BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK ORTAMDA BELGELERİN GÜVENLİ PAYLAŞIMI; ÜLKE UYGULAMALARI VE ÜLKEMİZ İÇİN ÖNERİLER

Mustafa YILMAZ

İdari Uzmanlık Tezi

MART 2013

Ankara

©Bu eserin tüm telif hakları

Bilgi Teknolojileri ve İletişim Kurumuna aittir.

Kaynak gösterilmeden alıntı yapılamaz.

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-044-3

BTK Yayın No T 0156

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK ORTAMDA BELGELERİN GÜVENLİ PAYLAŞIMI; ÜLKE UYGULAMALARI VE ÜLKEMİZ İÇİN ÖNERİLER

Mustafa YILMAZ

İdari Uzmanlık Tezi

MART 2013

Ankara

Mustafa YILMAZ tarafından hazırlanan "Elektronik Ortamda Belgelerin Güvenli Paylaşımı; Ülke Uygulamaları ve Ülkemiz İçin Öneriler" adlı bu tezin İdari Uzmanlık tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Şeref SAĞIROĞLU
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından İdari Uzmanlık tezi olarak kabul edilmiştir.

Başkan : _____
Kurum Başkan Yardımcısı Deniz YANIK

Üye : _____
Daire Başkanı Nihat SÜMER

Üye : _____
Bilişim Uzmanı Mehmet Kaşif TİRYAKİ

Üye : _____
Prof. Dr. Şeref SAĞIROĞLU

Üye : _____
Müdür Murat AYDIN

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

İÇİNDEKİLER v
ÖZET i
ABSTRACT ii
TEŞEKKÜR iii
TABLOLAR LİSTESİ iv
ŞEKİLLER LİSTESİ v
KISALTMALAR LİSTESİ vii
GİRİŞ 1
1. ELEKTRONİK ORTAMDA GÜVENLİ BELGE OLUŞTURULMASI 6
1.1. e-Belge Nedir 6
1.1.1. e-Belgenin üretim ortamları 7
1.2. e-Belge Yönetim Süreci 8
1.3. EBYS ve e-Belge Kriterleri 10
1.3.1. Tanımlanabilirlik 14
1.3.2. Onay ve kayıt bilgisi 14
1.3.3. Bütünlük 15
1.3.4. Yapısal özellikler 15
1.3.5. Teknolojik özellikler 16
1.3.6. e-Belge güvenliğinin sağlanması 16
1.4. e-Belgenin Yaşam Döngüsü 18
1.4.1. e-Belgenin üretimi 20
1.4.2. e-Belgenin dağıtımı 21
1.4.3. e-Belgenin kullanımı 22
1.4.4. e-Belgenin bakımı 22
1.4.5. e-Belgenin tasfiyesi 23
1.4.5.1. e-Belgenin arşivlenmesi 23
1.4.5.2. e-Belgenin imhası 25
2. ELEKTRONİK ORTAMDA BELGE PAYLAŞIM YÖNTEMLERİ 26
2.1. Sanal Özel Ağ 26
2.1.1. Uzaktan erişim sanal özel ağ 28

2.1.2. Siteden siteye sanal özel ağ 29
2.2. Güvenli Yuva Katmanı 30
2.2.1. Güvenli yuva katmanının çalışma şekli 32
2.3. Dosya Aktarım Protokolü/Güvenli Dosya Aktarım Protokolü 34
2.4. e-Posta 36
2.4.1. e-Postanın yapısı 36
2.4.2. Başlık bölümü 36
2.4.3. Gövde bölümü ve çok amaçlı internet posta uzantıları 37
2.4.4. e-Posta hizmeti araçları 37
2.4.5. e-Posta işleme servisi 38
2.4.6. e-Posta işleyişi 38
2.4.7. e-Posta güvenlik mekanizmaları 40
2.5. Kayıtlı Elektronik Posta (KEP) 40
2.5.1. KEP sistemi ile ilgili standart çalışmaları 43
2.5.2. UPU'nun çalışmaları 43
2.5.3. ETSI'nin çalışmaları 44
2.5.4. CEN'in çalışmaları 45
2.5.5. KEP sistemi çalışma adımları 46
2.5.6. KEP sisteminin güvenlik özellikleri 48
2.5.6.1. Güvenli e-imza 49
2.5.6.2. Kimlik doğrulama 50
2.5.6.3. Güvenli etkileşim 50
2.5.6.4. Virüslerden korunma 51
2.6. Kiralık Hat 51
3. e-BELGEYE İLİŞKİN MEVZUAT VE STANDARTLAR 54
3.1. Ülkemizde Durum 54
3.1.1. Ulusal mevzuatta e-belgeye ilişkin düzenlemeler 55
3.1.1.1. Vergi Usul Kanunu 58
3.1.1.2. Bilgi Edinme Hakkı Kanunu ve Yönetmeliği 59
3.1.1.3. Elektronik İmza Kanunu ve ikincil düzenlemeler 62
3.1.1.4. Tebligat Kanunu'nda Değişiklik Yapılmasına Dair Kanun ... 64
3.1.1.5. Elektronik Tebligat Yönetmeliği 65

3.1.1.6. Türk Ticaret Kanunu 65
3.1.1.7. KEP sistemine ilişkin düzenlemeler 66
3.1.1.8. Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik 70
3.1.1.9. Devlet Arşiv Hizmetleri Hakkında Yönetmelik 71
3.2. Uluslararası Standartlar 71
3.3. Ülkemizdeki e-belge yönetimi standardı 74
4. DÜNYADA VE TÜRKİYE'DE e-BELGE PAYLAŞIMINA İLİŞKİN UYGULAMALAR 78
4.1. Ülkemizdeki Uygulamalar 79
4.1.1. e-Yazışma Projesi 79
4.1.1.1. e-Yazışma Paketi 80
4.1.1.2. e-Yazışma Paket yapısı 81
4.1.1.3. e-Yazışma Paketi bileşenleri 83
4.1.1.4. Mesaj paylaşım 84
4.1.2. Ulusal Yargı Ağı Projesi (UYAP) 84
4.1.3. Merkezi Nüfus İşleri Sistemi (MERNİS) 84
4.1.4. BTK'da e-ortamda e-belge paylaşımı içeren uygulamalar 86
4.1.4.1. Mobil Cihaz Kayıt Sistemi 86
4.1.4.2. Numara Taşınabilirliği Sistemi 86
4.1.4.3. Online Şikâyet Bildirim Sistemi 87
4.1.5. e-Devlet uygulaması 87
4.2. e-Belge ve paylaşım yöntemleri ilişkileri 88
4.3. Dünyada e-Belge Paylaşımı ve KEP Uygulamaları 89
SONUÇ 95
ÖNERİLER 103
KAYNAKLAR 108
EKLER 118
Ek 6-1. e-Ortamda e-Belgelerin Güvenli Paylaşım Anketi İçin Yurt Dışı Kurum ve Kuruluşlara Gönderilen Üst Yazı 118
Ek 6-2. e-Ortamda e-Belge Güvenli Paylaşım Yurt Dışı Anket Soruları 119

Ek 6-3. e-Ortamda e-Belgelerin Güvenli Paylaşım Anketi İçin Yurt İçi Kurum ve Kuruluşlara Gönderilen Üst Yazı 120
Ek 6-4. e-Ortamda e-Belgelerin Güvenli Paylaşım Yurt İçi Anket Soruları . 121
Ek 6-5. Yurt İçi ve Yurt Dışı Anket Sonuçları 124
Ek 0-6. Pratik KEP işlemlerine ilişkin örnek uygulama..... 144
Ek 6-7. KEP sistemi ile ileti gönderim işlemleri..... 150
ÖZGÜNLÜK BİLDİRİMİ 155

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Elektronik Ortamda Belgelerin Güvenli Paylaşımı; Ülke Uygulamaları ve Ülkemiz İçin Öneriler
Türü	İdari Uzmanlık
Yazar	Mustafa YILMAZ
Teslim Tarihi	19/03/2013
Anahtar Kelimeler	Elektronik belge, kayıtlı elektronik posta, e-belgenin güvenli paylaşımı, elektronik belge yönetim sistemi
Tez danışmanı	Prof. Dr. Şeref SAĞIROĞLU
Sayfa Adedi	155

Çağımızda hemen herkesin kullanmak zorunda kaldığı Bilgi ve İletişim Teknolojileri (BİT), günlük yaşantımıza sürekli yenilikler ve kolaylıklar sunmaktadır. BİT ayrıca paralelinde bizleri güvenlik zafiyetleri ile de tedirgin etmektedir. Bilgisayar teknolojilerinin iletişim imkânlarının artması, genişleyen ağlar üzerinde dolaşan bilgi ve belgelerin güvenlik riskini de aynı oranda artırmaktadır. Bu çalışmada elektronik ortamda (e-ortam) güvenli belge oluşturma ve elektronik belgeye (e-belge) ilişkin mevzuat ve standartlar ayrıca e-belge paylaşımı için yaygın olarak kullanılan mevcut yöntemler ve altyapılar güvenlik bağlamında incelenmiştir. Çalışmanın sonucunda; Kayıtlı Elektronik Posta (KEP) sisteminin, kamu ve özel sektör ile bireylerin bilgi ve belge paylaşımının güvenliği konusunda gerek yasal güvence altına alması, gerek teknik güvenirliği üst seviyeye taşıması nedenleriyle güvenli e-belge paylaşımı için uygun kullanım aracı olduğu tespit edilmiştir. Dünya ve ülkemizde henüz çok yeni olan güvenli e-belge paylaşım yöntemi KEP'in ülkemizde yaygın kullanımı konusunda, KEP sisteminin düzenleyici ve denetleyici kurumu olan Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) önemli görevler düşmektedir. Bu tez çalışmasında BTK, devlet, özel sektör ve bireyler açısından bazı tespitler ve önerilerde bulunulmuştur.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATION AUTHORITY	
Thesis	Secure Sharing of Electronic Documents, Country Applications and Proposals for Our Country
Type	Administrative Expertise Thesis
Author	Mustafa YILMAZ
Submission Date	19/03/2013
Key Words	electronic document, registered electronic mail, Secure Sharing of electronic document, electronic document management system
Advisor	Prof. Dr. Şeref SAĞIROĞLU
Total Pages	155

ICT, being used nearly by everyone in our age, introduces innovations and facilities to our daily lives. ICT also disturbs us by its security vulnerabilities. While the means of computers to communicate with each other improve, security risk of data and documents flowing over enhancing networks also increase. Creation of secure documents in electronic environment (e-environment), standards and legislation related to electronic documents (e-documents) and methods and infrastructure widely used in electronic document sharing are examined in security ontext in this study.

As a result of this study: Registered Electronic Mail (REM) system is determined as an appropriate method for public-private-citizen electronic documents and data sharing security thanks to legally securing and increasing technical solidity. Information and communication Technologies Authority (ICTA), regulatory body for REM, is supposed to be in charge of widespread usage of REM which is quite new in Turkey and the world at the moment. Besides these some proposals including increasing awareness, methods to be chosen and roles to be played by ICTA is submitted. In this study some indications and suggestions had been made to BTK, public and private sector and individuals.

TEŞEKKÜR

Tez çalışmam için değerli vakitlerini ayıran ve sunmuş olduğu kıymetli katkıları ile çalışmamın bu aşamaya gelmesine destek veren başta tez danışmanım Prof. Dr. Şeref SAĞIROĞLU'na, KEP konusunda sahip oldukları bilgi ve belgeyi benden esirgemeyen Daire Başkanları Cafer CANBAY ve K.Sacid SARIKAYA'ya, Başkanlık Müşaviri Mustafa ÜNVER ve Bilişim Uzmanı Demet KABASAKAL'a, tezime genel katkıları ve şahsıma gösterdikleri anlayıştan dolayı Başkanlık Müşaviri Savaş YILDIRIM, Müdürüm Murat AYDIN, Bölge Müdürü Mustafa GÜNEŞ, İdari Uzman Dr. Süleyman GÜNGÖR, Bilişim Uzmanları Ayşe Gül MİRZAOĞLU, Meltem TURHAN, Özgür ÖZTÜRK, Afşin BÜYÜKBAŞ, M. Salim KETEVANLIOĞLU, İletişim Uzmanı Adil ALAN, mesai arkadaşlarım ve aileme teşekkürlerimi borç bilirim.

TABLOLAR LİSTESİ

Tablo 2.1 ETSI KEP Standardı Dokümanları 45
Tablo 2.2 KEP Sisteminin Uyumlu Olması Talep Edilen ISO/IEC 27002 Güvenlik Özellikleri 49
Tablo 3.1 Yasal Düzenlemeler ve Standartlar 57
Tablo 3.2 Ülkemiz ve Uluslar arası Bazı Standartların Özellikleri 77
Tablo 5.1 Belge paylaşımında kullanılan yöntemlere göre değerlendirme ... 96
Tablo 5.2 KEP GZFT (SWOT) Analizi 101
Tablo Ek 6.1 Anketin 7 nci sorusuna verilen cevapların dağılımı 129
Tablo Ek 6.2 Anketin 5 inci sorusuna verilen cevapların dağılımı 140

ŞEKİLLER LİSTESİ

Şekil 1-1. Belge Yönetim Sistemi Tasarımı 9
Şekil 1-2. Belge Yönetim Sisteminin e-Dönüşümü 10
Şekil 1-3. Belge Yönetim Süreçleri 19
Şekil 2-1. VPN'nin Genel Yapısı 28
Şekil 2-2. İki Uzak Siteyi İnternet Üzerinden Bağlayan Sanal Özel Ağ 30
Şekil 2-3. Güvenli Yuva Katmanı Bağlantısı 31
Şekil 2-4. SSL Bağlantısı ile Güvenlik Göstergeleri 32
Şekil 2-5. SSL'in Çalışma Prensibi 33
Şekil 2-6. Örnek SFTP kullanımı 35
Şekil 2-7. Posta İşleme Servisinin Görevi 38
Şekil 2-8. e-Posta Hizmetinin İş Akışı 39
Şekil 2-9 KEP'in Çalışma Prensibi 46
Şekil 2-10 Kiralık Hat kullanımı 53
Şekil 3-1. Gerçek Kişiler İçin Başvuru Formu 61
Şekil 3-2. Tüzel Kişiler İçin Başvuru Formu 62
Şekil 4-1. e-Yazışma Projesi 80
Şekil 4-2. Şifrelenmiş e-Yazışma Paketi 82
Şekil 4-3. Açılmış e-Yazışma Paketi 82
Şekil 4-4. e-Yazışma Paketi Bileşenleri 83
Şekil 4-5. e-Belge ve bilginin paylaşımına genel bakış 89
Şekil Ek 6-1 Anketin 3 üncü sorusuna verilen cevapların dağılımı 124
Şekil Ek 6-2 Anketin 3 üncü sorusuna verilen cevapların dağılımı 125
Şekil Ek 6-3 Anketin 5 inci sorusuna verilen cevapların dağılımı 126
Şekil Ek 6-4 Anketin 6 ncı sorusuna verilen cevapların dağılımı 127
Şekil Ek 6-5 Anketin 8 inci sorusuna verilen cevapların dağılımı 130
Şekil Ek 6-6 Anketin 11 inci sorusuna verilen cevapların dağılımı 132
Şekil Ek 6-7 Anketin 12 nci sorusuna verilen cevapların dağılımı 133
Şekil Ek 6-8 Anketin 13 üncü sorusuna verilen cevapların dağılımı 134
Şekil Ek 6-9 Anketin 14 üncü sorusuna verilen cevapların dağılımı 135
Şekil Ek 6-10 Anketin 1 inci sorusuna verilen cevapların dağılımı 136

Şekil Ek 6-11 Anketin 2 nci sorusuna verilen cevapların dağılımı 137
Şekil Ek 6-12 Anketin 3 üncü sorusuna verilen cevapların dağılımı 138
Şekil Ek 6-13 KEP Sistemi ilk giriş ekranı görünümü..... 144
Şekil Ek 6-14 KEP Sistemi Kimlik Bilgileri giriş ekranı görünümü..... 145
Şekil Ek 6-15 KEP Sistemi Adres ve İletişim Bilgileri ekranı görünümü..... 146
Şekil Ek 6-16 KEP Sistemi Hesap ve Tarife Seçenekleri ekranı görünümü 148
Şekil Ek 6-17 KEP Sistemi Ödeme Seçenekleri ekranı görünümü 149
Şekil Ek 6-18 KEP Sistemi Kullanıcı Girişi ekranı görünümü..... 150
Şekil Ek 6-19 KEP Sistemi SMS Şifre Doğrulama ekranı görünümü 151
Şekil Ek 6-20 KEP Sistemi İşlem ekranı görünümü..... 152
Şekil Ek 6-21 KEP Sistemi Posta ekranı görünümü 152
Şekil Ek 6-22 KEP Sistemi Yeni Posta ekranı görünümü 153
Şekil Ek 6-23 KEP Sistemi e-İmza ekranı görünümü..... 154

KISALTMALAR LİSTESİ

AAA	Açık Anahtar Altyapısı
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ADSL	Asimetrik Sayısal Abone Hattı (Asymmetric Digital Subscriber Line)
ASCII	Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (American Standard Code for Information Interchange)
ATM	Eşzamansız İletim (Asynchronous Transfer Mode - Modu)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİT	Bilgi ve İletişim Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CEN	Avrupa Standardizasyon Komitesi (European Committee for Standardization)
CNIPA	Kamu Yönetimi Ulusal Bilişim Merkezi (The National Centre for ICT in Public Administration)
DNS	Alan Adı Sistemleri (Domain Name System)
DPT	Devlet Planlama Teşkilatı (Kalkınma Bakanlığı)
e-Belge	Elektronik Belge
EBYS	Elektronik Belge Yönetim Sistemi
e-Fatura	Elektronik Fatura
e-Ortam	Elektronik Ortam

e-Posta	Elektronik Posta
EPCM	Elektronik Posta Sertifikasyon İşareti (Electronic Postal Certification Mark)
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
ESI	Elektronik İmzalar ve Altyapılar
e-Tebligat	Elektronik tebligat
e-Ticaret	Elektronik ticaret
ETSI	Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute)
FR	Çerçeve Röle (Frame Relay)
FTP/SFTP	Dosya Aktarım Protokolü (File Transfer Protocol/Secure File Transfer Protocol)
IMAP	İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol)
IP	İnternet Protokolü (Internet Protocol)
ISS	İnternet Servis Sağlayıcısı
ISO/IEC	Uluslararası Standartlar Örgütü / Uluslararası Elektroteknik Komisyonu (International Standards Organization / International Electrotechnical Commission)
KEP	Kayıtlı Elektronik Posta
KEPHS	Kayıtlı Elektronik Posta Hizmet Sağlayıcı
KPS	Kimlik Paylaşım Sistemi
L2L	Siteden siteye bağlantı (Site to Site)
MCKS	Mobil Cihaz Kayıt Sistemi

MERNİS	Merkezi Nüfus İşleri Sistemi
MIME	Çok Amaçlı İnternet Posta Uzantıları (Multipurpose Internet Mail Extensions)
S/MIME	Güvenli/Çok Amaçlı İnternet Posta Uzantıları (Secure/Multipurpose Internet Mail Extensions)
MHS	Posta İşleme Servisi (Mail Handling Service)
MPLS/IP-MPLS	Çok Protokollü Etiket Anahtarlama (Multi Protocol Label Switch)
NTS	Numara Taşınabilirliği Sistemi
OPC	Açık Paketleme Kuralları (Open Packaging Conventions)
PGP	Oldukça İyi Mahremiyet (Pretty Good Privacy)
PKI	Açık Anahtar Altyapısı (Public Key Infrastructure)
POP	Posta Ofis Protokolü (Post Office Protocol)
PTT	Posta ve Telgraf Teşkilatı Genel Müdürlüğü
RYUUEHY	Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik
S	Sayı
s	Sayfa
SePS	Güvenli elektronik Posta Hizmetleri (Secure electronic Postal Services)
SDH	Eşzamanlı Sayısal Sıradüzen (Synchronous Digital Hierarchy)
SMTP	Basit Posta Aktarım Protokolü (Simple Mail Transfer Protocol)

SSL	Güvenli Yuva Katmanı (Secure Sockets Layer)
STK	Sivil Toplum Kuruluşları
TBD	Türkiye Bilişim Derneği
T.C.	Türkiye Cumhuriyeti
TCP/IP	İletişim Kontrol Protokolü / İnternet Protokolü (Transmission Control Protocol/Internet Protocol)
TDM	Zaman Bölmeli Çoklama (Time Division Multiplexing)
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
TNB	Türkiye Noterler Birliği
TS	Türk Standartları
TSE	Türk Standartları Enstitüsü
TWS	Tahsilât Web Servisi
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UPU	Uluslararası Posta Birliği (Universal Postal Union)
UYAP	Ulusal Yargı Ağı Projesi
VPN	Sanal Özel Ağ (Virtual Private Network)
WDM	Dalga Boyu Bölmeli Çoklama - Wavelength (Division Multiplexing)
WWW	İnternet-Dünyayı Çevreleyen Ağ (World Wide Web)
YPK	Yüksek Planlama Kurulu

GİRİŞ

1960'larda askeri amaçlı, 1970 ve 1980'li yıllarda ise üniversitelerde araştırma amaçlı olarak kullanılan bilgi teknolojileri, bugün gelinen noktada teknoloji ile iletişimin yaygınlaşması sonucu bilgi ve iletişim teknolojilerine (BİT) evirilerek ekonomik ve sosyal hayatımızın hemen her alanında yerini almıştır. Bilgi Çağı olarak tanımlanan içinde bulunduğumuz çağda, toplumlar ve devletler mevcut yapılarını daha önce görülmemiş bir hızda kaçınılmaz olarak değiştirmektedir.

BİT'de yaşanan gelişmeler, kurum ve kuruluşların iş süreçlerinde değişimlere neden olmuştur. Bu değişimin en önemli göstergelerinden birisi, kurum ve kuruluşlar tarafından sunulan hizmetlerin her geçen gün artan ölçüde elektronik uygulamalara (e-devlet, e-ticaret, e-eğitim vb) konu olmasıdır. Bu gelişmelere bağlı olarak, kurum ve kuruluşlar da iş süreçlerini e-ortama taşımaya ve resmi yazışmalar, tebligatlar, başvurular, ihtarnameler ve sözleşmeler de dâhil olmak üzere e-ortamda çok sayıda bilgi ve belge üretmeye başlamıştır.

23/01/2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ile güvenli elektronik imza (e-imza) tanımlanmış ve güvenli e-imza ile imza altına alınmış olan belgeler ıslak imza ile aynı hukuki geçerliliğe sahip kılınmıştır. Böylece kurum ve kuruluşların kendi bünyelerinde ve diğer kurum ve kuruluşlar ile yapacakları bilgi ve belge paylaşımında, kâğıt ortam yerine e-ortamda[1] oluşturulan e-belgelerin[2] de yazılı belgelere eşdeğer nitelikte olması sağlanmıştır. e-Dönüşüm Türkiye

---

[1] 02/12/2004 tarihli ve 25658 sayılı Resmi Gazete'de yayımlanan Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelikte tanımlanan *elektronik ortam,* bu çalışmada *e-ortam* olarak ifade edilmiştir.

[2] 02/12/2004 tarihli ve 25658 sayılı Resmi Gazete'de yayımlanan Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelikte tanımlanan *elektronik belge*, bu çalışmada *e-belge* olarak ifade edilmiştir.

Projesi, 2005 Yılı Eylem Planının[3] 37 nci maddesinde, *"elektronik ortamlarda üretilecek, kayıt altına alınacak, başka birimlere ya da kurumlara iletilecek, saklanacak ya da gerektiğinde imha edilecek elektronik bilgi ve belgelerin kayıt, iletim, paylaşım, imha ve güvenlik açılarından tabi olacakları usul ve esaslar ile kurumlarda oluşturulacak elektronik kayıt sistemlerinin birbirleriyle uyumlu işlemesi ve etkin bir şekilde yönetilmesine ilişkin asgari standartların belirlenmesi"* öngörülmüştür. Söz konusu eylem, Türk Standartları (TS) 13298 numaralı Elektronik Belge Yönetimi Standardı'nın Türk Standartları Enstitüsü (TSE) tarafından 29/06/2009 yılında yayımlanmasıyla tamamlanmıştır. Böylece e-ortamda üretilen bilgi ve belgelerin belirli standartta üretilmesi, yönetilmesi ve arşivlenmesine ilişkin esaslar belirlenmiştir.

Bununla birlikte e-ortamda üretilen bilgi ve belgenin yasal zorunluluk, maliyet düşüklüğü, iş ve işlemlerin hızlı bir şekilde gerçekleştirilmesi gibi sebeplere paralel olarak, üretilen her belgenin güvenli bir şekilde kaydedilmesi, kullanılması, saklanması ve paylaşılması daha fazla önem kazanmaya başlamıştır. Paylaşılan bu belgelerin "belge özelliklerinin"[4] bir bütün olarak bozulmadan varlığını ve güvenliğini koruyabilmesi, paylaşım aşamasındaki taraflar açısından da önemlidir. Bu önem, taraflar arasında etkin bilgi ve belge paylaşımının sağlanabilmesini, kurumsal bilgi ve belgelerin önceden belirlenen bir sistem içerisinde düzenlenmesini zorunlu kılmaktadır. Bu nedenle, elektronik hizmetleri kullanan ya da e-ortamdaki bilgi ve belgelerini paylaşan tarafların, e-ortamda işlemleri güvenli bir şekilde gerçekleştirmek ve muhataplarıyla karşılıklı güveni sağlamak için uygun güvenlik kontrollerine ve mekanizmalarına sahip olması önem arz etmektedir.

---

[3] 27 Şubat 2003 tarihinde yayımlanan 2003/12 sayılı Başbakanlık Genelgesi ile başlatılan e-Dönüşüm Türkiye Projesi, 2003 yılı sonunda hazırlanan Kısa Dönem Eylem Planının uygulanmasıyla hayata geçirilmiştir. Kısa Dönem Eylem Planının zamanında bitirilemediği için 2005 yılına aktarılan eylemler ile yeni eylemleri ihtiva eden orta vadeli Bilgi Toplumu Stratejisi hazırlanıncaya kadar uygulanması amacıyla bir yıl süreli 2005 Eylem Planı, 2005/05 sayılı Yüksek Planlama Kurulu kararı olarak 01/04/2005 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

[4] Belge özellikleri: Tanımlanabilirlik, bütünlük, onay ve kayıt bilgisi, yapısal özellikler, üretim sorumluluğu ve mülkiyet, teknolojik özellikler (Kandur, 2006, s.51-57)

Bu çerçevede e-belgenin, e-ortamda paylaşımı için bugün dünyada; Sanal Özel Ağ (VPN), Güvenli Yuva Katmanı (SSL), Kiralık Hat, Dosya Aktarım Protokolü (FTP) ve e-Posta gibi yöntemler yaygın olarak kullanılmaktadır. Ancak söz konusu yöntemler güvenli e-belge paylaşımına ilişkin çeşitli kriterleri sağlamaları açısından farklılaşmaktadır.

e-Ortamda bilgi ve/veya belge paylaşımı için yaygın olarak kullanılan elektronik posta (e-posta), iş ve işlemlerin kesintisiz devam etmesine olanak sağladığı için önemli bir araç haline gelmiş olmakla birlikte, e-postaya güvenin sağlanabilmesi için ilave güvenlik hizmetlerine gereksinim duyulmaktadır. Bu nedenle bazı Avrupa Birliği (AB) üyesi ülkelerin öncülüğünde e-ortamda iletilen e-posta mesajlarının kaynak doğrulamasını ve teslim edildiğine dair delili sağlayan bir sistem olarak Kayıtlı Elektronik Posta (KEP) sistemi ve uygulamaları geliştirilmiştir.

e-Ortamda üretilen bilgi ve belge miktarının her geçen gün artması ve bu belgelerin kişiler ve kurumlar arasında hukuki geçerliliğe sahip şekilde paylaşılmasının sağlanması konusu ülkemizde de "e-Dönüşüm Türkiye İcra Kurulu"nun gündemine gelmiş ve çözüm olarak KEP sistemi üzerinde durulmuştur. Ayrıca 2010 yılında Kalkınma Bakanlığı tarafından başlatılan e-yazışma projesinde Kamu kurum ve kuruluşlarının kendi aralarında veya gerçek ve tüzel kişilerle yaptıkları yazışmaların KEP sistemi vasıtasıyla iletilmesi öngörülmektedir.

14/02/2011 tarihli ve 27846 sayılı ve Resmi Gazete'de yayımlanan 6012 sayılı Türk Ticaret Kanun'un 18 inci maddesi üçüncü fıkrasında; *"Tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar noter aracılığıyla, taahhütlü mektupla, telgrafla veya güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile yapılır"* ifadesi ile 1525 inci maddesi ikinci fıkrasında; *"Kayıtlı elektronik posta sistemine, bu sistemle yapılacak işlemler ile bunların sonuçlarına, kayıtlı posta adresine sahip gerçek kişilere, işletmelere ve*

şirketlere, kayıtlı elektronik posta hizmet sağlayıcılarının hak ve yükümlülüklerine, yetkilendirilmelerine ve denetlenmelerine ilişkin usul ve esaslar Bilgi Teknolojileri ve İletişim Kurumu tarafından bir yönetmelikle düzenlenir." ifadeleri ile KEP hizmeti ülkemizde resmiyet kazanmıştır.

Akabinde, Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 16/05/2012 tarihli ve 28294 sayılı Resmi Gazete'de Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, BTK'nın internet sayfasında Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul ve Esasları düzenleyen 06/06/2012 tarihli ve 2012/DK-15/259 sayılı Kurul Kararı yayımlanmıştır.

Günümüzde hemen herkes, her türlü veriyi e-ortamda düşük bir maliyet ve kolaylıkla edinebildiği yaygın olan standart e-posta uygulaması ile paylaşmaktadır. e-Posta, özellikle devlet uygulamalarında ve ticari alanda yoğun bir şekilde kullanılmaya da başlanmıştır. e-Postanın, göndericisi ve alıcısının kimliklerinin kesin olarak belirlenememesi, teknik ve hukuki geçerliliğe sahip olamaması, iletinin postada kaybolması, yetkisiz kişilerin kolay bir şekilde elde etmesi veya değiştirmesi gibi sorunlar ancak ilave güvenlik önlemleri ile aşılabilir. KEP genel anlamda e-postaların alıcısının ve göndericisinin kimliklerinin doğrulanmasına, aynı zamanda gönderildiğine, alındığına ve okunduğuna ilişkin hukuki delillerin elde edilmesine imkân veren bir uygulamadır. Dolayısıyla KEP sayesinde e-posta iletişimi güvenli hale geldiği gibi aynı zamanda da hukuki geçerlilik kazanmaktadır. Bu nedenle e-ortamda özellikle hukuki geçerliliğe sahip bilgi ve belge paylaşımında KEP sisteminin kullanılması yerinde bir karar olacaktır.

e-Ortamda bilgi ve e-belge paylaşımında yaygın olarak kullanılmakta olan VPN, SSL, VPN özel ağ, kiralık hat gibi uygulamalar aynı zamanda e-posta

ve KEP sistemi türü uygulamaların işletilmesinde altyapı olarak önemli bir göreve sahiptir (Şekil 4-5).

Bu çalışmanın amacı, üstesinden gelinmesi gereken bir sorun olan, e-belgelerin güvenli paylaşımı düşüncesinden hareketle; dünyada ve ülkemizdeki mevcut yöntem ve uygulamaların düzenleme ve uygulama boyutlarını incelemek, bu konuda ülkemiz ve BTK adına farkındalık oluşturulması ve tercih edilmesi gereken yönteme ilişkin bazı öneriler sunmaktır.

Çalışmanın birinci bölümünde, e-ortamın temel taşı olan e-belge kavramı, kriterleri, yaşam döngüsü ve oluşturulması gereken ortamı oluşturan Elektronik Belge Yönetim Sistemi (EBYS) hakkında bilgiler yer almaktadır.

İkinci bölümde, günümüzde yaygın olarak kullanılan e-belgenin paylaşım yöntemleri ve bileşenleri incelenmektedir.

Üçüncü bölümde, ülkemizde ve dünyada e-belgeye ilişkin standartlara değinilmiş olup ayrıca ülkemizde e-ortamda yapılan iş ve işlemler hakkında yayımlanmış olan mevzuat ele alınmıştır.

Dördüncü bölümde, ülkemizde kamu kurum ve kuruluşları tarafından e-ortamda gerçekleştirilen iş ve işlemlere ilişkin büyük çaplı uygulamaların yanında BTK'da kullanılmakta olan bilgi ve e-belge paylaşımına ilişkin bazı uygulamalara değinilmiştir. Ayrıca bazı ülkelerin güvenli e-belge paylaşımı uygulamaları hakkında incelemelere yer verilmiştir. Bunlara ilaveten e-ortamda e-belgelerin güvenli paylaşımı konulu anket çalışmasının değerlendirmesi yapılmıştır.

Son olarak "Sonuç ve Öneriler" bölümünde tez çalışmasında elde edilen sonuçlar değerlendirilmiş ve BTK'ya yönelik önerilere yer verilmiştir.

1. ELEKTRONİK ORTAMDA GÜVENLİ BELGE OLUŞTURULMASI

Bilgi günümüzde önemli bir güç haline gelmiştir. Bilginin, BİT'deki gelişmelerin desteği ile daha sistematik yönetilmesi için e-ortamın yoğun bir şekilde kullanılması gerekmektedir (Önaçan vd., 2012, s.13).

Günümüzde birbirini besleyen iki kaynak haline dönüşen bilgi ve BİT ile pek çok alanda yaşanan değişim süreci; üretilen belgelerin geleneksel kâğıt ortamından geri dönülemeyecek bir şekilde e-ortama aktarılmasını, yaygın kullanımıyla ifade edecek olursak, kâğıt belgelerin e-belgeye dönüşmesini mecbur kılmaktadır.

e-Belgenin kağıt belgeye kıyasla hızlı ulaşımı, kolaylıkla sınıflandırılması, aynı belge üzerinde birden fazla kişinin aynı anda çalışabilmesi, kağıt ve diğer büro malzemelerinde tasarruf sağlaması gibi pek çok avantajı olmasına rağmen e-belgelerin güvenliğini sağlamanın, kağıt belgelere oranla daha zor olduğu çok aşikardır.

1.1. e-Belge Nedir

e-Belgeler, e-ortamda oluşturulan aynı zamanda e-ortamda saklanabilen ve kullanılabilen belge olarak tanımlanmaktadır (Odabaş, 2009, s.413). Diğer bir tanıma göre ise e-Belge, genellikle bilgisayar teknolojileri veya diğer elektronik cihazlar yardımı ile e-ortamda kurum ve kuruluşların faaliyetleri sonucunda üretilen, kullanılan, saklanan veya imha edilen belgelerdir (Aydın ve Özdemirci, 2011, s.106).

Geleneksel devlet hizmetlerinin tamamı e-ortamdan sunulmaya başladığında yani e-devlet modeline geçildiğinde ulusal, kurumsal veya kişisel olarak alınan kararlar, uygulanan süreçler ve varılan anlaşmaların en önemli ve tek delili e-belgeler olacaktır (Altın, 2008, s.152).

e-Belgeler, e-ortamda hazır yazılımlarla üretilen belgeler olabileceği gibi, sonradan e-ortama çeşitli elektronik araçlarla aktarılarak oluşturan belgeler de olabilir. Kâğıt belgelerin tarayıcı aracılığı ile e-ortama aktarılması, sesli ve hareketli belgelerin, ilgili donanım ve yazılımın yardımı ile e-ortama aktarılması gibi hususlar buna örnek verilebilir.

e-Devlet uygulamasının bir bütün olarak oluşturulması bakımından e-belge, hayati önem taşımaktadır. e-Devlet uygulamasının istenilen faydaya ulaşabilmesi için e-belge'nin başta kamu olmak üzere toplumun tüm kesimlerince güvenli bir şekilde paylaşılıyor olması gerekmektedir.

1.1.1. e-Belgenin üretim ortamları

02/12/2004 tarihli ve 25658 sayılı Resmi Gazete'de yayımlanan Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmeliğin 4 üncü maddesinin (e) fıkrasında *Elektronik belge: Elektronik ortamda oluşturulan, gönderilen ve saklanan her türlü belgeyi,* şeklinde ifade edilmiştir. Aynı yönetmeliğin aynı maddesinin (d) fıkrasında ise *Elektronik ortam: Belge ve bilgilerin üzerinde bulunduğu her türlü bilgisayarı, gezgin elektronik araçları, bilgi ve iletişim teknolojisi ürünlerini,* şeklinde ifade edilmiştir.

Elektronik belge, elektronik araçlar aracılığı ile üretilen ve bu araçlar üzerinde kullanılabilen belgelerdir. e-Belgenin üretimi, günümüz e-belge üretim aygıtları olan e-ortam yani bilgisayar, bilgisayara bağlı harici donanım (tarayıcı, ses ve görüntü donanımları, optik okuyucular v.s.) gibi bilgi ve iletişim teknolojisi ürünleri ile gerçekleştirilebilir. e-Belge günümüzde yoğun olarak bilgisayarlar üzerinde bulunan hazır yazılımlar (word, excel gibi) ile üretilerek güvenli e-imza ile imzalanması gibi çeşitli ilave uygulamalara tabi tutulabilmektedir.

1.2. e-Belge Yönetim Süreci

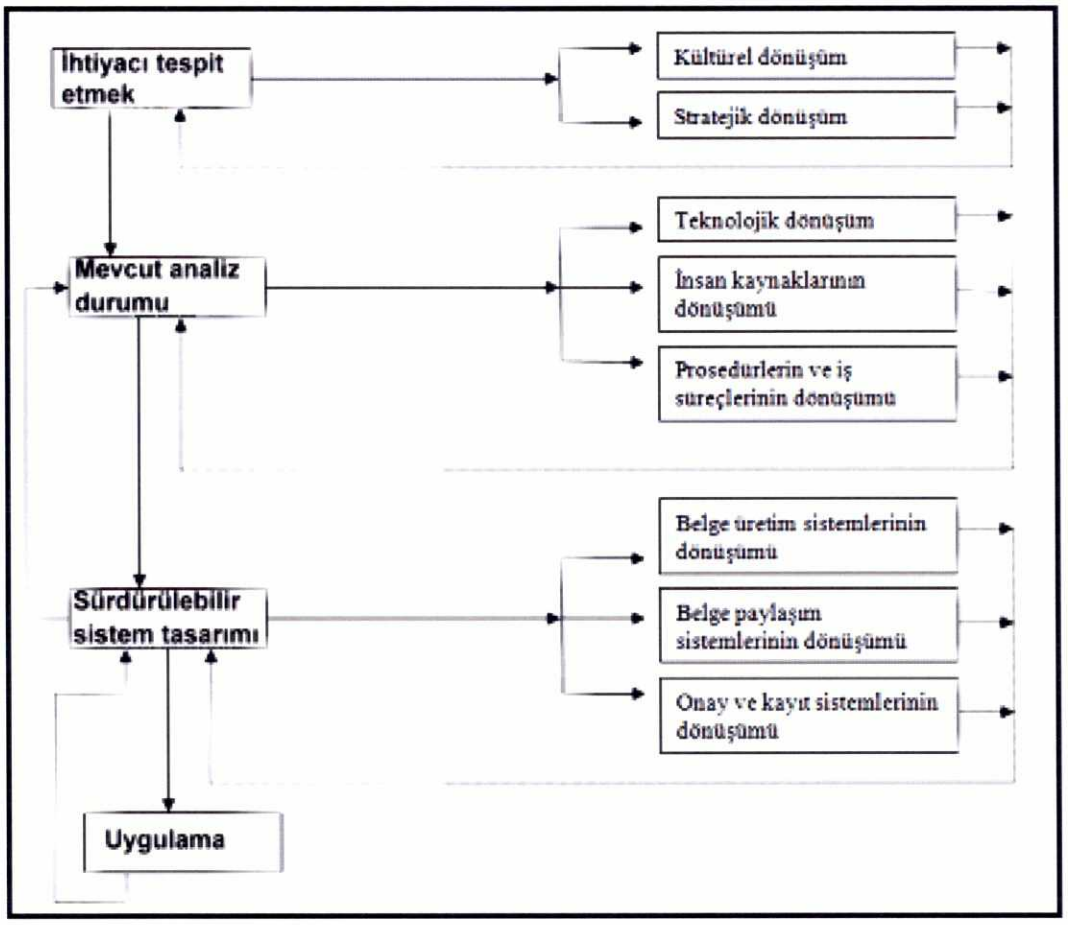
e-Belgelerin e-ortamda etkin yönetimi ve kontrolü için bu belgelerin üretiminden önce, EBYS'nin oluşturulması önem arz etmektedir. EBYS'nin tasarım aşamasında her bir e-belgenin oluşturulması ve tanımlanmasına ilişkin:

- ✓ Muhafaza süreleri
- ✓ İmha tarihleri
- ✓ Erişim sınırları
- ✓ Erişim yetkilileri
- ✓ Güvenli saklama
- ✓ Güvenli erişim
- ✓ Güvenli paylaşım

gibi konularda kararların sistemli bir şekilde alınması gerekmektedir (Aydın ve Özdemirci, 2011, s.107).

Etkin ve yönetilebilir bir belge yönetim sistemi tasarımı için her kurum veya kuruluş, kendi iç dinamiklerinden kaynaklanan farklılıklar açısından ya da belirli bir marka veya ürüne bağımlı kalmamak ve özel sektör rekabetini engellememek adına; kendi yapısına göre modelleme ile süreç planlaması yapmalı, uygun yazılım ve donanımları kullanmalıdır. Doğası gereği çok yönlü iş, işlemler ile çıktıları bünyesinde barındıran e-devlet uygulaması, EBYS aracılığıyla kuralları önceden belirlenmiş e-belge disiplinleri ile yönetilmelidir. Bu durumu özetleyen belge yönetim sistem tasarımı, Şekil 1-1'de gösterilmiştir.

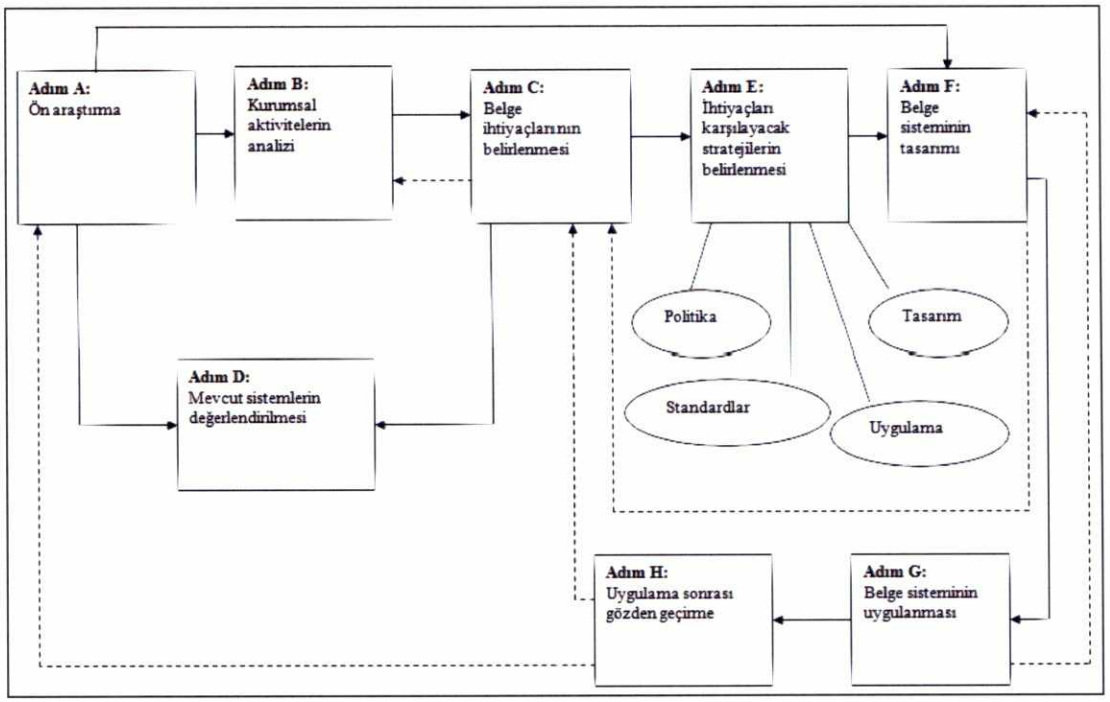
Şekil 1-1. Belge Yönetim Sistemi Tasarımı



Kaynak : Kandur, 2008, s.7

Belge yönetim sisteminin geleneksel yöntemlerden, e-ortama dönüşümü, Şekil 1-2'de yer almaktadır.

Şekil 1-2. Belge Yönetim Sisteminin e-Dönüşümü



Kaynak : Kandur, 2008, s.8

TS 13298 Elektronik Belge Yönetimi Standardı, kurum ve kuruluşlarda bilgi ve belge üretim süreçlerini, yönetim süreçlerine dâhil eden bir modeli ortaya koyan sistem kriterlerini içermektedir (Özdemirci ve Yalçınkaya, 2009, s.3).

1.3. EBYS ve e-Belge Kriterleri

2007'de yayımlanmış, 2009 yılında güncellenmiş olan TS 13298 Elektronik Belge Yönetimi Standardı'nda *Elektronik belge yönetimi: Kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinden kurum faaliyetlerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetmek* şeklinde tanımlanmaktadır.

Geleneksel yöntemlerle kâğıt ortamında üretilen ve yönetilen belgeler, günümüzde artık kaçınılmaz bir şekilde yerini e-belgelere bırakmaktadır. Gerek e-ortamda üretilen gerekse başka ortamlarda üretilerek e-ortama

aktarılan belgelerin yönetim şekli geleneksel yöntemlerden farlılık arz etmektedir. Üretim ortamının değişikliği ile belgelerin yönetimi içinde başlayan bu yeni süreci yönetebilmek, gereklilikleri doğru analiz edilmiş ve sağlam olarak yapılandırılmış bir EBYS ile gerçekleşebilir (Altın, 2008, s.283).

EBYS, kurumsal iş süreçlerine dayalı olarak e-belgelerin oluşturulması, kurum içinde üretilen veya kurum dışından alınan e-belgelerin kayıt altına alınması, korunması, dağıtımının yapılması, kullanılması, arşivlenmesi, imha edilmesi gibi işlemleri uygulayabilmek için lüzumlu olan her çeşit teori ve uygulamayı içeren oldukça büyük bir yapıdan oluşmaktadır (Odabaş, 2009, s.416).

EBYS, özetle; kâğıtsız çalışma ortamı açısından, kurum ve kuruluşların faaliyetleri sonucu üretilmiş bilgilerin yazılı veya görsel çıktılarının yani belgelerinin değerlendirilmesi, kullanımı, paylaşılması, ulaşılması ve yaşam döngüsü süresince sistemli bir şekilde e-ortamda saklanması gibi iş ve işlemlere yön veren elektronik denetim ve yönetim faaliyetleridir (Güler ve Ömürgönülşen, 2011, s.225).

Etkin ve yönetilebilir bir EBYS ile e-belgelerin, e-ortamda;

- ✓ Üretilmesi
- ✓ Onay sonrası e-imza ile imzalanması
- ✓ Sürüm takibi
- ✓ Saklanması
- ✓ Ağ ile ilişkili olarak dağıtımı
- ✓ Otomatik arşiv işlemlerinin yapılması ve imhası
- ✓ Güvenlik takibinin yapılması
- ✓ Raporlanması
- ✓ Başka EBYS'ler ile entegrasyonu

gibi ihtiyaçların temini hedeflenmelidir (Önaçan vd., 2012, s.14).

e-Belgenin, belge vasfını kazanabilmesi için bazı kriterlere ve özelliklere göre oluşturulması gerekmektedir. Kâğıt ortamlarda oluşturulan belgeler yasa veya diğer düzenlemelere uygun olması, içerisinde gerekli bilgileri barındırması ve imzalanmış veya mühürlenmiş olması gerekmektedir. Söz konusu durum e-belgeler için de geçerlidir. e-Belgelerin hukuki, yönetim ve ispat bakımından belge kimliğini edinebilmesi için;

- ✓ Özgünlük (e-belgenin orijinal halinde bulunan bütün özelliklerini muhafaza etmesi),
- ✓ Güvenirlik (e- belgenin taşıması gereken özellikleri ve bu özellikleri uygulamaya aktarma şeklini gösteren yasalar, politikalar, programlar, standartlar tamamıyla uyum içinde olmalıdır),
- ✓ Bütünlük
- ✓ Kullanılabilirlik (e-belgenin e-devlet uygulaması başta olmak üzere, halen ve gelecekte kullanılacak sistem ve uygulamalarla çalışabilir olması)

şeklinde ifade edilen dört temel özelliği taşıması gerekmektedir. Bu özelliklere sahip e-belgelerin, yaşam döngüsünü tamamlayabilmesi ve kurum ve kuruluşların beklentilerine cevap verebilmesi için etkin ve güvenli bir sistem ile yönetilmesi ancak EBYS ile sağlanabilir (Yıldız, 2010, s.6).

Altın, EBYS'nin önemini şu şekilde vurgulamaktadır: e-Devlet sosyal, sağlık, hukuk, ticaret gibi pek çok alanda değişimleri ve dönüşümleri beraberinde getiren büyük bir yapılanmadır. Toplumun tamamını ilgilendirdiği için yapılacak olası bir hata, telafisi mümkün olmayan sonuçlar doğurabilir. Bu sebeple, e-devlet yapısını oluşturmanın anlamı sadece bir internet sitesi oluşturarak e-ortamda e-belge üretmek ve kullanmak değildir. Hizmet sunumuna geçilmeden evvel altyapı çalışmaları konusunda titizlik gösterilmelidir. Altyapı çalışmalarında öncelikle ele alınması gerekli konular içerisinde bilginin güvenliği ile bütünlüğünü sağlayan e-imza ile e-belge yönetimi bulunmaktadır (Altın, 2008, s.152).

BİT sayesinde bilginin hızla çoğaldığı ve eş zamanlı olarak aynı hızla eskidiği bir zaman dilimi yaşanmaktadır. Bilgi, e-belgeler üzerinde oluşturulduktan sonra güncelliğini yitirmeden ilgili ve yetkili kişilerin kullanımına sunulmalı, güvenli bir şekilde kurum içinde ve dışındaki muhataplarıyla paylaşılabilmeli ve kurumsal hafıza açısından değer ifade eden e-belgeler önemine göre ayıklanarak imha edilebilmeli veya sonsuza kadar saklanabilmelidir.

Bilgi, kurum ve kuruluşlar için en önemli varlıktır. Kurum ve kuruluşların değerleri ve kimlikleri, sahip oldukları veya ürettikleri bilgileri ile ölçülmekte ve belirlenmektedir. Artık kamu kurumları ve kuruluşları yönettikleri bilginin oldukça büyük bir bölümünü e-ortama aktarmış durumdadır. Böylece BİT'in önemi her geçen gün artmaktadır. BİT'in yaygın kullanımı, aynı zamanda bilginin karşılaşacağı riskleri de beraberinde getirmektedir. Kurum ve kuruluşların elinde bulundurdukları bilgi ve e-belgelerin güvenliğine dair tedbirlerin alınmasını kaçınılmaz kılmaktadır. Kurum ve Kuruluşlarca oluşturulan, işlenen, kullanılan, paylaşılan, arşivlenen ve imha edilen bilgi ve e-belgeler ile karşılıklı kurum ve kuruluşlar arası paylaşılan bilgi ve e-belgeler gizliliği, bütünlüğü ve erişilebilirliğini muhafaza etmek güvenliğin birinci hedefidir. Bilgi Güvenliği Yönetim Sistemi (BGYS) bu birincil hedefi yerine getirmek için tasarlanmıştır. e-Belge ve bilgi güvenliğinin temini, güvenlik önlemlerinin tespit edilmesi ve uygulamaya konulması ile sınırlandırılamaz. Daima yeni güvenlik zafiyetleri ve saldırılar aynı zamanda bilgi sistemlerinde kesintisiz devam eden teknolojik gelişmeler nedeniyle ortaya çıkan değişiklikler dikkate alınarak güvenliğin düzenli bir şekilde sağlanması, lüzumu halinde güncellemeler ve değişiklikler yapılması mecburi bir hal almaktadır. Bilgi ve e-belgenin güvenliğini sürekli sağlayabilmek için, bütün bu uygulamalar, gereksinimler ve kaynaklar dikkate alınarak etkili ve verimli olarak yönetilmelidir. Söz konusu yönetim ise BGYS ile gerçekleşebilir. Bu nedenle bütün kurum ve kuruluşlarda BGYS kurulmalıdır (Devlet Planlama Teşkilatı (DPT), 2009, s.28-29).

EBYS;

- ✓ e-Belgelerin değiştirilmesini önler
- ✓ e-Belgelerin yok edilmesini önler
- ✓ Mutlaka saklama planlarına sahip olmalıdır
- ✓ e-Belgeler sadece saklama planlarına uygun olarak denetim altındaki ortamlarda imhası yapılır
- ✓ Gündelik faaliyetlerin yapılması ile birlikte kurumsal belleğin muhafazası ve kurumsal işlemlere delil sağlayan e-belgelerin güvenirliğinin teminine yöneliktir (Yılmaz, 2013, s.2).

1.3.1. Tanımlanabilirlik

e-Belgenin tanımlanabilirliği; üreticisi, yazarı, alıcısı ve e-belgeye ilişkin tarih verilerinin kayıt altında tutulması ile sağlanır. EBYS, e-belgenin bütünlüğünü muhafaza etmeli ve gerek kullanım aşamasında gerekse e-belge bütünlüğü sorgulandığında, bütünlüğün bozulmadığını ispat edebilmelidir (Özdemirci ve Yalçınkaya, 2009, s.7).

Bir belgenin tanımlanabilirlik bilgileri hiçbir zaman bir başka belgede bulunmamalıdır. Çünkü belge bazında sorgulama ile ulaşım, görüntüleme, arşivleme gibi işlemlerde tanımlanabilirlik bilgilerini oluşturan belge üreticisi, yazarı, alıcısı ve tarih bilgilerinden faydalanılır. Dolayısıyla e-belgenin EBYS içerisinde işlem görebilmesi için tanımlanabilirliği gereklidir.

1.3.2. Onay ve kayıt bilgisi

EBYS, üretilen veya e-ortama aktarılan belgelerin, ilgilisi tarafından onaylanması ve kurumsal kayıt sistemi içerisinde yer alması imkânını sağlayacak teknolojileri içermelidir. Eğer herhangi bir sebeple teknik açıdan bu mümkün değilse, söz konusu bağımsız sistemlerle bütünleşmiş çalışabilme yeteneğine sahip olmalıdır. Bununla birlikte bu sistemlerin yasa ve standartlara uygun olmasının sağlanması gereklidir. Geleneksel evrak

yönetim uygulamalarında belgelerin hukuki geçerliliği, o belgelerin yetkililerince imzalanması ve evrak kayıt uygulamasında yer alması ile sağlanırken (Kandur, 2006, s.56), EBYS'lerde e-belgenin hukuki geçerliliği onay veya e-imza uygulamalarını destekleyecek altyapı sayesinde sağlanmaktadır. Bu nedenle kurum ve kuruluşların organizasyon yapılarında belirlenmiş onay mekanizmaları ve imzaya yetkili kişilerin bilgileri önceden EBYS içerisinde tanımlanmalı ve kullanılan donanım, yazılım ve yetkili bilgileri kesintisiz bir şekilde kayıt altına alınmalıdır.

1.3.3. Bütünlük

Odabaş, (2006, s.129) e-belgelerde bütünlüğü; "e-belgenin içerik, bağlam, yapı ve sunumdan oluşan dört unsurundan tümüne sahip olması" şeklinde tarif etmektedir.

e-Belge ile birlikte e-belge hakkında yaşam döngüsü içerisinde izlenen ve kaydedilen her olayın bilgi bütünlüğü açısından korunması, taşındığı başka ortamlarda sistem farklılıklarının dikkate alınarak bilgi kaybının yaşanmaması için tek bir sisteme bağımlı kalınmayacak şekilde oluşturulmasına dikkat edilmesi gerekmektedir.

1.3.4. Yapısal özellikler

Kandur, e-belgenin yapısal özellikleri konusunda EBYS'nin önemine işaret ederek belgenin üretimi aşamasında üretici tarafından oluşturulan, kullanıcılarca görülmesini istediği sunum, biçim ve dosya formatından oluşan özelliklerinin, EBYS tarafından korunması gerektiğinin altını çizmektedir (Kandur, 2006, s.57).

e-Belge, kullanım amaçlarına göre düz metinler, çizim, resim, sunum, video gibi farklı tür ve yapılarda üretilebilmektedir. Bununla birlikte her belge içerisinde hazırlayıcısı tarafından oluşturulmuş, metin içerisinde bir kelimenin kalın yazılması, sunum içerisinde bir karakterin hareketli olması, resim

içerisinde renk tonunun farklılığı gibi bazı özellikler de bulunabilmektedir. Bu türde olan e-belgelerin yapısal özelliklerinin EBYS tarafından olduğu gibi korunmasının sağlanması gereklidir.

1.3.5. Teknolojik özellikler

EBYS, e-belgelerin üretilmesine, iletilmesine, depolanmasına ve kullanılmasına imkân sağlayan teknolojik özelliklerini kayıt altına almalıdır. Bunlar donanım, yazılım, veri ve dosya formatı, sistem yönetimi başlıkları altında bulunan detayları içermektedir (Kandur, 2006, s.57-58).

Gerek sistem, gerekse yazılım eskimelerinden veya başka nedenlerle yapılan donanım ve yazılım değişiklikleri neticesinde önceden üretilen bilgi ve belgelerin bütünlüğünün bozulmaması veya kaybolmaması için ilk kullanım anından itibaren ana bellek, veri depolama üniteleri, işlemci gibi donanım parçalarının model, miktar ve kapasitesi gibi teknolojik özelliklere ilişkin değişiklik titizlikle kaydedilmelidir. Uygulama yazılımları, işletim sistemi yazılımları, güvenlik yazılımları gibi her çeşit yazılım üzerinde yapılan güncelleme ya da başka bir yazılıma geçişin bütün aşamaları da kayıt altında tutulmalıdır. Yazılımda güncellemeler veya değişiklikler durumunda da, eski e-belgelerin erişilebilirliği mutlaka göz önünde tutulmalıdır.

1.3.6. e-Belge güvenliğinin sağlanması

e-imza, e-belgenin özgünlüğü, bütünlüğü ve kim tarafından onaylandığı gibi güvenlik unsurları açısından vazgeçilmez bir yardım sunmaktadır. Çünkü e-imzanın kendisi elektronik veriye iliştirilen veya mantıksal bir bağlantısı bulunan, kimlik teyidinin yapılması amacıyla kullanılan elektronik bir veridir. Islak imzanın sahip olduğu kanıtlayıcılığa benzer şekilde herhangi bir e-belgeye eklenen imzalama verisi sayesinde, belgeyi imzalayan kişiye ilişkin kimlik bilgilerinin, belgenin içeriğinde değişiklik yapılmadığının ve belgenin zaman kayıtlarının doğrulanması mümkün olmaktadır. Bir e-belgeye hukuki

geçerlilik kazandırılabilmesi için o belgenin Nitelikli Elektronik Sertifikaya dayanılarak üretilen Güvenli Elektronik İmza ile imzalanması gereklidir (TÜBİTAK, 2008).

e-İmza sadece bir altyapıdan oluşmaktadır. e-İmzanın, uygulamalarda işlerlik kazanabilmesi için mevcut yapıya uyum sağlamasına yardımcı olacak ilave yazılımlara ihtiyaç bulunmaktadır. Örneğin EBYS'de e-imzanın işlerlik kazanabilmesi için öncelikle kurum ve kuruluşta bilgi ve belge üretici faaliyetlerin e-ortama aktarılması, ardından e-imza ile çalışabilir duruma getirilmesi zorunludur (Karakoçak vd., 2006, s. 11).

e-Belgelerde, hukuki açıdan içeriğinin sonradan değiştirilip değiştirilmediğinin tespiti önemli bir sorun olarak ortaya çıkmakta olup e-belgelerin yargılamada kanıt olarak kullanılmasına da engel teşkil etmektedir. (Erturgut, 2003, s.66). Söz konusu sorun e-imza uygulaması ise çözüme ulaşmıştır.

Belge yapıları farklılık arz etse de, imza altına alınması ile e-belge geleneksel belge kadar hukuki geçerlilik ve oluşacak sorumlulukların kanıtı olacaktır. Bu bakımdan güvenli e-imza, sağladığı geçerlilik açısından bir kâğıt üzerinde oluşturulan geleneksel ıslak imza gibidir. Tek farkları kâğıt veya e-ortamda olmalarıdır (Ahi, 2004).

e-Belgelerin kimlik tespitleri e-imza yardımıyla gerçekleştirilir. Bu yöntem ile e-belgenin kimliğinin anlaşılması, güvenirliğinin ve orijinalliğinin temini ile birlikte ağ üzerinden iletilmesi, kullanımı ve saklanması esnasında güvenliğin sağlanması hedeflenmektedir (Çiçek, 2011, s.89).

e-Belge güvenliği için belgenin özellikleri şöyle tanımlanabilir: EBYS içerisinde işleme tabi tutulabilmesi, ana belgenin eklentileri ile birlikte kayıt bilgisi, bütünlüğü, onay ve yazarı, oluşturulma tarihi gibi, yapısal özellikleri ve teknolojik özellikleri kayıt altına alınmış ve korunmuş olmalıdır.

e-Belge yönetimi ile geleneksel belge yönetimi arasında dikkat çeken fark veri güvenliğidir. e-Belge yönetimi kapsamında muhafaza edilen belgelerin yaşam süreçleri boyunca içerik, biçim ve ilişkisel açıdan bütünlüğünün muhafaza edilerek yönetilmesi gerekir (Altın, 2008, s.283).

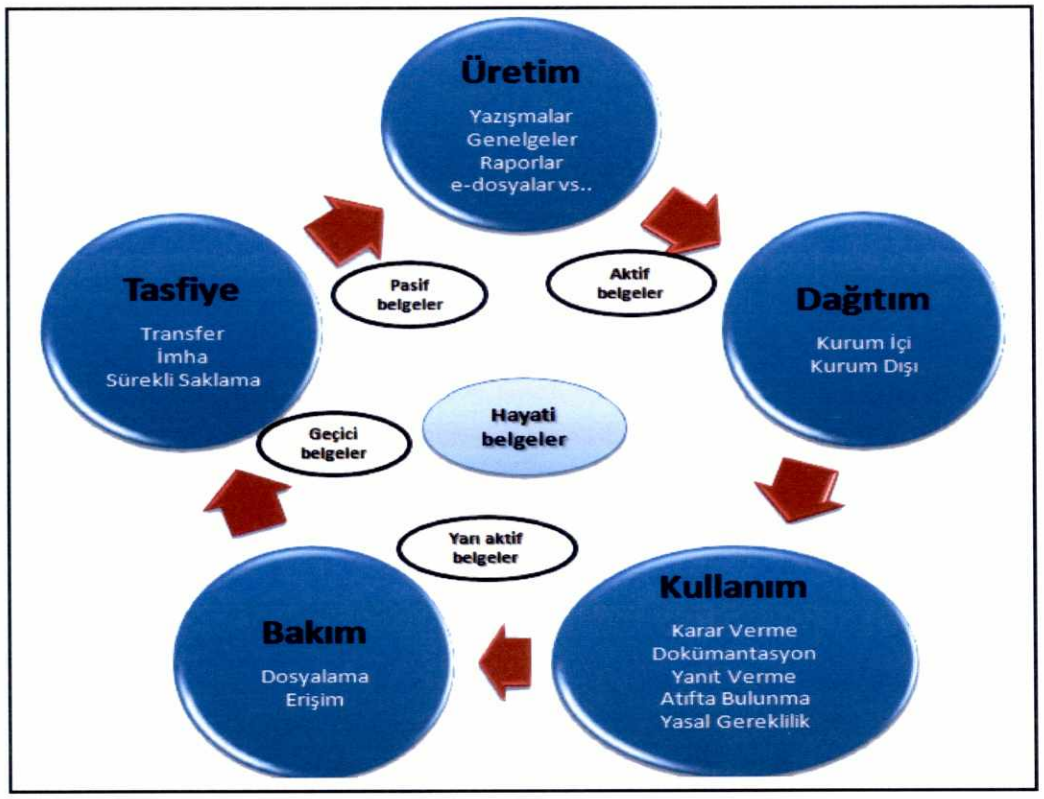
1.4. e-Belgenin Yaşam Döngüsü

Bir belgenin oluşturulmasından, saklanmasına veya imhasına kadar geçen sürece "belgenin yaşam döngüsü" adı verilir. Yaşam döngüsünün;

- ✓ İlk evresinde belge yönetimi disiplini, bazı gerekçelere dayanılarak elde edilmesi zorunlu olan belgelerin üretilmesi ve istenmeyen belgelerin ise üretilmesinin engellenmesine ilişkin kurallara işlerlik kazandırmaktır.
- ✓ İkinci evresinde kayıt altına alınmış bilgi ve belgeye en hızlı şekilde ulaşmak için amacına uygun olarak oluşturulmuş dosyalama sistemi içerisinde yer alan belgelerin kullanılabilirliğinden azami faydayı sağlayacak yöntemler belirlenmektedir. Bu evrede halen güncelliğini muhafaza eden belgeler üzerinde erişim, kullanım, dosyalama ve görüntüleme gibi işlemler yürütülür.
- ✓ Üçüncü evresinde zamanla ihtiyaca binaen belge üzerindeki işlem sıklığı azaldıkça, güncel belgeler vasfı, yerini yarı güncel ya da güncel olmayan belgelere bırakır ve bu duruma gelmiş olan belgelerin bu evrede ayrıştırma gibi bazı işlemlerden sonra ait olduğu kuruluşun belge merkezi veya arşivinde muhafaza altına alınır.
- ✓ Dördüncü ve son evresinde ise belgeler ayıklama, imha veya süreli-süresiz saklama işlemlerine tabi tutulur (Odabaş, 2008, s.124).

Bir amaca hizmet için e-ortamda üretilecek ve gerekliliği konusunda karar verilecek, ilgili taraflarca güvenli bir şekilde kullanılabilmesine imkân sağlanacak, bakımı yapılacak, kullanım süresi bitimi imha edilecek veya arşivlenecek e-belgenin, her evresinde önceden belirlenmiş yönetim süreci Şekil 1-3'de gösterilmiştir.

Şekil 1-3. Belge Yönetim Süreçleri



Kaynak: Kandur, 2009'dan uyarlanmıştır

e-Belgenin yaşam döngüsü konusunda akademisyenler tarafından birbirine yakın tanımlamalar yapılmıştır. Ancak bu tez için Kandur'un beş aşamalı yaşam döngüsü (Şekil 1-3) tanımı esas alınmıştır.

Çiçek ve Bozlağan, ISO 15489'da e-belgenin yönetim sisteminin sorumluluk ve bir disiplin altında olması gerektiğini şu şekilde ifade ederler: Kurumsal açıdan bilgiyi oluşturan veya saklayan belge yönetimi, bir kurumda belgelerin verimli ve bir sisteme bağlı olarak oluşturulması, korunması, ulaşılması, kullanılması ve arşivlenmesi veya imhası kurumsal faaliyetleri oluşturan bilgi ile birlikte kanıtların belgelerle kaydedilmesi görevlerini yürüten yönetim katmanı olarak adlandırılabilir (Çiçek ve Bozlağan, 2008, s.201).

1.4.1. e-Belgenin üretimi

e-Belge üretimi, belge yaşam döngüsünün ilk evresidir. Her şeyden önce üretilecek e-belge, kurum ve kuruluşların amaçları için anlam ifade eden içeriğe sahip olmalı ve kanıt niteliği taşımalıdır. Üretim, elektronik olarak oluşturulan e-belgeler olabileceği gibi kâğıt ortamından tarayıcılar vasıtasıyla da aktarılmış olabilir. Çok farklı biçimlerde ve sistemlerde üretilen ve farklı sistemlerdeki kullanıcılara hitap edecek olan e-belgeler için ulusal ve uluslararası standartlar önem arz etmektedir.

e-Belgelerin üretim aşamasında kontrolü, kağıt belgelerle karşılaştırıldığında daha güç yönetilir bir süreçtir. Bu nedenle belgeler üretilmeden önceki aşamada sistem tanımlanmalı ve arşive veya imhasına kadar olan süreç tespit edilmelidir. Kurum faaliyetleri sonucu üretilen e-belgelere ilaveten kullanılan e-posta veya internet gibi kanallarla da e-belge üretimi gerçekleştirilebilir. Özellikle internet ortamında üretilen belgeler, yapısal farklılıkları gereği diğer belgelerden ayrı yöneltilmelidir. Bu belgelerin aktif bir yapıda olması nedeniyle değişmiş her halinin önceki hali ile bağlantısı kurulmalıdır (Aydın, 2005, s.93).

e-Belge üretimini, binanın temeli olarak düşünebiliriz. Sağlam bina için temel ne kadar önemli ise sağlıklı analizler ile oluşturulacak e-belge, belge yaşam döngüsü için o derece önemlidir. Güvenliği ve standartları ön planda tutarak, doğru sistemler ve kriterler tespit edilerek, kullanıcı rolleri belirlenerek oluşturulacak belgelerin yönetimi ve kullanımı için sonradan oluşacak birçok sorun önlenmiş olacaktır. e-Belgeler; Word, Excel, PDF, Powerpoint, Text Document, Access, AVI, MP 3, MPG, MPEG, JPEG, GIF, HTML, e-Posta vb. olmak üzere çeşitli türlerde üretilmektedir.

1.4.2. e-Belgenin dağıtımı

e-Belgenin dağıtımı, kurum içinde üretilen e-belgelerin, aktif işlem görmeye başladıklarında, önceden oluşturulmuş bulunan altyapılar yardımı ile kurum içi/dışı kullanıma sunulmaları olabileceği gibi, kurum dışında üretilen e-belgelerin güvenlik kontrolleri yapıldıktan sonra EBYS'ne aktarılarak farklı yollarla kurum içi kullanıma açılması işlemleridir.

EBYS'de oluşturulan ve onay işlemleri tamamlanan e-belgenin, EBYS'den sonra KEP'e yönlendirilerek dağıtımının yapılmasını sağlayacak bir yapının oluşturulması gerekmektedir. Söz konusu yapı, kuruluştan çıkan ve kuruluşa gelen bütün e-belgelerin merkezi olarak kontrolünün yapılması amacıyla sadece kuruluşun genel evrak bölümünde oluşturulmalı (merkezi-kontrollü yapı) ya da daha gevşek bir yapıda e-belgelerin dağıtımını sağlamak maksadıyla ihtiyaç duyulan tüm bölümlerde oluşturulmalıdır (dağıtık-esnek yapı) (Önaçan vd., 2012, s.21). EBYS ile üretilen e-belgelerin taraflar arasında KEP sistemleri aracılığı ile paylaşılabilmesi için ETSI 102-640[5] standardına uygun KEP paketlerinin oluşturulması gereklidir. Bu nedenle KEP sistemi vasıtasıyla gelen ve gönderilen e-belgeyi içeren KEP paketini EBYS uyumlaştıracak yazılımlarına ihtiyaç olabilir. EBYS'nin bu standardı destekleyen özelliklere haiz olması gerekir.

---

[5] ETSI 102-640
http://www.etsi.org/deliver/etsi_ts/102600_102699/1026400603/01.01.01_60/ts_1026400603v010101p.pdf

1.4.3. e-Belgenin kullanımı

e-Belge kullanımı, belgelerin iş ve işlemlerde kullanım aşamasında bilgi alma, cevaplama, analiz yapma, arşivleme, ilgi tutma, hukuki kanıt olarak kullanılma vs. işlemlere tabi tutulmasıdır.

e-Belgelerin kullanım fonksiyonları önce EBYS ortamındaki belge ve bilgiler üzerinde arama, görüntüleme, raporlama, yazdırma, internet ortamından erişim ve tanımlanan fonksiyonları kullanıcıya bir ara yüz ile sunma gibi özellikleri barındırmalıdır (Kandur, 2006 s.36).

1.4.4. e-Belgenin bakımı

e-Belge bakımı konusunda, aşağıda yer alan değerlendirmede görüleceği gibi, gelişen teknolojilerin önceden oluşturulmuş e-belgeler üzerinde kaçınılmaz etkilerinden bahsedilmektedir. Ayrıca bu değerlendirmede, gerek yazılım gerekse donanım açısından değişmiş olan teknolojilere uyumlaştırmaların zamanında yapılması gerekliliği vurgulanmaktadır.

Mevcut manyetik depolama araçlarından olan CD-ROM'lar 10 ila 25 yıl sonra özelliklerini kaybetmektedir. Dolayısıyla üzerinde bulunan veriler de ulaşılamaz hale gelmektedir. Sabit diskler üzerinde bulunan verilerde zamanla kullanılamaz hale gelebilir. Gerek donanım teknolojisinin sürekli gelişimi gerekse yazılım teknolojisinin iki yıldan daha az yaşam süresinin olması e-belgelerin arşivlenmesi açısından hayati önem taşımaktadır. e-Belgelerin yaşam döngüsünün her evresinde BİT'deki gelişmeler takip edilmeli ve e-belgenin uyumu derhal sağlanmalıdır (Aydın, 2005, s.94). Bu uyum sağlanırken, belgenin özgünlüğünün korunması göz önünde tutulmalıdır.

e-Belgenin üretim sonrası yaşam alanları yani bulundurulacağı ortam, e-belgeye erişim şekilleri yani yazılımlar, değişen teknoloji ile birlikte içeriği

bozulmadan üretildiği biçimden farklı biçime dönüştürülmesi, e-belgeye kimlerin hangi yetkilerle erişeceği gibi konuların sürekli takibi ve gerekli müdahalelerin zamanında yapılması lazımdır. e-Belgenin yaşam döngüsünü sürdürebilmesi açısından yukarda sayılanlar hayati önemde olmakla birlikte e-belge için yapılan tüm bu iş ve işlemler gerektiğinde e–belgenin bozulmadığının delili olarak sunulabilecek şekilde kayıt altına alınmalıdır.

1.4.5. e-Belgenin tasfiyesi

e-Belgenin yaşam döngüsünde son aşama olan e-belgenin tasfiyesinde e-belgeler arşivleme veya imha işlemlerine tabidir.

1.4.5.1. e-Belgenin arşivlenmesi

Al ve Al'ın (2003, s.2-5)'de ifade ettikleri gibi elektronik arşivin (e-arşiv);

- ✓ e-Belge ve bilgiye kâğıt belgelere oranla daha süratli erişim imkânı
- ✓ Belgeleri ve klasörleri saklamak için ihtiyaç olan fiziki alan ve masrafları minimize etmesi
- ✓ Kullanıcıların ihtiyaç duydukları belgeye ulaşım için mekân değiştirme mecburiyetini ortadan kaldırması
- ✓ Farklı kullanıcıların aynı anda bir belgeyi kullanabilmesi

gibi nitelikleri sebebiyle e-belgelerin niteliklerinin belirlenmesinde güncel, yarı güncel ve arşivlik gereç için de ilişkili ağların kullanılması gerekmektedir.

Arşivleme konusunda e-belgenin içerik, yapı, bağlam, sunum, davranış ve fonksiyonellik olarak 6 temel faktörün bozulmadan saklanabilmesine dikkat edilmelidir. e-Belgenin arşivleme öncesi sahip olduğu içeriğin, etkileşim özellikleri ve fonksiyonlarını bozulmaya uğramadan arşivlendikten sonra da sürdürebilmesi temel amaç olarak kabul edilmektedir. Bu konuda en büyük engel olarak sistem eskimelerinin olduğu değerlendirilmektedir (Dağdaş, 2005, s.22).

Aydın ve Özdemirci (2011, s.107) e-belgelerin arşivlenmesinde arşivleme sistemlerinin önemini şu şekilde ifade etmektedirler: e-Belge yönetiminde arşivleme paylaşılmış e-belgenin tasniflenmesi, düzenlenmesi ve ulaşılabilirliğinin sağlanmasını içermektedir. Arşivleme sistemi, e-belgeleri saklanma sürelerince yönetebilmeli ve EBYS yapılarıyla uyumlu bir şekilde çalışabilmelidir.

2008/16 sayılı Başbakanlık Genelgesi'nde, Elektronik Belge Standartları'nda arşivleme, "*Elektronik belgeler oluşturulma aşamasında kamu kurum ve kuruluşlarınca üretilen elektronik bilgi ve belgelerin idari, mali, hukuki ve tarihi gerekçelerle korunmasının sağlanması ve bunların gelecek nesillere aktarılması ancak standart belge yapılarının oluşturulması ile mümkündür. Elektronik belgeye ilişkin standartlar ile belgelerin korunmasına ve erişimine imkân sağlayacak tedbirlerin elektronik belge yönetim sistemlerinin tasarım aşamasında ele alınması gerekmektedir*" şekilde ifade edilmiştir.

Aynı Genelgede, TS 13298 numaralı standart e-belgelerin kayıt altına alınması, kullanılması ve arşivlenmesi konularında kamu kurum ve kuruluşlarının kullanacağı EBYS için temel bir kaynak olarak belirtilmektedir.

Kamu kurum ve kuruluşlarında üretilen e-belgelerin standartları belirlenirken, e-devlet uygulamasının bütünlüğü ve Devlet Arşivleri Genel Müdürlüğünün iş ve işlemlerine uyumluluk da dikkate alınmalıdır. Arşivleme işleminin, kesintiye uğratılmaması devletin işleyişi bakımından dikkat edilmesi gereken önemli bir husustur.

Arşivlenmesi gerekli bilginin önceden belirlenmesi ve muhafazasındaki başarı, kütüphaneciler, veri işleyiciler, kayıt yöneticileri ve diğer bilgi ve belge uzmanları arasında yapılacak olan işbirliği ile tesis edilmelidir Düzenli (2006, s.65). İfadesi ile arşivleme konusunda kararın, farklı alanlarda görevli uzman kişilerce alınması gerektiğine dikkat çekmektedir.

1.4.5.2. e-Belgenin imhası

TS 13298 Elektronik Belge Yönetimi Standardı'nda, "*Tasfiye, kurumsal gereksinimler açısından saklanmasına gerek kalmayan belgelerin kurum belge sisteminin dışına çıkarılması olarak, tasfiye işlemi de artık ihtiyaç duyulmayan belgelerin kurum içinde veya kurum dışında başka bir kuruma/birime transfer edilmesini ya da imha edilmesini öngörür*" şeklinde tanımlanmıştır.

e-Belgelerin tasfiyesini, iş süreci içinde ihtiyaç duyulmayan e-belgelerin imha edilmesi olarak tanımlamaktadır. e-Belgenin üretim aşamasında belirlenen ömrünün dolması, sonradan verilecek karar üzerine veya başka geçerli nedenlerle imhası sayesinde etkin kullanımda olmayan verinin EBYS içinden ayıklanması sağlanacaktır. e-Belgenin tasfiyesi, keyfi kararlarla değil yasal veya kurumsal gereklilikler ile önceden verilmiş bir karar ile sağlanmalıdır. Verilen bu kararlar ayrıca kayıt altına alınmalıdır. Zamanında yapılan imhalar sistemlerde rahatlama sağlayacağı gibi, belgelerin daha kolay yönetilmesini de beraberinde getirecektir. Bir başka avantaj ise güncelliğini yitirmiş belgelerin, güncel belgelere karışmasının da önüne geçilmiş olacağından sistemin etkin kullanmasına da imkân verecektir (Aydın, 2005, s.94-95).

İmhasına karar verilen ve silinen e-belgelerin, gelişen teknoloji sayesinde tekrar elde edilebilmesi mümkün olabilmektedir. Bu işlem iyi niyetli olarak yapılabileceği gibi aksi bir durum da söz konusu olabilir. Bu nedenle, e-belge yaşam döngüsünün tüm evrelerinde olduğu gibi tekrar elde edilmesi sakıncalı olabilecek belgelerin imha işlemlerinde de uzman desteğine başvurulmalıdır.

2. ELEKTRONİK ORTAMDA BELGE PAYLAŞIM YÖNTEMLERİ

BİT, her geçen gün yeni uygulamalar üretmekle birlikte üretilen her uygulamaya da alternatif ürünler geliştirmektedir. e-Belgenin, e-ortamda paylaşımı için günümüzde yaygın olarak kullanılan uygulamalar; VPN, SSL, e e-Posta, FTP, Kiralık hat ve henüz yeni bir uygulama olan KEP'dir. Bu hususlar aşağıda alt başlıklarda kısaca özetlenmiştir.

2.1. Sanal Özel Ağ

e-Ortamda belgelerin güvenli paylaşımı konusundaki teknolojilerden bir tanesi olan VPN, lokal internet servis sağlayıcı (İSS) ve kurumsal yerel ağlar üzerinde güvenli bir tünel içerisinden veri transferi işlemi ile yapar. Bir başka ifade ile özel ya da internet gibi çok kullanıcılı ağlar üzerinde iki nokta arasında gerçekleştirilen bağlantıdır (MEB, 2008b, s.12).

Ortak kullanımlı veri ağları üzerinden, kurum iletişim ağlarına gerçekleştirilecek olan bağlantıların güvenilirliğini sağlamak için VPN kullanılmaktadır. Gönderilen bilgi paketlerinin şifrelenerek iletilmesi, genel veya özel anahtar yardımı ile gerçekleştirilir (Yüksel, 2007, s.79).

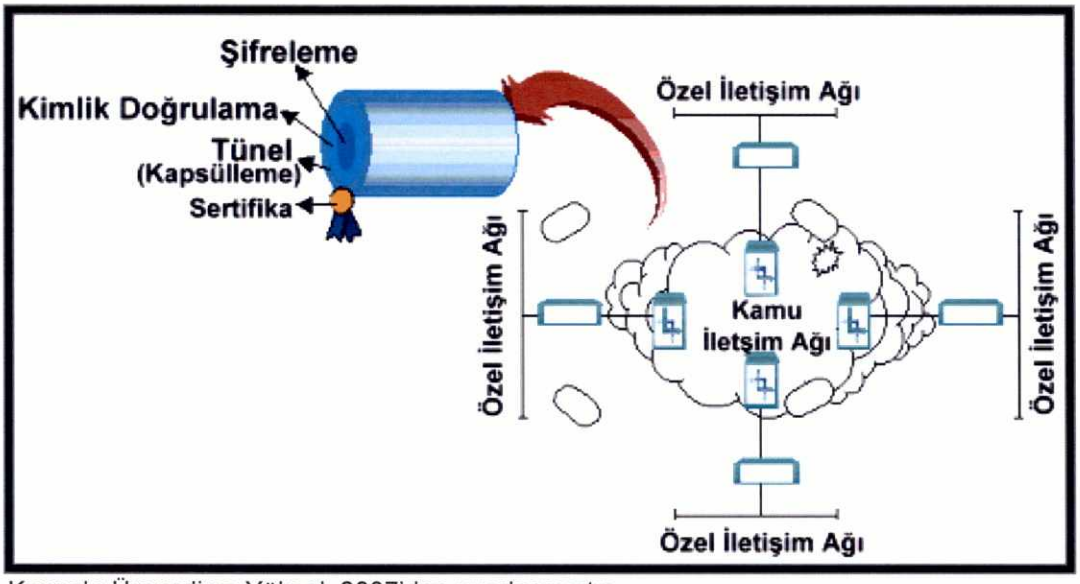
VPN'ler, mevcut ağlar üzerinde sanal bir ağ oluşturma biçimidir. Söz konusu sanal ağ, kimi durumlarda şifrelenmiştir ve yalnızca ağa eklenmiş ve kimliği tespit edilen bilgisayarlar arasında trafiğe müsaade eder. VPN bağlantısı genellikle evinde çalışanların kamuya açık internet vasıtasıyla dâhili bir kuruluş ağına ulaşması amacı ile kullanılır (Sarıöz, 2013, s.17).

VPN işlemi için özel ağ ile kamu ağları arasında VPN yazılımı veya donanımın kullanılıyor olması gerekir. Kullanıcılar aralarında uzak mesafeden veri paylaşımı yapmak istendiğinde, veri paketleri öncelikle gönderenin kendi özel ağında bulunan VPN sistemine ulaşır. Daha sonra kamu ağı üzerinde bulunan, veri paylaşımında bulunacağı kullanıcının ağını koruyan VPN

sistemi üzerinden alıcıya ulaşır. Özel ağlar üzerinde, tüm ağda var olan VPN sistemleri kendi aralarında sanal tüneller oluşturur. VPN sistemleri, içeriği özel olan bilgi paketlerini koruma işlevini kendi aralarında oluşturdukları sanal tüneller aracılığı ile sağlar. VPN sistemlerinin sağladığı güvenlik aşamaları şunlardır:

- ✓ Sertifikasyon: Tüm ağ üzerinde var olan VPN sistemleri benzer sertifikasyon ismini taşır. Benzer isimde olmayan VPN sistemine diğer VPN sistemleri güvenmeyerek bağlantıyı engelleyecektir.
- ✓ Şifreleme: Özel ağdan kamu ağına bilgi paketleri ulaştırılmadan önce şifreleme işlemine tabi tutulur. Şekil 2-1'de görüldüğü üzere herkese açık olan kamu ağında paketler, yetkisiz kullanıcılar tarafından incelense dahi içeriğinin anlaşılması imkânsızdır. Şifreleme işlemi anahtar kod ile oluşturulan belirli kurallara göre yapılır. Bahsi geçen kod, VPN sistemleri tarafından sürekli değiştirilerek çözülmesi imkânsız hale getirilir.
- ✓ Tanımlama ve Sorgulama: Önceden şifrelemeye tabi tutulmuş veri paketleri, şifrelemeyi yapan VPN sisteminin imzasını da içerir. Söz konusu imza ilavesi iki amaca hizmet eder: Birinci amaç, gönderilmiş veya alınmış olan mesajın güvenirliğinin garanti altına alınması, ikincisi ise göndericinin kimlik tespitinin yapılmasıdır.
- ✓ Tünelleme: VPN sistemleri, şifreleme işlemine tabi tutulmuş bilgi paketlerini, güvenliğin olmadığı diğer kamu ağları üzerindeki sanal tüneller aracılığı ile gönderir. Söz konusu tüneller, gönderici ve alıcı VPN sistemlerinin İnternet Protokol (IP) adreslerinden oluşmaktadır. Gönderilmek istenen bilgi, bahsi geçen paketler içine yeni bilgi eklenmesi şeklinde yapılır. Göndericinin ve alıcının gerçek IP'leri böylece gizlenmiş olur (Ünverdi ve Yüksel, 2007, s.1-2).

Şekil 2-1. VPN'nin Genel Yapısı



Kaynak: Ünverdi ve Yüksel, 2007'den uyarlanmıştır.

2.1.1. Uzaktan erişim sanal özel ağ

VPN bağlantı çeşitlerinden olan uzaktan erişim VPN bağlantı şekli, çalışmasını evinden yapan veya hareket halinde olan kullanıcıların, çok kullanıcılı ortam olan internet türü ortak bir ağın sağlamış olduğu altyapı aracılığı ile özel ağ üzerinde bulunan bir sunucuya ulaşmalarına imkân sağlar. Kullanıcı tarafından değerlendirildiğinde VPN, bilgisayarla (VPN istemci) kuruluşun sunucusunu ağlar üzerinde buluşturan bir bağlantıdır. Mantıksal olarak gönderilen veri paketleri, ayrı bir özel ağ içerisinden iletiliyormuş şeklinde görüldüğünden, kullanılan ya da ortak ağın altyapısının bir önemi yoktur (Microsoft, 2012a).

Demir'in (2010, s.11) değerlendirmelerine göre; "Uzak erişim VPN bağlantılar daha çok düşük bant genişliği olan kullanıcılar için yapılandırılmış VPN tipidir. Uzak erişim VPN tipinde Tünel Modu kullanılır". Yine Demir'in (2010, s.10) ifadeleri ile "Tünel Modu, Taşıma modundan farklı olarak, VPN'i cihazdan-cihaza değil, bir ağdan başka bir ağa güvenli iletim için kullanılmak üzere oluşturulan bir moddur".

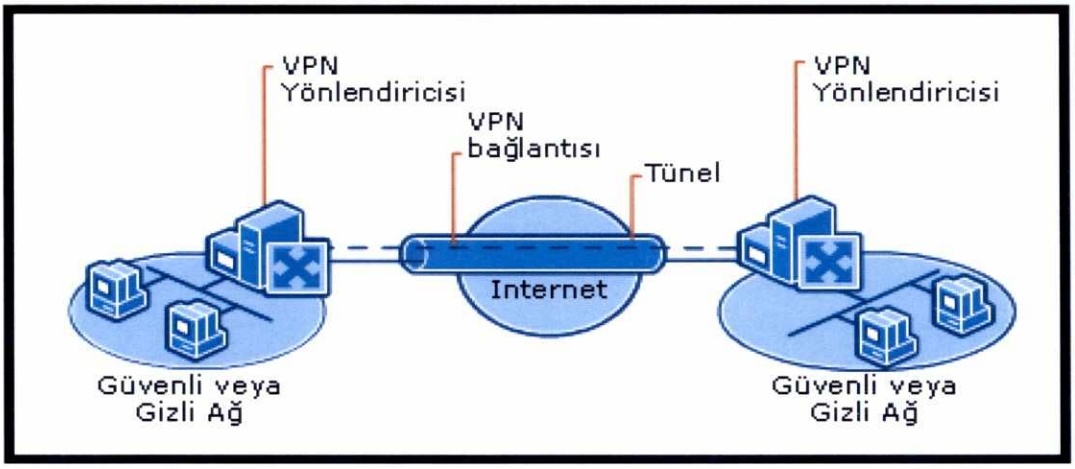
2.1.2. Siteden siteye sanal özel ağ

Uçlar arası VPN bağlantılar, VPN uç cihazları üzerinde, güvenli veri transferi sağlamak için tünel modu kullanır. Uçlar arası VPN bağlantıları genellikle Siteden Siteye Bağlantı (L2L) olarak adlandırılır. L2L sayesinde her bir bölgedeki VPN sonlandırıcı cihaz, arada meydana gelen veri transferi trafiğinin izinsiz kullanıcılardan korunması işlemini gerçekleştirir (Demir, 2010 s.10-11).

Siteden siteye sanal özel ağ (Şekil 2-2) veri gönderim amaçlı bu uygulama ile ağlara istenmeyen bağlantının engellenmesi için şifreli kimlik sorgulaması yapılır. Şifreleme ile yapılacak haberleşmenin başka kullanıcıların haberleşmeyi dinlemesi ve verilere müdahalesi engellenir.

VPN bağlantılarında, aktarılan veri paketleri şifrelenerek korunmaktadır. VPN bağlantı türlerinde ve internet gibi bilgilerin her zaman izinsiz kullanıcılar tarafından ele geçirilme riski olan ortamlarda yapılacak olan özel veri transferlerinde daima veri şifrelemesi gereklidir. Uzaktan erişimlerde, VPN bağlantıları için Noktadan Noktaya Tünel Protokolü, IP Güvenliği şifrelemesi de Katman 2 Tünel Protokolü birlikte kullanılır. Veri paketlerinin şifrelenmesi, VPN istemci ve VPN sunucu arasında yapıldığından çevirmeli ağ istemci ve bağlantı sağlayıcısı olan ISS arasında bağlantılarda şifreleme yapmaya ihtiyaç bulunmamaktadır (Erkut, 2006, s.69-70).

Şekil 2-2. İki Uzak Siteyi İnternet Üzerinden Bağlayan Sanal Özel Ağ



Kaynak : Microsoft, 2012a

2.2. Güvenli Yuva Katmanı

SSL sunucusu, bilgisayar ağlarında belge ve bilgi gönderiminde güvenliği ve gizliliği korumak amacıyla Netscape tarayıcısı tarafından oluşturulmuş bir güvenlik protokolüdür. SSL 3.0 sürümünün, 1996 yılında piyasada kullanılması ile birlikte İnternet-Dünyayı çevreleyen ağ (WWW) ortamında bulunan bütün (İnternet Explorer, Netscape Navigator v.b.) internet tarayıcılarının kullandığı geniş bir alana sahip olmuştur. İnternet üzerinde belge ve bilgi paylaşan tarafların kimlik doğrulaması, SSL protokolü kapsamında elektronik sertifikalar ile yapılmaktadır. SSL, gönderilen belge ve bilginin sadece hedeflenen adreste çözümlenmesini sağlar. Belge ve bilgi gönderim öncesi şifrelenir, çözümlenmesi ise kesinlikle doğru kullanıcı tarafından yapılabilir. Karşılıklı olarak doğrulamaların yapılması ile işlemin, belgenin ve bilginin bütünlüğü ile aynı zamanda gizliliği korunmuş olur. Günümüzde kullanılan SSL teknolojisinde 4256 değişik anahtarın kullanılıyor olmasının yanında, 256 bitlik şifreleme esası da kullanılmaktadır.

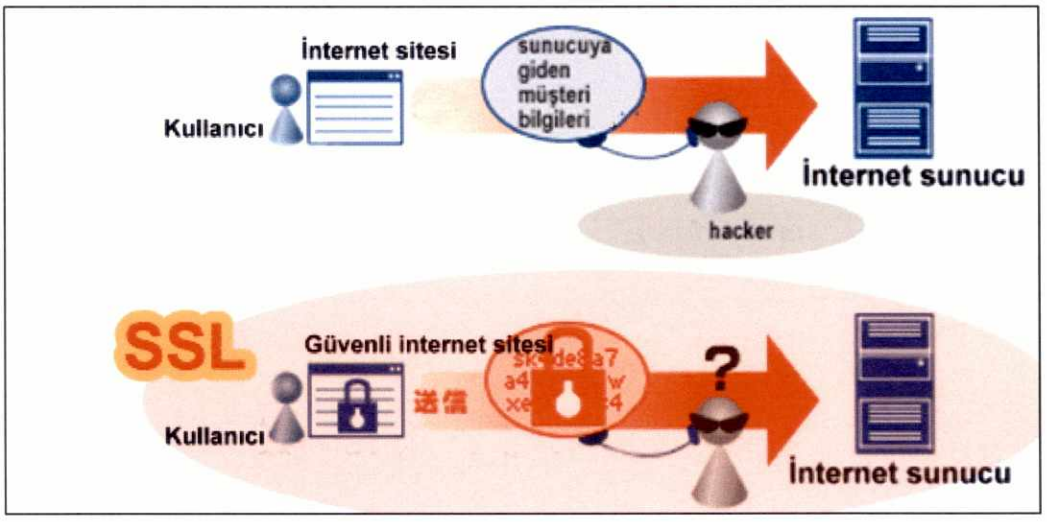
SSL Protokolü tarafından sağlanan bağlantı güvenliğinin özellikleri aşağıda yer almaktadır;

- ✓ Bağlantı gizlidir

- ✓ Belge ve bilgi paylaşan karşılıklı kullanıcıların kimlikleri doğrulanır
- ✓ Belge ve bilgi paylaşımı akışı içerisinde belge ve bilgi bütünlüğünün kontrolü de sağlanır (Sayın, 2009, s.63-64).

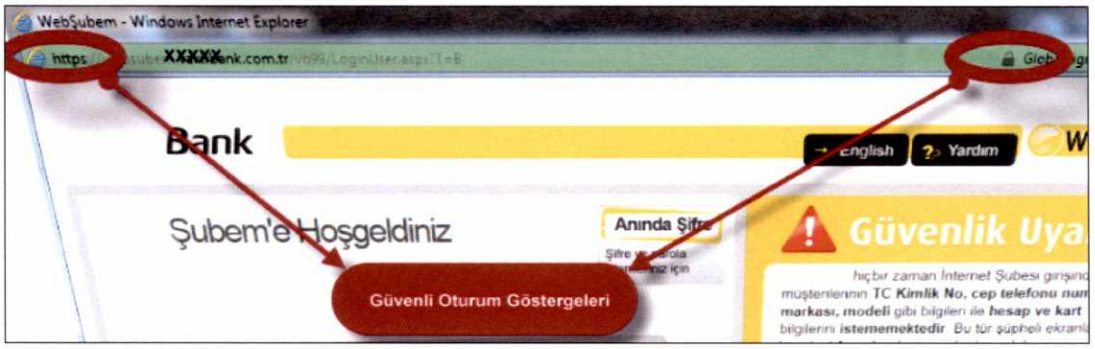
SSL, internet ortamı gibi herkese açık alanda belge aktarımının güvenli bir şekilde yapılmasını sağlamak amacıyla, herkese açık bir anahtar şifrelemesi ile birlikte özel anahtar şifrelemesini aynı anda kullanabilen yapıda geliştirilmiş bir teknolojidir. Bir kuruluşun güvenlik amaçlı olarak müşterileri ile kendi sunucusu arasında bağlantı için kullandığı SSL örneği Şekil 2-3'de verilmiştir.

Şekil 2-3. Güvenli Yuva Katmanı Bağlantısı



Kaynak: Garanti, 2012'den uyarlanmıştır.

Şekil 2-4. SSL Bağlantısı ile Güvenlik Göstergeleri



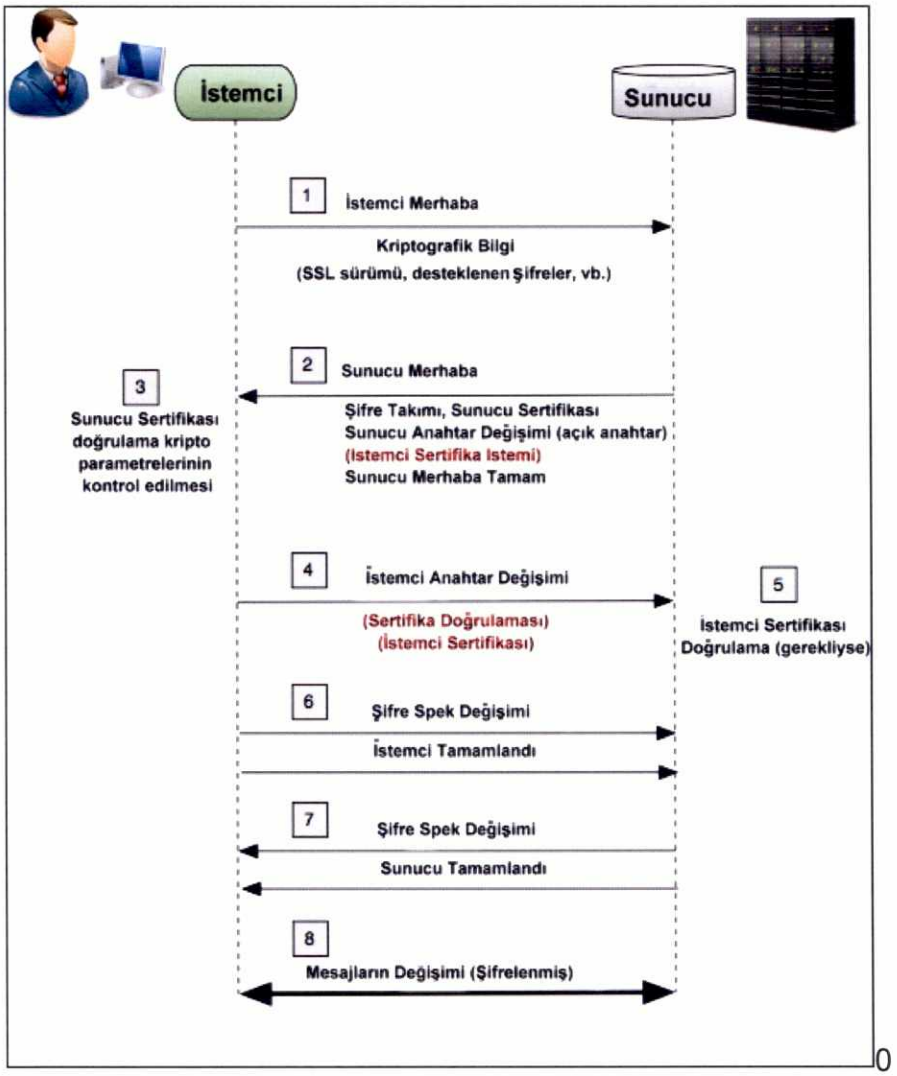
Şekil 2-4'te görüldüğü gibi, SSL ile yapılan erişimlerde, oturumun güvenli şekilde sağlandığı, tarayıcının adres çubuğunda bulunan güvenlik göstergesinde adresler, "https://" şeklinde olmalıdır. Ayrıca "kilit" simgesine tıklandığında sertifikanın detayı görüntülenebilmektedir. Görüntülenen detayda sertifikanın, bağlantının gerçekleştirildiği adresin sahibine ait olup olmadığı tespit edilebilecektir.

SSL, bilgiyi gönderen sunucu bilgisayar ile bilgiyi alan istemci bilgisayarın birbirini tanıma işlemi yürütür. Bu şekilde bilginin hedeflenen bilgisayarlar arasında paylaşılacağı doğrulanmış olur. Bilgi gönderilmeden önce otomatik olarak şifrelenir. Şifrelenen bilgi sadece hedeflenen adreste çözümlenebilir. Sunucu ve istemci işlemlerin gizliliği ve bilgi bütünlüğünün bozulmaması için kendi aralarında doğrulama yaparlar.

2.2.1. Güvenli yuva katmanının çalışma şekli

Aşağıdaki Şekil 2.5'de görüldüğü üzere; istemci adına işlem yapan tarayıcı güvenli bir siteye bağlandığı takdirde önce karşı tarafın kimliğini sorgular. Sorgunun muhatabı olan sunucu sertifikasını, istemci adına işlem yapan tarayıcıya iletir. Tarayıcı almış olduğu kimlik bilgileri içerisinde yer alan sertifikayı hazırlayan kurumun attığı imza ile kendinde bulunan sertifika kurumunun bilgilerini karşılaştırarak kontrol eder.

Şekil 2-5. SSL'in Çalışma Prensibi



Kaynak: (yaSSL, 2012, s.116)

Tarayıcı, sertifika üzerinde belirtilen adres ile bağlantıyı gerçekleştirdiği adresin doğruluğunu kontrol eder. Şayet kimlik, onaydan geçer ise şifreli bağlantı için anahtar seçim süreci hazırdır. Tarayıcı ve sunucu bir defaya mahsus kullanım için oturum şifresini tespit ederler. Oturum süresince tüm bilgi ve belge alış verişlerini bu şifreyi kullanarak gerçekleştirirler.

SSL protokolü kullanılarak bir siteye erişim sağlandığında sunucu ile tarayıcı arasında başkalarının izleyemeyeceği şifreli bir iletişim başlayacaktır. SSL şifrelemeye ilaveten verilerin değiştirilip değiştirilmediğini kontrol edecektir.

Şifreleme, internet tarayıcısına internet sitesi arasında güvenli bir şekilde iletişimi sağlamak için lüzumlu bilgileri temin eden bir sertifikaya dayanır. Sertifikalar internet sitesini ve söz konusu internet sitesinin sahibini ya da kuruluşu da tanımlar (Microsoft, 2012b).

SSL, standart e-posta gönderip almak, anlık ileti gönderip almak, internet üzerinden alışveriş yapmak, bankacılık işlemleri yapmak gibi uygulamalarda güvenliği sağlamak için kullanılır (MEB, 2008a, s.23). Söz konusu sertifikalar, bağlantı yapmaya çalıştığımız internet sitesini sahtesinden ayrıştırmamızda bize yardımcı olacaktır. İnternet kullanıcıları, SSL sayesinde bağlandığı sunucunun adresini doğrulayabilir veya bağlandığı sunucuya bilgi göndermeden önce sunucu sahibinin kimliğini sorgulayabilir.

2.3. Dosya Aktarım Protokolü/Güvenli Dosya Aktarım Protokolü

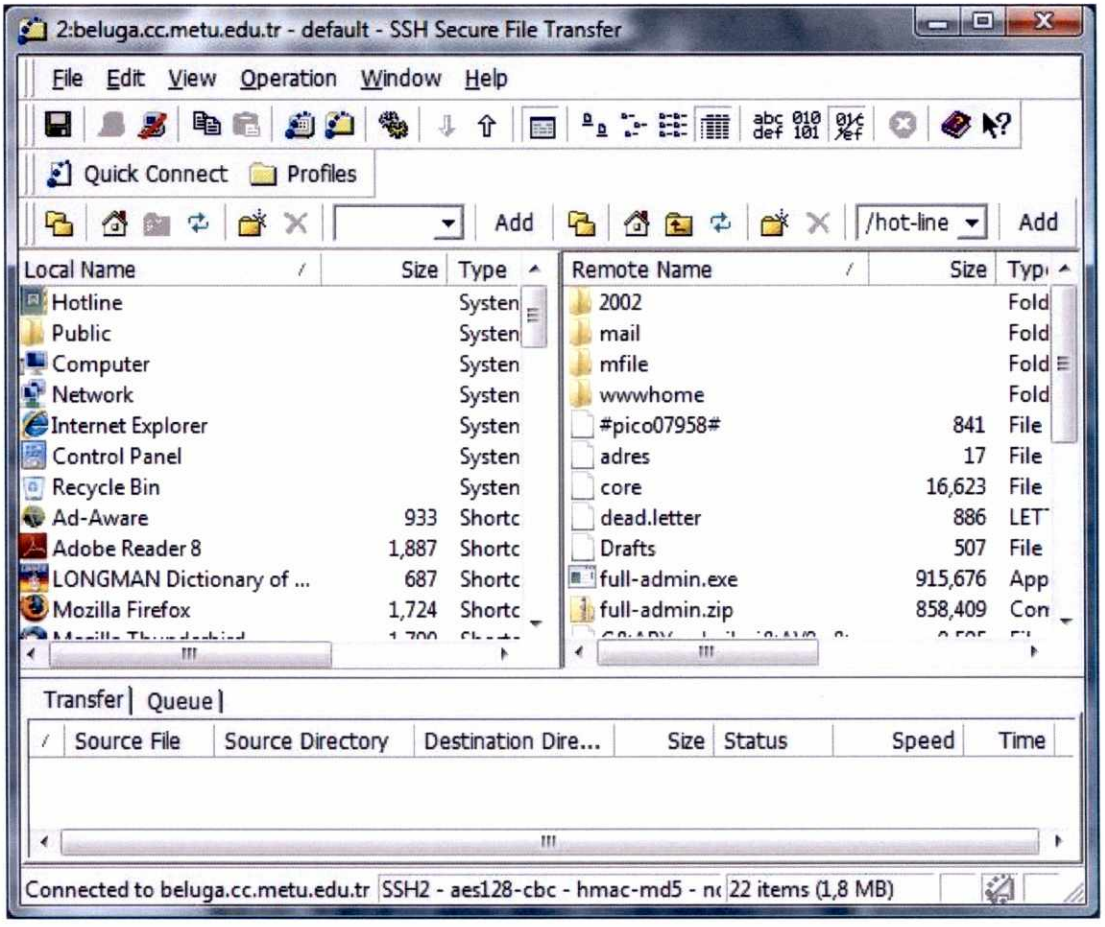
FTP, dosyaları internet üzerinden aktarmak için kullanılan bir protokoldür (Microsoft, 2013). FTP ile internete bağlı olan bilgisayarlar arasında karşılıklı belge paylaşımı, belgeler üzerinde düzenleme yapabilme gibi işlemler gerçekleştirilebilmektedir.

FTP'de, DOS işletim sistemi, günümüz internet tarayıcıları ve programlar üzerinden hedef bilgisayarlara kullanıcı adı ve şifre kullanılarak bağlantı sağlanabilmektedir. Bağlantının sağlandığı cihaz, kişisel bir bilgisayar olabileceği gibi herkesin kullanımına açık bir bilgisayar da olabilir. FTP ile işlem yapabilmek için (İTÜ/BİDB, 2013);

- ✓ Bağlantı yapılacak olan bilgisayarın internet adresi
- ✓ Bağlantı yapılacak olan bilgisayarda dosyalarına ulaşılacak hesapla ilgili kullanıcı adı ve şifresi
- ✓ İnternete bağlı olan ve FTP yazılımı mevcut bir bilgisayar
- ✓ Bağlanmak istenen bilgisayarda, FTP protokol komutlarını yorumlayacak işler vaziyette bir FTP istemcisi

Güvenli Dosya Aktarım Protokolü (SFTP) ise FTP'nin sağlamış olduğu dosya aktarımı özelliğine ek olarak bu veri alışverişinin güvenli olarak gerçekleştirilebilmesi sağlamaktadır. SSH ve benzeri güvenli iletişim altyapıları ile kullanılmakta ve paylaşılan verilerin gizliliği korunmaktadır. SFTP bağlantısına ilişkin örnek Şekil 2-6'da gösterilmiştir. SFTP internet üzerinden güvenli belge paylaşımının sağlanmasına yönelik olarak SSL veya TLS kullanılabilmektedir (IETF, 2005).

Şekil 2-6. Örnek SFTP kullanımı



Kaynak: ODTÜ BİDB, 2013

2.4. e-Posta

e-Posta genel ifadesi ile internet üzerindeki posta sistemidir. e-Posta, e-ortamda bilgi ve belge paylaşımında en yaygın kullanılan uygulamalardandır. e-Posta ile ilgili temel bazı bilgiler alt başlıklarda verilmiştir.

2.4.1. e-Postanın yapısı

Geleneksel posta, zarf ve içinde yer alan mektuptan oluşur. e-Postanın yapısını da buna benzeterek tanımlamak mümkündür. e-Posta gönderisinde gönderici ve alıcıya ilişkin bilgileri içeren başlık bölümü zarfa ve iletinin yazı, resim, ses vs. içeriği geleneksel postadaki mektuba benzetilebilir.

2.4.2. Başlık bölümü

e-Postanın başlık bölümünde, oluşturma tarihi ve oluşturulan adres alanlarının bulunması mecburi olup diğer alanlar seçimliktir. Başlık kısmında bulunan alan başlıkları aşağıdadır;

- ✓ Oluşturulma tarih alanı
- ✓ Oluşturucu alanları
- ✓ Hedef adres alanları
- ✓ Kimlik alanları
- ✓ Bilgilendirici alanlar
- ✓ Yeniden gönderme alanları
- ✓ Takip alanları
- ✓ İsteğe bağlı alanlar

2.4.3. Gövde bölümü ve çok amaçlı internet posta uzantıları

e-Postanın gövde bölümü, gönderici tarafından alıcıya gönderilmek üzere hazırlanan bilgi ve belgelerin bulunduğu kısımdır.

e-Posta mesaj yapısının standardı Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (ASCII) karakter dizisinden meydana gelmektedir. Bu durum farklı yapılardan oluşan verilerin iletilmesi konusunda yetersiz kalmış olup, mesaj içeriğinde yer alan ses, resim, video gibi verilerinin iletilmesi amacıyla Çok Amaçlı İnternet Posta Uzantıları (MIME) geliştirilmiştir. MIME ile e-posta mesaj başlık kısmında yeni özellikler tanımlanmıştır. e-Posta mesajının oluşturulması aşamasında ilave edilen bu bilgiler yardımı ile e-posta alıcısının mesaj içeriğinde bulunan veriyi oluşturulduğu biçimde yeniden biçimlendirmesi sağlanmaktadır (Öztürk, 2009, s.7-8).

MIME ile tanımlanan 5 ana ortam tipi vardır (Avlanmaz, 2012, s.20);

- ✓ Yazı (Text)
- ✓ Resim (Image)
- ✓ Ses (Audio)
- ✓ Video (Video)
- ✓ Uygulama (Application)

2.4.4. e-Posta hizmeti araçları

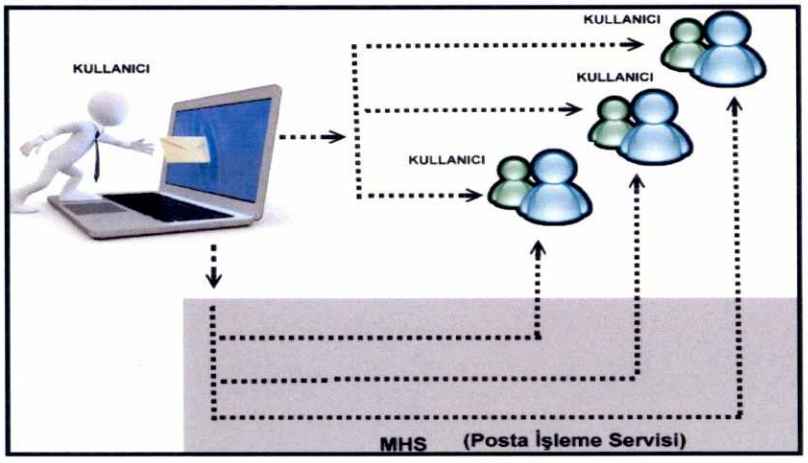
e-Posta hizmetinin bileşenleri; mesajın, gönderici tarafından oluşturulduğu noktadan, alıcısına ulaştığı nokta dâhil olan süreç içerisindeki araçlardan oluşur. e-Posta hizmetinde bir iletinin gönderici e-posta sunucusundan alıcı e-posta sunucusuna iletilmesi bir haberleşme standardı olan Basit Posta Aktarım Protokolü (SMTP) çerçevesinde gerçekleşmektedir. Bir e-posta iletisinin sunucu üzerinden alınarak istemci üzerine kopyalanması ve çeşitli e-posta araçlarıyla bu iletilerin kullanıcı tarafından görüntülenmesi ve

yönetilmesi ise Posta Ofis Protokolü (POP) veya İnternet Mesaj Erişim Protokolü (IMAP) kuralları dâhilinde gerçekleşmektedir. Günümüzde bu protokollerden, POP3 yani POP'un üçüncü sürümü ve IMAP4 yani IMAP'nin dördüncü sürümü kullanılmaktadır (Öztürk, 2009, s.15,20-23).

2.4.5. e-Posta işleme servisi

Posta İşleme Servisi (MHS), Şekil 2.7'de görüldüğü gibi e-postanın, göndericiden alıcıya iletilmesinin yönetimi ve ulaşmasını sağlayan servistir (Öztürk, 2009, s.9).

Şekil 2-7. Posta İşleme Servisinin Görevi

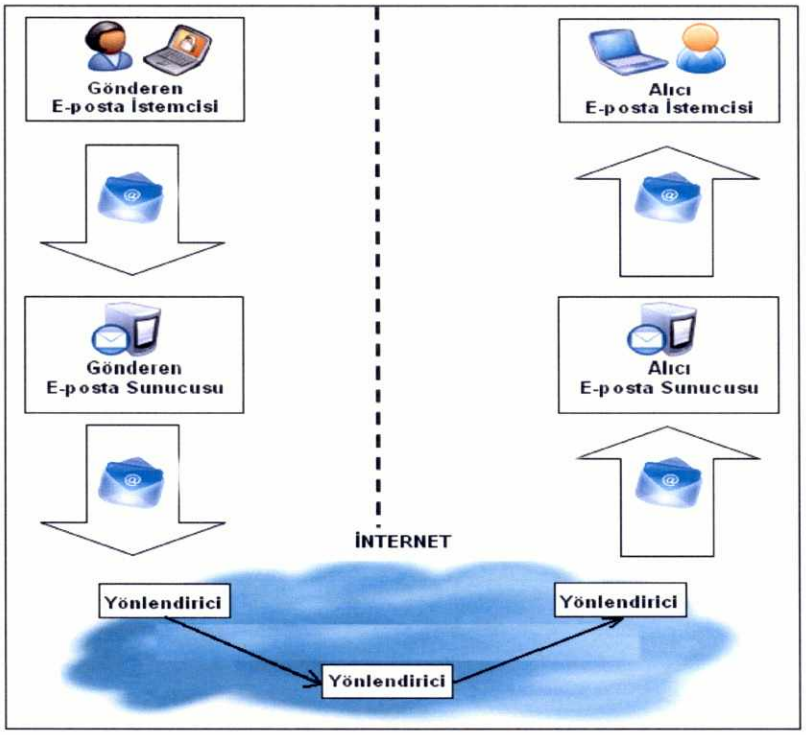


Kaynak: Crocker, 2004, s.5'den uyarlanmıştır

2.4.6. e-Posta işleyişi

e-Posta işleyişi, (Şekil 2-8) hizmet araçlarının belli kurallar çerçevesinde uyumlu bir şekilde çalışmasıyla gerçekleşmektedir.

Şekil 2-8. e-Posta Hizmetinin İş Akışı



Kaynak: Öztürk, 2009, s.9'dan uyarlanmıştır.

e-Posta gönderme işlemi, göndericinin istemci bilgisayar üzerinde kurulu olan e-posta araçları vasıtasıyla (MS Outlook, Mozilla Thunderbird vb.) oluşturduğu iletiyi (mesaj içeriği, mesaj başlığı, alıcı listesi, eklemeler vb.) SMTP standardını kullanarak e-posta servis sağlayıcısındaki e-posta sunucu üzerinde bulunan posta gönderme aracına iletir (Kioskea, 2012).

Posta gönderme aracı, iletinin e-posta sunucusunun uyguladığı kurallara uygunluğunu ve ardından iletinin internet mesaj standartlarına uygunluğunu kontrol eder. Bu aşamaya kadar sorun yok ise, SMTP'ye uygun olarak öncelikle mesajdaki adrese göre mesajın takip edeceği yolu belirler (Avlanmaz, 2012, s.25).

Sonraki adımda ise Alan Adı Sistemlerindeki (DNS) posta değişim kayıtlarını sorgular. Eğer mesajın gideceği adres, yerel ağda ise internet trafiğine girmeden sunucu üzerinde tanımlı bulunan kişinin posta kutusuna iletir.

Adresin uzak ağda olma durumunda ise e-posta iletisi internet üzerinden taşınarak alıcıya iletilir. İşlemlerin tamamı SMTP kurallarına uygun olarak gerçekleştirilir (Kavi, 2012).

2.4.7. e-Posta güvenlik mekanizmaları

Taşıma Katmanı Güvenliği (TLS), SSL, Oldukça İyi Mahremiyet (PGP), Güvenli/Çok Amaçlı İnternet Posta Uzantıları (S/MIME) olarak adlandırılan güvenlik mekanizmaları, bilgisayarlar arasında güvenli bağlantılar oluşturmak ve verinin güvenliği ile güvenirliğini sağlamak amacıyla geliştirilmiş yöntemlerdir. Bu yöntemlere kısaca bakılacak olursa;

- ✓ TLS: IP tabanlı iletişimde güvenli bilgi ve belge aktarımını sağlayan protokol olup SSL protokolü baz alınarak oluşturulmuştur. Karşılıklı veri alış verişi sırasında, bilgilerin şifrelenerek gönderilip alınmasını sağlayarak e-posta iletilerinin güvenli bir biçimde taşınmasını sağlamaktadır.
- ✓ SSL: İstemci ile sunucu arasındaki bilgi alış verişinde gönderilen ve alınan bilgiyi şifreleyerek güvenli bir iletişim ortamı oluşturmaktadır.
- ✓ PGP: e-Posta iletiminde verilerin korunması için üretilmiş olup dünyada en yaygın kullanılan e-posta şifreleme ve sayısal imzalama uygulamasıdır. Bu şifreleme mekanizması e-posta iletilerinin içeriğine üçüncü tarafların erişimini önlemektedir.
- ✓ S/MIME: e-Posta formatına AAA kullanarak sayısal imza ve şifreleme özelliklerini ilave etmiştir (Öztürk, 2009, s.73-74-75).

2.5. Kayıtlı Elektronik Posta (KEP)

14/02/2011 tarihli ve 27846 sayılı ve Resmi Gazete'de yayımlanan 6012 sayılı Türk Ticaret Kanun'un 18 inci maddesinin 3 üncü bendinde yer alan *"Tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar noter aracılığıyla,*

taahhütlü mektupla, telgrafla veya güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile yapılır." hüküm ile KEP sisteminin kanuni dayanağı oluşturulmuştur. Aynı Kanun'un 1525 inci maddesi ikinci fıkrasında; yer alan *"Kayıtlı elektronik posta sistemine, bu sistemle yapılacak işlemler ile bunların sonuçlarına, kayıtlı posta adresine sahip gerçek kişilere, işletmelere ve şirketlere, kayıtlı elektronik posta hizmet sağlayıcılarının hak ve yükümlülüklerine, yetkilendirilmelerine ve denetlenmelerine ilişkin usul ve esaslar Bilgi Teknolojileri ve İletişim Kurumu tarafından bir yönetmelikle düzenlenir."* hüküm ile KEP sistemine ilişkin düzenlemeleri hazırlama görevi BTK'ya verilmiştir. Bu görev kapsamında BTK tarafından 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelikte KEP, *Elektronik iletilerin, gönderimi ve teslimatı da dâhil olmak üzere kullanımına ilişkin olarak hukukî delil sağlayan, elektronik postanın nitelikli şekli* olarak tanımlanmaktadır.

KEP farklı kullanıcılar arasında e-belge paylaşımı ve e-belgenin saklanmasını sağlayan, hukuki olarak geçerli ve teknik açıdan güvenli bir e-postadır. Bu şekilde tanımlanan KEP; SMTP protokolü destekli, güvenli e-imza ve zaman damgası kullanılan, Kayıtlı Elektronik Posta Hizmet Sağlayıcısı (KEPHS) aracılığı ile gönderici ve alıcının kimliklerinin tespit edilmesini, iletinin değiştirilmemesini, göndericinin gönderdiğini ya da alıcının aldığını inkar edememesini temin eden bir sistemdir (Önaçan vd., 2012, s.10).

Kısaca KEP sistemi, e-ortamda yapılan gönderilerin kimin tarafından kime ne zaman gönderildiğini ve alıcıya ne zaman iletildiğinin kesin bir şekilde tespit eden sistemdir. e-Postanın göndericisi ve alıcısı arasında bir katman olan KEP, bilinen hizmetlere ilave olarak;

1. Gönderici ve alıcının kimliklerinin doğrulanmasına
2. Gönderim talebinin kabul edilip edilmediğine
3. Gönderimin yapılıp yapılmadığına

4. Gönderinin alıcının posta kutusuna iletilip iletilmediğine
5. Gönderinin alıcı tarafından indirilip indirilmediğine
6. Bu işlemlerin yapılış zamanlarına

ilişkin zorunlu delilleri sağlamaktadır. KEP üzerinden gönderilen ileti, bu farkları dolayısıyla sıradan e-postadan ayrılmakta ve hukuken geçerli delil değeri kazanmaktadır (Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), 2010, s.8-9-10).

Bu sistemle gerçekleştirilebilen bazı uygulamalar:

- ✓ Diğer kurumlar ile
  - Teklif
  - İhale şartnamesi
  - Sözleşme yapma/yenileme/fesih
  - Sipariş formu
  - İhbar/ihtar
- ✓ Kurum içi
  - Kurum içi duyurular
  - İstifa mektubu
  - Talimat
  - Sözleşme yapma/yenileme/fesih
  - Atama/görevlendirme
- ✓ Kamu kurumlarının e-ortamda resmi yazışma yapmaları,
- ✓ Tacirlerin ihtar, ihbar ve benzeri e-beyanları birbirlerine yöneltmeleri,
- ✓ Elektronik faturaların muhataba gönderilmesi,
- ✓ e-Ortamda idari, mali ve adli tebligat hizmeti verilmesi,

- ✓ Tüketici şikâyet ve taleplerinin ucuz, hızlı ve kolay bir şekilde muhataba iletilmesi,
- ✓ Vatandaşlar arasında, güvenli e-imza, zaman damgası ve KEPHS gibi güvenlik unsurları kullanılarak güvenli e-posta haberleşmesinde kullanılması,
- ✓ e-Ortamda oluşturulan ve e-ortamda muhafaza edilen değerlerin (Fikir ve Sanat Eserleri Kanunu kapsamındaki eserlerin) güvenli olarak saklanması

şeklinde sıralanabilir. Ancak e-ortama aktarılan belge çeşitlerinin artması ile birlikte KEP sisteminin kullanılabileceği alanların artacağı öngörülmektedir.

2.5.1. KEP sistemi ile ilgili standart çalışmaları

KEP sistemi ile ilgili olarak çeşitli uluslararası kurum ve kuruluşların standartlara ilişkin çalışmaları bulunmaktadır. Bu başlık altında; AB müktesebatına uyum kapsamında, Avrupa'da konuya ilişkin standartları belirlemekle yetkili kuruluş olan ETSI ve Avrupa Standardizasyon Komitesi (CEN) ile ülkemizin de üyesi bulunduğu Evrensel Posta Birliği'nin (UPU) çalışmalarına yer verilmiştir.

2.5.2. UPU'nun çalışmaları

Birleşmiş Milletler'in postaya ilişkin kuruluşu olan UPU posta hizmetlerinin etkin biçimde yürütülebilmesini teminen ilgili standartların belirlenmesini amaçlamaktadır. UPU'nun "Kayıtlı Elektronik Posta İşlevsel Özellikleri" standart belgesi aşağıdaki teknik standartlar ile yakın ilişki içerisinde hazırlanmıştır (Alkan vd., 2010, s.8):

- ✓ UPU – Güvenli Elektronik Posta Hizmetleri (SePS) ara yüz özellikleri – Bölüm A: Kavramlar, şemalar ve işlemler

- ✓ UPU - SePS – Bölüm B: Elektronik Posta Sertifikasyon İşareti (EPCM) Hizmeti
- ✓ ETSI – Kayıtlı Elektronik Posta: Mimari, Formatlar ve Bilgi Güvenliği Yönetimi Süreçleri.

2.5.3. ETSI'nin çalışmaları

KEP sisteminin esasları, Fransa'da yerleşik bir bağımsız standart kuruluşu olan ETSI tarafından belirlenmiştir. ETSI söz konusu çalışmalarını; üreticiler, şebeke işletmecileri, ulusal kurumlar, hizmet sağlayıcılar, araştırma kuruluşları, kullanıcı grupları ve danışmanlık kuruluşları da dâhil olmak üzere 62 ülkeden 700'ü aşkın üyesi ile işbirliği içerisinde oluşturulan Özel Görev Grupları (Special Task Forces) bünyesinde yürütmektedir (ETSI, 2012a, 2012b).

ETSI'nin, KEP'e ilişkin çalışmaları; ilgili Özel Görev Grubu tarafından AB üye ülkelerinin ilgili kurum ve kuruluşları (kamu kurumları, standardizasyon kurumları, e-posta hizmet sağlayıcıları, yerel uzmanlar vb.), diğer bağımsız kuruluşlar ve AB üyesi olmayan ülkelerin kurum ve kuruluşları arasında KEP sisteminin mevcut veya potansiyel uygulamaları konusunda yaptığı bir araştırma ve bu araştırmanın sonuçlarına dayanan bir teknik rapor olarak somutlaşmaktadır. Söz konusu raporda yer alan sonuçlar ışığında, KEP sisteminde kullanılacak olan imza formatlarının ve söz konusu imzaları uygulayacak olan Güvenli Hizmet Sağlayıcıların süreçlerinin belirlenmesi gibi çeşitli konularda teknik standartların tanımlanması amaçlanmaktadır. Bu çalışmalar sonunda ETSI tarafından belirlenen teknik standartlara Tablo 2-1'de yer verilmektedir (ETSI, 2011).

Tablo 2.1 ETSI KEP Standardı Dokümanları

Standart No	Standart Adı	Bölüm	Bölüm Adı
ETSI TS 102 640	Kayıtlı Elektronik Posta (KEP): Mimari, Formatlar ve Politikalar	1	Mimari
		2	KEP'in İmzalanmış Delilleri için Veri Gereksinimleri ve Formatları
		3	KEP Yönetim Alanı için Bilgi Güvenliği Politika Gereksinimleri
	Kayıtlı Elektronik Posta (KEP): Mimari, Formatlar, Politikalar ve Profiller	4	KEP Yönetim Alanı Değerlendirme Profilleri
		5, 6	KEP Yönetim Alanı Birlikte Çalışabilirlik Profilleri

Kaynak: Kabasakal, 2013, s.3

2.5.4. CEN'in çalışmaları

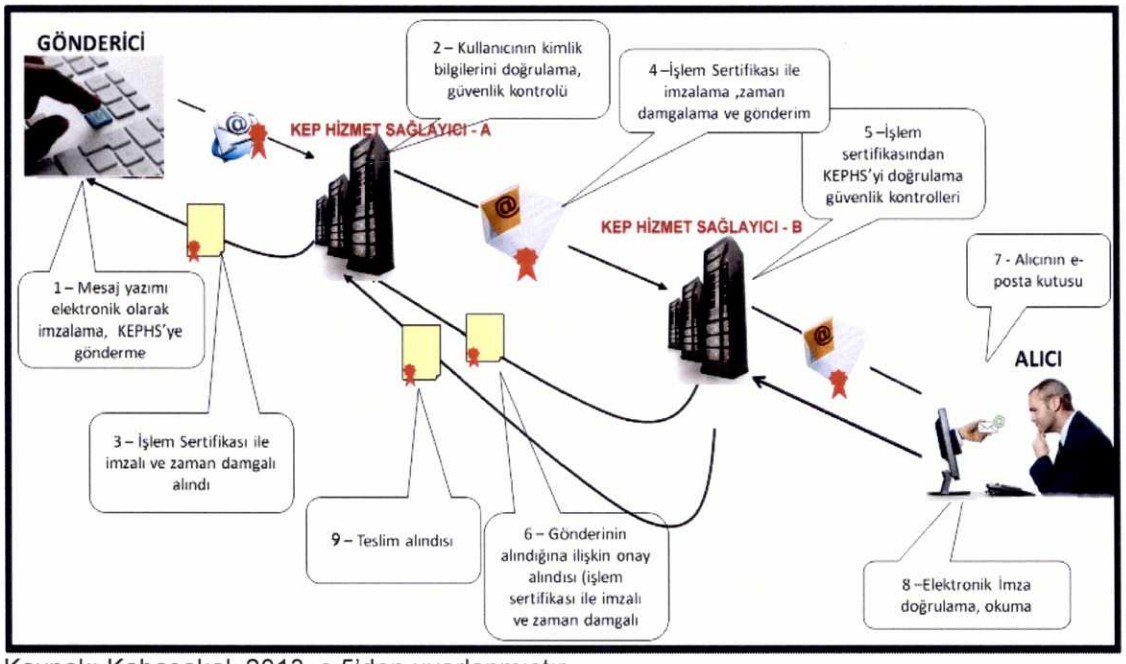
Başka görevlerinin yanı sıra elektronik platformlara ilişkin standart çalışmalarını da yönetmekte olan CEN'e Türkiye dahil 33 ülke üyedir. CEN tarafından tavsiye edilen standartlar, üye ülkelerin tümünde ulusal standartlar olarak da tanımlanmış durumdadır (CEN, 2009a).

CEN elektronik haberleşmede tarafların kimlik tanımlamalarının benzersiz olması gerekliliğine dikkat çekmektedir. Bu bağlamda e-posta ile bilgi ve belge paylaşımının hukuken geçerliliğinin sağlanmasına yönelik olarak ETSI'nin yukarıda bütünü gösterilen KEP standardı dokümanlarından ETSI TS 102 640-2: Elektronik İmzalar ve Altyapılar (ESI); "KEP: Mimari, Formatlar Politikalar ve Profiller" standardının "KEP'in İmzalanmış Delilleri için Veri

Gereksinimleri ve Formatları" başlıklı bölümünün kullanılmasını önermektedir (CEN, 2009b).

2.5.5. KEP sistemi çalışma adımları

Şekil 2-9 KEP'in Çalışma Prensibi



Kaynak: Kabasakal, 2013, s.5'den uyarlanmıştır.

Şekil 2-9'da gösterilen KEP sisteminin fonksiyonel şemasında belirtildiği üzere sistem aşağıdaki adımlar çerçevesinde çalışmaktadır (Kabasakal, 2013, s.4).

1. e-Posta göndericisi, oluşturduğu e-postasını göndermeden önce kendi güvenli e-imzasıyla imzalar ve yetkili bir Elektronik Sertifika Hizmet Sağlayıcıdan (ESHS) zaman damgası ile damgaladıktan sonra kayıtlı olduğu KEPHS'ye bağlanarak KEP adresi üzerinden gönderimini kendi KEPHS'sine yapar.
2. KEPHS kendisine gönderilen KEP sahibine ait kimlik doğrulaması ile güvenlik kontrolünü yapar.
3. KEPHS tarafından göndericiye, mesaj ile birlikte gönderenin kimliği, gönderilme tarihi, iletinin KEPHS tarafından teslim alındığına ilişkin bilgileri

içeren e-imza ile imzalanmış ve zaman damgası ile damgalanmış bir alındı belgesi gönderilir.

4. KEPHS, normal posta benzeri, göndericinin ve alıcının kimliğine dair bilgiler ve e-postaya ilişkin bilgiler ve e-postanın kendisinden oluşan bir gönderim zarfı hazırlar. Hazırladığı gönderim zarfını, güvenli e-imza altına alır ve hukuken geçerli olan zaman damgasını iliştirir. Bu şekilde belgede sonradan bir değişiklik yapılmadığına ilişkin güvenirlik teminatı oluşturan veri bütünlüğü garantisi sağlamış olur. Bu gönderim zarfı alıcının KEPHS'ne gönderilir.
5. Alıcının KEPHS'si göndericinin KEPHS'si tarafından kendisine iletilen gönderim zarfı üzerinde özgünlük, bütünlük, e-imza gibi güvenlik kontrollerini yapar.
6. Alıcının KEPHS'si, gönderici KEPHS'ne iletinin teslim alındığına dair bir gönderim zarfı yollar.
7. Alıcının KEPHS'si teslim aldığı gönderim zarfını, alıcının e-postasına gönderir.
8. Alıcı, e-postasına gelen gönderim zarfını, e-imzası ile ve doğrulama yaparak kullanır.
9. Alıcının KEPHS'si, e-postayı alıcıya iletmiş ise e-postayı gönderen kişiye "teslim edildi belgesi" gönderir. Tersi bir durum yani iletilemedi ise iletilemediğine dair "teslim edilemedi belgesi" gönderir.

KEP sisteminde yukarıda bahsedilen gönderim şekli ile e-posta tesliminin güvenliği ve hukuki geçerliliği sağlanmaktadır. Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 16 ncı maddesinin birincin fıkrasının (ı) bendine göre, *"KEP sisteminin tüm süreçlerine ve işleyişine ilişkin bilgi, belge ve elektronik veriler ile, işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kayıtları gizliliğini, bütünlüğünü ve erişilebilirliğini koruyarak en az yirmi yıl süreyle saklamakla"* ifadesi ile KEPHS'nin delilleri saklama yükümlülüğü getirilmiş ve süresi belirlenmiştir. KEPHS, bu süreç ile ilgili deliller ve işlem kayıtları istendiğinde taraflara veya ilgili makamlara sunar.

KEPHS'ler KEP hesabı kullanıcıları ile aralarındaki internet bağlantılarında halen SSL protokolünü kullanmaktadır. TNB KEPHS tarafından KEPHS'lerin birbirleri ile olan bağlantılarında kapalı devre VPN kullanımı düşünüldüğü ifade edilmektedir (ETLACAKUŞ, Sözlü Görüşme, 2013).

KEP sistemini kullanmak isteyen gerçek ve tüzel kişiler BTK tarafından yetkilendirilen KEPHS'lere başvurmak zorundadırlar. KEP hesabı edinmek isteyen gerçek kişiler nüfus cüzdanı, ehliyet gibi kimlik yerine geçen belgeler ile KEPHS'lere bizzat başvurarak veya KEPHS'lerin internet sayfalarından güvenli e-imzaları ile kolay bir şekilde gerçekleştirilebilmektedir. KEP hesabına erişim yine KEPHS'lerin internet siteleri üzerinden kolayca sağlanmakta ve yaygın şekilde bilinen standart e-posta ara yüzüne benzer bir ekranla, gelen e-postalara ulaşılabilmekte yeni bir e-posta e-imza ile imzalanarak muhataba gönderilebilmektedir. Bu uygulamalara ilişkin örnekler Ek 6-6'da yer almaktadır.

2.5.6. KEP sisteminin güvenlik özellikleri

KEPHS'lerce söz konusu KEP sisteminde üretilen deliller ve bu delillerin üretildiği verilerin öncelikli olarak korunması gerekmektedir. Ayrıca KEP sitemi tarafından üretilen mesajlar, gönderim zarfları ve iletilerinde gizlilik sağlanmalı ve ikincil öncelikte koruma altında tutulmalıdır. Güvenlik ihtiyaçlarının ve risklerin tespitinde ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi Standardı öncelik oluşturabilmektedir. Tüm bunlara ilaveten ISO/IEC 27002 Bilgi Güvenliği Yönetim Sistemi Uygulama Kodları standardının Tablo 2.2'de belirtilen bölümlerine uyumluluğun sağlanması gerekmektedir (Alkan vd, 2011, s.47-48).

Tablo 2.2 KEP Sisteminin Uyumlu Olması Talep Edilen ISO/IEC 27002 Güvenlik Özellikleri

Konu	Standardın İlgili Başlığı
Varlık yönetimi	Bölüm 7
İnsan kaynakları güvenliği	Bölüm 8
Fiziksel ve çevresel güvenliğin sağlanması	Bölüm 9
İletişim ve operasyon yönetimi	Bölüm 10
Erişim kontrollerinin denetimi	Bölüm 11
Bilgi sistemlerinin güvenlik gereksinimleri	Bölüm 12
Bilgi güvenliği olaylarının yönetimi	Bölüm 13
İş sürekliliği	Bölüm 14
Uygunluk	Bölüm 15

Kaynak: Alkan vd, 2011, s.48

2.5.6.1. Güvenli e-imza

Bilgi ve belge güvenliğinin sağlanmasında en önemli araçlardan birisi olan güvenli e-imza konusunda 5070 Sayılı Elektronik İmza Kanunu ile düzenleme yapılmıştır. KEP bünyesindeki en önemli unsurlardan birisi de güvenli e-imzanın ve zaman damgasının kullanılmasıdır.

5070 sayılı Elektronik İmza Kanun'u oluşturulur iken yabancı mevzuatta bulunan düzenlemeler ile Avrupa Komisyonu'nun e-imzalara ilişkin 99/93/EC sayılı Direktifi temel alınmıştır (Keser vd., 2004, s.8).

KEP sisteminde bulunması gereken bir başka güvenlik özelliği de günlük kayıtlarının en az günde bir defa kayıt altına alınması ve her seferinde zaman damgası ile damgalanmasıdır. Zaman damgası, istenilen herhangi bir zamana ilişkin günlük kayıtlarına kolayca erişilebilmesi ve bunların değiştirilemez olmasının sağlanması açısından önem arz etmektedir.

5070 sayılı Elektronik İmza Kanunu'nun 3 üncü maddesinde (h) bendinde belirtildiği üzere, "*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" şeklinde tarif edilmektedir. Bu nedenle zaman damgasının kullanılması KEP sisteminde delillerin hukuki boyutu ve işlemin kesin zamanının tespiti açısından önemlidir.

2.5.6.2. Kimlik doğrulama

KEP sistemi kullanıcılarının, sisteme erişimi esnasında kimlik doğrulamasından geçirilmesi gerekmektedir. Söz konusu kimlik doğrulaması, KEPHS'nin tercihine göre; bir kullanıcı adı ve şifre kullanımı yoluyla yapılabileceği gibi, güvenli elektronik imza, elektronik kimlik kartı vb. yöntemlerle de yapılabilir. Kimlik doğrulaması, KEP mesajının KEP sisteminde kayıtlı bir kullanıcı tarafından gönderilip gönderilmediğinin belirlenmesini sağlar (Alkan vd, 2011, s.49).

2.5.6.3. Güvenli etkileşim

KEP sisteminin bir başka güvenlik gereksinimi ise taraflar arasında iletilen KEP mesajlarının, inkâr edilemezliğini ve bütünlüğünü sağlamasıdır. Bu amaçla, KEP mesajları, gönderici tarafta zarf olarak nitelendirilen bir başka mesaj içine yerleştirilerek güvenli e-imza ile imzalanır. Alıcı tarafta ise zarf üzerinde bulunan güvenli e-imza doğrulanarak zarf açılmakta ve KEP mesajı alınmaktadır (Alkan vd, 2011, s.49).

KEP mesajını göndericiden alıcıya ileten her bağlantıda güvenli iletişim protokolleri kullanılır. Bu protokoller, genel olarak yukarıda incelenmiş olan TLS tabanlı olan IMAPS, POP3S, HTTPS; güvenli bir iletişimin aktivasyonunu gerektiren SMTP, STARTTLS, POP3STLS, güvenli bir iletişim kanalı sağlayan IPSec vb. olabilir.

2.5.6.4. Virüslerden korunma

İnternet tabanlı tüm bilişim sistemlerinde olduğu gibi, KEP sistemi de internet yoluyla yayılabilen virüs vb. kötücül yazılımlardan kaynaklanabilecek güvenlik riskleri ile karşı karşıya kalabilir. Böyle bir durumda sisteme kayıtlı tüm kullanıcıların zarar görme ihtimali vardır. KEPHS'nin söz konusu riskleri bertaraf etmek için gerekli tedbirleri alması gerekmektedir (Alkan, vd, 2011, s.50).

2.6. Kiralık Hat

Herhangi bir telekomünikasyon işletmecisinden kiralanmış, kablolu veya kablosuz, uçtan uca veri iletişimi sağlayan hatlara kiralık hat olarak adlandırılmakta olup (Çanakkale Onsekiz Mart Üniversitesi, 2013), 92/44/EC sayılı Avrupa Komisyonu Direktifi'nin 'Tanımlar' başlıklı 2 nci maddesinin ikinci fıkrasında, "*şebeke sonlanma noktaları arasında şeffaf iletim kapasitesi sağlamak için sunulan ve isteğe bağlı anahtarlama veya yönlendirme işlevini içermeyen telekomünikasyon altyapısı*" olarak tanımlanmaktadır. (BTK, 2013b).

Şebeke işletmecisi tarafından bir kullanıcıya tahsis edilmiş olan noktadan noktaya haberleşme kanalı veya devresi olarak tanımlanan (INTVEN, TETRAULT, 2000) geleneksel kiralık hatların yanı sıra özellikle bağlantı hızlarının artması ile birlikte İnternet üzerinden de kiralık hat hizmetleri sunulmaktadır. Diğer taraftan geleneksel kiralık hatlar üzerinden kullanıcılara İnternet erişimi de sağlanmaktadır (ATLAS ON-LINE, 2013).

Geleneksel olarak, TDM (Zaman Bölmeli Çoklama), SDH (Eşzamanlı Sayısal Sıradüzen) ve/veya WDM (Dalga Boyu Bölmeli Çoklama) vb. devre anahtarlamalı şebekeler üzerinden sunulmakla birlikte ATM (Eşzamansız İletim Modu) veya MPLS/IP-MPLS (Çok Protokollü Etiket Anahtarlama), FR (Çerçeve Röle), Metro Ethernet, ADSL (Asimetrik Sayısal Abone Hattı) gibi

paket anahtarlamalı şebekeler üzerinden sunulan kiralık hat hizmetleri de bulunmaktadır. (BTK, 2013b).

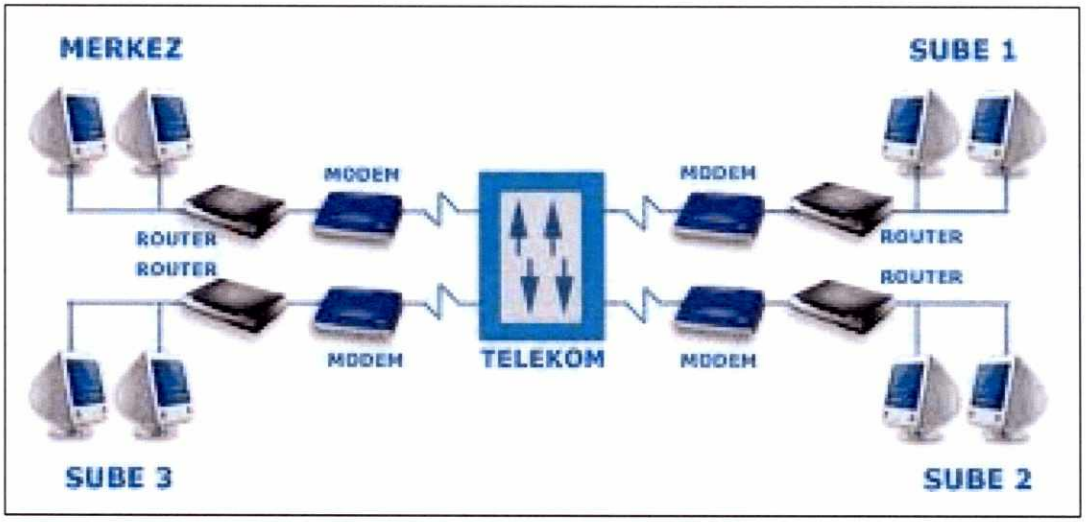
Farklı şebekeler veya sonlanma noktaları arasında doğrudan ve adanmış bir bağlantı şekli olan kiralık hat ile birden fazla nokta arasında e-belgeler de SSL, VPN, FTP gibi yöntemler kullanılarak güvenli şekilde paylaşılabilmekte olup Çebi (2013) kiralık hatlara ve söz konusu hatların gerekliliklerine ilişkin olarak aşağıdaki hususları belirtmektedir;

Farklı şebekeler arasında doğrudan bağlantı şekli olan kiralık hat uygulamasını Çebi (2013) aşağıdaki şekilde ifade etmiştir;

- ✓ Kiralık hatlar, iki veya daha fazla noktada bulunan şebekeler arasında tesis edilen ve söz konusu şebekeleri direkt olarak birbirine bağlayan bir hat olarak tanımlanabilir
- ✓ Bilgi ve e-belge paylaşımı için bağlantı kurulmak istenen noktalara ilave edilen modemler vasıtası ile bağlantı gerçekleştirilmekte, her iki nokta arasında sabit hatlar tesis edilmektedir
- ✓ Bağlantı sağlanmak isteyen noktaların sayıları arttıkça tesis edilmesi gereken hat sayısı da artar

Şekil 2-10'da kiralık hatların kullanımına ilişkin bir örneğe yer verilmiştir.

Şekil 2-10 Kiralık Hat kullanımı



Kaynak: ERİZA, 2013

3. e-BELGEYE İLİŞKİN MEVZUAT VE STANDARTLAR

3.1. Ülkemizde Durum

Ülkemizde e-ortamda birlikte çalışabilirlik konusunda 2009 yılında DPT (günümüzde Kalkınma Bakanlığı) koordinatörlüğünde yapılan çalışmalar kapsamında, e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi hazırlanmıştır. Bu Rehber'in amacı; *"başta kamu kurumları olmak üzere kamuya e-ortamda hizmet veren bütün kurumlar arasında birlikte çalışabilirliği sağlamak ve bu çerçevede yetki, sorumluluk, esas, prensip yöntem ve kriterler ile teknik standartları belirlemek"* şeklinde ifade edilmiştir. Rehber;

- ✓ *Genel esaslar ve birlikte çalışabilirlik politikası,*
- ✓ *Bilginin sunumu, taşınması, değişimi, entegrasyonu, güvenliği ve geliştirilen çözümlerin yaşam döngülerine ilişkin teknik standartlar,*
- ✓ *Önümüzdeki dönemde yürütülecek Rehber'i tamamlayıcı nitelikteki çalışmalar"*

şeklinde üç bölümden oluşmaktadır.

> "Birlikte çalışabilir e-devlet yapısı farklı gruplar için farklı birlikte çalışabilirlik ihtiyaçları taşır. Bunlardan ilki, sistemin doğrudan kullanıcısı olan ve sistemle ilişkilerden doğrudan etkilenen vatandaştır. İkinci grup iş dünyası olup, veri değişimi ihtiyaçları bir öncekine göre daha karmaşıktır. Rehber'in odak noktası; kamunun, gerek merkezi kurum ve kuruluşları, gerekse yerel yönetimleri içerecek şekilde, kendi içinde birlikte çalışabilirliğinin sağlanması ve buna karşılık gelen ihtiyaçların belirlenmesi ve karşılanmasıdır" (DPT, 2009, s.3).

e-Belgenin yaşam döngüsü ile birlikte e-ortamı oluşturan yazılım ve donanım tercihi, birlikte çalışabilirlik, kalite, tutarlılık gibi faktörler bir bütün olarak düşünülmelidir. Oluşturulan, işlenen, kullanılan, paylaşılan, arşivlenen ve imha edilen e-belgelerde ulusal ve uluslararası kurumlar tarafından geliştirilen standartlara ve mevzuata uygunluk bir zorunluluktur.

3.1.1. Ulusal mevzuatta e-belgeye ilişkin düzenlemeler

e-Belge mevzuat düzenlemeleri; Vergi Mevzuatı, Bankacılık Mevzuatı, Bilgi Edinme Kanunu, Türk Ticaret Kanunu ve e-İmza Kanunu gibi düzenlemelere dayanmaktadır. Ayrıca Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik, Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik, Devlet Arşiv Hizmetleri Hakkında Yönetmelik, 2008/16 Sayılı Başbakanlık Genelgesi (e-Belge Standartları) konu ile ilgili çeşitli hususları içermektedir (Tablo 3-1).

04/12/2003 tarihli ve 2003/48 sayılı Başbakanlık Genelgesi ile e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı uygulamaya konulmuş ve e-Dönüşüm Türkiye İcra Kurulu oluşturulmuştur. Bahsi geçen Kurul tarafından hazırlanan ve Eylül 2004 tarihinde Kalkınma Bakanlığı tarafından yayımlanan e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı'nda bulunan hedeflerden bazıları şunlardır;

- ✓ *"Elektronik ortamdaki sözleşmelerin tanınması için bir çalışma yapılması ve gerekliliği halinde yasal düzenlemelerin tamamlanması*
- ✓ *Elektronik ortamda fikrî hakların korunması için gerekli yasa çalışmasının yapılması*
- ✓ *Dış ticarette e-belge uygulamalarının yaygınlaştırılması*
- ✓ *Vergi beyanı, tahakkuku ve ödemelerinin elektronik ortamda yapılmasının sağlanması*
- ✓ *Tarihi arşivlerdeki tasnifi tamamlanan belgelere ait katalog bilgileri ile görüntülerinin elektronik ortamda hizmete sunulması*
- ✓ *Birinci basamak sağlık kurumlarında elektronik sağlık kaydının oluşturulması*
- ✓ *Dış ticarette e-belgenin uluslararası dolaşımının sağlanması"*

e-Dönüşüm Türkiye İcra Kurulu, Yüksek Planlama Kurulunun (YPK) onayına sunulmak üzere Eylem Planı hazırlamıştır. e-Dönüşüm Türkiye Projesi

kapsamında 2005 Yılı Eylem Planı, YPK tarafından onaylanarak 24/03/2005 tarihinde bir tebliğ ile yayımlanmıştır. Söz konusu Eylem Planı'nın 37 nci maddesinde "*Elektronik ortamlarda üretilecek, kayıt altına alınacak, başka birimlere ya da kurumlara iletilecek, saklanacak ya da gerektiğinde imha edilecek elektronik bilgi ve belgelerin kayıt, iletim, paylaşım, imha ve güvenlik açılarından tabi olacakları usul ve esaslar ile, kurumlarda oluşturulacak elektronik kayıt sistemlerinin birbirleriyle uyumlu işlemesi ve etkin bir şekilde yönetilmesine ilişkin asgari standartların belirlenmesi hususlarında çalışmalar yapılacaktır*" şeklinde bir görev tanımı yapılmıştır.

Söz konusu görev Devlet Arşivleri Genel Müdürlüğüne ve daha sonra Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümüne verilmiştir. Çalışmalar neticesinde sistem kriterleri, belge kriterleri ve üst veri elemanları başlıkları ile üç bölüm olarak hazırlanan standart, TS 13298 Elektronik Belge Yönetimi adı ile Haziran 2007'de yayımlanmış ve anılan standartta 2009 yılında güncelleme yapılmıştır (Kandur, 2011, s.6).

Tablo 3.1 Yasal Düzenlemeler ve Standartlar

Kurum/Kanun No Yönetmelik	Konusu	Resmi Gazete Tarihi	Resmi Gazete Sayı
BAŞBAKANLIK	Devlet Arşiv Hizmetleri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik	08/08/2001	24487
2004/8125	Resmî Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik	02/12/2004	25658
Devlet Arşivleri Genel Müdürlüğü	Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli	2006	
2008/16	Elektronik Belge Standartları Genelgesi	16/07/2008	26938
TS	TS 13298 Elektronik Belge Yönetimi Standardı	29/06/2009	
BTK	Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik	06/01/2005	25692
BTK	Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ	06/01/2005	25692
6099	Tebligat Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun	19/01/2011	27820
Adalet Bakanlığı	Elektronik Tebligat Yönetmeliği	19/01/2013	28533
BDDK	Kartları ve Kredi Kartları Hakkında Yönetmeliği	10/03/2007	26458
e-Dönüşüm Türkiye İcra Kurulu	e-Dönüşüm Türkiye İcra Kurulu Kararı	15/07/2009	28
6102	6102 Sayılı Türk Ticaret Kanunu	14/02/2011	27846
BTK	Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik	25/08/2011	28036
BTK	Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ	25/08/2011	28036
BTK	İşlem Sertifikasına İlişkin Usul ve Esaslar	06/06/2012	2012/DK-15/249
4982	Bilgi Edinme Hakkı Kanunu	24/10/2003	25269
2004/7189	Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik	27/04/2004	25445
4731	17/8/1999 ve 12/11/1999 Tarihlerinde Meydana Gelen Depremlerden Zarar Görenlerin Vergi Borçları ve Vergi Cezalarının Terkini ile Vergi Usul Kanunu, Katma Değer Vergisi Kanunu, Harçlar Kanunu ve Organize Sanayi Bölgeleri Kanununda Değişiklik Yapılması Hakkında Kanun	30/01/2001	24626
5070	Elektronik İmza Kanunu	23/01/2004	25355
BTK	Elektronik Haberleşme Güvenliği Yönetmeliği	20/07/2008	26942
BTK	Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ	16/05/2012	28294
Gümrük ve Ticaret Bakanlığı	Ticaret Şirketlerinde Anonim Şirket Genel Kurulları Dışında Elektronik Ortamda Yapılacak Kurullar Hakkında Tebliğ	29/08/2012	28396

3.1.1.1. Vergi Usul Kanunu

e-Belge, elektronik defter ve elektronik kayıt tanımları mevzuatımızda ilk olarak 2001 yılında Vergi Usul Kanunu ile düzenlenmiştir. 30/12/2001 tarihli ve 4731 sayılı Kanunun 4 üncü maddesi ile 04/01/1961 tarihli ve 213 sayılı Vergi Usul Kanunu'nun 242 nci maddesine eklenen 2 nci fıkrada e-belge "*şekil hükümlerinden bağımsız olarak bu Kanuna göre düzenlenmesi zorunlu olan belgelerde yer alan bilgileri içeren elektronik kayıtlar bütünüdür*" şeklinde yer almıştır. Kanun'un aynı fıkrasında elektronik defter, "*Elektronik defter, şekil hükümlerinden bağımsız olarak bu Kanuna göre tutulması zorunlu olan defterlerde yer alması gereken bilgileri kapsayan elektronik kayıtlar bütünüdür*" şeklinde ifade edilmiştir. Söz konusu kanunun devamında "*Elektronik kayıt, elektronik ortamda tutulan ve elektronik defter ve belgeleri oluşturan, elektronik yöntemlerle erişimi ve işlenmesi mümkün olan en küçük bilgi öğesini ifade eder*" hükmü ile elektronik kayıt tanımlamıştır.

Ülkemizde 2001 yılında ticaret alanında başlayan yasallaştırma süreci gereği e-belge, elektronik defter ve elektronik kayıt mevzuatta tanımlanmış olup BİT'deki gelişmelere paralel olarak mevzuatımız bu konuda yenilenmeye devam etmektedir.

e-Belgenin güvenliği konusunda, 5228 sayılı Kanun ile 213 sayılı Kanunun 257 nci maddesinin birinci fıkrasının (4) numaralı bendi "*Bu Kanunun 149 uncu maddesine göre devamlı bilgi vermek zorunda olanlardan istenilen bilgiler ile vergi beyannameleri ve bildirimlerin, şifre, elektronik imza veya diğer güvenlik araçları konulmak suretiyle internet de dahil olmak üzere her türlü elektronik bilgi iletişim araç ve ortamında verilmesi, beyanname ve bildirimlerin yetki verilmiş gerçek veya tüzel kişiler aracı kılınarak gönderilmesi hususlarında izin vermeye veya zorunluluk getirmeye, beyanname, bildirim ve bilgilerin aktarımında uyulacak format ve standartlar ile uygulamaya ilişkin usul ve esasları tespit etmeye, bu zorunluluğu*

beyanname, bildirim veya bilgi çeşitleri, mükellef grupları ve faaliyet konuları itibarıyla ayrı ayrı uygulatmaya,...." şeklinde güncellenmiştir.

Söz konusu maddeye ilave fıkrada e-ortamda belge kabul edileceği şu şekilde belirtilmiştir: *"Birinci fıkranın (4) numaralı bendi uyarınca Maliye Bakanlığının beyanname ve bildirimlerin yetki verilmiş gerçek veya tüzel kişiler aracı kılınarak gönderilmesi hususunda izin vermesi veya zorunluluk getirmesi halinde, (mükellef veya vergi sorumlusu ile gönderme işini yapacak kişiler arasında özel sözleşme düzenlenmek kaydıyla) elektronik ortamda gönderilen beyanname ve bildirimler, mükellef veya vergi sorumlusu tarafından verilmiş addolunur".*

Ticaret hayatında belgelerin, e-ortamda oluşturulması ve iletilmesine ilaveten güvenliğinin sağlanması için e-imza, şifre gibi güvenlik araçlarının kullanılmasından bahsedilmesi söz konusu kanunda yapılan değişiklikler ile e-belgenin hukuki geçerliği konusunda önemli bir çalışma olmuştur.

3.1.1.2. Bilgi Edinme Hakkı Kanunu ve Yönetmeliği

Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde uygulanmak üzere 24/10/2003 tarihli ve 25269 sayılı Resmi Gazete'de yayınlanan 09/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 3 üncü maddesinde belge; "*Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plan, film, fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcıları*" şeklinde tanımlanmıştır.

Söz konusu Kanun kapsamında bilgi edinme başvurularının geleneksel yöntemler ile yapılabileceği gibi, 6 ncı maddesinde belirtildiği şekilde e-ortamda da yapılabileceği, 12 nci maddesinde ise başvuruya cevapların yazılı veya e-ortamda başvuru sahibine bildirileceği belirtilmiştir.

Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik ise 27/04/2004 tarihli ve 25445 sayılı Resmi Gazete'de yayımlanmıştır. Mezkûr Yönetmeliğin Kapsam başlıklı 2 nci maddesinde, bu Yönetmeliğin tüm kamu kurum, kuruluş ve kurulları ile kamu kurum niteliğindeki meslek kuruluşlarını bağlayacağı hüküm altına alınmıştır. Bahsi geçen Yönetmeliğin geçici 4 üncü maddesinde "*Kurumsal internet sayfası bulunmayan kurum ve kuruluşlar iki ay içinde internet sayfalarını oluştururlar*" ifadesi ile kamu kurum ve kuruluşlarının elektronik ortamda bilgi edinme başvurularını kabul edebilir altyapıyı oluşturmaları gerekmektedir.

Söz konusu Yönetmeliğin geçici 5 inci maddesinde yer alan, "*Kurum ve kuruluşların bilgi edinme birimleri iki ay içinde elektronik posta yoluyla başvuru kabul edecek elektronik posta adreslerini oluşturarak internet sayfalarından kamuoyunun bilgisine sunarlar*" ifadesi ile kamu kurum ve kuruluşlarının e-ortamda bilgi edinme başvuruları için e-posta adreslerini belirleyerek kamuoyuna duyurması gerekliliği belirtilmiştir. Yönetmeliğin 6 ncı maddesinde ise, dosya planlarını, faaliyet raporlarını, kanun, tüzük, yönetmelikler, Bakanlar Kurulu Kararları, diğer düzenleyici işlemler ve mevzuat değişiklikleri gibi bilgi ve belgeleri kamu kurum ve kuruluşlarınca BİT marifetiyle yayınlamalarının gerektiği belirtilmektedir.

Ayrıca bilgi edinme başvurularının e-ortamda yapılabilmesi için gerçek ve tüzel kişiler adına iki ayrı başvuru formu belirlenmiştir. Başvurulara cevap verme yöntemleri ise elektronik yolla yapılan başvuruda belirtilen e-posta adresine veya yazılı şekilde olabileceği ifade edilmiştir. Mezkûr Yönetmeliğin 10 uncu maddesinde, e-ortamda yapılan başvurular için Yönetmeliğin ekinde yer alan formların kullanılmasının zorunlu olduğu, ancak bu formun ilgili kurum ve kuruluşun internet sitesi üzerinden çevrimiçi yolla veya doldurulmuş formların e-posta yoluyla gönderilebileceği belirtilmiştir. Ayrıca e-ortamda sadece bilgi edinme başvuru formları ile değil e-imzalı belgeler ile de başvuru yapılabileceği belirtilmektedir (Eken, 2005, s. 143).

Söz konusu Yönetmeliğin "Başvuruların kabulü, değerlendirilmesi ve işleme konulması" başlıklı 14 üncü maddesinde, e-ortamda yapılan başvurularda, başvuru sahibinin verdiği T.C. kimlik numaraları, ad ve soyadlarının İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünün internet sayfasından kişinin beyan ettiği bilgilerle tutarlılık tespiti yapılabileceğini ifade etmektedir. Kurum içerisinde, elektronik başvuruların ilgili birimlere e-ortamda veya başvurunun yazıcı çıktısı alınarak yönlendirilmesi ifade edilmiştir.

Hız ve Yılmaz'a (2004, s.77) göre, bilgi edinme başvuruları için söz konusu Yönetmelikle belirlenen formların kullanılması mecburiyeti, Bilgi Edinme Kanunu'nun ruhuna aykırı olacaktır. Ancak kullanım kolaylığı ve başvurunun geçerli sayılması için bildirilmesi şart olan bilgilerin eksiksizliğini sağlaması sebebiyle bu uygulamanın başvuru sahiplerinin yararına olduğundan sürdürülmesi faydalı olacaktır.

e-Ortamda gerçek kişiler için Şekil 3-1'de tüzel kişiler için ise Şekil 3-2'de belirlenen bilgi edinme başvuru formları aşağıda gösterilmiştir.

Şekil 3-1. Gerçek Kişiler İçin Başvuru Formu

BİLGİ EDİNME BAŞVURU FORMU

Gerçek Kişiler İçin

TC Kimlik No * 0 — TC Kimlik Numaranızı öğrenmek için tıklayınız!

Adı *

Soyadı *

Cinsiyeti *

Adres *

Posta Kodu 0

Telefon 0

Cep Telefonu 0

Faks 0

İl *

İlçe *

Cevap Şekli *

E-Posta Adresi *

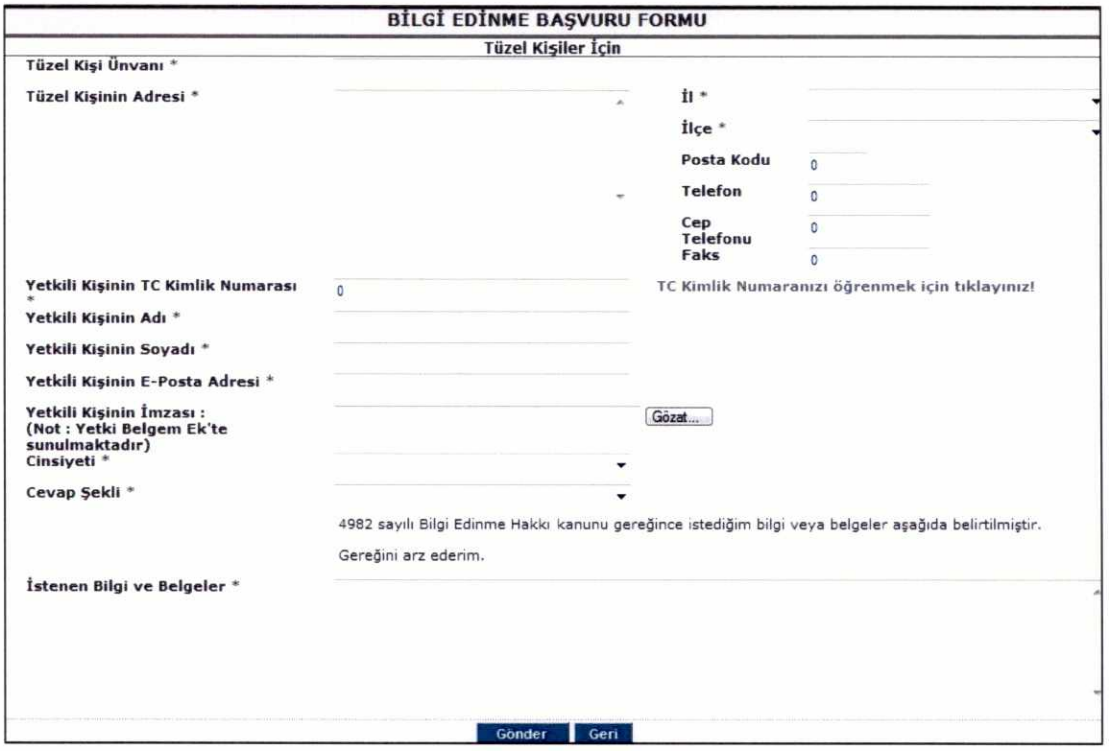
4982 sayılı Bilgi Edinme Hakkı kanunu gereğince istediğim bilgi veya belgeler aşağıda belirtilmiştir.
Gereğini arz ederim.

İstenen Bilgi ve Belgeler *

Gönder | Geri

Kaynak: BTK, 2013a

Şekil 3-2. Tüzel Kişiler İçin Başvuru Formu



BİLGİ EDİNME BAŞVURU FORMU

Tüzel Kişiler İçin

Tüzel Kişi Ünvanı *

Tüzel Kişinin Adresi *

İl *

İlçe *

Posta Kodu

Telefon

Cep Telefonu

Faks

Yetkili Kişinin TC Kimlik Numarası *

TC Kimlik Numaranızı öğrenmek için tıklayınız!

Yetkili Kişinin Adı *

Yetkili Kişinin Soyadı *

Yetkili Kişinin E-Posta Adresi *

Yetkili Kişinin İmzası : (Not : Yetki Belgem Ek'te sunulmaktadır)

Gözat...

Cinsiyeti *

Cevap Şekli *

4982 sayılı Bilgi Edinme Hakkı kanunu gereğince istediğim bilgi veya belgeler aşağıda belirtilmiştir.

Gereğini arz ederim.

İstenen Bilgi ve Belgeler *

Gönder Geri

Kaynak: BTK, 2013a

3.1.1.3. Elektronik İmza Kanunu ve ikincil düzenlemeler

23/01/2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanan, 5070 sayılı Elektronik İmza Kanunu'nun 3 üncü maddesinin (b) bendinde "*Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" şeklinde tanımlanmıştır. e-İmzanın ıslak imza ile aynı yasal geçerliliğe sahip kılınması ise bu Kanun'un 22 nci maddesi ile "*Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir*" ifadesinin Borçlar Kanununa eklenerek sağlanmıştır.

5070 sayılı Elektronik İmza Kanunu'nun 4 üncü maddesinde "*güvenli elektronik imza; münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini*

sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan", şeklinde tanımlanmış ve söz konusu Kanun'un 5 inci maddesinde de güvenli e-imzanın, elle atılan imza ile aynı hukukî sonucu doğuracağı hüküm altına alınmıştır. Bununla birlikte aynı Kanun'un 23 üncü maddesi ile 18/06/1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu'nun 295 inci maddesine "*Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.*" hükmü eklenerek e-ortamda güvenli e-imza ile oluşturulan verilerin senet hükmünde olduğu belirtilmiştir.

06/01/2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanan e-İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile e-İmzanın hukuki ve teknik yönleri, uygulanması, ESHS ve e-imza kullanım sürecindeki aktörlerin yükümlülükleri belirlenmiştir.

e-İmzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirlemek amacı ile 06/01/2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanan, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in kapsamı; nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve hizmetlerine ilişkin teknik hususlardır.

Hâlihazırda Elektronik Bilgi Güvenliği A.Ş. (E-Güven), TUBİTAK-UEKAE (Kamu Sertifikasyon Merkezi), TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş., EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (E-Tuğra), Emniyet Genel Müdürlüğü Sertifikasyon Merkezi (EGMSM) olmak üzere 5 adet ESHS BTK tarafından yetkilendirilmiştir.

Güvenli e-imza ile günümüz teknolojilerini kullanarak iş ve işlemlerin güvenli bir şekilde gerçekleştirilmesi sayesinde verimliliğin artırılması, iş süreçlerinin hızlanması, bürokrasinin azaltılması, küreselleşmenin getirdiği yeni dünya düzeni ile bütünleşilmesi, küresel ticari pazarlara açılınması ve geleneksel yöntem olan kâğıttan e-belgeye dönüşüm mümkün olabilecektir (Sağıroğlu ve Alkan, 2005).

5070 sayılı Elektronik İmza Kanunu'nda yer alan güvenli e-imza ile imzalanmış e-belgenin hukuki kanıt olacağı hükmünden sonra mevzuatımızda artarak e-belgeye yer verilmeye başlanmış olması beklenir.

3.1.1.4. Tebligat Kanunu'nda Değişiklik Yapılmasına Dair Kanun

19/01/2011 tarihli ve 27820 sayılı Resmi Gazete'de yayımlanan 6099 sayılı Tebligat Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 2 nci maddesinde *"Tebligata elverişli bir elektronik adres vererek bu adrese tebligat yapılmasını isteyen kişiye, elektronik yolla tebligat yapılabilir. Anonim, limited ve sermayesi paylara bölünmüş komandit şirketlere elektronik yolla tebligat yapılması zorunludur."* hükmü ile e-tebligat ticaret hayatında asli yol olarak gösterilmiştir. Aynı maddede yer alan *"Elektronik yolla tebligat, muhatabın elektronik adresine ulaştığı tarihi izleyen beşinci günün sonunda yapılmış sayılır"* ifadesi yer almaktadır. Söz konusu Yönetmeliğin 2 inci maddesinin son paragrafında *"Bu maddenin uygulanmasına ilişkin usûl ve esaslar yönetmelikle belirlenir"* ifadesi üzerine Adalet Bakanlığı tarafından yayımlanan 19/01/2013 tarihli ve 28533 sayılı Elektronik Tebligat Yönetmeliği'nin 3 üncü maddesinin (b) bendinde *"Elektronik tebligat adresi: Muhatap ve tebligatı çıkaran merciye ait olan elektronik tebligata elverişli kayıtlı elektronik posta adresini"* şeklinde ifade edilerek e-tebligatların KEP sistemi ile yapılmasının gerekliliği ortaya çıkmaktadır.

Bununla paralel olarak 14/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu'nun 18 inci maddesinin üçüncü

fıkrasında tacirler arasında ihbar veya ihtarların, güvenli e-imza kullanılarak KEP sistemi ile yapılabileceği ifade edilmiştir.

3.1.1.5. Elektronik Tebligat Yönetmeliği

Adalet Bakanlığı tarafından hazırlanan ve 19/01/2013 tarihli ve 28533 sayılı Resmi Gazete'de yayımlanan Elektronik Tebligat Yönetmeliği, e-ortamda yapılacak tebligatlara ilişkin usul ve esasları düzenlemektedir. Yönetmelik çerçevesinde; Genel yönetim altında bulunan kamu kurum ve kuruluşları ile yargı makamları, il özel idareleri, belediyeler, köy hükmi şahsiyetleri, barolar ve noterler tarafından PTT vasıtasıyla yapılacak elektronik tebligatları kapsamaktadır.

Söz konusu Yönetmelik, Tebligat Kanununun içerdiği düzenlemeyle uyumlu biçimde anonim, limited ve sermayesi paylara bölünmüş komandit şirketlere, elektronik yolla tebligat yapılması zorunluluğu getirilmiş olup gerçek kişiler ve diğer tüzel kişilerin ise elektronik tebligattan (e-Tebligat) isteğe bağlı olarak yararlanabilecekleri hükmü getirilmiştir.

3.1.1.6. Türk Ticaret Kanunu

14/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan Türk Ticaret Kanunu'nun 1525 inci maddesinin birinci fıkrasında "*ihbar, ihtar gibi ticari faaliyetlere ilişkin elektronik beyanlar ise Tarafların açıkça anlaşmaları ve 18 inci maddenin üçüncü fıkrası saklı kalmak şartıyla, ihbarlar, ihtarlar, itirazlar ve benzeri beyanlar; fatura, teyit mektubu, iştirak taahhütnamesi, toplantı çağrıları ve bu hüküm uyarınca yapılan elektronik gönderme ve elektronik saklama sözleşmesi, elektronik ortamda düzenlenebilir, yollanabilir, itiraza uğrayabilir ve kabul edilmişse hüküm ifade eder*" ifadesi ile karşılıklı anlaşmaya ve rızaya dayalı olmak şartıyla e-ortamda işlem yapılabileceği hüküm altına alınmıştır.

KEP ise 1525 inci maddenin ikinci fıkrasında "*Kayıtlı elektronik posta sistemine, bu sistemle yapılacak işlemler ile bunların sonuçlarına, kayıtlı posta adresine sahip gerçek kişilere, işletmelere ve şirketlere, kayıtlı elektronik posta hizmet sağlayıcılarının hak ve yükümlülüklerine, yetkilendirilmelerine ve denetlenmelerine ilişkin usul ve esaslar Bilgi Teknolojileri ve İletişim Kurumu tarafından bir yönetmelikle düzenlenir. Yönetmelik bu Kanunun yayımı tarihinden itibaren beş ay içinde yayımlanır*" şeklinde yer almıştır.

3.1.1.7. KEP sistemine ilişkin düzenlemeler

e-Dönüşüm Türkiye İcra Kurulu'nun 15/07/2009 tarihli ve 28 sayılı, Kayıtlı Elektronik Posta Sistemi konulu kararı şu şekildedir. "*Elektronik ortamdaki iş ve işlemlerin teknik olarak güvenli ve hukuken geçerli bir şekilde farklı taraflar arasında yapılabilmesine olanak sağlayan Kayıtlı Elektronik Posta Sistemi 26 Aralık 2008 tarihli ve 26 sayılı toplantısında İcra Kurulumuzca ele alınmıştır. Kurulumuz, değerlendirmeleri neticesinde, Bilgi Teknolojileri ve İletişim Kurumu ile Başbakanlık ve Adalet Bakanlığı'nın konu üzerinde birlikte çalışmalar yapmasını Kararlaştırmıştır. Karar doğrultusunda mezkûr kurumların yaptığı ve Kurulumuza arz edilen çalışmalar değerlendirilmiş ve Bilgi Teknolojileri ve İletişim Kurumu Kayıtlı Elektronik Posta Sistemi Konusunda düzenleyici çerçevenin oluşturulması amacıyla çalışmalar yapmak üzere görevlendirilmiştir.*"

Söz konusu Kararı müteakip 13/01/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu'nun 1525 inci maddesine dayanılarak düzenlenmiş olan ve 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelikte, KEP sisteminin hukuki, teknik yönleri ve işleyişi konusunda usul ve esaslar düzenlenmektedir. Söz konusu Yönetmelik;

- ✓ KEP sistemine

- ✓ Yapılacak olan işlemler ve sonuçlarına
- ✓ Kayıtlı elektronik posta adresi sahiplerine
- ✓ KEPHS'lerin hak ve yükümlülüklerine
- ✓ KEPHS'lerinin yetkilendirmelerine
- ✓ KEPHS'lerinin denetimlerine

ilişkin usul ve esasları kapsamaktadır.

Aynı Yönetmelik'te, KEP üzerinden yapılan işlemlerde bilgi ve belgenin güvenliği konusuna, 5 inci maddesinin (f) ve (g) bentlerinde yer verilmiştir. Yönetmeliğin 14 üncü maddesinde ise KEPHS'ler tarafından KEP sisteminde sadece elektronik iletinin karşılıklı alış verişi değil aynı zamanda e-belgenin saklanması ve gerektiğinde üçüncü taraflara kanıt olabilecek hizmetlerin de sunulması sağlanmıştır.

Yönetmeliğin 15 inci maddesinde belirtilen; KEPHS'nin KEP sistemi ile sunduğu hizmetlere ait kayıtlar ile KEP delillerinin senet hükmünde olduğu, aksi ispat edilinceye kadar kesin delil sayılacağı belirtilirken KEP sisteminin en önemli özelliği ortaya konulmuştur. Ayrıca KEP hesabı kullanılarak yapılan bütün işlemlere ait hukuki sonuçların hesap sahibini bağlayacağı ifade edilmiştir.

Anılan Yönetmeliğe dayanarak çıkartılan ve 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlan KEP sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, KEP sistemine ilişkin süreçleri ve teknik kriterleri detaylı olarak düzenlemektedir. Kapsam olarak ise KEPHS'nin işleyişine, KEPHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline ve hizmetlerine ilişkin teknik hususları içermektedir.

Mezkûr Tebliğ ile "Kayıtlı elektronik posta hizmet sağlayıcısının işleyişi" başlığı altında bulunan 5 inci maddesinde KEPHS, işleyişinin bütün

aşamalarında ETSI TS 102 640, standardına uyacaklarını belirtmektedir. "Algoritma ve parametreler" başlığı altında ise KEPHS, elektronik imza, işlem sertifikası ve özetleme algoritmalarına ilişkin olarak 06/01/2005 tarih ve 25692 sayılı Resmî Gazete'de yayımlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in "Algoritmalar ve Parametreler" başlığı altında bulunan 6 ncı (Değişik: RG-30/1/2013-28544) maddesinde, *İmza oluşturma ve doğrulama verileri ile özetleme algoritmalarının, ETSI TS 102 176-1 standardına ve aşağıda yer alan şartlara uygun olması gerekir.*

a) İmza sahibinin imza oluşturma ve doğrulama verileri:
i. RSA için en az 2048 bit veya
ii. DSA için en az 3072 bit veya
iii. DSA Eliptik Eğrisi için en az 256 bit
b) ESHS'nin imza oluşturma ve doğrulama verileri:
i. RSA için en az 2048 bit veya
ii. DSA için en az 3072 bit veya
iii. DSA Eliptik Eğrisi için en az 256 bit
c) Özetleme algoritması:
i. SHA-256 veya
ii. SHA-384 veya
iii. SHA-512 veya
iv. WHIRLPOOL

şartlara uyar ifadesi yer almaktadır. "Kayıtlı elektronik posta uygulama esasları" başlığı altında bulunan 7 inci maddesinde ise KEPHS'lerin; KEP uygulama esaslarını ETSI TS 102 640 standardına uygun olarak hazırlayacaklarını ve KEPHS, her KEP hesabı için en az 100 MB depolama alanı sunacaklarını gönderilen ve alınan orijinal iletilerin büyüklük sınırlaması 10 MB'nin altında olamayacağını, Depolama alanı dolduğunda KEPHS ilgili KEP hesabından orijinal ileti gönderilmesinin engellenebileceğini ancak ileti alınmasını engelleyemeyeceğini belirtilmiştir. "Güvenlik kriterleri" başlığı altında bulunan 8 inci maddesinde ise KEPHS, güvenlik kriterlerine ilişkin olarak; ETSI TS 102 640, TS ISO/IEC 27001 veya ISO/IEC 27001, BS 10012 ve ISO/IEC 27031 standartlarına uyacaklarını beyan etmiştir. "Erişilebilirlik" başlığı altında bulunan 9 uncu maddesinde ise KEPHS, engelli kişilerin KEP sisteminden yararlanmalarını sağlamak amacıyla W3C'nin "Web erişilebilirlik girişim yönergesi" (Web Content Accessibility Guidelines)'ne uyar şeklinde

ifade edilmiştir. "Belgeler" başlığı altında bulunan 10 uncu maddesinde ise *KEPHS;*

a) TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğunu,

b) Elektronik imza oluşturma araçlarının;

i. FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

ii. CWA 14167-2'de belirtilen kriterlere uygunluğunu veya

iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu yetkili kurum veya kuruluşlardan alınan belgelerle belgelendirir şeklinde belirtmiş olup bir alt madde olarak ise KEPHS'nin BS 10012 ve ISO/IEC 27031 standartlarına uygunluğunu BTK'ya beyan etmesi gerektiği hüküm altına alınmıştır.

16/05/2012 tarihli ve 28294 sayı ile Resmi Gazete'de yayımlanan, Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, kayıtlı elektronik posta hesabı adreslerinin yapısına ve kayıtlı elektronik posta rehberinin oluşturulmasına, güncellenmesine, işletilmesine ve kullanılmasına ilişkin usul ve esasları belirlemektedir. Bu Tebliğ, KEP sistemini kuran ve işleten KEPHS ile bu sistemden hizmet alan tarafları kapsamaktadır.

06/06/2012 tarihli ve 2012/DK-15/249 sayılı Kurul kararı ile "Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul ve Esaslar" düzenlenmiştir. Bu düzenleme ile KEPHS'lerin hizmetlerine ilişkin işlem verilerini imzalamak için kullandığı işlem sertifikasının oluşturulması, kullanılması, iptali ve yenilenmesi ile ilgili usul ve esasları belirlenmiştir. Burada işlem sertifikası, "KEPHS'nin hizmetlerine ilişkin işlem verilerini imzalamak için kullandığı elektronik sertifikayı"[6] şeklinde tanımlanmış olup işlem sertifikasının oluşturulması, kullanılması, iptali ve yenilenmesini içeren

---

[6] Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı (23/01/2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu md.3 (ı) bendi).

hükümlere yer verilmiştir. Bu Usul ve Esaslara göre; İşlem sertifikasının oluşturulması işlemi, KEPHS'ler için işlem sertifikasıyla yapılacak işlemlerde kendisini temsil edecek kişi adına ESHS tarafından işlem sertifikası üretilmesidir.

BTK tarafından yetkilendirilen KEPHS'lerin KEP sistemindeki rolü, gönderilen ve alınan e-postaların iletilmesi ve söz konusu e-postalara ilişkin kayıtların ilgili standart ve düzenlemelere uygun şekilde tutulması olarak tanımlanabilir. KEPHS, yetkilendirme esasına dayalı olarak faaliyet yürüten hizmet sağlayıcı kuruluşlardır. Türkiye Noterler Birliği (TNB) Kayıtlı Elektronik Posta Hizmet Sağlayıcılığı ve Ticaret A.Ş. ile Posta ve Telgraf Teşkilatı Genel Müdürlüğü (PTT) 2012 yılında, TÜRKKEP A.Ş. ise 2013 yılında BTK tarafından KEPHS olarak yetkilendirilmiştir.

3.1.1.8. Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik

Bütün kamu kurum ve kuruluşlarını kapsayan, resmî yazışma kurallarını belirlemek ve bilgi, belge alışverişinin sağlıklı, hızlı ve güvenli bir biçimde yürütülmesini sağlamak amacı ile Resmi Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik 02/12/2004 tarihli ve 25658 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Mezkûr Yönetmeliğin 4 üncü maddesinde, e-ortamda üretilen, iletilen ve muhafaza edilen her türlü belge e-belge olarak tanımlanmış olup 5 inci maddesinde de, yazışmaların kâğıt ortamında yapılabileceği gibi e-ortamda da yapılabileceğinden söz edilmiş ve e-ortamda yazışmaların yapılabilmesi amacıyla her kurum için e-posta zorunluluğu getirilmiştir. Burada e-ortamda hazırlanan yazılarda, güvenli e-imza kullanılması da düzenlenmiştir.

3.1.1.9. Devlet Arşiv Hizmetleri Hakkında Yönetmelik

e-Ortamda üretilen veya e-ortama aktarılan belgelerden yasal zorunluluk veya başka nedenlerle arşivlenmesi gerekli olanların yine e-ortamda çok uzun yıllar aslına sadık şekilde korunması başlı başına önemli bir konudur.

Mevzuatımızda elektronik arşiv konusu, 16/05/1988 tarihli ve 19816 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Devlet Arşiv Hizmetleri Hakkında Yönetmelik ve 08/08/2001 tarihinde ilave edilen Ek Madde 1'de bulunan "*Elektronik ortamlarda teşekkül eden bilgi ve belgelerden arşiv malzemesi özelliği taşıyanların kaybını önlemek ve devamlılığını sağlamak amacıyla bir kopyası cd, disket veya benzeri kayıt ortamlarına aktarılmak suretiyle muhafaza edilir. Bu tür malzemelerin muhafaza, tasnif, devir vb. arşiv işlemlerinde diğer tür malzemeler için uygulanan hükümler uygulanır*" hükmü ile girmiştir. e-Ortamda üretilen belgelerden arşivlenmesi gerekenlerin yine e-ortamda saklanması gerektiği belirtilmiştir.

16/07/2008 tarihli ve 26938 sayılı Resmi Gazete'de yayımlanan 15/07/2008 tarihli 2008/16 sayılı Başbakanlık Genelgesi'nde belge yönetimi, "*kamu adına görev yapan kurum ve kuruluşların faaliyetleri sonucu oluşan belgelerin kayıt altına alınması ve bu belgelerin istenildiği anda erişilebilir şekilde yönetilmesi, kurumsal faaliyetlerin ayrılmaz bir parçası ve kamu görevidir*" şeklinde ifade edilmiştir. Aynı genelge ile e-belgelerin kayıt altına alınması, kullanılması ve arşivlenmesi konularında çalışmalar yapmak üzere Devlet Arşivleri Genel Müdürlüğü görevlendirilmiştir.

3.2. Uluslararası Standartlar

e-Belgelerin güvenliği, kayıt altına alınması, kullanılması ve arşivlenmesi gibi bir dizi konuda geliştirilen uluslararası standartlar TBD'nin Elektronik Belge Yönetimi Çalışma Grubu'nun raporunda sıralanmıştır. TBD'nin Elektronik Belge Yönetimi Çalışma Grubu'nun Raporu'ndan (2009, s.36-42) hareketle

incelenecek olursa, bilgi ve belge yönetimine ilişkin uluslararası standartların başlıcaları şunlardır:

- ✓ **ISO 15489:2001 kodlu Belge Yönetimi Standardı:** Belgelerin yönetimini düzenlemeye yönelik bilgileri içeren standarttır.
- ✓ **ISO/IEC 11179:2003-2005 Bilgi Teknolojisi Veri Elemanlarının Özellikleri ve standardizasyonu:** Veri elemanlarının özelliklerini yani uygulamaya yönelik veri modelleri, veri tabanları gibi düzenlemeleri kapsayan standarttır.
- ✓ **ISO 5127:2001 Bilgi ve Dokümantasyon Terimler Standartları:** Uluslararası bilgi ve belge alışverişini geliştirmek üzere düzenlenmiş bir standarttır.
- ✓ **ISO 23081:2006-2009 Kayıt Yönetim Süreçleri; Üst Veri Standardı:** ISO 23081:2006 kayıt yönetim üst verisinin yönetim ilkelerini içeren standarttır. Bu standarda 2011 yılında bazı eklemeler yapılmıştır.
- ✓ **ISO/IEC TR 20943:2004 Üst Veri içerik tutarlılığını sağlamak için gereken yöntemler:** Değer platformlarının kayıtlarındaki nitelikleri ve bu kayıtlarda farklılık olmaması için işlem yöntemlerini içeren bilgilerden oluşan standarttır.
- ✓ **TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi:** Oluşturulma şekline bakılmaksızın bilginin, ihtiyaç duyulduğunda kullanıma elverişli tutularak, bozulmaya uğramamış haliyle, yetkili kişiler vasıtasıyla ulaşımını da içeren düzenlemeleri esas alan standarttır.
- ✓ **NSO-Z39 50:1995-2003 Bilgi Erişim Hizmet ve Protokolü (Information Retrieval : Application Service Definition & Protocol Specification):** Amerikan Ulusal Bilgi Standartları Kuruluşu (National Information Standards Organization – NISO) tarafından yayımlanan bu protokol bilgisayar sistemlerinin karşılıklı olarak konuşmalarının temini için geliştirilmiş bir standart niteliğindedir.
- ✓ **NSOZ-39 87:2006 Görüntü Sözlüğü (Data Dictionary – Technical Meta Data for Digital Still Images):** Görüntüleme yazılım ve donanımları ile e-

ortama aktarılan dokümanların yönetimi ve bunların meta verilerini tanımlamak üzere test amaçlı oluşturulan bir standarttır. Bu standart, 2011 yılında revize edilmiştir.

- ✓ **Üst Veri Terimleri Standartları:** 2008 yılında oluşturulan kar amacı gütmeyen bir organizasyon olan Dublin Core Metadata Initiative (DCMI) tarafından yönetilmekte olan ve ilgili tüm tarafların katılımına açık bir forum aracılığıyla geliştirilen birlikte çalışabilir üst veri standartlarıdır. Bu standartlar, e-ortama bir şekilde aktarılmış bulunan bilgi kaynaklarının tanımlanmasına ilişkin bilgileri içermektedir. Söz konusu standartlar, günümüzde de geliştirilmeye devam etmektedir.
- ✓ **e-Ortamda Üretilen ve aklanan Bilginin Yasal Gerçekliğini Sağlama Standardı (BSI DISC 0008A code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically):** e-Ortamda var olan bilginin, hukuki geçerlik kazanabilmesi için hazırlanmış bir standarttır.
- ✓ **Belgelerin Yönetimi İçin Geliştirilmiş Program (ANSIARMA Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records):** Kuruluşlar için çok önemi idari, yasal ve mali belgelerin yönetiminin sağlaması adına geliştirilen programdır.
- ✓ **DoD. (Department of Defense):** Öncelikle Amerikan Savunma Bakanlığı'nda belge yönetimi yazılımlarında gerekli nitelikleri belirlemek üzere oluşturulmuş bir standarttır.
- ✓ **Elektronik Belge Yönetimi İçin Gereksinimler Modeli (MoReq Specification: Model requirements for the management of electronic records):** 2001 yılında e-belge yönetiminin fonksiyonel ihtiyaçlarını belirlemek için geliştirilen bir standarttır. 2008 ve 2010 yıllarında çeşitli eklemeler ve değişiklikler yapılmıştır.
- ✓ **İngiltere Elektronik Belge Yönetim Sistemleri (ERMSUKElectronic Records Management SystemsUnited Kingdom):** İngiliz Milli Arşivlerince e-belge yazılımları için standartları düzenlemek amacı ile hazırlanmıştır.

- ✓ **InterPARES:** Amerika Birleşik Devletleri (ABD) ve Kanada tarafından desteklenen bir projedir, e-belgelerin diplomatik geçerliliği ve belge niteliklerinin tespitine ve muhafazasına ilişkin standartları oluşturmaktadır.

Bunlara ilaveten, aşağıdaki uluslararası standartlar da bilgi ve belge yönetimi ile ilişkilidir:

- ✓ **ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi için Uygulama Esasları:** Kurum ve kuruluşlarca oluşturulacak olan bilgi güvenliği yönetim sistemlerinin hangi prosedürlere uygun olarak yönetilmesi ve işletilmesi gerektiğini ortaya koymaktadır.
- ✓ **ISO 16175:2010-2011 Bilgi ve Belgelendirme – Elektronik Ofis Ortamlarındaki Kayıtlara İlişkin Prensipler ve Fonksiyonel Gereksinimler:** Kurum ve kuruluşlardaki sayısal kayıtların oluşturulmasında ve yönetilmesinde kullanılan yazılımlar için dünya çapında birlikte çalışabilir fonksiyonel gereksinimleri ve prensipleri ortaya koymayı amaçlamaktadır.
- ✓ **ISO 30300:2011 Bilgi ve Belgelendirme – Kayıt Yönetim Sistemi – Temel Hususlar ve Sözlük:** Kayıt yönetim sistemlerine uygulanabilecek standartlarda yer alan terim ve tanımları sunmaktadır (Arma, 2013, s.12-15-25).

3.3. Ülkemizdeki e-belge yönetimi standardı

Kalkınma Bakanlığı tarafından 2009 yılında yapılan çalışmalar kapsamında, e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi'nde yer alan birlikte çalışabilirliği sağlama ayrıca kurumlara hareket serbestliği temin edecek ve rekabet ortamı oluşturacak şekilde belirlenmesi önemlidir.

Bahsi geçen Rehber'de, birlikte çalışabilirliği mümkün kılma ve rekabeti artırma hedefi kapsamında açık standartların kullanımının benimsendiği ifade edilmiş olup açık standardın asgari özellikleri şunlardır:

- ✓ Standardın, kar amacı gütmeyen kuruluş tarafından üretilmiş, gelecekte söz konusu kuruluş tarafından destekleneceği deklare edilmiş ve tüm kesimlerin katılım sağlayabileceği bir karara bağlama aşamasında gerçekleştirilmelidir.
- ✓ Söz konusu belge yayımlanmış, ücretsiz veya cüzi bir ücret ile çoğaltılabilir, paylaşılabilir, kullanılabilir olmalıdır.
- ✓ Standarda ait fikri haklar, geri alınamaz biçimde olan bir hak talebinden bağımsız olmalıdır.
- ✓ Standardın tekrar kullanımında engel bulunmamalıdır (DPT,2009,s.6-8).

TS 13298 numaralı standart, e-belge yönetimi konusundaki ilk standarttır. Söz konusu standart, kurumlarda oluşturulan ya da üretilmesi olası elektronik dokümanların[7] belge özelliğinin muhafazası için ihtiyaç duyulan standartların tespit edilmesi amaçlamaktadır. Genel olarak bu standartta;

- ✓ EBYS'nin ihtiyacı olan sistemler
- ✓ EBYS için lüzumlu belge yönetimine ilişkin teknikler ve uygulamalar
- ✓ e-Belgelerin yönetilebilmesi için ihtiyaçlar
- ✓ e-Ortamda oluşturulmamış olan belgelerin yönetim fonksiyonlarının e-ortamda yürütülebilmesine olan ihtiyaçlar
- ✓ e-Belgelerde olması gereken diplomatik özellikler[8]
- ✓ e-Belgelerin hukukiliğinin sağlanması adına alınması gerekli tedbirler
- ✓ Güvenli e-imza ve mühür sistemlerinin uygulanmasına ilişkin ihtiyaç duyulan sistem alt yapısının belirlenmesi

hususları yer almaktadır (TSE, 2013).

---

[7] Doküman: Kurumsal faaliyetlerin yerine getirilmesinde üretilen ya da toplanan, henüz belge vasfı kazanmamış her türlü kayıtlı bilgi (TS 13298 Elektronik Belge Yönetimi, s.1)

[8] Diplomatik özellik: Belgelerin orijinalliğinin tespit edilmesinde kullanılabilecek her türlü içerik, format, ilişki ve sunum özellikleri. (TS 13298 Elektronik Belge Yönetimi, s.1)

16/07/2008 tarihli ve 26938 sayılı Resmi Gazete'de yayımlanan Elektronik Belge Standartları konulu 2008/16 numaralı Başbakanlık Genelgesi'nde, "*Elektronik belgelerin kayıt altına alınması, kullanılması ve arşivlenmesi konularında çalışma yapma görevi e-Dönüşüm İcra Kurulu'nun 9 Eylül 2004 tarih ve 7 numaralı Kararı ile Devlet Arşivleri Genel Müdürlüğü'ne verilerek TS 13298 numaralı standardın yayınlanması sağlanmıştır. Hazırlanan bu standart kamu kurum ve kuruluşlarının kullanacakları elektronik belge yönetim sistemleri için temel bir kaynak teşkil etmektedir*" ifadesi ile kamu kurum ve kuruluşları tarafından yürütülecek olan EBYS'nin temel kaynağının TS 13298 numaralı standart olduğu belirtilmektedir.

Ayrıca bu Genelge'de yer alan, "*Kamu kurum ve kuruluşları oluşturacakları elektronik belge yönetim sistemlerinde TS 13298 numaralı standarda göre işlem yapacak, ayrıca üretmiş oldukları elektronik belgenin kurumlar arası paylaşımını www.devletarsivleri.gov.tr internet adresinde belirlenen kurumlar arası elektronik belge paylaşım hizmeti kriterlerine göre gerçekleştirecektir. Genelgenin yayımı tarihinden önce kurulan sistemler ise ilgili kamu kurum ve kuruluşlarınca gözden geçirilerek iki yıl içinde standarda uyumlu hale getirilecektir*" ifadesi, kurumlar arası belge paylaşımı işlemlerinde www.devletarsivleri.gov.tr adlı internet sitesinde bulunan hizmet kriterlerinin de dikkate alınması gerektiğini vurgulamaktadır.

TS 13289'de yer alan; "*e-belge yönetimi, kurumların gündelik işlerini yerine getirirken oluşturdukları her türlü dokümantasyonun içerisinden kurum aktivitelerinin delili olabilecek belgelerin ayıklanarak bunların içerik, format ve ilişkisel özelliklerini korumak ve bu belgeleri üretimden nihai tasfiyeye kadar olan süreç içerisinde yönetmektir*" ifadeleri ile bu alanda yeknesaklık sağlanması öngörülmektedir.

Bölüm 3.2 de "Uluslararası Standartlar" başlığı altında yer alan ülkemizdeki ve bazı uluslararası standartları içeriği itibariyle incelediğimizde ortaya çıkan durum Tablo 3-2'de gösterilmektedir.

Tablo 3.2 Ülkemiz ve Uluslar arası Bazı Standartların Özellikleri

KONU	STANDARTLAR										
	TS 13298	ISO 15489:2001	ISO / IEC 11179:2005-2005	ISO 230811:2006-2009	TS ISO / 27001:2005	NSOZ39 50:1995-2003	ISO/IEC 27002:2005	ISO 16175:2010-2011	MoReq Specification:2001	BSI DISC 0008A	ANSIARMA Vital Records Programs
e-Belge Güvenliği	X										
Bilgi Güvenliği					X		X				
Güvenli Paylaşım	X							X			
e-Belge-Bilgi Yönetimi	X	X					X	X	X		X
Veri Elemanı Niteliği			X								
Yasal Geçerlilik										X	
e-Belge Oluşturma	X										
e-Belge Arşivlenmesi	X										
Üst Veri				X							
Hizmet Protokolü						X					

Kaynak: (TBD, 2009, s.36-42) ve (Arma, 2013, s.12-15-25)'den yorumlanmıştır

Tablo 3-2'de görüldüğü gibi; TS 13298 e-belge güvenliği, e-belge-Bilgi yönetimini, güvenli paylaşım, e-belge arşivlenmesi ve e-belge oluşturma konularını, ISO 15489 e-belge yönetimini, ISO / IEC 11179 veri elemanı niteliğini, ISO 230811 üst veriyi, ISO/IEC 27001 bilgi güvenliği, NSOZ39 50:1995-2003 Hizmet Protokolünü, ISO/IEC 27002:2005 bilgi güvenliği ve e-belge-bilgi yönetimini, ISO 16175 güvenli Paylaşım ve e-Belge-Bilgi Yönetimini, MoReq Specification e-belge yönetimini, BSI DISC 0008A yasal geçerliliği, ANSIARMA Vital Records Programs ise e-belge yönetimini içermektedir.

Özellikle AB'de e-ortamda güvenli belge paylaşım amaçlı uygulamalar, ülkeler bazında farklılıklar göstermektedir. ETSI tarafından geliştirilmiş olan KEP sistemi çalışmaları güvenli elektronik posta için bir standart oluşturmaktadır.

4. DÜNYADA VE TÜRKİYE'DE e-BELGE PAYLAŞIMINA İLİŞKİN UYGULAMALAR

e-Ortamda e-belgelerin güvenli paylaşımı; ülke uygulamaları ve ülkemiz için öneriler yapabilmek adına dünya ve ülkemizdeki mevcut durum tespitinin mutlaka yapılması gerekmektedir. Bu bağlamda:

- ✓ Üretilen belgelerin ne kadarını e-ortamda oluşturdukları
- ✓ e-Ortamda oluşturulan e-belgelerin standartlara uyum sağlayıp sağlamadığı
- ✓ Hangi standardı tercih ettikleri ve tercih nedenleri
- ✓ Kullandıkları altyapı
- ✓ e-Belgelerin üretilmesi ve güvenli paylaşılması konusunda karşılaştıkları problemler ve nedenleri
- ✓ e-Ortamda güvenli e-belge paylaşımında kullanılan standartlar ve bu standartları tercih nedenleri

konularında farkındalık ve aksaklıkların tespiti amaçlanmıştır.

e-Ortamda güvenli e-belge paylaşılması konusunda Kasım 2010 yılında yurt içinde ve yurt dışında olmak üzere iki farklı anket yapılmış olup söz konusu anket katılımcıları; kamu kurumları, özel sektör kuruluşları ve üniversitelerden oluşmaktadır.

- ✓ e-Belge oluşturulması, kullanılması ve paylaşımına ilişkin yapılan anket çalışması Ek 6-1 ve Ek 6-2'de yer almaktadır. Söz konusu çalışma e-belge oluşturulması, kullanılması ve güvenli e-belge paylaşımı konusunda ülkemiz ile yurt dışı uygulamalarda eş düzeylilik olduğunu göstermektedir. Ayrıca anket verilerine göre ülkemizde güvenli e-belge paylaşımı konusunda farkındalığın oluşturulması gerekliliği değerlendirilmektedir. Ankette e-ortamda e-belgelerin güvenli paylaşımı konusunda karşılaşılan en büyük engel mevzuattan kaynaklanan problemlerin olduğu tespit edilmiştir. Ancak anketin yapıldığı tarih olan

2010'dan sonra ülkemizde bu konuda yapılan çalışmalar neticesinde e-belgelerin e-ortamda güvenli ve hukuki geçerliliğe sahip bir şekilde paylaşımına ilişkin ihtiyaç duyulan mevzuat altyapısı tamamlanmıştır.

4.1. Ülkemizdeki Uygulamalar

Ülkemizde e-ortamda e-belge paylaşımı konusunda çok sayıda geliştirilmiş uygulanma kullanılmaktadır. Bunlardan bazıları e-Yazışma Projesi, KEP ve Ulusal Yargı Ağı Projesi (UYAP), Merkezi Nüfus İşleri Sistemi (MERNİS), e-Devlet Kapısı Uygulaması olarak sayabiliriz.

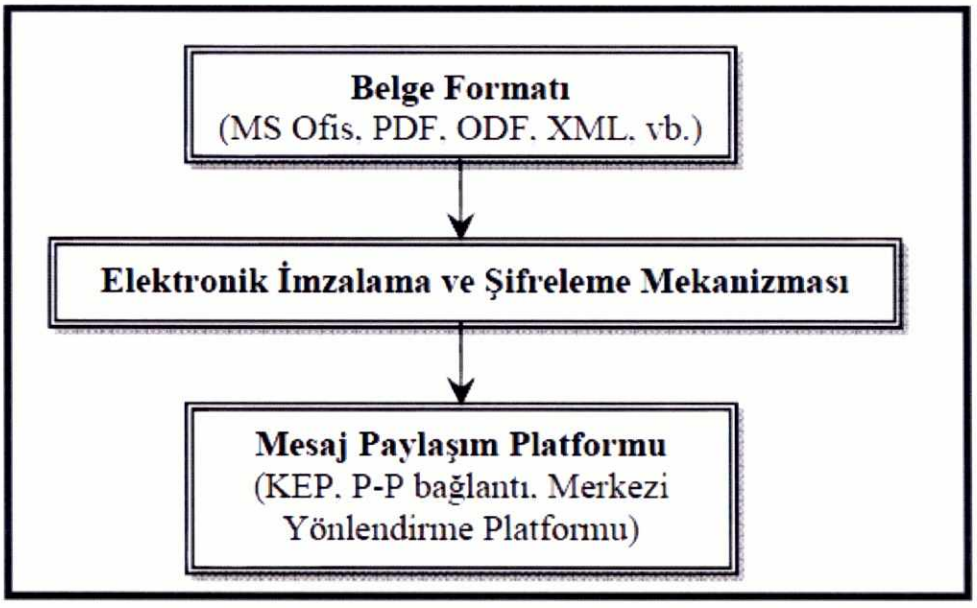
4.1.1. e-Yazışma Projesi

Ülkemizin bilgi toplumuna geçişi açısından önceliklerini ve 2006 ile 2010 tarihleri aralığında uygulanması gereken tedbirleri belgeleyen Bilgi Toplumu Stratejisi 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararı ile uygulamaya geçilmiştir. Bilgi Toplumu Stratejisi eki Eylem Planın 73 numaralı "Ortak Hizmetlerin Oluşturulması" ibaresi ile de kamu kurum ve kuruluşlarında ortak olarak yürütülen bazı faaliyetlerin merkezi olarak yerine getirilmesi için çalışmalar yapılması düşünülmüş ve eski adı Devlet Planlama Teşkilatı Müsteşarlığı olan Kalkınma Bakanlığı bahsi geçen eylemin sorumlusu olarak belirlenmiştir. Söz konusu eylem gereğince; kamu kurum ve kuruluşları arasında resmi yazışmaların e-ortamda yapılmasını teminen ortak kurallar setinin oluşturulması için 2010 yılında Kalkınma Bakanlığı tarafından "e-Yazışma Projesi" çalışmaları başlatılmıştır (T.C. Kalkınma Bakanlığı, 2011a).

Kalkınma Bakanlığı tarafından 2010 yılında başlatılmış olan e-Yazışma projesi, kamu kurum ve kuruluşları arasında resmi belgelerin, ortak norm ve standartlar ile e-ortamda paylaşımına yönelik bir çalışma olarak hazırlanmaktadır. e-Yazışma projesi, Şekil 4-1'de genel hatları ile gösterilmiş olup söz konusu proje, henüz Cumhurbaşkanlığı, Başbakanlık, Adalet

Bakanlığı, İçişleri Bakanlığı, Dışişleri Bakanlığı ve Kalkınma Bakanlığı'nı kapsayan pilot uygulama aşamasındadır.

Şekil 4-1. e-Yazışma Projesi



Kaynak: Civelek ve Turan, 2010, s.17

4.1.1.1. e-Yazışma Paketi

Kamu kurum ve kuruluşlarının hazırladıkları resmi yazıları e-ortamda paylaşabilmeleri için, ekleri ile birlikte tek bir paket haline dönüştürülmesi e-Yazışma Paketi olarak adlandırılmaktadır.

e-Yazışma Paketi, resmi belgeye ait bilgi ve eklerin önceden belirlenmiş biçime uygun olarak oluşturulmuş olan sadece tek dosyadır. Söz konusu paket, resmi belgeye ilişkin bilgi ve ekleri içermesi ile birlikte e-Yazışma Paketinin kendisine mahsus tanım bilgilerini de ihtiva eder. Ekleri ile birlikte belgenin, e-Yazışma Paketine dönüştürülmesi sonrası bir bütün halinde elektronik olarak tek seferde güvenli e-imza ile imzalanabilmesi önemli bir özelliktir. Bu özellik sayesinde, farklı alıcılara gönderilecek her kopyası için tekrar imzalanması gerekmeyecektir (T.C. Kalkınma Bakanlığı, 2011b).

4.1.1.2. e-Yazışma Paket yapısı

e-Yazışma Paketi, Açık Paketleme Kuralları (OPC) esas alınarak tanımlanmıştır. OPC, yaygın bir biçimde kullanılan ZIP dosya yapısını temel alan geniş amaçlı bir dosya/bileşen paketleme aracıdır. Uluslararası açık bir standart olan OPC, ISO/IEC 29500-2:2008 dokümanında tanımlanmıştır (İş Yazılım, 2012).

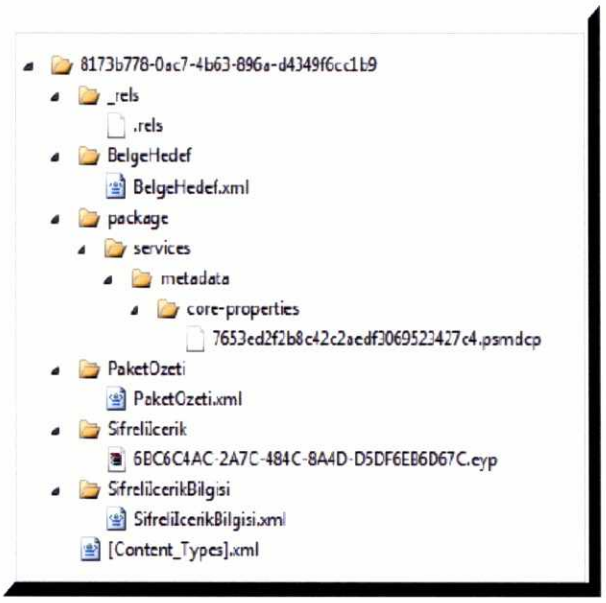
Söz konusu projenin en önemli özelliği sistem ve teknoloji bağımlılığını en aza indirerek esnek bir yapıyı öngörmesidir. Bu nedenle e-Yazışma Paketi, OPC temel alınarak oluşturulmuş ve söz konusu standarda ek olarak belirlenmiş kurallar ile hazırlanan paket farklı sistemlerde de çalışabilmektedir.

TBD'nin Kamu-BİB Aylık Bilgilendirme Toplantısı sunumunda e-Yazışma Paketi yapısı aşağıdaki maddeler halinde özetlenmiştir (T.C Kalkınma Bakanlığı, 2012, s.8):

- ✓ ZIP dosya yapısını temel alan bir OPC paketidir
- ✓ Paket bileşenleri, paket içinde klasörler içerisinde saklanır
- ✓ Paketi oluşturan bileşenler veri kaynaklarında ayrı ayrı saklanabilir ya da ayrık bileşenler bir araya getirilerek paket tekrar oluşturulabilir
- ✓ Paketin ayrıştırılması ve tekrar bir bütün haline getirilmesi pakete atılan imzaları bozmaz

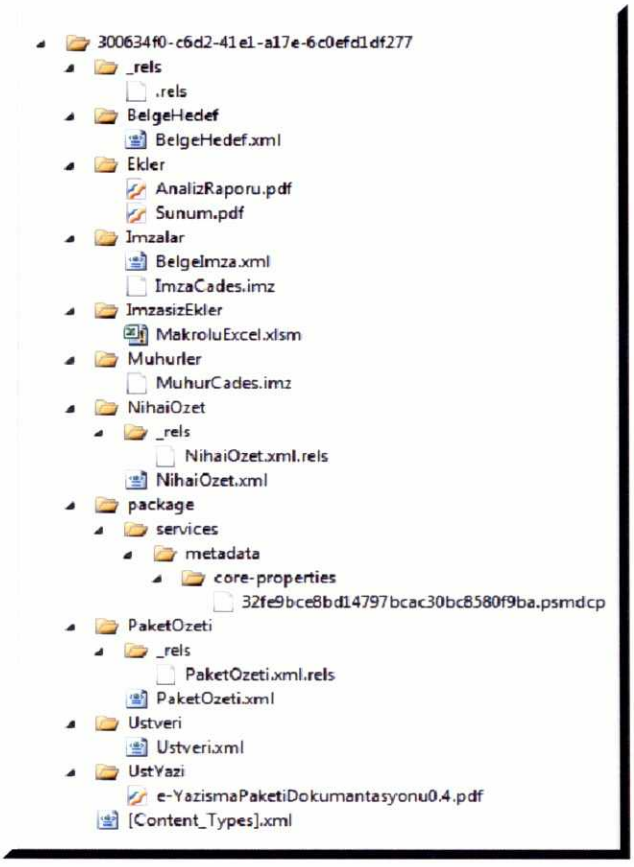
Söz konusu e-Yazışma Paketinin, şifrelenmiş hali Şekil 4-2'de, ZIP dosyalarını açabilen bir uygulama ile açılmış hali Şekil 4-3'da gösterilmiştir.

Şekil 4-2. Şifrelenmiş e-Yazışma Paketi



Kaynak: T.C. Kalkınma Bakanlığı, 2011a, s.9

Şekil 4-3. Açılmış e-Yazışma Paketi



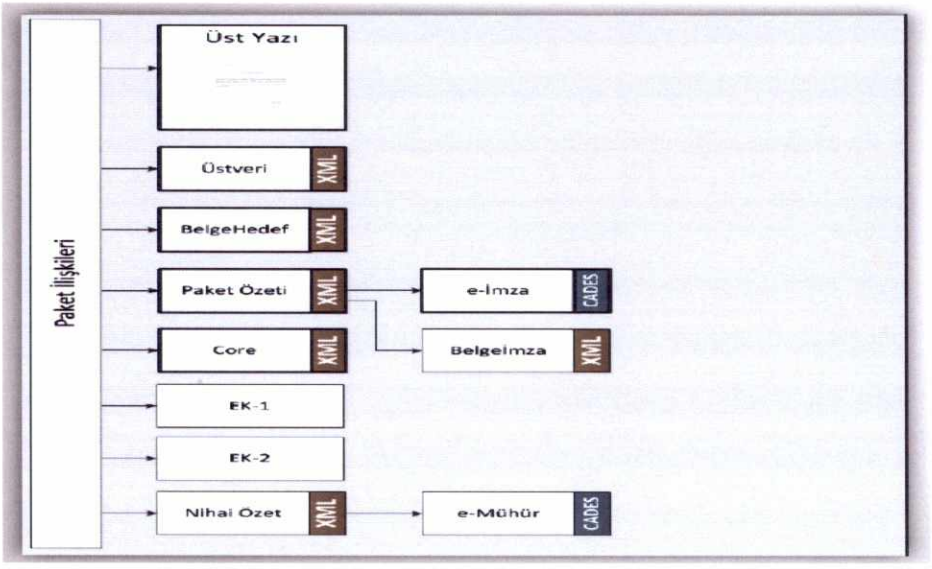
Kaynak: T.C. Kalkınma Bakanlığı, 2011a, s.9

4.1.1.3. e-Yazışma Paketi bileşenleri

Şekil 4-4'de görüldüğü üzere e-Yazışma Paketi resmi belge, ekleri, belge hakkında üstveri, e-imza, e-mühür, ilgili özetlerden oluşan tek bir paket haline dönüşmektedir (T.C Kalkınma Bakanlığı, 2012a, s.12-13-14);

- ✓ İletilen belgeye ilişkin bileşenler
  - ✓ Üst Yazı
  - ✓ Üst Veri
  - ✓ e-imza
  - ✓ Belge İmza
  - ✓ Ek
  - ✓ e-Mühür
- ✓ Paket yapısına ilişkin bileşenler
  - ✓ Core
  - ✓ Paket Özeti
  - ✓ Nihai Özet
- ✓ Şifreli paket Bileşenleri
  - ✓ Şifreli İçerik
  - ✓ Şifreli İçerik Bilgisi
  - ✓ Belge Hedef
  - ✓ Paket Özeti
  - ✓ Core

Şekil 4-4. e-Yazışma Paketi Bileşenleri



Kaynak: T.C Kalkınma Bakanlığı, 2012a, s.14

4.1.1.4. Mesaj paylaşım

e-Yazışma Projesi çerçevesinde, elektronik olarak imzalanan belgelerin iletildiğinin garanti altına alınması ve ne zaman iletildiğinin tespit edilebilir olması gerekmektedir. Bu doğrultuda, KEP sistemi gündeme gelmektedir (Civelek ve Turan, 2010, s.21). Henüz tamamlanmamış olan e-Yazışma Projesi çalışmaları devam etmektedir.

4.1.2. Ulusal Yargı Ağı Projesi (UYAP)

Adalet Bakanlığı'nın tüm birimleri ile bağlı ve ilgili birimlerinde kullanılabilen bir iletişim sistemi olup avukatlara ve vatandaşlara adli hizmetlere e-ortamda erişim imkânı veren, e-Dönüşüm ve e-devlet projesi kapsamında, e-adalet hizmeti sunmayı hedefleyen bir projedir. UYAP hızlı, fonksiyonel, etkili, güvenilir ve şeffaf bir yargı mekanizması oluşturmak, bürokratik prosedürleri azaltmak adalet dağıtımını hızlandırmak gibi amaçlara sahip olmakla birlikte, Adalet Bakanlığı merkez ve taşra teşkilatı, tüm hukuk, ceza ve idare mahkemeleri, Cumhuriyet Başsavcılığı, infaz ve icra-iflas daireleri, Ceza Tevkif ve Islah Evleri, Adli Tıp Birimleri, Denetimli Serbestlik Birimleri vs. tarafından kullanılmaktadır. UYAP üzerinden e-ortamda dosya inceleme ve dilekçe sunma, dava açma, avukatlarının performansını değerlendirme, dosyaları alma ve raporlarını gönderme gibi iş ve işlemler yapılmaktadır. UYAP dış ortam ile bağlantısını VPN üzerinden yapmaktadır (UYAP, 2012, s.2,4,5,43).

4.1.3. Merkezi Nüfus İşleri Sistemi (MERNİS)

MERNİS, kişilerin durumlarına ilişkin bilgilerini e-ortama taşıyan ve söz konusu bilgilerdeki değişiklikleri ülkemizde bulunan farklı 957 merkezden bir ağ üzerinden anında güncelleyen ve erişimi sağlayan bir projedir. Söz konusu proje ile bilgi ve e-belgelerin güvenli paylaşımı, güncellemelerin en kısa sürede yapılması ve vatandaşlara sunulan hizmetin verimli olması

hedeflenmiştir. Proje ile ülkemiz kamu kurum ve kuruluşlarının, vatandaşlara verdikleri farklı numaralar tek numaraya indirilerek kullanım kolaylığı sağlanmıştır. MERNİS Projesi, sağladığı bilgi ve e-belge desteği ile başta devlet olmak üzere herkesin iş ve işlemlerinde önemli ölçüde zaman ve kırtasiye tasarrufu sağlamış olup e-devlet projelerinin de giriş anahtarı olmuştur. Söz konusu Projenin genel hatlarıyla sağladığı hizmetler şunlardır;

- ✓ Nüfus kayıtlarını e-ortama taşıyarak ilçe nüfus veri tabanlarının hazırlanmasını ve hizmetin güncelliğini sağlamak
- ✓ Nüfus hizmetlerinin ilçelerde BİT vasıtasıyla yerine getirilmesini; ilçe nüfus veri tabanlarını Merkezde birleştirerek Merkezi Nüfus Veri Tabanını kurulmasını sağlamak
- ✓ Her vatandaşına birer kimlik numarası verilmesini temin etmek
- ✓ T.C. Kimlik numaraları vasıtasıyla, kamu ve özel sektöre ilişkin uygulamalar arasında çalışanlara ait bilgilerin iletişiminin, vatandaşların tekil şekilde belirlendiği bir yapı vasıtasıyla çevrim-içi çalışmasını temin etmek
- ✓ Nüfusa ilişkin istatistiklerinin BİT yardımı ile doğru bir şekilde üretilmesini sağlamak
- ✓ Kimlik bilgilerini kurum ve kuruluşlar ile paylaşarak hizmet sürelerini kısaltmak, güvenilirlik sağlamak (T.C. İçişleri Bakanlığı, 2009).

1976 yılında Kalkınma Bakanlığı tarafından projelendirilen ve Kasım 2002 sonu itibariyle kullanıma açılan MERNİS Projesi, halen işlerliğini sürdürmektedir (T.C. İçişleri Bakanlığı, 2008).

Çeşitli kurumların faydalanabildiği Kimlik Paylaşım Sistemi (KPS) hizmetinden yararlanabilmesi için kullanıcı bilgisayarının, XML internet servislerini çağırabilme ve (SOAP 1.2) WS-Security 1.1, WS-Trust 1.3 ve WS-SecurityPolicy 1.2 internet servis güvenliği standartlarını desteklemesi gerekmektedir. KPS'de sadece bir noktadan kimlik doğrulaması yapılmaktadır. İnternet servis kullanıcıları direkt olarak KPS üzerinden değil,

farklı bir güvenlik anahtarı servisinden (Security Token Service) giriş yapabilmek adına kullanıcı adı ve şifreleri vasıtasıyla anahtar edinerek KPS'ye bilgi çağrısı yapabilecektir. KPS servislerinin güvenliği genel olarak SSL ile sağlanmaktadır (T.C. İçişleri Bakanlığı, 2013).MERNİS Projesi, Türkiye'nin en büyük veri tabanına sahiptir (Eroğlu, 2006, s.84).

4.1.4. BTK'da e-ortamda e-belge paylaşımı içeren uygulamalar

BTK bünyesinde, e-ortamda farklı konuları içeren uygulamalarda e-belge paylaşımları yapılmaktadır. Söz konusu uygulamaların veri iletişimi güvenli kanallar üzerinden yapılmaktadır.

4.1.4.1. Mobil Cihaz Kayıt Sistemi

5809 sayılı Kanun ile Türkiye'deki bütün elektronik kimlik bilgisine haiz cihazların (GSM şebekelerinden hizmet alan cep telefonu, modem, el bilgisayarı, POS cihazı, vb.) kayıt altında tutulması görevi BTK'ya verilmiştir. İthalatçı firmaların IMEI kayıt işlemi başvurularına ilişkin tüm belgeler (gümrük beyannamesi vb.) e-ortamda e-imzalı olarak sisteme yüklenmektedir. Mobil Cihaz Kayıt Sistemi (MCKS) Projesi, bu amaca hizmet için oluşturulmuştur (Sümer, Sözlü Görüşme, 2012).

4.1.4.2. Numara Taşınabilirliği Sistemi

01/02/2007 tarihli ve 26421 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş bulunan Numara Taşınabilirliği Yönetmeliği'ne göre, numara taşınabilirliği; abonenin numarasını değiştirmeden hizmet aldığı işletmeciyi, değiştirebilmesidir. Abonenin hizmet aldığı (verici) işletmeciden ayrılıp başka bir işletmeciye (alıcı) geçme işlemleri BTK'da bulunan Merkezi Referans Veri Tabanı üzerinden gerçekleştirilmektedir. Bu işlem ise numara taşıma işlemleri için abone kayıt merkezlerince hazırlanan başvuru belgeleri e-ortamdan alınmaktadır (Sümer, Sözlü Görüşme, 2012).

4.1.4.3. Online Şikâyet Bildirim Sistemi

BTK tarafından 2012 yılında hizmete açılan Online Şikâyet Bildirim Sistemi; tüketicilerin BTK tarafından yetkilendirilmiş işletmecilerden almış oldukları hizmetlere ilişkin şikâyetlerini e-ortamda kabul etmektedir. e-Ortamda kabul edilen şikâyetler, konularına ve ilgilisine göre tasnif işleminin ardından, Kurum içi veya işletmecilere yine e-ortamda iletilerek, karşılığında alınan cevaplar tüketiciye e-ortamda gönderilmektedir (Sümer, Sözlü Görüşme, 2012).

4.1.5. e-Devlet uygulaması

e-Devlet Kapsı üzerinden halen kamu kurum ve kuruluşlarının vermiş olduğu hizmetlere vatandaş ve iş dünyası tarafından kolayca erişim sağlanmaktadır. e-Devlet Kapısı kullanıcılarına, yapacakları sorgulamalar neticesinde erişecekleri ve talep edecekleri bilgi ve e-belgelerin (sabıka kaydı, sosyal güvenlik bilgileri, bilgi edinme başvuruları gibi) yine e-Devlet Kapısı uygulaması ile KEP sistemi üzerinden iletilmesi ile gerek bilgi ve e-belge gerekse iletime ilişkin tüm süreçler resmiyet kazanacaktır. Dolayısı ile hem devlet açısından hem de kullanıcı açısından bürokrasi azaltılmış olacaktır.

e-Devlet Kapısı, ülkemiz kamu kurumlarının sunmuş olduğu hizmetlerine internet üzerinden tek bir adresten (portal) ulaşım imkanı sunan bir uygulamadır. (Türksat, 2013a).

e-Devlet Kapısı ile kullanıcılara sunulan hizmetler aşağıda şekilde gruplandırılabilir:

- ✓ Bilgilendirme hizmetleri
- ✓ Entegre elektronik hizmetler

- ✓ Ödeme işlemleri
- ✓ Kurum ve kuruluşlara kısa yollar

✓ Güncel bilgiler ve duyurular
✓ Kurumlardan vatandaşlara mesajlar

Bunlara ilaveten kamu kurumları arasında bilgi ve belgelerin paylaşımı e-Devlet Kapısı üzerinden sunulan hizmetler ile sağlanmaktadır (Türksat, 2013b).

e-Devlet Kapısı sistemi, güvenlik amaçlı olarak elektronik sertifika kullanmaktadır (Türksat, 2013c).

Kullanıcıların e-ortam üzerinden verilecek olan kamu hizmetlerine değişik platformlardan, güven içerisinde ve bir noktadan ulaşabilecekleri, vatandaşın ve iş dünyasının ihtiyaçlarını hedef almış, beraber çalışabilen ve bütünleşik hizmetlerin verileceği, katılımcı ve saydam aynı zamanda hesap verebilir bir devlet olgusunu ifade eden e-devletin daha dinamik ve etkili kamu yönetimine erişebilmek için önemli bir araç olduğu bir gerçektir (Metin, 2012, s.98).

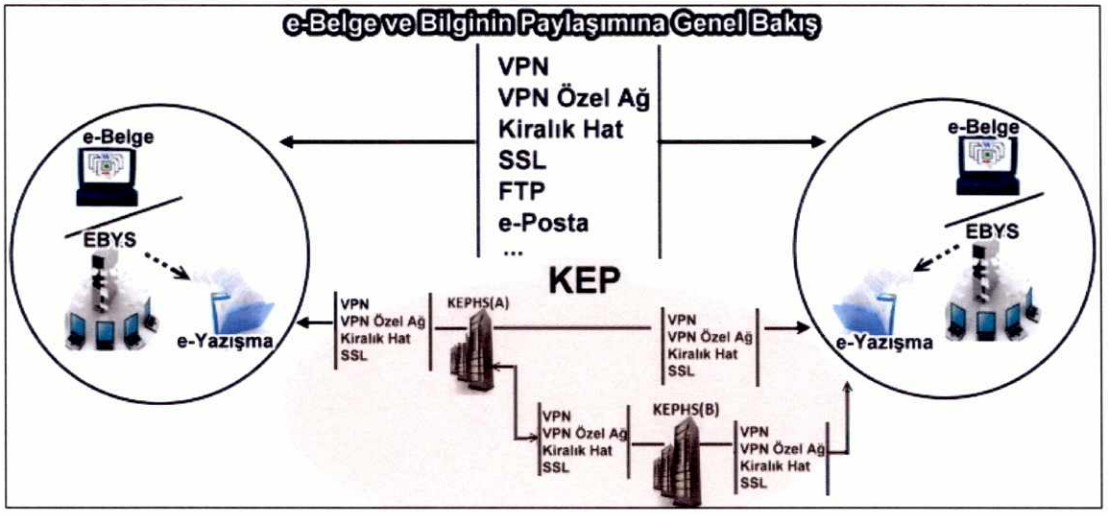
e-Devlette kamu bilgilerinin vatandaşa sunulmasında geleneksel devletin aksine, vatandaş kamu kurumları ile karşı karşıya getirilmez. Vatandaş sistemle iletişime geçer, sistemin ardında çalışan kuruluşlar gerekli işlemi yaparak vatandaşa tekrar sistem aracılığıyla hizmet verir (Erdal, 2004, s.2).

4.2. e-Belge ve paylaşım yöntemleri ilişkileri

Günümüzde modern devletler, vatandaşının zaman gözetmeden ve her yerden rahatça erişebileceği bir e-devlet yapısı hedeflemektedirler. BT'deki hızlı gelişmeler bunu temin edecek seviyededir. Bu kapsamda EBYS ile veya e-ortamda hazır yazılımlarla üretilen e-belge ve bilgilerin, yaygın olarak kullanılan VPN, SSL, FTP ile ayrıca VPN ve SSL üzerinden e-posta, henüz yeni bir uygulama olan KEP ve diğer uygulamalarla paylaşılmaktadır. Verilerin büyüklüğü, türleri ve kullanım amaçları açışından her bir paylaşım yöntemi ayrı bir amaca hizmet etmektedir. Örneğin paylaşımı çok yoğun olan e-belge ve bilgilerin VPN üzerinden yapılmasının uygun olabileceği gibi

paylaşım yoğunluğu fazla olmayan ve bireysel e-belge ve bilgi paylaşımında KEP'in kullanılması uygun olabilmektedir. EBYS'de üretilecek e-belgelerin ve paylaşım yöntemlerine ilişkin genel resim Şekil 4-5 de gösterilmiştir.

Şekil 4-5. e-Belge ve bilginin paylaşımına genel bakış



4.3. Dünyada e-Belge Paylaşımı ve KEP Uygulamaları

Günümüz iletişimde bilgi ve e-belge paylaşımında çok sayıda farklı uygulamalar kullanılmaktadır. Söz konusu yaygın kullanıma sahip uygulamalara VPN, VPN Özel ağ, Kiralık Hat, SSL, FTP gibi örnekler verilebilir. Ancak bahsi geçen uygulamaların yasal düzenlemeleri bulunmamaktadır. Buna karşın yasal düzenlemeleri oluşturulmuş, bilgi ve e-belgenin paylaşımı esnasında yapılan her işlem için delil üreten ve üretilen bu delilleri hukuken geçerli kabul edilen KEP sistemi, ülke uygulamaları başlığı altında ele alınmıştır.

Dünyada e-belge paylaşımı konusunda farklı uygulamalar kullanılmaktadır. Ancak günümüzde KEP, e-belge ve bilgi paylaşımında yaygın olarak kullanılan e-posta'nın son derece güvenli hale dönüştürülmüş yeni bir sürümü olarak düşünülebilir. KEP, AB üyesi ülkeler birlikte çalışabilirliği sağlamak

adına yine AB ülkeleri öncülüğünde geliştirilmekte ve kullanılmakta olan bir uygulamadır.

KEP sistemi ve bileşenleri resmi bir telekomünikasyon standardı olarak (ETSI/TS 102 640) ETSI tarafından hazırlanmış ve Ocak 2010 yılında yayımlanmıştır. Ancak 2000 yılından itibaren İtalya, Fransa, Almanya, Belçika, İspanya, İsveç ve ABD başta olmak üzere bazı ülkeler gerekli düzenlemelerini yaparak KEP sistemini uygulamaya başlamış olup ve birçok ülkede söz konusu uygulamaya geçmek üzere çalışmalarını yürütmektedir (Samast, 2010, s.3).

AB ülkelerinde, ETSI tarafından başlatılan çalışmalar öncesi KEP konusunda farklı uygulamalar hayata geçirilmiştir. Ancak söz konusu farklı uygulamalar, beraberinde farklı standartları getirmiştir. Örneğin; Fransa, İtalya ve Belçika'da KEPHS'ler için özel olarak yasal düzenleme yapılmıştır. Diğer bazı ülkelerde ise söz konusu hizmet kamu idarelerince, noterlik işlevini de kapsayacak şekilde verilmektedir. İspanya ve İsveç'te bu hizmetin verilmesi için özel bir yasa mevcut değildir (Tanrıkulu, 2009, s.318).

Bu ülkelerdeki durumdan kısaca söz etmek gerekirse;

✓ **ABD:** 2000 yılında "Electronic Signatures in Global and National Commerce Act" ile KEP'in yasal altyapısını düzenlemiş olan ABD uygulamaya başlamıştır (Samast, 2010, s.3).

✓ **Fransa:**

2000/31/AB sayılı e-Ticaret Direktifinin iç hukuka uyarlanabilmesine ilişkin 17/06/2005 tarihli KEPHS'ler için özel bir yasa yapılmıştır. Fransa'da KEP hizmeti, ANAFOR isimli bir kuruluş tarafından sunulmaktadır. Söz konusu kuruluş, kamu yararına bir kuruluş olup standardizasyon faaliyeti yürütmektedir. Fransa'nın mevzuatına göre KEP kullanılarak elde edilen delil

ve mesajlar mahkemeye sunulup değerlendirilmesine karşın tek başına hukuki geçerliliği sağlayamamaktadır (Alkan vd, 2011, s.69).

✓ **Avusturya:**

e-Devlet uygulamaları alanında diğer Avrupa ülkelerine kıyasla ortalamanın üzerinde gelişmeler sağlamış bir olan ülkedir. Birçok alanda fiziki ortamda bulunan bilgilerini e-ortama taşımakla birlikte bu alanda önemli hamleler gerçekleştirmekte, yeni projeler ve stratejiler geliştirmektedir. Bahsi geçen ülkenin uygulamaya koyduğu e-devlet projelerinden olan kurumlar arasında e-belge paylaşılması ve buna bağlı olarak e-tebligat projesidir. Avusturya'da e-belgenin, e-tebligat vasıtasıyla iletimin, hukukiliği sağlanmış ve yeni kanunlar hazırlanmıştır. Bu kanunlardan en önemlisi e-devlet kanunudur. Bahsi geçen kanunla kanun koyucu genel anlamda e-devlet projelerinin genel çerçevesini belirlemiş ve sonrasında detay konular olarak e-tebligat, e-ödeme gibi alt konulara değinmişlerdir (Tanrıkulu, 2009, s.318).

✓ **Belçika:**

Belçika'da bireysel ve şirket kullanıcıları olmak üzere iki çeşit kullanıcı türü vardır. Şirketler ve kullanıcılar arasında fatura gönderme ve gönderilen bu faturaları ödeme işlemleri için KEP sistemi kullanılmaktadırlar. Belçika'da İtalya benzeri yasal düzenleme çalışmaları yapmaktadır. Belçika Posta ve Telekom İdaresi'nin iştiraki şeklinde KEPHS hizmetlerini sunmak için Certipost isimli bir şirket kurulmuştur (Alkan vd, 2011, s.68-69).

✓ **Hollanda:**

Kamusal hizmetlerden kaynaklanan iş ve işlemlerinin yüzde 25 ini e-ortama taşımıştır. Söz konusu ülke e-Devlet için Eylem Programı hazırlamış olup bu çerçevede başlatılan çalışmalar yerel ağ altyapısının geliştirilmesi ve güvenli iletişime yöneliktir. Bu çerçevede e-belgeyi koruma, sürdürülen altyapı çalışmalarının önemli bir parçası olarak düşünülmekte olup Ulusal Arşiv ve İçişleri Bakanlığı'nın ortaklaşa bir projesi dâhilinde geliştirildiğine vurgu yapılmaktadır (Külcü, 2006, s.209).

✓ **İngiltere:**

Avrupa'da belge yönetimini ve belge koruma çalışmalarını etkileyen ilk yasa, İsveç'te 1973 yılında kabul edilen Veri Koruma Yasası'dır. Söz konusu yasal düzenleme ile vatandaşların elektronik veya diğer belgelere serbestçe ulaşmasına zemin hazırlamış ve bilginin gizliliğine ilişkin ilkeleri belirlemiştir. 1981 yılında Avrupa Konseyi Veri Koruma Konvansiyonu'nun düzenlediği toplantıda varılan kararlar neticesinde, birçok Avrupa ülkesi kendi ulusal veri koruma düzenlemelerini yapmışlardır. Söz konusu kararlar ile bazı Avrupa ülkeleri ile birlikte İngiltere'de veri koruma yasalarını anayasal güvence altına aldığı, geliştirilen düzenlemeler kapsamında 1984 yılında İngiliz Parlamentosu'nun kabul ettiği Veri Korum Yasası'nda yer alan belge yönetimi çalışmalarına ayrıntılı bir şekilde yer vermiştir. Devletin Modernizasyonu Raporunu, 2004 yılında kabul etmiş olup 2005 yılında ise Bütün kamu kurum ve kuruluşlarında üretilen belgelerin yalnızca e-belgelerden oluşması, merkezi ve yerel kamunun sunduğu hizmetlerin tamamının çevrimiçi olarak da uygulanmıştır (Külcü, 2006, s.206-209).

✓ **İspanya:**

İspanya KEP hizmetlerini özel yasalar düzenlemiş olduğu iki ayrı yapı üzerinden uygulamakta olup, söz konusu yasal düzenlemeler iletinin gönderilmesi, tebliğ edilen zaman ve tarihi ile e-ortamda iletilen tebligatın deliline ilişkin hususları kapsamaktadır (Alkan vd, 2011, s.70).

✓ **İsveç:**

AB ülkelerinden farklı olarak KEP hizmeti diğer hizmetler ile birlikte bir alt hizmet olarak uygulanmaktadır. Kamu İhale Kanunu içinde yapılmış olan yasal düzenlemeler çerçevesinde KEP sistemi özellikle deniz aşırı yapılan ihalelerde kullanılmaktadır Chamber Sign İsveç, İsveç Ticaret Odaları Birliği'ne bağlı, e-ortamda KEP hizmeti sunan bir kuruluş olarak faaliyet yürütmektedir (Alkan vd, 2011, s.70).

✓ **İtalya:**

KEP ile; geleneksel yöntem olan iadeli taahhütlü posta benzeri bir uygulama geliştirmiştir. Söz konusu uygulamada; gönderilen mesaj, göndericinin KEPHS'sine ulaştığında, KEPHS göndericiye iletisinin kabul ya da reddedildiğine dair bir mesajı göndericisine iletir. Alıcının KEPHS'si ise bir başarılı ya da başarısız dağıtım listesi iletmektedir. İtalya'da bu konuda ayrıntılı bir hukuki düzenleme yapmıştır. Söz konusu ülkede yapılmış olan düzenlemeler çerçevesinde yapılan tespitler şu şekildedir;

- ✓ Uygulanan bu sistemin tamamında üretilen deliller hukuki geçerliğe sahip kılınmıştır.
- ✓ KEPHS'lerin hizmet sunabilmeleri için Kamu Yönetimi Ulusal Bilişim Merkezi (CNIPA) tarafından akredite edilmiş olmaları gerekmektedir.
- ✓ CNIPA, KEPHS'leri denetleyen kuruluş olarak da davranmaktadır.
- ✓ KEP'e ilişkin sertifika otoritesi olarak da görev yapan CNIPA, KEPHS'ler tarafından mesajların imzalanması için kullanılan sertifikaları da düzenlemektedir.

İtalya, 28/01/2005 tarihinde KEP hizmetine ilişkin düzenlediği Kanun'la KEPHS'lerin kuruluş ve işleyişini ayrıntılı bir şekilde hüküm altına almıştır (Alkan vd, 2011, s.67-68). İtalya'da halen KEPHS sayısı 27'dir. KEP'e ilişkin sertifika otoritesi olarak da görev yapan İtalyan CNIPA'sına, KEPHS'lerin her iki ayda bir KEP günlük toplam mesaj sayısını, gönderme yükümlülüğü vardır. KEP hizmet performansı kapsamında 2012 yılının Kasım-Aralık aylarında 91.488.442 adet, 2012 yılının Eylül-Ekim aylarında 91.488.442 adet, 2011 Kasım-Aralık aylarında 101.347.540 adet mesaj üretilmiştir (Agenzia Per L'Italia Digitale, 2013).

✓ **Almanya:**

2009 yılında ise Almanya, KEP sistemini "e-Devlet 2.0" uygulamasının ayrılmaz bir ilavesi olarak De-Mail System adıyla 2009'da Friedrichshafen'da, ülke çapında ise 2010 yılında yaygınlaştırmıştır. e-Ortamda e-tebligat

hizmetlerini ve kamu kurum ve kuruluşları arasında e-belge paylaşımı işlemlerini Vatandaş Portalı Kanun Tasarısı ile uygulamaya koymuştur. Söz konusu tasarı ile Almanya'da kullanıcıların akredite olan servis sağlayıcılardan, kimliklerini ibraz ederek e-tebligat yapabilmek için "De-Mail" adında KEP hesabı alabilmelerine imkân sağlamıştır. Kullanıcılar bahsi geçen e-posta vasıtasıyla güvenli ve şifreli bir şekilde e-posta gönderebilecekler ve alabileceklerdir. Gönderici gönderdiği e-postalar için De-Mail sisteminden hukuken kabul edilmiş onaylama kaydı alabilecektir. KEPHS bahsi geçen onaylama kaydını e-imza altına almak zorundadır. Bu uygulama ile resmi kurum ve kuruluşlarda yazışmaların e-ortamda güvenilir ve hukuki sonuçları olacak şekilde iletilmesi temin edilmiş olacaktır. 06/03/2012 tarihinde De-posta hizmeti sunacak olan üç adet De-posta servis sağlayıcı akredite olmuştur (Bundesamt für Sicherheit in der Informationstechnik, 2013).

SONUÇ

Bu çalışma boyunca ortaya konulan literatür incelemesi, anket uygulaması ve GZFT (SWOT) analizi yoluyla elde edilen sonuçlar ve bulgular aşağıda alt başlıklar halinde değerlendirilmiştir.

Günümüz dünyasında "e-" dalgası ve güvenlik arayışı.

21. yüzyıl idari, ticari ve sosyal hemen her alandaki iş ve işlemlerin e-ortamda yapılacağı/yürütüleceği bir yüzyıl olacaktır. Günümüz dünyasında adeta bir "e-" dalgası yayılmaktadır. e-Devlet, e-Posta, e-Ticaret, e-Okul, e-Banka gibi ticaretten eğitime kadar hemen herkesin ve her kesimin mecburen kullanacağı bu uygulamalar gündelik yaşantımızın birer parçası haline gelmiş bulunmaktadır. BİT, mesafeleri kısaltarak zaman tasarrufu ve mekân kolaylığı ile bizlere sağladığı avantajların yanında farklı ve yeni sorunlar da üretmektedir.

Bu çalışmanın ilgi alanı açısından bakıldığında, elektronik uygulamaların kolay, ucuz, hızlı olmak gibi avantajlarına rağmen, e-ortamda güvenli bir şekilde e-belge paylaşımı konusunda güvenlik zafiyetleri varlığını sürdürmektedir. Bu durumda da e-ortamda yapılan iş ve işlemler sonucu, üretilen e-belgelerin hukuki açıdan da geçerli olacak şekilde güvenli paylaşımı en temel ihtiyaç olarak kendini göstermektedir.

e-Belge paylaşıma ilişkin uygulamalar.

e-Belgenin güvenli paylaşımı konusunda günümüzde yaygın olarak kullanılan uygulamalar e-posta, VPN, SSL, Kiralık Hat, FTP/SFTP gibi uygulamalardır. Zaman Damgası ve güvenli e-İmza ise günümüz elektronik haberleşme araçlarının güvenlik bütünlük ve inkâr edilemezlik gibi çok kritik unsurları tesis etmek amacıyla kullanmış oldukları altyapı ve uygulamalardır.

e-Posta, VPN, SSL, Kiralık Hat, FTP/SFTP, Zaman Damgası, Güvenli e-İmza ve KEP e-belgenin hukuki düzenlemeler, teknik güvenirlik, uluslararası standartlara uygunluk, işlemin yapıldığının inkâr edilemezliği, işlemi yapanın kimliğinin belirlenmesi ve işlem zamanının tespiti açılarından değerlendirilmiştir. Bu değerlendirmenin sonuçları aşağıdaki Tablo 5-1 de gösterilmektedir:

Tablo 0.1 Belge paylaşımında kullanılan yöntemlere göre değerlendirme

e-Belge paylaşımında kullanılan yöntemlerin karşılaştırılması	Güvenli e-İmza	Zaman Damgası	Sanal Özel Ağ (VPN: Virtual Private Network)	Güvenli Yuva Katmanı (SSL: Secure Sockets Layer)	Standart Elektronik Posta	Kiralık Hat	FTP/SFTP	Kayıtlı Elektronik Posta (KEP)
Hukuki düzenleme	++	++	+(1)	+(1)	-	+(1)	+(1)	++
Teknik güvenilirlik (değişmezlik)	+	+	+	+	-	+	+	+
Uluslararası standartlara uygunluğu	+	+	+	+	+	+	+	+
İşlemin yapıldığının inkâr edilmezliği	+	-	+(1)	+(1)	-	+(1)	+(1)	++
İşlemi yapan kişinin kimliğinin belirlenmesi	++	-	+(2)	+(3)	-	+(2)	-	++
İşlemin yapıldığı kesin zamanın tespiti	-	++	+	+	-	+	+	++

(1) Taraflar arası yapılacak özel sözleşmeler ile.
(2) Bağlantı halinde olan bilgisayarların kimliği tespit edilebilmektedir.
(3) Bağlantı halinde olan tarafın sertifikası tespit edilebilmektedir.

Hukuki düzenlemeler noktasında; KEP, Güvenli e-İmza ve Zaman Damgası yasal zemini haiz olduğundan bu konudaki geçerliliği sağladığı görülmektedir. VPN, SSL, Kiralık Hat, FTP/SFTP ve e-posta hususlarında ise benzeri özel bir hukuki çerçeve bulunmamaktadır. Ancak VPN, Kiralık Hat, FTP/SFTP ve SSL taraflar arası yapılacak sözleşmelerle işlemlerine hukuken geçerlilik kazandırabilmektedir.

Standart e-postalar, gönderim aşamasında yol üzerinde okunabilir. Bir başkası, herhangi biri adına e-posta gönderimi yapabilir. Söz konusu durum e-postanın başlık bölümünün incelenmesi ile anlaşılsa dahi bunun garantisi bulunmamaktadır. Ayrıca çoğu kez yetkisiz işlem yapanı yakalamak mümkün olamamaktadır. e-Postanın bir başka olumsuz yanı, mesajı gönderen sonradan mesajı göndermediğini inkar edebilmektedir. Özellikle finans işlemlerinde bu konu önemlidir; şöyle ki bir banka müşterisi e-posta ile verdiği havale emrini inkâr edebilir, bankanın elindeki havale emrini içeren e-posta doğru olsa bile geçersizdir çünkü herkes söz konusu o e-postayı gönderebilir (Levi, 2003).

Standart e-posta ile gerçekleştirilen bilgi ve e-belge paylaşımı internette yetkisiz olarak başkalarının müdahalesine ve iletinin içeriğinde değişiklik yapabilme imkânlarına açıktır ayrıca teknik ve hukuken güvenli olmayan bir paylaşım yöntemidir (Berber, 2010).

Bilindiği üzere, dünya genelinde en çok kullanılan kitle iletişim araçlarından bir tanesi olmasına rağmen, e-Posta hizmeti günümüzde teknik güvenilirlik açısından beklentileri tam olarak karşılayamamış bir hizmet olup bir takım önlem ve eklentilerle desteklenmeye çalışılmıştır. Dünya genelinde en çok kullanılan kitle iletişim araçlarından bir tanesi olmasına rağmen, yine de yeterli derecede teknik güvenirlik içerdiği düşünülmemektedir. e-Posta ile günümüz ileti paylaşımlarında çeşitli yazılımlar aracılığı ile göndericinin kimliği, bilgisayarın adresi veya içeriği değiştirilebilmekte, alıcı ise kendisine ulaşmadığını inkar edebilmektedir. Güvenli e-İmza, Zaman Damgası, SSL, VPN, Kiralık Hat, FTP/SFTP ve KEP'i incelediğimizde ise özellikle güvenlik gereksinimlerini karşılamak için üretilen uygulamalar olduğundan yeterli düzeyde teknik güvenilirliği sağladıkları değerlendirilmektedir.

Diğer taraftan, söz konusu uygulamaların tümünün uluslararası standartlar çerçevesinde oluşturulduğu ve dünya genelinde kabul görmüş bir dizi standartlar ile işletildiği görülmektedir.

İşlemin yapıldığının inkâr edilmezliği konusunda VPN, Kiralık Hat, SSL, FTP/SFTP, Güvenli e-İmza ve KEP net olarak delil sunmasına rağmen, e-Posta bu hususta yetersiz kalmaktadır. Gerçek alıcı kişi adına yetkisiz kişilerce açılacak olan e-posta adreslerinin kullanılabiliyor olması yapılacak işlemlerin inkâr edilebileceğini göstermektedir.

İşlemi yapan kişinin kimliğinin belirlenmesinin, Güvenli e-İmza ile KEP (Güvenli e-imza destekli olması nedeniyle) tarafından güçlü bir şekilde desteklemesine rağmen VPN ve Kiralık Hat, yalnızca kimliği tespit edilen bilgisayarlar arasında trafiğe müsaade ettiği için Kiralık Hat ve VPN'de bağlantı halinde olan bilgisayarların kimliği tespit edilebilmektedir. Benzer şekilde, SSL'de sertifika üzerinden kimlik kontrolü yapılması nedeniyle işlemi yapan tarafların sertifikaları tespit edilebilmektedir. FTP/SFTP ise kullanıcı adı ve şifre girişi ile uygulama gerçekleştirildiği için işlemi yapan kişinin kimliği belirlenememektedir, e-Posta ve Zaman Damgasında işlemi yapan kişinin kimliğine ilişkin kesin bir bilgi verilmemektedir.

İşlemin yapıldığı kesin zamanının tespiti konusunda teknik ve hukuki bağlayıcılık anlamında sadece Zaman Damgası ve KEP sistemi (zaman damgasını kullandığı için) net bir şekilde öne çıkmaktadır. Güvenli e-İmza söz konusu konuda yetersiz kalmaktadır. Bilindiği üzere günümüzde yaygın şekilde e-postaya yetkisiz kişilerin yapmış olduğu müdahaleler neticesinde e-posta işlemin yapıldığı kesin zamanının tespiti konusunda tartışma konusu olabilmektedir.

Günümüzde iş ve işlemlerin sürekliliği için e-ortamda bilgi ve e-belge paylaşımının, yaygın kullanım aracı e-postadır. Bir e-postanın içeriğinin değiştirilmesi, gönderici olarak görünen kişinin gerçek gönderici olmaması, mesajın gönderilmiş ya da alınmış olduğunun ispatlanamaması gibi problemler mevcut sistemde yaşanan gerçeklerdir.

KEP ile "e-" uygulamalar daha güvenli ve tasarruf sağlamakta.

KEP'in devlet, vatandaş ve ticaret boyutu düşünüldüğünde tüm tarafların gerek kendi aralarında gerekse diğer taraflarla e-ortamda yapacakları e-belge paylaşımında e-belge bütünlüğünün bozulmadığı ve hukuki geçerlik konusunda güven verici önemli bir uygulama olacağı değerlendirilmektedir.

KEP sisteminin uygulanması ile ülkemizde e-ticaret ve e-devlet uygulamalarının yaygın olarak kullanımını teşvik edeceği, geleneksel yöntemler ile oluşan kâğıt, posta ve arşivleme maliyetleri ve zaman israfının, KEP ile çok büyük oranda minimize edileceği, çevrenin korunmasına katkıda bulunulacağı, iş ve işlemlerin hızlanması ile önemli ölçüde verimin artacağı ve maliyetlerin düşeceği değerlendirilmektedir.

Çeşitli kamu kurum ve kuruluşları ile özel sektör kuruluşları e-belge ve bilgi paylaşımında birbirinden farklı standartlara sahip çeşitli altyapı ve uygulamalar kullanmaktadır. Söz konusu altyapı ve uygulamaların birbirleri ile iletişiminde ayrıca yazılım ve donanım tercihlerdeki kısmen de olsa bilgi eksiklileri güvenli e-belge ve bilgi paylaşımında riskler içermektedir. Dolayısıyla yapılan yatırımlar amaca hizmet etmeyebilir. Bu nedenlerden dolayı ülkemizde e-ortamda e-belgelerin güvenli paylaşımı konusunda yapılan yatırımların mükerrerliği ve kaynak israfı KEP sistemi ile önlenmiş olacaktır.

KEP ile tebligata ilişkin sorunlar giderilmektedir.

Yargı alanında yaşanan gerek tebligatın muhataba ulaşması yönünde aksaklıkların meydana gelmesi, gerekse bu tür e-belge ve bilgi güvenliğinin, e-ortamda çok zor sağlanması gibi problemlere çözüm noktasında KEP önemli bir katkı sunmaktadır. Muhatap açısından bakıldığında KEP sistemi ile muhatap, tebligatı rahat bir şekilde alacaktır. Örneğin tebligata muhatap olan kişinin uzun süreli yurtdışında bulunması nedeniyle ikametgâh adresine

yapılacak tebligata zamanında ulaşamaması gibi fiziki ortamdan kaynaklanan problemler KEP hesabı ile giderilmiş olacaktır. Tebligatın e-ortamda tüm adımları için üretilen deliller neticesinde hukukiliği sağlanmış olacaktır. e-Belgenin bütünlüğü korunmuş ve bir başkasının ulaşamaması garanti altına alınmış olacaktır.

KEP uluslararası kabul görmüş bir uygulamadır.

AB'de ETSI tarafından e-posta konusunda, uluslararası standardı sağlamak adına KEP uygulaması geliştirilmektedir. Ülkemizin AB'ye uyum çerçevesinde ortak standart amacı ile geliştirilen KEP sistemini dikkate almasında fayda vardır. Ülkemiz, AB'ye uyum sürecinden vazgeçse dahi KEP, gelecekte AB ülkeleri ile iş ve işlemlerimizde kullanacağımız bir uygulama olacaktır.

Uyuşmazlık halinde KEPHS'ler tarafsız üçüncü kuruluşlardır.

KEP sisteminde iletilerde belgelerin gönderici ve alıcısının kimler olduğunun yanı sıra ne zaman gönderildiği ve teslim alındığı bilgilerini üreten, muhafaza eden üçüncü ve tarafsız olan yetkilendirilmiş kuruluşlar olarak KEPHS'ler mevcuttur. Taraflar arasında paylaşılan bilgi ve e-belgelerin paylaşanlardan biri tarafından iletildiğinin inkâr edilmesi veya e-belge içeriğinin değiştirilmiş olduğunun iddia edilmesi gibi durumlarda güvenilen ve üçüncü taraf olarak hizmet sunan KEPHS'lerin tutmuş olduğu kayıtlar hukuki delil niteliğinde olacaktır.

KEP sistemi kullanımına ilişkin, GZFT (SWOT) analizi Tablo 5.2'de yer almaktadır.

Tablo 0.2 KEP GZFT (SWOT) Analizi

Güçlü Yanlar	**Zayıf Yanlar**
Hukuki geçerlik	Bilginin KEPHS üzerinden taşınması
Fırsatlar	**Tehditler**
Ülkemiz, bazı ülkelerin örnek alacağı bir KEP uygulaması gerçekleştirebilir.	✓Kurumların oluşturacakları EBYS sisteminde kullanılacak uygun olmayan mimari ✓Kullanıcıların e-uygulamalara karşı gösterecekleri direnç

KEP, hukuken geçerli ve teknik açıdan güvenli e-posta olarak tanımlanmaktadır. KEP, yaygın e-postaya ek olarak e-postanın;

- ✓ Göndericisinin tespiti
- ✓ Alıcısına ne zaman ulaştığını veya ulaşmadığını,
- ✓ Alıcısı tarafından açılıp açılmadığını
- ✓ e-Postaya tekrar ulaşılabilmesi

gibi işlemlere ilişkin delil setini sunan bir sistemdir.

Ülkemizde KEP'e ilişkin yasal düzenlemeler.

KEP sistemi ile e-postalar bağımsız ve güvenilir bir üçüncü taraf olan KEPHS'lerce gönderilip alınmaktadır. e-Postanın gönderiminden teslim alınmasına kadar olan süreç içerisinde bütün işlemlere ait güvenli e-imza ve zaman damgası kullanılarak elde edilen ve saklanan kayıtlar delil mahiyetinde olup hukuken geçerli belgelerdir.

14/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu'nun 18 inci maddesi ile tüzel kişiler (şirketler) tarafından ihbarlar, ihtarlar, itirazlar ve benzeri beyanlar, fatura, teyit mektubu, iştirak taahhütnamesi, toplantı çağrıları, sözleşme gibi belgelerin elektronik olarak

gönderilmesi için KEP sisteminin kullanılması hüküm altına alınmış ve ülkemizdeki KEP sisteminin kanuni dayanağı oluşturulmuştur. Aynı Kanun'un 1525 inci maddesinin (2) numaralı bendi ile KEP sistemine, KEPHS'lerin hak ve yükümlülüklerine, yetkilendirilmelerine ve denetlenmelerine ilişkin ikincil düzenlemeleri yapmak üzere BTK görevlendirilmiştir.

Bu kapsamda; BTK tarafından hazırlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de, Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de, Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, 16/05/2012 ve 28294 sayılı Resmi Gazete'de, Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul Esas 06/06/2012 tarihli ve 2012/DK-15259 sayılı Kurul Kararı BTK'nın resmi internet sitesinde yayımlanmıştır. Sayılan bu mevzuat ile KEP, ülkemizde ETSI tarafından belirlenen standartlara da uyumlu yasal altyapıya kavuşmuştur. Tarafların KEP kullanımı ve uygulamalarını gözlemek için yaşananların gözlenmesi ve ortaya çıkacak aksaklıkların çözümcü bir yaklaşımla değerlendirilmesi gerekmektedir.

ÖNERİLER

Bu çalışma kapsamında geliştirilen öneriler BTK, Devlet, işletmeler ve vatandaş açısından sunulmaktadır.

BTK açısından;

BTK, KEP uygulaması konusunda öncü olabilir.

5809 sayılı Elektronik Haberleşme Kanunu'nun ilkeler başlığının altında yer alan 4 üncü maddenin (g) bendinde *"Teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımlarının teşvik edilmesi* " şeklindeki ifadeden hareketle, her şeyden önce KEP sisteminin düzenleyicisi ve denetleyicisi olan BTK'nın, henüz faaliyete geçmiş olan söz konusu sistemi kendi bünyesinde kullanarak diğer kamu kuruluşları ve özel sektör kuruluşlarına bu konuda öncülük etmesi gerektiği düşünülmektedir.

BTK, KEP sistemi kullanıcılarına öncülük etmesi için e-imza dâhil olmak üzere kendi EBYS'sini en kısa sürede aktif hale getirmeli ve bunun üzerine Kurum içi ve Kurum dışı ile güvenli bir şekilde işletmecilerden kabul ettiği çeşitli başvuru formları, kamuoyu görüşlerinin alınması, tüketici şikâyetleri, bilgi edinme gibi e-ortam uygulamalarında e-belge paylaşımı yapılabilen KEP sistemini kurmasının uygun olacağı değerlendirilmektedir.

BTK, vatandaşı KEP konusunda bilgilendirebilir.

BTK tarafından KEP sistemi ile herkesin güvenli bir şekilde bilgi ve e-belge paylaşabilecekleri konusunda, başta televizyon olmak üzere basın yayın organlarında tanıtıcı kısa filmler ile bütün vatandaşlar bilgilendirmesinin ve teşvik edilmesinin uygun olacağı değerlendirilmektedir.

BTK'nın ülkemizde KEP sistemi konusunda farkındalık oluşturulması adına başta kamu kurum ve kuruluşları olmak üzere özel sektöre ait dernek, birlik ve vakıf gibi kurum ve kuruluşlarda bilgilendirme toplantıları, eğitim seminerleri gibi etkinlikleri kesintisiz bir şekilde düzenlenmesi gerektiği düşünülmektedir.

BTK, KEP konusunda uluslararası koordinasyon sağlayabilir.

BTK koordinatörlüğünde sektör ve bireylerin e-belgeleri uluslararası düzeyde de güvenli paylaşımı için meydana gelecek aksamalar bağlamında kamu ve özel sektör kurum ve kuruluşlarında gerekli komisyonlar oluşturulup çalışmaların en kısa sürede başlatılması ve bu sayede belirlenen gereklilik ve beklentiler BTK tarafından, üyesi bulunduğu uluslararası kuruluşlarda temsil ve temin edilmesinin gerekliliği değerlendirilmektedir.

BTK, KEP konusunda yazılım/donanım tekelleşmesini önleyebilir.

KEP sistemi uygulama sürecinin başlangıç aşamasında iken, gerek halen kullanılan yazılım ve donanımlar ile üretilecek e-belge ve bilgiler açısından gerekse ileri tarihlerde ihtiyaç duyulacak arşivlenmiş bilgi ve e-belgelerin o günün şartlarındaki yazılım ve donanımlara uygunluğu açısından kullanıcıları belirli bir yazılıma ya da üreticiye mecbur bırakmayacak şekilde tasarlanmalıdır. Aksi halde KEP uygulamasının, belirli şirket ya da şirketlerin pazarlama platformuna dönüşmesi ve karşı tepkiler ile işlemez hale gelebilmesi kaçınılmaz bir sonuç olacaktır. Bu bağlamda BTK, KEPHS'lerin uyacağı kuralları ve alacağı tedbirleri yapacağı düzenlemeler ile açıkça ve önceden belirlemesinin yerinde olacağı düşünülmektedir.

BTK, KEP ile e-yazışma konusunda Kalkınma Bakanlığı ile işbirliği yapabilir.

Bütün kamu kurum ve kuruluşları için birlikte çalışabilirlik olmazsa olmaz bir koşuldur. Halen Kalkınma Bakanlığında bu yönde çalışmalar sürdürülmektedir. Sürdürülen bu çalışmalar kapsamında e-Yazışma Projesi devam etmektedir. Söz konusu Proje'nin çalışabilirliği açısından en önemli faktörlerden bir tanesi e-belgelerin e-ortamda güvenli paylaşılmasının sağlanmasıdır. Bu konuda bütün kamu kurumlarında farklı uygulamalar farklı standartları beraberinde getireceğinden yönetilmesi güç bir hal alacaktır. KEP sistemi söz konusu farklılıkları ortadan kaldıran bir uygulama olacağından kurumlar arası güvenli e-belge paylaşımı konusunda kamu açısından bir çözüm olacaktır. BTK, söz konusu projeye ve kamuda EBYS uygulamalarına ilişkin çalışmalara öncülük etme ya da etkin katılım sağlama potansiyeline sahip uzman bir kuruluştur. Bundan dolayı üzerine düşen sorumluluğu yerine getirecek bir ataklıkla konuya yaklaşma ve söz konusu projenin koordinasyonunu sağlayan Kalkınma Bakanlığı ile gerekli işbirliği yapmasının uygun olacağı düşünülmektedir.

KEP, KEPHS'ler aracılığı ile önemli bir hizmet sunmaktadır. Bu da yeni bir katma değerli hizmet alanı olarak elektronik arşivlemeyi ortaya çıkaracaktır. KEP iletileri ve Elektronik Tebligatların posta kutusunda saklanmasına ilişkin saklama kapasitesinin ihtiyaca ve gelişen teknolojiye dayalı olarak esnek tutulması ayrıca teknolojik değişikliklerde yaygın kullanılan yazılım ve donanımların göz önünde bulundurulması gibi konularda BTK'nın hazırladığı ikincil düzenlemelerde bu hizmet alanını göz önünde bulundurmasının uygun olacağı düşünülmektedir.

Devlet, işletmeler ve vatandaş açısından;

Yasal zorunluluk.

4/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu'nun 18 inci maddesinin üçüncü fıkrasında tacirler arasında ihbar veya ihtarların, güvenli e-imza kullanılarak KEP sistemi ile yapılabileceği hüküm altına alınmıştır. Dolayısıyla Türk Ticaret Kanunu şirketleri e-ortamda yapılacak işlemlerde KEP kullanmaya zorlamaktadır. Adalet Bakanlığı tarafından hazırlanan ve 19/01/2013 tarihli ve 28533 sayılı Resmi Gazete'de yayımlanan Elektronik Tebligat Yönetmeliği ise e-ortamda yapılacak tebligatlara ilişkin usul ve esasları düzenlemektedir. Söz konusu yönetmelik çerçevesinde; Genel yönetim altında bulunan kamu kurum ve kuruluşları ile yargı makamları, il özel idareleri, belediyeler, köy hükmi şahsiyetleri, barolar ve noterler tarafından PTT vasıtasıyla yapılacak elektronik tebligatları kapsamaktadır. Bahsi geçen yönetmelik ile de tebliğat çıkarmaya yetkili kamu kurum ve kuruluşlarını e-tebligat çıkarmaya dolayısıyla da KEP sistemini kullanmaya mecbur bırakmaktadır. Diğer yandan, kamu ihalelerine katılmak isteyenlere KEP kullanıcısı olma zorunluluğu getirilmesi ve EKAP sisteminin KEP ile uyumluluğunun sağlanması da KEP sisteminin uygulanmasını yaygınlaştıracaktır.

Devlet, bilgilerinin gizliliği için kendi KEP sistemini işletebilir.

Devletin, kendi kurum ve kuruluşları arasında yapılacağı resmi yazışmaları, güvenlik ve ödeyeceği ücret bağlamında KEPHS'ler üzerinden değil kendisinin kuracağı bir KEPHS üzerinden yapmasının yerinde bir karar olacağı değerlendirilmektedir.

Vatandaş ve Devlet açısından KEP uygulaması, bürokrasiyi büyük ölçüde önleyebilir.

Vatandaş tarafından e-Devlet Kapısı uygulaması üzerinden ya da kamu kurum kuruluşlarının e-uygulamaları ile yapılacak olan sorgulamalar sonucu elde edilecek e-belge ve bilgilerin (sabıka kaydı, sosyal güvenlik bilgileri, bilgi edinme başvuruları gibi) kullanıcıya KEP sistemi üzerinden iletilmesi ile gerek iletilen bilgi ve e-belge gerekse talebin karşılanması resmiyet kazanacağından vatandaş ve devlet açısından iş yükü azaltılmış olacaktır.

KEP kullanımının yaygınlaşması için teşvik edilebilir.

KEP kullanımının yaygınlaşması açısından bireysel kullanıcıların KEPHS'lere yapmaları gereken ödemenin tamamı veya bir miktarını kamunun karşılaması yerinde bir teşvik anlamı taşıyacağı düşünülmektedir.

Başbakanlık KEP sisteminin kurumlar arası ortak kullanımı açısından girişimde bulunabilir.

Başbakanlık tarafından, ülkemizde bütün kamu kurum ve kuruluşlarının gerek kendi aralarında gerekse özel sektör kurum ve kuruluşları ile kamu kurumları arasında güvenli e-belge paylaşımı konusunda KEP sisteminin kullanılmasını teşvik edecek ve zorunlu kılacak bir yönetmeliğin yayımlanması gerekliliği düşünülmektedir.

KAYNAKLAR

AGENZIA PER L'ITALIA DIGITALE, 2013, DigitPA Resmi İnternet Sitesi, PEC / Kullanım İstatistikleri Sayfası ve PEC / Kamu Yöneticilerin Listesi Sayfası, http://www.digitpa.gov.it/pec, (15/02/2013)

AHİ Gökhan, 2004, Türk Hukuku'nda Yeni Bir Boyut: Elektronik İmza Kanunu, http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=16&YazarNo=19, (28/01/2013)

AL Umut, AL Pınar, 2003, Elektronik Bilgi Kaynaklarının Seçimi, Bilgi Dünyası, C.4, S.1, s.1-14), http://www.unak.org.tr/BilgiDunyasi/4-1.htm (28/01/2013)

ALKAN Mustafa, ÜNVER Mustafa, KABASAKAL Demet, GÜNAYDIN Yüksel, 2011, Kayıtlı Elektronik Posta Sistemi Teknik Yapısı, Özellikleri ve İşleyişi, Bilgi Teknolojileri ve İletişim Kurumu

ALTIN Esin, 2008, Türkiye'de Elektronik İmza ve Elektronik Devlet Uygulamaları: Elektronik Belge Yönetimi Açısından Bir Değerlendirme Denemesi, Türk Kütüphaneciliği C.22, S.3, s.279-295, http://tk.kutuphaneci.org.tr/index.php/tk/article/view/2062/4089 (03/11/2012)

ARMA International Educational Foundation, 2012, A Guide to Commonly Used National and International Records Management Standards and Best Practices, http://www.armaedfoundation.org/pdfs/V_Jones_RIMStandards_Update2012.pdf, (11/02/2013)

ATLAS ON-LINE, 2013, İnternet sitesi, Hizmetlerimiz / İnternet Hizmetleri / Leased Line Sayfası, http://www.atlas.net.tr/services-line.php (22/07/2013)

AVLAMAZ İbrahim, 2012, Elektronik Postaların Kaynaklarına Ulaşmak İçin Başlıklarının İncelenmesi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, s.20

AYDIN Cengiz, 2005, Bilgi Dünyası, Bilgi teknolojilerinin Belge Yönetimine Etkisi ve Elektronik Belge Yönetimi, C.6, S.1, s.93-99

AYDIN Cengiz ve ÖZDEMİRCİ Fahrettin, 2011, Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması BİLGİ

DÜNYASI, C.12, S.1, s.105-127, http://www.unak.org.tr/BilgiDunyasi/12-1.htm, (23/01/2013)

BERBER Keser Leyla, 2010, Sağlık Bilişim Derneği Çalışma Grupları-Makaleler, Kişisel sağlık verilerinin Elektronik İletişim Yöntemleriyle İletimi, standartları ve çözüm yolları, http://www.sabiyap.org/makaleler.php?mak_id=20 (08/07/2013)

BÖKE Kaan vd., 2011, Sosyal Bilimlerde Araştırma Yöntemleri, Alfa Yayınları, İstanbul.

BTK, 2013a, Bilgi Edinme Sayfası, http://www.btk.gov.tr/bilgi_edinme/index.php, (03/02/2013)

BTK, 2013b, Nihazi Pazar Analizi Dokümanı, Nisan 2013 http://btk.gov.tr/elektronik_haberlesme_sektoru/sektorel_rekabet/piyasaanalizleri/dosyalar/Ek1_TP_Kiralik_Devre_PazAnalizi_nihai.pdf (22/07/2013)

BUNDESAMT für Sicherheit in der Informationstechnik, 2013, De-Mail Sayfası, https://www.bsi.bund.de/DE/Home/home_node.html (15/02/2013)

CEN, 2009a, About us, http://www.cen.eu/CEN/aboutus/Pages/default.aspx, (30/11/2012)

CEN, 2009b, "Cyber-Identity: Unique identification systems for organisations and parts thereof", s. 1-9, ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/CWA16036CyberID.pdf, (30/11/2012)

CİVELEK Yüksel Dilek ve TURAN Karahan Hamide, 2010, Kurumlar Arası e-Yazışma Çalışma Raporu, Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi Başkanlığı, http://www.e-yazisma.gov.tr/docs/e-Yazisma_Projesi_Calisma_Raporu.pdf (03/12/2012)

CROCKER D., 2004, Internet Mail Architecture, s.5, http://tools.ietf.org/html/draft-crocker-email-arch-12, (01/02/2013)

ÇANAKKALE Onsekiz Mart Üniversitesi, 2013, Kiralık Hat-Mini NASIL sayfası, http://docs.comu.edu.tr/howto/leased-line-howto-intro.html (02/07/2013)

ÇEBİ Yalçın, 2013, Dokuz Eylül Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, İnternet'e Erişim Yöntemleri E-Haberleşme, E-Ticaret Sunumu, http://www.google.com.tr/url?sa=t&rct=j&q=Kiral%C4%B1k%

2BDevre%2B(Leased%2BLine)%2Bnedir&source=web&cd=31&ved=0CCYQFjAAOB4&url=http%3A%2F%2Fyalcin.cs.deu.edu.tr%2Fimyo%2Fbil2013%2FInternet_E-Ticaret_E-Posta.ppt&ei=FwDTUZr1C4TCPM61gOgE&usg=AFQjCNGDnxR1PuXqh9_xiLd3mRh6fBOIaQ (02/07/2013)

ÇİÇEK Niyazi, BOZLAĞAN Recep, 2008, Akademik İncelemeler, C.3, S.2, s.190-222. http://www.aid.sakarya.edu.tr/uploads/Pdf_2008_2_77.pdf (03/11/2012)

ÇİÇEK Niyazi, 2011, Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme, Bilgi Dünyası, C.12, S.1, s.87-104, http://www.unak.org.tr/BilgiDunyasi/12-1.htm, (28/01/2013)

DAĞDAŞ Yasemin , 2005, Elektronik Belge Tanımlaması Ve Uluslararası Elektronik Belge Tanımlama Standartları Yüksek Lisans Tezi, T.C.Marmara Üniversitesi Türkiyat Araştırmaları Enstitüsü Bilgi ve Belge Yönetimi Bölümü, İstanbul

DEMİR Fuat, 2010, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, Güvenli Veri İletiminde Kullanılan VPN Tiplerinin Uygulaması ve Performans Analizi, Yüksek Lisans Tezi

DPT, 2009, e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi, Sürüm 2.0, Bilgi Toplumu Dairesi

DÜZENLİ Ümit Nihal, 2006, Arşiv Yönetimi: Türkiye Cumhuriyet Merkez Bankası Örneği, Uzmanlık Yeterlilik Tezi, Ankara

EKEN Musa, 2005, Yönetimde Şeffaflık, Sakarya Kitabevi, Adapazarı

ERİZA, 2013, Network(Ağ)Kurulum Hizmetleri Sayfası, http://www.eriza.com.tr/network-remote.asp, (03/07/2103)

ETLACAKUŞ Necati, 30/05/2013, Sözlü Görüşme, TNB BİM Müdürü, Ankara, Necati.etlacakus@tnb.org.tr

ERDAL Murat, 2004, Elektronik Devlet e-Türkiye ve Kurumsal Dönüşüm, Filiz Kitabevi, İstanbul

ERKUT İlhan, 2006, Noktadan Noktaya Protokol, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü

EROĞLU Tuğba, 2006, e-Devlet Uygulamaları Çerçevesinde MERNİS Projesi ve Beklentiler, Sayıştay Dergisi, Sayı 62, http://dergi.sayistay.gov.tr/Default.asp?sayfa=2, (21/02/2013)

ERTURGUT Mine, 2003, Elektronik İmza Kanunu Bakımından E-belge ve E-imza, Bankacılar Dergisi, S.48

ETSI, 2010, ETSI TS 102 640-4 V2.1.1, Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM), http://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf (28/11/2012)

ETSI, 2011, Electronic Signatures Applied to Registered Emails: formats and policies, http://portal.etsi.org/STFs/STF_HomePages/STF318/STF318.asp, (30/11/2012)

ETSI, 2012a, Current Specialist Task Forces, http://portal.etsi.org/stfs/STF_HomePages/STF_List.asp, (30/11/2012)

ETSI, 2012b, An overview of the European Telecommunication Standards Institute, http://www.etsi.org/WebSite/document/aboutETSI/ETSIGenericPresentation2012_updatedSpring2012.pdf, (30/11/2012)

GÜLER Mustafa ve ÖMÜRGÖNÜLŞEN Uğur, 2011, Türkiye'de e-İmza Alanındaki Hukuki Düzenlemeler ve Bazı Kamu Kurumlarındaki e-İmza Uygulamaları, Sosyoekonomi Bilimsel Hakemli Süreli, s.198-230, http://www.sosyoekonomi.hacettepe.edu.tr/2011-1-tr.html, (21/02/2013)

GÜNELİ Nihan, 2013, Elektronik Tebligat Yönetmeliği Hakkında, Information and Technology Law Journal, http://www.internetlawturkey.com/pages/articles-in-turkish, (04/02/2013)

HIZ Yüksel, YILMAZ Zekeriya, 2004, Bilgi Edinme ve Dilekçe Hakkı, Seçkin Yayıncılık, Ankara, http://www.unak.org.tr/BilgiDunyasi/gorusler/2005/1/89-97.pdf, (01/11/2012)

IETF, 2005, Securing FTP with TLS, http://www.ietf.org/rfc/rfc4217.txt (03/07/2013)

INTVEN Hank, TETRAULT McCarthy, 2000 Telecommunications Regulation Handbook, Appendix C, s.8

İŞ YAZILIM, 2012, E-Yazışma Taslak Paketi Yayınlandı, TÜM HABER VE DUYURULAR / E-Yazışma Taslak Paketi Yayınlandı, http://www.isyazilim.com.tr/kamusis/haber/eyazisma_taslak_paketi_yayinlandi-38.html, (02/11/2012)

İTÜ/BİDB, 2013, Destek, Makaleler, Derlemeler ve Denemeler, Sistem Derlemeleri Sayfası, http://www.bidb.itu.edu.tr/?d=576, (02/07/2013).

KABASAKAL Demet, 2013, Kayıtlı Elektronik Posta İnternet ve Yaşam Platformu – III, 19/01/2013 TODAİE Sunumu

KABASAKAL Demet, 2011, Yeni Türk Ticaret Kanunu Hükümleri Işığında "Dijital Şirket" Konferansı, http://cyberlaw.bilgi.edu.tr/post/11357480920 (01/02/2013)

KANDUR Hamza, 2006, Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli (v.2.0) Gözden geçirilmiş 2. Basım, İstanbul, s.1-111

KANDUR Hamza, 2008, Kamu Kurumlarında Belge Yönetim Sistemlerinin E-Dönüşümü ve Modellenmesi, http://www.unak.org.tr/unak08/, (05/11/2012)

KANDUR Hamza, 2009, Elektronik Belgelerin Standartlarla Yönetimi. Elektronik Belge Yönetimi Bilgilendirme Toplantısı, Devlet Arşivleri Genel Müdürlüğü, 13-17 Nisan 2009, Ankara.

KANDUR Hamza, 2011, Türkiye'de Kamu Kurumlarında Elektronik Belge Yönetimi: Mevcut Durum Analizi ve Farkındalığın Artırılması Çalışmaları, Bilgi Dünyası, C.12 S.1 s.2-12, www.unak.org.tr/BilgiDunyasi/gorusler/2011/cilt12/sayi1/2-12.pdf (20/06/2012)

KARAKOÇAK Kemal, NANECİ Erdal, ATLACAKUŞ Necati, 2006 Elektronik imza el kitabı, Ankara Barosu Yayınları, Ankara, http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/until2007/elektronik06.pdf

KARASAR Niyazi, 1991, Araştırmalarda Rapor Hazırlama, Sanem Matbaacılık, Ankara.

KAVI, 2012, Kavimailing List Manager Help-Chapter 7. http://support.kavi.com/khelp/kmlm/user_help/html/how_email_works.html, (22/12/2012)

KESER Leyla vd, 2004, Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, Bilgi Üniversitesi Yayını, http://bthukuku.bilgi.edu.tr/pages/left_07.asp, (11/12/2012)

KIOSKEA, 2012, How email Works (MTA, MDA, MUA), http://en.kioskea.net/contents/courrier-electronique/fonctionnement-mta-mua.php3 (21/12/2012)

KÜLCÜ Özgür, 2006, Bilgi Dünyası, Küreselleşme Sürecinde Avrupa Birliği'nde Belge Yönetimi Uygulamaları ve Türkiye, C.7, S.2, s.202-229, http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/K%C3%BCresellefl flme%20S%C3%BCrecince%20Avrupa%20Birli%C2%A4i%E2%80%99nde%20Belge.pdf, (01/11/2012)

LEVİ Albert, 2003, Nasıl bir e-posta güvenliği, Bilişim Güvenlik, Mart/Nisan 2003, in Turkish, sayfa 38 – 40, http://people.sabanciuniv.edu/~levi/ (08/07/2013)

MEB, 2008a, Meslekî Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, Bilişim Teknolojileri Ağ Güvenliği (Yazılım), http://megep.meb.gov.tr/mte_program_modul/modul_pdf/481BB0064.pdf, (15/11/2012)

MEB, 2008b, Meslekî Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, Bilişim Teknolojileri Ağ Temelleri, http://hbogm.meb.gov.tr/modulerprogramlar/kursprogramlari/bilisim/moduller/agtemelleri.pdf, (29/01/2013)

METİN Abdullah, 2012, Türkiye'de E-devlet Uygulaması ve E-devletin Bürokrasiye Etkisi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S.7, s.97-108, http://www.e-dusbed.com/OncekiSayilarDetay.aspx?Sayi=2012-1, (28/01/2013)

MİCROSOFT, 2012a, Windows Server, VPN Nedir Sayfası, http://technet.microsoft.com/tr-tr/library/cc731954(v=ws.10), (14/11/2012)

MİCROSOFT, 2012b, Windows Destek, Güvenli Yuva Katmanı (SSL) sertifikaları hakkında bilgi alma sayfası, http://windows.microsoft.com/tr-TR/windows-vista/Get-information-about-Secure-Sockets-Layer-SSL-certificates, (14/07/2012)

MİCROSOFT, 2013, Windows Destek, Dosya Aktarım Protokolü (FTP): sık sorulan sorular, http://windows.microsoft.com/tr-tr/windows-vista/file-transfer-protocol-ftp-frequently-asked-questions, (02/07/2013)

ODABAŞ Hüseyin, 2008, Elektronik Belge Düzenleme Yaklaşımları ve Türkiye'de E-Devlet Uygulamalarında Elektronik Belge Yönetimi, Sosyal Bilimler Enstitüsü Dergisi, Atatürk Üniversitesi, C.12, S.2, s.121-142. http://e-dergi.atauni.edu.tr/index.php/SBED/article/viewFile/537/529, (04/10/2010)

ODABAŞ Hüseyin, 2009, Bilgi Kaynaklarının İşletiminde Elektronik Doküman Yönetimi ve Elektronik Belge Yönetimi Sistemlerinin Rolü, Akademik Bilişim '09, 11-13 Şubat 2009, Harran Üniversitesi, Şanlıurfa, s.411-421, www.ab.org.tr/ab09/sunum/11.ppt, (18/09/2010)

ODTÜ BİDB, 2013, http://faq.cc.metu.edu.tr/index.php?yanit=241&lnk=ayrinti_sonuc (05/07/2013)

ÖNAÇAN Mehmet Bilge Kağan, MEDENİ Tunç Durmuş, ÖZKANLI Özlem, 2012, Elektronik Belge Yönetim Sistemi (EBYS)'nin Faydaları ve Kurum Bünyesinde EBYS Yapılandırmaya Yönelik Bir Yol Haritası, Sayıştay Dergisi S.85/ Nisan-Haziran, http://dergi.sayistay.gov.tr/icerik/der85m1.pdf (06/11/2012)

ÖZDEMİRCİ Fahrettin, YALÇINKAYA Bahattin, 2009, Belge Yönetiminde Değişim Süreci, 8. Ulusal Büro Yönetimi ve Sekreterlik Kongresi, 14-16 Ekim s.1-18 Ankara, http://beyas.ankara.edu.tr/dosyalar/Yararli_dokumanlar/8_buro_yon_sem.pdf, (06/10/2010)

ÖZTÜRK Özgür, 2009, E-postalarda SPAM Sorunu ve Çözüm Önerileri. Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi

SAĞIROĞLU Şeref ve ALKAN Mustafa, 2005, Her yönüyle E-imza, Ankara: Grafiker Yayınları

SAMAST Yüksel, 2010, Kayıtlı Elektronik Posta (KEP) Sistemi, Akademik Bilişim 10-12 Şubat, Muğla, http://ab.org.tr/ab10/liste.html, (05/02/2013)

SARIÖZ Mustafa, 2013, Linux'te Güvenlik, Fatih Üniversitesi, www.fatih.edu.tr/~msarioz/.../9.1.Bilg_224_linuxta_guvenlik.ppt (19/02/2013)

SAYIN Meltem, 2009, Sermaye Piyasaları'nda Elektronik Ticaret ve Banka Çalışanları Üzerine Bir Araştırma, Yüksek Lisans Tezi

SÜMER Nihat, 02/04/2013, Sözlü Görüşme, BTK Bilişim Sistemleri Dairesi Başkanı, Ankara, nsumer@btk.gov.tr

TANRIKULU Cengiz, 2009, Türk ve Avusturya Hukukunda Elektronik Tebligat, Barolar Birliği Dergisi, S.85, s.315-331, http://tbbdergisi.barobirlik.org.tr/, (04/02/2013)

T.C. İÇİŞLERİ BAKANLIĞI, 2013, Teknik Bilgi Sayfası, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Resmi İnternet Sitesi, https://kpsbasvuru.nvi.gov.tr/Kps.aspx, (20/02/2013)

T.C. İÇİŞLERİ BAKANLIĞI, 2008, MERNİS Projesinin Tarihçesi, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Resmi İnternet Sayfası, http://www.nvi.gov.tr/Hakkimizda/Projeler,Mernis_Dundenbugune.html (15/02/2013)

T.C. İÇİŞLERİ BAKANLIĞI, 2009, Genel Olarak MERNİS, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü Resmi İnternet Sayfası, http://www.nvi.gov.tr/Hakkimizda/Projeler,Mernis_Genel.html (15/02/2013)

T.C. KALKINMA BAKANLIĞI, 2011a, Bilgi Toplumu Dairesi, e-Yazışma Projesi, İnternet Sayfası, s.12, http://www.e-yazisma.gov.tr/SitePages/projeHakkinda.aspx, (02/12/2012)

T.C. KALKINMA BAKANLIĞI, 2011b, Bilgi Toplumu Dairesi, e-Yazışma Teknik Rehberi, Versiyon 1.0, s.7, http://www.e-yazisma.gov.tr/SitePages/dokumanlar.aspx, (01/12/2012)

T.C. KALKINMA BAKANLIĞI, 2012, Kamu-BİB Aylık Bilgilendirme Toplantısı, e-yazışma Projesi, s.1-33, http://www.bilgitoplumu.gov.tr/Documents/1/Diger/eYazisma_%20Projesi_%20Kamu_%20BIB.pdf, (02/12/2012)

T.C. SAYIŞTAY BAŞKANLIĞI, 2006, Performans Denetimi Raporu, e-Dönüşüm Türkiye Projesi Çerçevesinde Yürütülen Faaliyetler, http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-3eDTR/2006-eDTR.pdf, (22/01/2013)

TBD, 2009, Kamu-BİB Kamu Bilişim Platformu XI, Elektronik Belge Yönetimi, Sürüm 0.2, 1. Çalışma Grubu

TDK, 2013, Resmi İnternet Sitesi, http://www.tdk.org.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.511cdf043d3538.96918061 (14/02/2013)

TSE, 2013, Standartlar Sayfası, http://bilisim.tse.org.tr/-b-standardlar-b-/ebys, (02/02/2013)

TÜBİTAK, 2008, Elektronik İmza Hakkında Bilgiler, TÜBİTAK, 2011, Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi, Bilgem, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, Kamu Sertifikasyon Merkezi, http://www.kamusm.gov.tr/dosyalar/rehberler/guvenli_belge_rehberi.pdf (30/01/2013)

TÜRK TELEKOM, 2013, Kiralık Devre Sayfası, http://www.turktelekom.com.tr/tt/portal/KurumsalUrun/KOBI/Data-ve-Genis-Bant-Hizmetleri/Noktadan-Noktaya-Erisim-Hizmetleri/Kiralik-Devre/nedir (02/07/2013)

TÜRKSAT Uydu Haberleşme Kablo TV ve İşletme A.Ş, 2013a, Hakkımızda Sayfası, https://www.turkiye.gov.tr/, (25/05/2013)

TÜRKSAT Uydu Haberleşme Kablo TV ve İşletme A.Ş, 2013b, Sıkça Sorulan Sorular Sayfası, https://www.turkiye.gov.tr/, (25/05/2013)

TÜRKSAT Uydu Haberleşme Kablo TV ve İşletme A.Ş, 2013c, Güvenliğiniz İçin Sayfası, https://www.turkiye.gov.tr/, (25/05/2013)

UYAP, 2012, UYAP Resmi İnternet Sayfası, UYAP Sunumları, http://www.uyap.gov.tr/yayinlar/sunum/index.html (14/02/2013)

ÜNVERDİ N. Özlem, YÜKSEL Zeynep, 2007, Ağ Güvenliği Ve Güvenlik Duvarında VPN Uygulaması, EMO yayını, www.emo.org.tr/ekler/c246594da24758e_ek.pdf (29/01/2013)

yaSSL, 2012, CyaSSL User Manual Version 2.10, 11 Mayıs 2012, http://www.yassl.com/documentation/CyaSSL-Manual.pdf, (21/11/12)

YILDIZ Özcan Rıza, 2010, Elektronik Belge Yönetim Sistemleri ve Denetim, Sayıştay Dergisi, S.78, http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=78, (25/01/2013)

YILMAZ Mustafa, 2013, TS 13298 Standardı Işığında Elektronik Belge Yönetim Sistemleri, Akademik Bilişim Konferansları, http://ab.org.tr/ab13/kabul.html, (02/02/2013)

YÜKSEL Zeynep, 2007, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, Ağ Güvenliği ve Güvenlik Duvarında VPN ve Nat Uygulamaları, Yüksek Lisans Tezi

EKLER

Ek 0-1. e-Ortamda e-Belgelerin Güvenli Paylaşım Anketi İçin Yurt Dışı Kurum ve Kuruluşlara Gönderilen Üst Yazı

ICTA
Information and Communication Technologies Authority

REPUBLIC OF TURKEY
Information and Communication Technologies Authority

REFERENCE: B.62.0.BTK.0.77-799/ 69352 – 31156 10../11./2010
SUBJECT : Secure Exchange of Documents Via Electronic Media

Dear Sir/Madam,

Information and Communication Technologies Authority (ICTA) is a regulatory body of the telecommunication sector in Turkey. As it is known, telecommunications technology is one of the fastest developing technologies. As a regulatory body, the Authority follows the latest technologies and international applications in telecommunications sector closely. Therefore, the Authority is in charge implementing the national plan to spread and generalize electronic signature and its applications. As you know, secure exchange of documents via electronic media is one of the important subject that telecommunications sector encountered.

In order to extend developments in secure exchange of documents via electronic media as a part of telecommunications sector, Mr. Mustafa YILMAZ, expert in ICTA's Information Technologies and Coordination Department, has been in charged to propose a model by taking knowledge of other countries about secure exchange of documents via electronic media.

On this purpose, your knowledge and experience will be useful and we will be pleased if you could answer the questions in the the following link (**http://www.btk.gov.tr/anket/mst/anket.htm**). In case of any questions you can contact with Mr. Mustafa YILMAZ (myilmaz@btk.gov.tr)

Thank you for your help and cooperation.

Best wishes.

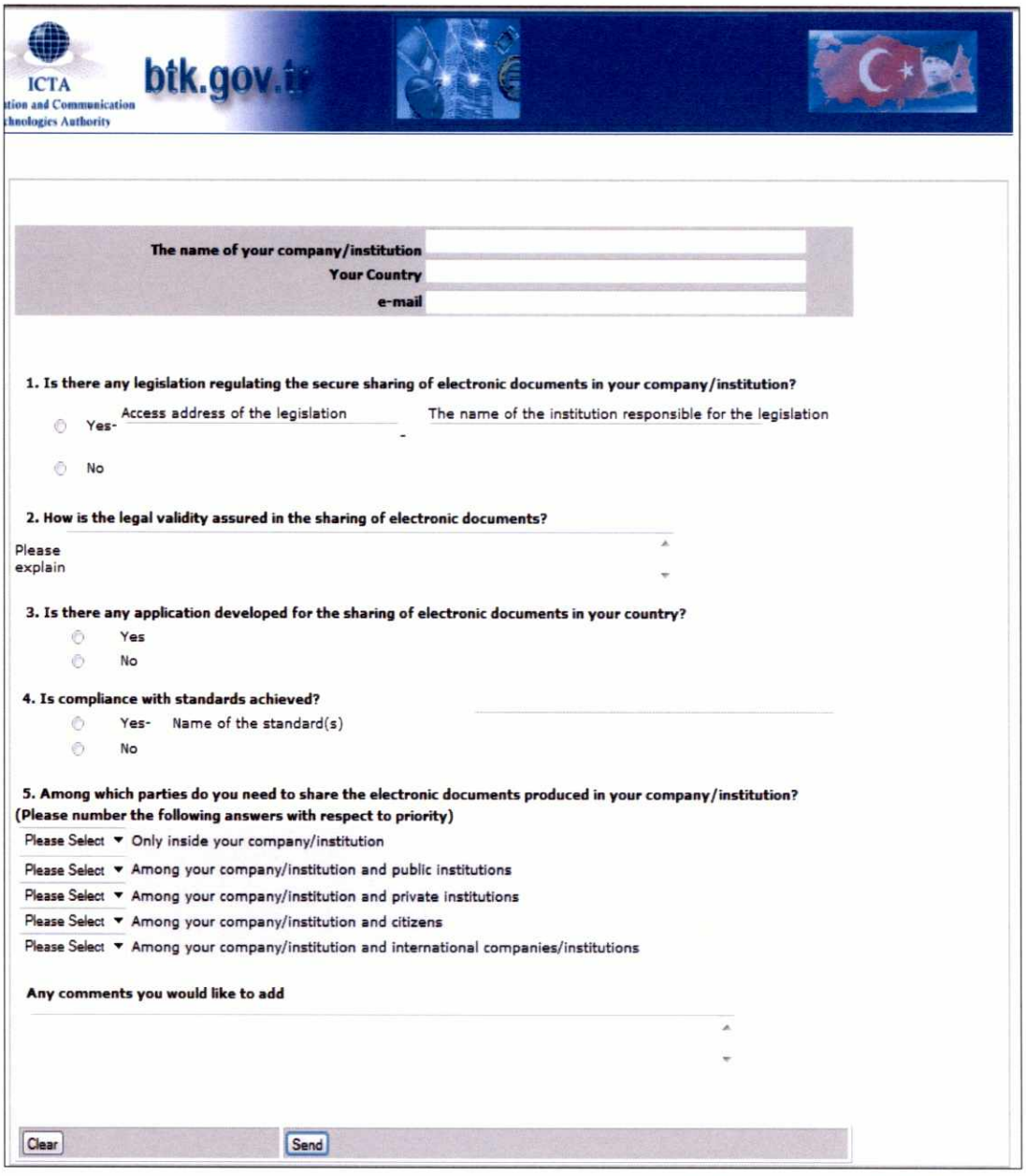
Assoc. Prof. Dr. Mustafa ALKAN

Vice Chairmen of
Information and Communication Technologies Authority

10./ 11 / 2010 Uzman : M.YILMAZ
10./ 11/ 2010 Dai.Bşk. : M. ÜNVER

Correspondence Address:
Telekomünikasyon Kurumu
Yeşilırmak Sok. No:16
06430 Demirtepe-Kızılay/Ankara TURKİYE
Phone: +90 (312) 294 70 58
Fax: +90(312)294 71 73
e-mail: myilmaz@btk.gov.tr
http://www.tk.gov.tr

Ek 0-2. e-Ortamda e-Belge Güvenli Paylaşım Yurt Dışı Anket Soruları



ICTA
tion and Communication
chnologies Authority

btk.gov.tr

The name of your company/institution

Your Country

e-mail

1. Is there any legislation regulating the secure sharing of electronic documents in your company/institution?

Yes- Access address of the legislation — The name of the institution responsible for the legislation

No

2. How is the legal validity assured in the sharing of electronic documents?

Please explain

3. Is there any application developed for the sharing of electronic documents in your country?

Yes

No

4. Is compliance with standards achieved?

Yes- Name of the standard(s)

No

5. Among which parties do you need to share the electronic documents produced in your company/institution? (Please number the following answers with respect to priority)

Please Select ▾ Only inside your company/institution

Please Select ▾ Among your company/institution and public institutions

Please Select ▾ Among your company/institution and private institutions

Please Select ▾ Among your company/institution and citizens

Please Select ▾ Among your company/institution and international companies/institutions

Any comments you would like to add

Clear Send

Ek 0-3. e-Ortamda e-Belgelerin Güvenli Paylaşım Anketi İçin Yurt İçi Kurum ve Kuruluşlara Gönderilen Üst Yazı

BTK
BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

T.C.
BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU
Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı

K - Q
TSE-ISO-EN
9000

Sayı : B.62.0.BTK.0.77-799- 60923-21242 30/09/2010

Konu: Elektronik Ortamda Belgelerin Güvenli Paylaşımı

Elektronik ortamda üretilen bilgi ve belgenin artan önemine paralel olarak, güvenli bir şekilde kaydedilmesi, iletilmesi, saklanması, paylaşılması da çok fazla önem kazanmaya başlamıştır. Paylaşılan bu belgelerin "Belge Özelliklerinin" bir bütün olarak bozulmadan varlığını ve güvenliğini koruyabilmesinin, paylaşım aşamasında ki taraflar açısından da önemli olduğu aşikardır. Bu önem taraflar arasında etkin bilgi ve belge paylaşımının sağlanabilmesi, kurumsal bilgi ve belgelerin belli bir sistem içerisinde düzenlenmesini zorunlu kılmaktadır. Bu nedenle, elektronik hizmetleri kullanan ya da elektronik ortamdaki bilgi ve belgelerini paylaşan tarafların, elektronik ortamda işlemleri güvenli bir şekilde gerçekleştirmek ve muhataplarıyla karşılıklı güveni sağlamak için uygun güvenlik kontrollerine ve mekanizmalarına sahip olması önem arz etmektedir.

Kurumumuzda "Elektronik Ortamda Belgelerin Güvenli Paylaşımı" konulu bir uzmanlık tezi hazırlanmaktadır. Bu tezde Elektronik Ortamda Belgelerin Güvenli Paylaşımına ilişkin ülkemizdeki mevcut durumu ortaya koyabilmek amacıyla http://www.btk.gov.tr/anket/mst/anket.htm adresinde yer alan anket sorularının şirketiniz/kurumunuz ilgili ve yetkili kişileri tarafından 15.11.2010 tarihine kadar cevaplanması çok büyük katkı sağlayacaktır.

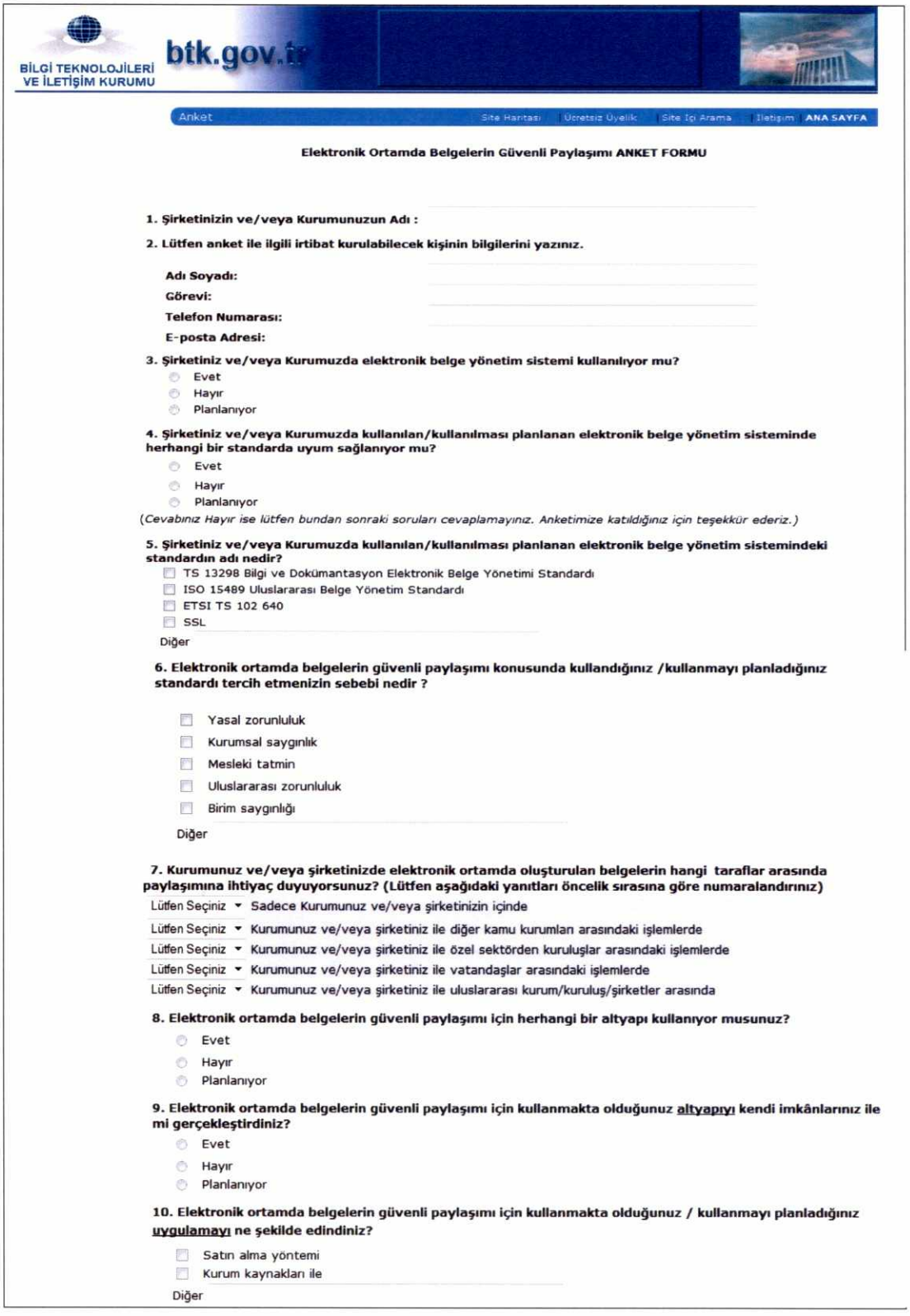
Gereğini arz/rica ederim.

Mustafa ÜNVER
Kurum Başkan Yardımcısı V.

Bilgi Teknolojileri ve İletişim Kurumu
GMK Bulvarı Yeşilırmak Sk. No : 16
06430 Demirtepe / ANKARA
Tel : (312) 294 70 58 Fax : (312) 294 71 73
Elektronik Ağ: www.btk.gov.tr

Ayrıntılı bilgi için irtibat: M.YILMAZ Uzman

Ek 0-4. e-Ortamda e-Belgelerin Güvenli Paylaşım Yurt İçi Anket Soruları



BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

btk.gov.tr

Anket | Site Haritası | Ücretsiz Üyelik | Site İçi Arama | İletişim | ANA SAYFA

Elektronik Ortamda Belgelerin Güvenli Paylaşımı ANKET FORMU

1. Şirketinizin ve/veya Kurumunuzun Adı :

2. Lütfen anket ile ilgili irtibat kurulabilecek kişinin bilgilerini yazınız.

Adı Soyadı:

Görevi:

Telefon Numarası:

E-posta Adresi:

3. Şirketiniz ve/veya Kurumuzda elektronik belge yönetim sistemi kullanılıyor mu?

- Evet
- Hayır
- Planlanıyor

4. Şirketiniz ve/veya Kurumuzda kullanılan/kullanılması planlanan elektronik belge yönetim sisteminde herhangi bir standarda uyum sağlanıyor mu?

- Evet
- Hayır
- Planlanıyor

(Cevabınız Hayır ise lütfen bundan sonraki soruları cevaplamayınız. Anketimize katıldığınız için teşekkür ederiz.)

5. Şirketiniz ve/veya Kurumuzda kullanılan/kullanılması planlanan elektronik belge yönetim sistemindeki standardın adı nedir?

- TS 13298 Bilgi ve Dokümantasyon Elektronik Belge Yönetimi Standardı
- ISO 15489 Uluslararası Belge Yönetim Standardı
- ETSI TS 102 640
- SSL

Diğer

6. Elektronik ortamda belgelerin güvenli paylaşımı konusunda kullandığınız /kullanmayı planladığınız standardı tercih etmenizin sebebi nedir ?

- Yasal zorunluluk
- Kurumsal saygınlık
- Mesleki tatmin
- Uluslararası zorunluluk
- Birim saygınlığı

Diğer

7. Kurumunuz ve/veya şirketinizde elektronik ortamda oluşturulan belgelerin hangi taraflar arasında paylaşımına ihtiyaç duyuyorsunuz? (Lütfen aşağıdaki yanıtları öncelik sırasına göre numaralandırınız)

Lütfen Seçiniz ▾ Sadece Kurumunuz ve/veya şirketinizin içinde

Lütfen Seçiniz ▾ Kurumunuz ve/veya şirketiniz ile diğer kamu kurumları arasındaki işlemlerde

Lütfen Seçiniz ▾ Kurumunuz ve/veya şirketiniz ile özel sektörden kuruluşlar arasındaki işlemlerde

Lütfen Seçiniz ▾ Kurumunuz ve/veya şirketiniz ile vatandaşlar arasındaki işlemlerde

Lütfen Seçiniz ▾ Kurumunuz ve/veya şirketiniz ile uluslararası kurum/kuruluş/şirketler arasında

8. Elektronik ortamda belgelerin güvenli paylaşımı için herhangi bir altyapı kullanıyor musunuz?

- Evet
- Hayır
- Planlanıyor

9. Elektronik ortamda belgelerin güvenli paylaşımı için kullanmakta olduğunuz altyapıyı kendi imkânlarınız ile mi gerçekleştirdiniz?

- Evet
- Hayır
- Planlanıyor

10. Elektronik ortamda belgelerin güvenli paylaşımı için kullanmakta olduğunuz / kullanmayı planladığınız uygulamayı ne şekilde edindiniz?

- Satın alma yöntemi
- Kurum kaynakları ile

Diğer

11. Elektronik ortamda belgelerin güvenli paylaşımı konusunda karşılaştığınız problemlerin varsa sebebi;

- [ ] Maddi
- [ ] İnsan kaynağı yetersizliği
- [ ] Süreçlerin belirsizliği
- [ ] Yazılımların yetersizliği
- [ ] Donanım yetersizliği
- [ ] Yönetim desteği eksikliği
- [ ] Mevzuattan kaynaklanan problemler
- [ ] Teknik Problemler
- [ ] Uygulamaya İlişkin Problemler
- [ ] Yeterli eğitimli personel olmayışı
- [ ] Uygulamayı/Altyapıyı geliştiren tarafın yetersizliği
- [ ] Kullanım sürecinin başında olunması
- [ ] Güvenli kullanımın tam tesis edilememesi

Diğer

12. Elektronik ortamda belgelerin güvenli paylaşımı uygulamanızla kullanmış olduğunuz belge, üretilen belgenin yüzde kaçına karşılık gelmektedir?

- ○ % 5
- ○ % 10
- ○ % 15
- ○ % 20
- ○ % 20 den fazla

13. Elektronik ortamda belgelerin güvenli paylaşımı uygulamanız için hangi Kurum /Kuruluş ile işbirliği yapıyorsunuz/planlıyorsunuz? (Uygun olanları işaretleyiniz)

- [ ] Devlet Arşivleri Genel Müdürlüğü
- [ ] UEKAE
- [ ] TSE
- [ ] TURKSAT
- [ ] BTK
- [ ] Hiçbiri

14. Ülkemizde elektronik ortamda güvenli belge paylaşımı için sizce yeni bir düzenlemeye ihtiyaç var mı?

- ○ Evet
- ○ Hayır
- ○ Planlanıyor

15. Eklemek istedikleriniz

Formu Kaydet Formu Sıfırla

e-Belge Paylaşımına İlişkin Anket Uygulaması

Anket aracılığı ile dünyada ve ülkemizdeki kurum ve kuruluşların oluşturdukları belgelerin ne kadarını e-ortamda oluşturdukları, e-ortamda oluşturulan e-belgelerin standartlara uyum sağlayıp sağlamadığı, hangi standardı tercih ettikleri, tercih nedenleri, kullandıkları altyapı, e-belgelerin üretilmesi ve paylaşılması konusundaki karşılaştıkları problemler ve nedenleri, e-ortamda e-belge paylaşımında kullanılan standartlar ve bu standartları tercih nedenleri gibi farkındalık ve aksaklıkların tespiti amaçlanmıştır.

e-Ortamda e-belgelerin güvenli paylaşımı konulu yapılmış olan araştırma, ankete dayanmaktadır. Anket, nicel araştırma yöntemi olup bu yöntemde tarama modeli esas alınmıştır (Böke vd, 2011, s.277). Anılan yöntemde araştırmanın modeli olarak esas alınan değişkenlerin tür ya da miktarının birer birer oluşumlarını tespit etmeye yönelik gerçekleştirilen tekil tarama modeli uygulanmıştır (Karasar, 1991, s.79).

Araştırmada her soru kendi içinde değerlendirildiğinden ve değişkenlerin birbirlerine olan etkileri ve birbirleriyle ilişkileri araştırılmadığından anket sorularının güvenilirliğine ilişkin "ki kare" testi benzeri bir uygulamaya gidilmemiştir. Araştırmada basit değerlendirme yöntemi ile % değerler kullanılmıştır.

Anketler yurt içi ve yurt dışı kamu kurumları, özel sektör kurum ve kuruluşları ve üniversitelerde e-ortamda yapılmıştır. Yurt içinde yaklaşık 50 adet kamu kurumu, üniversite ve özel sektör kuruluşuna "e-ortamda e-belgelerin güvenli paylaşımı" konulu anket soruları gönderilmiştir. Ancak ankete 39 adet kurum ve kuruluş cevap vermiştir. AB ülkelerinin 50 adet kurum ve kuruluşuna göndermiş olduğumuz anketimize 11 adet kurum ve kuruluştan cevap gelmiştir.

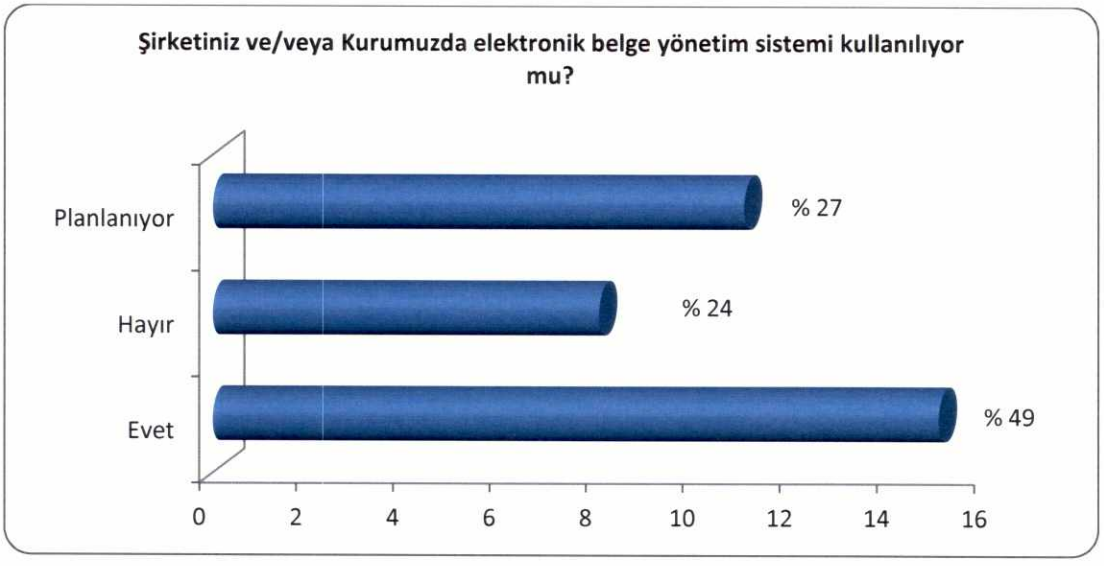
Ek 0-5. Yurt İçi ve Yurt Dışı Anket Sonuçları

➢ Yurt İçi Anket Sonuçları

Yurt içi ankete ilişkin sorular EK 6-4'de yer almaktadır. Anketin 1 ve 2 nci soruları katılımcıların kişisel ve iletişim bilgilerini içermektedir. Söz konusu ankete verilen cevap ve değerlendirmeler aşağıda yer almaktadır.

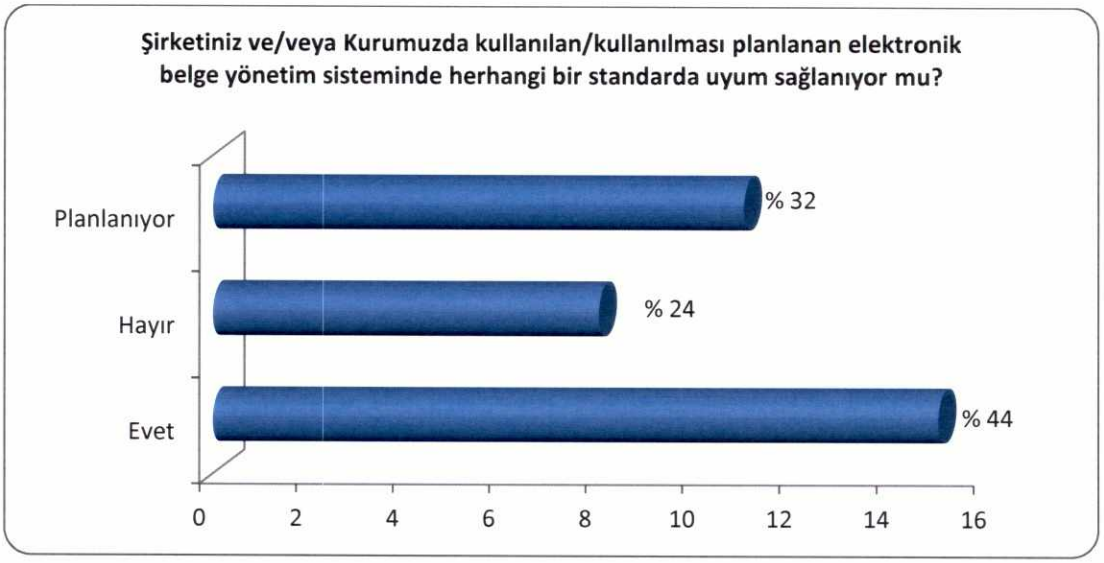
✓ Anketin, "Şirketiniz ve/veya Kurumuzda EBYS kullanılıyor mu?" sorusunda,
  - ✓ "Evet" seçeneği 18 tercihle % 49,
  - ✓ "Hayır" seçeneği 9 tercihle % 24,
  - ✓ "Planlanıyor" seçeneği 10 tercihle % 27 olmuştur.

Şekil Ek 0-1 Anketin 3 üncü sorusuna verilen cevapların dağılımı



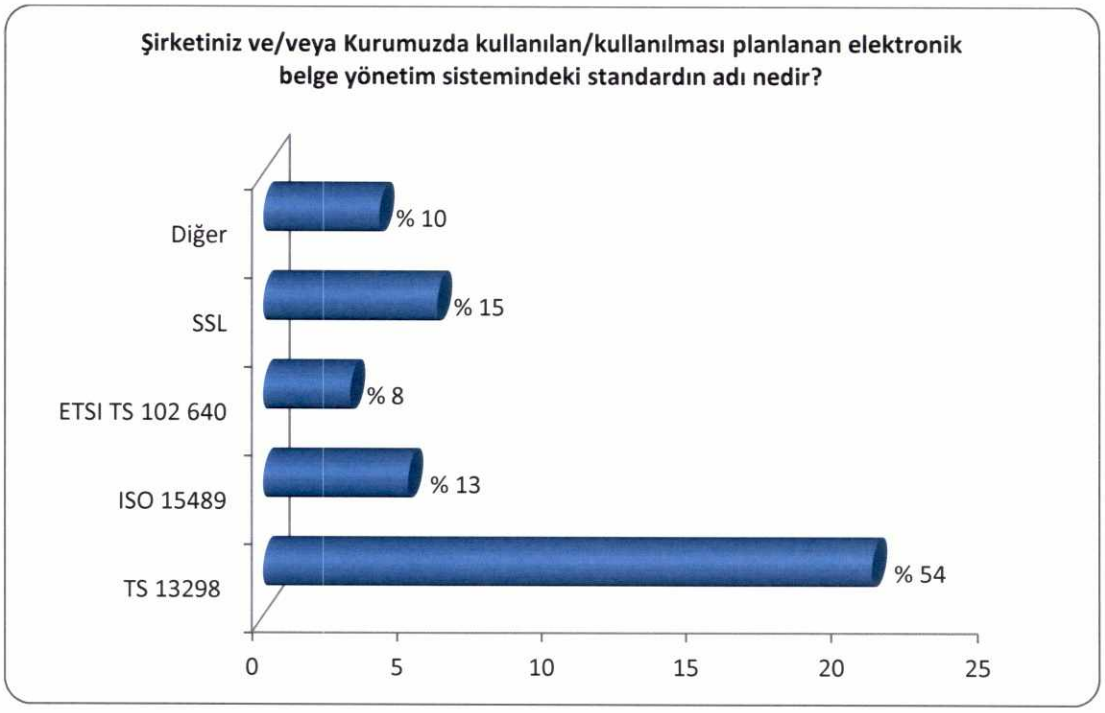
- ✓ Anketin "Şirketiniz ve/veya Kurumuzda kullanılan/kullanılması planlanan EBYS'de herhangi bir standarda uyum sağlanıyor mu?" sorusunda,
  - ✓ "Evet" seçeneği 15 tercihle % 44,
  - ✓ "Hayır" seçeneği 8 tercihle % 24
  - ✓ "Planlanıyor" seçeneği 11 tercihle % 32 olmuştur.

Şekil Ek 0-2 Anketin 3 üncü sorusuna verilen cevapların dağılımı



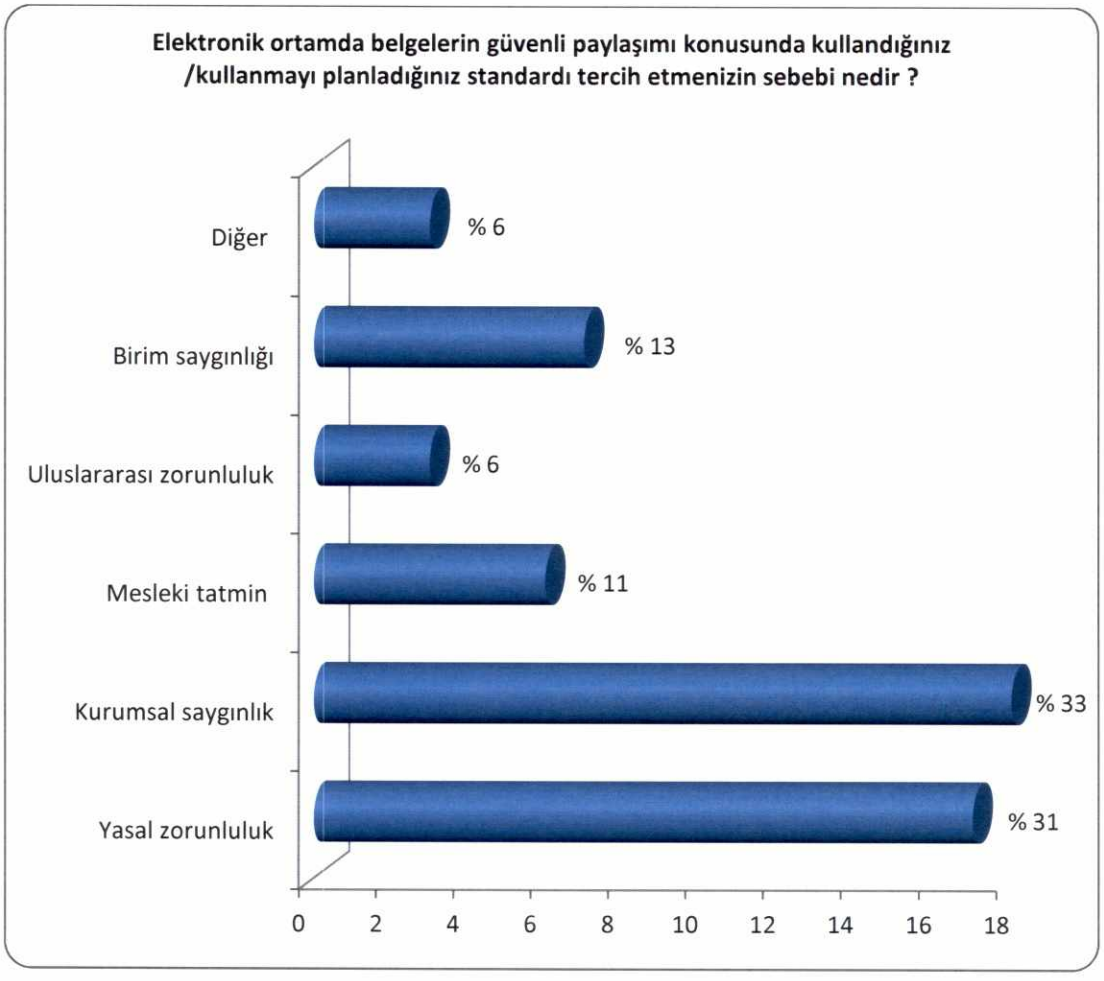
- ✓ Anketin "Şirketiniz ve/veya Kurumuzda kullanılan/kullanılması planlanan EBYS'deki standardın adı nedir?" sorusunda,
  - ✓ "TS 13298" seçeneği 21 tercihle % 54,
  - ✓ " ISO 15489" seçeneği 5 tercihle %13,
  - ✓ "ETSI TS 102 640" seçeneği 3 tercihle % 8,
  - ✓ "SSL" seçeneği 6 tercihle % 15
  - ✓ "Diğer" seçeneği 4 tercihle % 10 olmuştur.

Şekil Ek 0-3 Anketin 5 inci sorusuna verilen cevapların dağılımı



- ✓ Anketin "e-Ortamda e-belgelerin güvenli paylaşımı konusunda kullandığınız /kullanmayı planladığınız standardı tercih etmenizin sebebi nedir?" sorusunda,
  - ✓ "Yasal zorunluluk" seçeneği 17 tercihle % 31,
  - ✓ "Kurumsal saygınlık" seçeneği 18 tercihle % 33,
  - ✓ "Mesleki tatmin" seçeneği 6 tercihle % 11,
  - ✓ "Uluslararası zorunluluk" seçeneği 3 tercihle % 6,
  - ✓ "Birim saygınlığı" seçeneği 7 tercihle % 13,
  - ✓ "Diğer" seçeneği 3 tercihle % 6 olmuştur.

Şekil Ek 6-4 Anketin 6 ncı sorusuna verilen cevapların dağılımı



- ✓ Kurumunuz ve/veya şirketinizde e-ortamda oluşturulan belgelerin hangi taraflar arasında paylaşımına ihtiyaç duyuyorsunuz? Anket sorusunda sıralanan seçenekler arasında 1'den 5'e kadar bir tercihte bulunmaları istenmiş olup,

  - ✓ "Sadece Kurumunuz ve/veya şirketinizin içinde" şıkkında "1. Tercih" 20 seçim, "2. Tercih" 2 seçim, "3 ve 4 tercihler" 0, "5 tercih" ise 5 seçim.

  - ✓ "Kurumunuz ve/veya şirketiniz ile diğer kamu kurumları arasındaki işlemlerde" şıkkında "1. Tercih" 1 seçim, "2. Tercih" 14 seçim, "3. Tercih" 2 seçim, "4. Tercih" 4 seçim, "5. Tercih" 3 seçim.

  - ✓ "Kurumunuz ve/veya şirketiniz ile özel sektörden kuruluşlar arasındaki işlemlerde" şıkkında "1. Tercih" 1 seçim, "2. Tercih" 4 seçim, "3. Tercih" 6 seçim, "4. Tercih" 9 seçim, "5. Tercih" 5 seçim.

  - ✓ "Kurumunuz ve/veya şirketiniz ile vatandaşlar arasındaki işlemlerde" şıkkında "1. Tercih" boş, "2. Tercih" 1 seçim, "3. Tercih" 15 seçim, "4. Tercih" 5 seçim, "5. Tercih" 4 seçim.

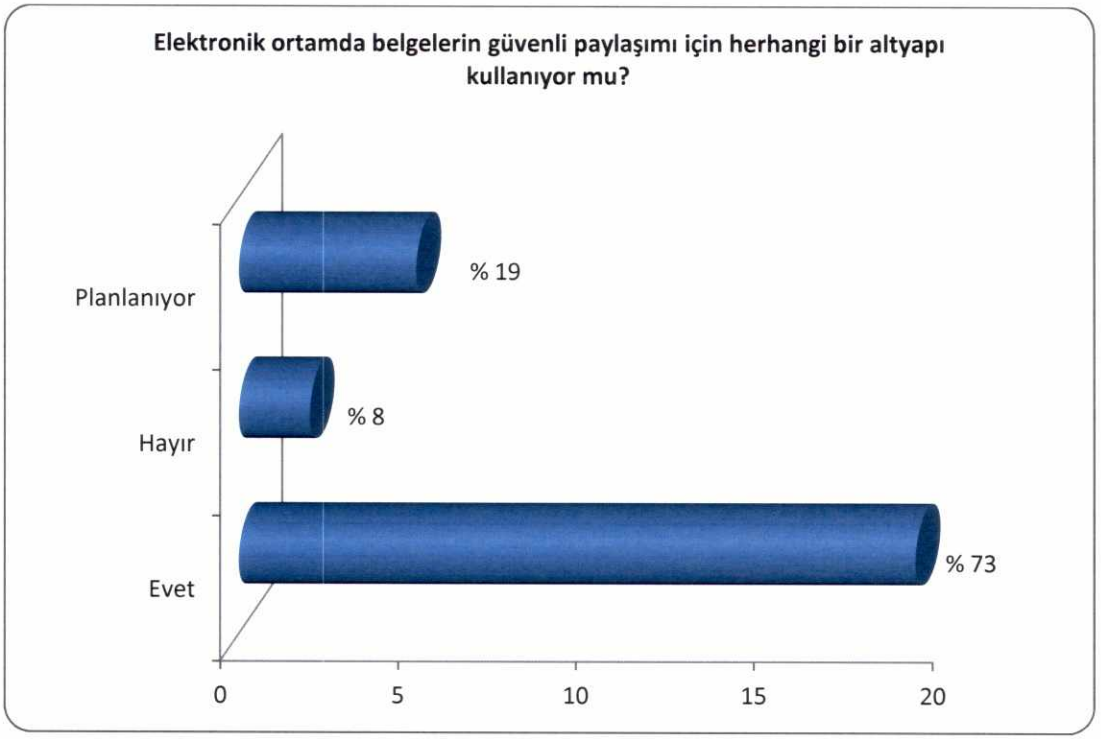
  - ✓ "Kurumunuz ve/veya şirketiniz ile uluslararası kurum/kuruluş/şirketler arasında" şıkkında "1. Tercih" boş, "2. Tercih" 1 seçim, "3. Tercih" 1 seçim, "4. Tercih" 4 seçim, "5. Tercih" 18 seçim oluştur.

Tablo Ek 0.1 Anketin 7 nci sorusuna verilen cevapların dağılımı

Kurumunuz ve/veya şirketinizde e-ortamda oluşturulan e-belgelerin hangi taraflar arasında paylaşımına ihtiyaç duyuyorsunuz? (Lütfen aşağıdaki yanıtları öncelik sırasına göre numaralandırınız)	**1**	**2**	**3**	**4**	**5**
Sadece Kurumunuz ve/veya şirketinizin içinde	20	2			5
Kurumunuz ve/veya şirketiniz ile diğer kamu kurumları arasındaki işlemlerde	1	14	2	4	3
Kurumunuz ve/veya şirketiniz ile özel sektörden kuruluşlar arasındaki işlemlerde	1	4	6	9	5
Kurumunuz ve/veya şirketiniz ile vatandaşlar arasındaki işlemlerde		1	15	5	4
Kurumunuz ve/veya şirketiniz ile uluslararası kurum/kuruluş/şirketler arasında		1	1	4	18

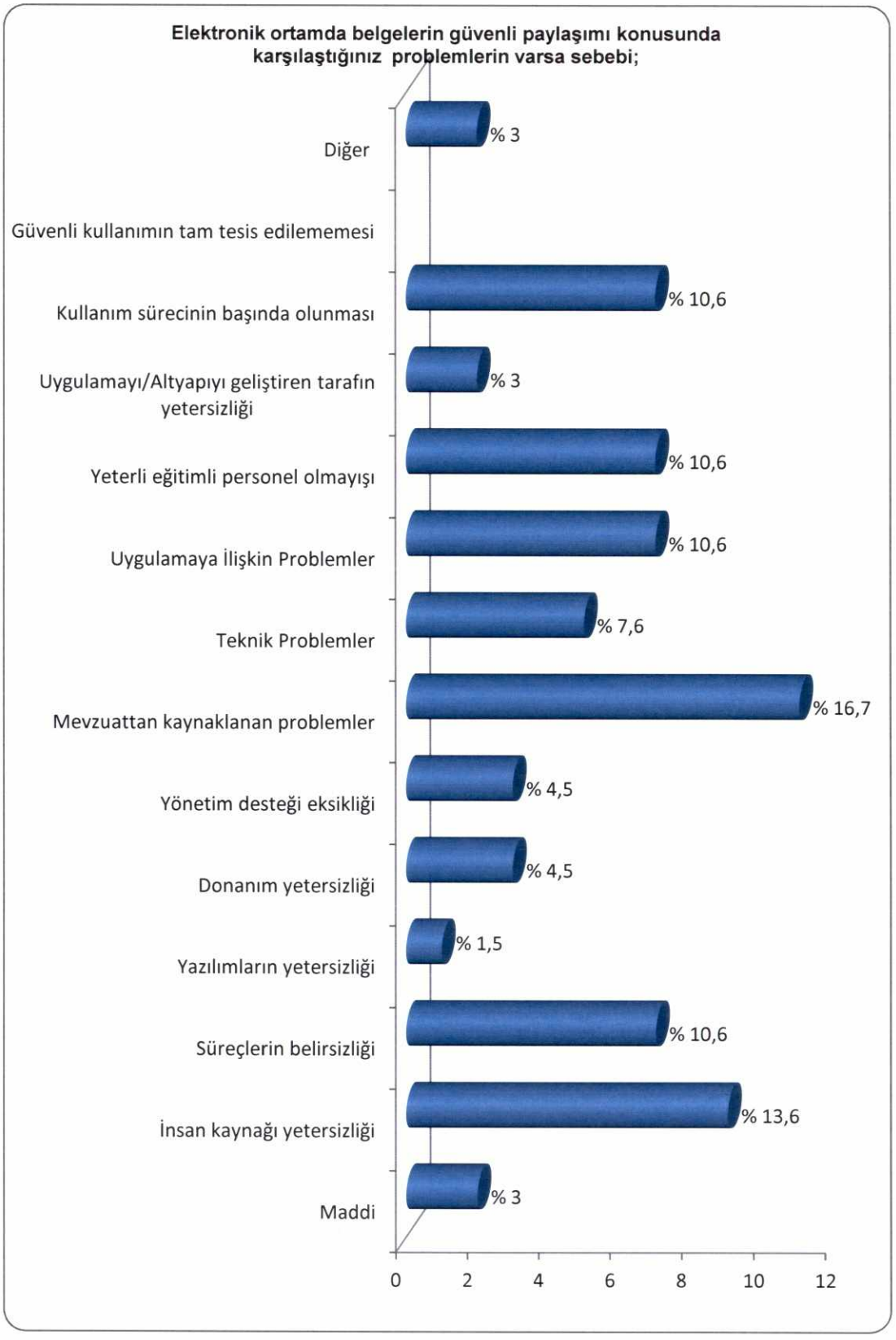
- ✓ Anketin "e-Ortamda e-belgelerin güvenli paylaşımı için herhangi bir altyapı kullanıyor mu?" sorusunda,
  - ✓ "Evet" seçeneği 19 tercihle % 73,
  - ✓ "Hayır" seçeneği 2 tercihle %8,
  - ✓ "Planlanıyor" seçeneği ise 5 tercihle % 19 olmuştur.

Şekil Ek 0-5 Anketin 8 inci sorusuna verilen cevapların dağılımı



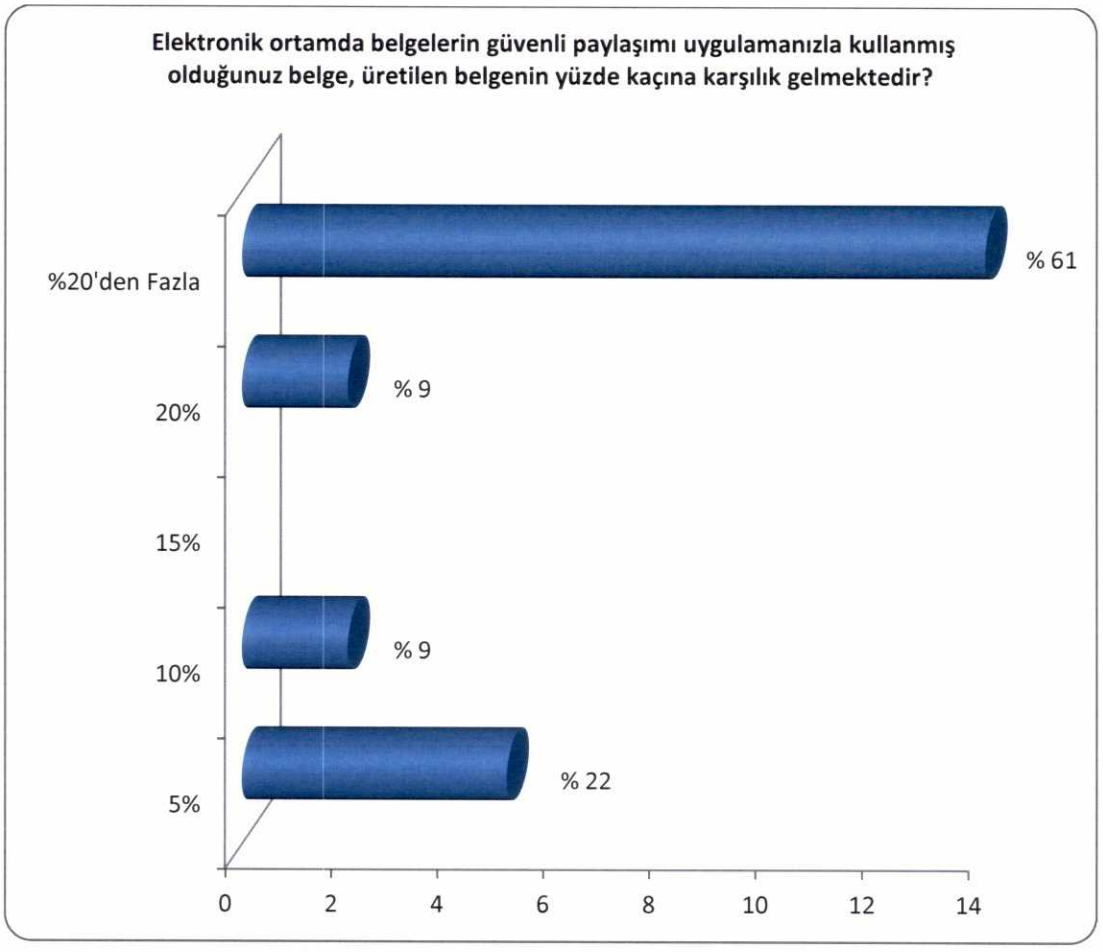
- ✓ Anketin "e-Ortamda e-belgelerin güvenli paylaşımı konusunda karşılaştığınız problemlerin varsa sebebi" sorusunda,
  - ✓ "Maddi" seçeneği 2 tercihle % 3,
  - ✓ "İnsan kaynağı yetersizliği" seçeneği 9 tercihle % 14,
  - ✓ "Süreçlerin belirsizliği" seçeneği 7 tercihle % 11,
  - ✓ "Yazılımların yetersizliği" seçeneği 1 tercihle % 1,
  - ✓ "Donanım yetersizliği" seçeneği 3 tercihle % 4,
  - ✓ "Yönetim desteği eksikliği" 3 tercihle % 4,
  - ✓ "Mevzuattan kaynaklanan problemler" seçeneği 11 tercihle % 17,
  - ✓ "Teknik Problemler " seçeneği 5 tercihle % 7,
  - ✓ "Uygulamaya İlişkin Problemler" seçeneği 7 tercihle % 11,
  - ✓ "Yeterli eğitimli personel olmayışı" seçeneği 7 tercihle % 11,
  - ✓ "Uygulamayı/Altyapıyı geliştiren tarafın yetersizliği" seçeneği 2 tercihle % 3,
  - ✓ "Kullanım sürecinin başında olunması" seçeneği 7 tercihle % 11,
  - ✓ "Güvenli kullanımın tam tesis edilememesi" seçeneği boş,
  - ✓ "Diğer" seçeneği 2 tercihle % 3 olmuştur.

Şekil Ek 0-6 Anketin 11 inci sorusuna verilen cevapların dağılımı



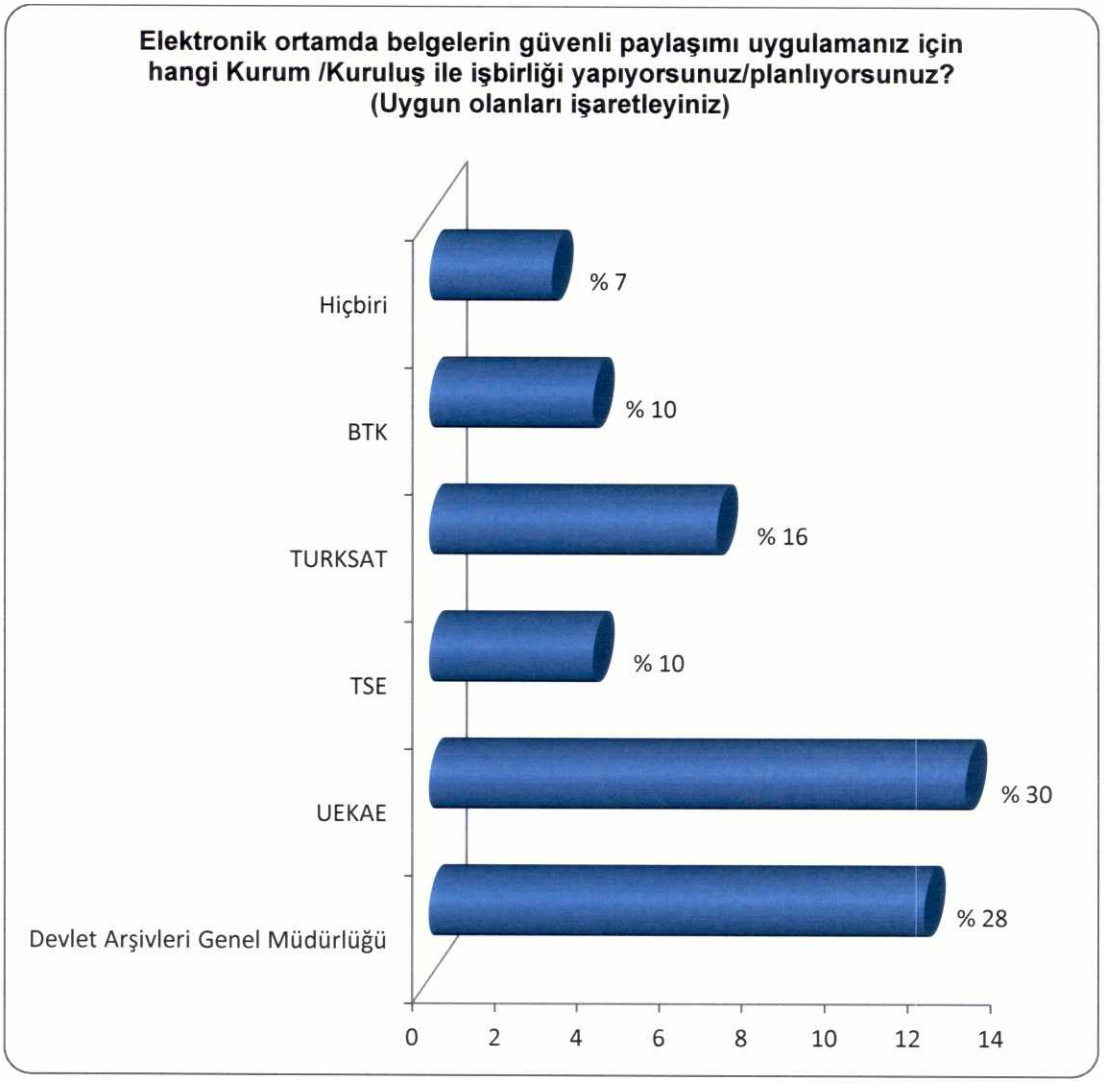
- ✓ Anketin "e-Ortamda e-belgelerin güvenli paylaşımı uygulamanızla kullanmış olduğunuz belge, üretilen belgenin yüzde kaçına karşılık gelmektedir?" sorusunda,
  - ✓ "% 5" seçeneği 5 tercihle % 22,
  - ✓ "% 10" seçeneği 2 tercihle % 8,
  - ✓ "% 15" seçeneği 0,
  - ✓ "% 20" seçeneği 2 tercihle % 8,
  - ✓ "% 20" den fazla seçeneği 14 tercihle % 61 olmuştur.

Şekil Ek 0-7 Anketin 12 nci sorusuna verilen cevapların dağılımı



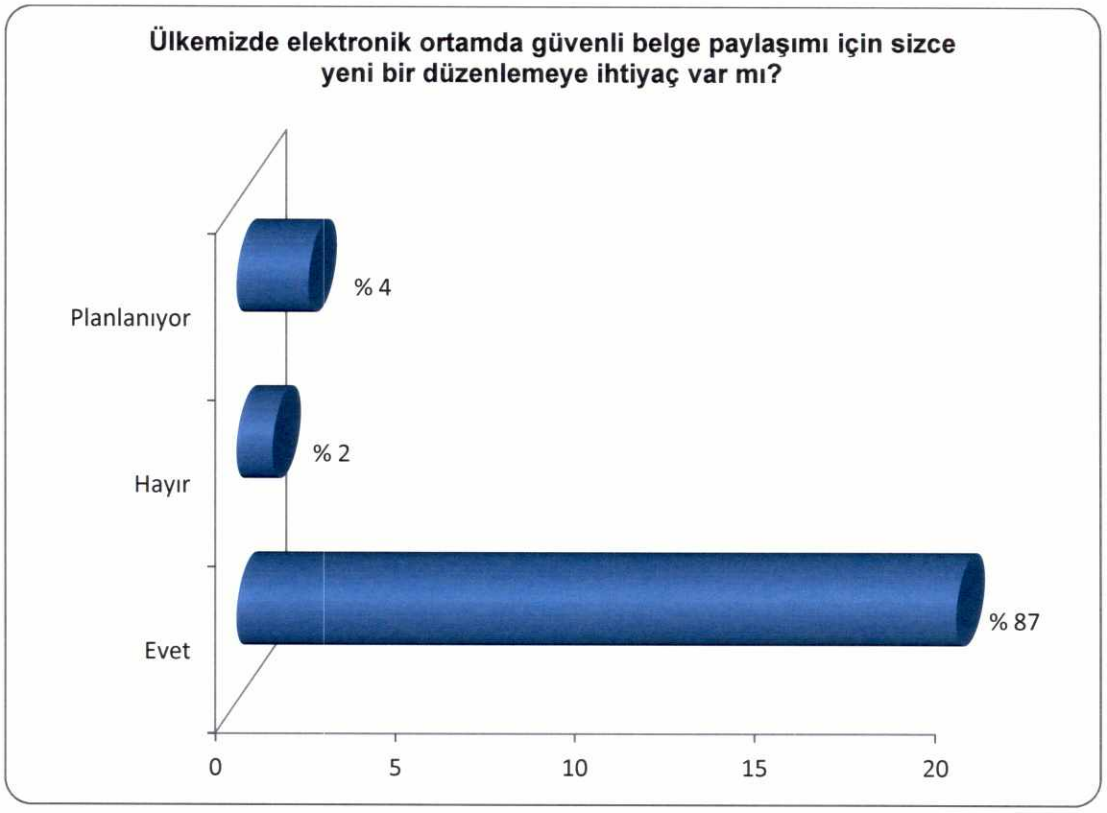
- ✓ Anketin "e-Ortamda e-belgelerin güvenli paylaşımı uygulamanız için hangi Kurum /Kuruluş ile işbirliği yapıyorsunuz/planlıyorsunuz? (Uygun olanları işaretleyiniz)" sorusunda,
  - ✓ "Devlet Arşivleri Genel Müdürlüğü" seçeneği 12 tercihle % 28,
  - ✓ "UEKAE" seçeneği 13 tercihle % 30,
  - ✓ "TS" seçeneği 4 tercihle % 10,
  - ✓ "TURKSAT" seçeneği 7 tercihle % 16,
  - ✓ "BTK" seçeneği 4 tercihle % 10,
  - ✓ "Hiçbiri" seçeneği 3 tercihle % 7 olmuştur.

Şekil Ek 0-8 Anketin 13 üncü sorusuna verilen cevapların dağılımı



- ✓ Anketin "Ülkemizde e-ortamda güvenli e-belge paylaşımı için sizce yeni bir düzenlemeye ihtiyaç var mı?" sorusunda,
  - ✓ "Evet" seçeneği 20 tercihle % 87,
  - ✓ "Hayır" seçeneği 1 tercihle % 4,
  - ✓ "Planlanıyor" seçeneği 2 tercihle % 9 olmuştur.

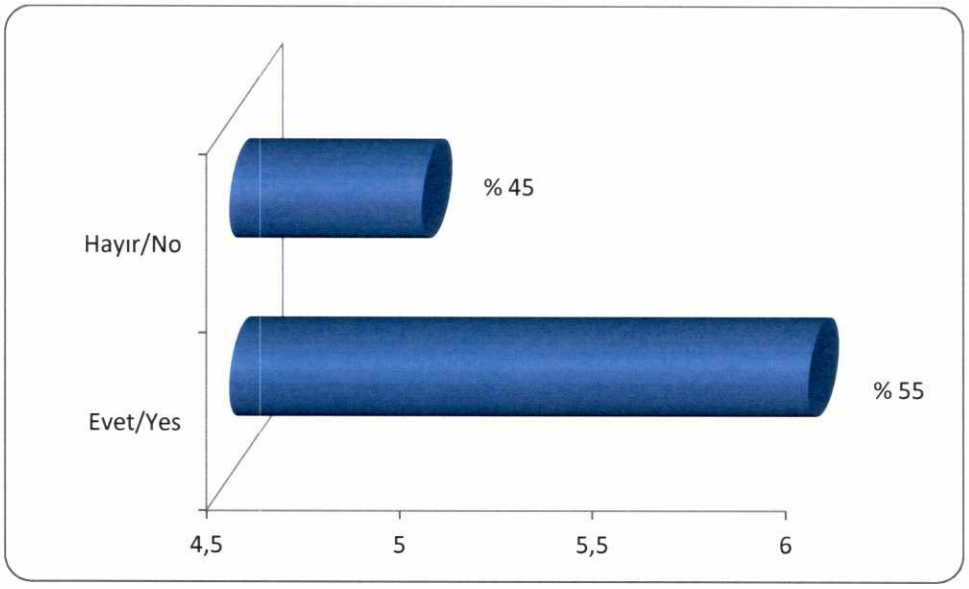
Şekil Ek 0-9 Anketin 14 üncü sorusuna verilen cevapların dağılımı



Yurt Dışı Anket Sonuçları ve Yorumlanması

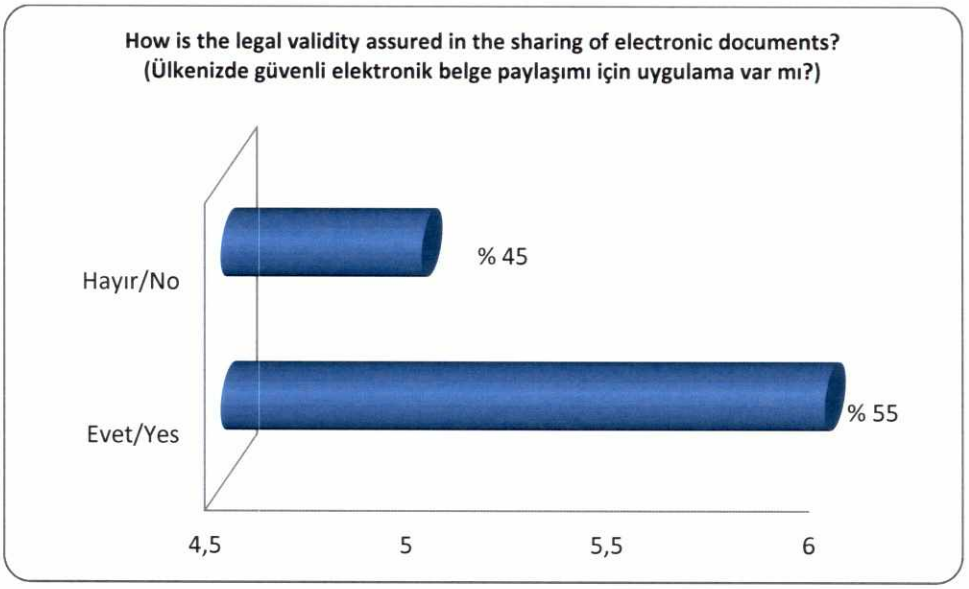
- ✓ Anketin "İşyerinizde güvenli e-belge paylaşımı uygulaması kullanıyor musunuz?" sorusunda,
  - ✓ "Evet" seçeneği 6 terhcihle % 55,
  - ✓ "Hayır" seçeneği 5 tercihle %45 olmuştur.

Şekil Ek 0-10 Anketin 1 inci sorusuna verilen cevapların dağılımı



- ✓ Anketin "Ülkenizde güvenli e-belge paylaşımı için uygulama var mı?" sorusunda,
  - ✓ "Evet" seçeneği 6 terhcihle % 55,
  - ✓ "Hayır" seçeneği 5 tercihle %45 olmuştur.

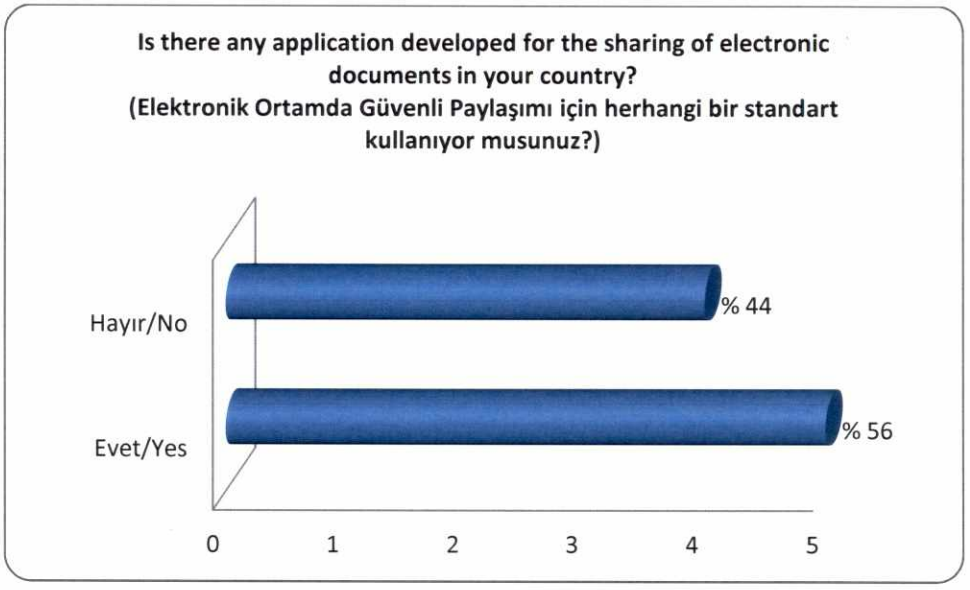
Şekil Ek 0-11 Anketin 2 nci sorusuna verilen cevapların dağılımı



✓ Anketin "e-Ortamda e-belgenin güvenli paylaşımı için herhangi bir standart kullanıyor musunuz?" sorusunda,

- ✓ "Evet" seçeneği 5 terhcihle % 56,
- ✓ "Hayır" seçeneği 4 tercihle %44 olmuştur.

Şekil Ek 0-12 Anketin 3 üncü sorusuna verilen cevapların dağılımı



- ✓ Anketin "Kurumunuz ve/veya şirketinizde e-ortamda oluşturulan e-belgelerin hangi taraflar arasında paylaşımına ihtiyaç duyuyorsunuz? (Lütfen aşağıdaki yanıtları öncelik sırasına göre numaralandırınız)" sorusunda,
  - ✓ "Sadece Kurumunuz ve/veya şirketinizin içinde" şıkkında "1 seçeneği" 3 tercih, "2 seçeneği" 2 tercih, "3 seçeneği" 1 tercih, "4 seçeneği" 0 tercih, "5 seçeneği" 2 tercih,
  - ✓ "Kurumunuz ve/veya şirketiniz ile diğer kamu kurumları arasındaki işlemlerde" şıkkında "1 seçeneği" 4 tercih, "2 seçeneği" 0 tercih, "3 seçeneği" 2 tercih, "4 seçeneği" 2 tercih, "5 seçeneği" 0 tercih,
  - ✓ "Kurumunuz ve/veya şirketiniz ile özel sektörden kuruluşlar arasındaki işlemlerde" şıkkında "1 seçeneği" 2 tercih, "2 seçeneği" 1 tercih, "3 seçeneği" 3 tercih, "4 seçeneği" 1 tercih, "5 seçeneği" 1 tercih,
  - ✓ "Kurumunuz ve/veya şirketiniz ile vatandaşlar arasındaki işlemlerde" şıkkında "1 seçeneği" 2 tercih, "2 seçeneği" 2 tercih, "3 seçeneği" 1 tercih, "4 seçeneği" 2 tercih, "5 seçeneği" 1 tercih,
  - ✓ "Kurumunuz ve/veya şirketiniz ile uluslararası kurum/kuruluş/şirketler arasında" şıkkında "1 seçeneği" 2 tercih, "2 seçeneği" 0 tercih, "3 seçeneği" 1 tercih, "4 seçeneği" 4 tercih, "5 seçeneği" 1 tercih olmuştur.

Tablo Ek 0.2 Anketin 5 inci sorusuna verilen cevapların dağılımı

Kurumunuz ve/veya şirketinizde e-ortamda oluşturulan belgelerin hangi taraflar arasında paylaşımına ihtiyaç duyuyorsunuz? (Lütfen aşağıdaki yanıtları öncelik sırasına göre numaralandırınız)	**1**	**2**	**3**	**4**	**5**
Sadece Kurumunuz ve/veya şirketinizin içinde	3	2	1	0	2
Kurumunuz ve/veya şirketiniz ile diğer kamu kurumları arasındaki işlemlerde	4	0	2	2	0
Kurumunuz ve/veya şirketiniz ile özel sektörden kuruluşlar arasındaki işlemlerde	2	1	3	1	1
Kurumunuz ve/veya şirketiniz ile vatandaşlar arasındaki işlemlerde	2	2	1	2	1
Kurumunuz ve/veya şirketiniz ile uluslararası kurum/kuruluş/şirketler arasında	2	0	1	4	1

Yurt içi bulgu ve yorumlar

- ✓ Katılımcılardan %49 unun EBYS kullanıyor ve %27 sinin kullanmayı planlıyor olması, önemli bir oran olsa da iş ve işlemlerin e-ortama aktarım artış hızı dikkate alındığında geriye kalan % 24 lük oranın en azından birlikte çalışabilirlik açısından ülke çapında uygulanacak güvenli e-belge paylaşımını aksatacak önemli bir oran olduğu açıktır (Şekil Ek 6-1).

- ✓ Katılımcıların kurumlarındaki e-belge yönetiminde belli bir standarda uyum sağlayıp sağlamadıkları sorusuna verilen cevaplarda, kullananların %44, kullanmayı planlayanların ise %32 oranında olması olumlu bir durumdur (Şekil Ek 6-2). Ancak geriye kalan %24 lük kısmın kullanmaması veya kullanmayı planlamıyor olması ileride muhtemel birlikte çalışabilirlik problemlerinin yaşanacağının göstergesidir.

- ✓ Anket katılımcılarından EBYS kullanıcılarının % 54 oranında TS 13298 standardını tercih etmiş olması, söz konusu standardı ülkemiz için önemli kılmaktadır (Şekil Ek 6-3).

- ✓ Ülkemiz kullanıcılarının, e-ortamda e-belgelerin güvenli paylaşılması konusunda kullandıkları veya kullanmayı planladıkları standardı tercih etmelerinin nedenlerine bakıldığında, kurumsal saygınlık %33 ile birinci sırada yer alırken, yasal zorunluluk ise %31 ile ikinci sırayı almıştır. (Şekil Ek 6-4). Bununla birlikte gerek resmi yazışmaların paylaşımında, gerekse özel sektörün iş ve işlemlerinde asıl dikkat edilmesi gereken hususun kurumsal saygınlıktan ziyade yasal zorunlulukların doğuracağı hukuki sonuçların olabileceği değerlendirilmektedir. Bu soruyu cevaplayan katılımcılardan "hayır" seçeneğini işaretleyenlerin devam etmeleri istenmemesine rağmen yapılan inceleme neticesinde tüm katılımcıların tüm sorulara cevap verdiği anlaşılmış ve verilen cevapların değerlendirilmesi neticesinde elde edilen bulguların anlamlı görülmesi nedeniyle tüm cevaplar değerlendirmeye alınmıştır.

- ✓ Kullanıcıların e-ortamda oluşturdukları e-belgelerin sadece kendi kuruluşları içerisinde paylaşımı konusu ilk tercihleri olarak yer almasına karşın, diğer kamu kurum ve kuruluşları ile e-belge paylaşımı konusundaki tercihleri ikinci sırada yer almaktadır. Bu durumda kamu kurum ve kuruluşlarının e-ortamda iş ve işlem yapma konusunda sürükleyici bir rol üstlendiği değerlendirilmektedir (Tablo Ek 6-1).

- ✓ Anket katılımcılarından e-ortamda e-belgelerin güvenli paylaşımı için herhangi bir altyapı (e-imza gibi) kullananların oranı %73 olarak ortaya çıkarken kullanmayı planlayanlar ise %19 dur. Toplamda %92 gibi oldukça yüksek bir orana ulaşmış olması güvenlik konusundaki farkındalığın oldukça yüksek olduğuna işaret etmektedir (Şekil Ek 6-5).

- ✓ Ankette e-ortamda e-belgelerin güvenli paylaşımı konusunda karşılaşılan en büyük engel olarak birinci sırada %17 gibi bir oranla mevzuattan kaynaklanan problemlerin işaretlenmiştir (Şekil Ek 6-6). Ancak anketin yapıldığı tarihten sonra ülkemizde belirli bir mevzuat altyapısı oluşmuş ve 6102 sayılı Türk Ticaret Kanunu'nun 1525 inci maddesi kapsamında BTK tarafından, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 25/08/2011 tarihinde, Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, 16/05/2012 tarihinde, Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul Esaslar ve 06/06/2012 tarih ve 2012DK-15259 sayılı Kurul Kararı ile yayımlanmıştır. Böylece e-belgelerin e-ortamda güvenli ve hukuki geçerliliğe sahip bir şekilde paylaşımına ilişkin ülkemizde ihtiyaç duyulan mevzuat altyapısı tamamlanmıştır.

- ✓ Anket katılımcıları, kurumlarında üretilen e-belgelerin % 61 ini, e-ortamda güvenli e-belge olarak paylaştıklarını ifade etmektedir. Bu durum, e-belgelerin güvenli paylaşımındaki artışın, bu artışa paralel güvenliğin önemini ortaya koymaktadır (Şekil Ek 6-7).
- ✓ Anket katılımcıları tarafından e-ortamda e-belgelerin güvenli paylaşımı için işbirliği yapılan ikinci kuruluş olarak Devlet Arşivleri Genel Müdürlüğü'nün %28 gibi bir oranda tercih edilmesi bu kuruluşa önemli bir görev yüklemektedir (Şekil Ek 6-8).
- ✓ Anket verilerine göre katılımcıların % 87 si ülkemizde e-ortamda güvenli e-belge paylaşımı için yeni bir düzenlemeye ihtiyaç duyduklarını ifade etmektedir (Şekil Ek 6-9). Ancak anketin yapıldığı tarihten sonra ülkemizde ihtiyaç duyulan mevzuat altyapısı yukarıda açıklandığı şekilde tamamlanmıştır.

Yurt dışı bulgu, yorum ve Ülkemiz ile karşılaştırılması

✓ Yurt dışından ankete katılanların %55 i e-ortamda güvenli e-belge paylaştıklarını ifade etmişlerdir (Şekil Ek 6-10). Yurt içinde yapılan ankete katılanlara sorulan "e-ortamda e-belgelerin güvenli paylaşımı için herhangi bir altyapı kullanıyor musunuz" sorusuna verilen cevaplar değerlendirildiğinde %73 oranla "evet" seçildiği tespit edilmiştir (Şekil Ek 6-5). Yurt dışı ve yurt içi katılımcıların "evet" yüzdeleri karşılaştırıldığında ülkemizdeki oranın daha yüksek çıkmış olması olumlu değerlendirilmektedir.

✓ Yurt dışından ankete katılanların %55 i de e-ortamda güvenli e-belge paylaşımı için bir uygulama kullandıklarını beyan etmişlerdir (Şekil Ek 6-11). Benzer bir soru olarak yurt içindeki katılımcılara sorduğumuz "herhangi bir altyapı kullanıyor musunuz" (Şekil Ek 6-5) sorusuna katılımcıların %73 ü evet cevabını vermiş olup bu durumun ülkemizin yurtdışına göre daha iyi seviyede olduğunu göstermesi bakımından olumlu olduğu değerlendirilmektedir.

✓ Yurt dışından ankete katılanların %56 sı, e-ortamda güvenli e-belge paylaşımı için bir standart kullandıklarını ifade etmişlerdir (Şekil Ek 6-12). Aynı soruya yurt içi katılımcılarının verdiği cevaplar incelendiğinde "evet" seçeneğinin %44 olarak gerçekleştiği görülmektedir. Ancak halen planlama aşamasında olduklarını ifade edenlerin oranı olan %32 dikkate alındığında (Şekil Ek 6-2) yakın bir zaman diliminde ülkemizle yurt dışı arasındaki farkın kapanacağı değerlendirilmektedir.

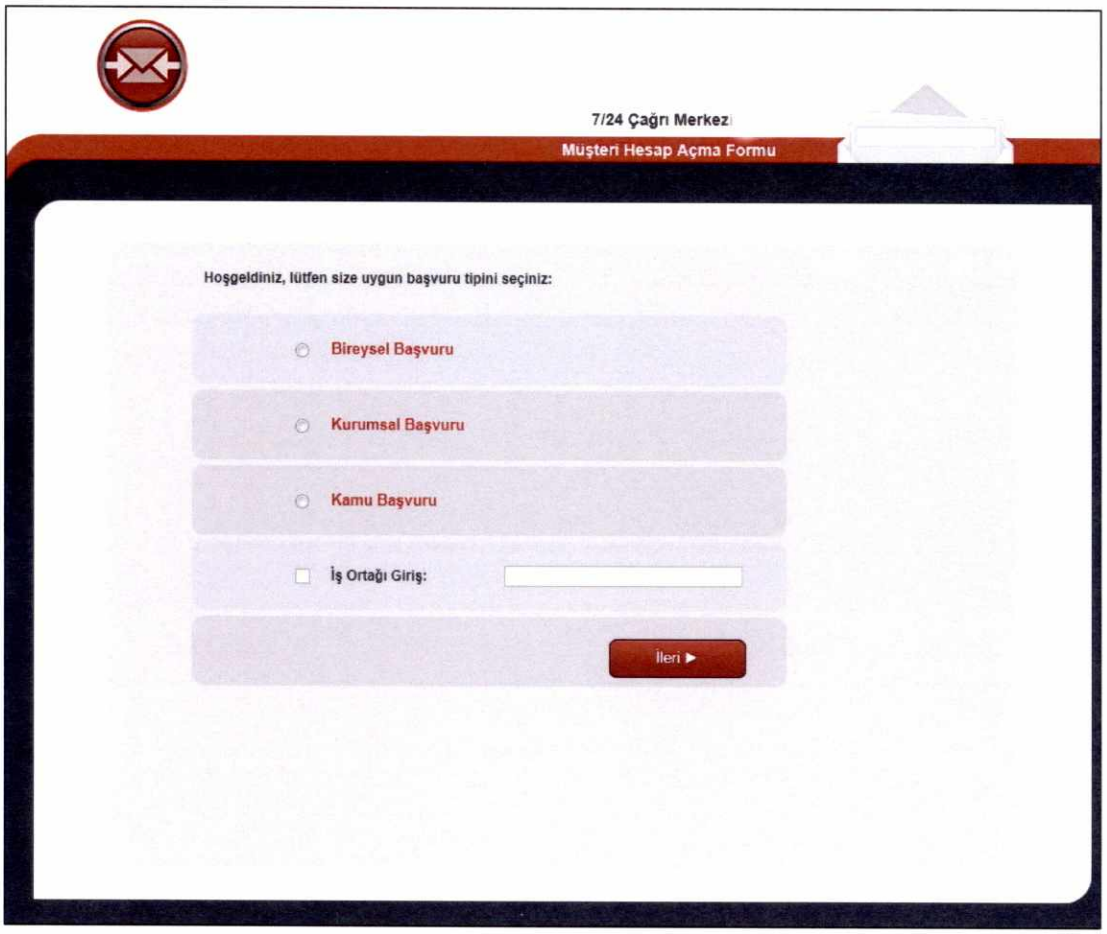
✓ Yurt dışından ankete katılanların söz konusu e-ortamda güvenli e-belge paylaşımında sadece kendi kurumları içinde ve diğer kamu kurumları ile paylaşımları en yüksek tercih olarak işaretlenmiş (Tablo Ek 6-2) olup ülkemiz tercihleri ile (Tablo Ek 6-1) benzerlik taşımaktadır.

Ek 0-6. Pratik KEP işlemlerine ilişkin örnek uygulama

İnternet üzerinden KEP hesabı edinme adımları

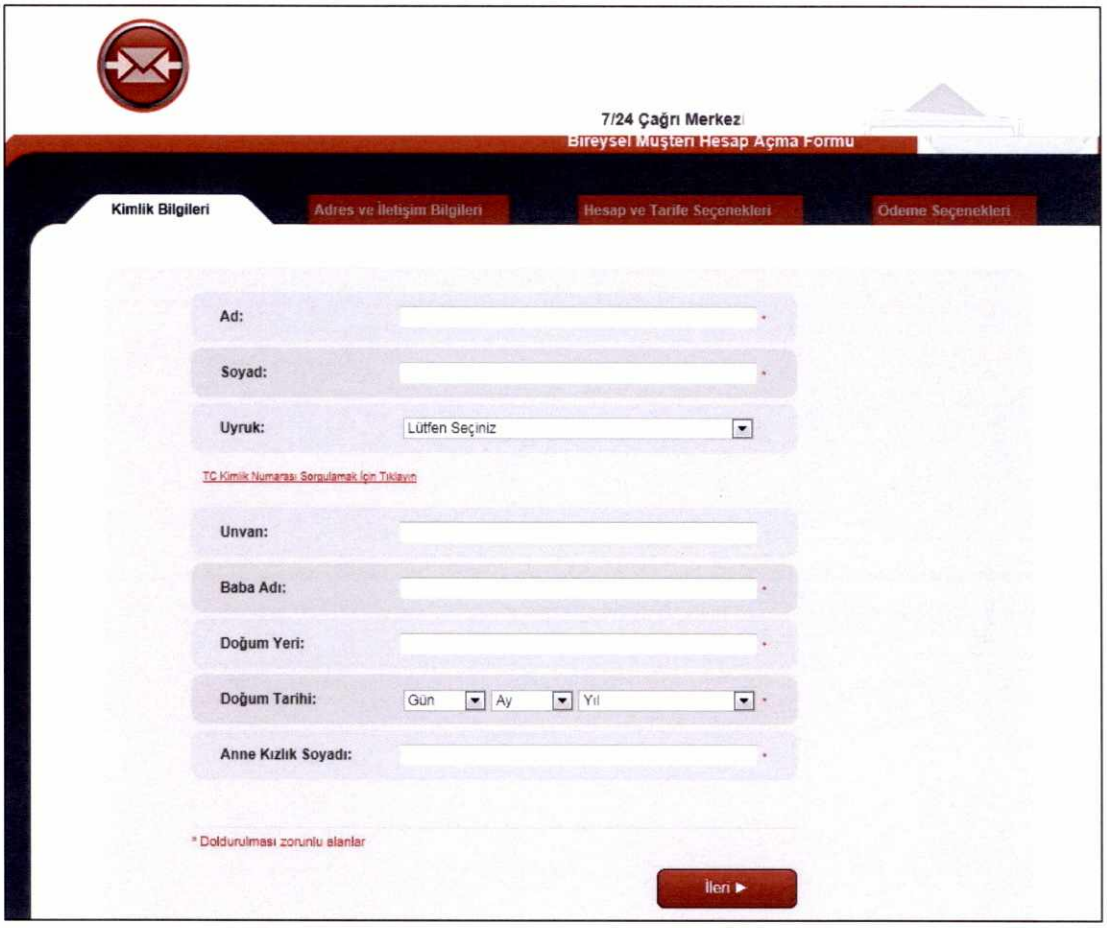
1. İlgili KEPHS'ye ait internet sitesi üzerinden Çevirim içi Başvuru seçeneği sonrası açılan "Müşteri Hesap Açma Formu" penceresi üzerinde bulunan Bireysel Başvuru, Kurumsal Başvuru, Kamu Başvuru ve İş Ortağı Giriş seçeneklerinden duruma uygun olan birinin seçimli yapılır ve "İleri" simgesi ile devam edilir (Şekil Ek 6-13).

Şekil Ek 0-13 KEP Sistemi ilk giriş ekranı görünümü



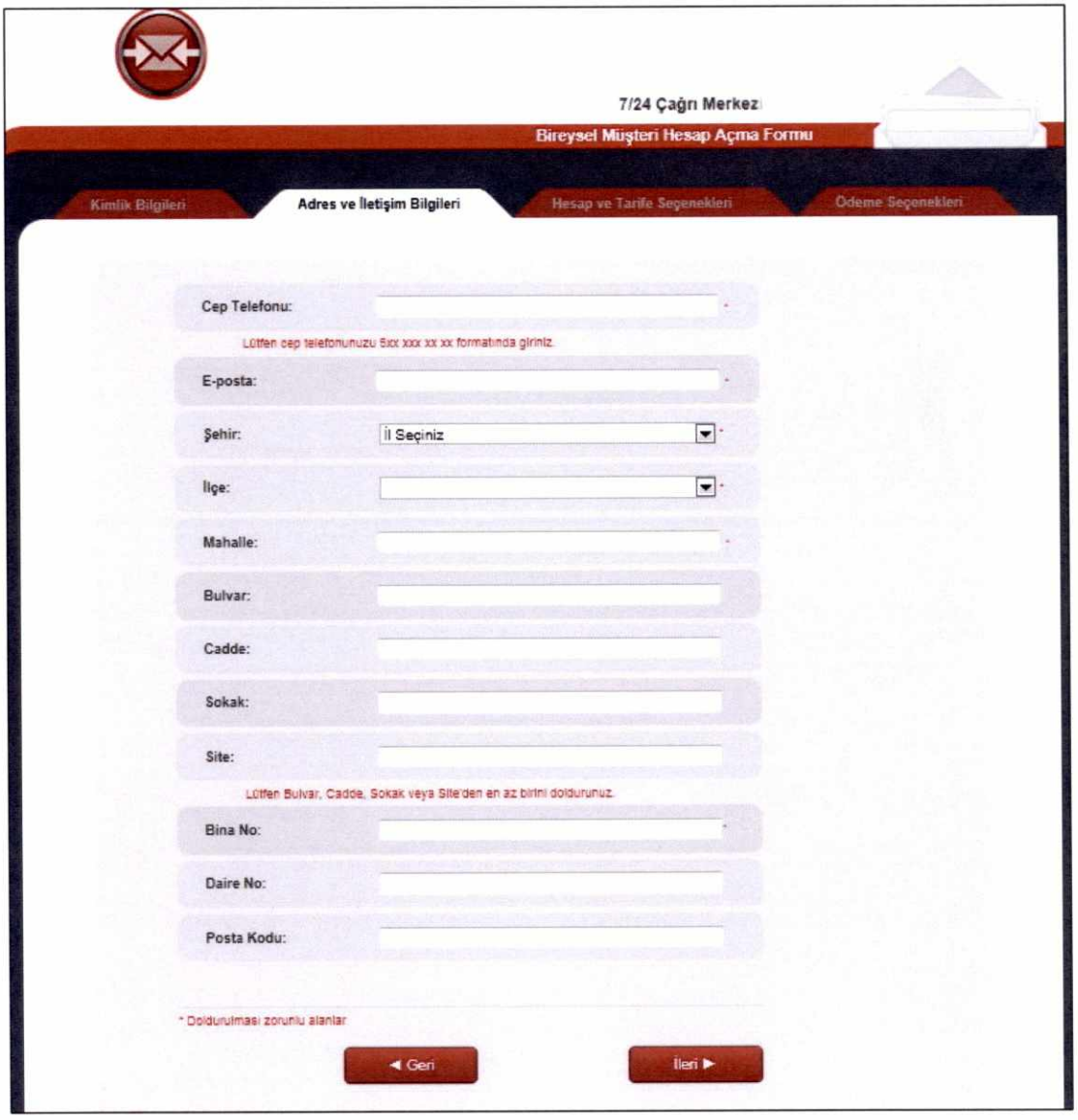
2. "Kimlik Bilgileri" penceresinde kimliğe ilişkin bilgilerin girişi yapılarak "İleri" simgesi ile devam edilir (Şekil Ek 6-14).

Şekil Ek 0-14 KEP Sistemi Kimlik Bilgileri giriş ekranı görünümü



3. "Adres ve İletişim Bilgileri" penceresinde adres, cep telefonu ve e-postaya ilişkin bilgilerin girilmesinin ardından İleri" simgesi ile devam edilir (Şekil Ek 6-15).

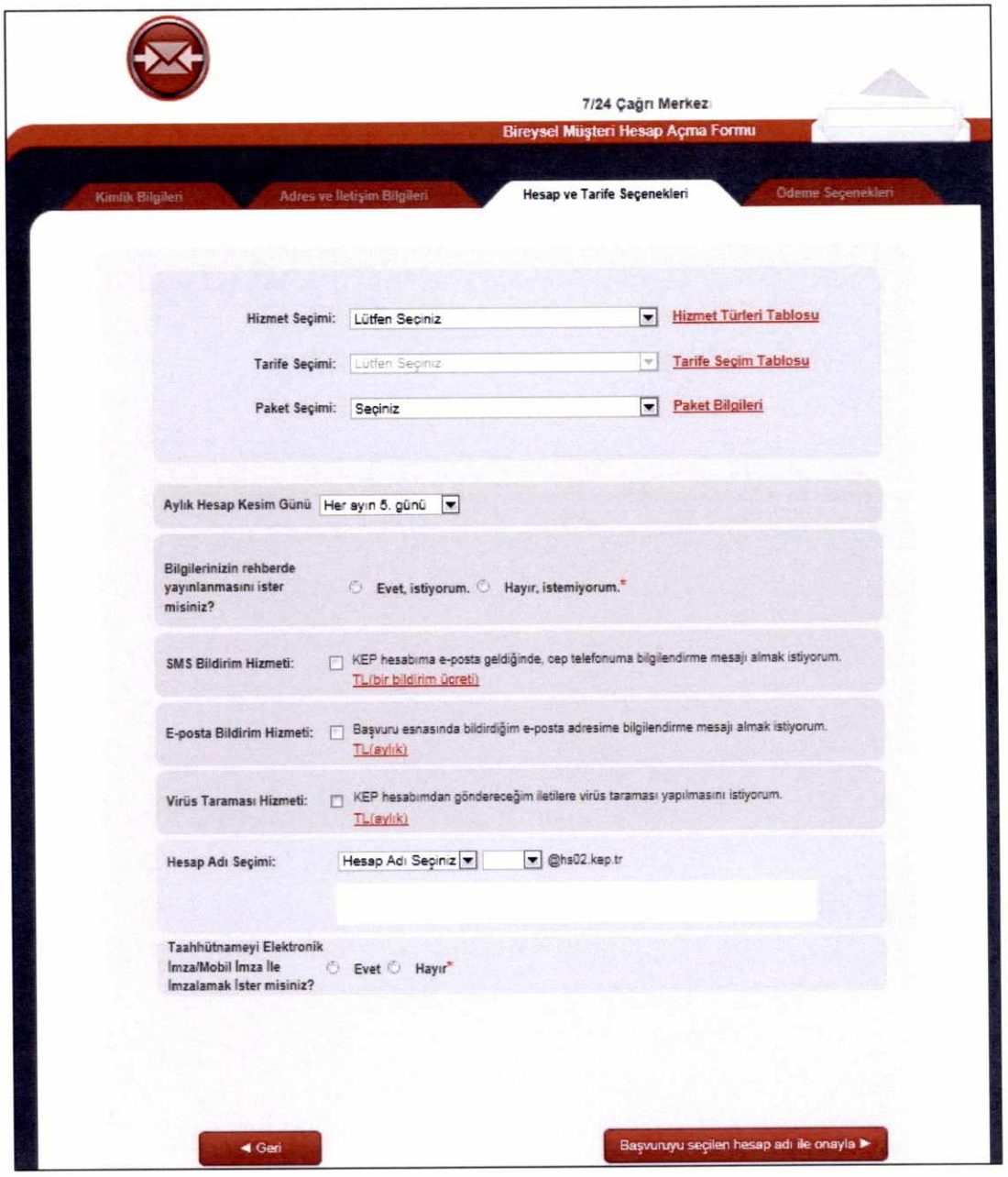
Şekil Ek 0-15 KEP Sistemi Adres ve İletişim Bilgileri ekranı görünümü



4. Adımda bulunan (Şekil 6-16) "Hesap ve Tarife Seçenekleri" penceresinde
   - ✓ "Hizmet Seçim" alanına "Hizmet Türleri Tablosu"ndan, "Gönder Al" veya "Sadece Al" seçeneklerinden bir tanesi seçilir.
   - ✓ "Tarife Seçimi " alanına "Tarife Seçim Tablosu"ndan bir önceki seçime göre; "Gönder Al" seçimi yapılmış ise "Gönder Al Standart", "Sadece Al" seçimi yapılmış ise "KEP Bizden" veya "Sadece Al Standart" seçimi yapılır.
   - ✓ "Aylık Hesap Kesim Günü" alanında bulunan tarihlerden bir tanesinin seçimi yapılır.
   - ✓ "Bilgilerinizin rehberde yayınlanmasını ister misiniz?" sorusuna "Evet" veya "Hayır" seçimi yapılır.
   - ✓ Gelecek olan e-postanın Cep Telefonu ile Ücretli bildirimi için "SMS Bildirim Hizmeti:" tercihi edilebileceği
   - ✓ Başvuru esnasında önceden bildirilen farklı bir e-posta adresine bilgilendirme mesajı almak istenmesi halinde ise "E-posta Bildirim Hizmeti:" seçeneği de yine ücret karşılığı tercih edilebilir.
   - ✓ KEP hesabından gönderilecek iletilere virüs taraması yapılması isteniyor ise
   - ✓ "Virüs Taraması Hizmeti:" seçeneği işaretlenir.
   - ✓ "Hesap Adı Seçimi" seçeneğinde istenilen hesap adı yazılarak
     - o kurumkisaadi@hs02.kep.tr
     - o birimadi@kurumkisadi.hs02.kep.tr
     - o Adi.soyadi@kurumkisadi.hs02.kep.tr
     - o Projeadi@kurumkisadi.hs02.kep.tr
     - o şeklinde KEP hesabının adı belirlenir.
   - ✓ "Taahhütnameyi Elektronik İmza/Mobil İmza İle İmzalamak İster misiniz?" sorusuna ise "Evet" veya "Hayır" tercihlerinden bir tanesi işaretlenir.
   - ✓ Uyarı olarak "KEP hesabının açılması için gerekli belgeleri (tıklayınız), en yakın kimlik doğrulama merkezine (tıklayınız) en geç 7 iş günü içinde ulaştırmanız gerekmektedir. 7 iş günü içinde evrak teslimi ve kimlik doğrulama işlemini tamamlamazsanız, başvurunuz iptal edilecek ve yapacağınız ödeme iade edilmeyecektir. Gerekli belgelerin eksiksiz olarak TNB KEP'e ulaşmasından sonra en geç 3 iş günü içinde KEP hesabınız

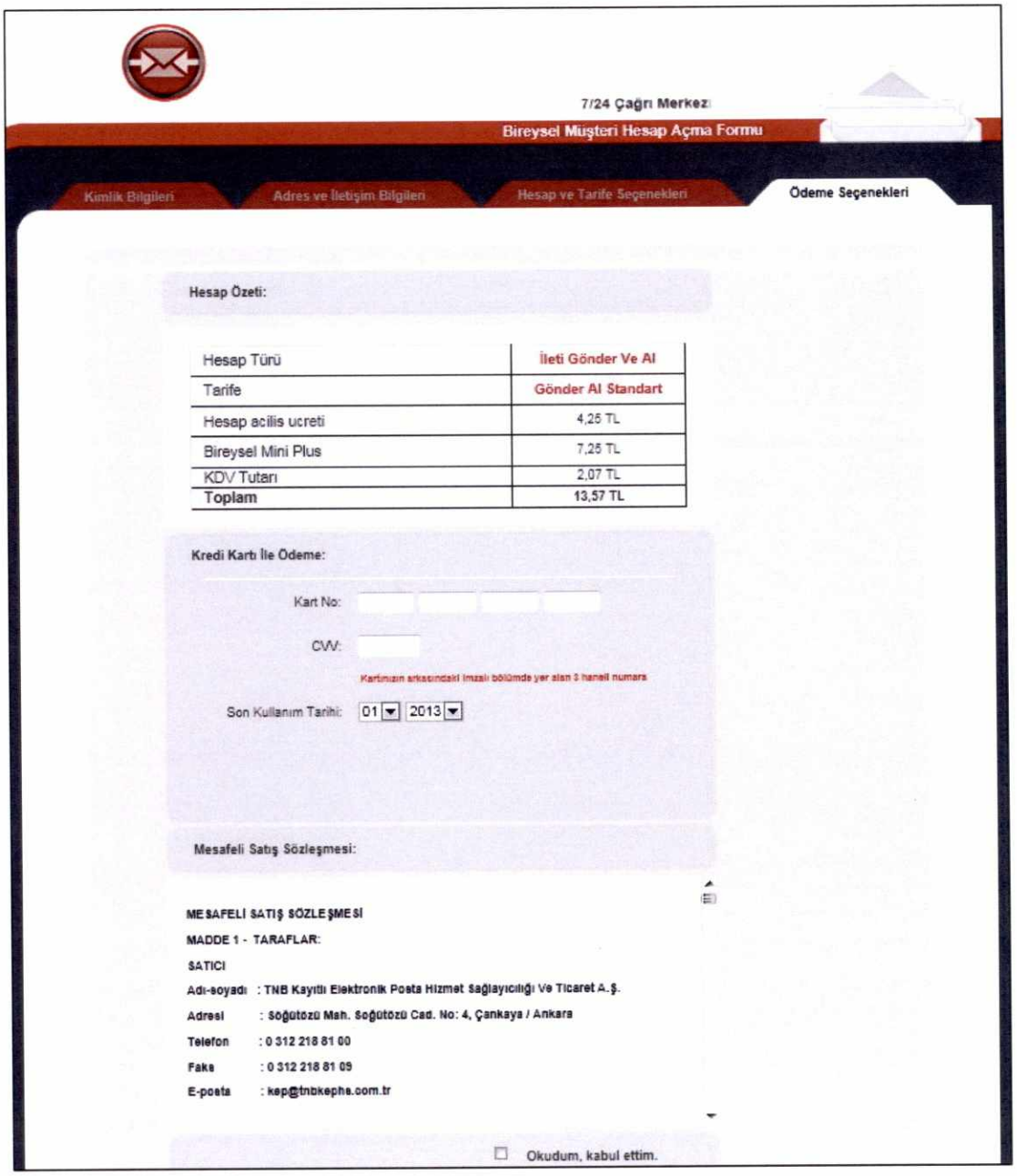
açılacaktır." mesajı ekranda yer almaktadır. Gerekli belgeler ve en yakın kimlik doğrulama merkezi için yukarıda verilen (tıklayınız) adreslerine ulaşılabilir. "İleri" simgesi ile bir sonraki adıma geçilir.

Şekil Ek 0-16 KEP Sistemi Hesap ve Tarife Seçenekleri ekranı görünümü



5. "Ödeme Seçenekleri" penceresinde; ödenecek olan "Hesap özeti tablosu", "Kredi Kartı ile Ödeme" alanı ve "Mesafeli Satış Sözleşmesi" bulunmaktadır. "Mesafeli Satış Sözleşmesi"nin okunup kabul edildiğine dair seçenek işaretlenerek işlem gerçekleştirilmiş olur (Şekil 6-17).

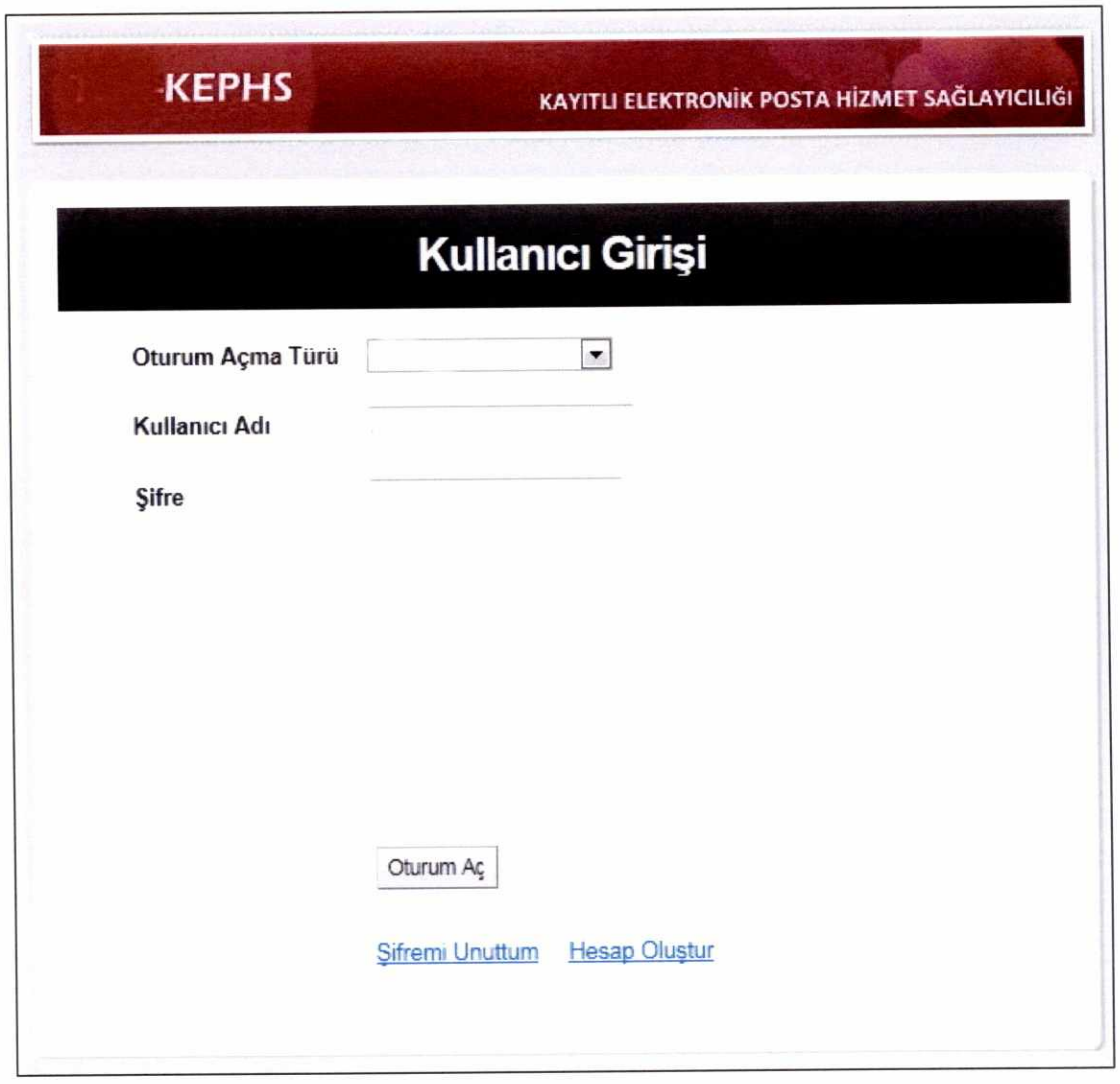
Şekil Ek 0-17 KEP Sistemi Ödeme Seçenekleri ekranı görünümü



Ek 0-7. KEP sistemi ile ileti gönderim işlemleri

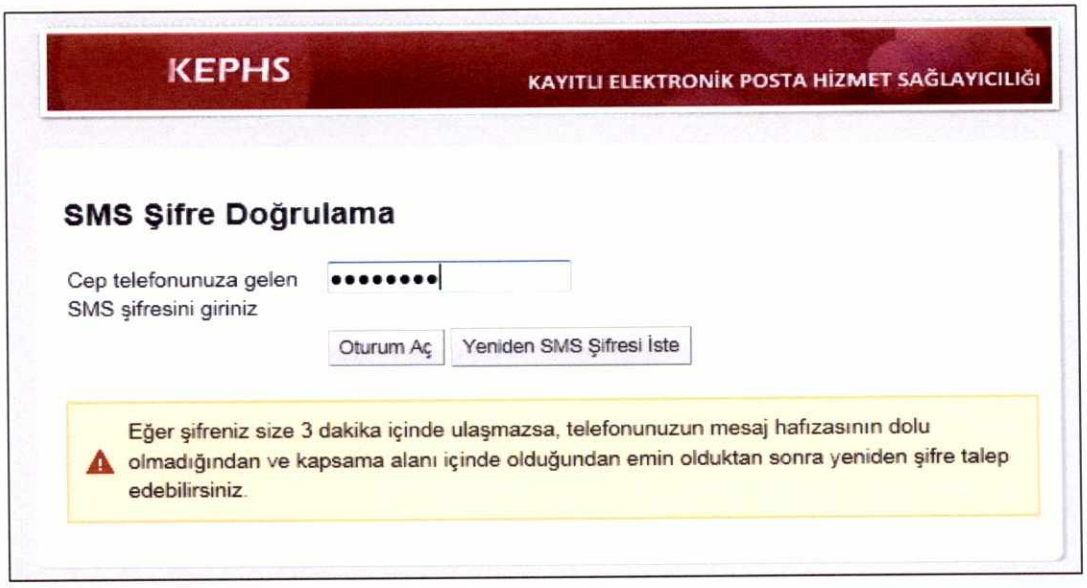
1. Kullanıcının hesabı bulunduğu KEPHS'nin internet sayfasından "KEP Oturumunu Aç" seçeneğinden ulaşılan "Kullanıcı Girişi Sayfası"nda "Oturum Açma Türü" seçeneğinden "SMS Şifre, e-İmza veya Mobil İmza" seçeneklerinden biri seçilir. Kullanıcı Adı, Şifre ve/veya (Kullanıcı Adı veya Şifrenin yanlış girilmesi halinde, yeniden Kullanıcı Girişi işlemi için) Doğrulama kodu girişi sonrası "Oturum Aç" simgesine tıklanarak bir sonraki adıma geçilir (Şekil Ek 6-18).

Şekil Ek 0-18 KEP Sistemi Kullanıcı Girişi ekranı görünümü



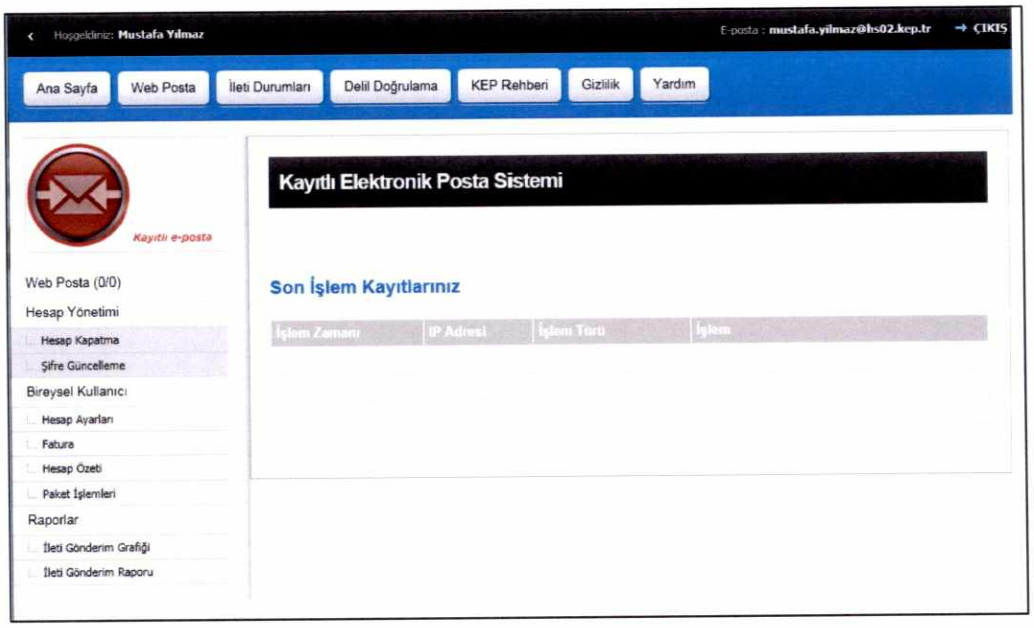
2. "SMS Şifre Doğrulama" işlemi için hesap sahibinin cep telefonuna gelen 3 dakika geçerlik olan şifre, "Cep telefonunuza gelen SMS şifresini giriniz" alanına yazılır ve "Oturum Aç" simgesi devam edilir (Şekil Ek 6-19).

Şekil Ek 0-19 KEP Sistemi SMS Şifre Doğrulama ekranı görünümü



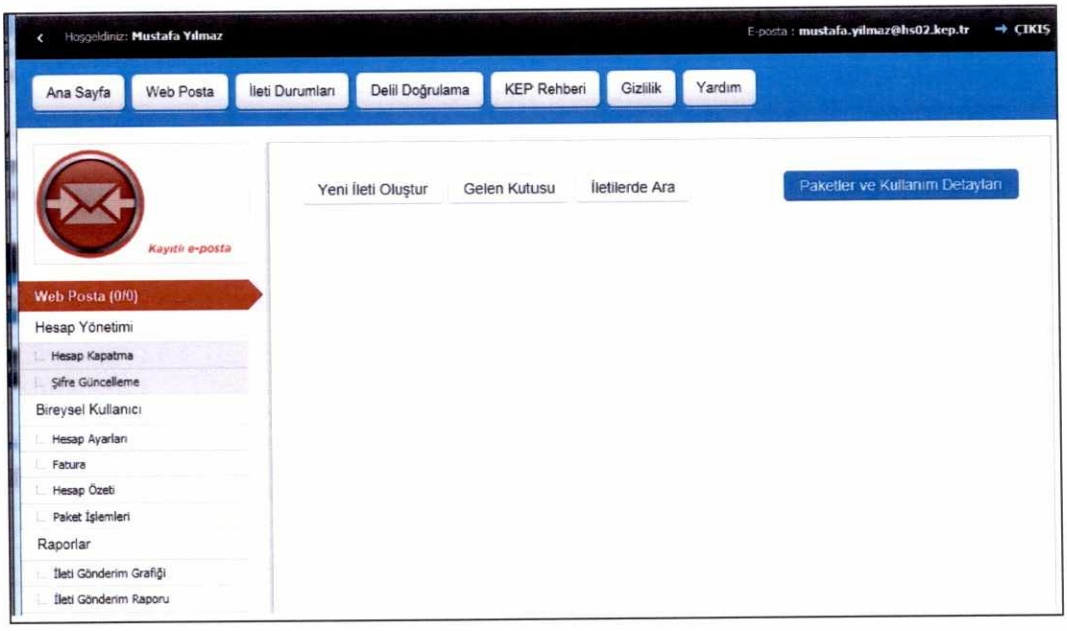
3. Ana Sayfa, Web Posta, İleti Durumları,Delil Doğrulama, KEP Rehberi, Gizlilik, Yardım, Web Posta, Hesap Yönetimi, Hesap Kapatma, Şifre Güncelleme, Bireysel Kullanıcı, Hesap Ayarları, Fatura, Hesap Özeti, Paket İşlemleri, Raporlar, İleti Gönderim Grafiği, İleti Gönderim Raporu gibi menülerden oluşan KEP sistemi İşlem sayfasında bulunan ve menülerde yer alan işlemlerimizi gerçekleştirebiliriz (Şekil Ek 6-20).

Şekil Ek 0-20 KEP Sistemi İşlem ekranı görünümü



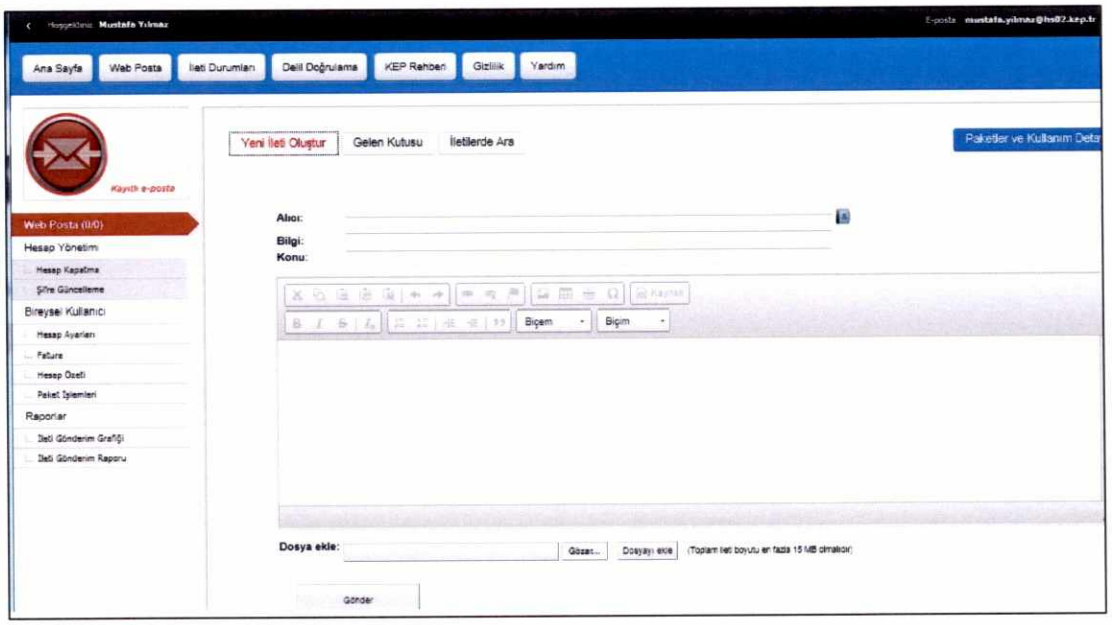
4. e-Postaya ilişkin işlemlerimiz için "Web Posta" seçeneği ile yeni ileti oluşturabilir, gelen e-postamızı okuyabilir, e-postalarımızda arama yapabiliriz. Yeni bir ileti oluşturmak için "Yeni İleti Oluştur" seçeneği ile işlem devam eder (Şekil Ek 6-21).

Şekil Ek 0-21 KEP Sistemi Posta ekranı görünümü



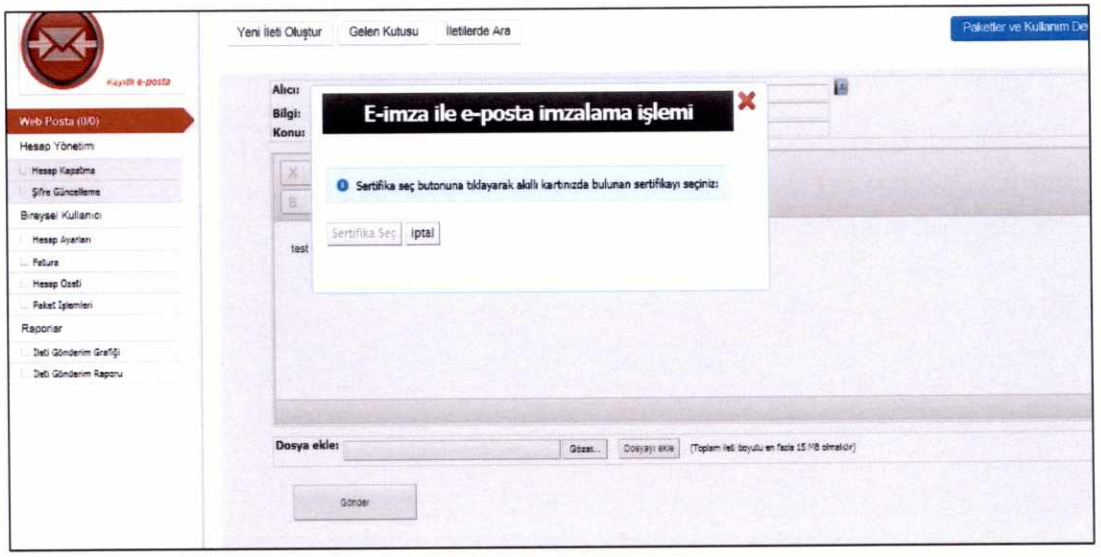
5. Alıcının, Bilgi, Konu, Metin, Dosya Ekle alanlarının ve Gönder simgesinin bulunduğu bu pencerede mesajımızı oluşturabilir varsa e-belge ekleyebiliriz. "Gönder" simgesi ile bir sonraki adıma geçilir (Şekil Ek 6-22).

Şekil Ek 0-22 KEP Sistemi Yeni Posta ekranı görünümü



6. e-İmzalama için kullanıcıya ait sertifika seçilerek gönderim işlemi gerçekleştirilmiş olur (Şekil Ek 6-23).

Şekil Ek 0-23 KEP Sistemi e-İmza ekranı görünümü



ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Mustafa YILMAZ