T.C.

SELÇUK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

E-İMZA GÜVENLİĞİNİN ARTIRILMASINA YÖNELİK KONUM DAMGASI SİSTEMİ ÖNERİSİ VE UYGULAMASI

Mustafa ÖZLÜ

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalını

Ocak-2011

KONYA

TEZ KABUL VE ONAYI

Mustafa ÖZLÜ tarafından hazırlanan "E-İmza Güvenliğinin Artırılmasına Yönelik Konum Damgası Sistemi Önerisi ve Uygulaması" adlı tez çalışması 18/02/2011 tarihinde aşağıdaki jüri tarafından oy birliği / ~~oy çokluğu~~ ile Selçuk Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Yrd. Doç.Dr. Abdurrahman SAVAŞ	.....
Danışman Yrd. Doç.Dr. Mesut GÜNDÜZ	.....
Üye Yrd. Doç.Dr. Ahmet BABALIK	.....

Yukarıdaki sonucu onaylarım.

Prof. Dr. Bayram SADE
FBE Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Mustafa ÖZLÜ

17.01.2011

ÖZET

YÜKSEK LİSANS TEZİ

E-İMZA GÜVENLİĞİNİN ARTIRILMASINA YÖNELİK KONUM DAMGASI SİSTEMİ ÖNERİSİ VE UYGULAMASI

Mustafa ÖZLÜ

Selçuk Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç.Dr. Mesut GÜNDÜZ

2011, 78 Sayfa

Jüri
Yrd. Doç.Dr. Abdurrahman SAVAŞ
Yrd. Doç.Dr. Mesut GÜNDÜZ
Yrd. Doç.Dr. Ahmet BABALIK

Elektronik İmza; sahip olduğu kimlik doğrulama, bütünlük ve inkâr edilemezlik özellikleri ile ıslak imzaya eşdeğer olmasının yanı sıra sanal ortamda ihtiyaç duyulan güvenlik, güvenilirlik ve hukuki açıdan geçerlilik ihtiyaçlarına da cevap veren bir teknolojidir. E-imzanın artan kullanım oranları ile birlikte bir takım güvenlik problemleri ortaya çıkmıştır. Bu güvenlik problemleri şifreleme sistemleri, e-imza uygulamaları, servisler veya altyapılara ilişkin olabildiği gibi ıslak imzada karşılaşılabilen, sahte imzaya karşılık gelebilecek yetkisiz kullanım, yetkisiz imzalama problemleri de olabilmektedir.

Bu tez çalışmasında, e-imzanın yetkisiz kullanımına karşı, elektronik olarak imzalanan belgelerin güvenliğini artıracak yeni bir sistem önerilmiştir. Küresel yer belirleme sisteminden de yararlanacak olan bu sistem e-imzalı belgelerin nerede imzalandığının tespit edilmesine ve e-imza kullanımın konum açısından sınırlanabilmesine olanak sağlamıştır. Çalışma kapsamında önerinin gerçekleşebilirliğini ortaya koymak için geliştirilen e-imza güvenliğinin artırılmasına yönelik konum damgası sistemi uygulaması başarılı sonuçlar vermiştir.

Anahtar Kelimeler: Elektronik İmza, Küresel Yer Belirleme Sistemi, Veri Güvenliği

ABSTRACT

MS THESIS

LOCATION STAMP SYSTEM PROPOSAL AND APPLICATION FOR DEVELOPING ELECTRONIC SIGNATURE SAFETY

Mustafa ÖZLÜ

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF SELÇUK UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE
IN COMPUTER ENGINEERING

Advisor: Assist. Prof.Dr. Mesut GÜNDÜZ

2011, 78 Pages

Jury
Assist. Prof.Dr. Abdurrahman SAVAŞ
Assist. Prof.Dr. Mesut GÜNDÜZ
Assist. Prof.Dr. Ahmet BABALIK

Electronic Signature; with its authentication, integrity and non reputation features and besides being equivalent with wet signature, is a technology responding to the needs for internet security, reliability and legally acceptability. The usage of e-signature and with the development of the rates brought few security problems with it. These security problems can be about code system, e-signature applications, and services or can be about substructures. Besides they can be about fake signatures looks like wet signature, responding to unauthorized usage, unauthorized signature problems.

In this study, unauthorized usage against e- signature's and to increase the safety of electronically signed documents a new system is suggested. The system which will be able to utilise the Global Positioning System so the user will be able define the geographical coordination's which its e-signature document has been signed and the location of the e-signature usage can be limited. In order to show the materialisation of the suggestion and improve e- signature safety, the applications of the Location Stamp System has been developed and has came out with successful solutions.

Keywords: Data Security, E-Signature, Global Positioning System

TEŞEKKÜR

Bu tezin yazımının süresince beni yönlendiren, yakın ilgi ve önerileriyle yol gösteren ve desteğini esirgemeyen danışmanım, Sayın Hocam Yrd. Doç.Dr. Mesut GÜNDÜZ'e teşekkür ederim.

Eğitim hayatım boyunca yardımlarını ve desteklerini esirgemeyen sevgili anneme, babama ve eşime sonsuz teşekkür ederim.

Mustafa ÖZLÜ

KONYA-2011

İÇİNDEKİLER

KISALTMALAR

AAA	Açık Anahtar Altyapısı
A-GPS	Assisted Global Positioning System – Yardımlı Yer Belirleme Sistemi
API	Application Programming Interface – Uygulama Programlama Arayüzü
BSI	British Standarts Institute - İngiliz Standartlar Enstitüsü
CBS	Coğrafi Bilgi Sistemi
CEN	Comité Européen de Normalisation – Avrupa Standartlar Komisyonu
CWA	CEN Workshop Agreement - CEN Çalıştay Kararı
DES	Data Encryption Standard - Veri Şifreleme Standardı
EC	European Commmision – Avrupa Komisyonu
E-İMZA	Elektronik İmza
E-POSTA	Elektronik Posta
ESHS	Elektronik Sertifika Hizmet Sağlayıcı
ETSI	European Telecommunications Standarts Institute - Avrupa Telekomünikasyon Standartları Enstitüsü
GPS	Global Positioning System – Küresel Yer Belirleme Sistemi
KAMU SM	Kamu Sertifikasyon Merkezi
KDS	Konum Damgası Sistemi
MD	Message Digest – Mesaj Özet Algoritması
NAVSTAR	Navigation Satellite Timing and Ranging
OCS	Operating Control System
PKCS	Public Key Cryptography Standard - Açık Anahtar Alt Yapısı Standardı
PKI	Public Key Infrastructure - Açık Anahtar Altyapısı
PPS	Precise Positioning Service - Duyarlı Konum Belirleme Servisi
SMTP	Simple Mail Transfer Protocol - E-posta Gönderme Protokolü
SSH	Secure Shell - Güvenli Kabuk
SPS	Standart Positioning Service – Standart Konum Belirleme Servisi
SSL	Security Socket Layer - Güvenli Soket Katmanı
VPN	Virtual Private Network - Sanal Özel Ağ
WWW	Wolrd Wide Web - Dünya Çapında Ağ
ZD	Zaman Damgası

1. GİRİŞ

Elektronik İmza, internet ortamının hızlı gelişimine paralel olarak hayatımızda her gün daha fazla yer bulan, sanal ortamda yapılan işlemlerde ihtiyaç duyulan güvenlik, güvenilirlik ve hukuki açıdan geçerlilik ihtiyaçlarına da cevap veren bir teknolojidir. Artan kullanım oranlarıyla birlikte güvenliğe ilişkin çeşitli problemler de ortaya çıkmakta, bu teknoloji çeşitli tehditlere ve saldırılara maruz kalabilmektedir. Bu saldırıları önlemek ve güvenliği artırmak için şifreleme algoritmaları ile ilgili bir takım çalışmalar yapıldığı, fakat yetkisiz kullanıma ilişkin çalışmaların yetersiz olduğu görülmüştür.

Günümüzde elektronik imzaya ilişkin güvenlik önlemleri genelde içerik ve özet fonksiyonları için bir takım şifreleme algoritmalarından ibarettir. Fakat bu algoritmalar kırılamaz değildir, hatta bazıları kırılmıştır. Bu yüzden e-imza gibi sonuçları itibariyle ıslak imzaya eşdeğer olan ve büyük önem arz eden bir yapıya ilişkin güvenliği sadece şifreleme algoritmalarından ibaret olarak düşünmemek, alternatif güvenlik tedbirleri düşünmek ve tasarlamak ve hayata geçirmek gerekmektedir.

Bu çalışmada amaç hukuki açıdan ıslak imza ile aynı sonuçları doğuran elektronik imza ile imzalanan dosyaların yetkisiz kullanımına karşı elektronik olarak imzalanan, konum bilgisi eklenmiş dosyanın geldiği konumun ve imzalanan dosyanın açılabileceği konumun belirlenerek gönderim hedefinin doğrulanması suretiyle güvenlik özelliklerinin artırılmasıdır. Bu bağlamda elektronik imzalı belgeye, elektronik imzalama işleminin nerede gerçekleştiğine ilişkin küresel yer belirleme sisteminden elde edilen konum bilgilerinin eklenmesi ve bu bilgilerin doğrulanabilmesi önerilmektedir. Bu sayede elektronik imza işlemin gerçekleştiği yer de ispatlanabilir olacaktır.

Elektronik İmzanın güvenliğini artırmaya yönelik gerçekleştirilen bu çalışmanın ikinci bölümünde kaynak araştırmasına yer verilecektir. Materyal ve metod bölümünde çalışmamızın temellerini oluşturan elektronik imza ve küresel yer belirleme sistemi ana hatlarıyla ele alınacak, bölümün devamında metod olarak önerdiğimiz Konum Damgası Sistemi ve bu sistemin gerçeklenebilirliğini gösteren yazılım uygulamaları anlatılacaktır. Dördüncü bölümde araştırma ve tartışmalara yer verilecek olan çalışma sonuç ve öneriler bölümü ile son bulacaktır.

2. KAYNAK ARAŞTIRMASI

MARCO ve arkadaşlarına göre (1998) elektronik ortamda üretilen, saklanan ve iletilen bilgilerin güvenilir olması için güvenlik özelliklerini sağlayacak şekilde saklanması ve iletilmesi gereklidir. Çünkü elektronik ortamda servis ve protokollerin sağladığı kolaylıkları yanında; sahtecilik, aldatma, mesaj başlığını/içeriğini değiştirme, yeniden oluşturma gibi yöntemler kullanılarak ve farklı kaynaktan, farklı içerikli mesaj gönderilerek alıcı ve göndericinin yanıltılması mümkün olabilmektedir.

Saygı ve Yeşil'in (2006) de işaret ettiği gibi, e-imza kullanımının yaygınlaşması, elektronik imzaya karşı duyulan güvenin tesis edilerek toplumda kabul edilmesine de bağlıdır ve elektronik imzanın güvenliği, ele alınması gereken hususlar arasındadır. Bu nedenle elektronik imza güvenliğinde önemli olan algoritma ve parametrelerle ilgili bir araştırma yapılması gerekmektedir.

Spalka, Cremers ve Langweg (2002) sınırlı da olsa bazı kötücül yazılım türlerinin e-imza oluşturma sürecine olan olumsuz etkilerini ele almışlardır. Çalışmalarında Almanya'daki e-imza oluşturma uygulamalarının (IOU) en tehlikeli kötücül yazılım türlerinden biri olan Truva atları ile nasıl sekteye uğratılabileceğini örnekler ile gözler önüne sermişlerdir.

WANG ve arkadaşlarının tespitine göre (2005) tüm dünyada standart olarak kullanılmakta olan elektronik imza şemaları, genelde "MD Ailesi"ne mensup özet fonksiyonlarını kullanmaktadır. MD ailesinin en önemli temsilcileri olan MD4, MD5, RIPEMD, RIPEMD-160, SHA-0, SHA-1, SHA-256 ve SHA-512 özet fonksiyonları aynı yapıtaşlarını kullanmakta ve küçük farklarla birbirlerinden ayrılmaktadır. WANG ve arkadaşları son yıllarda yaptıkları çalışmalarla bu özet fonksiyonlarının bir kısmının kriptografik olarak güvenli olmadığı ortaya çıkarmışlardır.

CEN (Comité Européen de Normalisation – Avrupa Standartlar Komisyonu) elektronik imza güvenliği'ne bir çok standardı ortaya koymuştur. Türkiye'de bu standartlara dayanarak TÜBİTAK Kamu Sertifikasyon Merkezi (2005), Bilgi Teknolojileri İletişim Kurumu'nun yayınladığı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in (2005) kapsamında kamu kurumları için e-imza güvenliğine ilişkin bir dokuman oluşturmuştur.

Bu dokümanda güvenli elektronik imza oluşturma ve doğrulama yazılımlarının sağlaması gereken şartlar kontrol listesi olarak verilmiştir. Bu dokümanda güvenli elektronik imza oluşturma ve doğrulama yazılımlarının sağlaması gereken şartlar

kontrol listesi olarak verilmiştir. Doküman iki bölümden oluşmaktadır. Birinci bölümde güvenli elektronik imza oluşturma yazılımlarının sağlaması gereken özellikler belirtilmiştir. İkinci bölümde güvenli elektronik imza doğrulama yazılımlarının sağlaması gereken özellikler belirtilmiştir. Kontrol listesi hazırlanırken CWA (Cen Workshop Agreement) 14170 ve CWA 14171 dokümanları referans alınmıştır. Listede CWA'e göre sağlanması zorunlu olan, opsiyonel ve koşullu olarak sağlanması gereken özellikler belirtilmiştir. Zorunlu olarak belirtilen özelliklerin yazılım tarafından sağlanması gerekmektedir. Kontrol listesinde bilgilenme amaçlı istenen, yazılımla ilgili diğer bilgiler de mevcuttur.

Tebliğe göre aşağıdaki bileşenlerin aksi belirtilmedikçe ve özel bir durum olmadıkça güvenli elektronik imza oluşturma yazılımı içerisinde bulunması CWA 14170'e göre zorunludur.

1. Kullanıcı Belgesinin Sunulması (Signer's Document Presentation) Bileşeni
2. İmza Özellikleri Görüntüleyici (Signature Attribute Viewer) Bileşeni
3. İmza Sahibi Etkileşimi (Signer Interaction Component) Bileşeni
4. İmzalanacak Veri Formatı (Data To Be Signed Formatter) Bileşeni
5. İmza Sahibi Kimlik Doğrulama (Signer Authentication) Bileşeni
6. Veri Özetleme (Data Hashing) Bileşeni
7. Güvenli Elektronik İmza Oluşturma Aracı İletişimcisi (SCDev/SCA Communicator)
8. Güvenli Elektronik İmza Oluşturma Aracı Kimlik Doğrulama (SCDev/SCA Authenticator) –Conditional

Aşağıdaki bileşenlerin için ise aksi belirtilmedikçe ve özel bir durum olmadıkça güvenli elektronik imza doğrulama yazılımı içerisinde bulunması CWA 14171'e göre zorunluluğu vardır.

1. İmza dosyası içeriğindeki bilgilerin elde edilmesi
2. İmzanın doğrulanması ve doğrulama verilerinin elde edilmesi
3. Doğrulama verilerinin eklenerek gelişmiş imza formatının oluşturulması

1980'li yıllarda ABD tarafından Küresel yer belirleme sistemi (GPS - Global Positioning), Rusya Federasyonu tarafından GLONASS (Global Navigation Satellite System) geliştirilmiştir. Kennedy (2002), GLONASS ve GPS sistemlerinin birbirlerine çok benzeyen sistemler olmasına rağmen GPS dünyada daha yaygın olarak kullanılmakta olduğunu tespit etmiştir.

Enge'ye (2003) göre GPS, uydu sinyalleri yardımıyla, herhangi bir yer ve zamanda, her türlü hava koşullarında, global bir koordinat sisteminde, yüksek duyarlılıkta, ekonomik olarak, anında ve sürekli konum ve zaman bilgilerini belirlemeye olanak veren yüksek doğruluklu küresel konum belirleme ve navigasyon sistemidir. GPS hem askeri hem de sivil kullanım alanları olan bir sistem olup, çoğunluğu sivillerden oluşan 20 milyon kullanıcısı mevcuttur.

Doğru ve Uluğtekin (2005), günümüzde navigasyonun gelişmekte olan konum belirleme ve iletişim tekniklerini, sayısal haritaları, bilgisayar ve avuç içi araç teknolojilerini kullanan, özel olarak tasarlanmış navigasyon sistemleri aracılığı ile yapılmakta olduğunun altını çizmişlerdir. Bu sistemlerin navigasyonu, daha ilgi çekici ve kolay bir hale getirdiğini söylemişlerdir. Aynı zamanda bu gelişmeler ile navigasyon, günlük hayatın parçası olan sıradan bir aktivite olmaktan çıkıp birçok teknolojiyi içinde bulunduran bir pazar haline geldiğini vurgulamışlardır.

Çınar'a (2004) göre radyo navigasyon araçları ile elektronik sinyaller yayarak daha karmaşık türde navigasyon yapmak mümkündür. Bu sinyallerin islenmesi ile kullanıcı, konumunu belirli doğruluk sınırları içerisinde belirleyebilmektedir.

Kahraman ve Seke'ye göre (2004) sabit alıcı gözlem yaptığı tüm uydulara ait uydu-alıcı uzaklıklarını (kod ya da faz pseudorange) hesaplayarak bu değerleri kendi duyarlı konumundan yararlanarak hesapladığı (olması gereken) pseudorange'ler ile karşılaştırır. Aradaki farklar gözlem hatası olarak yorumlanır ve bu farklar konumu belirlenecek olan noktalardaki hareketli alıcı /alıcılar tarafından kaydedilen gözlemlere düzeltme olarak getirilerek hareketli alıcının konumu doğru olarak belirlenir. Söz konusu düzeltmeler hareketli alıcılara, alıcılar arasındaki uzaklığa bağlı olarak portatif telsizler, yer istasyonları ve uydular vasıtasıyla yayınlanmaktadır.

Avcı, Doğru ve Kılıç'a göre (2002) günümüzde Loran ve Global Konum Belirleme Sistemi (GPS) saatleri uyuşumu sağlanarak kombine sistemler oluşturulmuştur. Böylelikle kullanıcının, iki uydu ve bir Loran istasyonu kullanarak konum belirlemesine olanak sağlamıştır.

Kahveci ve Yıldız'a (2005) göre GPS sistemlerinde radyo vericileri, yüksek yörüngelerde dolaşarak daha fazla kapsama alanı sağlayan uydulara yerleştirilmektedir. Uydular referans noktaları gibi hareket etmekte ve üç boyutlu konumlamanın yapılabilmesi için uydulara olan mesafeler ölçülmektedir.

3. MATERYAL VE YÖNTEM

Bu çalışmada ana materyaller elektronik imza ve küresel yer belirleme ele alınmıştır. Yöntem olarak ise Konum Damgası Sistemi önerilmiştir. Bu bölümün alt bölümlerinde bu konulara ilişkin bilgilere yer verilecektir.

3.1. ELEKTRONİK İMZA

3.1.1. E-imza nedir?

Türkiye'de 2005'te yürürlüğe giren 5070 Sayılı Elektronik İmza Kanunu, Elektronik İmza'yı: "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlamıştır (5070 Sayılı Elektronik İmza Kanunu, 2004) (EK-A). 13 Aralık 1999 tarihli Avrupa Birliği 99/EC /93/EC sayılı Elektronik İmza Direktifi'nde ise elektronik imza, doğrulama yöntemi olarak hizmet veren ve başka bir elektronik veriye eklenmiş veya mantıksal olarak ilişkilendirilmiş elektronik biçimindeki veri olarak tanımlanmıştır. Tanımdan da anlaşılacağı gibi bir Elektronik İmza'nın bilgi bütünlüğü, kimlik doğrulama, inkâr edilemezlik özelliklerine sahip olması gerekmektedir.

Elektronik imza ve el ile atılan ıslak imza kanunen eşdeğerdir ve elektronik imza ile oluşturulmuş veriler senet hükmündedir (5070 Sayılı Elektronik İmza Kanunu, 2004) (EK-A). Bu yüzden elektronik imza güvenliği büyük önem arz etmektedir. İlter (2005) elektronik imza, elektronik ortamda muhatapların kesin olarak tespit edilmesini sağlaması ve güvensizlik duygusunu ortadan kaldırması sebebiyle e-devlet ve e-ticaret uygulamalarının gerçekleştirilmesinde hayati öneme sahip unsurlardan birisidir. DUMORTIER ve arkadaşlarına göre (2003) bu nedenle, elektronik imza ile ilgili hukuki düzenlemeler dünya genelinde son yıllarda yürürlüğe konulmaya başlanmıştır. Türkiye'de Elektronik İmza Kanunu, Avrupa Birliği'nde Elektronik İmza Direktifi ile elektronik imzaların hukuki açıdan tanınmasına imkân sağlamıştır.

5070 Sayılı Elektronik İmza Kanunu'na göre e-imza kanunların resmi şekle veya özel bir merasime gerek duyduğu hukuki işlemler olan, noterlik işlemleri, tapu işlemleri, evlenme merasimleri, veraset ve intikal ile teminat sözleşmelerinde uygulanmamaktadır. Yakın tarihlerde ortaya çıkan bir takım güvenlik gereksinimlerden ötürü elektronik imza ile ilgili birçok yasal düzenleme gerçekleşmiştir (EK-B).

3.1.2. Elektronik imzanın altyapısı

5070 sayılı Kanunda belirtilen hükümler ve kullanılan terminoloji dikkate alındığında ilgili şartların günümüzde "Açık Anahtar Altyapısı" (AAA) ile sağlanabileceği görülmektedir. Saygı ve Yeşil (2006) AAA'nın, sayısal imzanın dayandığı teknoloji olan açık anahtar şifrelemesinden (asimetrik şifreleme) doğduğunu belirtmişlerdir. Buna göre açık anahtarla şifrelenen bir veri, sadece bu anahtarın gizli olanı kullanılarak deşifre edilebilir. Gizli anahtar kişiye özeldir ve sadece o kişi tarafından bilinir ve kullanılır. Bu anahtar çiftinin diğeri olan açık anahtar ise farklı şekillerde kullanıcılara duyurabilir. Duyuru işlemi, bir web sitesinden ya da e-posta ile yapılabilir. Gizli anahtarların, güvenliği yüksek ortamlarda üretilmesi ve korunmaları gereklidir. Bunun için akıllı kart gibi donanımlar kullanılır.

Türkiye'de E-imza ile ilgili düzenleyici kuruluş olan Bilgi Teknolojileri ve İletişim Kurumu'na göre (2005), bir AAA tipik olarak kök sertifika otoritesi, alt sertifika otoritesi, kayıt otoritesi, elektronik sertifikalar, güvenlik politikaları, güvenen taraf gibi bileşenlerden oluşur. Sertifika otoriteleri, gizli anahtarlara karşılık gelen açık anahtarların kişinin kimlik bilgileriyle ilişkilendirildiği elektronik sertifikaları üretir ve yayınlar. AAA kullanılarak oluşturulan bir elektronik imzanın kimden geldiğinin belirlenmesi, imzalanmış metnin elektronik ortamdaki doğruluğunun ve bütünlüğünün sağlanması, atılan imzanın imza sahibi tarafından inkâr edilememesi sağlanmış olur.

3.1.3. Elektronik imzanın özellikleri

5070 Sayılı Elektronik İmza Kanunu'na göre elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

İTO (2009) yaptırdığı çalışmada, bir elektronik mesaj veya iletiye eklenen ve göndereni eşsiz bir şekilde tanımlayan veya kopya ve/veya taklit edilmesi çok zor olan bir sayısal kod olarak tanımlanan sayısal imza (elektronik imza) da bulunması gereken en önemli özellikleri şöyle sıralamıştır;

- Yazılı dokümanlarda kullandığınız imzalar gibi, e-imzalar da günümüzde e-posta veya elektronik verilerin yazarlarını/sahiplerini tanılamada kullanılmaktadır.

- Elektronik İmzalar, Elektronik Sertifikalar kullanılarak yaratılır ve doğrulanırlar.

- Bir bilgiyi imzalamak, güvenli bir alışverişi gerçekleştirmek için kendi özel Elektronik Sertifikanıza ihtiyaç vardır.
- Günümüzde uluslararası yasama organları e-imzaları ıslak imzalar gibi yasal olarak bağlayıcı ve uluslararası çapta kabul edilebilir kılmak için yasalar çıkarmışlardır.

Gen Bilim (2006) E-imza özelliklerini 4 başlıkta incelemiştir, bunlar;

3.1.3.1. Kimlik kanıtlama

Kimlik kanıtlama, iletişimin kaynağı veya başlangıcı ile ilgilidir. Mesaj kimden geldi veya gelen mesaj hakiki bir mesaj mı yoksa sahte bir mesaj mı sorularına cevap alınmasını sağlayan AAA sisteminin bu fonksiyonu, dijital sertifika ile birlikte sağlanmaktadır.

3.1.3.2. Bütünlük

Bütünlük fonksiyonu iletişimin doğru ve eksiksiz şekilde tamamlandığını gösterir. Alıcının aldığı doküman, göndericinin gönderdiği dokümanla aynı mı, gönderim işlemi tamamlandı mı ve doküman depolanma veya gönderilme sırasında değişime uğradı mı gibi sorular bu başlık altında yanıt bulmaktadır.

3.1.3.3. İnkâr edilemezlik

İnkâr edilemezlik fonksiyonu iletilen mesajın göndericisi tarafından iletildiğinin kanıtlanmasına yarar. Mesajı gönderen, mesajı göndermediğini ve bu mesajın kendisine ait olmadığını bu fonksiyon sayesinde iddia edemez.

3.1.3.4. Gizlilik

Veri güvenliği iletişim ağlarında çok önemli bir role sahiptir. İş planları, finansal işlemler, fikri mülkiyet, kişisel veriler, üçüncü kişilere ait bilgiler gibi hassasiyeti olan verilerin güvenliğinin en yüksek düzeyde sağlanması gerekir. İletişim ağlarında güvenliği sağlamak için matematiksel bir işlem olan şifreleme kullanılmaktadır. Veri güvenliğinde iki tür şifreleme tekniği kullanılmaktadır. Bunlar, simetrik ve asimetrik şifreleme teknikleridir.

3.1.4. Elektronik sertifika ve nitelikli elektronik sertifika

3.1.4.1. Elektronik sertifika

5070 Sayılı Elektronik İmza Kanunu'na göre Elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik kaydı ifade eden sertifikalara Elektronik Sertifika adı verilmektedir. Elektronik sertifikalar, kanuna uygun olarak faaliyette bulunacak elektronik sertifika hizmet sağlayıcılarından (ESHS) belirli bir ücret karşılığında temin edilmektedir.

Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluğunu garanti edecektir. Elektronik sertifikalar, atılan imzanın doğruluğunun teyit edilebilmesi için gereklidir.

3.1.4.2. Nitelikli elektronik sertifika

5070 sayılı Elektronik İmza Kanununun 9 uncu maddesinde belirtildiği şekilde; "nitelikli sertifika" olduğuna dair bir ibareyi, sertifika hizmet sağlayıcısının (ESHS) kimlik bilgilerini ve kurulduğu ülke adını, imza sahibinin teşhis edilebileceği kimlik bilgilerini, sertifikanın geçerli olduğu süreyi ve sertifikanın seri numarasını barındıran elektronik sertifikalara Nitelikli Elektronik Sertifika "NES" adı verilmektedir. Türkiye'de sağlanan elektronik imza hizmeti Nitelikli Elektronik Sertifika ile olmaktadır.

Bilgi Teknolojileri ve İletişim Kurumu tarafından ESHS olarak yetkilendirilmemiş birçok yerli ve yabancı firma bireysel e-imza hizmeti vermektedir.

Ama bunların hukuken bir değeri yoktur. Sadece kimlik tanımlamaya yarar, yani bir nevi kartvizit görevi görürler. Türkiye'de ESHS'ler tarafından sağlanılan Nitelikli Elektronik Sertifika (NES) Güvenli Elektronik imza ile aynı anlama gelmektedir.

3.1.5. Elektronik imza nasıl kullanılır

İTO (2009) çalışmasına göre elektronik imza sertifikaları bir imzalama işlemi için imza sahibi tarafından güvenli elektronik imza oluşturma aracı ve bu araca erişimi sağlayan bir şifrenin girilmesi sayesinde imza sahibinin iradesi ile kullanılabilmektedir.

Nitelikli Elektronik Sertifika (Güvenli Elektronik İmza) Hizmet Sağlayıcıları elektronik imza kurulumunu yaptıktan sonra kullanıcılara e-imzalarını kullanabilmeleri için Güvenli Elektronik İmza Oluşturma Araçları ile gelirler. Bu araçlar, Flash belleğe benzeyen Token adı verilen Akıllı Çubuklar veya akıllı kartlar ve bunları destekleyen yazılımlar şeklinde kullanıcılara sunulabilir.

Hizmet Sağlayıcısı, kullanıcıya (e-imza sahibine) sertifikasını kredi kartı gibi bir donanım (akıllı kart) üzerinde veriyor ise kullanıcı kart ile birlikte bu kartın okuyucusuna da ihtiyaç duyacaktır. Bu kart okuyucu sertifika satın alınırken beraberinde verilebilir veya kullanıcının kendisinin alması gerekebilir. Böyle bir araç temini gerçekleştirileceği zaman kart okuyucusu ile ilgili bilgilerin de doğru şekilde elde edilmesi daha sonra ekstra bir masrafla karşılaşılmasını önleyecektir.

Gelişmiş elektronik imzanın unsurlarını taşıyan bir elektronik imzanın, nitelikli elektronik sertifikaya dayanması ve güvenli imza oluşturma araçları ile oluşturulmuş olması gerekmektedir. Bu gerekliliğe Türk hukukunda, "güvenli elektronik imza" kavramı denilmiştir. Buna göre güvenli elektronik imzada bulunması gereken özellikler şunlardır:

- Münhasıran imza sahibine bağlı olmalı,
- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmuş olmalı,
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamalı,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamalıdır.

3.1.6. Elektronik imza oluşturma araçları

İmza oluşturma araçları; elektronik imza oluşturmak üzere kullanılan yazılım veya donanımı ifade etmektedir. 5070 sayılı Kanun'da "güvenli" elektronik imza oluşturma araçlarına değinilmiş ve aşağıdaki özelliklerin sağlanması şart koşulmuştur:

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

3.1.7. Elektronik imza kullanım alanları ve yararları

E-imzanın, elektronik iletişim de daha güvenli bir ortam oluşturabilecek olması nedeniyle gerek kişiler ve kurumlar gerekse serbest piyasa da olumlu etkiler ortaya çıkaracağı düşünülmektedir. Elektronik imzanın sağlayacağı yararlar İTO (2006) genel olarak şöyle sıralanmıştır;

- Güvenilir bir kimliklendirme ve onay mekanizmasıyla güvenli olarak elektronik ortamlarda işlemlerin yapılabilmesine katkılar sağlayacaktır.
- İş ve işlemler hızlıca yapılabilecektir.
- İş maliyetleri düşecek, verimlilik artacaktır.
- İş takipleri kolaylaşabilecektir.
- Elektronik ortamlarda meydana gelebilecek güvenlik zafiyetleri ve açıklar ortadan kaldırılabilecektir.

- Elektronik ortamlara güven artacak dolayısıyla elektronik ortamlarda yapılabilecek iş ve işlemlerde artışlar meydana gelecektir.
- e-ticaret hacimleri artacaktır.

E-imzanın, bankalar ve finans kurumları, şube ağına sahip sigorta şirketleri, kamu kurum ve kuruluşları, holdingler ve diğer büyük şirketler, üniversiteler, yüksek iletişim ve bilgi güvenliği gereksinimi olan organizasyonlar başta olmak üzere orta ve uzun vadede yaygın bir uygulama alanı bulacaktır. Gerek kamusal gerekse ticari alandaki muhtemel e-imza uygulamaları arasında aşağıdakiler sayılabilir (İTO,2006):

Kamusal Alandaki Uygulamalar:

- Her türlü başvurular (Sınavlar, Pasaport vb.),
- Kurumlar arası iletişim (Emniyet Müdürlükleri, Nüfus ve Vatandaşlık İşleri Müdürlükleri vb.),
- Sosyal güvenlik uygulamaları,
- Sağlık uygulamaları (Sağlık personeli, hastaneler, eczaneler),
- Vergi ödemeleri,
- Elektronik oy verme işlemleri.

Ticari Alandaki Uygulamalar:

- İnternet bankacılığı,
- Sigortacılık işlemleri,
- Kâğıtsız ofisler,
- E-Sözleşmeler,
- E-Sipariş

3.1.8. Elektronik imza ve güvenlik

Güvenlik hayatın her noktasında büyük önem arz etmektedir. E-imza'nın hukuki sonuçları itibariyle ıslak imzaya eşdeğer olarak kabul edilmesi, E-imza güvenliğinin önemini artırmıştır. Elektronik imzada, güvenliğin temel prensipleri, elektronik ortamda

saklanan ve iletilen bilgilerin güvenilir olması için verinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması yanında, üretici / göndericinin kimliğinin doğrulanması olarak tanımlanabilir. Bu kapsamda elektronik ortamda üretilen, saklanan ve iletilen bilgilerin güvenilir olması için güvenlik özelliklerini sağlayacak şekilde saklanması ve iletilmesi gereklidir. Levi (2004)'ye göre elektronik ortamda servis ve protokollerin sağladığı kolaylıkları yanında; sahtecilik, aldatma, mesaj başlığını/içeriğini değiştirme, yeniden oluşturma gibi yöntemler kullanılarak ve farklı kaynaktan, farklı içerikli mesaj gönderilerek alıcı ve göndericinin yanıltılması mümkün olabilmektedir.

Canbek ve Sağıroğlu'a göre (2005,2007) e-imza özetleme fonksiyonları veya açık anahtar altyapısı gibi, günümüz bilgi işlem güç ve kapasitesi ile çözülmesi veya kırılması neredeyse imkânsız olan şifreleme algoritmaları kullanılmaktadır. E-imza; şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan, kaba kuvvet, sözlük, ortadaki adam, salt şifreli metin, bilinen düz metin, seçilen düz metin veya şifreli metin saldırıları gibi kriptoanaliz yöntemlerinin kullanıldığı kriptografik saldırılara karşı son derece etkin bir korunma sağlayabilmektedir.

3.1.8.1. Zaman damgası

Zaman Damgası E-imza Kanunu'nun 3.maddesinde "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt" olarak tanımlanmaktadır. Zaman damgası elektronik ortamda doküman ve sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için kullanılır.

Elektronik ortamdaki işlemlere güvenilir zaman bilgisi eklenebilmesini sağlayan zaman damgası, üzerinde zaman bilgisi olması gereken elektronik başvuru, tutanak, sözleşme ve benzeri her türlü elektronik veri üzerinde kullanılabilir.

TÜBİTAK UEKAE (2007), Kamu Sertifikasyon Merkezi'ne göre, Zaman Damgası, elektronik kayıtların veya belgelerin zamanının tespiti için eşsiz bir olanak sağlamaktadır. Bir elektronik imzanın atıldığı zamanın tam olarak belirlenmesine ve e-imzalı elektronik verilerin arşiv amaçlı olarak uzun dönemli saklanabilmesine olanak sağlayan bu teknoloji, günümüz uygulamalarında giderek daha çok önem kazanmaktadır. Zaman Damgaları belli bir verinin belirtilen bir tarihte var olduğunu

kanıtlarlar. Zaman Damgası Sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar.

Bir sözleşmenin imzalandığı, paranın transfer edildiği, başvurunun yapıldığı vs. tarih ve saati kanıtlama ihtiyacı günümüz e-ticaret, e-devlet uygulamaları için hayati önem taşımaktadır. Bununla birlikte yeni bir çizim, tasarım, fotoğraf, düşünce, araştırma, formül, algoritma, kitap gibi fikri ve mülki kullanım hakkı elde edilmek istenen her türlü elektronik veri için zaman damgası alınabilir.

3.2. KÜRESEL YER BELİRLEME SİSTEMİ

3.2.1. Küresel yer belirleme sistemi nedir?

Küresel Yer Belirleme Sistemi (GPS, Global Positioning System), dünyanın herhangi bir yerinde bulunan bir kullanıcının, uydular aracılığıyla kendi konumunu belirlemesine yarayan bir sistemdir. Bu sistem konum belirlemede düzenli olarak kodlanmış bilgiler yollayan bir uydu ağını kullanır. Bu ağ teknolojisi, uydular arasındaki mesafeyi ölçerek Dünya üzerindeki kesin yeri tespit etmeyi mümkün kılar.

İşeri'ye göre (2006) GPS sistemi ilk uydunun 1978'de ateşlenmesiyle başlamıştır. 24 uyduluk Ağustos 1994'de tamamlanmıştır. Projenin devamlılığı ve geliştirilmesi ile ilgili bütçe ABD Savunma Bakanlığı'na aittir. Bu sistem öncelikle harekâtlarda yönün bulunması, askeri çıkartmalarda ve roket atışlarında kullanma gibi askeri amaçlar hedeflenerek kurulmuştur. Sistem 1980'lerde sivil kullanıma açılmış ve hayati önem taşıyan bir araç olarak önemini daha da artırmıştır.

Enge'ye göre (2003) GPS sistemi, günümüzde askeri, sivil ve bilimsel alanlarda konum belirleme ve izleme fonksiyonlarını sağlamak için kullanılan uydu tabanlı 3 boyutlu navigasyon sistemi olarak da tanımlanabilir. Çoğunluğu sivillerden oluşan 20 milyon kullanıcısı vardır.

Misra ve Enge'ye göre (2001) GPS ile konum belirleme ve navigasyon hizmetleri iki farklı seviyede sunulmaktadır. Bunlar; Duyarlı Konum Belirleme Hizmeti (PPS, Precise Positioning Service) ve Standart Konum Belirleme Hizmeti (SPS, Standart Positioning Service)'dir. PPS, yüksek doğruluklu konum, hız ve zaman belirleme hizmeti olup yalnızca ABD Savunma Bakanlığı tarafından yetkilendirilmiş kullanıcılara açıktır. SPS ise PPS'e göre daha düşük doğruluklu konum, hız ve zaman belirleme hizmeti olup sivil, asker tüm kullanıcılara açıktır. ABD Savunma Bakanlığı

tarafından geliştirilen GPS, uydu sinyalleri yardımıyla, herhangi bir yer ve zamanda, her türlü hava koşullarında global bir koordinat sisteminde, yüksek duyarlılıkta, ekonomik olarak, anında ve sürekli konum, hız ve zaman bilgilerini belirlemeye olanak verir.

Ersoy'a göre (1997) uydu teknikleri ile konum belirleme yöntemlerinden GPS, uydulardan yayınlanan radyo sinyaller yardımıyla noktalar arası görüş olmaksızın her türlü hava koşullarında, gece-gündüz, süratli, doğru ve ekonomik olarak üç boyutta konum belirleme sistemidir. Sistemin amacı; yörüngeleri bilinen uydulardan eş zamanlı olarak gönderilen sinyaller yardımıyla noktaların konumlarını mutlak olarak belirleyebildiği gibi, bağıl uzaklıkların ölçülmesi ile noktaların konumları duyarlı bir şekilde belirlemektir.

3.2.2. GPS nasıl çalışır?

"NAVSTAR/GPS" (Navigation Satellite Timing And Ranging/Global Positioning System) uydu tabanlı radyo navigasyon sistemidir. Bu sistemin temelinde 20,200 Km yükseklikteki yörüngede bulunan ve sürekli olarak zaman ve kendi pozisyon bilgisini gönderen 24 adet "Navstar" GPS uydusu vardır. Bir GPS alıcısı ise en az 3, en çok 12 adet uyduyu izleyerek kendi pozisyonunu belirler, ayrıca alıcının hangi hızda hareket ettiği ve hangi yöne gittiği bilgisini üretir (Kahveci ve Yıldız, 2005).

3.2.2.1. GPS sinyali özellikleri

Leick'e göre (2004) GPS ölçmelerinde, elektromanyetik dalgalar kullanılarak uydulardan kullanıcılara veri akışı sağlanmaktadır. Her GPS uydusu konum belirleme amaçlı olarak L1(Link1) ve L2(Link2) olmak üzere iki temel frekansa sahiptir. L1 ve L2 frekansları 10.23 MHz olan temel frekansın 154 ve 120 tam katları alınarak elde edilmiş olup L1 frekansı 1575.42 Mhz ve L2 frekansı 1227.60 Mhz'dir. GPS sisteminin tasarımı aşamasında birçok taşıyıcı frekans incelenmiştir. İnceleme sonucunda, frekans tahsisindeki kolaylıklar ve iyonosferik etkilerin diğer bantlara göre çok daha küçük olması nedeniyle L-bandı kullanımı tercih edilmiştir.

Özenç 2003'te GPS sisteminde çift frekans olmasının amaçları; L1 frekansının herhangi bir nedenle kesilmesi ya da elektronik karıştırmaya maruz kalması durumunda L2 frekansının yedek frekans görevi görmesi ve çift frekans özelliğinden yararlanarak iyonosferik düzeltme olanağı sağlaması olarak sıralanabilir demiştir.

Derelioğlu'na (2007) göre GPS alıcısı kendi yerini belirleyebilmek için uydudan aldığı sinyalleri üçgenleme (triangulation) yöntemiyle çözer. GPS uyduları dünyaya göre kendi yerlerini bilirler ve alıcılarda kendilerinin bir uyduya olan mesafelerini onlardan aldıkları radyo sinyalinin yolculuk süresinden hesaplarlar. En az 3 uyduya olan uzaklığının hesaplanması sonucu, bir GPS alıcısı kendi koordinatını üçgenleme yöntemiyle hesaplar. 4.uydu ile yükseklik bilgisi alınmış olur. 5.uydu ile de diğer uyduların nerelerde olduğu, dolayısıyla ölçüm yapılan uydulardan biri coğrafi yapının zorluğundan veya yörüngesinden dolayı görme sınırları dışına çıktığında kullanılacak olan uydunun pozisyon bilgisini üretir. GPS uydularının üzerinde 4 adet atomik saat mevcuttur. Ayrıca her bir uyduda diğer bütün uyduların anlık ve muhtemel bulundukları yerlerin pozisyon bilgilerinin bulunduğu bir veritabanı bulunur ve bu veri kütüğü sık sık yeryüzü istasyonlarından gelen bilgilerle güncellenirler.

Derelioğlu (2007) çalışmasında kullanıcıda bulunan GPS alıcısı, herhangi bir anda dünya çevresinde kendi yörüngelerinde bulunan 24 uydudan en az 4 tanesinin sürekli yaydığı sinyalleri alarak, sinyalin varış zamanına dayanan mesafe kestirimi yaptığını söylemiştir. Bu mesafe kestirimi sözde mesafe (pseudorange) olarak adlandırılır, çünkü alınan GPS işaretinde hatalar mevcuttur. Günümüzde kullanılan konum belirleme yöntemi, nonlineer sözde mesafe denklemlerini lineerleştirir ve önceden tanımlı başlangıç konum noktasından yararlanarak, iteratif yolla kullanıcı konumunu belirlemeye çalışır. GPS sistemi ile alıcının konumunu belirleme işlemi, 4 bilinmeyenli bir denklemi çözmektir. Bu bilinmeyenler, kartezyen konum koordinatları x, y, z ve GPS saat hatasıdır. Bu çözüme ulaşmak için kullanıcı en az 4 tane uydunun görüşünde olmalıdır.

3.2.2.2. Uyduların konumunun önemi

GPS alıcısı yerini belirlemek için, öncelikle uyduların kesin yerini bilmelidir ve onlara ne kadar uzaklıkta olduğunu bulmalıdır. İşeri'ye (2006) göre alıcı uydudan iki çeşit bilgi alır. Bunlardan birisi, uyduların konumlarını bildiren "almanac data – almanak bilgisi " dır. Almanak bilgisi sürekli olarak yollanır ve GPS' in hafızasında saklanır. Bu sayede GPS her uydunun yörüngesini bilir ve olması gereken konumu hesaplar. Uydular konum değiştirdikçe almanak bilgisi yenilenir.

Uydu yörüngelerinde ufak sapmalar meydana gelebilir. Bu sapmaların hesaplanması için kontrol bölümü uyduların yörünge bilgilerini sürekli olarak izler.

Elde edilen bu hata verileri ana kontrol merkezine ulaştırılır ve düzeltilerek buradan uydulara geri gönderilir. Bu düzeltilmiş kesin konum bilgilerine Ephemeris Data(Geçici Bilgi) adı verilir. Bu bilgiler güncelliğini 4 ila 6 saat arasında korur. Ephemeris bilgisi daha sonra kodlanarak GPS alıcısına gönderilir. Almanak ve Ephemeris bilgilerini alan GPS alıcısı, uyduların kesin konumlarını sürekli olarak belirler.

3.2.2.3. Zamanlamanın önemi

İşeri'ye göre (2006) GPS alıcısının uyduların kesin konumlarını bilmesinin yanı sıra uydulara olan uzaklığını da bilmesi gerekir. Bu sayede, dünya üzerindeki yerini hesaplayabilir. Bunun için basit bir formül kullanılır. Uyduya olana uzaklık; gönderilen sinyalin geliş süresiyle, hızının çarpımına eşittir.

(Geliş Süresi x Hız = Mesafe)

Uzaklığı belirlemek için kullanılan bu formülde, hızı zaten bilmekteyiz. Radyo dalgasının hızı, atmosferdeki ufak etkiler sayılmazsa, Işık Hızına eşittir. (c = 300.000 km/sn)

Bundan sonra, formülün zaman kısmının hesaplanması gerekir. Çözüm uydulardan gelen kodlanmış sinyallerin içinde saklıdır. Gönderilen koda Pseudo-Random Kod adı verilir. Böyle adlandırılmasının sebebi, çok düzensiz bir sinyal olmasıdır. GPS alıcısı da aynı kodu üreterek, uydudan gelen kodla eşleştirmeye çalışır. Bu iki kodu karşılaştırarak aradaki gecikmeyi tespit eder, bu gecikme miktarı ile ışık hızının çarpımı mesafeyi verir.

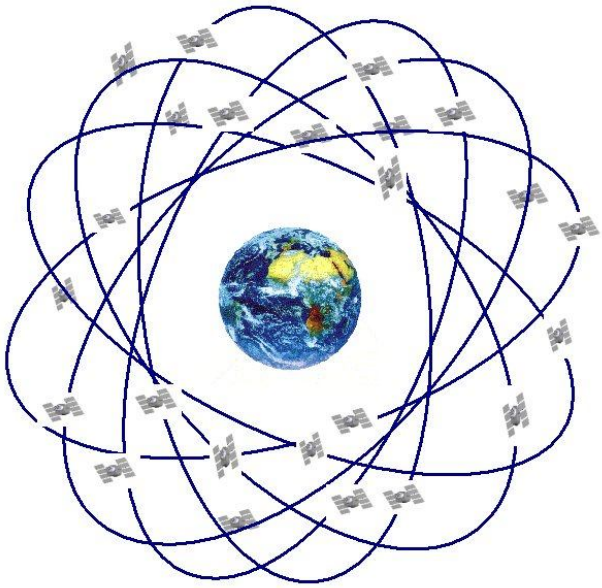
Yaklaşık olarak bir uydudan sinyalin dünyaya ulaşma süresi 0,06 saniyedir. Saniyenin binde birinde oluşacak bir hata, mesafe ölçümünde 300 km' lik bir kaymaya sebep olacaktır. GPS alıcısının saati, uydudaki saatler kadar hassas değildir. Alıcıya bir Atom Saati koymak ise çok pahalı ve çok hantal olurdu. Bu yüzden, uyduya olan mesafe ölçümü, Pseudo Range olarak adlandırılır. Bu bilgiyi kullanarak pozisyon belirlemek için, 4 uydu kullanılarak saat hatasını minimuma indirinceye kadar ölçüm yapılır.

3.2.3. GPS'in bölümleri

Topatan'a göre (2008) GPS sistemi 3 ana kısımdan oluşur. Bunlar uzay bölümü, yerkürede kontrol birimi (kontrol bölümü) ve alıcı kısmıdır (kullanıcı bölümü). Uzay bölümü 24 uydudan oluşur. Uydular, sıfır noktası Dünya'nın merkezi olmak üzere toplam 6 yörünge düzlemine yerleştirilmiştir. Her bir yörünge düzleminde 4 uydu bulunmaktadır. Uydu ile Dünya merkezi arasındaki mesafe yaklaşık 26,600 km'dir.

3.2.3.1. Uzay bölümü

GPS uyduları yer yüzeyinden yaklaşık 20200 km. yükseklikte, 6 orbital yüzeyinde, her yüzeyde 4 uydu olmak üzere, 24 tanedir. Yörüngeleri dairesel şekilde ekvator civarında birbirlerine eşit mesafede ve yine birbirlerine 60° lik açı ile yerleşirler. Bu şekilde, tüm dünyanın her anda 4 ile 8 arasında uydu ile kapsama altına alınması sağlanır. GPS uyduları, radyo alıcı-vericileri, atomik saatler, bilgisayarlar ve sistemi işletmek için çesitli yardımcı ekipmanlar bulundururlar. Her uydu uzaydaki konumunu içeren mesaj yayınlar ve bundan faydalanarak kullanıcılar kendi konumunu belirleyebilirler (Hofmann ve ark., 2001).



Şekil 3.2.3.1. Uzay Bölümü (Gps Navigation System, 2010)

3.2.3.2. Kontrol bölümü

Wells ve ark. (1987) göre Kontrol Bölümü, GPS uydularını sürekli izleyerek, doğru yörünge ve zaman bilgilerini sağlar. Dünya üzerinde 5 adet kontrol istasyonu

bulunmaktadır. Bunlardan dördü insansız, biri insanlı ana kontrol merkezidir. İnsansız kontrol merkezleri, topladıkları bilgileri ana merkeze yollarlar. Ana merkezde bu bilgiler değerlendirilerek gerekli düzeltmeler uydulara bildirilir. Uydular zamanla bozucu etkilere maruz kalmaktadırlar. Yani çok azda olsa yörüngelerinden sapmaktadırlar. Bu uydular kontrol bölümü tarafından gerekli manevralar ile tekrar yörüngelerine oturtulurlar. Bu işlem için gerekli enerji uyduların güneş panelleri aracılığıyla güneş enerjisinden sağlanmaktadırlar.

Misra ve Enge'ye göre (2003) kontrol bölümü, ana kontrol istasyonu ile yer antenleri ve izleme istasyonlarını içeren OCS (Operating Control System)'den oluşmaktadır. Dünya üzerinde uygun dağıtılmış 5 sabit izleme istasyonundan GPS uyduları sürekli izlenmektedir. Bu istasyonlardan Colorado Springs ana kontrol istasyonu, Hawaii, Ascension Island, Diego Garcia ve Kwajalein ise izleme istasyonlarıdır.

3.2.3.3. Kullanıcı bölümü

Kullanıcı bölümü yeryüzünde elinde GPS alıcısına sahip herkesi ifade etmektedir. Çeşitli amaçlarla GPS kullanarak yerini belirlemek isteyen herhangi bir kişi, sistemin kullanıcı bölümünde kabul edilir.

3.2.4. GPS kullanım alanları

Wells 1986'da, GPS gibi uzayda konum belirleme sistemlerinin en önemli ve benzersiz özelliklerinden biri, konum belirlemede kullanılan sinyallerin, dünyanın herhangi bir yerindeki kullanıcılar tarafından her an kullanılabilir olmasından dolayı sistem tam olarak kullanıldığında, geniş bir kullanıcı kitlesine hizmet verecektir, demişti. Günümüzde bunun gerçekleşmeye başladığı görülmektedir.

Yeryüzünün şekil, gravite alanı jeodezi bilimi tarafından belirlenir. Zamana bağlı olarak okyanus hareketleri, Ay ve güneşin etkisi, tektonik hareketler gibi kuvvetlerden dolayı yeryüzünün şekli ve gravite alanı değişime uğramaktadır Chen'e göre (1991) bu hareketler GPS yardımıyla üç boyutlu olarak ölçülebilmektedir.

GPS' in diğer klasik ölçme teknikleri ile karşılaştırıldığında üstün tarafları şu şekilde sıralanabilir (Tuşat, 2003);

- Noktalar arası görüş zorunluluğu ortadan kalkmıştır. GPS alıcı anteninin uydu sinyalini izleyebilmesi için gökyüzünü görmesi yeterlidir.
- Nokta yeri seçiminde noktaların en yüksek yerlerde olması gibi zorunluluklar ortadan kalkmıştır. Gereksinim duyulan ve GPS ölçüsünün yapılmasına olanak veren her yerde nokta tesisi yapılabilmektedir.
- GPS ölçülerinin yapılması büyük oranda hava şartlarından bağımsızdır.
- Gece gündüz sürekli ölçüm yapılabilmektedir.
- GPS ölçülerinin yapılışındaki hız ve aletlerin kullanım kolaylığı, ölçü hatalarının az olması (anten yüksekliği ölçümü hariç) nedenleriyle ekonomik bir sistemdir.
- Üç boyutlu nokta koordinatları elde edilmektedir.
- Elde edilen jeodezik doğruluklar en duyarlı klasik jeodezik tekniklerle elde edilenlerle eşit ya da daha iyidir.

3.2.4.1. Sivil kullanım alanları

Kahveci ve Yıldız'a göre (2005) GPS konum belirleme uygulamalarının, sivil amaçlı kullanım alanlarını sıralayacak olursak;

- Kara, deniz ve hava araçlarının navigasyonu
- Jeodezik ve jeodinamik amaçlı ölçümler
- Kadastral ölçümler
- Kinematik GPS destekli fotogrametrik çalışmalar
- Yerel ve global deformasyon ölçmeleri
- Araç takip sistemi
- Uçakların, görüşün sınırlı ya da hiç olmadığı hava koşullarında iniş ve kalkışı
- Aktif kontrol ağları
- CBS veri tabanlarının geliştirilmesi
- Turizm, tarım, ormancılık, spor
- Asayiş
- Hidrografik ölçmeler

3.2.4.2. Askeri kullanım alanları

Kahveci ve Yıldız'a göre (2005) GPS konum belirleme uygulamalarının, askeri amaçlı kullanım alanlarını sıralayacak olursak;

- Kara, deniz ve hava araçlarının navigasyonu
- Arama-Kurtarma
- Hedef bulma
- Füze güdümü
- INS sistemlerinin desteği
- Uçakların, görüşün sınırlı ya da hiç olmadığı hava koşullarında iniş ve kalkışı

3.3. KONUM DAMGASI SİSTEMİ ÖNERİSİ

3.3.1. Konum damgası sistemi önerisi

Konum Damgası Sistemi önerisi, küresel yer belirleme sisteminden yararlanarak elektronik imza işlemin gerçekleştiği konum bilgilerinin belgeye eklenip doğrulanabilmesini ve belgenin gönderildiği konumun sınırlandırılabilmesini esas almaktadır.

Konum Damgası önerisi elektronik imza güvenliğine ilişkin, işlemin gerçekleştiği konum bilgilerinin de doğrulanmasını öneren Konum damgası önerisi, GPS sisteminden yararlanmayı öngörmektedir.

Konum Damgası Sistemi'nde mevcut elektronik imza atma sisteminde imzalanan veriye ek olarak GPS'in sağladığı koordinat bilgileri de eklenir. Elektronik imza bilgileri doğrulama bilgilerine ek olarak koordinat bilgileri de doğrulanır. Buradaki koordinat doğrulaması, kullanıcının sistem çerçevesine bir web ara yüzünde önceden tanımladığı koordinat bilgilerinin dosyadaki konum bilgileri ile karşılaştırılması işlemidir. Kullanıcı konum doğrulaması gerçekleştirmek istiyorsa, öncelikle ilgili ara yüzden bu özelliği aktif etmeli ve elektronik imzayı hangi koordinat aralığında kullanacağını belirlemelidir. Konum Damgası Sisteminde doğrulama yapılırken buradaki tanımlama esas alınmaktadır.

Kullanıcının konum damgalı elektronik imza kullanımı için Koordinat verileri gerekmektedir. Bu gereksinim, bazı mobil cihazlarla birlikte gelen GPS verileri olabileceği gibi, masaüstü bilgisayarlar için temin edilecek GPS alıcılarıyla da

gerçekleşebilir. Bir kullanıcı gerçekleştireceği imzalama işleminde konum doğrulama özelliğini kullanmak istiyorsa minimum donanım gereksinimlerine ek olarak GPS alıcısına sahip olmalıdır. Bu alıcı, GPS'in yapısı gereği gökyüzünü görecek şekilde konumlanmış olmalı, güvenli veri hatları ile imzalama işleminin gerçekleşeceği ortama bağlı olmalı, veri aktarabilir olmalıdır.

Konum Damgası ile e-imza işleminin nerede gerçekleştiği ispatlanabilir olacaktır. Bu sayede mevcut elektronik imza ya da mobil imzanın çalındığı veya kaybolduğu durumlarda kullanıcı bu durumu fark edene kadar geçen sürede mobil imzanın yetkisiz kullanımı önüne bir de konuma ilişkin doğrulama kriteri geldiğinden güvenlik belli düzeyde artmış olacaktır.

Konum bilgilerini de içeren bir e-imza, mevcut sisteme göre dünyanın her yerinden gerçekleşebilecek bir işlemi kullanıcı kontrolü dâhilinde ve kullanıcı lehine sınırlandırdığından güvenlik artırıcı olarak görülebilir. Ayrıca burada bahsedilen konum bilgisini içeren sistem ekonomik olarak da nitelenebilir, konum bilgileri sağlamada kullanılan GPS verileri, GPS alıcı cihazlara ücretsiz olarak sunulmaktadır.

Tüm bu anlatılanlar aşağıdaki örnekle açıklanmıştır. Örneğin kullanıcı konum damgalı e-imza işleminin işyerinin bulunduğu Kızılay/Ankara'da gerçekleştirmek istiyor. Bu durumda öncelikle imzasının kullanmak istediği bölgeleri sisteme tanıtmış olması gerekmektedir (İş, ev, tatil bölgesi vb.).

Varsayalım ki işyerinin küresel koordinatları 39°55'13.88" kuzey paraleli ve 32°51'16.43" doğu meridyeninin kesişim noktasındadır (Şekil 3.3.1.1.). Kullanıcı bu durumda GPS alıcı cihazının ileteceği konum bilgisinde meydana gelecek sapmaları da dikkate alarak işyerini de içerisine alan bir koordinat aralığı belirlemek ve bunu sisteme tanıtmak durumundadır. Burada belirlenecek koordinat aralığı kullanıcı tarafından tanımlanabileceği gibi, harita üzerinde seçilen bir nokta için metre cinsinden bir aralığın belirlenmesi ile de sağlanabilir.

Şekil 3.3.1.1. 39°55'13.88" kuzey paraleli ve 32°51'16.43" doğu meridyenindeki işyeri

Şimdi de Kullanıcının, e-imza kullanımı için koordinat aralığını 39°55'03.00" - 39°55'22.00" kuzey paralelleri ile 32°51'01.00" - 32°51'30.00" doğu meridyenleri olarak seçtiğini, bu koordinat bilgilerini konum damgalı e-imza işlemlerinde kullanmak üzere kullanıcı ara yüzünde kaydettiğini ve e-imza işlemlerinde konum damgası özelliğini aktive ettiğini varsayalım. Bu aşamadan itibaren elektronik olarak imzalanan dokümanlara GPS alıcısından gelen koordinat bilgileri de eklenir. E-imza doğrulama sırasında, imzalanan belge içerisinde iletilen bu koordinat bilgileri, kullanıcının daha önceden tanımlamış olduğu aralıklardan birinde ise konum onaylanmış, konum doğrulaması yapılmış demektir (Şekil 3.3.1.2.).

Şekil 3.3.1.2. İşyerinin çevresinde 250 metre yarıçapındaki dairenin kullanılabilecek konum alanı

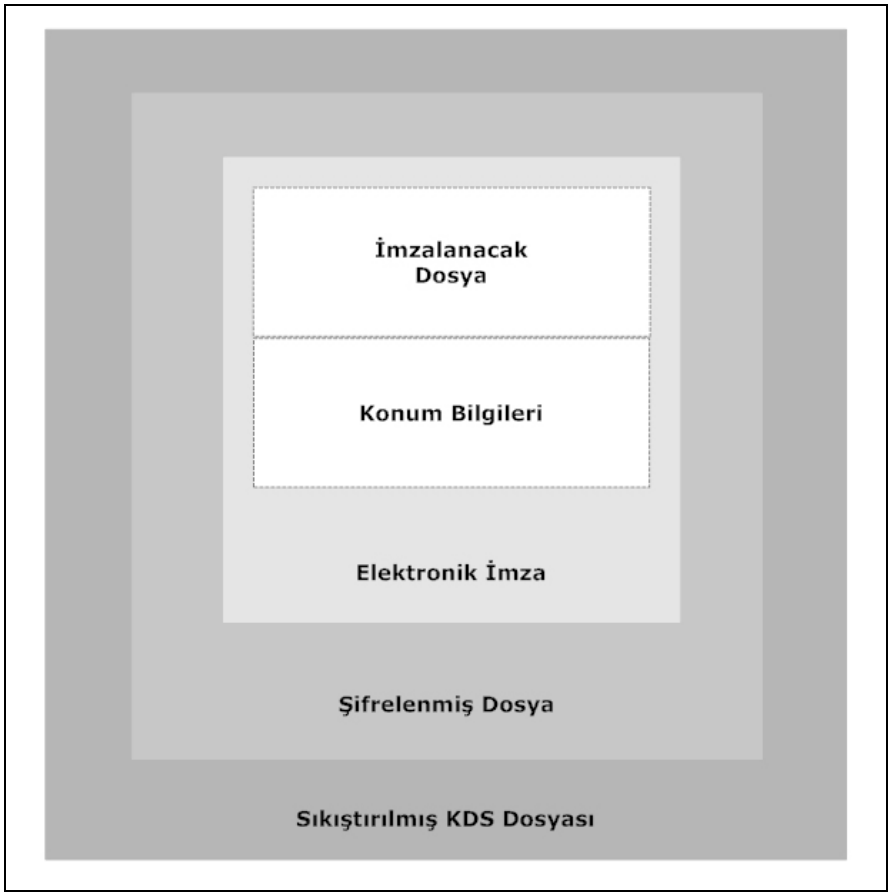
3.3.1.1. KDS dosyası ve yapısı

Konum Damgası önerisi çerçevesinde imzalanmış ve doğrulanacak olan dosyalar "Konum Damgası Sistemi" nin ilk harflarinden oluşan KDS uzantısını alırlar.

E-imza bilgilerine ek olarak konum bilgilerini de içeren bu yeni tip .kds uzantılı dosya KDS uygulamasınca oluşturulabilir ve doğrulanabilir. Bu dosya temel olarak aşağıdaki bilgi ve işlemlerden oluşur:

- İmzalanacak metin belgesi,
- Konum bilgilerinin şifrelenerek eklenmesi işlemi
- Elektronik İmzalama işlemi,
- Dosyayı kriptografik algoritmayla şifrelenmesi işlemi,
- Dosyayı sıkıştırma işlemi

Dosyanın yapısı Şekil 3.3.1.3.'te gösterilmiştir.



Şekil 3.3.1.3. KDS uzantılı KDS Dosyasının Yapısı

3.3.1.2. Haversin formülü

Dünyanın geoid şeklinden ötürü iki koordinat arası ölçüm sağlıklı olarak ölçülememektedir. Haversin dünyanın geoid şeklini de hesaba katacak şekilde yeni bir ölçüm formülü geliştirmiştir. Küresel üçgenin açılarını ve kenar uzunluklarını çözmek için çeşitli teoremler kullanılır. Yüksek bir hassasiyet oranına ihtiyaç duymuyorsanız ve hesaplamanın hızlı olması sizin için önemli ise Haversine formülünü kullanılabilir. Haversine formülü küresel trigonometrideki genel bir formülün özel bir durumudur (Özcan, 2010). KDS uygulaması hesaplamalarında bu formülü java koduna dönüştürerek uygulamıştır.

Haversin formülü Tablo 3.3.1.2.1'de gösterilmiştir.

Tablo 3.3.1.2. Haversin Formülü

R = earth's radius (mean radius = 6,371km)

Δ lat = lat2− lat1

Δ long = long2− long1

$a = \sin^2(\Delta lat/2) + \cos(lat1).\cos(lat2).\sin^2(\Delta long/2)$

$c = 2.\text{atan2}(\sqrt{a}, \sqrt{(1-a)})$

d = R.c

KDS uygulamasında formülün mesafe farkını hesaplayan java metoduna dönüştürülmüş hali Tablo 3.3.1.2.2'de gösterilmiştir.

Tablo 3.3.1.2.2. Haversin formülünden yararlanarak mesafe farkı bulan java metodu

```
public static int yaricapMesafeBul(double lat1, double lng1, double lat2,
                                   double lng2,double yaricap) {
            double earthRadius = 3958.75;
            double dLat = Math.toRadians(lat2 - lat1);
            double dLng = Math.toRadians(lng2 - lng1);
            double a =
               Math.sin(dLat / 2) * Math.sin(dLat / 2) + Math.cos(Math.toRadians(lat1)) *
               Math.cos(Math.toRadians(lat2)) * Math.sin(dLng / 2) *
               Math.sin(dLng / 2);
            double c = 2 * Math.atan2(Math.sqrt(a), Math.sqrt(1 - a));
            double dist = earthRadius * c;
            int meterConversion = 1609;
            int durum = 0;
            double uzaklik = (dist * meterConversion);
            if (uzaklik > yaricap){
               System.out.println("UZAK");
               durum=1;
                    } else   {
                  System.out.println("YAKIN");
                  durum=0;
               } System.out.println("uzaklık :" + uzaklik + "yarı çap :" + yaricap);
            return durum;    }
```

3.4. KONUM DAMGASI SİSTEMİ UYGULAMASI

3.4.1. KDS uygulaması hakkında

KDS Uygulaması, Konum damgası sisteminden yararlanmak isteyen, imzaladığı belgelere konumla ilgili sınırlama getirmek isteyen kullanıcıların kullanımı için özel olarak geliştirilmiş bir uygulamadır. Kullanıcı bu uygulamayı kullanmak için öncelikle elektronik imzası ile KDS sistemine kayıt olur. Kaydolduktan sonra kullanıcı girişi gerçekleştirerek, elektronik imzasının kullanımına izin verdiği konumları tanımlayacak ve bu özelliği aktive edecektir. Bu tanımlama ve aktivasyondan sonra masaüstü uygulaması ile mevcut elektronik imzalama sürecinde belgelere GPS alıcısından sağlanan koordinat bilgileri eklenecektir. Belgeyi alan kişi elektronik imzalanmış ve konum damgası bilgisi eklenmiş belgelerde masaüstü uygulaması ile elektronik imzanın yanı sıra ve belge sahibinin belirtmiş olduğu konum aralığını kontrol eden konum doğrulaması işlemini de gerçekleştirebilecektir.

3.4.2. KDS uygulaması özellikleri ve veritabanı

KDS Uygulamasını geliştirmek için Java Development Kit 6, Oracle JDeveloper Studio 11.1.1.2 geliştirme ortamı, Apache Tomcat web sunucusu ve MySQL veritabanı kullanılmıştır. KDS masaüstü uygulaması Nesneye yönelik programlama kavramına göre Java programlama dilinde kodlanmıştır. Grafik çizimler için SmartDraw kullanılmıştır.

Uygulama yazımı sırasında ihtiyaç duyulan yerlerde (Open Source) açık kaynak kodlu kütüphanelerden istifade edilmiştir. Uygulamanın kullandığı sınıflara EK-C'de sunulmuştur.

KDS Uygulamasının gerçekleşebilmesi için bir takım fiziki teçhizat ve bilgilere gereksinim duyulmuştur. Çalışma sonunda detayları verilecek olan uygulama ile ilgili gereksinimleri iki başlıkta inceleyeceğiz.

Fiziki Gereksinimler

- USB GPS Alıcısı
- Nitelikli Elektronik Sertifika (E-imza)

- 1 Adet Web Sunucusu (Web uygulaması için)
- 1 Adet İnternete Bağlı Bilgisayar (Masaüstü uygulaması için)

Bilgi Gereksinimleri

- E-imza ve GPS API Bilgisi
- Coğrafi Bilgi Sistemi ve Küresel Yer Belirleme Sistemi Bilgileri
- Veri Yapıları Bilgisi
- Belge Tipleri ve Yapılarıyla İlgili Bilgiler
- Şifreleme Algoritmaları Bilgisi
- Nesneye Yönelik ve Web Tabanlı Programlama Bilgisi
- Veritabanı Tasarımı ve Uygulaması Bilgisi

Konum Damgası Sistemi (KDS) uygulamasının veritabanı kds isimli bir mySQL veritabanıdır. Bu veritabanı 4 adet tablodan oluşmaktadır. Bu tablolar, alanları ve açıklamaları aşağıdaki Tablo 3.4.2.1., Tablo 3.4.2.2., Tablo 3.4.2.3. ve Tablo 3.4.2.3.'te gösterilmiştir.

Tablo 3.4.2.1. KDS üyeler tablosu

UyeId	int(11)	KDS Üye numarası
Uyetcno	varchar(200)	Şifrelenmiş Üye TC Kimlik Numarası
Uyekartno	varchar(200)	Şifrelenmiş Üye Kart Seri Numarası
Uyesifre	varchar(200)	Şifrelenmiş Üye KDS Şifresi
Uyeadi	varchar(200)	Üye Adı ve Soyadı
Uyedurum	int(1)	KDS Üyelik Aktiflik / Pasiflik Durumu
UyeIptal	int(1)	KDS Üyelik Sonlandırma Durumu

Tablo 5.2.2. KDS konum tanımları tablosu

Tanid	int(11)	Konum Tanım Numarası
UyeId	int(11)	KDS üye numarası
Konumismi	varchar(200)	Belirlenen Konumun İsmi
Enlemdeger	varchar(200)	Doğrulanacak Enlem Değeri
Boylamdeger	varchar(200)	Doğrulanacak Boylam Değeri
Alan	int(5)	Doğrulanacak Koordinat Aralık Yarıçap Değeri (Metre Cinsinden)
Aktif	int(1)	Tanımın Aktiflik / Pasiflik Durumu
Silindi	int(1)	Tanımın Silinme Durumu

Tablo 5.2.3. KDS hedef tanımları tablosu

Hedefid	int(11)	Hedef Tanım Numarası
UyeId	int(11)	KDS üye numarası
Hedefismi	varchar(200)	Belirlenen Hedefin İsmi
Enlemdeger	varchar(200)	Doğrulanacak Enlem Değeri
Boylamdeger	varchar(200)	Doğrulanacak Boylam Değeri
Alan	int(5)	Doğrulanacak Koordinat Aralık Yarıçap Değeri (Metre Cinsinden)
Aktif	int(1)	Tanımın Aktiflik / Pasiflik Durumu
Silindi	int(1)	Tanımın Silinme Durumu

Tablo 5.2.4. KDS erişimler ve işlemler tablosu

Eid	int(11)	Erişim numarası
Uyekartno	varchar(200)	Şifrelenmiş Üye Kart Seri Numarası
Uyetcno	varchar(200)	Şifrelenmiş TC Numarası
Tarih	Datetime	İşlem Tarihi
Islem	Text	İşlem Açıklaması
Ipadres	varchar(50)	İşlemin Gerçekleştiği IP Adresi

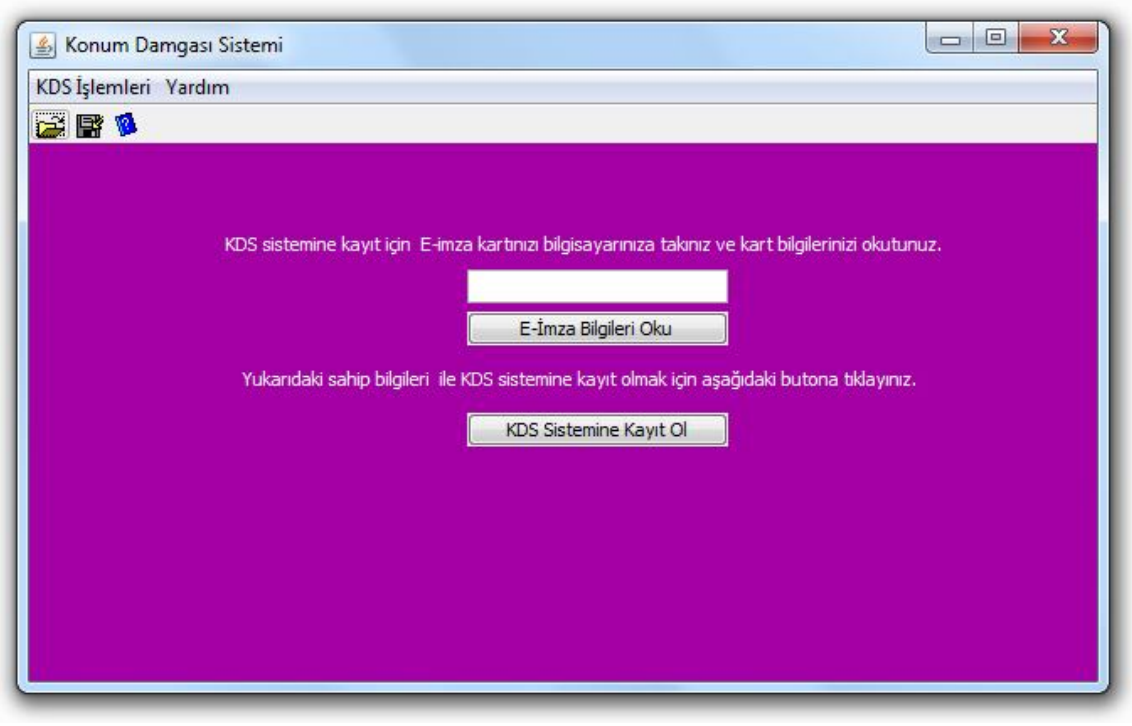
3.4.3. KDS masaüstü uygulaması

KDS sisteminin istemci tarafında çalışan ve kullanıcı kaydı, kullanıcı girişi, konum tanımlama, kullanıcı imzalama, kullanıcı doğrulama, kullanıcı durum aktif/pasif, kullanıma kapatma, kullanıma açma, kullanıcı oturum işlemleri gibi işlemlerin gerçekleştirildiği masaüstü uygulamasıdır.

3.4.3.1. KDS kullanıcı kaydı

KDS uygulamasını kullanıcı kaydı ekranı kullanıcıların e-imza kartları ile KDS sistemine kayıt olmalarını sağlayan ekrandır Şekil (3.4.3.1.). Bu ekranda çalışırken öncelikle e-imza kartı takılmalı ve "E-imza Bilgilerini Oku" butonuna tıklanmalıdır. Ekranda kart kullanıcı ismi görüntülendiğinde "KDS Sistemine Kayıt Ol" tıklanır. Böylelikle kullanıcıya ait kart bilgileri ile KDS web sunucusundaki merkezi veritabanına kullanıcı kaydı gerçekleştirilmiş olur.

Uygulama kullanıcı kaydının ardından KDS sisteminde kullanılmak üzere şifre belirlenmesini ister. Bu aşamada KDS masaüstü ve KDS web uygulamalarında kullanılmak üzere şifre belirlenir ve kaydedilir.

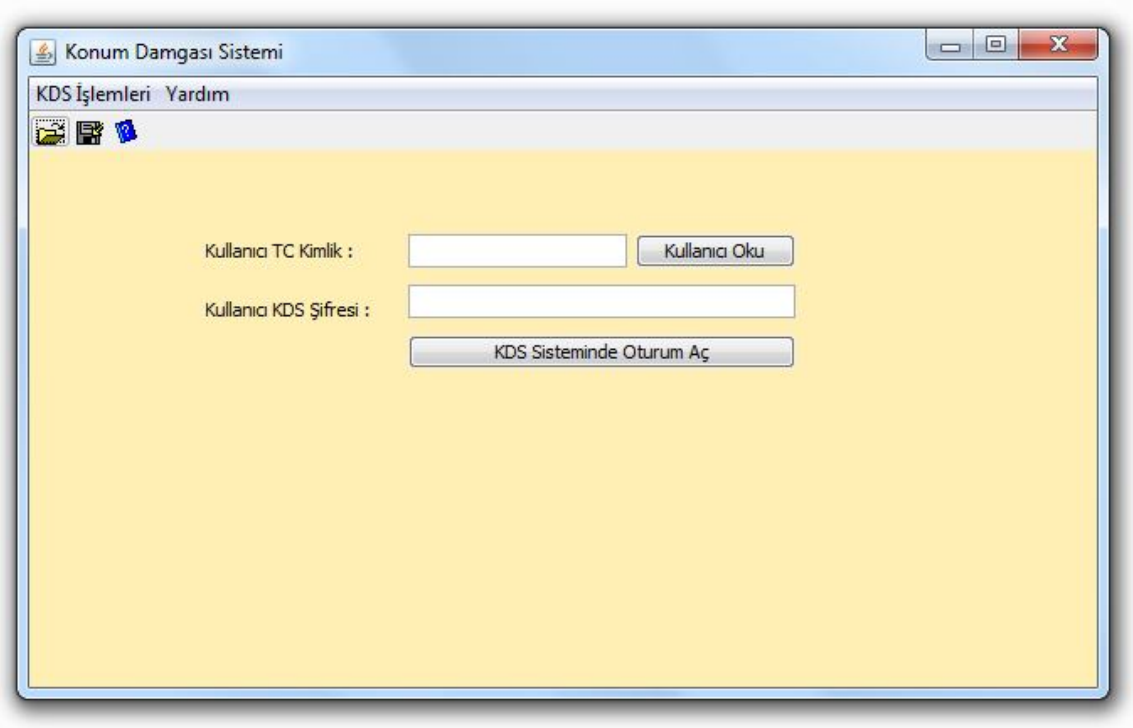


Şekil 3.4.3.1. KDS kullanıcı kayıt ekranı

3.4.3.2. KDS kullanıcı girişi

Konum damgalı elektronik imzalama işlemi gerçekleştirmek için KDS masaüstü uygulamasına kullanıcı girişi yapılması şarttır. Konum damgalı elektronik imza doğrulama için ise KDS kullanıcı giriş işlemine gerek yoktur. Herhangi bir kullanıcı kayıt olmaksızın doğrulama yapabilmektedir.

KDS uygulamasını kullanıcı girişi ekranı kullanıcıların e-imza kartları ile KDS sistemine giriş yapabilmelerini sağlar Şekil (3.4.3.2.). Bu ekranda öncelikle e-imza kartı takılmalı ve "Kullanıcı Oku" butonuna tıklanmalıdır. Ekranda kart kullanıcısının TC kimlik numarası görüntülendiğinde daha önceden belirlenmiş olan KDS kullanıcı şifresi ile sisteme giriş yapar ve imzalama adımına geçebilir.



Şekil 3.4.3.2. KDS kullanıcı girişi ekranı

3.4.3.3. KDS tanımlama

KDS uygulaması elektronik olarak imzalanmış dosya içerisindeki konum bilgilerini doğrulayarak çalışmaktadır. Bu durum kullanıcının kullanım öncesinde KDS sistemini nerelerde kullanacağını daha önceden tanımlamış olmasını gerektirir. Benzer şekilde gönderilecek olan dosyanın açılacağı hedef konumlar da bu ekranda tanımlanır.

KDS uygulaması tanımlama işlemi web sunucusunda çalışacak şekilde Google Map API'den yararlanılarak geliştirilmiştir. Kullanıcı bu ekranda KDS sisteminde kullanmak istediği konumları ve hedefleri tanımlamaktadır Şekil (3.4.3.3.).

Konum Tanımlama İşlem Adımları:

1-Kullanıcı oturumu aç

2-Haritadan konum seç (Enlem ve boylam seçimi)

3-Seçilen konuma isim ver

4-Konum etki alanını belirle

5-Konumu kaydet

6-Oturumu kapat

Hedef Tanımlama İşlem Adımları:

1-Kullanıcı oturumu aç

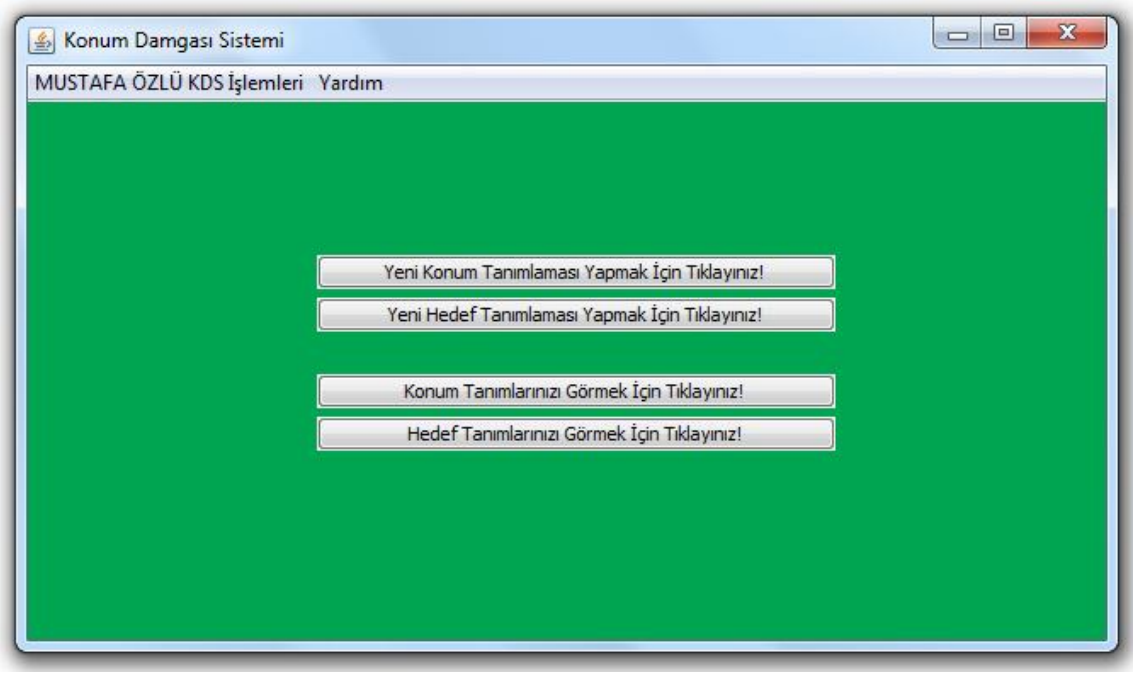
2-Haritadan konum seç (Enlem ve boylam seçimi)

3-Seçilen hedefe isim ver

4-Konum etki alanını belirle

5-Konumu kaydet

6-Oturumu kapat



Şekil 3.4.3.3. KDS kullanıcı konum tanımlama ve görüntüleme bağlantı ekranı

3.4.3.4. KDS kullanıcı imzalama

Konum damgalı elektronik imzalama işlemi gerçekleştirmek için KDS masaüstü uygulamasına kullanıcı girişi yapılması şarttır. İmzalama işlemi kullanıcı imzalama ekranında gerçekleştirilir Şekil (3.4.3.4.).

İmzalama işlemi sırasında imzalanan dosyanın hangi hedeflerde açılabileceğini belirlemek için KDS web sunucusundan kullanıcının önceden belirlemiş olduğu hedef konumlar indirilip seçildikten sonra bu bilgi dosyaya da eklenir.

Konum damgalı elektronik imzalama işlem adımları :

1- İmzalanacak metin dosyasını (.txt uzantılı) seç
2- GPS alıcısından konum bilgilerini al
3- Alınan konum bilgilerini kriptografik algoritmayla şifrele
4- Şifre anahtarını kriptografik algoritmayla şifrele
5- Şifrelenmiş konum bilgilerini ve şifre anahtarını imzalanacak metne ekle
6- KDS web uygulamasından imzalayan kişinin hedef tanım listesini al
7- Hedef listesinden dosyanın açılabileceği hedefleri seç
8- Seçilen hedefleri şifrele ve dosyaya ekle

9- Dosyayı kullanıcı kartı ile elektronik imzala

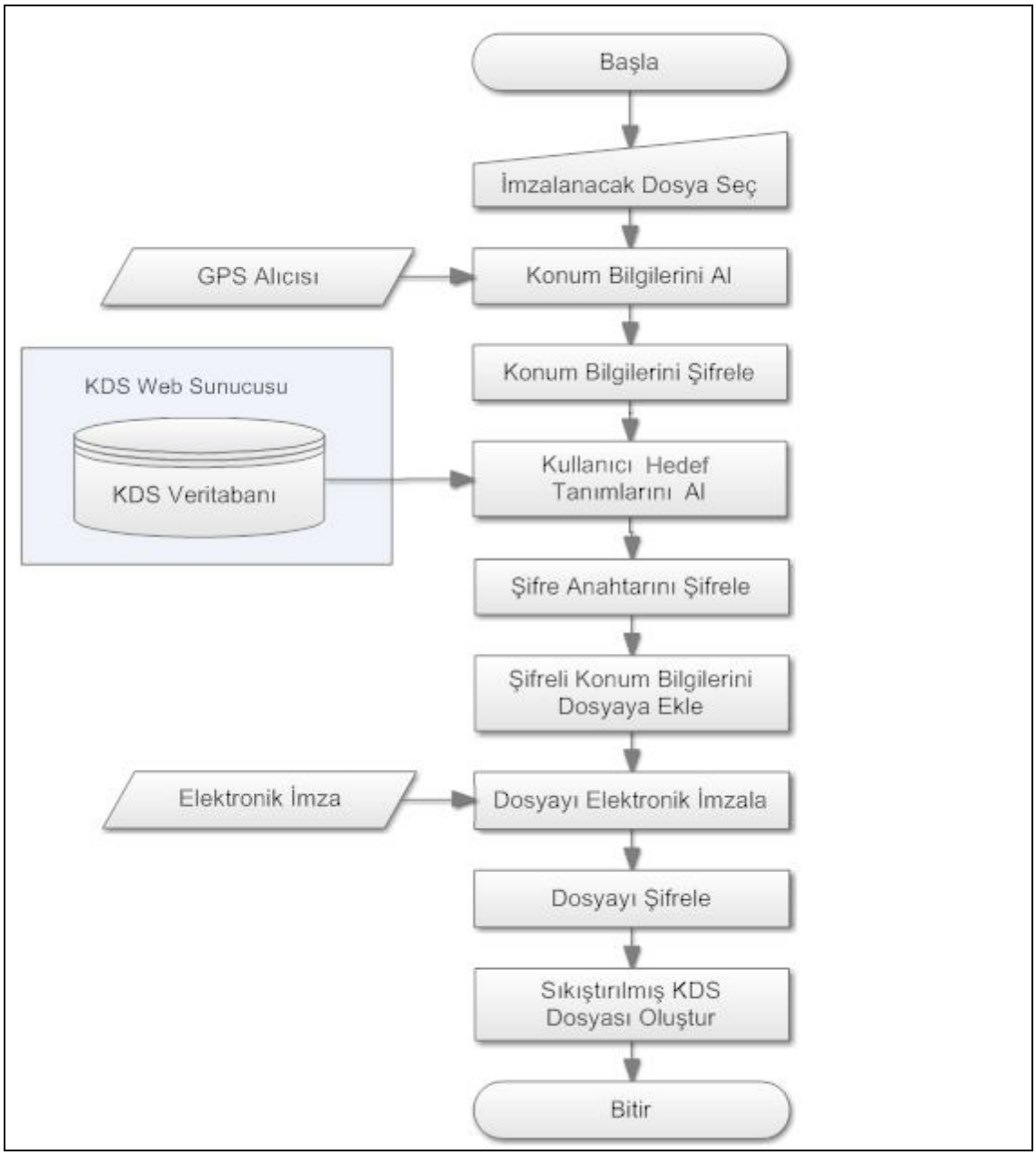
10- Dosyayı kriptografik algoritmayla şifrele

11- Dosyayı sıkıştır

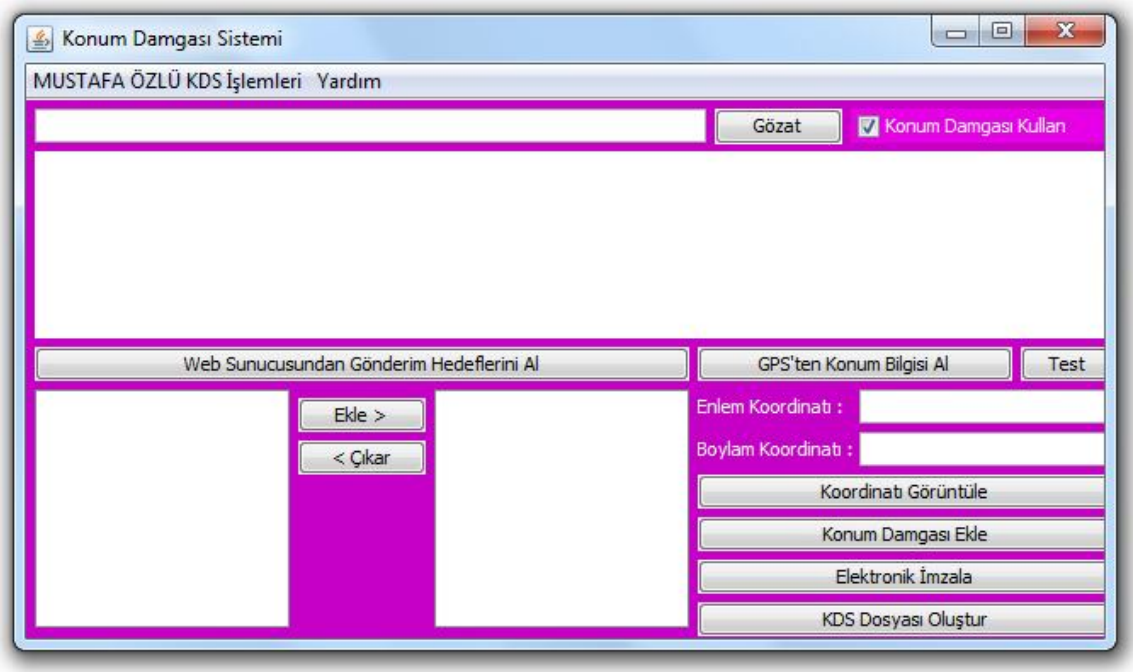
12- Dosyayı KDS uzantılı kaydet

13- Dosya Hazır

Konum damgalı elektronik İmzalama Akış Şeması Şekil 3.4.3.4.1.'de gösterilmiştir.



Şekil 3.4.3.4.1. KDS dosya imzalama işlemi akış şeması



Şekil 3.4.3.4.2. KDS kullanıcı dosya imzalama ekranı

3.4.3.5. KDS dosyası konum damgası doğrulama

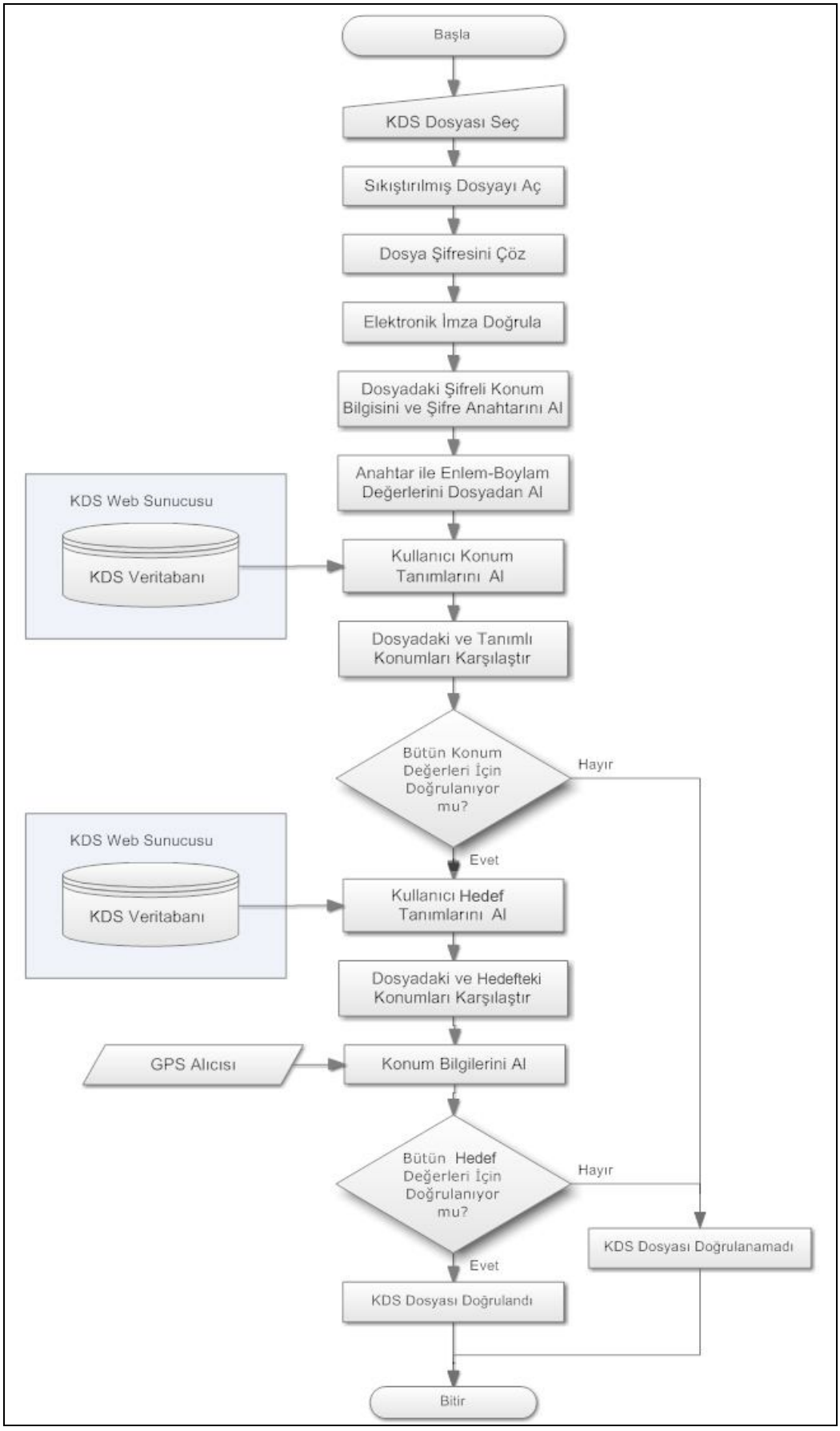
KDS uygulamasında doğrulama işlemi yapılırken kullanıcı girişi yapma şartı yoktur. Kullanıcılar kendilerine gönderilen kds uzantılı dosyayı KDS uygulaması doğrulama ekranı ile doğrulayabilirler Şekil (3.4.3.5.). KDS kullanıcıları konum damgalı elektronik imzalanmış bir dosyanın doğrulanmasını engellemek istediklerinde, kullanım durumlarını pasif ederek doğrulama işleminde sınırlandırma yapabilmektedirler.

Konum damgalı elektronik doğrulama işlem adımları :

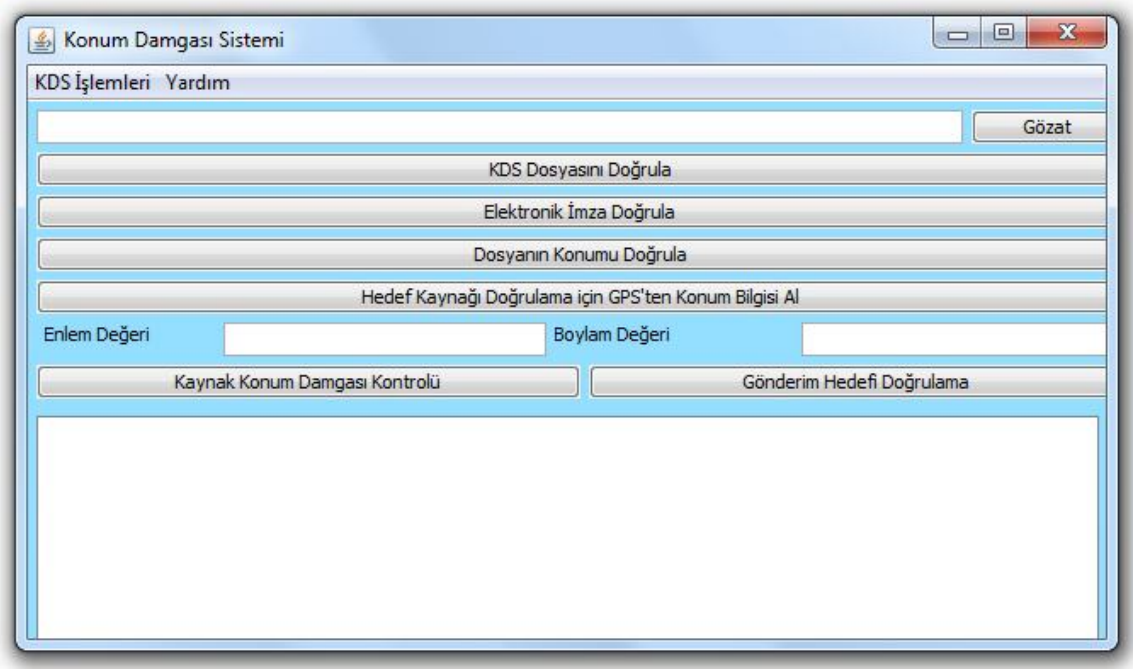
1- Doğrulanacak KDS dosyasını seç
2- KDS dosyasının şifresini çöz
3- Sıkıştırılmış KDS dosyasını aç
4- Dosyayı içerisindeki elektronik imzayı doğrula
5- Dosyayı içerisindeki şifreli konum bilgisini ve şifre anahtarını al
6- Anahtar ile şifreyi çözerek enlem ve boylam değerlerini elde et
7- KDS web uygulamasından imzalayan kişinin konum tanım listesini al
8- Dosyadaki konum değerleriyle tanımlı konumları mesafe yönünden karşılaştır
9- KDS web uygulamasından dosyanın içerisinde tanımlanan hedef tanım listesini al

10- GPS cihazından alınan konum değerleriyle tanımlanmış hedef konumları mesafe yönünden karşılaştır
11- İmzalanan konum ve hedef konum tanımları için sonuç pozitif ise konum damgalı elektronik imzalı dosya doğrulanmış ve işlem başarıyla sonuçlanmış demektir.

Konum damgalı elektronik doğrulama işlemi akış şeması Şekil 3.4.3.5.1. de gösterilmiştir.



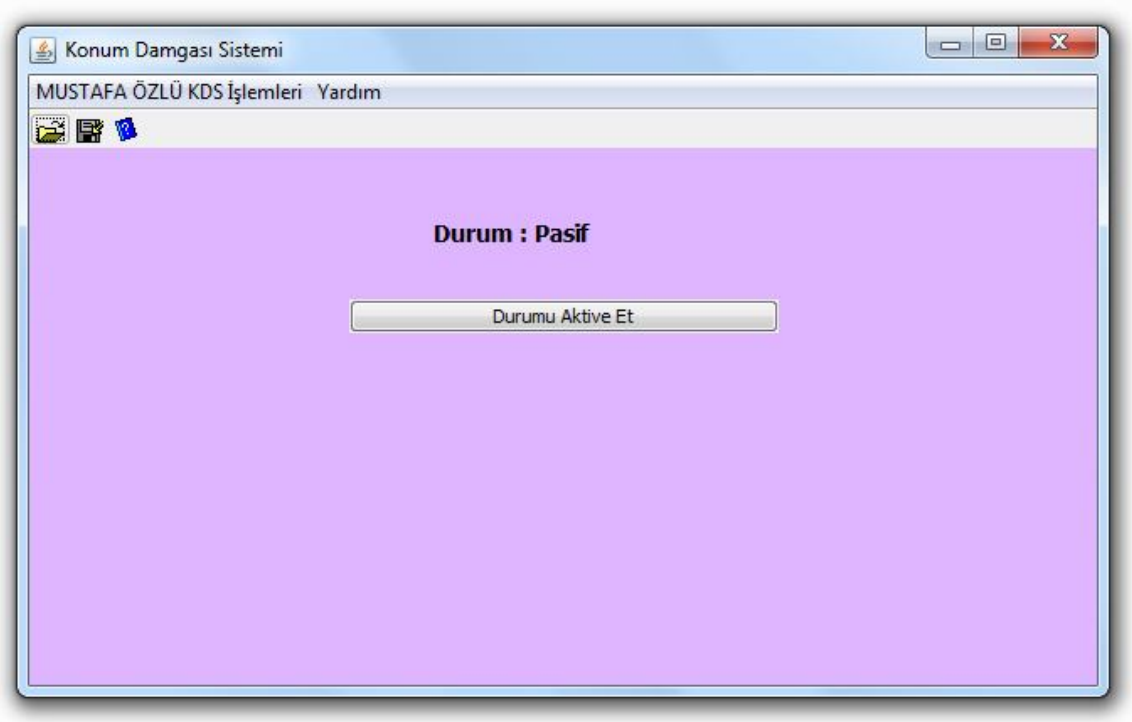
Şekil 3.4.3.5.1. KDS dosyası konum damgası doğrulama işlemi akış şeması



Şekil 3.4.3.5.2. KDS kullanıcı konum damgası doğrulama ekranı

3.4.3.6. KDS kullanıcı durum aktif/pasif

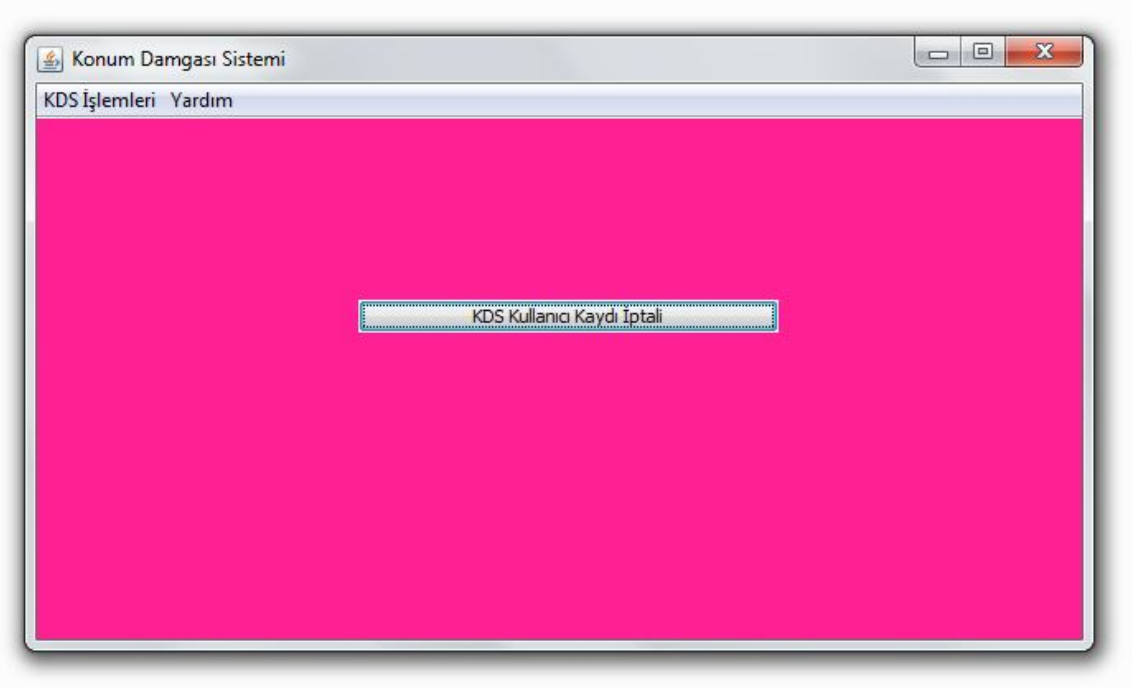
KDS uygulaması kullanıcıları Konum damgalı elektronik imzalama işlemi gerçekleştirmek istemedikleri zamanda kullanım durumlarını aktif ya da pasif ederek kullanıma sınırlandırma yapabilmektedirler. Bu işlem için KDS kullanıcı durum ekranı kullanılmaktadır Şekil (3.4.3.6.).



Şekil 3.4.3.6. KDS kullanıcı durumu bilgi ve güncelleme ekranı

3.4.3.7. KDS kullanıma kapatma

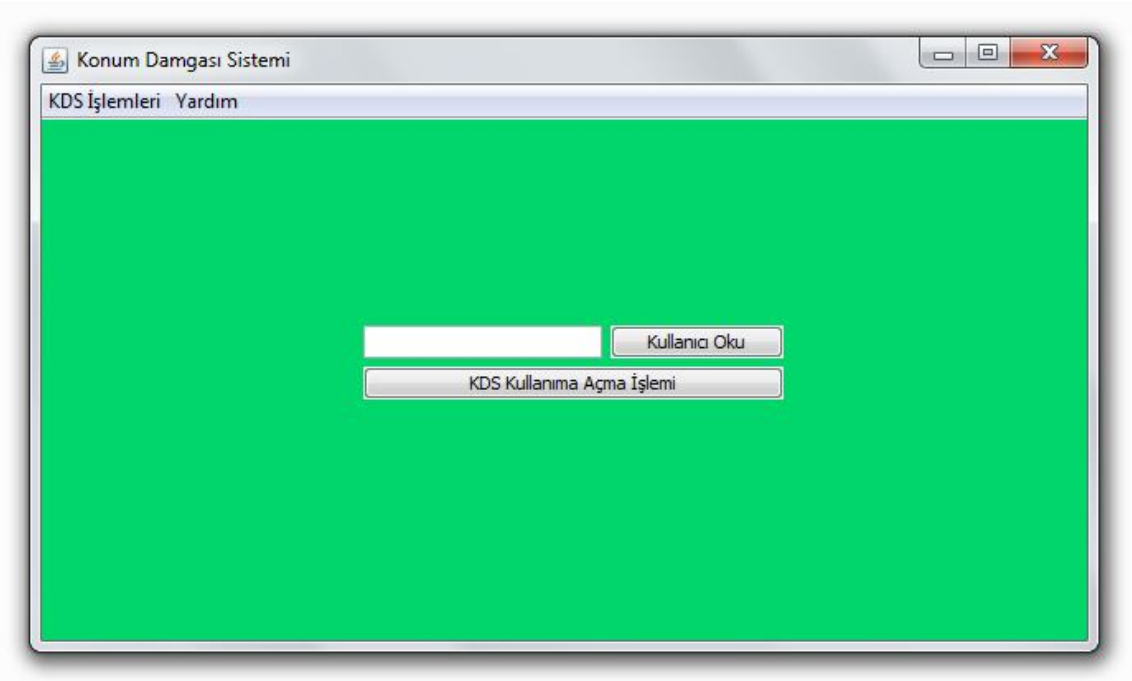
KDS uygulaması kullanıcılarının kullanıcı kayıtlarını iptal etmek için kullandıkları ekrandır Şekil (3.4.3.7.). İptal edilen kullanıcı hesabı tekrar kullanıma açılana kadar kullanılamaz.



Şekil 3.4.3.7. KDS kullanıcı kaydı iptal ekranı

3.4.3.8. KDS kullanıma açma

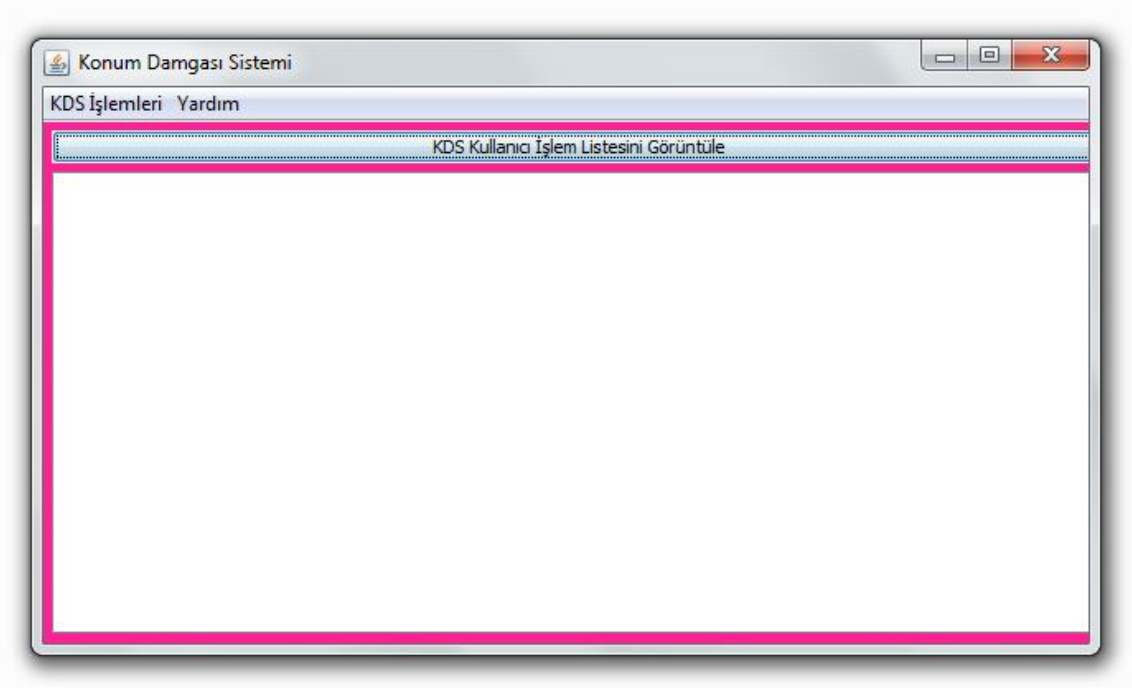
KDS uygulaması kullanıcılarının kullanıcı hesaplarını tekrar devreye almak ve kullanıma açmak için kullandıkları ekrandır Şekil (3.4.3.8.).



Şekil 3.4.3.8. KDS Kullanıma Açma Ekranı

3.4.3.9. KDS kullanıcı işlem listesi

KDS masaüstü uygulamasında oturum açmış kullanıcılar bu ekran aracılığıyla geçmiş işlemlerini web sunucusundan indirerek görüntüleyebilmektedirler Şekil (3.4.3.9.).



Şekil 3.4.3.9. KDS erişimler ve işlemler listesi ekranı

3.4.3.10. KDS kullanıcı oturum kapat

KDS masaüstü uygulamasında oturum açmış kullanıcılar bu menü aracılığı ile oturumlarını ve uygulamayı kapatabilmektedir.

3.4.4. KDS web uygulaması

KDS sisteminin istemci tarafında çalışan ve kullanıcı girişi, konum bilgisi tanımlama/düzenleme, kullanıcı bilgi görüntüleme ve şifre düzenleme gibi işlemlerin gerçekleştirildiği web ve java applet tabanlı uygulamadır.

KDS Web Uygulaması için bir web sunucu kiralanmış, web hosting oluşturulmuş ve www.e-imza.web.tr alan adı alınarak uygulamanın bu adresten çalışabilmesi sağlanmıştır. Uygulama veritabanı olarak mySQL veritabanı kullanmaktadır ve bu veritabanı da yine aynı web sunucusunda yer almaktadır.

3.4.4.1. KDS kullanıcı girişi

KDS web uygulamasında web arayüzünde oturum açmak için java appletidir. Bu applet ile kds masaüstü uygulaması olmadan tanımlarına erişme, tanımları düzenleme, şifre değiştirme gibi işlemleri gerçekleştirilebilir.

3.4.4.2. KDS konum/hedef tanımlama ve düzenleme

KDS web uygulamasında tanımlama yapmak ve tanımları düzenlemek için ilgili web sayfasına ulaşmayı sağlayan ekrandır. Bu ekran ile masaüstü olmadan da konumlarda değişiklik ve güncelleme yapılabilir.

3.4.4.3. KDS konum kullanıcı şifre bilgileri düzenleme

KDS web uygulamasında KDS kullanıcı şifresini değiştirmek için kullanılan ekrandır. Bu ekran ile KDS kullanıcı şifresi kolayca değiştirilebilir. Şifre değişikliğinin sadece webdeki java applet uygulaması ile gerçekleştirilmesine izin verilmiştir.

3.4.4.4. KDS yeni konum ve hedef tanımlama

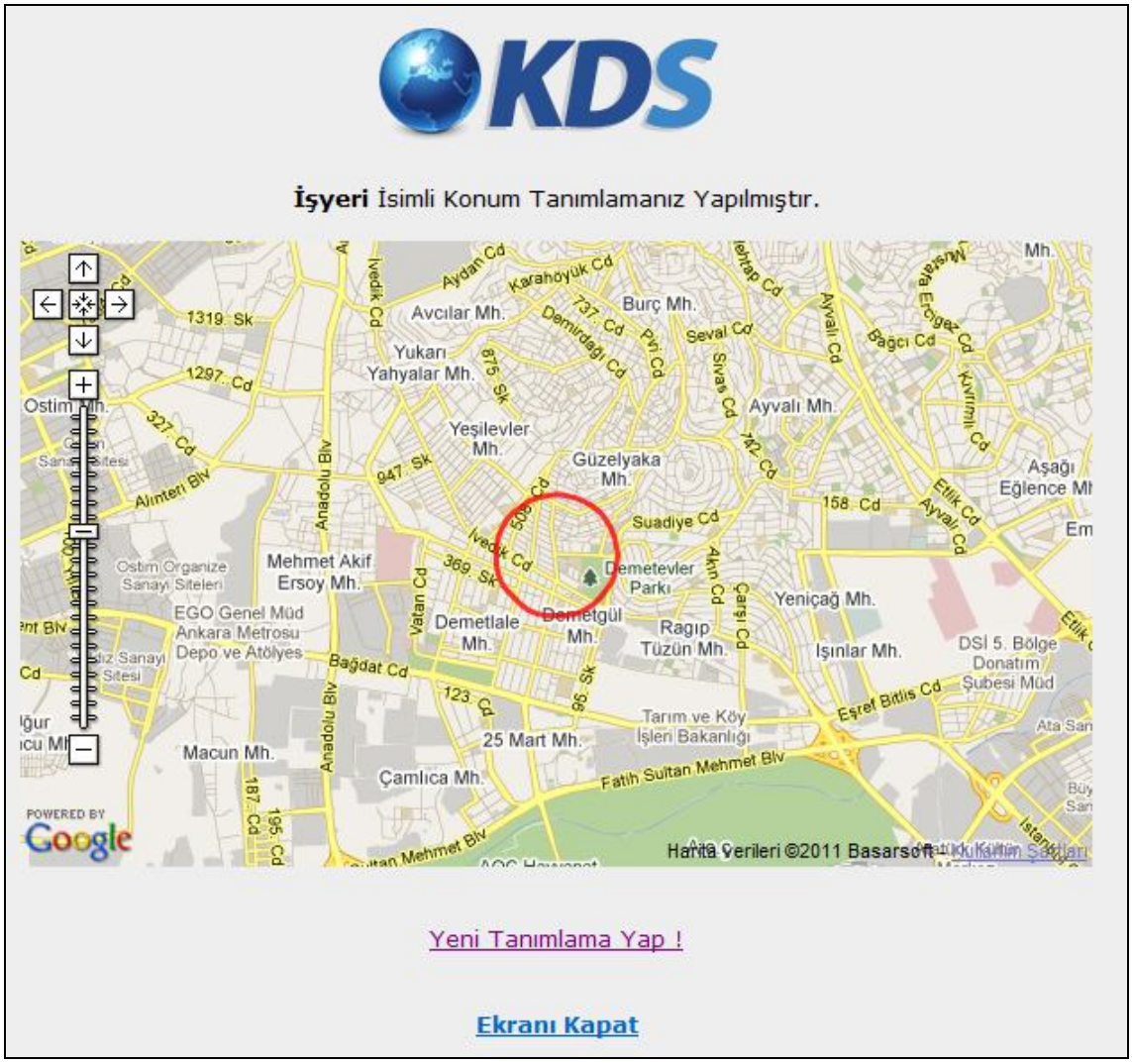
KDS Masaüstü ya da web uygulamasında oturum açmış olan kullanıcılar, tanımlama ekranlarındaki “Yeni konum tanımla” ve“Yeni hedef tanımla” butonlarına tıkladıklarında bu sayfaya erişmektedirler.

Bu sayfa kullanıcıya açmış olduğu oturumda e-imzasını kullanmak istediği konumları tanımlama imkanı sağlamaktadır (Şekil 3.4.4.4.1). Google Maps API’den de istifade eden bu sayfa ile fare hareket ettirilerek kolayca enlem ve boylam değerleri elde edilebilir. Ayrıca gene bu sayfada konuma isim verebilir ve etki alanı seçilebilir. Etki alanı imzanın kullanılmak istendiği dairesel bölgenin yarıçapına eşittir.

Şekil 3.4.4.4.1. KDS konum tanımlama ekranı

Konum Tanımlama Ekranını ile bir konum tanımlandığında sonuç olarak konumun hangi alanı kapsadığını gösteren bir gösterim ekranı açılacaktır (Şekil 3.4.4.4.2) .

Bu ekranda kırmızı ile gösterilen alan etki alanı olup bu alan dışında gerçekleşen konum damgalı e-imzalama işlemleri geçersiz sayılacak ve bu alanlar dışında imzalanan bu dosyalar açılamayacaktır.



Şekil 3.4.4.4.2. KDS kaydedilen konum görüntüleme ekranı

3.4.4.5. KDS konum tanım listesi

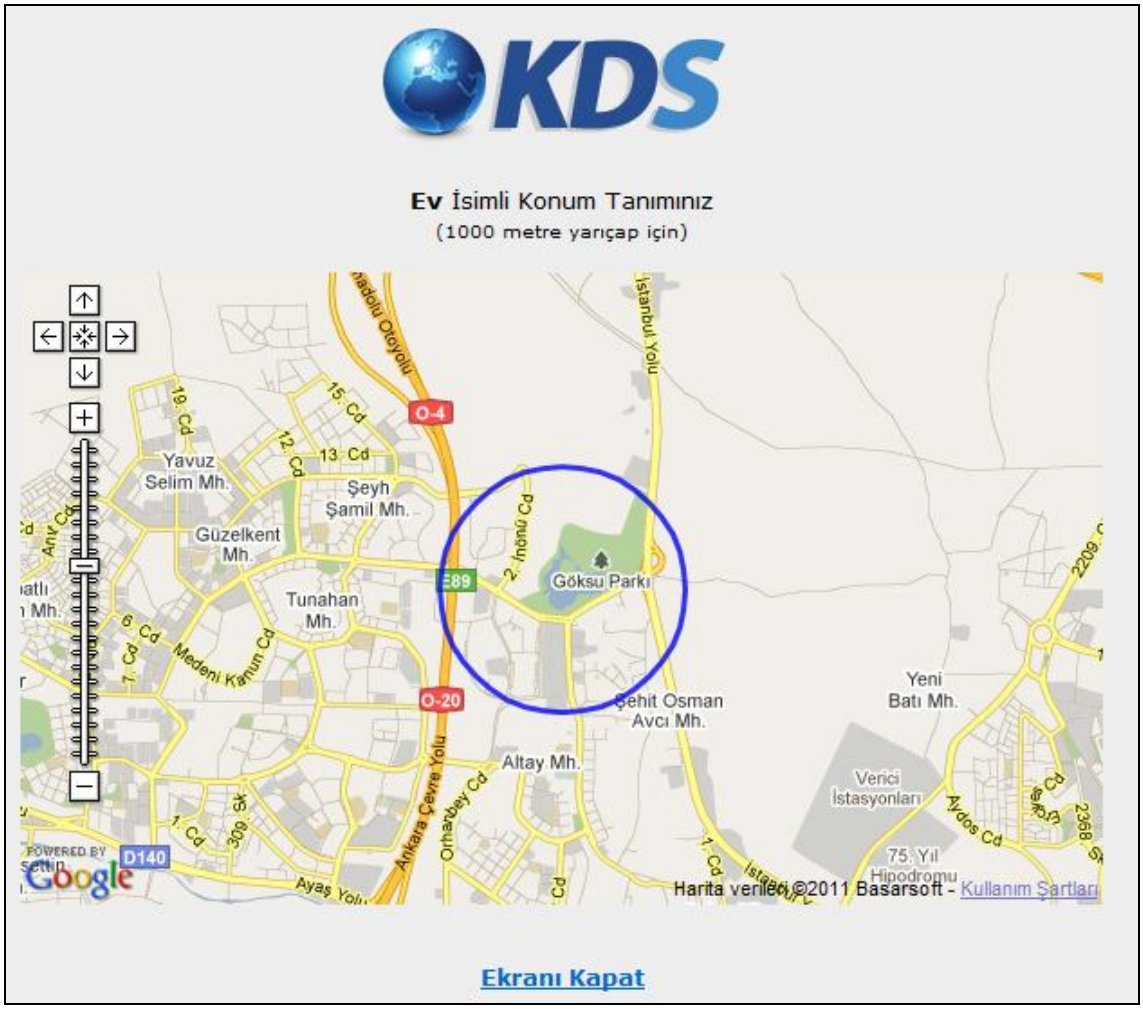
KDS web uygulamasının en önemli ekranlarından bir de tanım listesi ekranıdır. Bu ekranda tanımlar listesine ulaşabilir, buradan istenilen bir tanım silinebilmekte, devre dışı bırakılabilmekte ya da yeniden devreye alınabilmektedir (Şekil 3.4.4.5.1.). Bu ekrana KDS Masaüstü ve Web Applet uygulamalarından erişilebilmektedir. Yapılan değişiklikler derhal uygulamaya yansımaktadır.

Tanımlı konum bilgisinin durumu değiştirilmek istendiğinde durum başlığı altındaki butonlara tıklanması yeterlidir. Eğer buradaki durum kırmızı ise o tanım kullanılamaz demektir. Yeşil ise bu tanım doğrulama işlemleri için devrede demektir. Bir tanımı silmek için ise sil başlığı altında yer alan sil butonuna tıklanması yeterlidir.

Silinmiş tanımlar sistemde silinmiş olarak işaretlenir fakat doğrulama işlemine herhangi bir etkileri yoktur.

Şekil 3.4.4.5.1. KDS tanımlanmış konum bilgileri ekranı

KDS web uygulamasında bir tanımın hangi etki alanına sahip olduğunu görüntülemek için tanım önündeki dünya butonuna tıklanmalıdır. Böylelikle açılacak yeni bir ekranda bu tanımın etki alanı mavi bir çember içinde görüntülenecektir (Şekil 3.4.4.5.2.).



Şekil 3.4.4.5.2. KDS tanımlanan konum gösterimi ekranı

4. ARAŞTIRMA VE TARTIŞMA

Yakın tarihlerde ortaya çıkan bir takım güvenlik gereksinimlerden ötürü elektronik imza ile ilgili yeni yasal düzenlemeler gerçekleşmiştir. Bu düzenlemelerden sonuncusu elektronik ortamda doküman ve sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlama gereksinimi sonucu ortaya çıkan ve elektronik imza işlemlerinde, işlemin gerçekleştiği zamanın ispatlanabilir olması için kullanılan Zaman Damgası uygulamasıdır.

Benzer bir biçimde ilerleyen zamanda elektronik imza işleminin gerçekleştiği yerin, yani imzalamanın nerede gerçekleştiğinin ispatlanabilir olmasına ihtiyaç duyulabileceği düşünülmektedir.

Mevcut E-imza işlemlerinde, işlemin gerçekleştiği zamanın ispatlanabilir olması için yer alan Zaman Damgası; E-imza Kanunu'nun 3.maddesinde "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt" olarak tanımlanmaktadır.

Zaman damgası elektronik ortamda doküman ve sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlama gereksinimi sonucu ortaya çıkmıştır. İlerleyen zamanda e-imza işleminin nerede gerçekleştiğine dair benzer bir gereksinim ortaya çıkması muhtemeldir.

Elektronik olarak imzalanan belgelerin güvenliğini artırmak için küresel yer belirleme sisteminden de yararlanan KDS sisteminin kullanılması ile elde edilen sonuçlar aşağıda listelenmiştir.

Elektronik imza ile imzalanmış belgelere ilişkin sonuçlar şöyledir;

- Belgelerin açılabileceği alanlar tanımlanabilir hale gelmiştir,
- Belgelerin nerede imzalandığı belirlenebilir hale gelmiştir,
- Belgelerin açılabildiği alan sınırlandırılabilmiştir,
- Belgelerin nerede açılabileceği belirlenebilir hale gelmiştir,
- Belgelerin gönderildiği alan sınırlandırılabilmiştir,
- Belgelerin nerede gönder doğrulanabilir hale gelmiştir,
- Belgeler şifreleme metotları ve yeni bir yapı ile tek bir formata kavuşmuştur.

E-imza ve Küresel yer belirleme sistemi teknolojileri özellikle son yıllarda geniş kesimlere hitap eden ve kullanımı hızla yaygınlaşan teknolojiler olmuşlardır. E-imza, güvenilir kimliklendirme ve onay mekanizmasıyla güvenli olarak elektronik ortamlarda iş ve işlemlerin hızlıca yapılabilmesi, iş maliyetlerinin düşmesi, iş takiplerinin kolaylaşması, güvenlik zafiyetlerinin ve açıkların azalması, e-ticaret hacimleri artması gibi yararları olan bir teknolojidir.

Küresel yer belirleme sisteminin ise koordinatlar arası görüş zorunluluğunun ve koordinat yeri seçiminde noktaların en yüksek yerlerde olması gibi zorunlulukların ortadan kalkması, yer belirlemenin hava şartlarından bağımsız hale gelmesi, gece gündüz sürekli yer belirleme yapılabilmesi, üç boyutlu yer koordinatları elde edilmesi gibi yararları vardır.

KDS sistemi, bu iki teknolojinin yararlı özelliklerinden faydalanıp, elektronik imza işleminin güvenliğine ilave güvenlik katmayı öneren bir sistemdir. YÖK Ulusal Tez Merkezi veritabanında ve internet üzerinde erişilebilen yayınlarda yapılan araştırmada e-imza ve küresel yer belirleme sistemine ve farklı alanlarda kullanımlarına ilişkin çokça çalışmaya rastlanmıştır. Bu çalışmalarda e-imza güvenliği ve küresel yer belirleme sisteminin bir arada geçtiği benzer bir çalışmaya rastlanmamıştır.

5. SONUÇ VE ÖNERİLER

5.1. Sonuçlar

Elektronik imza konusunda şimdiye kadar yapılan çalışmaların odağında mevcut yapı çerçevesinde bir takım standartlara uyum ve şifreleme teknikleri ile güvenliği artırmak yer almaktaydı. Bu öneride ise farklı ve mevcut yapının dışında güvenlik artırıcı ilave bir sistem ortaya konmuştur.

Bu çalışmada, e-imzanın yetkisiz kullanımına karşı, elektronik olarak imzalanan belgelerin güvenliğini artıracak "Konum Damgası Sistemi" önerilmiştir. Küresel yer belirleme sisteminden de yararlanan bu sistem, elektronik imzalı belgelerin nerede imzalandığının tespit edilmesine ve elektronik imza kullanımının konum açısından sınırlanabilmesine imkân sağlamıştır.

Çalışmada da detaylı anlatıldığı gibi elektronik imza güvenliği çeşitli şekillerde tehdit altındadır. Bu öneri bu tehdidi minimuma indirmek için yeni bir ilave sistem önermektedir. Önerilen bu yeni sistemin güvenliği ve güvenilirliği artıracağı muhakkaktır. Çalışma, öneriyi anlatmakta ve uygulamasını ortaya koymaktadır. Çalışma kapsamında önerinin gerçekleşebilirliğini ortaya koymak için geliştirilen e-imza güvenliğinin artırılmasına yönelik konum damgası sistemi uygulaması başarılı sonuçlar vermiştir.

KDS önerisi ile elektronik imzalı belgelerin açılabileceği alanlar tanımlanabilmiş, belgelerin nerede imzalandığı ve nerelerde açılabileceği belirlenebilir hale gelmiştir. Belgelerin nerede imzalandığı doğrulanabilir hale gelmiş, belgeler şifreleme metotları ve yeni bir yapı ile tek bir formata kavuşmuştur. Bütün bu özellikler sayesinde elektronik imzalanan belgelerin güvenliği artırılmıştır.

Devletimiz, e-dönüşüm Türkiye projesi ile vatandaşlara devletle olan bütün işlerinde kuyruklardan ve bürokrasiden uzak, teknolojiden hızlı ve etkin bir biçimde yararlanmak suretiyle hizmetleri çevrimiçi sunmayı amaçlamaktadır. Ülkemizde e-dönüşümün anahtarı olarak görülen elektronik imzanın günlük hayatımızdaki yeri ve önemi, özellikle elektronik imza kanunu ile elektronik imzaların hukuki açıdan tanınması ile artırmıştır.

Elektronik imzanın daha da güvenli olması, vatandaşın elektronik imzaya olan güvenini de artıracaktır. Elektronik imzanın güvenliğini artırmaya yönelik araştırmalar

gerçekleştirerek farklı bakış açılarıyla yeni algoritmalar ve yaklaşımlar geliştirmeyi hedefleyen bu çalışmanın, elektronik imzanın güvenliği, gelişimi ve yaygınlaşması sürecine, dolaysıyla e-devlet/e-dönüşüm sürecine katkı sağlayacağı düşünülmektedir.

E-dönüşüm ve e-devlet sürecine önemli katkıları olan elektronik imzanın güvenliğinin bu alanda yapılacak yeni çalışmalarla artırılabileceğine inanmaktayız. KDS sistemi önerisinin elektronik imzanın güvenliği, gelişimi ve yaygınlaşması sürecine katkı sağlaması ve yeni ufuklar açması umulmaktadır.

5.2. Öneriler

KDS sisteminin ülke çapında hayata geçirilebilmesi için idari, teknik, hukuki ve standartlar çerçevesinde detaylı ve yoğun araştırma, inceleme ve çalışmalar gerçekleştirilmesi önerilmektedir.

Bu çalışmalar; e-imza kart okuyucularına GPS alıcılarının entegre edildiği cihaz geliştirilmesi, bu cihazlar için GPS sinyali alım kalitesinin yükseltilmesi alanlarında gerçekleşebilir.

GPS verisinin uydulardan alınamadığı yerlerde Yardımlı Küresel Konumlandırma Sistemi'nden (Asisted GPS) destek alınması ile ilgili çalışmalar gerçekleştirilebilir.

Konum damgası sisteminin uluslar arası teknik standartlara uyumluluğu, sistemin hukuki ve idari olarak temellendirilmesi, sistemin metin dosyaları dışında farklı tipte dosyalara uygulanabilmesi ve sabit mekanlar için geçerliliği olan ve nitelikli konum bilgisinin sağlanması vb. konularda da çalışmalar yapılması yararlı olacaktır.

KDS sistemi kapsamında, küresel yer belirleme sisteminden alınan konum bilgilerinin herhangi bir cihazdan değil, sertifika makamlarınca belirlenmiş cihazlar kullanılarak tespit edilmesi, açık hava görmeyen yerler için ise bu yere ait konumun bu cihazlar tarafından önceden tespit edilip saklanması ve kullanılması ile ilgili çalışmalar yapılması önerilmektedir.

KDS sistemi yeni bir öneridir ve sistemin elektronik imzanın sahip olduğu hukuki geçerlilik dışında herhangi bir hukuki tabanı yoktur. KDS sisteminin kabul görmesi ve kullanılması durumunda hukuki gereksinim ve şartların da ortaya konulması gerekecektir. Burada tıpkı zaman damgası sisteminde olduğu gibi hukuki bir zeminin oluşması gündeme gelecektir. KDS sisteminin hukuki durumu ile ilgili çalışmalar yapılabilir.

KDS sistemin mevcut şifreleme algoritmaları geliştirilerek daha güçlü bir biçimde şifrelenmiş kds dosyaları oluşturulabilmesi için farklı şifreleme tekniklerinin ne şekilde uygulanabileceği ve kullanılabileceğinin araştırılacağı çalışmalar yararlı olacaktır.

KDS sistemin farklı uygulama ve sistemlerle uyum içerisinde çalışmasını sağlayacak web servisleri yazılabilir. Bu düşünceden yola çıkarak KDS web servislerinin ne şekilde tasarlanabileceği ve kullanılabileceğinin araştırılacağı çalışmalar da yapılabilir.

6. KAYNAKLAR

5070 Sayılı Elektronik İmza Kanunu, 23 Ocak 2004 Tarih ve 25355 sayılı Resmi Gazete, Kanun Kabul Tarihi: 15 Ocak 2004.

Avcı, Ö., Doğru, A. , Kılıç, C., 2002, Filo Yönetim Sistemleri, Bitirme Ödevi, İ.T.Ü. İnşaat Fakültesi, İstanbul.

Bilgi Teknolojileri ve İletişim Kurumu, 2010, E-imza Faydalı Bilgiler, http://www.tk.gov.tr/eimza/E-Imza_Faydali_bilgiler.htm [Ziyaret Tarihi: 15 Aralık 2010].

Bilgi Teknolojileri ve İletişim Kurumu, 2005, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliği, 06.01.2005 tarih ve 25692 sayılı Resmi Gazete.

Büyükbaş, A., 2005, CDMA ve UMTS: Üçüncü Nesil Mobil Haberleşme Teknolojilerinin Karşılaştırılması, Türkiye Önerisi, Telekomünikasyon Kurumu, Ankara, 1-2.

Canbek, G., Sağıroğlu, Ş., 2005, Şifre Bilimi Tarihine Genel Bakış–II, Telekom Dünyası, 36–44, Haziran.

Canbek, G., Sağıroğlu, Ş., 2007, Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü Dergisi, Cilt 23, No: 1–2, s. 1–12, Kayseri,.

Cert TR, 2010, Spoofed/Forged Email, http://www.cert.org/tech_tips/ email_spoofing.html, [Ziyaret Tarihi: 15 Aralık 2010].

Çınar, T., 2004, Global Navigation Satellite Systems – GNSS, Hava Harb Okulu Komutanlığı HUTEN, İstanbul.

Derelioğlu B., 2007, GPS ve GPRS Tabanlı Geniş Alan Ağı Uygulaması, Gazi Üniversitesi, FBE, Yüksek Lisans Tezi, Ankara.

Doğru, A., Uluğtekin, N., 2005, CBS Uygulaması Olarak Araç Navigasyon Sistemleri, Ege CBS Sempozyumu, 27-29 Nisan 2005, İzmir.

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

Enge P., 2003, GPS Modernization: Capabilities of the New Civil Signals, Australian International Aerospace Congress, Australia, 85-86.

Ersoy, N., 1997, İstanbul Nirengi Çalışmalarının Yersel ve GPS Ölçüleri İle

Değerlendirilmesi ve Analizi, Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, Jeodezi Ve Fotogrametri Anabilim Dalı, Üniversite Yayın No: YTÜ. En.Dr.-97.0330/Enstitü Yayın No: En.FBE-97.008 YTÜ Basım Yayın Merkezi, İstanbul.

Gen Bilim, 2006, Elektronik İmza Hakkında Temel Bilgiler, http://www.genbilim.com/index.php?option=com_content&task=view&id=470, [Ziyaret Tarihi: 20 Aralık 2010].

Gps Navigation System, 2011, http://www.gps-navigations.net/wp-content/uploads/2011/01/Gps-Satellite-Orbits1.jpg, [Ziyaret Tarihi: 3 Ocak 2011].

Hofmann-Wellenhof, B., Lichtenegger, H. and Collins, J., 2001. Global Positioning System Theory and Practice, Springer-Verlag Wien,New York

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

İşeri B., 2006, Personel Yer Belirleme Sisteminde GPS Desteğinin Kullanılması, Dicle Üniversitesi, FBE, Yüksek Lisans Tezi, Diyarbakır.

İTO, 2009, Elektronik İmza, Bilişim Teknolojileri ve E-ticaret Şubesi, http://www.ito.org.tr/wps/wcm/connect/ 57dbd5004dc0a089b85ef8ad5be93185/e-imza.doc, Nisan 2009, [Ziyaret Tarihi: 11 Aralık 2010].

Kahraman, S., Seke, E., 2004, DGPS Tekniği ile Es Zamanlı Konum Belirleme, Osman Gazi Üniversitesi, Eskişehir.

Kahveci, M., Yıldız, F., 2005, GPS Global Konum Belirleme Sistemi Teori-Uygulama, Nobel, Ankara,1-2.

Kennedy, M., 2002, The Global Positioning System and GIS, Taylor & Francis, New York, 1-2.

Leick, A., 2004, GPS Satellite Surveying, Wiley, USA, 72.

Levi A., 2004 , Nasıl bir E-posta güvenliği, Sabancı Üniversitesi Mühendislik ve Doğa bilimleri Fakültesi, İstanbul.

Marco de Vivo, Gabriella O. De Vivo, Germinal Iserm, 1998, Internet Security Attacks at the Basic Levels, Operating Systems Review, ACM Press, Vol. 32 No 2.

Mısra, P., Enge, P., 2001, Global Positioning System: Signals, Measurements, and Performance, Ganga-Jamuna Press, Lincoln, 10-20.

Özcan İ., GPS Koordinatları Verilen İki Nokta Arası Uzaklık , 2010, http://www.yaztasarla.com/csharp/gps-koordinatlari-verilen-iki-nokta-arasi-uzaklik.html, [Ziyaret Tarihi: 8 Aralık 2010].

Özenç R.F., 2003, Lokal Alan Diferansiyel GPS Hassas Yaklaşması ve Gözlem Sonrası Hesaplama Yöntemiyle Uygulaması, Yüksek Lisans, Gazi Fen Bilimleri Enstitüsü, Ankara, 34-41.

Saygı Z., Yeşil S., 2006, Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar, Ulusal E-İmza Sempozyumu Bildiri Kitabı.

Spalka, A., Cremers, A. B., Langweg, H., 2002, "Trojan Horse Attacks on Software for Electronic Signatures", Informatica 26, 191–203.

TÜBİTAK UEKAE Kamu Sertifikasyon Merkezi, 2005, E-imza Uygulaması Kontrol Listesi, http://www.kamusm.gov.tr/tr/Kurumsal/Musterilerimiz/ KontrolListesi.pdf ,[Ziyaret Tarihi: 28 Aralık 2010].

TÜBİTAK UEKAE Kamu Sertifikasyon Merkezi, 2007 Zaman Damgası, http://www.kamusm.gov.tr/tr/Hizmetler/Zamandamgasi/, [Ziyaret Tarihi: 20 Aralık 2010].

Topatan S., 2008, GPS Konum Belirleme Algoritmalarının Uygulanması, İstanbul Teknik Üniversitesi, FBE, Yüksek Lisans Tezi, İstanbul.

Wang, Lai, Guo, Chen, Yu., 2005, Cryptanalysis for Hash Functions MD4 and RIPEMD. Advances in Cryptology-Eurocrypt'05. Springer-Verlag.

Wang, Lin, Yu., 2005, Finding Collisions in the Full SHA-1. Advances in Cryptology-Crypto'05. Springer-Verlag.

Wang, Yu., 2005, How to Break MD5 and Other Hash Functions. Advances in Cryptology-Eurocrypt'05. Springer-Verlag.

Wang, Lin, Yu., 2005, Efficient Collision Search Attacks on SHA-0. Advances in Cryptology-Crypto'05. Springer-Verlag.

Wells, D., Beck, N., Delikaraoğlu, D., Kleusberg, A., Krakivsky, E.J., Lachapelle G., Richart, B.L., Nakiboğlu, M., Schwarz, K.P., Tranquilla, J.M., Vonicek, 1986, P. Guide to GPS Positioning Canadian GPS Associates , Frederiction http://www.spaceondtech.com/ spacedata/constellations/nauster_gps/ , [Ziyaret Tarihi: 18 Kasım 2010].

EK-A. ELEKTRONİK İMZA KANUNU

Kanun No: 5070

Kabul Tarihi: 15.01.2004

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 yirmi milyar 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.

EK-B. TÜRKİYE'DE ELEKTRONİK İMZAYA İLİŞKİN DÜZENLEMELER

E-imza konusunda özellikle 5070 sayılı kanun ve sonrasında yapılmasına ihtiyaç duyulan düzenlemeler ivedilikle gerçekleştirilmiştir. Bunlar: [7]

- Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Rehberi'ne İlişkin Kurul Kararı (18.04.2007 tarih ve 2007/DK-77/207 sayılı Kurul Kararı)
- Nitelikli Elektronik Sertifika, Zaman Damgası ve İlgili Hizmetlerin Ücretlerinin Belirlenmesine İlişkin Kurul Kararı (20.12.2006 tarih ve 2006/DK-77/760 sayılı Kurul Kararı)
- Güvenli Elektronik İmza Oluşturma ve Doğrulama Uygulamaları ile Güvenli Elektronik İmza Formatlarına Dair Usul ve Esaslar Hakkında Kurul Kararı (01.06.2006 tarih ve 2006/DK-77/353 sayılı Kurul Kararı)
- 5070 Sayılı Elektronik İmza Kanunu (23.01.2004 tarih ve 25355 sayılı Resmi Gazete)
- 5728 Sayılı Kanun (08.02.2008 tarih ve 26781 sayılı Resmi Gazete)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (06.01.2005 tarih ve 25692 sayılı Resmi Gazete)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (17.10.2006 tarih ve 26322 sayılı Resmi Gazete)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (04.02.2006 tarih ve 26070 sayılı Resmi Gazete)
- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (06.01.2005 tarih ve 25692 sayılı Resmi Gazete)
- Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ (26.06.2008 tarih ve 26918 Sayılı Resmi Gazete'de yayımlanan)

- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ (20.06.2006 tarih ve 26204 sayılı Resmi Gazete)
- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ (21.01.2006 tarih ve 26056 sayılı Resmi Gazete)
- Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ (18.06.2005 tarih ve 25849 sayılı Resmi Gazete)
- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26.08.2004 tarih ve 25565 sayılı Resmi Gazete)
- Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005 tarih ve 25709 sayılı Resmi Gazete)
- Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı (27.01.2005 tarih ve 25709 sayılı Resmi Gazete)
- 2004/21 Sayılı Başbakanlık Genelgesi (06.09.2004 tarih ve 25575 sayılı Resmi Gazete)
- 2006/13 Sayılı Başbakanlık Genelgesi (19.04.2006 tarih ve 26144 sayılı Resmi Gazete)

EK-C. KDS UYGULAMASINDA KULLANILAN SINIFLAR

```
import com.uf.comm.serial.SerialPort;
import com.uf.gps.ConnectException;
import com.uf.gps.Connection;
import com.uf.gps.Descriptor;
import com.uf.gps.GPSEvent;
import com.uf.gps.GPSListener;
import com.uf.gps.Position;
import com.uf.gps.protocols.NMEA.NMEAHandler;
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Desktop;
import java.awt.Dimension;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.Font;
import java.awt.GridBagConstraints;
import java.awt.GridBagLayout;
import java.awt.Insets;
import java.awt.Rectangle;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.DataInputStream;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.FileReader;
import java.io.FileWriter;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.io.IOException;
import java.io.OutputStream;
import java.net.URI;
```

```
import java.net.URISyntaxException;
import java.security.KeyStore;
import java.security.MessageDigest;
import java.security.PrivateKey;
import java.security.spec.AlgorithmParameterSpec;
import java.util.Arrays;
import java.util.Calendar;
import java.util.Collection;
import java.util.GregorianCalendar;
import java.util.Iterator;
import java.util.List;
import java.util.Vector;
import java.util.zip.GZIPInputStream;
import java.util.zip.GZIPOutputStream;
import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import javax.swing.BoxLayout;
import javax.swing.DefaultButtonModel;
import javax.swing.filechooser.FileFilter;
import javax.swing.ImageIcon;
import javax.swing.JButton;
import javax.swing.JCheckBox;
import javax.swing.JFileChooser;
import javax.swing.JFrame;
import javax.swing.JLabel;
import javax.swing.JMenu;
import javax.swing.JMenuBar;
import javax.swing.JMenuItem;
import javax.swing.JOptionPane;
```

```
import javax.swing.JPanel;
import javax.swing.JPasswordField;
import javax.swing.JScrollPane;
import javax.swing.JTextArea;
import javax.swing.JTextField;
import javax.swing.JToolBar;
import javax.swing.SwingConstants;
import mtb.kds.code.DosyaGuvenlik;
import mtb.kds.code.DosyaSifrele;
import mtb.kds.code.ElektronikImza;
import mtb.kds.code.KonumDamgasi;
import mtb.web.WebIletisim;
import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder;
import tr.com.cs.signer.cert.C_Certificate;
import tr.com.cs.signer.cert.C_KeyStore;
import tr.com.cs.signer.cms.C_FileSigner;
import tr.com.cs.signer.cms.C_SignedData;
import tr.com.cs.signer.cms.C_SignerInfo;
import tr.com.cs.signer.cms.C_Verifier;
import tr.com.cs.signer.util.C_Logger;
import tr.gov.kamusm.imzager.api.AkilliKart;
import tr.gov.kamusm.imzager.api.AkilliKartSeti;
import tr.gov.kamusm.imzager.api.Sertifika;
```

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Mustafa ÖZLÜ
Uyruğu : T.C.
Doğum Yeri ve Tarihi : Erbaa, 1981
Telefon : 0 505 267 65 00
Faks : 0 312 303 11 73
e-mail : mustafaozlu@gmail.com

EĞİTİM

Derece		Adı, İlçe, İl	Bitirme Yılı
Lise	:	Ankara Tevfik İleri Anadolu İmam Hatip Lisesi	1999
Üniversite	:	Selçuk Üniversitesi Bilgisayar Mühendisliği	2007
Yüksek Lisans	:		
Doktora	:		

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2000-2002	Uzay Bilgisayar	Web Tasarımcı
2002-2003	SFN Tanıtım	Web Programcısı
2003-2004	Sır Ajans	Programcı
2005-2011	Türk Patent Enstitüsü	Bilgisayar Mühendisi

UZMANLIK ALANI

Yazılım Geliştirme, Veritabanları, Web Uygulama Geliştirme

YABANCI DİLLER

İngilizce