler kontrollü bir vaziyette uluslararası standartlara uygun şekilde yapılır. Bu işlemi yapan kişi ya da kişiler kesinlikle işlem yaptığı kişinin gizli anahtarını bilemez ve sistemde göremez. Kişinin hiçbir suretle bu işleme ilişkin anahtar bilgilerinin kayıtları tutulamaz. Tüm bu işlemler her ESHS'ın kendi web adresinde yayınladığı Sertifika İlkeleri ve Sertifika Uygulama Esaslarına uygun şekilde yapılır. Bu sürece ilişkin gerekli denetlemeler Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılmaktadır. Tüm bu süreçten sonra kişinin nitelikli elektronik sertifikası üretilir. Kişinin talebi doğrultusunda kişinin NES'i, ESHS'ın bir dizininde yayınlanır. Oluşturulan bu NES'in üzerinde ESHS'ın elektronik imzası bulunmaktadır.

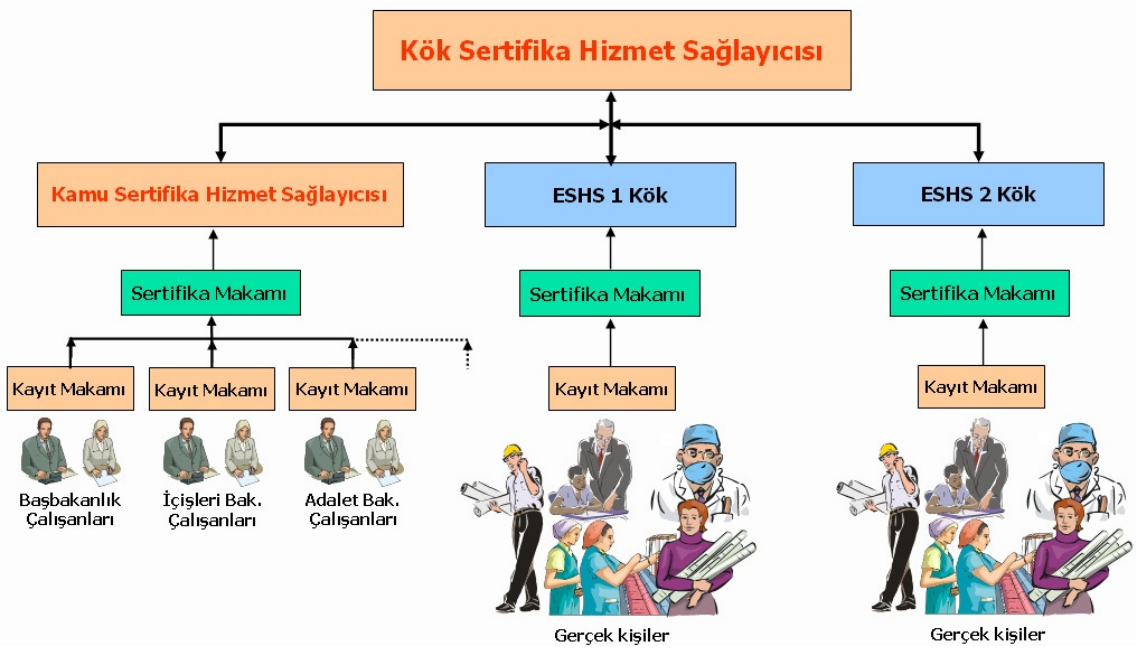
Kök Sertifika ESHS'ın yayınlamış olduğu NES'leri imzalayan birimdir. ESHS'ın elektronik imzası, yayınlamış olduğu NES'lerin güvenliği açısından çok önemlidir. Bu sebeple ESHS'ın en önemli bileşenidir. ESHS'ında kök sertifikasının da bağlı olduğu bir kök sertifika vardır. ESHS'ın NES'ini de o kök sertifika imzalar. Ülkemizde en üst düzeydeki kök sertifika TUBITAK-UEKAE'dır.

Ülkemizde olduğu gibi, diğer ülkelerde de birden fazla ESHS olabilmektedir. Bu durumda bunların hepsi merkezi kök sertifikaya bağlıdır. Böyle durumlarda her ESHS'ın NES'i daha önce belirtildiği üzere kök sertifika tarafından imzalanır. Farklı ESHS'lardan alınmış elektronik imzaların haberleşmesi durumunda, ESHS'lar kendi aralarında çapraz sertifikasyon yaparak iletişim kurarlar. Şekil 5.2 de ülkemizdeki ESHS'ların hizmet modeli görülmektedir (Çelikyılmaz, 2005).

Elektronik imza kullanılarak yapılan işlem taraflarından biri, elektronik imzayı doğrulamak istediğinde elektronik imza sahibinin NES'i kullanılır. ESHS'lar tarafından üretilen bu NES'ler belirli bir süre geçerlidir. Doğrulama yapacak kişi, elektronik imzanın sahibi onay vermiş ise ESHS'ın yayınlamış olduğu dizinden kişinin NES'ine ulaşır. Eğer kişi NES'inin yayınlanmasına izin vermediyse elektronik imza sahibinden NES'i talep edilmelidir.

ESHS'ın dizininden ya da kişiden alınan NES'in geçerliliğinin sorgulamak için iki farklı yol vardır. Bunlardan birincisi ESHS'ın internet adresinden iptal edilen NES'leri düzenli olarak yayınlanan listelerin kontrol edilmesidir. Yayınlanan bu listeler Sertifika İptal Listesi (SIL) olarak tanımlanır. İkinci yöntem ise NES'in iptal durumunu anlık olarak bize veren Çevrim İçi Sertifika Durum Protokolü (ÇİSDUP) yönteminin kullanılmasıdır. Bu yöntemde ESHS ile bağlantı kurularak, NES'in iptal durumu bilgisi ESHS'ın elektronik imzası ile imzalanarak kişiye döndürülür.

Bir NES'in iptal durumu kontrol edilecek ise ilk olarak SIL listelerinde kontrol edilmesi gereklidir. İptal edilmiş ise gereksiz yere ÇİSDUP yöntemi ile veri trafiğinin önüne geçilmiş olur. Bir NES'in iptal durum kontrolünde hangi yöntem (SIL ya da ÇİSDUP) kullanılırsa kullanılsın mutlak suretle üzerlerindeki elektronik imza kök sertifikaya ulaşıncaya kadar doğrulanmalıdır.



Şekil 5.2 ESHS'ların hizmet modeli

ESHS'ların temel görevleri aşağıdaki gibidir.

- 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
- Sertifika ilkeleri (Sİ) ve Sertifika Uygulama Esaslarına göre hizmet verme
- Tüm bu hizmetleri sürekli kılma

5.2.3 Elektronik İmza Donanımı

Elektronik imzayı oluşturmak için kişinin gizli anahtar verisi şifreli olarak bir donanımda

tutulur. Bu donanım USB token ya da akıllı kart olabilir (Şekil 5.3). Kullanılan bu donanımlar yalnızca bir kere veri yazılabilen donanımlardır. Yazılan gizli anahtar bilgisi hiçbir suretle donanım dışına çıkarılamaz.

Şekil 5.3 Elektronik imza donanımları

Elektronik İmza donanımları EAL-4+* uluslararası standardında olmalıdır. Elektronik İmza donanımları harici güvenlik olarak şifre bilgisi ile korunur. Bu şifreyi yalnızca elektronik imza donanımının sahibi bilir. ESHS tarafından kişiye kapalı bir zarf ile bu şifre bilgisi ulaştırılır. Bu şifre girilmeden işlem yapılamaz. Şifre girildikten sonra gizli anahtar bilgisi üretilerek elektronik imza oluşturulmak için kullanılabilir.

Bu donanımların içerisinde donanım sahibinin elektronik sertifikası da bulunmaktadır. Uygun yazılımlar ile istenildiği takdirde sertifika görüntülenebilmekte ve farklı bir ortama alınabilmektedir.

5.3 Modelde Veri Gizliliğin Sağlanması

Elektronik imza teknolojisinde, sadece elektronik verinin özeti şifrelendiği için veri gizliliği sağlanamamaktadır. Fakat sanal ortamda elektronik imza ile gerçeklenecek projelerde mutlak suretle veri gizliliği sağlanmalıdır. Elektronik imza kullanılan bir sistemde veri gizliliğini sağlamak için kriptoloji biliminden yararlanır.

Sanal ortamda veri gizliliğini sağlamak için kriptoloji temeline dayanan SSL kullanılır. SSL anahtar tabanlı kriptografik bir yöntemdir. Asimetrik algoritmalar kullanır.

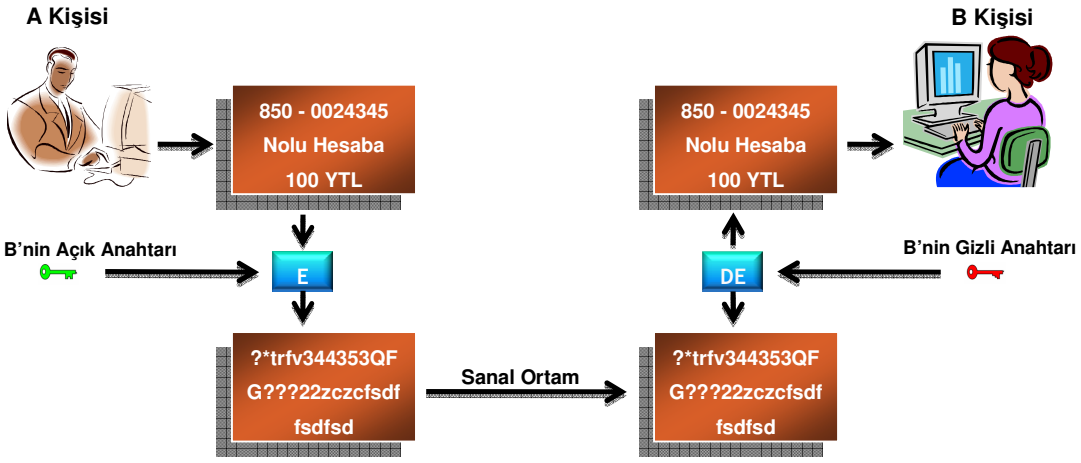
SSL'in çalışma prensibi, A kişisi B kişisine veri gizliliği sağlanmış bir mesaj göndermek istediğinde, B kişisinin anahtar çiftinden açık anahtar ile şifreler. Şifrelenmiş mesaj sanal ortamda B kişisine ulaşır. Şifrelenmiş mesaja sanal ortamda erişilse bile, sadece B kişisinin gizli anahtarı ile açılabileceğinden içeriğine ulaşılamayacaktır. Şifrelenmiş mesaj B kişisine

* EAL-4+: Metodik olarak geliştirilmiş ve test edilmiş güvenlik seviyesi.

ulaştığında B kişisi gizli anahtarı ile mesajın şifresini çözerek mesaja ulaşacaktır (Şekil 5.4).

SSL protokolü günümüzde gizliliğin önem arz ettiği birçok kurumun haberleşmesinde kullanılmaktadır. Özellikle yurt genelinde birçok şubesi olan bankaların genel müdürlüğü ile şubeleri arasındaki haberleşme SSL ile yapılmaktadır. Aynı şekilde bankaların internet şubelerinin hepsinde müşteri ile banka arasındaki iletişim SSL protokolü ile sağlanmaktadır. Sanal ortamda ülkemizde ve dünyada elektronik imza ile gerçeklenen hemen hemen tüm uygulamalarda veri gizliliği SSL ile sağlanmaktadır.

SSL'de kullanmak için anahtar çiftlerinin üretimi, yönetimi vb. işlemleri özel kuruluşlar üstlenmiştir. Bu konuda ülkemizde ve dünyada çözüm geliştiren birçok kurum mevcuttur.

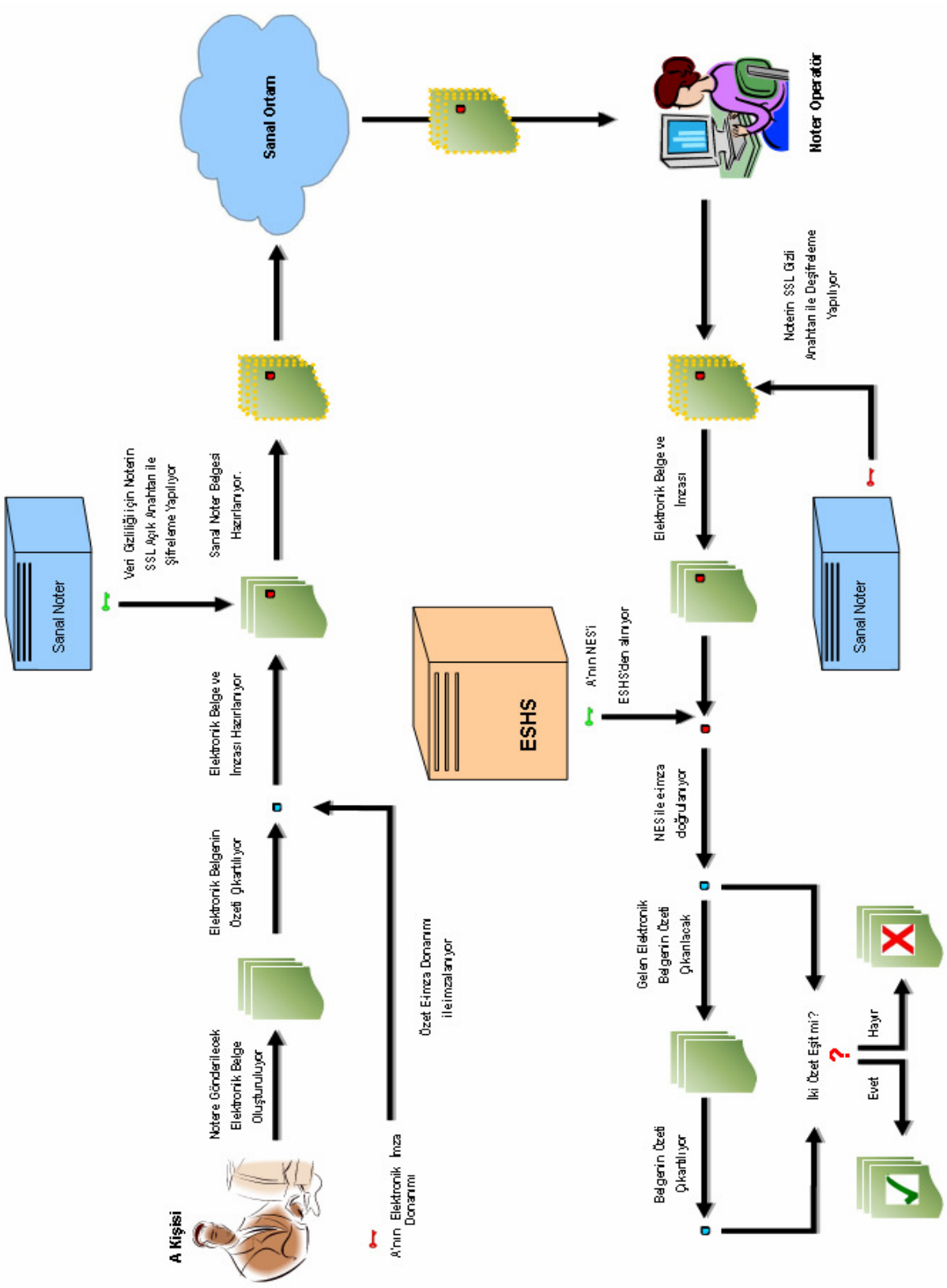


Şekil 5.4 SSL ile haberleşme örneği

5.4 Elektronik İmza Kullanan Bir Haberleşme Senaryosu

Senaryoda, sanal ortamda bir noter ile A kişisi haberleşmektedir. A kişisi elektronik imza sahibidir. Senaryoda, A kişisinin elektronik imzasını kullanarak bir elektronik belgeyi notere ulaştırma süreci ele alınmıştır.

Şekil 5.5'te görüldüğü gibi, ilk olarak A kişisi tarafından notere gönderilecek elektronik belge (ihtarname, tebligatname, elektronik defter vb.) oluşturulur.



Şekil 5.5 Elektronik imza kullanan bir haberleşme senaryosu

Elektronik belge oluşturulduktan sonra özetleme algoritması (SHA–1) ile elektronik belgenin özeti çıkartılır. Çıkartılan bu özet, A kişisinin elektronik imza donanımı ile şifrelenerek elektronik belgenin elektronik imzasını oluşturulur. Elektronik imza elde edildikten sonra elektronik belgeyi ve elektronik imzayı içeren bir paket haline getirilir. Elektronik imza elde edildikten sonra gizliliği sağlamak için SSL sunucudan açık anahtar alınır. İmza ve belgeyi içeren paket SSL sunucudan alınan açık anahtar ile şifrelenir. Bu işlemden sonra notere gönderilecek elektronik veri hazırlanmıştır.

Hazırlanan elektronik veri sanal ortamda A kişisi tarafından notere ulaştırılır. Bu süreçte elektronik veri üçüncü bir kişi tarafından elde edilse bile hiçbir anlam ifade etmez. 3. kişi elektronik belgenin içeriğine ulaşamaz. 3.kişi tarafından elektronik belgenin içeriği değiştirilirse doğrulama sürecinde bu durum tespit edilir. Bu durumda, elektronik imza geçersiz olmaktadır.

Elektronik veri notere ulaştığında, A kişisinin göndermiş olduğu elektronik belgeye ulaşmak için doğrulama işlemleri yapılır. İlk olarak SSL sunucudan sadece noter tarafından bilinen gizli anahtar bilgisi alınır. Bu anahtar bilgisi ile sanal ortamdan gelen verinin şifresi çözülür ise veri gizliliğinin sağlandığı sonucuna varılır ve işleme devam edilir. Şifre çözme işleminden sonra A kişisinin göndermiş olduğu elektronik belge ve bu belgenin elektronik imzası ortaya çıkmıştır. Fakat bu elektronik belgenin kim tarafından gönderildiği henüz doğrulanmamıştır. Bu süreç için, A kişisinin NES'i ESHS'dan alınır. Alınan NES'in geçerliliğine yönelik SIL listeleri ve ÇİSDUP ile geçerliliği kontrol edilir. NES geçerli ise NES'deki açık anahtar ile elektronik imzanın şifresi çözülür. NES'teki açık anahtarın elektronik imzanın şifresini çözmesi kişinin kimliğini doğrular ve inkâr edememesini sağlar. Şifre çözme sonucu bir elektronik veri (X özeti) ortaya çıkar. Gelen elektronik veriden elde edilen elektronik belgenin özetleme algoritması (SHA–1) ile özeti (Y özeti) elde edilir. Eğer iki özet aynı ise veri bütünlüğünün de sağlandığı sonucuna varılır.

Yukarıdaki senaryoda noter tarafında, elektronik belgenin gizliliği, elektronik belgenin bütünlüğü, kimlik doğrulama ve elektronik belgenin inkâr edilememesi sağlanmıştır. Günlük hayatta yaptığımız noter işlemlerinde olduğu gibi gerekli koşullar yerine getirilmiştir.

Bu senaryoda, tezin amacı olan sanal noterin ne şekilde gerçeklenebileceği görülmektedir. Temelde tüm noter işlemleri bu dört koşul yerine getirilerek yapılır. Hukuki sınırlamalar ve işin mahiyetinden dolayı yapılamayacak noter işlemleri bu söylemin dışındadır.

6. ELEKTRONİK İMZA İLE YAPILABİLECEK NOTERLİK İŞLEMLERİ

Daha önceki bölümlerde belirtildiği gibi, elektronik imza ile tüm noter işlemlerini sanal ortamda modellemek mümkün değildir. Fakat bir önceki bölümde ele alınan senaryoda, noterin bir işlem yapmak için gerekli temel koşulların sanal ortamda ne şekilde gerçeklenebileceği görülmüştür. Bu sonuca göre, noterin kişisel bilgisini gerektiren, muhakemesine ihtiyaç duyulan ve elektronik imza ile yapılamayan işlemlerin dışında ki noter işlemleri sanal ortamda yapılabilir. Sanal ortamda noter işlemleri yapabilmek için teknolojik modellemenin yanında hukuki düzenlemeler (yönetmelik, tebliğ, genelge vb.) de yapılmalıdır. Bir sonraki bölümde, ihtiyaç duyulan hukuki düzenlemeler ele alınacaktır.

Sanal ortamda yapılacak noter işlemleri belirlenir iken, noterlik kanunu ve mevcut hukuki yapı temel alınarak belirlenmiştir. Bu işlemlerin sayısı hukuki düzenlemeler ile arttırılabilir.

Sanal ortamda gerçeklenebilecek noterlik işlemleri altı başlık altında incelenecektir (Akçeşme ve Sönmez, 2008).

- Elektronik belgeye, elektronik zaman damgası vurmak.
- Elektronik belgenin elektronik imzasını ve üzerindeki tarihi onaylamak.
- Elektronik belgenin saklanması ve istendiğinde belgelenmesi.
- Özel kanunda hükmü bulunmayan defterleri onaylamak.
- Tebligat işleri.
- İhtarname ve İhbarname işleri.

6.1 Elektronik Belgeye Elektronik Zaman Damgası Vurmak

Günlük hayatta özgün bir konuda yapılan çalışmaların, sahip ya da sahiplerinin fikri ve sınaî mülkiyetinde olduğunu kanıtlamak için zaman bilgisine ihtiyaç duyulur. Bu sebeple çalışmanın ya da fikrin sahip ya da sahipleri zaman bilgisini elde etmek için çeşitli kurumlara onaylatır veya kendilerine iadeli taahhütlü olarak gönderirler. Böylece gelecekte oluşabilecek ihtilaflar durumunda, hangi zamanda eserin ya da çalışmanın elinde olduğunu kanıtlamış olurlar.

Zaman bilgisini elde etmek için en çok tercih edilen yöntem, ilgili belgenin notere onaylatılmasıdır. Noterler, zaman bilgisini kayıt altına alarak hukuki geçerliliği olan belgeler düzenlerler. Zaman damgası hizmetine toplumun her kesiminde ihtiyaç duyulur (Mutlu ve Babür, 2008).

- Yazarlar (makale, senaryo, şiir, bilimsel eser vb.)
- Müzisyenler (şarkı, reklâm müzikleri, besteler vb.)
- Tasarımcılar (grafikler, fotoğraflar, mimari tasarımlar, iç mimari tasarımlar)
- Mutimedia ürün üretenler (CD, video, klip vb.)
- Kurumlar (Reklâm ajansları, yazılım firmaları, yayınevleri, çeviri büroları vb.)
- Bilim adamları ve AR-GE çalışanları
- Sağlık Kuruşları
- Diğer (İş fikri sahipleri, icat sahipleri, her türlü özgün fikir sahibi)

Yukarıdaki sınıflandırmada görüldüğü gibi toplumun hemen hemen her kesiminde zaman damgası ihtiyacı vardır.

Günlük hayatta yapılan birçok işlem elektronik ortama taşınmıştır. Örneğin özgün bir çalışma olarak sizlere sunulan bu yüksek lisans tez çalışması da bir bilgisayar yardımı ile elektronik ortamda yazılmıştır. Elektronik ortamda kopyalamanın ne kadar kolay olduğu düşünülür ise zaman damgası hizmetinin ne kadar önemli bir işlem olduğu anlaşılır. Çünkü bu tezin sunumu yapılmadan önce kopyalanıp başka bir amaçla kullanılması tüm çalışmanın farklı bir kişiye mal edilmesini ve haksız bir fayda edinimine sebep olur.

Fikirlerin ve çalışmaların çalınmasının ve izinsiz kullanılmasının önüne geçmek için tek çözüm o fikrin ya da çalışmanın sizin elinizde olduğu zaman bilgisini kanıtlamaktır. Bunun içinde tek çözüm zaman damgasıdır.

Zaman damgası hizmeti, Noterlik Kanunu'nun 60. maddesinin 4. bendinde "Bu kanuna uygun olarak dışarıda yazılıp getirilen kâğıtların üzerindeki imza, mühür veya herhangi bir işareti veya tarihi onaylamak" şeklinde düzenlenmiştir (TNB, 2007). Bu kanun maddesine göre noterler bir belge üzerinde herhangi bir işareti, tarihi, imzayı onaylayıp ve tarih atarak hukuki geçerliliğini sağlarlar.

Noterlik Kanunu'nda dikkat edilmesi gereken, noterin ilgili belgeye zaman damgası vurmak için içeriği ile ilgilenmemesidir. Başka bir deyişle noterin kişisel bilgisi ya da muhakemesini gerektirecek bir durum söz konusu değildir. Kişi istediği takdirde bir belgeye adını soyadını yazıp, bu belgeye zaman damgası hizmeti almak için noterde işlem yaptırabilir. Tez çalışmasının her bölümünde üzerinde durulan ("noterin kişisel bilgi ve muhakemesine ihtiyaç

duymayan işlemler sanal ortamda yapılabilir") modele göre zaman damgası hizmeti sanal ortamda yapılabilir.

Bu hizmet için, Elektronik İmza bölümünde işlenen senaryoya göre elektronik imza ile imzalanmış elektronik belge sanal ortamda notere ulaştırılır. Noter kişinin kimliğini elektronik sertifikası ile doğruladıktan sonra, tarih bilgisini elektronik belge üzerine ekleyerek kendi elektronik imzası ile kişiye sanal ortamda ulaştırır. Bu işlem kurulacak bir otomasyon ile sanal ortamda modellenebilir. Hatta pilot bir çalışmadan sonra, otomasyonun noter tarafı kişiye bağlı olmaktan çıkarılıp tam bir otomasyonda sağlanabilir.

Hali hazırda ülkemizde bu konuda hizmet veren bir kurum mevcuttur (Akçeşme ve Sönmez, 2008). Fakat önerilen çözümde noter kişinin göndermiş olduğu elektronik belgeyi kendi sisteminde muhafaza etmektedir. Bu kurum ise elektronik belgenin özet algoritması ile özetini çıkarıp sisteminde onu muhafaza etmektedir. Bu kurumun yaptığı tüm işlemler hukuki olarak noterde yapılan işlemlerle eştir. Kanuni ispat bakımından hiçbir farkı bulunmamaktadır.

Sanal ortamda modellenecek böyle bir sistemin topluma katabileceği birçok fayda vardır. En önemli fayda, işlem yapmak için zaman kavramını ortadan kaldıracaktır. Noterin çalışma saatleri ile işlem yapamayan ve çalışmasını, fikrini tehlikeye atan birçok kişi vardır. Günümüz şartları ile değerlendirildiğinde noterdeki işlem süreci ihtiyaç sahiplerini zaman damgası almak için caydırmaktadır. Sanal ortamda böyle bir model ile bu sorunlarda aşılmış olacaktır. Genel bir değerlendirme yapılır ise, ne kadar çok zaman damgası hizmeti alınır ise gelecekte toplumda oluşabilecek ihtilaflar bir o kadar azalacaktır.

6.2 Elektronik Belgenin Elektronik İmzasını ve Üzerindeki Tarihi Onaylamak

Günlük hayatta yapılan işlemlerde, taraflardan birinin ıslak imzasını inkâr etmesi durumunda mahkeme Hukuk Usulü Muhakemeleri Kanununa 308–313 maddesine göre işlem yapar [6]. HUMK'a göre mahkeme tarafları isticvap (sorguya çekmek) eder. Bu şekilde hâkim inkâr edilen imzanın inkâr eden kişiye ait olup olmadığı konusunda kanaat sahibi olamazsa belgeyi imza ettiği iddia edilen kişiyi istiktab (imza attırmak) eder. Bu şekilde kanaat edemezse, bilirkişi tarafından incelenmesi kararını verir. Bilirkişi tarafından verilen karar doğrultusunda hâkim tarafından karar verilir.

Yukarıda bahsedilen anlaşmazlıklarla karşılaşmak istemeyen işlem tarafları kişinin imzasının noterden bir şerh ile belgelendirmesini talep ederler.

Bu işlem Noterlik Kanunu'nun 90. Maddesi "Hukuki işlemlerin altındaki imzanın

onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır" ve 91. Maddesi "Onaylama, imzanın noter huzurunda atılması veya kendisine ait olduğunun ilgili tarafından kabulü ile kabildir" düzenlenmiştir (TNB, 2007). Bu maddelere göre noter bir belgedeki imza ve tarihi kendi huzurunda veya kendisine ait olduğunu kabul etmesi durumunda bir şerhle belgelendirmektedir.

Noterin yapmış olduğu bu işlemde zaman damgası hizmetinde olduğu gibi noterin bilgisini ya da muhakemesini gerektiren bir durum yoktur. Bu sebeple bu işlemde sanal ortamda zaman damgası hizmetinde olduğu gibi gerçeklenebilir. Kişi aynı şekilde elektronik imzasını içeren belgeyi sanal ortamda notere ulaştırır. Noter gerekli doğrulama ile kişinin kimlik bilgisini tespit eder. Aynı şekilde noter hazırlayacağı bir şerh belgesini kendi elektronik imzası ile imzalayarak ilgili kişiye gönderir.

Noterlik kanunu temel alınarak, böyle bir işlemin sanal ortamda gerçeklenmesinin hiçbir sakıncası yoktur. Fakat bölümün en başında belirtilen ihtilafın oluşması durumunda, yani kişinin elektronik imzasını inkâr etmesi durumunda mahkemenin yaklaşımı farklı olacaktır. Çünkü işlem elektronik imza ile yapılmış olduğu için hâkimin HUMK'un 308. maddesinde öngörülen isticvap ve istiktab yollarını izlemesi mümkün değildir. Burada ESHS teknik altyapısı kullanarak kişinin kimliği her zaman doğru bir şekilde tespit edilebilir. Bu sebeple hâkim ya da bilirkişi kişinin kimliğini ve elektronik imzasının geçerli olup olmadığını çok kolay bir şekilde tespit edebilir.

Görülüyor ki Noterlik Kanunu temel alınarak böyle bir işlemin sanal ortama taşınması tezin amacı ile örtüşmektedir. Diğer yandan işlemin elektronik imza ile yapılması durumunda noterde bu işlemi yapmak gereksiz olmaktadır. Noterin bu işlemini hukuki geçerliliği olan ESHS üstlenmektedir.

Elektronik İmza Kanunu ile ıslak imza ve elektronik imza ile eş kılınmıştır. Fakat elektronik imzanın kurumların kanunlarında nasıl kullanılacağına yönelik düzenlemeler yapılmamıştır. Bu sebeple yukarıda değinilen kanunlara göre her ikisi de doğru olan yaklaşımlar ortaya çıkmaktadır.

6.3 Elektronik Belgenin Saklanması ve İstendiğinde Belgelenmesi

Noterler yapmış oldukları noter işlem kayıtlarının bir kopyasını kâğıt üzerinde kendi arşivlerinde saklamaktadırlar. Bunun yanında 2000'li yıllardan itibaren noterler yapmış oldukları işlem kayıtlarını elektronik olarak da tutmaktadırlar. Tutulan bu kayıtlar elektronik olarak noterin insiyatifinde arşivlenmektedir. Noterin insiyatifinde olmasının sebebi esas

olanın kâğıt ortamında tutulan kayıtlar olmasıdır.

Kişi ya da kurumlar geçmiş yıllarda yapmış oldukları noter işlemlerine ait kayıtlara ihtiyaç duyabilirler. Kendilerine verilen noter işlem kayıtlarını kaybetmiş olmaları durumunda noterlerden işlem kayıt örneklerini temin edebilirler. Bu durum Noterlik Kanunu'nun 94. maddesinde "Noterler tarafından yapılan işlemlerin örnekleri, ancak ilgililerine, kanuni mümessil veya vekillerine yahut da mirasçılarına verilir." şeklinde düzenlenmiştir (TNB, 2007).

Kanuna göre, kişi ya da kurum ilgili noter işlem örneklerini, noterden almak için noter işleminin taraflarından biri olması gereklidir. Bunun dışında noter işlem örnekleri ancak mahkeme kararı ile verilebilir.

İlgili kişinin noter işlem kayıt örneklerini almak için bizzat notere gitmesi gereklidir. Çünkü kişinin noter işlem kayıtlarının ilgilisi olduğunu kimlik tespiti ile kanıtlaması gereklidir. Kişi noter işlemi yapılan noterden farklı bir şehirde ise, bu işlem için noter kayıtlarının ilgili noterden bulunduğu şehirdeki bir notere getirtmesi gereklidir. Bu işlem, zaman alan ve masrafı kişi tarafından karşılanacak bir işlemdir.

Yukarıda ki noter işleminde görüldüğü gibi, noterin kişisel bilgi ve muhakemesine ihtiyaç duymadan, yalnızca kişinin kimlik tespitinin yapıldığı bir noter işlemidir. Bu sebeple diğer işlemlerde olduğu gibi sanal ortamda da gerçeklenebilir. Kişi noterden talep ettiği noter işlem örneğini belirterek bir elektronik belge hazırlamalı ve bu elektronik belgeyi elektronik imzası ile imzalamalıdır. Bir sonraki aşamada bu elektronik belge sanal ortamda notere ulaştırılır. Elektronik ortamda talebi alan noter kişinin ilgili olup olmadığını kontrol ederek ilgili ise, elektronik imzası ile elektronik noter işlem örneğini imzalayarak kişiye gönderir.

Sanal ortamda gerçeklenecek böyle bir modelleme, önceki işlemlerde olduğu gibi zaman kavramını ortadan kaldıracak, kişi istediği zaman noter işlem örneğini talep edebilecektir. Bu sistem ülkemizdeki tüm noter kayıtlarının elektronik olarak bir noktada tutulmasını sağlayacaktır. Bu işlem doğal afetlerden (deprem, sel, su baskını) doğabilecek noter işlem kayıt örneklerinin kaybını da önleyecektir. Bu konuda yakın tarihte 17 Ağustos 1999 depreminde Sakarya, İzmit, Karamürsel, Gölcük Noterlikleri ile Sakarya Noter Odasının çöktüğü ve birçok belgenin yok olduğu bilinmektedir [7]. Bunun yanında, ülkemizdeki tüm noterlerden işlem kayıt örneklerini alınabilecek, süre ve maliyet azalacaktır.

6.4 Özel Kanunda Hükmü Bulunmayan Defterleri Onaylamak

Günümüzde ticari olsun olmasın hemen hemen tüm defterler elektronik ortamlarda tutulmaktadır. Fakat kanun gereği tutulan bu defterler kâğıda basılararak belirli aralıklarla (genelde yılsonları) noterlere onaylatılır. Bu işlemin amacı işletmelerin defterler üzerinde tahrifatını önlemek ve işlemleri kayıt altına almaktır. Ülkemizdeki işletmelerin büyüklüğü göz önüne alındığında, orta büyüklükteki bir işletmenin bile binlerce sayfa defter onayı noterler tarafından yapılmaktadır.

Defter onaylama işlemi Noterlik Kanunu'nun 107. Maddesinde "Özel kanununda hüküm bulunmayan hallerde defter onaylaması, defterin baş ve son sayfasına kaç sayfadan ibaret olduğu yazılmak ve her sayfası numaralanıp mühürlenmek suretiyle yapılır." şeklinde düzenlenmiştir (TNB, 2007).

Noterler burada diğer örneklerde olduğu gibi defterini içeriği ile ilgilenmeyip, hangi işletmeye ait olduğunu belirtip, sayfa sayısını vb. bilgileri belirleyerek işlemi yapar.

Yapılan bu işlemde noterin bilgisi ya da muhakemesine yönelik bir işlem yoktur. Bu sebeple bu noter işleminin sanal ortamda yapılması mümkündür. İşletme özel kanunda hükmü bulunmayan defter kayıtlarını zaten elektronik olarak tutmaktadır. İşletme yetkilisi bu defter kayıtlarını ve işletmeye yönelik bilgilerin olduğu bir elektronik belgeyi elektronik imzası ile imzalayarak sanal ortamda notere ulaştırabilir. Bu elektronik kayıtları alan noter kişinin kimlik doğrulamasını yaparak, kanunda öngörüldüğü üzere baş ve son sayfasını kaç sayfa olduğunu belirten bir noter kaydını ve işletmenin defter kayıtlarını elektronik imzası ile imzalayarak işletmeye gönderebilir.

Sanal ortamda gerçekleştirilecek böyle bir modelleme, mevcut uygulamadan çok daha efektif bir çözüm olacaktır. Defter onaylarında noterler defterin her sayfasını mühürlemektedir. Fakat o sayfanın bir kopyası alınmamaktadır. Bu sebeple sayfaların içeriği tahrifata açıktır. Fakat bu işlem sanal ortamda yukarıda bahsedilen modelde olduğu gibi yapılır ise veri bütünlüğü de sağlanacağı için hiçbir şekilde tahrif edilemez. Tereddüde düşüldüğünde noterde tutulan kopya ile karşılaştırılarak kolayca sonuca ulaşılabilir.

6.5 Tebligat İşleri

Noterlerin görevlerinden biri de kendisine getirilen her türlü yazılı belgeyi muhatabına göndermektir. Mahkemeler, kamu kurumları, barolar ve noterler tebligat işlemlerini yoğun olarak kullanan kurumlardır. Tebliğ etme işlemi Tebligat Kanununa göre yapılır.

Noterlerin tebligat işleri noterlik kanununun 70. Maddesinde "Tebliği istenen her nevi kâğıt, Tebligat Kanunu hükümlerine göre muhatabına tebliğ olunur. Tebliğ tutanağı dairedeki nüshaya bağlanır. Tebliğin yapıldığı veya yapılamadığı ilgilisine verilecek nüshasına yazılıp onaylanır" şeklinde düzenlenmiştir (TNB, 2007).

Noterler tebligat işlemlerinde de diğer örneklerde olduğu gibi kişisel bilgi ve muhakeme gerektiren bir işlem yapmamaktadır. Bu sebeple sanal ortamda diğer işlemler gibi modellenebilir. Burada kişinin notere gitmeden sanal ortamda ilgili elektronik belgeyi ve tebligatın yapılacağı kişiye ilişkin bilgileri girdikten sonra elektronik imzasıyla imzalayarak sanal ortamda notere ulaştırabilir. Noter ilgili elektronik belgeyi aldıktan sonra gönderen kişinin kimliğini doğrulayarak, tebliğ edilmek istenen elektronik belgeyi posta hizmetleri ile ilgilisine tebliğ edebilir. Posta işlemlerinden sonra, notere iletilen tebliğ sonucu elektronik belgeye eklenerek tebligatı yapan kişi ya da kuruma noterin elektronik imzasıyla iletilebilir.

Sanal ortamda tebligat işlemleri için uzun vadede hedeflenmesi gereken posta hizmetlerini tamamen ortadan kaldırarak, kişinin elektronik posta adresine tebligatı göndermektir. Fakat şu an için kişiyle bir elektronik postayı ilişkilendirmek mümkün değildir. Gelecekte BTK ya da bir kamu kurumunun yöneteceği bir ISP ile, kişinin kimlik bilgisine bağlı bir elektronik postanın ilişkilendirmesi durumunda tebligatın direkt kişinin elektronik postasına yapılması söz konusu olabilir.

6.6 İhtarname ve İhbarname İşleri

Yaşantımızda yapılan her ticari ilişkide taraflar edimlerini yerine getirmezler. Bu ve benzeri ihtilafları mahkemeye taşımadan önce taraflar aralarındaki söylemleri, talepleri hukuki geçerliliği olacak şekilde belgelemek isterler. Yapılan bu ihtarname ve ihbarname işlemleri noterler aracılığıyla yapılır. Yapılan bu ihtarname ve ihbarname işleminin bir kopyası da noterde saklanır. Noter ihtarname ve ihbarname işlemini iadeli taahhütlü posta ya da APS (Acele Posta Sistemi) ile ilgili kişiye gönderir. Notere posta kurumu tarafından tebliğ sonucu gönderildiğinde, tebliğin yapılıp yapılmadığı bilgisi kişiye verilir.

İhtarname ve ihbarname işleri Noterlik Kanunu'nun 106. Maddesinde "Her türlü hukuki işlemlere ait ihtarname ve ihbarname:

- İstemde bulunan ve diğer tarafın ad ve soyadları ile açık adreslerini,
- İhtar ve ihbar konusunu,

- İstemde bulunanın imzasını,
- Tebliğ şerhini, noterin imza ve mührünü ve tarihi (Yazı ve rakam ile),

kapsar (TNB, 2007).

İhtarname ve ihbarnameler ilgili tarafından yazılıp tebliğ için notere getirebileceği gibi, notere de yazdırılabilir." şeklinde düzenlenmiştir. Bu kanunda da görüleceği üzere tebligat işlerinde olduğu gibi noterin kişisel bilgi ve muhakemesini gerektirmemektedir. Bu sebeple bu işlem de sanal ortamda gerçeklenebilir. Kişi ihtar etmek istediği kişinin açık adres bilgisini, ihtar ve ihbar konusundan oluşan elektronik belgeyi elektronik imzası ile imzalayarak sanal ortamda notere ulaştırılabilir. Noter tarafından gerekli kimlik doğrulaması yapıldıktan sonra ihtarname ilgili kişiye klasik noter hizmetlerinde (iadeli taahhütlü posta, APS) olduğu gibi ulaştırılabilir.

Sanal ortamda, bu modelde olduğu gibi yapılacak ihtarname işleminde postayla kişiye gönderilecek ihtarname üzerinde ihtar eden kişinin ıslak imzası olmayacaktır. Bu durumda ihtarname hukuki olarak geçersiz gözükse de, diğer yandan ıslak imzayla eş olan elektronik imzanın noter tarafından doğrulanmış olması ihtarname işleminin hukuki geçerliliğini sağlar. Bu ve benzeri durumlarda oluşabilecek yorum farklılıklarından dolayı sanal noter hizmetleri için Noterlik Kanunu ve diğer ilişkili kanunlarda çeşitli düzenlemeler yapılmalıdır. Bu durum bir önceki madde de belirtilen tebligat işlemlerinde de geçerlidir.

Bu sebeple ihbarname işlemlerinde belirtildiği üzere uzun vadede hedeflenen kişinin elektronik posta adresine ihtarname göndermek olmalıdır.

7. HUKUKİ GEREKSİNİMLER

Teknolojik gelişmeler ile beraber günlük hayatta yapılan birçok işlem sanal ortamda modellenmiştir. Bankacılıktan alışverişe, eğitim hizmetlerinden iletişime, birçok işlem artık sanal ortamda yapılmaktadır. Fakat bu işlemlerin hukuki bağlayıcılığı mutlak değildir. Bunun nedeni, işlemlerin yasalarda tanımlanan yapılış şekli ile sanal ortamda yapılış şeklinin aynı olmamasıdır. Başka bir ifade ile işin sanal ortamda yapılması yasalar ile düzenlenmemiştir. Bir diğer neden de sanal ortamda yapılan işlemlerin manipule edilme riskidir.

Sanal ortamda yapılan işlemde, taraflar arasında ihtilaf oluşması durumunda, mahkemeler tarafların delil olarak gördüğü birçok materyali somut delil olarak kabul etmemektedir. Sanal ortamda yapılan işlemlerde mahkemeler bilirkişi raporları ve kendi takdirlerini kullanarak karar vermektedir. Aynı işlem yasalarda tanımlandığı şekilde yapılmış ise taraflar arasındaki her türlü ıslak imzalı, antetli evraklar somut delil olarak kabul edilmektedir. Söz gelimi bir ticari ilişkide eğer karşı tarafla sözleşme yapılmış ve ıslak imza ile imzalanmış ise, sözleşme hukuki olarak bağlayıcı olmakta, taraflar durumu inkâr edememektedir. Bu ticari ilişkinin sanal ortamda yapılması durumunda taraflar, elektronik posta, faks vb. elektronik donanımlar ile sözleşme yapmaktadır. Taraflar arasında bir ihtilaf oluşması durumunda faks örnekleri, elektronik posta kayıtları vb. kayıtlar mutlak delil sayılmamaktadır. Islak imza ile yapılmış bir sözleşme somut delil sayılır iken elektronik deliller takdiri delil sayılmaktadır.

Hukuki eksikliklere rağmen sanal ortamda yapılan işlem hacmi geçmişten günümüze kadar sürekli artmıştır, halen de bu artış devam etmektedir. Bu sebeple, kamu yararını gözeten birçok devlet, çözüm olarak elektronik imzayı benimsemiştir. Özellikle 2000'li yıllardan sonra birçok ülke tarafından elektronik imzaya ilişkin kanunlar çıkartılmıştır. Bu kanunların ana teması, belirli sınırlamalar dışında elektronik imzanın, ıslak imza ile aynı hukuki sonucu doğurduğunun kabul edilmesidir.

Diğer ülkelerde olduğu gibi ülkemizde de 15 Ocak 2004 tarihinde 5070 sayılı Elektronik İmza Kanunu kabul edilmiştir. 23 Ocak 2004 tarihinde 25355 sayılı Resmi Gazete'de yayımlanarak, 6 ay sonra 23 Temmuz 2004 tarihinde yürürlüğe girmiştir.

7.1 5070 Sayılı Elektronik İmza Kanununun Değerlendirilmesi

5070 sayılı Elektronik İmza Kanunu dört bölümden oluşmaktadır. İlk bölümde amaç, kapsam ve tanımlar verilmektedir. İkinci bölümde elektronik imzanın teknik altyapısına yönelik tanımlamalar yapılmıştır. Üçüncü bölümde denetim ceza hükümleri ele alınmıştır. Son bölümde çeşitli hükümler başlığı altında tanımlamalara yer verilmiştir. Ekler bölümünde 5070

sayılı elektronik imza kanun metnine ulaşabilir.

Elektronik imza kanununun kabulünden sonra ihtiyaç duyulan yönetmelik çıkarmaya, tebliğ ve kararlar almaya Bilgi Teknolojileri ve İletişim Kurumu yetkili kılınmıştır. Bu işlemlerin yanında ESHS'ların yönetimi ve denetim süreci de bu kurumun sorumluluğundadır. Bu kurum ihtiyaç duyulan yönetmelik, tebliğ ve kurul kararlarını Elektronik İmza Kanunu'nu temel alarak yayınlamıştır. Fakat tüm bu düzenlemeler elektronik imzanın teknik altyapısına yöneliktir. Oysaki elektronik imza kanununun çıkış noktası, günlük hayatta yapılan işlemlerin sanal ortamda hukuki bağlayıcılığı olacak şekilde yapılmasıdır.

5070 sayılı kanunun son bölümündeki 22. maddede ("22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14. maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir.

Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir.") elektronik imzanın borç ilişkilerinde ıslak imza ile aynı hukuki sonucu doğuracağı belirtilmiştir. Bu kanuna dayanarak, sanal ortamda elektronik imza kullanılarak yapılan sözleşmeler hukuki olarak geçerlidir. İhtilaf oluşması durumunda elektronik imzalı sözleşme somut delildir.

4982 sayılı Bilgi Edinme Hakkı Kanunu, demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir [8]. Bu kanunun 6. maddesine ("Bilgi edinme başvurusu, başvuru sahibinin adı ve soyadı, imzası, oturma yeri veya iş adresini, başvuru sahibi tüzel kişi ise tüzel kişinin unvanı ve adresi ile yetkili kişinin imzasını ve yetki belgesini içeren dilekçe ile istenen bilgi veya belgenin bulunduğu kurum veya kuruluşa yapılır. Bu başvuru, kişinin kimliğinin ve imzasının veya yazının kimden neşet ettiğinin tespitine yarayacak başka bilgilerin yasal olarak belirlenebilir olması kaydıyla elektronik ortamda veya diğer iletişim araçlarıyla da yapılabilir.") göre elektronik ortamdan başvuru yapılabileceği belirtilmesine rağmen ifade net değildir. Bu sebeple Milli Eğitim Bakanlığı kendi bünyesinde bilgi edinilmesi için yönetmelik ("Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik") çıkarmıştır. Bu yönetmelikte 4982 sayılı Bilgi Edinme Hakkı Kanunu 6. maddesine bağlı kalınarak aşağıdaki şekilde düzenlenmiştir.

"Gerçek kişiler tarafından elektronik posta yoluyla yapılacak başvurular, başvuru sahibinin adı ve soyadı, oturma yeri veya iş adresine ilave olarak kimlik doğrulama amacıyla kullanılacak T.C. kimlik numarası belirtilmek suretiyle, istenen bilgi veya belgenin bulunduğu kurum ve kuruluşun bilgi edinme biriminin elektronik posta adresine EK-1'de yer alan form doldurulmak suretiyle yapılır. Gerçek veya tüzel kişiler tarafından, 5070 sayılı

Elektronik İmza Kanunu gereğince elektronik imza kullanılarak gönderilen başvurularda, T.C. kimlik numarası aranmaz.” [9].

Yukarıda 4982 sayılı Bilgi Edinme Hakkı Kanunu bağlı kalınarak yayınlanan yönetmelikte büyük bir tezat vardır. Elektronik formlara kişi ilgili bilgileri girerek bilgi edinme başvurusu yapabilmektedir. Sanal ortamda bu şekil yapılan bilgi talebinde kişinin kimlik doğrulamasının yapılması mümkün değildir. Doğru olan ikinci maddede düzenlenen kişinin elektronik imza ile başvuru yapmasıdır. Burada yayınlanan yönetmeliğin ilk maddesinde kişinin kimlik tespiti manipüle edilebilir.

3071 sayılı Dilekçe Hakkının Kullanılması Kanunu, Türk vatandaşlarının ve Türkiye'de ikamet eden yabancıların kendileriyle veya kamu ile ilgili dilek ve şikâyetleri hakkında, Türkiye Büyük Millet Meclisi’ne ve yetkili makamlara yazı ile başvurma haklarının kullanılma biçimini düzenlemektir [10]. Bu kanunun 4. maddesine (“Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerde, dilekçe sahibinin adı-soyadı ve imzası ile iş veya ikametgâh adresinin bulunması gerekir.”) göre başvuru işleminin elektronik imza ile yapılması düzenlenmemiştir. 5070 sayılı kanun ile elektronik imzanın bazı sınırlamalar dışında tüm işlemlerde kullanılabileceği düşünülmektedir. Fakat 3071 sayılı kanuna göre başvuru işleminde elektronik imzanın kullanılması kanunda düzenlenmediği için kullanılması mümkün değildir.

Tezin konusu olan noter işlemlerinin de sanal ortamda mevcut noter kanunu ile yapılması mümkün değildir. Dilekçe kanunun da olduğu gibi noter kanununda da yapılacak işlemlerde elektronik imza kullanılabileceğine yönelik bir düzenleme yapılmamıştır. Ülkemizin birçok kanununda işlemlerin elektronik imza kullanılarak yapılmasına yönelik bir düzenleme yoktur. 5070 sayılı kanun ile elektronik imzanın hukuki bağlayıcılığı var olmasına rağmen, kanunlarda işlemin elektronik imza ile yapılabileceği düzenlenmediği için işlem yapılması mümkün değildir.

7.2 Elektronik İmzanın Hukuki İspat Gücü

Elektronik imza ile yapılan tüm işlemler hukuki olarak, adi senet statüsündedir. Adi senet, “resmi bir makam veya memurun katılımı olmaksızın, bizzat hukuki ilişkilerin taraflarınca düzenlenen senetlerdir”. Hukuk Usulü Muhakemeleri kanununda adi senetlerin ispat gücü; “Bir adi senet, senet altında imza tarafından ikrar edilirse kesin delil teşkil eder” şeklinde tanımlanmıştır [11].

Tezin içeriğinde, verilen modelde noter işlemlerinin elektronik imza kullanılarak yapılması

öngörülmektedir. Böyle bir modelde, elektronik imza ile işlem yapan taraflardan birinin noter olması, elektronik imzanın hukuki tanımıyla çelişmektedir. Çünkü artık taraflardan biri resmi bir makam olacaktır. Oysaki elektronik imza ile yapılan işlemler resmi bir makamın katılımı olmadığı için adi senet olarak tanımlanmıştır. Bu durumda yapılan işlem adi senet statüsünde mi değerlendirilecektir? Burada üzerinde durulması gereken konu, elektronik imza ile yapılan işlemlerin neden hukuki açıdan adi senet olarak tanımlandığıdır. Bunun sebebi, işlem taraflarından kaynaklanan güven zafiyeti mi, yoksa teknolojik altyapıya olan güven zafiyeti midir? İşlem taraflarına olan güven zafiyeti var ise bu işlemi bir noter elektronik imza ile yapması veya koordine edip işleme elektronik imzasını koyması durumunda bu işlem hukuki olarak hangi statüde değerlendirilecektir. Teknolojik altyapıya olan güven zafiyeti var ise elektronik imza ile yapılan işlemler, tarafların dışında üçüncü bir kurum olan ESHS tarafından teyit edilmektedir.

Islak imza ile imzalanmış adi senet statüsünde bir belgede, ihtilaf oluşur ise mahkemeler Hukuk Usulü Muhakemeleri Kanununa 308–313 maddesine göre işlem yapar. HUMK'a göre mahkeme tarafları isticvap eder sonuç elde edemezse taraflar istiktab edilir. Mahkemeler bu işlemleri yaparak sonuca ulaşmaya çalışır [11]. Sonuç elde edilememesi durumunda bilirkişi incelemesine başvurulur. Oysaki elektronik imza da ESHS kayıtlarından elektronik imzanın geçerliliği doğrulanır. Bu sebeple adi senet tanımlamasının elektronik imza işlemleri ile ne kadar örtüştüğü değerlendirilmelidir.

7.3 Sanal Noterin Hukuki Gereksinimleri

Noter işlemlerinde elektronik imza ve kriptolojik yöntemler kullanılarak, normal bir noterin sağlamış olduğu tüm güvenlik sağlanmış olsa da hukuki mevzuat daha önce de değinildiği üzere tam anlamıyla noterlik işlemleri yapmaya uygun değildir.

En temel hukuki gereksinim, noter kurumunun yapmış olduğu işlemlerde elektronik imza kullanılarak işlem yapılabileceğinin noter kanununda düzenlenmesidir. Eğer yapılacak noter işlemi noterin kişisel bilgi ve tecrübesini gerektiriyor ise bu konuda bir düzenlenmeye ihtiyaç yoktur. Daha genel bir ifade ile elektronik imza, kurumların iş yapısına uyarlanmalıdır.

Hukuki olarak noter kanununun etkileşimde olduğu kanunlar da sanal ortamda işlem yapmak için düzenlenmelidir. Bir önceki bölümde sanal ortamda yapılabilecek işlemler başlığı altında verilen tebligat işlemi bu konuya örnektir. Tebligat kanununun 8. maddesinde ("Tebliğ olunacak her nevi evrak, biri dosyasında konulmak ve diğeri tebliğ edilecek kimselere verilmek üzere lüzumu kadar nüshadan terekküp eder [12]. Bu nüshalarda iş sahibi veya

vekilinin imzası bulunur.") tebligat üzerinde iş sahibinin veya vekilinin ıslak imzasının bulunması gerektiği belirtilmiştir. Sanal ortamdaki modelde bu mümkün değildir. Burada amaçlanan iş sahibinin kimliğinin doğrulanması ve inkâr edilmemesinin sağlanmasıdır. Elektronik imza ile de bu amaç sağlanmaktadır. Bu nedenle tebligat kanununda da elektronik imza ile işlem yapılabilecek şekilde düzenlemeler yapılmalıdır.

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. Bu sigorta, sigortalıya karşı yapılan talepler sonucundaki yasal giderler için de teminat verir [13].

Sertifika Mali Sorumluluk Sigortası olay başına 10.000 (On bin YTL) ve Sözleşme süresince 1.000.000(Bir Milyon YTL) teminat tutarlarını vermektedir. Diğer sigorta teminatları ile mukayese edildiğinde teminat tutarları oldukça düşüktür, kişi ve kurumlara güven vermemektedir. Sadece noter işlemleri için değil tüm işlemlerde bu teminat tutarları daha yukarı çekilmeli, toplumun elektronik imzayı kullanması teşvik edilmelidir.

Elektronik imza uygulamalarında işlemi yapan elektronik sertifikaların geçerli olup olmadığının doğrulanma süreci çok önemlidir. Doğrulama sürecinde SIL listeleri veya ÇİSDUP sorgusu kullanılabilir. ÇİSDUP anlık olarak elektronik sertifikanın geçerliliğini bize verdiği için, noter uygulamalarında mutlaka her işlem için ÇİSDUP kullanılmalıdır. ÇİSDUP sorgusundan dönen ESHS'ın elektronik imzasını koyduğu sonuca göre işlem yapılmamalı, dönen sonuçtaki elektronik imza kök sertifikanın doğrulanmasına kadar devam edilmelidir.

Hukuki anlamda düzenleme gereken diğer bir konuda, sanal ortamda gerçeklenecek böyle bir modelde ne şekilde ücret tahsil edeceğidir. Noterlik Kanunu'na 115. maddesine ("Kesin giderin dökümü, işleme ait kâğıtların dairede kalan aslı ve örnekleri ile ilgilisine verilen asıl nüshasına, asıl nüsha dairede kalmışsa verilen örneklerden birine yazılır ve Maliye ve Gümrük Bakanlığınca bastırılacak seri numaralı özel makbuzdan iki nüsha düzenlenir. Gider dökümü asıl ve örnekler için ayrı ayrı gösterilir.") göre noterler Maliye ve Gümrük Bakanlığı'nca bastırılan makbuzları kullanarak ücreti peşin olarak noterde tahsil eder (TNB, 2007). Noterlerin ücret tahsil şekli de önerilen modele göre kanun ve yönetmeliklerde hukuki olarak düzenlenmelidir. Ücretlendirme için kontör sistemi ya da sanal poslar kullanılabilir.

8. PROTOTİP BİR SANAL NOTER UYGULAMASI

Bu bölümde, verilen modele göre prototip bir sanal noter uygulaması gerçeklenmiştir. Hazırlanan noter uygulaması sanal ortamda ihtarname işlemlerini yapmaya yöneliktir. Uygulama içerisinde modelin her aşaması görselleştirilerek okuyucuya verilmesi amaçlanmıştır.

Sanal ortamda noter işlemi yapmak için, işlem tarafları olan noter ve işlemi yapacak kişi için prototip uygulamada dört temel koşul yerine getirilmektedir. Bu koşullar;

- Noter ve noter işlemi yapmak isteyen kişi, sanal ortamdan kendisine ulaşan elektronik verileri kullanarak, birbirlerinin kimliğini doğrulayabilmektedir.
- Noter ve noter işlemi yapmak isteyen kişi birbirlerinin kimlik doğrulamasını yaptıktan sonra, işlemi inkâr edemez.
- Taraflar sanal ortamdan kendisine ulaşan elektronik verinin bütünlüğünü doğrulayabilir.
- Sanal ortamda noter işlemine konu olan elektronik verinin gizliliği sağlanır.

Yukarıdaki koşulları sanal ortamda modellemek için, teknolojik altyapının ne şekilde olması gerektiği önceki bölümlerde tanımlanmıştır. Hatırlanacağı üzere hukuki geçerliliği olan elektronik imza sanal ortamda noter işleminin temeli olmaktadır.

8.1 Uygulamanın Hazırlanmasında Kullanılan Teknolojiler ve İhtiyaçlar

Hazırlanan prototip uygulamada Microsoft ürünleri kullanılmıştır. Uygulamayı geliştirmek için Microsoft Visual Studio 2005 programı kullanılmıştır. Kodlama dili olarak C# kullanılmıştır. Veritabanı olarak SQL Server 2005 kullanılmıştır.

Farklı bilgisayarlarda uygulama test edilmiş olup sorunsuz çalıştığı gözlemlenmiştir. Uygulama Windows XP Professional ve Windows Vista Home Premium işletim sistemlerinde test edilmiştir. Prototip uygulamanın çalıştırılabilmesi için donanım konfigürasyonunun en az 1.60 GHZ işlemci ve 1024 MB bellek olmalıdır. Ayrıca kurulum için sabit diskte 15 MB boş alan olmalıdır. Program isteri olarak bilgisayarda SQL Server 2005 programı ve .NET Framework 2.0 yüklü olmalıdır.

8.2 Prototip Uygulamanın Yapısı

Uygulama bir masaüstü programı olarak geliştirilmiştir. Uygulama temel olarak iki bölümden oluşmaktadır. Birinci bölümde kişi elektronik olarak ihtarnameyi oluşturmakta ve elektronik imza donanımı ile elektronik belgeyi imzalamaktadır. İhtarname belgesinin oluşturulması için uygulama içerisinde taslak ihtarnameler vardır. Kişi burada ihtarnameye ilişkin temel bilgileri girdikten sonra otomatik olarak ihtarname oluşturulmaktadır.

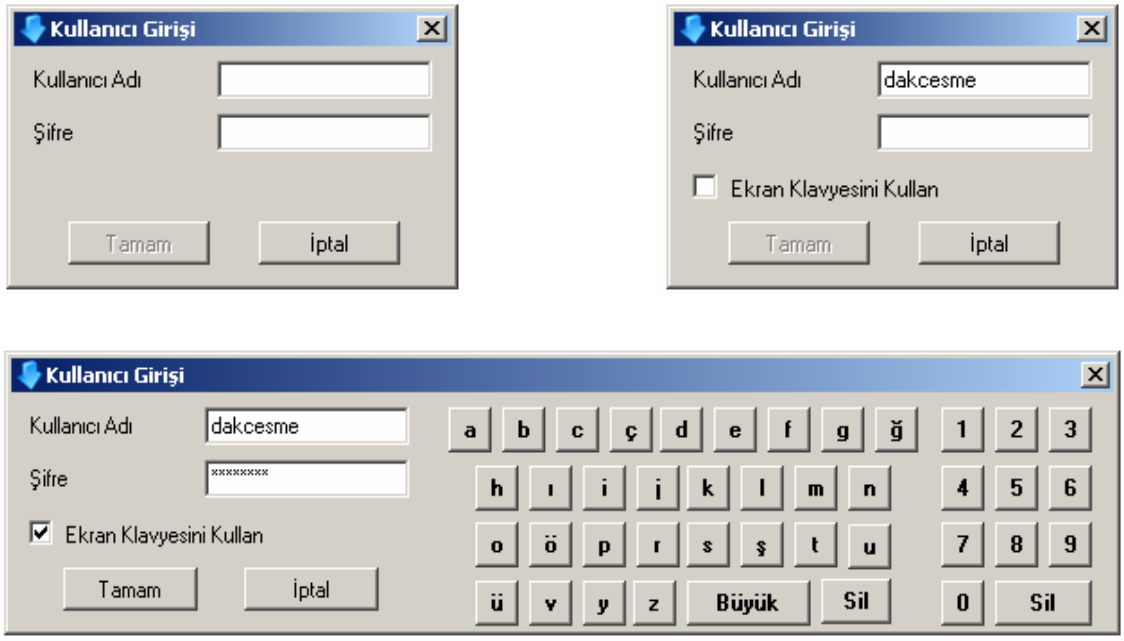
İkinci bölümde ise oluşturulan elektronik imzanın doğrulanma bölümüdür. Burada ESHS görevlerini üstlenen bir yapı modellenmiştir. Burada elektronik imza sahibinin oluşturulan yapıdan elektronik sertifikası alınmaktadır. Alınan sertifika kullanılarak elektronik imzanın doğrulanma işlemi yapılmaktadır. Bu süreç ayrıntılı olarak uygulama örneğinde görülecektir.

Uygulama basit anlamda, bir kişinin notere giderek ihtarname göndermek için yaptığı tüm işlemleri yerine getirmektedir. Farklı olarak noterin kişiye göndermiş olduğu ihtarname belgesi üzerinde ihtar eden kişinin ıslak imzasının olmasıdır. İhtarname işlemi, elektronik olarak yapıldığı için kişinin ıslak imzasının ihtar edilecek kişiye gönderilecek ihtarnamede olması mümkün değildir. Bu durum hukuki gereksinimler başlığı altında işlenmiş ve hukuki geçerliliğini engelleyecek bir durum olmadığı belirtilmiştir.

8.3 Prototip Uygulama ile Bir İhtarname İşleminin Yapılması

Hazırlanan prototip uygulama kullanılarak bir ihtarname işlemi aşağıdaki adımlar ile aşama aşama gerçeklenecektir.

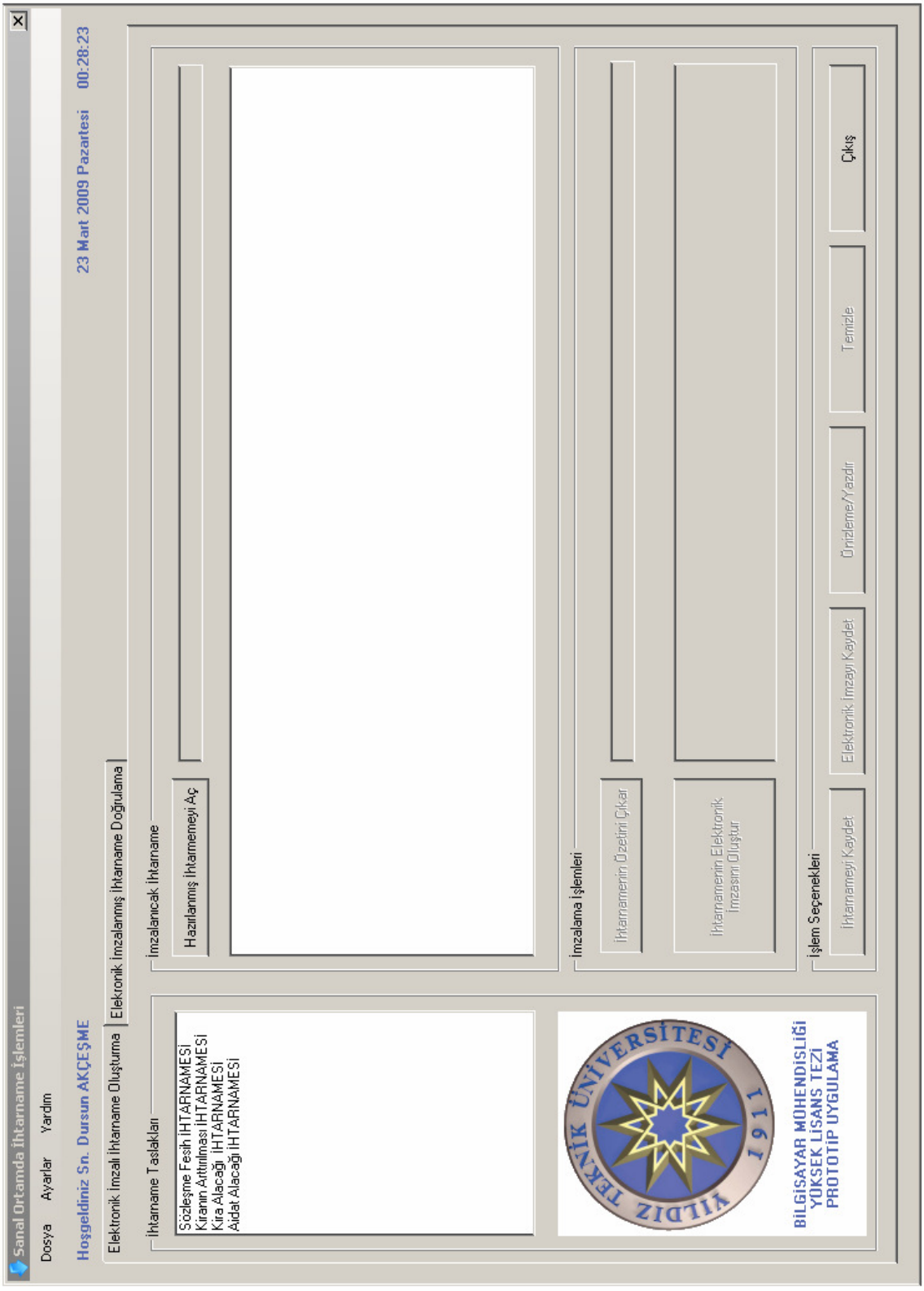
Uygulamayı çalıştırdığınızda kullanıcı adı ve şifre girmenizi isteyen bir ekranla karşılaşılır (Şekil 8.1). Sistemin veritabanında tutulan kullanıcı adı girilir. Şifre istenirse güvenlik amacı ile tasarlanmış ekran klavyesi kullanılarak girilebilir. Şifre girişi yapıldıktan sonra şifrenin özeti çıkartılır. Güvenlik amacı ile veritabanında şifrenin kendisi tutulmamaktadır. Kullanıcı tanımlamaları yapılır iken veritabanında şifrenin özeti tutulmaktadır. Bu sebeple kullanıcı şifre girişi yaptıktan sonra şifrenin özeti çıkartılarak veritabanında tutulan şifrenin özeti ile karşılaştırılır. Aynı ise kullanıcının sisteme girişine izin verilir.



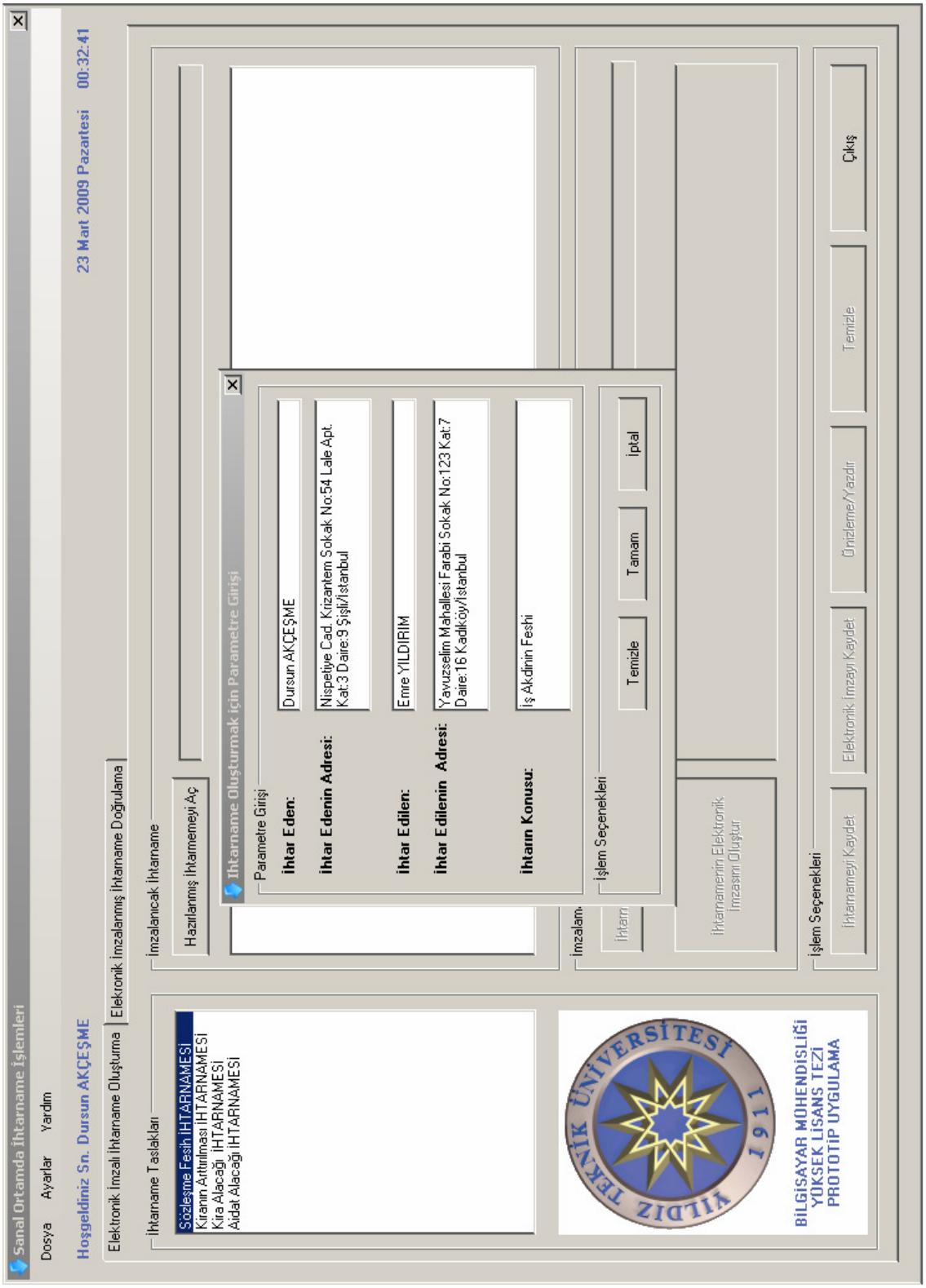
Şekil 8.1 Uygulama girişi

Giriş yapan kullanıcı sistemde tanımlı ise elektronik olarak ihtarname işlemlerinin yapıldığı ekrana ulaşılır. Uygulamanın ana ekranı iki bölümden oluşmaktadır (Şekil 8.2). Şekilde görüldüğü ilk bölüm "Elektronik İmzalı İhtarname Oluşturma" ikinci bölüm "Elektronik İmzalanmış İhtarname Doğrulama" olarak adlandırılmıştır. İlk bölüm ihtarnamenin oluşturulduğu ve kişinin elektronik imza donanımı ile oluşturulan ihtarnamenin imzaladığı bölümdür. İhtarnameyi oluşturmak için programın sol üst köşesinde ihtarname taslakları bulunmaktadır. Herhangi bir ihtarname taslağının üzerine tıklandığında, ihtarnamenin temel bilgilerini gireceği bir ekran açılmaktadır (Şekil 8.3). Bu ekrana ihtarnamenin temel bilgileri girildikten sonra tamam tuşuna basılarak, ihtarname otomatik olarak ekranda oluşur (Şekil 8.4).

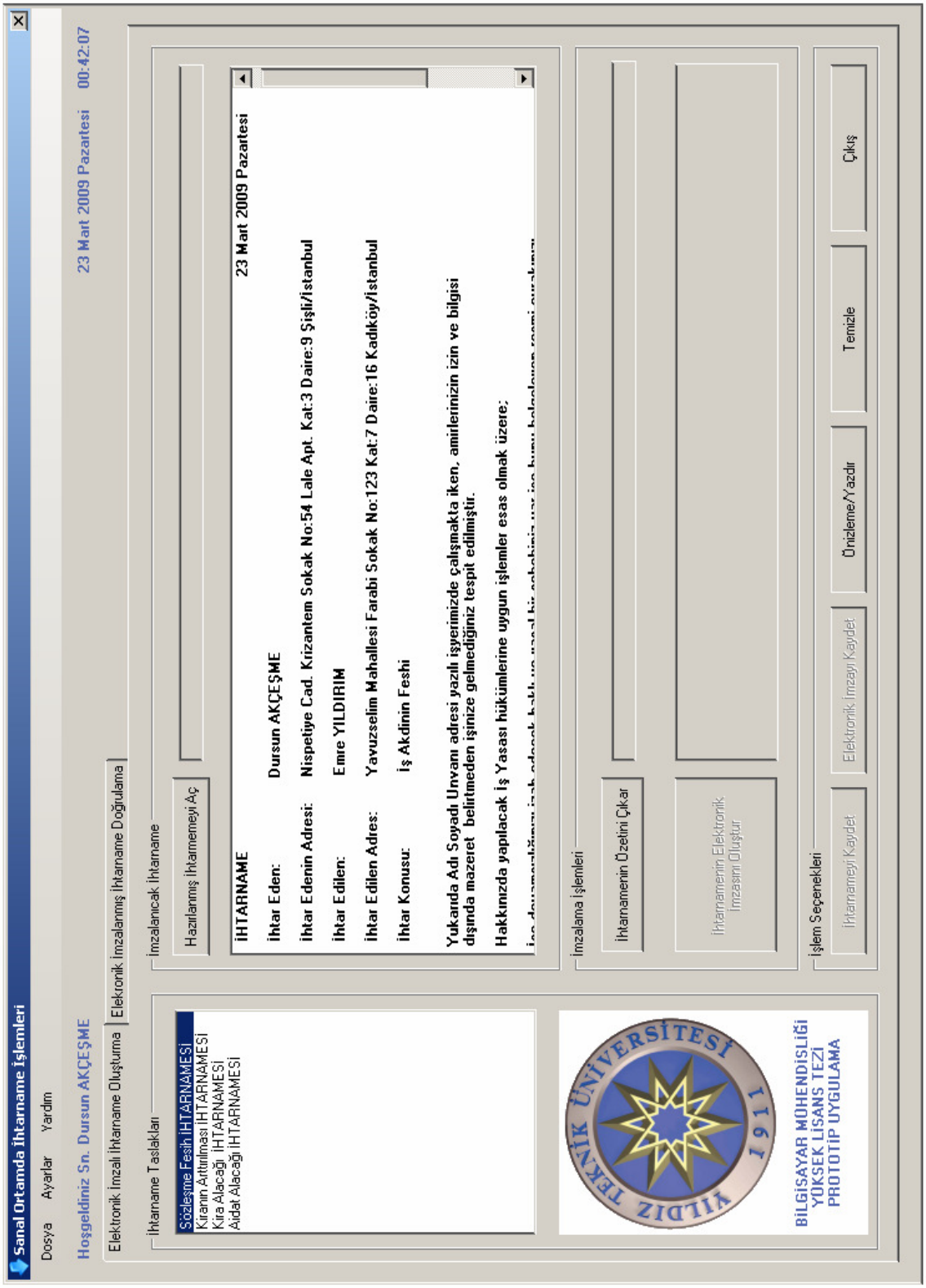
İhtarname oluşturulduktan sonra kişinin elektronik imza donanımı ile oluşturulan ihtarnamenin imzalanma süreci başlar. Önceki bölümlerde açıklandığı üzere ilk olarak elektronik ihtarnamenin özetleme algoritması ile özetini çıkartmak gereklidir. Bu işlem için ana ekranda görülen "İhtarnamenin Özetini Çıkar" butonuna basılarak ihtarnamenin özeti çıkartılır (Şekil 8.5).



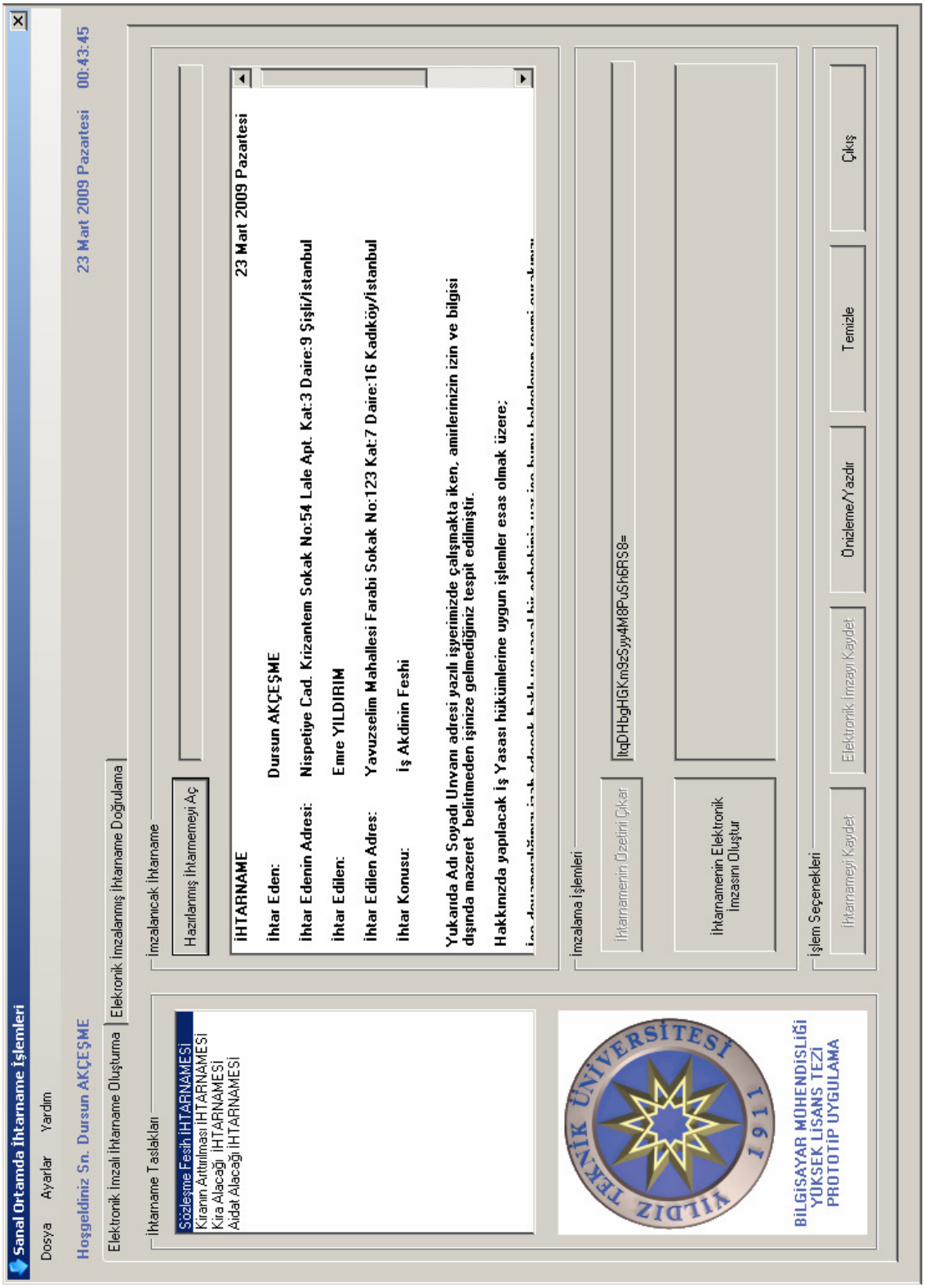
Şekil 8.2 Uygulama ana ekranı



Şekil 8.3 İhtarname parametre giriş ekranı



Şekil 8.4 İhtarname ekranı



Şekil 8.5 İhtarname özetinin çıkartılması

İhtarnamenin özeti oluşturulduktan sonra kişinin elektronik imza donanımı ile çıkartılan özet imzalanarak, elektronik ihtarnamenin elektronik imzası elde edilir (Şekil 8.7). Elektronik imza donanımı olmadan ihtarname imzalanamaz.

Prototip uygulamamızda elektronik imza donanımı usb flash bellekler kullanılarak modellenmiştir (Şekil 8.6). Flash belleklerin eşsiz olan id değeri, kişinin kimliğine bağlanmıştır.

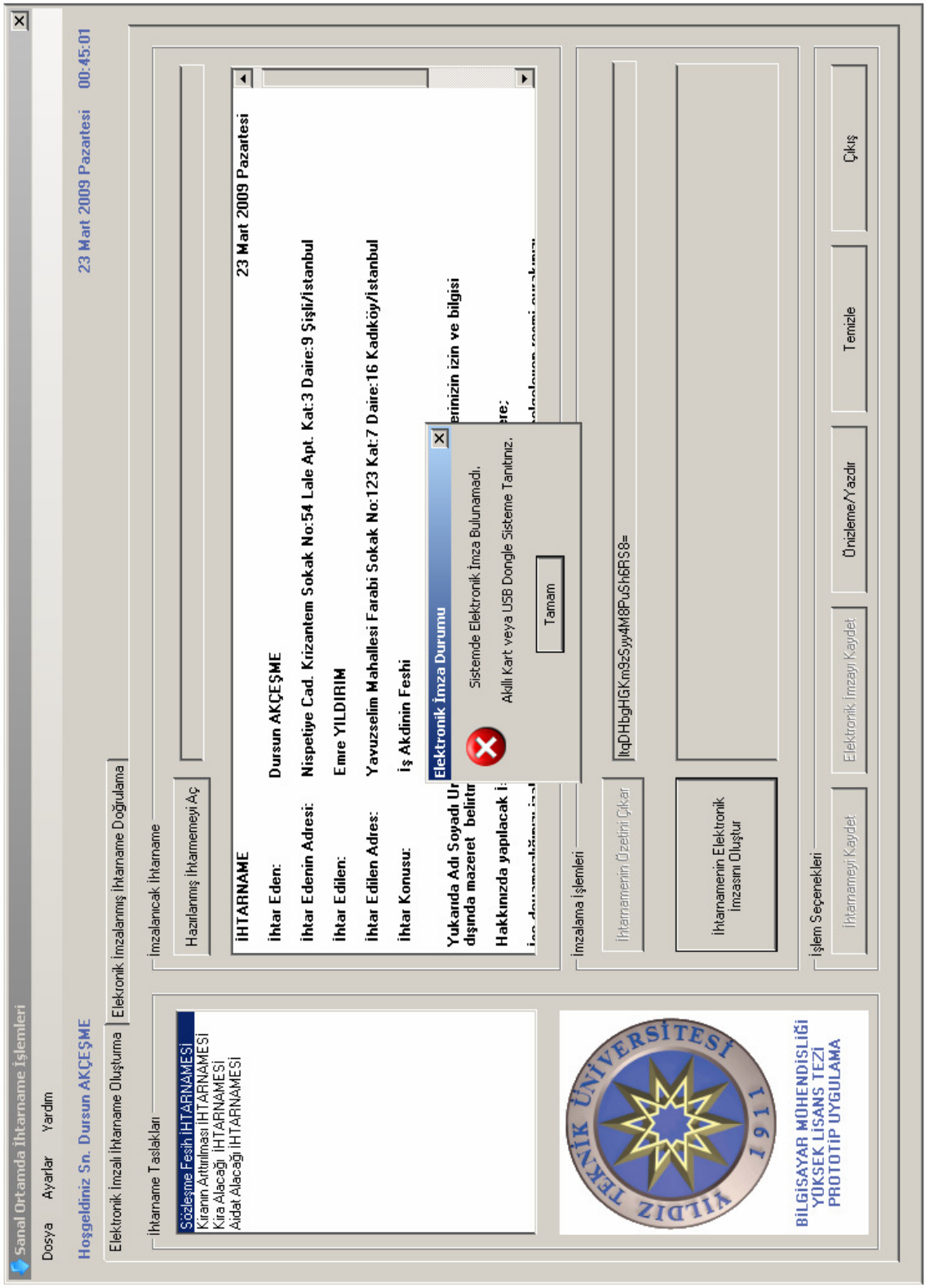
Şekil 8.6 Prototip uygulamada kullanılan elektronik imza donanımları

Elektronik imza donanımı bilgisayarın USB portuna takıldıktan sonra giriş yapan kullanıcı ile sisteme takılı olan elektronik imza donanımı karşılaştırılır. Eğer sistemde takılı olan donanım kişinin elektronik imza donanımı ise işleme devam edilir.

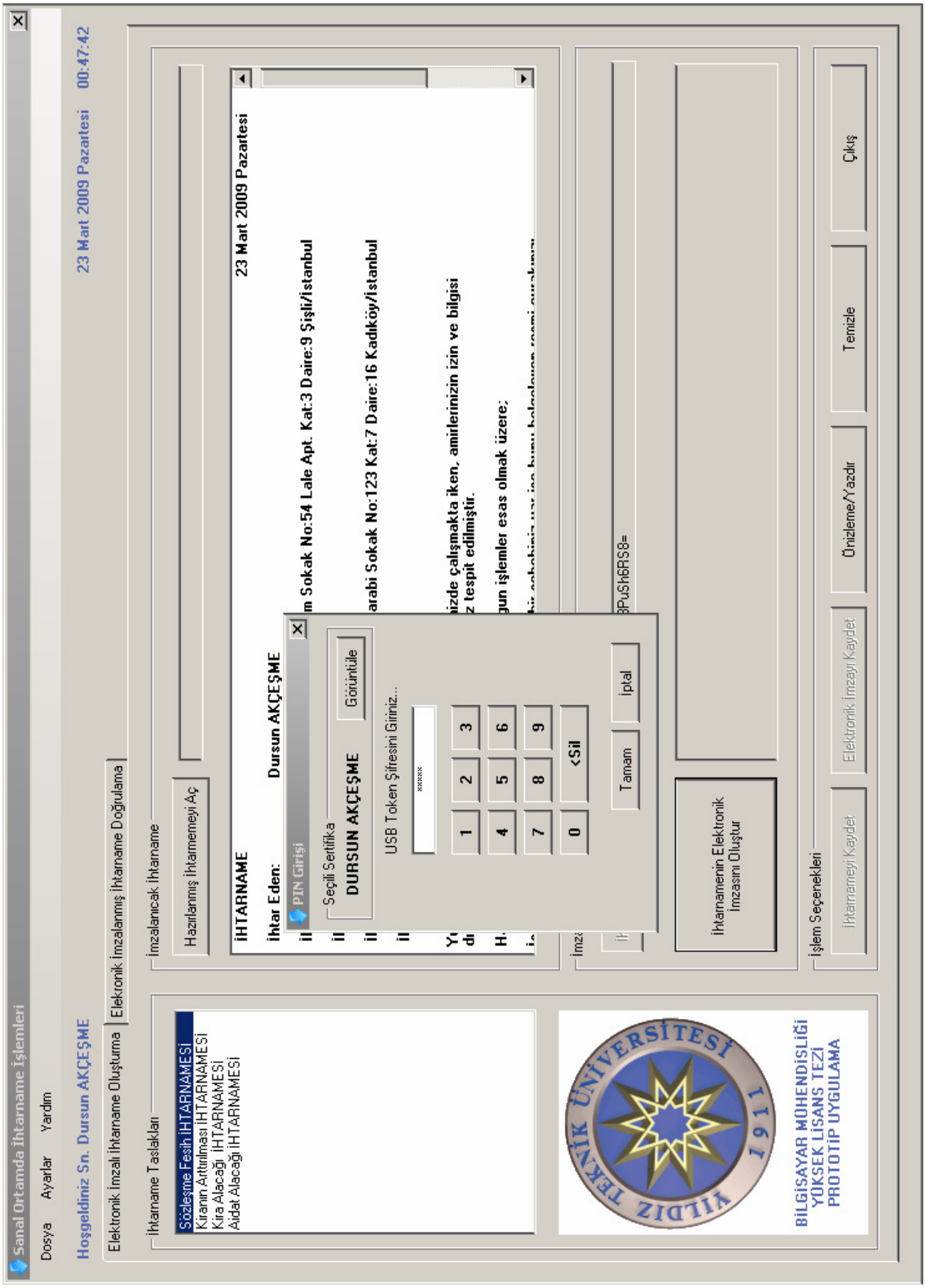
Elektronik imza donanımı kişinin ise donanımının şifresini gireceğimiz ekran açılır (Şekil 8.8). Yalnızca elektronik imza donanımının sahibinin bildiği şifre girilerek ihtarnamenin elektronik imzası oluşturulur (Şekil 8.9). Şifreyi doğru girmeden ihtarnamenin elektronik imzasını oluşturmak mümkün değildir.

İhtarnamenin elektronik imzası oluşturulduktan sonra istenirse, elektronik ihtarname uygulamadaki önizleme butonuna basılarak tekrar gözden geçirilir. Herhangi bir hata yok ise ihtarnameyi kaydet butonu ile ihtarname kaydedilir. Daha sonra aynı şekilde elektronik imza kaydet butonu ile elektronik imza kaydedilir.

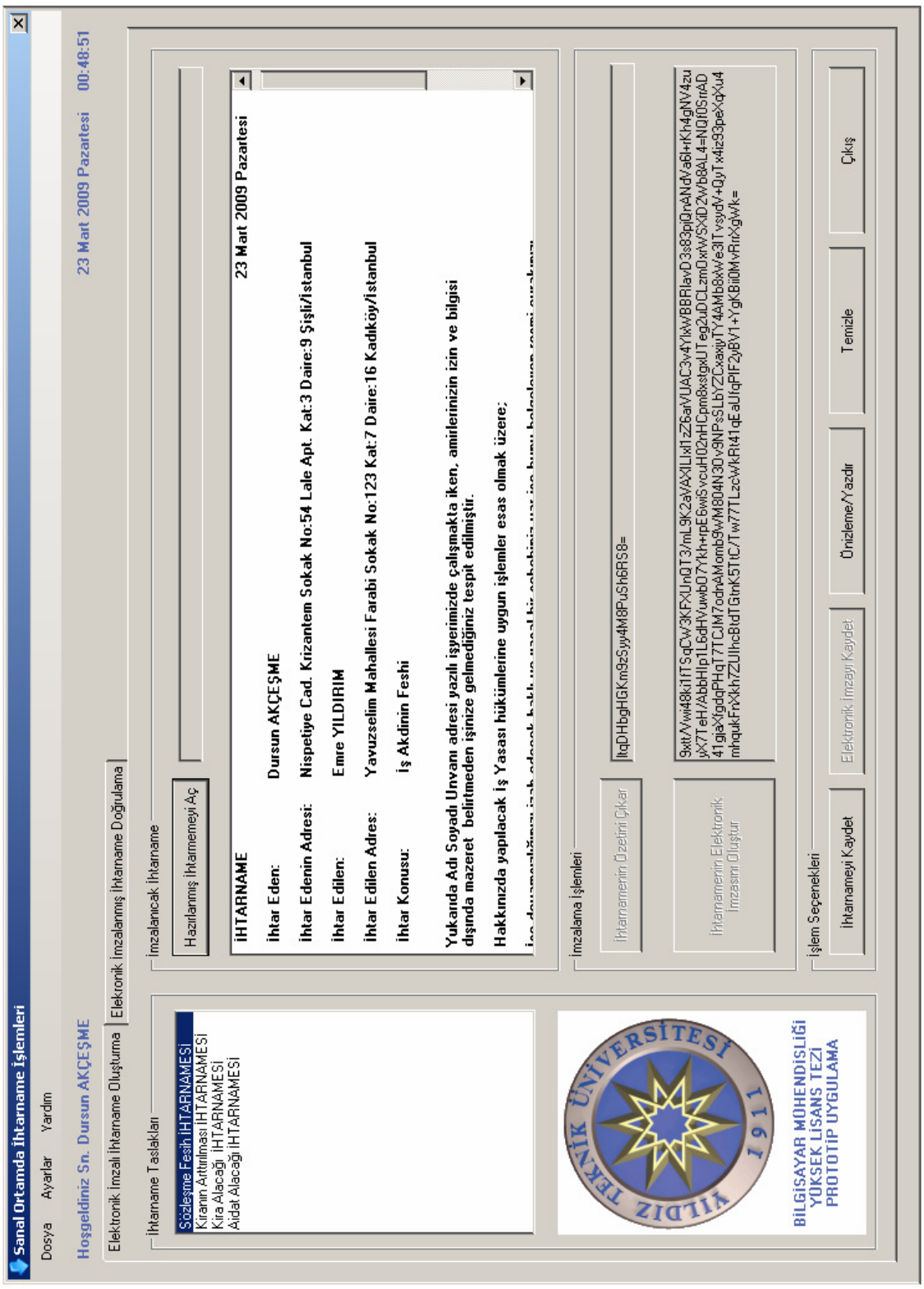
İhtarnamenin elektronik imzası oluşturulduktan sonra sanal ortamda SSL ile notere gönderilir. Noter tarafında ihtarnamenin doğrulama işlemleri yapılır.



Şekil 8.7 Sistemde elektronik imza donanımının bulunamama durumu



Şekil 8.8 Sistemde elektronik imza donanımının şifresinin girilmesi



Şekil 8.9 İhtarnamenin elektronik imzasının oluşturulması

8.4 Prototip Uygulama ile Bir İhtarname İşleminin Doğrulanması

Notere sanal ortamdan SSL kullanılarak ihtarname ve elektronik imzası ulaşır. Noter gerekli doğrulama işlemi için hazırlanan prototip uygulamanın "Elektronik İmzalanmış İhtarname Doğrulama" tabı kullanılır.

Noter prototip uygulamaya kullanıcı adı ve şifresiyle giriş yapar. Kullanıcı tarafından ihtarnameyi doğrulama ekranı seçilir (Şekil 8.10). Ekranın sol tarafında uygulamada kayıtlı olan elektronik sertifikalar görülmektedir. Ekranın sol alt tarafında iptal edilen sertifikalar görülmektedir.

Doğrulama işlemleri için ilk olarak sanal ortamdan notere ulaştırılan ihtarname "İhtarnameyi Seç" butonu tıklanarak ihtarname seçilir (Şekil 8.11). İhtarname seçildikten sonra, ihtarnamenin özet algoritması ile özeti çıkartılır. İhtarname ile birlikte gelen ihtarnamenin elektronik imzası "Doğrulanacak Elektronik İmzayı Seç" butonu tıklanarak seçilir (Şekil 8.12).

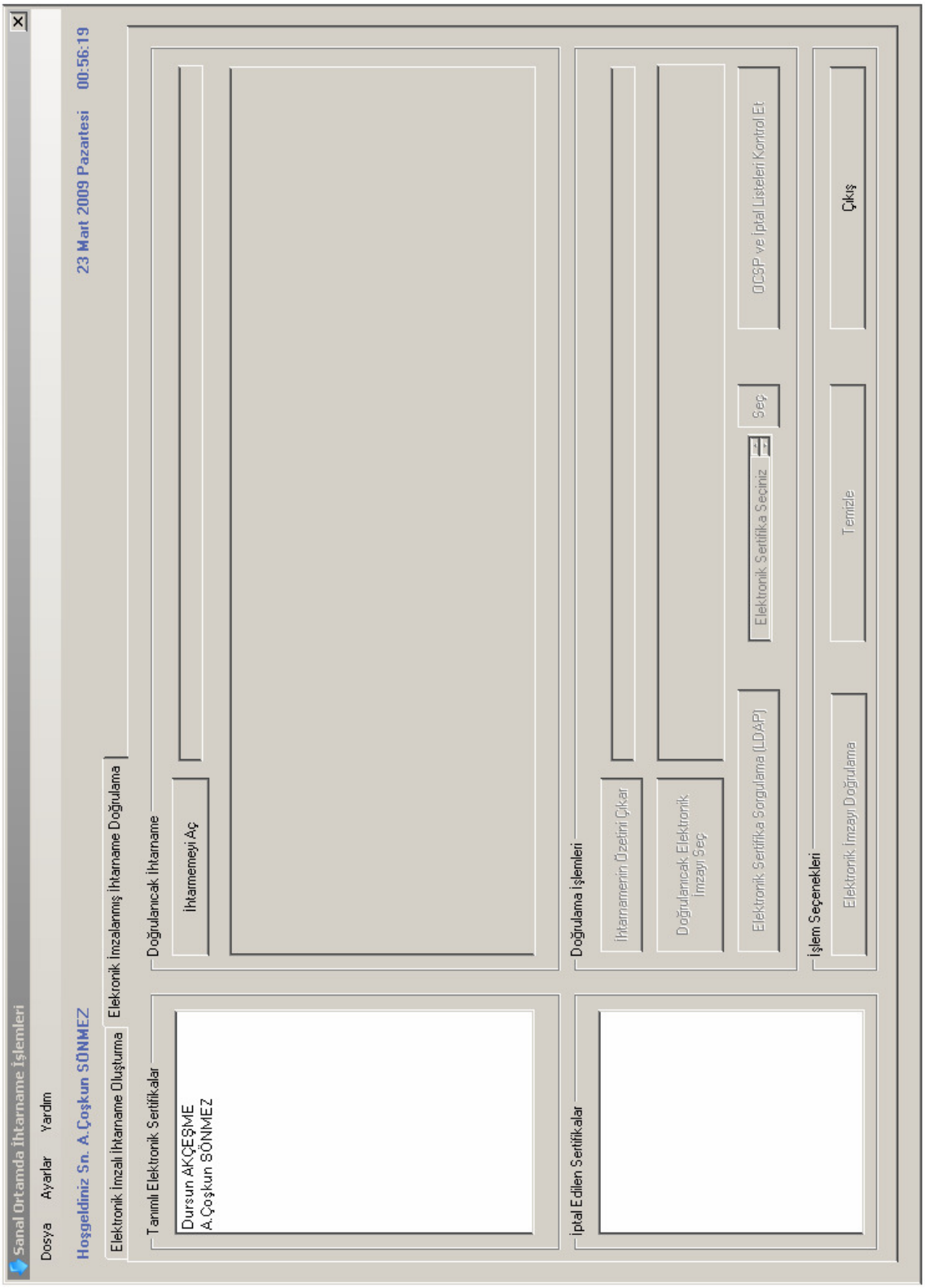
Doğrulama işlemi için, elektronik ihtarname sahibinin elektronik sertifikasına ihtiyaç duyulmaktadır. Bu işlem için uygulamada "Elektronik Sertifika Sorgulama (LDAP)" butonu tıklanarak kişinin elektronik sertifikası elde edilir (Şekil 8.13). Elde edilen elektronik sertifika ESHS'ın elektronik imzası ile ESHS'dan alınır. Sertifika geçerli ise uygulamada kullanılmak üzere eklenir. Uygulamanın bu modülü ESHS hizmetlerini temsil etmektedir.

Elektronik Sertifika alındıktan sonra imzayı doğrulamak için sertifika "Seç" butonu tıklanarak sertifika seçilir (Şekil 8.14).

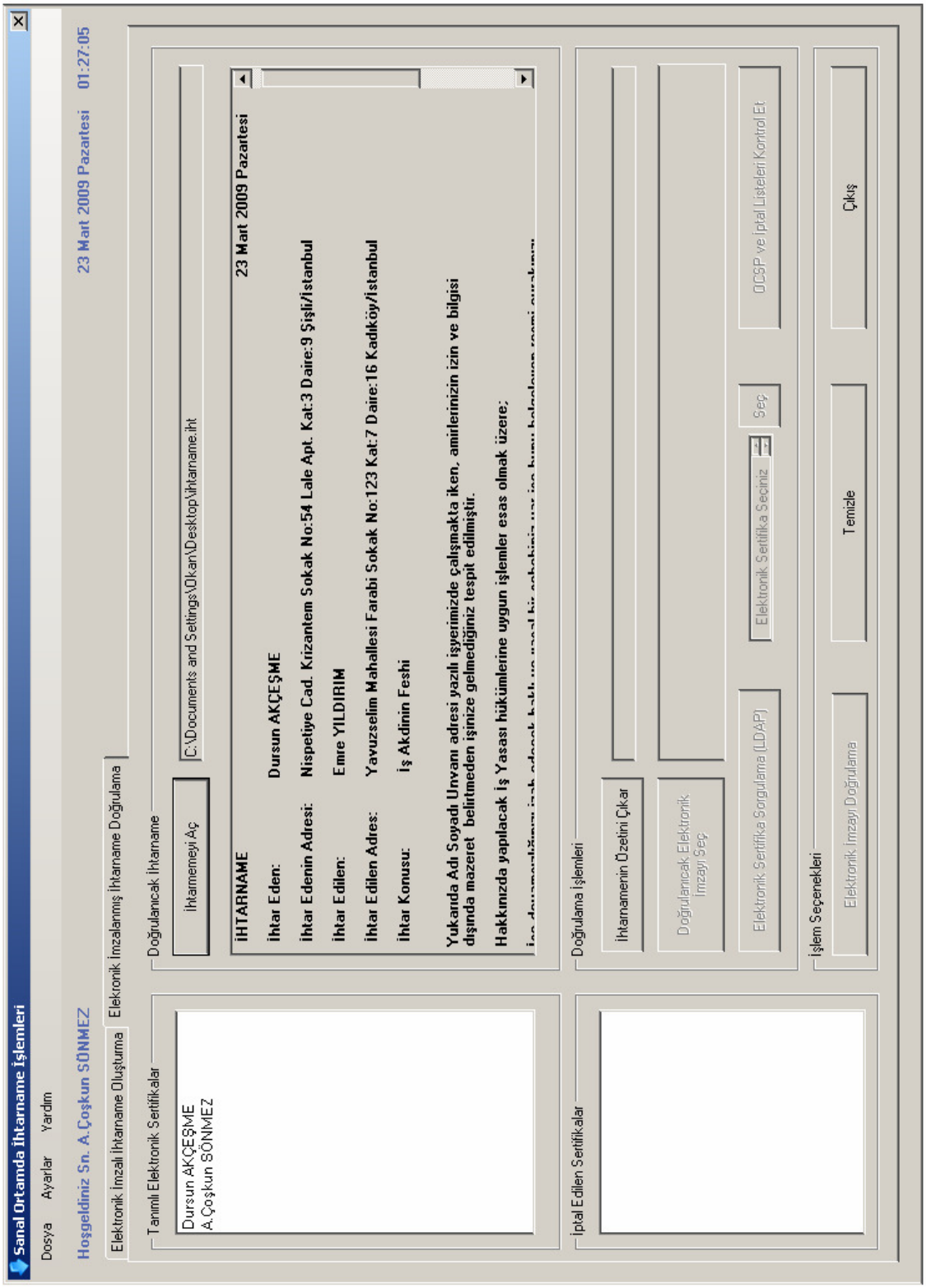
Elektronik imzayı doğrulamak için tüm gereksinimler karşılanmıştır. Bu aşamadan sonra "Elektronik İmzayı Doğrula" butonu tıklanarak doğrulama işlemi yapılır (Şekil 8.15). Eğer ihtarname sanal ortamdan notere ulaşırken veri bütünlüğü bozulmuş ise geçersiz olur (Şekil 8.16). Şekilde görüldüğü gibi kırmızı çerçeveye alınmış bölümde sadece bir nokta eklenerek veri bütünlüğü bozulmuştur. Bu ve benzeri bir durumda imza doğrulanamaz ve geçersiz olur.

Prototip uygulamada, ihtarname işleminin sanal ortamda ne şekilde yapılacağı aşama aşama verilmiştir. Uygulamada noter işleminin mutlak gerekliliği olan bütünlük, gizlilik, kimlik doğrulama ve inkâr edememe fonksiyonları sağlanmıştır.

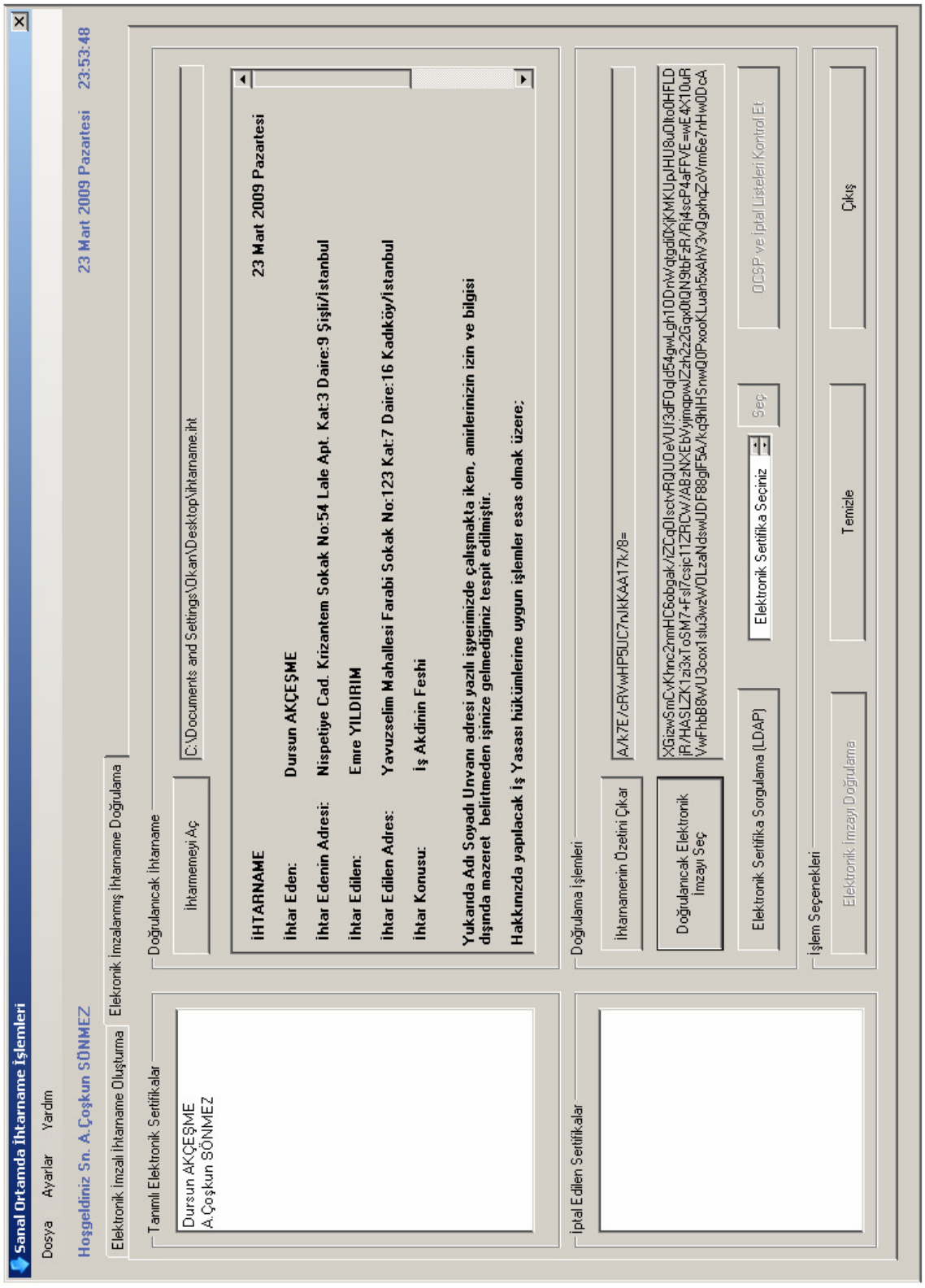
Tez boyunca üzerinde durulan model, basit olarak prototip uygulamada ortaya konulmuştur. Noterin modellenebilecek diğer hizmetleri de benzer şekilde sanal ortam için modellenebilir.



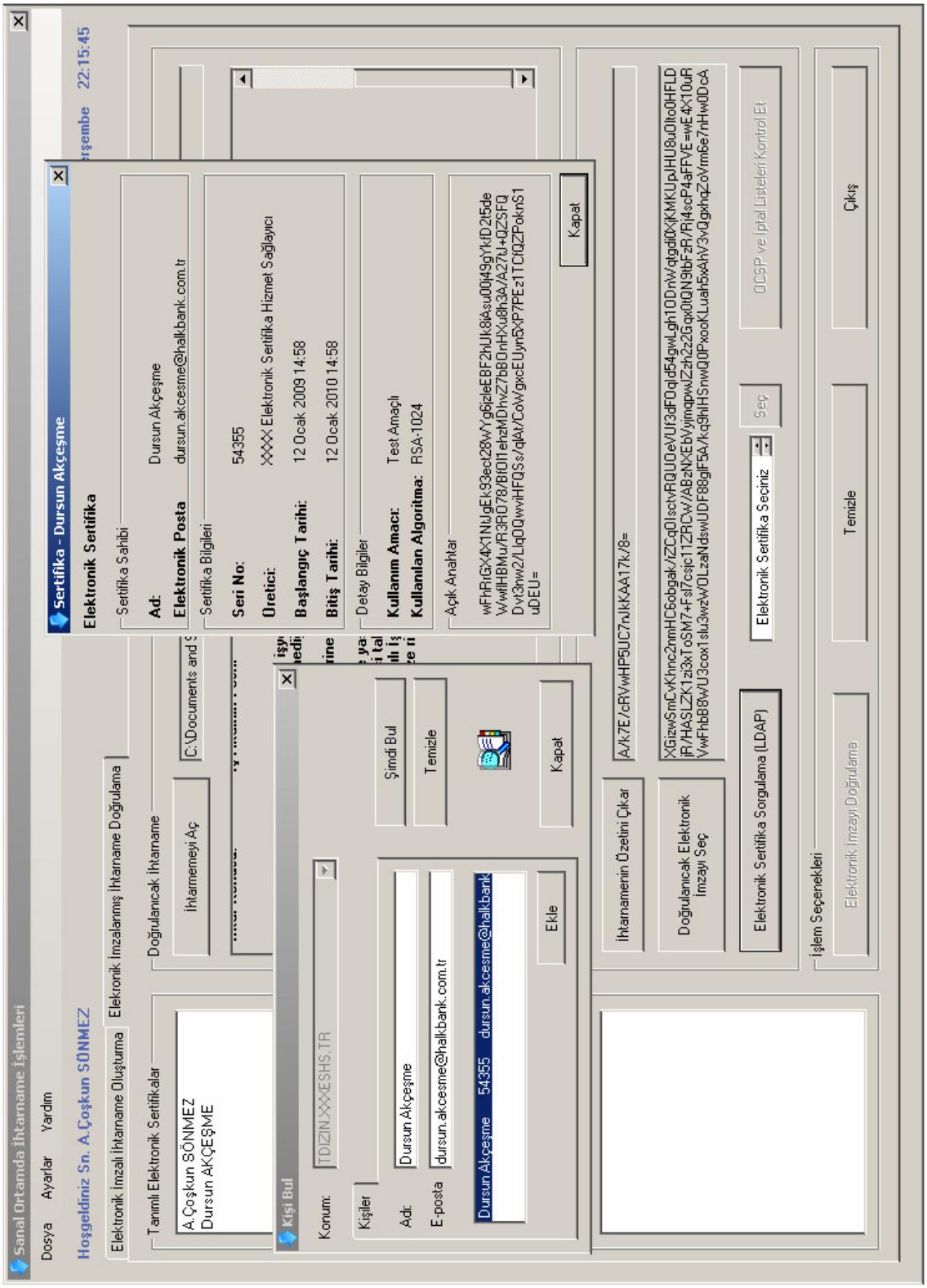
Şekil 8.10 İhtarname doğrulama ekranı



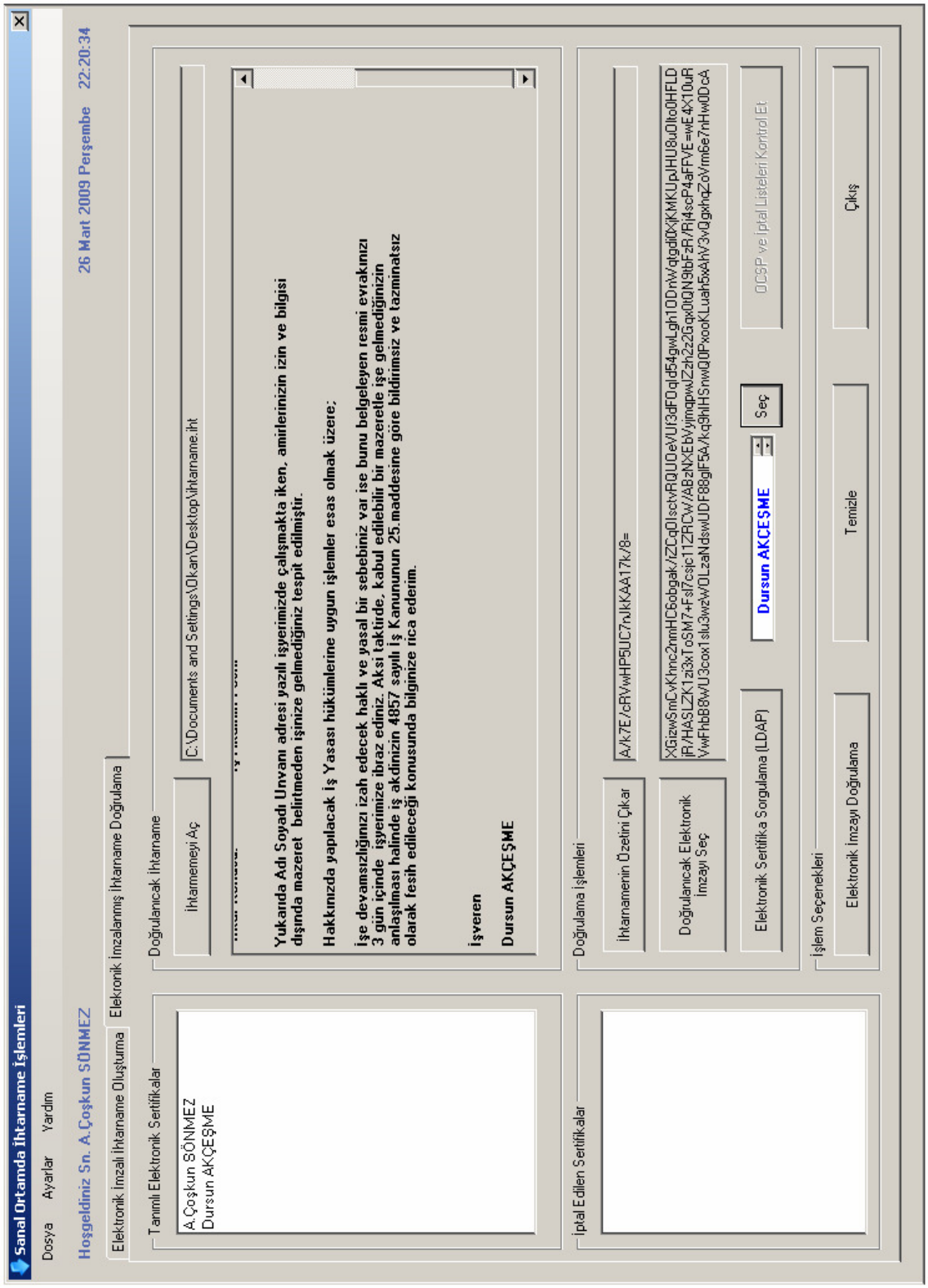
Şekil 8.11 Doğrulama yapılacak ihtarnamenin seçilmesi



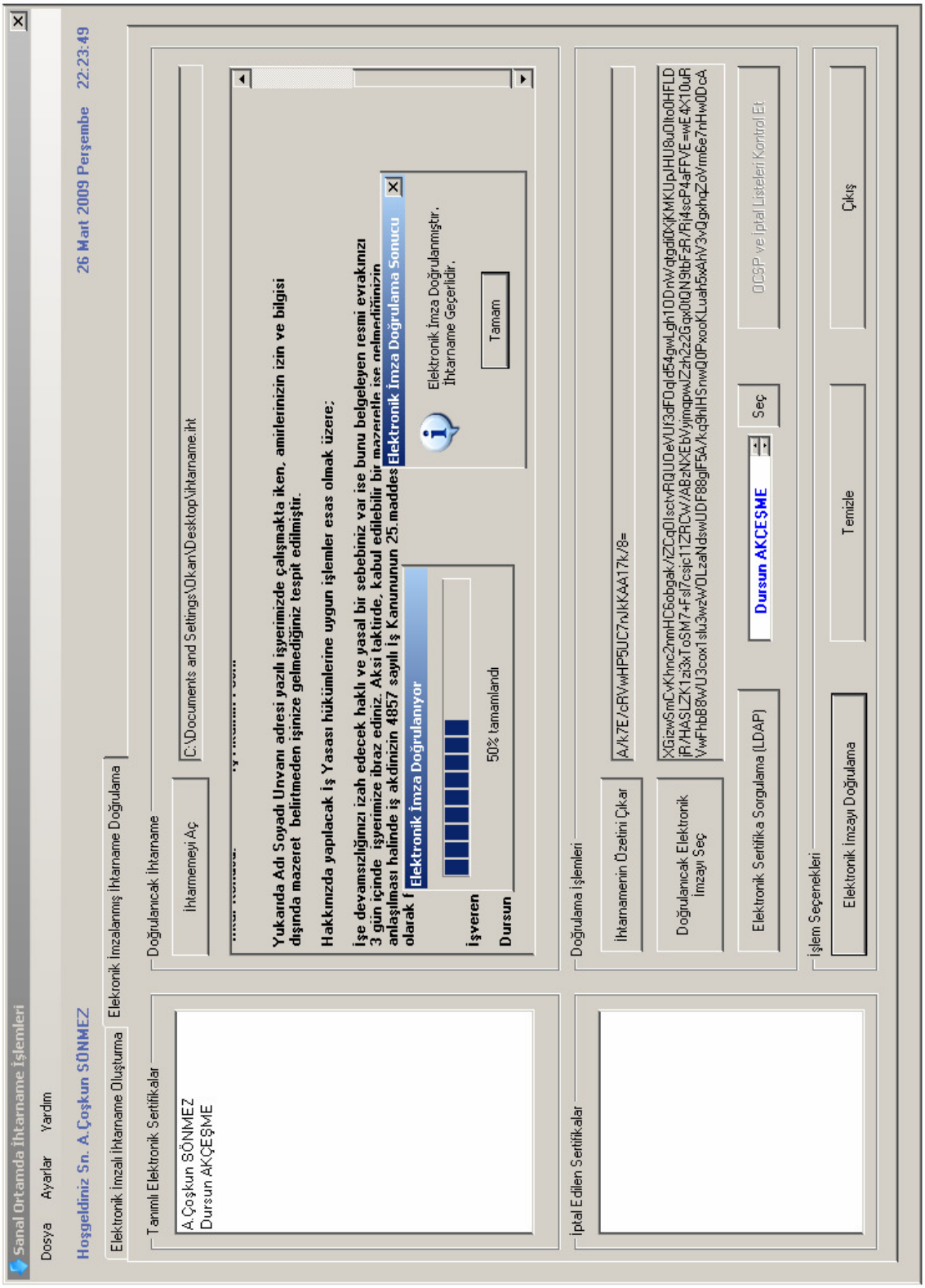
Şekil 8.12 İhtarnamenin özetinin çıkartılması ve doğrulanacak elektronik imzanın seçilmesi



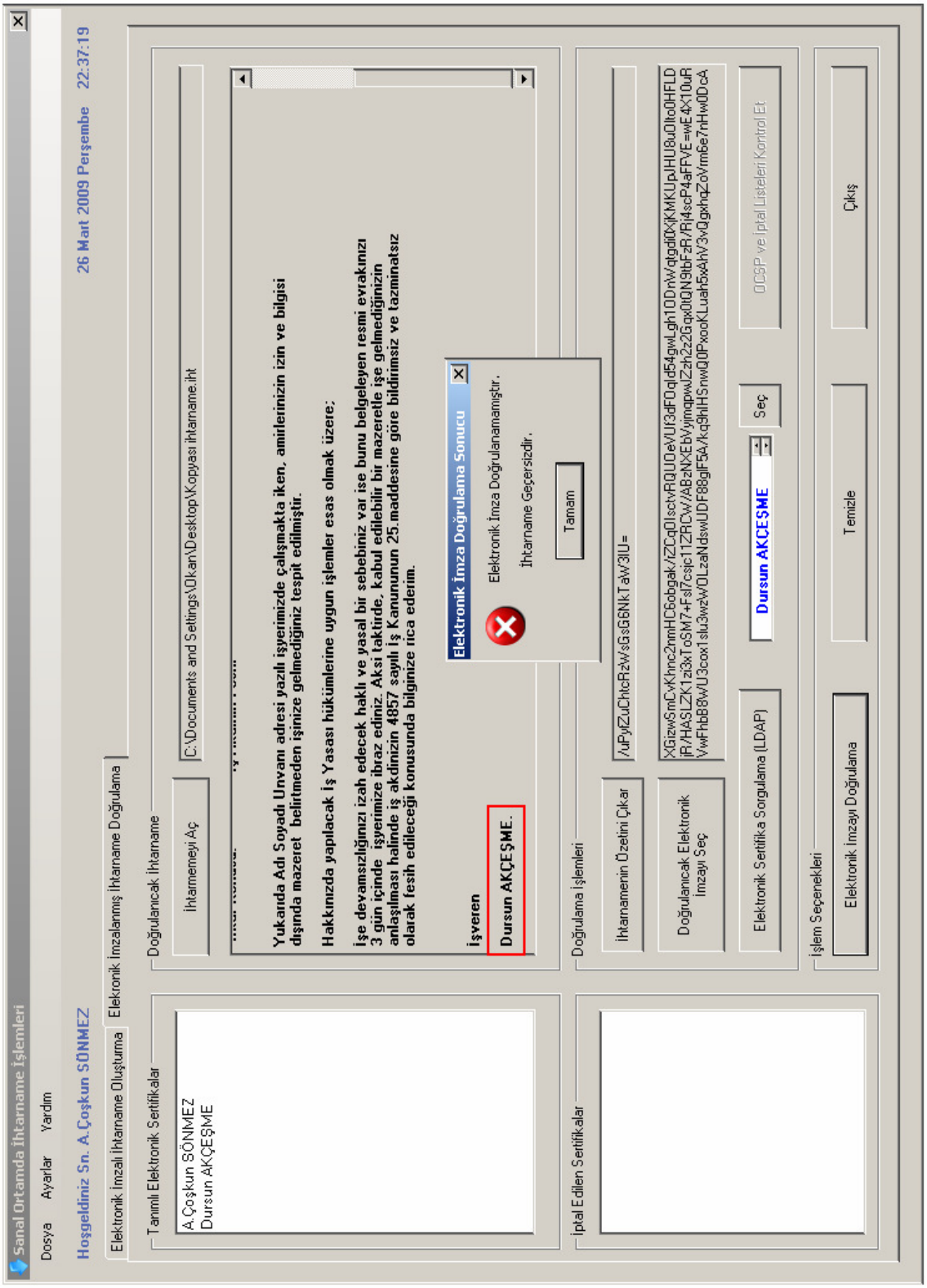
Şekil 8.13 Elektronik sertifikanın sorgulanması ve uygulamaya eklenmesi



Şekil 8.14 Elektronik sertifikanın seçilmesi



Şekil 8.15 Elektronik imzanın doğrulanması



Şekil 8.16 Veri bütünlüğünün bozulması ve elektronik imzanın geçersiz olma durumu

9. SONUÇLAR ve ÖNERİLER

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. İnternetin gelişimi ile beraber sanal ortam ister istemez hayatımızın bir parçası olmuştur. Bu değişime ayak uydurmak bir zorunluluk haline gelmiştir. Hiçbir şekilde sanal ortamdan soyutlanmak mümkün değildir.

Toplumun her ferdinin bir banka hesabı olduğu düşünülür ise bu kişi bir şekilde elektronik işlem yapmak zorundadır. Hesabına maaşı yatıyor ise ATM kullanmalı, hesap hareketleri incelemek için internet şube kullanmalıdır. Kamu hizmetleri içinde aynı şeyleri söyleyebiliriz. ÖSYM artık birçok sınav başvurusunu sanal ortamda almaktadır. Kurumlar artık faturaları kişinin posta adresine göndermek yerine, bir web adresinde yayınlamaktadır. Sağlık sektöründe de benzer gelişmeler yaşanmaktadır. Randevu işlemleri, tahlil sonuçları vb. tüm işlemler sanal ortamdadır. Gelecekte, tüm bu gelişmeler ile beraber bazı işlemler dışında kâğıt üzerinde işlem devri kapanacaktır.

Tüm bu gelişmeler ışığında, E-devlet kapısı olarak tanıtımı yapılan www.turkiye.gov.tr portalının açıldığı bugünlerde, tüm bu işlemlerin ihtiyaç duyduğu güven makamı noterlerin sanal ortamda ne şekilde olabileceğine yönelik bir çalışma yapılmıştır.

Noter hizmetlerine sanal ortamda ihtiyaç olduğu çok açıktır. Fakat tez çalışmasında belirtildiği üzere, noterlerin vermiş olduğu hizmetlerin tümümün sanal ortama taşınması hukuki mevzuattan ve yapılacak işin niteliğinden dolayı mümkün değildir. Fakat noter hizmetlerinin analizi yapıldığında, bazı noter işlemleri için dört koşulun yerine getirilmesinin yeterli olduğu görülmüştür. Çalışmada bu işlemleri sanal ortamda nasıl güvenli bir şekilde yapabileceğine yönelik bir model sunulmuştur.

Sanal ortamda, gerekli dört koşulu teknolojik olarak modellemek için, tüm dünyada kabul gören, ıslak imzanın sanal ortamda karşılığı olan elektronik imza kullanılmıştır. Elektronik imza altyapısı olan Açık Anahtar Altyapısı'nın noter işlemi için gerekli olan üç koşulu ne şekilde yerine getirdiği görülmüştür. Elektronik imza ile sağlanamayan veri gizliliğinin, yine benzer yöntemlerle sağlanabildiği görülmüştür. Çalışmada bu dört koşulun mevcut teknolojik koşullar ile modellenebileceği somut olarak ortaya konulmuştur.

Bu modelin gerçek hayatta işlemesi için dört koşulun yerine getirilmesi yeterli değildir. Çünkü teknolojik model noterin gerekli koşullarını yerine getirse de hukuki olarak bir anlam ifade etmemektedir. Her ne kadar hukuki geçerliliği olan elektronik imza, modelin temeli olsa

da noterlik kanununda bu işlem şekli düzenlenmemiştir. 5070 sayılı Elektronik İmza Kanunu yalnızca ıslak imza ile eş olduğunu ifade etmekte, nerede ne şekilde kullanılabileceğine yönelik bir tanımlama yapmamaktadır. Modelin hukuki geçerliliğinin olması için gerekli olan hukuki gereksinimler, ana hatlarıyla tez içeriğinde belirlenmiştir.

Çalışmada önerilen model prototip bir uygulama ile modellenmiştir. Uygulamada sanal ortamda modellenebilecek ihtarname işlemi seçilmiştir. Uygulama ihtarnamenin elektronik imzalı olarak oluşturulması ve oluşturulan ihtarnamenin doğrulanmasını kapsamaktadır.

Sanal Noter modeli ile kimlik doğrulamada karşılaşılan sahtekârlıkların da önüne geçilmektedir. Noter işlemi yapmak için yer ve zaman kavramını da ortadan kaldırmaktadır. Bunun yanında bu model ile tezin içeriğinde değinilen kıymetli evrak kaybının önüne geçilmesi, arşivleme ve raporlama yapılması da mümkün olmaktadır.

Yapılan bu çalışma, noter hizmetlerini sanal ortama taşımak için temel gereksinimleri belirlemiştir. Mevcut teknolojik koşulların tüm ihtiyacı karşıladığı aşikârdır. Bundan sonraki süreçte, belirlenen hukuki gereksinimler üzerine yoğunlaşılmalıdır. Elektronik imza ile yapılan işlemlerin adi senet olarak tanımlanmasının ne kadar doğru olduğu tartışılmalıdır.

Ülkemizde elektronik imza kullanılarak yapılan uygulamalar henüz emekleme aşamasındadır. İlk elektronik imza çalışması olan UYAP projesi ile başlayan süreç, Sanayi Bakanlığı, Başbakanlık Dış Ticaret Müsteşarlığı ve Türk Patent Enstitüsü ile devam etmiştir. Görüldüğü gibi yapılan çalışmaların hepsi devlet kurumudur. E-devletin bileşenleri sanal ortamda tek tek modellenmektedir. Fakat e-devletin güven makamı henüz oluşturulmamıştır.

Bu çalışmalardan bir sonraki adım şahsi fikrime göre sanal noter olmalıdır. Bankacılık sektörünün bir çalışanı olarak çalıştığım sektörden bir örnek vermek istiyorum. 80'li yıllarda bankacılık işlemleri hesap kartonları üzerinde takip edilmekteydi. Fakat günümüzde bankacılık işlemleri hesap kartonları üzerinde takip edebiliriz demek, ne kadar imkânsız ise, artan iş yüküyle beraber gelecekte noter hizmetlerini kâğıt üstünde yürütürüz demek o kadar imkânsızdır. Çünkü nasıl bankacılığın işlem hacmi arttıysa, sanal ortamda da e-ticaret hacmi artacak, e-sözleşme, e-fatura, e-devlet vb. uygulamalar artacaktır, bu gelişmelerin sonucunda sanal noter ihtiyacı daha da belirginleşecektir. Günümüz noter hacmi şu an için 80'li yılların bankacılık işlem hacmi düzeyindedir. Fakat bu işlem her geçen gün müthiş bir ivmeyle artmaktadır. Bu sebeple sanal ortamda noterin işlevlerini, gerekli güvenlik sağlanarak modellenmesi zorunluluk haline gelmiştir.

KAYNAKLAR

Akçeşme, D. ve Sönmez, A.Ç., (2008), "Bir Sanal Noter Uygulamasının Teknolojik ve Hukuki Gereksinimleri", Information Security and Cryptology Conference with International Participation (ISCTURKEY 2008), 25-27 Aralık 2008, Ankara.

Akçeşme, D. ve Sönmez, A.Ç., (2008), "Bir Sanal Noter Uygulamasının Gerektirdikleri", Ağ ve Bilgi Güvenliği Sempozyumu 2008, 16-18 Mayıs 2008, Girne/KKTC.

Çağlayan, M.U., (2003), "Bilgi Güvenliği: Dünyadaki Eğilimler", ULAKNET, Sistem Yönetimi Konferansı-Güvenlik, 3-4 Ekim 2003, Ankara.

Çelikyılmaz, S., (2005), "Türkiye'de Kurumlar İçin E-güven Altyapısı E-imza", Elektronik İmza Paneli, 10 Aralık 2005, İstanbul.

Dumortier, J., Kelm, S., Nilsson, H., Skouma, and G., Eecke, P.V., (2003), "The Legal and Market Aspectsof Electronic Signatures", Study Of The European Commission- DG İnformation Society, Service Contract Nr. C 28.400.

Eralp, Ö., Evci, Ö. ve Şentürk, B., (2008), "Ankara 56. Noteri Orhan Turan'la Röportaj", Bilişim ve Hukuk Dergisi, Ankara Barosu", Ankara.

Eralp, Ö., (2006), Mersin Noter Odası Başkanlığı, Bilişim ve Hukuk Sempozyumu, 21 Ocak 2006, Mersin.

Eren, A.M., (2005), "Açık Anahtarlı Kriptografi", Linux Kullanicilari Dernegi – Penguence Dergisi Sayı 2.

Kato, H., (2008), "e-Notarization in Japan", Japan National Notaries Association, May 2008, New Orleans.

Kodaz, H., (2003), "RSA Şifreleme Algoritmasının Uygulaması", Alaeddin Keykubad Kampüsü, Konya.

Kuran, N.H., (2004), "e-imza: Yeni Bir Çağın Başlangıcı", Elektronik İmza Paneli, 15 Temmuz 2004, Ankara.

Mutlu, N. ve Babür, Z.,(2008), "TASDIX; Fikir ve Sanat Eserleri Kanunu ve Elektronik İmza Kanunu'na istinaden, farklı sektörlerdeki eser sahiplerinin fikri mülkiyet haklarını korumada delil oluşturabilmesine olanak sağlayan bir internet uygulaması", Ağ ve Bilgi Güvenliği Sempozyumu 2008, 16-18 Mayıs 2008, Girne/KKTC

National Notary Association, (2007), "Ensuring Trustworthy and Reliable Electronic Documents Through Secure Enotarization", 8 August 2007.

Özenç, K., (2004), "E-imza Uygulamalarında Bilgi Güvenliği ve Teknolojik Altyapı", Telekomünikasyon Kurumu, 15 Temmuz 2004, Ankara.

Paul, G.L., (2004), "The "Authenticity Crisis" In Real Evidence", The Practical Litigator, November 2004.

Sağıroğlu, Ş. ve Alkan, M., (2005), Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara

Sağıroğlu, Ş., (2006), "İnternet ve Elektronik İmza" İnternet Haftası Etkinlikleri, 17 Nisan 2006, Ankara.

Türkiye Noterler Birliği (TNB), (2007), Noterlik Kanunu ve Noterlik Kanunu Yönetmeliği, Ankara

Wang, M., (2008), "Electronic Signatures Law in People's Republic of China", Ph.D (London) LL.M (Manchester) LL.B (ECUPL), May 27-30, 2008.

Yavuz, A., (2006), Digital Notary, YTÜ Computer Department Final Year Project, Yıldız Teknik Üniversitesi.

İNTERNET KAYNAKLARI

[1] http://turk.internet.com/haber/yazigoster.php3?yaziid=9354

[2] http://turk.internet.com/haber/yazigoster.php3?yaziid=9827

[3] http://www.merno.org/tarihce.asp

[4] http://www.alieskici.com/matematik/kriptografi_1.htm

[5] http://www.tk.gov.tr/eimza/eimza_yasasi.htm

[6] http://www.mevzuat.adalet.gov.tr/html/435.html

[7] http://enoter_hukuk.tripod.com/internetkomisyonu.htm

[8] http://www.mevzuat.adalet.gov.tr/html/1303.html

[9] http://www.meb.gov.tr/bilgiedinme/yonetmelik.html

[10] http://www.mevzuat.adalet.gov.tr/html/691.html

[11] http://turk.internet.com/haber/yazigoster.php3?yaziid=15107

[12] http://www.mevzuat.adalet.gov.tr/html/1015.html

[13] http://www.kamusm.gov.tr/tr/Bilgideposu/Mevzuat/e-imza/tarifetalimat.pdf

EKLER

Ek 1 Elektronik İmza Kanunu

23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete Kanun No. 5070

BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1.- Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

Kapsam

MADDE 2.- Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

Tanımlar

MADDE 3.- Bu Kanunda geçen;

a) Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

b) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

c) İmza sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi,

d) İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri,

e) İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,

f) İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri,

g) İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını,

h) Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı,

ı) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,

j) Kurum: Telekomünikasyon Kurumunu,

İfade eder.

İKİNCİ KISIM

Güvenli Elektronik İmza ve Sertifika Hizmetleri

BİRİNCİ BÖLÜM

Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Güvenli elektronik imza

MADDE 4.- Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı

MADDE 5.- Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

Güvenli elektronik imza oluşturma araçları

MADDE 6.- Güvenli elektronik imza oluşturma araçları;

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

Sağlayan imza oluşturma araçlarıdır.

Güvenli elektronik imza doğrulama araçları

MADDE 7.- Güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini

sağlayan,

İmza doğrulama araçlarıdır.

İKİNCİ BÖLÜM

Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar

Elektronik sertifika hizmet sağlayıcısı

MADDE 8.- Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak,

İle ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Kurum, yukarıdaki şartlardan birinin eksikliğini veya yerine getirilmediğini tespit ederse, bu eksikliklerin giderilmesi için, elektronik sertifika hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verir, bu süre içinde elektronik sertifika hizmet sağlayıcısının faaliyetlerini durdurur. Sürenin sonunda eksikliklerin giderilmemesi halinde elektronik sertifika hizmet sağlayıcısının faaliyetine son verir. Kurumun bu kararlarına karşı 19 uncu maddenin ikinci fıkrası hükümleri gereğince itiraz edilebilir.

Elektronik sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında bu maddede gösterilen şartları kaybetmeleri hâlinde de yukarıdaki fıkra hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcıları, Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır.

Nitelikli elektronik sertifika

MADDE 9.- Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

bulunması zorunludur.

Elektronik sertifika hizmet sağlayıcısının yükümlülükleri

MADDE 10.- Elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle,

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle,

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi

durumunda, bu işleyişin güvenliğini sağlamakla,

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

g)Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmekle,

yükümlüdür.

Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

Nitelikli elektronik sertifikaların iptal edilmesi

MADDE 11.- Elektronik sertifika hizmet sağlayıcısı;

a) Nitelikli elektronik sertifika sahibinin talebi,

b) Sağladığı nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,

c) Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,

Durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur.

Elektronik sertifika hizmet sağlayıcısı, faaliyetine son vermesi ve vermiş olduğu nitelikli

elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısı tarafından kullanımının sağlanamaması durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısının faaliyetine Kurum tarafından son verilmesi halinde Kurum, faaliyetine son verilen elektronik sertifika hizmet sağlayıcısının vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısına devredilmesine karar verir ve durumu ilgililere duyurur.

Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez.

Bilgilerin korunması

MADDE 12.- Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

Hukukî sorumluluk

MADDE 13.- Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden

bir kurtuluş kanıtı getirerek kurtulamaz.

Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenir.

Bu maddede öngörülen sertifika malî sorumluluk sigortası Türkiye'de ilgili branşta çalışmaya yetkili olan sigorta şirketleri tarafından yapılır. Bu sigorta şirketleri sertifika malî sorumluluk sigortasını yapmakla yükümlüdürler. Bu yükümlülüğe uymayan sigorta şirketlerine Hazine Müsteşarlığınca sekizmilyar lira idarî para cezası verilir. Bu para cezasının tahsilinde ve cezaya itiraz usulünde 18 inci madde hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür.

Yabancı elektronik sertifikalar

MADDE 14.- Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir.

Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılır. Bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki elektronik sertifika hizmet sağlayıcısı da sorumludur.

ÜÇÜNCÜ KISIM

Denetim ve Ceza Hükümleri

Denetim

MADDE 15.- Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir.

Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

İmza oluşturma verilerinin izinsiz kullanımı

MADDE 16.- Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve beşyüz milyon liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

Elektronik sertifikalarda sahtekârlık

MADDE 17.- Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullananlar, fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve birmilyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

İdarî para cezaları

MADDE 18.- Bu Kanunun;

a) 10 uncu maddesindeki yükümlülüklerinden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onmilyar lira,

b) 11 inci maddesindeki yükümlülüklerden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

c) 12 nci maddesi hükümlerine aykırı hareket edenler hakkında onmilyar lira,

d) 13 üncü maddesinin beş ve yedinci fıkralarındaki yükümlülükleri yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

e) 15 inci maddesi hükmüne aykırı hareket eden elektronik sertifika hizmet sağlayıcısına yirmimilyar lira,

İdarî para cezası Telekomünikasyon Kurulu tarafından verilir. Verilen para cezalarına dair kararlar ilgililere 7201 sayılı Tebligat Kanunu hükümlerine göre tebliğ edilir. Bu cezalara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, verilen cezanın yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir. Bu Kanuna göre verilen idarî para cezaları, Kurumun bildirimi üzerine 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre Maliye Bakanlığınca tahsil olunur.

İdarî nitelikteki suçların tekrarı ve kapatma

MADDE 19.- 18 inci maddedeki suçları işleyenlerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri hâlinde para cezaları iki kat olarak uygulanır, üçüncü kez işlemeleri hâlinde ise Kurum tarafından elektronik sertifika hizmet sağlayıcıları hakkında kapatma cezası verilir.

Kapatma cezası verilmesine ilişkin karar 7201 sayılı Tebligat Kanununa göre ilgililere tebliğ edilir. Bu karara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, yetkili makam tarafından verilen kapatma kararının

yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir.

DÖRDÜNCÜ KISIM

Çeşitli Hükümler

Yönetmelik

MADDE 20.- Bu Kanunun 6, 7, 8, 10, 11 ve 14 üncü maddelerinin uygulanmasına ilişkin usul ve esaslar, Kanunun yürürlük tarihinden itibaren altı ay içinde ilgili kurum ve kuruluşların görüşleri alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir.

Kamu kurum ve kuruluşları hakkında uygulanmayacak hükümler

MADDE 21.- Bu Kanunun 8 inci maddesinin dört ve beşinci fıkraları ile 15 ve 19 uncu maddesi hükümleri, elektronik sertifika hizmet sağlama faaliyeti yerine getiren kamu kurum ve kuruluşları hakkında uygulanmaz.

MADDE 22.- 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir.

Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir.

MADDE 23.- 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmiştir.

MADDE 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır.

MADDE 24.- 5.4.1983 tarihli ve 2813 sayılı Telsiz Kanununun 7 nci maddesinin birinci fıkrasına aşağıdaki (m) bendi eklenmiş ve mevcut (m) bendi (n) bendi olarak teselsül ettirilmiştir.

m) Elektronik İmza Kanunu ile verilen görevleri yerine getirmek,

Yürürlük

MADDE 25.- Bu Kanun yayımı tarihinden altı ay sonra yürürlüğe girer.

Yürütme

MADDE 26.- Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

ÖZGEÇMİŞ

Doğum tarihi	12.12.1981	
Doğum yeri	İstanbul	
Lise	1995-1999	İstanbul Ticaret Odası Anadolu Meslek Lisesi
Lisans	2000-2005	Sakarya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Lisans	2003-2008	Anadolu Üniversitesi İşletme Fakültesi İşletme Bölümü
Yüksek Lisans	2006-2009	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programı

Çalıştığı kurumlar

2006-2007	Cantaş İç ve Dış Ticaret Sogutma Sistemleri A.Ş. Bilgi İşlem Bölümü
2007-Devam ediyor	Türkiye Halkbankası A.Ş Yazılım Geliştirme Daire Başkanlığı