BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

KAYITLI ELEKTRONİK POSTA SİSTEMİ, DÜNYA UYGULAMALARI, TÜRKİYE İÇİN DÜZENLEYİCİ VE DENETLEYİCİ YAKLAŞIMLAR

Emrah GÜNEL

Bilişim Uzmanlığı Tezi

Haziran 2015

Ankara

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-143-3

BTK Yayın No T 0252

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

KAYITLI ELEKTRONİK POSTA SİSTEMİ, DÜNYA UYGULAMALARI, TÜRKİYE İÇİN DÜZENLEYİCİ VE DENETLEYİCİ YAKLAŞIMLAR

Emrah GÜNEL

Bilişim Uzmanlığı Tezi

Haziran 2015

Ankara

Emrah GÜNEL tarafından hazırlanan "*Kayıtlı Elektronik Posta Sistemi, Dünya Uygulamaları, Türkiye İçin Düzenleyici ve Denetleyici Yaklaşımlar*" adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Demet KABASAKAL
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Celalettin DİNÇER

Üye : Nihat SÜMER

Üye : Kemal Sacid SARIKAYA

Üye : Gökhan EVREN

Üye : Demet KABASAKAL

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

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	KAYITLI ELEKTRONİK POSTA SİSTEMİ, DÜNYA UYGULAMALARI, TÜRKİYE İÇİN DÜZENLEYİCİ VE DENETLEYİCİ YAKLAŞIMLAR
Türü	Bilişim Uzmanlığı Tezi
Yazar	Emrah GÜNEL
Teslim Tarihi	13 Haziran 2015
Anahtar Kelimeler	Kayıtlı Elektronik Posta, Güvenilir Hizmetler, Denetim Rehberi, Hizmet Sağlayıcı, KEPHS
Tez Danışmanı	Demet KABASAKAL
Sayfa Adedi	xii + 243

Özet

Kayıtlı elektronik posta (KEP), bilinen elektronik postaya ilave olarak elektronik postanın; göndericisi tarafından gönderilip gönderilmediği, alıcısına ulaşıp ulaşmadığı ve alıcısı tarafından okunup okunmadığı ile ilgili delil hizmetlerini sunan bir sistemdir. KEP, taraflar arasındaki iletişimin hukuki geçerliliğe sahip bir şekilde gerçekleşmesine ve hizmetlerin etkin, verimli, hızlı bir şekilde verilebilmesine olanak sağlaması nedeniyle elektronik ortamdaki hizmetlerin önemli bir bileşeni haline gelmiştir. Bu tezde genel olarak KEP sisteminin teknik ve hukuki altyapısı, bileşenleri, gelişim süreci, özellikleri ile KEP sistemine duyulan gereksinim, dünya uygulamaları ve ülkemizdeki mevcut durum ele alınarak değerlendirmeler yapılmış ve bu çerçevede Türkiye'deki mevcut düzenlemelere ilişkin çeşitli önerilere yer verilmiştir. Ayrıca KEP'e ilişkin düzenleme ve denetleme görevleri bulunan Bilgi Teknolojileri ve İletişim Kurumu'nun faaliyetlerini daha etkin ve verimli bir şekilde gerçekleştirmesi için yol haritası belirlenmeye çalışılmıştır.

ABSTRACT

INFORMATION AND COMMUNICATIONS TECHNOLOGIES AUTHORITY	
Thesis	REGISTERED ELECTRONIC MAIL SYSTEM, GLOBAL EXPERIENCES, REGULATORY AND SUPERVISORY APPROACHES FOR TURKEY
Type	ICT Expert Thesis
Author	Emrah GÜNEL
Submission Date	13 June 2015
Key Words	Registered Electronic Mail, Trusted services, Supervision Guide, Service Providers, REMSP
Advisor	Demet KABASAKAL
Total Page	xii + 243

Abstract

Registered electronic mail (REM) is a system which provides a confirmation mechanism for ensuring whether the electronic mail is sent by its sender, reached to its destination, and even read by the receiver. REM has become an important component of services requiring legal validity in the virtual environment, as it enables to perform efficient, effective and rapid communication between the parties. In this thesis, the evaluations are done by regarding the REM system's technical and legal infrastructure, components, development period and the need for REM system along with its features, world practices and the current status in Turkey and within this frame, various recommendations were provided regarding the current regulations. Another goal was to designate a course of action in order to make Information and Communication Technologies Authority's (BTK) activities more efficient and effective.

TEŞEKKÜR

Herşeyden ve herkesten önce bugünlere gelmemin vesilesi ve dolayısıyla bu tez çalışmasının sahipleri olan, sonsuza kadar kendilerine minnettar olacağım sevgili Anne ve Babama, bu tez çalışması süresi boyunca yaptığı fedakârlıkların yanında beni her fırsatta motive eden kıymetli eşim Sümeyra GÜNEL'e ve sevgili kızım Hümeyra Beren GÜNEL'e, danışmanım olarak bana rehberlik yapan, beni yönlendiren, yoğun çalışma temposuna rağmen hiçbir yardım talebimi geri çevirmeyen ve bilgi birikimini benimle paylaşan Sn. Demet KABASAKAL'a, olumlu, yapıcı eleştirileri ve değerli katkılarıyla çalışmamın olgunlaşmasına yardımcı olan değerli mesai arkadaşlarım Sn. Talat GÜÇLÜ, Sn. Onur GENÇER, Sn. Yüksel GÜNAYDIN, Sn. Sati ATİK, Sn. Ömer YAVUZ, Sn.Hidayet PINARAKAR, Sn. Abdülkadir GÜL ile desteğini hiçbir zaman esirgemeyen Daire Başkanım Sn. Kemal Sacid SARIKAYA'ya ve başta daire arkadaşlarım olmak üzere tüm diğer mesai arkadaşlarıma en içten teşekkürlerimi ve saygılarımı sunar, bu çalışmanın çok sevdiğim ülkeme faydalı olmasını dilerim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AAA	Açık Anahtar Altyapısı (Public Key Infrastructure-PKI)
AB	Avrupa Birliği (European Union-EU)
ABD	Amerika Birleşik Devletleri (United States of America-USA)
AdES	Gelişmiş Elektronik İmza (Advanced Electronic Signature)
AGID	İtalya Dijital Ajansı (The Agency for Italy Digital)
AP	Erişim Noktası (Access Point)
API	Uygulama Programlama Arayüzü (Application Programming Interface)
AS	Uygulanabilirlik Bildirimi (Applicability Statement)
ASCII	Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (American Standard Code for Information Interchange)
ASN	Soyut Sözdizin Gösterimi (Abstract Syntax Notation)
AU	Erişim Birimi (Access Unit)
BfDI	Alman Federal Veri Koruma Kurulu (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)
BGİ	Bilgi Güvenliği İlkeleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIA	İş Etki Analizi (Business İmpact Analysis)
BİT	Bilgi ve İletişim Teknolojileri (Information and Communication Technologies (ICT))
BS	İngiliz Standardı (British Standart)
BSI	Federal Bilgi Teknolojileri Güvenliği Ofisi (Bundesamt fur Sicherheit in der Informationstechnik)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CA	Sertifikasyon Otoritesi (Certification Authority)

CAdES	CMS Gelişmiş Elektronik İmza (CMS Advanced Electronic Signature)
CCITT	Uluslararası Telgraf ve Telefon Danışma Komitesi (Comité Consultatif International Téléphonique et Télégraphique)
CEM	Kayıtlı Posta Sistemi (Certified Electronic Mail)
CLS	Merkezi Arama Servisi (Central Lookup Service)
CMS	Kriptografik Mesaj Sözdizimi (Cryptographic Message Syntax)
CRL	Sertifika İptal Listesi-SİL (Certificate Revocation List)
CTSS	Uyumlu Zaman Paylaşımlı Sistem (Compatible Time Sharing System)
DA	Teslimat Aracı (Delivery Agent)
DDoS	Dağıtık Servis Kesintisi (Distributed Denial of Service)
DDS	Belge Teslim Sistemi (Document Delivery System)
DigitPA	Kamu Yönetiminde Ulusal Bilişim Merkezi (The National Centre for ICT in Public Administration)
DLNDLR	Alıcı Tarafından İndirildi/İndirilmedi (DownloadNonDownloadByRecipient)
DNDR	Alıcıya Teslim Edildi/Edilemedi (DeliveryNonDeliveryToRecipient)
DNS	Alan Adı Sistemi (Domain Name System)
DP	Teslim Noktası (Delivery Point)
DSN	Teslim Durum Bildirimi (Delivery Status Notifications)
E2EE	Noktadan Noktaya Şifreleme (End-to-End Encryption)
eID	Elektronik Kimlik Tespiti (Electronic Identification)
eIDAS	Elektronik Tanımlama ve Güven Hizmetleri (Electronic Identification and Trust Services)
EİK	Elektronik İmza Kanunu
ERV	Yasal Elektronik Haberleşme (Electronic Legal Communications)

ESHS	Elektronik Sertifika Hizmet Sağlayıcısı (Electronic Certificate Service Provider-ECSP)
ETSI	Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute)
ETSI TS	ETSI Teknik Özellikler (ETSI Technical Specification)
ETSI TR	ETSI Teknik Rapor (ETSI Technical Report)
FKM	Felaketten Kurtarma Merkezi
FTP	Dosya Aktarım Protokolü (File Transfer Protocol)
HSM	Donanımsal Güvenlik Modülü (Hardware Security Module)
HTTP	Hiper Metin Aktarım Protokolü (Hyper-Text Transfer Protocol)
IETF	İnternet Mühendisliği Görev Gücü (Internet Engineering Task Force)
IMAP	İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol)
IP	Internet Protokolü (Internet Protocol)
IPsec	İnternet Protokol Güvenliği (Internet Protocol Security)
ISMS	Bilgi Güvenliği Yönetim Sistemi (Information Security Management System)
ISO	Uluslararası Standardizasyon Örgütü (International Organization for Standardization)
ISO/IEC	Uluslararası Standardizasyon Örgütü / Uluslararası Elektroteknik Komisyonu (The International Organization for Standardization / International Electrotechnical Commission)
ISYS	İş Sürekliliği Yönetim Sistemi
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
ITU-T	Uluslararası Telekomünikasyon Birliği - Telekomünikasyon Standardizasyon Sektörü (International Telecommunication Union - Telecommunication Standardization Sector)

İC	İtalya Cumhuriyeti
İCK	İtalya Cumhurbaşkanlığı Kararnamesi
İSS	İnternet Servis Sağlayıcısı
KBYS	Kişisel Bilgiler Yönetim Sistemi
KEP	Kayıtlı Elektronik Posta
KEPHS	Kayıtlı Elektronik Posta Hizmet Sağlayıcısı
MASAK	Mali Suçları Araştırma Kurulu Başkanlığı
MDA	Mesaj Teslim Aracı (Message Delivery Agent)
MDN	Mesaj Devir Bildirimleri (Message Disposition Notifications)
MERNİS	Merkezi Nüfus İdare Sistemi
MERSİS	Gümrük ve Ticaret Bakanlığı Merkezi Sicil Kayıt Sistemi
MHS	Mesaj İşleme Sistemi (Message Handling System)
MIME	Çok Amaçlı İnternet Posta Uzantıları (Multipurpose Internet Mail Extensions)
MPLS	Çoklu Protokol Etiket Anahtarlama (Multiprotocol Label Switching)
MS	Mesaj Deposu (Messages Store)
MSA	Mesaj Gönderim Aracı (Message Submission Agent)
MTA	Mesaj Aktarım Aracı (Message Transfer Agent)
MTS	Mesaj Aktarım Sistemi (Message Transfer System)
MX	Posta Değişim (Mail Exchange)
NDN	Teslim Edilememe Bildirimi (Non-Delivery Notification)
NDR	Tesim Edilememe Raporu (Non-Delivery Report/Receipt)
NES	Nitelikli Elektronik Sertifika
nPA	Alman eID Kimlik Kartı (neuer Personalausweis)
NRD	Teslimin İnkâr Edilemezliği (Non-Repudiation of Delivery)

NRO	Kaynağın İnkâr Edilemezliği (Non-Repudiation of *Origin)*
NRR	Alındı Bildiriminin İnkâr Edilemezliği (*Non-Repudiation of Receipt*)
NRS	Gönderimin İnkâr Edilemezliği (*Non-Repudiation of Submission*)
NRT	Mesaj İletiminin İnkâr Edilemezliği (Non-Repudiation of Transfer)
OCSP	Çevrimiçi Sertifika Durum Protokolü-ÇİSDuP (Online Certificate Status Protocol)
OID	Nesne Belirteci (Object Identifier)
OSCI	Çevrimiçi Bilgisayar Arayüzü Hizmetleri (Online Services Computer Interface)
OTP	Tek Kullanımlık Şifre (One Time Password)
P2P	Eşten Eşe Bağlantı (Peer to Peer)
PAdES	PDF Gelişmiş Elektronik İmza (PDF Advanced Electronic Signatures)
PDAU	Fiziksel Teslim Erişim Birimi (Physical Delivery Access Unit)
PDF	Taşınabilir Belge Biçimi (Portable Document Format)
PEC	İtalyan Kayıtlı Elektronik Posta (Posta Elettronica Certificata)
PGP	Oldukça İyi Gizlilik (Pretty Good Privacy)
PIN	Kişisel Tanımlama Numarası (Personal Identification Number)
POP	Posta Ofis Protokolü (Post Office Protocol)
PTT	Posta ve Telgraf Teşkilatı
QEC	Nitelikli Elektronik Sertifika (Qualified Electronic Certificate)
QES	Nitelikli Elektronik İmza (Qualified Electronic Signature)
RDHK	Resmi Doküman Hizmetleri Kanunu
REM	Kayıtlı Posta Sistemi (Registered Electronic Mail)
RFC	Yorum Talepleri (Request for Comment)
RNRR	Alıcı Tarafından Erişildi/Erişilmedi (RetrievalNonRetrievalByRecipient)

RP	Alma Noktası (Reception Point)
RRAR	Alıcı KEPHS Kabul/Red (RelayToREMMDAcceptanceRejection)
RRF	Alıcı KEPHS'ye Teslim Edilemedi (RelayToREMMDFailure)
S/MIME	Güvenli/Çok Amaçlı İnternet Posta Uzantıları (Secure/Multipurpose Internet Mail Extensions)
SB	Sakla ve Bildir (Store and Notify)
Sİ	Sakla ve İlet (Store and Forward)
SLA	Minimum Hizmet Seviyesi (Service Level Aggrement)
SMTP	Basit Posta Aktarım Protokolü (Simple Mail Transfer Protocol)
SOA	Servis Tabanlı Mimari (Service Oriented Architecture)
SOAP	Basit Nesne Erişim Protokolü (Simple Object Access Protocol)
SSL	Güvenli Yuva Katmanı (Secure Socket Layer)
ssPIN	Sektöre Özel Kişisel Kimlik Numarası (Sector Specific Personal Identification Number)
TCP	İletim Denetim Protokolü (Transmission Control Protocol)
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
TSA	Zaman Damgası Hizmet Sağlayıcısı (Time-Stamping Authority)
TSL	Güvenilir Hizmetler Durum Listesi (Trust-service Status List)
TTK	Türk Ticaret Kanunu
TTP	Güvenilir Üçüncü Taraf (Trusted Third Party)
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UA	Kullanıcı Aracı (User Agent)
UPU	Evrensel Posta Birliği (Universal Postal Union)
UTC	Eşgüdümlü Evrensel Zaman (Coordinated Universal Time)
UYAP	Ulusal Yargı Ağı Projesi
VPN	Sanal Özel Ağ (Virtual Private Network)

W3C	Dünya Ağ Birliği (World Wide Web Consortium)
WCAG	Web Erişilebilirlik Girişim Yönergesi (Web Content Accessibility Guidelines)
XAdES	XML Gelişmiş Elektronik İmza (XML Advanced Electronic Signatures)
XML	Genişletilebilir İşaretleme Dili (Extensible Markup Language)

GİRİŞ

Son yıllarda fiziksel ortamda yürütülen birçok işlem artık elektronik ortamda gerçekleştirilmektedir. Özellikle internetin yaygınlaşması ve mobil cihazların kullanımının artmasıyla birlikte bilgi ve iletişim teknolojilerinin (BİT) kullanımı artmış, günlük yaşamın bir parçası haline gelmiş ve iletişim şekilleri de değişmeye başlamıştır. Bu gelişmeler ile birlikte elektronik posta, sosyal paylaşım siteleri, SMS, anlık mesajlaşma, VoIP gibi araçlar fiziksel iletişimin yerini almaya başlamıştır.

BİT'in hızla gelişmesine paralel olarak kurumlar, şirketler ve bireyler arasındaki iş ve işlemlerin elektronik ortamda gerçekleşme oranı her geçen gün artmaya ve taraflar arasında elektronik bilgi/belge paylaşımının hukuki geçerliliğe sahip bir şekilde gerçekleştirilmesi daha fazla önem kazanmaya başlamıştır.

Günümüzde elektronik ortamda bilgi/belge paylaşımında yaygın olarak kullanılan standart elektronik posta, iş ve işlemlerin kesintisiz devam etmesine olanak sağladığı için önemli bir araçtır. Ancak gönderilen, alınan, elektronik olarak arşivlenen veya basılı olarak saklanan bir elektronik postanın mevcut düzenlemeler çerçevesinde hukuki geçerliliğe sahip olmadığı da bilinen bir gerçektir.

Bununla birlikte içeriğinin değiştirilebilmesi, göndericisinin gönderen olarak görünen kişiden farklı olabilmesi, gönderilmiş veya alınmış olduğunun kanıtlanamaması da standart elektronik postanın bilinen problemleri arasındadır. Bu nedenle elektronik ortamda bilgi ve belgelerini paylaşan tarafların, işlemleri güvenli bir şekilde gerçekleştirmek ve muhataplarıyla karşılıklı güveni sağlamak için uygun güvenlik kontrollerine ve mekanizmalarına sahip olması gerekmektedir.

Kayıtlı Elektronik Posta (KEP) bu alanda büyük değişimler ve gelişmeler sağlaması beklenen, elektronik ticaret ile elektronik devlet projelerinin altyapısını oluşturacak asli unsurlardan biri olarak karşımıza çıkmaktadır.

Yasal olarak geçerli ve teknik olarak güvenli elektronik posta olarak tanımlanan KEP, bilinen standart elektronik postaya ilave olarak elektronik postanın;

- Göndericisi görünen kişi/kuruluş tarafından gönderilip gönderilmediğine,
- Alıcıya ulaşıp ulaşmadığına ve ne zaman ulaştığına,
- Alıcısı tarafından okunup okunmadığına

ilişkin delil hizmetleri sunan bir sistemdir.

KEP sisteminde elektronik postalar "güvenilir bir üçüncü taraf" rolünde olan Kayıtlı Elektronik Posta Hizmet Sağlayıcıları (KEPHS) vasıtasıyla gönderilip alınmaktadır. Bu sistemde bir elektronik postanın göndericiden alıcıya iletilmesi esnasında meydana gelen bütün işlemlere ilişkin kayıtlar güvenli elektronik imza ve zaman damgası kullanılarak tutulmakta; delil mahiyetinde ve hukuki geçerliliğe sahip belgeler olarak kabul edilmektedir.

Bu tezde genel olarak KEP sistemi ve teknik altyapısı, dünya uygulamaları, Türkiye'deki mevcut durum ele alınarak değerlendirmelerde bulunulmakta ve bu değerlendirmeler çerçevesinde ülkemizde KEP'e ilişkin hem düzenlemeler hem de Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yapılan KEPHS denetimlerine ilişkin çeşitli öneriler getirilmektedir.

Bununla birlikte bu çalışmayla 6102 sayılı Türk Ticaret Kanunu (TTK)[1] ile ülkemizde KEP'e ilişkin oluşturulan yasal çerçeve ve bu kapsamda BTK'ya verilen görev irdelenerek BTK'nın faaliyetlerini daha etkin ve verimli bir şekilde gerçekleştirmesi için yol haritası belirlenmeye çalışılmaktadır. Ayrıca KEP konusunda ülkemizde henüz kapsamlı bir çalışma yapılmamış olduğundan hazırlanan bu tezin referans bir kaynak olacağı değerlendirilmektedir.

[1] 6102 sayılı Türk Ticaret Kanunu 13/1/2011 tarihinde kabul edilmiş ve 14/2/2011 tarih ve 27846 sayılı Resmi Gazete'de yayımlanmıştır.

KEP'e ilişkin bu tezde ortaya konan yaklaşımlar temelde geleneksel kayıtlı postaya dayanmakta ve KEP'te bulunan özellikler genel olarak fiziki ortama göre belirlenmektedir. Bu nedenle tezin ilk bölümünde, günlük hayatın bir parçası olarak kullanılan ve aynı zamanda KEP'in fiziki ortamdaki karşılığı olan geleneksel kayıtlı posta ya da fiziki kayıtlı postanın temel çalışma mantığı ve güvenlik yaklaşımları ele alınmaktadır. Böylece KEP sisteminin hangi ihtiyaçlara ne şekilde çözüm getirdiğine ilişkin bir fikir oluşturulması hedeflenmektedir.

KEP sisteminde iş ve işlemler temelde elektronik postanın altyapı bileşenleri ve özellikleri kullanılarak gerçekleştirilmektedir. Bu nedenle tezin birinci bölümünde elektronik postanın yapısı, tarihi, işleyişi ve özellikleri ele alınmakta, genel mesaj işleme ve elektronik postanın yapısı incelenerek KEP sisteminin gelişimi ortaya konulmakta, KEP sisteminde bulunan güvenlik hizmetleri ve özelliklerinin temelleri irdelenmektedir.

İkinci bölümde elektronik postanın sahip olmadığı bazı özelliklerden yola çıkılarak mevcut ihtiyaçlar ortaya konulmakta ve bu ihtiyaçları karşılayan KEP sisteminin bileşenleri ve özellikleri ele alınmaktadır.

Üçüncü bölümde, KEP sistemini düzenlemiş ve hayata geçirmiş olan Almanya, İtalya ve Avusturya gibi ülkeler tarafından oluşturulan teknik altyapı, hazırlanan mevzuat, uygulanan politikalar ve bu ülkelerdeki mevcut durum ile konuya ilişkin Avrupa Birliği'nin (AB) yaklaşımı incelenmektedir. Bununla birlikte yapılan bu incelemeler ışığında bahse konu ülkelerdeki KEP sistemlerinin işleyişine göz atılarak değerlendirmeler yapılmaktadır.

Dördüncü bölümde, KEP'e ilişkin BTK tarafından hazırlanan ikincil düzenlemeler ile ilgili diğer mevzuat irdelenmekte, hâlihazırda ülkemizdeki mevcut durumun analizi yapılmakta ve bu kapsamda yapılması gereken düzenlemeler ortaya konulup değerlendirmelere ve önerilere yer verilmektedir. Ayrıca teknik ve idari yönleriyle KEP sisteminin yapısı incelenirken KEPHS'lerin denetimlerinde uygulanacak esaslar da ortaya konulmaktadır.

Tezin sonuç bölümünde ise, önceki bölümlerde incelenen dünya uygulamaları ve Türkiye'deki mevcut durum yine tez kapsamında yapılan değerlendirmeler çerçevesinde karşılaştırılmakta ve ülkemizdeki KEP sisteminin hukuki ve teknik altyapısına ilişkin önerilere yer verilmektedir. Yine aynı bölümde KEPHS'lerin BTK'ya yapmış oldukları bildirim sürecinde, yetkilendirilmelerinde ve rutin denetimlerinde kullanılmasının uygun olacağı değerlendirilen denetim kontrol listesi önerisine yer verilmektedir.

1. GELENEKSEL KAYITLI POSTA VE ELEKTRONİK POSTA

Günlük hayatın bir parçası olarak sıkça kullanılan geleneksel kayıtlı posta veya fiziki kayıtlı posta, önemli bilgi ve belgelerin güvenli bir şekilde taraflar arasında paylaşılmasını sağlayan bir iletişim aracı olarak kullanılagelmiştir.

Elektronik posta, bilgisayar ağları kullanılarak her türlü verinin taraflar arasında paylaşılabilmesine imkân sağlayan hızlı ve etkili bir iletişim yöntemidir (Baker ve Bowen, 2003). Elektronik posta ile taşınan mesajlar elektronik posta iletisi veya elektronik posta mesajı olarak adlandırılmaktadır (Öztürk, 2009).

KEP'e ilişkin ortaya konan yaklaşımlar temelde geleneksel kayıtlı postaya dayanmakta ve KEP'te bulunan özellikler genel anlamda fiziki ortamda varolanlara göre belirlenmektedir. Bununla birlikte KEP sisteminde de iş ve işlemler temelde elektronik postanın altyapı bileşenleri ve özellikleri kullanılarak gerçekleştirilmektedir. Bu nedenle bu bölümde; geleneksel kayıtlı postanın temel çalışma mantığı ve güvenlik yaklaşımları, elektronik postanın tarihi, yapısı, işleyişi ve özellikleri ele alınmaktadır.

1.1 Geleneksel Kayıtlı Posta

KEP (*Registered Electronic Mail: REM, Certified Electronic Mail: CEM*), geleneksel kayıtlı posta veya ülkemizde daha çok kullanılan adıyla taahhütlü postaya elektronik ortamda duyulan ihtiyaç sonucu ortaya çıkan bir sistemdir.

1.1.1 Geleneksel kayıtlı posta hizmetleri

Geleneksel posta geçmişten beri belge, mektup, kartpostal, koli veya diğer posta gönderilerini iletmek üzere kullanılmaktadır. Bu iletim genellikle Posta ve Telgraf Teşkilatı A.Ş (PTT), Amerika Birleşik Devletleri Posta Servisi (USPS) ve Canada Postgibi ülkelerin posta servis sağlayıcıları aracılığıyla gerçekleştirilmektedir. Bu gönderimlerde, postaların servis sağlayıcısına teslim edilmesiyle alıcısına teslim edileceği, kanunen yetkisi olanlar dışında (gümrük yetkilileri vb. gibi) ara aşamalarda

açılmayacağı, okunmayacağı veya incelenmeyeceği, herhangi bir fiziksel zarar görmeyeceği, kaybolmayacağı ve çalınmayacağı varsayılır. Ancak geleneksel postada gönderici, alıcıdan, gönderinin teslimi ile ilgili bir geri dönüş gelmemesi durumunda postanın alıcısına ulaşıp ulaşmadığına dair bilgi sahibi olamamaktadır.

Bu nedenle vergi beyannameleri, pasaportlar, kontratlar, senetler, mahkeme celpleri gibi daha yüksek güvenlik, güvenilirlik ve teslim alınmasına dair bildirim gerektiren değerli postaların gönderen tarafından takip edilmesi ve postanın alıcısına teslim edildiğine ilişkin kanıt sağlanması gibi katma değerli hizmetler posta hizmet sağlayıcıları tarafından verilmeye başlanmıştır. Bu hizmetler ülkelere ve hizmet sağlayıcılara göre değişmekle birlikte temel olarak gönderilen postaya ilişkin imzalı/imzasız teslim kanıtı sağlama, gönderinin belirli bir noktaya teslim edildiğine ilişkin kanıt sağlama veya gönderinin teslim alındığını kanıtlayacak alındı (*receipts*) belgesi oluşturma şeklinde çeşitlenebilmektedir. Bu şekilde bir alındı veya teslim kanıtı sağlayan posta hizmetleri kayıtlı posta olarak adlandırılmaktadır (Canada Post, 2015).

Normal postalar için yanlış alıcıya teslim, kaybolma, çalınma veya zarar görme gibi durumlar kabul edilebilmesine rağmen hassas ve değerli gönderilerin daha yüksek güvenlik ve güvenilirlik seviyesinde taşınmasına ihtiyaç duyulabilmektedir. Vergi beyannameleri, pasaportlar, kontratlar, senetler, mahkeme celpleri, çekler veya para transferleri gibi değerli gönderileri iletmek üzere daha yüksek güvenlik sunmak amacıyla kayıtlı posta, kayıtlı gönderi, güvenli gönderim veya taahhütlü posta olarak adlandırılan bazı katma değerli hizmetler verilmektedir.

Kayıtlı posta, gönderilerin bir alındı karşılığında posta hizmet sağlayıcısına verilmesinden itibaren alıcıya teslim edilmesine kadar geçen tüm süreçlerin kayıt altına alınmasıyla yürütülen bir hizmet çeşididir. Kayıtlı posta terimi de burada tutulan kayıtlardan türetilmiştir.

Kayıtlı postada herbir gönderi sisteme girdiğinde tekil bir takip veya yönlendirme numarası almaktadır. Bu takip numarası Evrensel Posta Birliği'nin (UPU) yayımlamış

olduğu "Posta gönderilerinin tanımlanması" başlıklı standarda (UPU, 1996) göre oluşturulmaktadır. Buna göre posta tanımlama numarası on üç karakterden oluşmaktadır. İlk iki karakter posta servisini tanımlamak üzere kullanılmaktadır. Takip eden sekiz karakter ise postanın hizmet sağlayıcıya teslim edildiği tarih itibariyle bir sene boyunca başka hiçbir gönderiye verilemeyecek olan bir numaradır. Sonraki bir karakter önceki numaranın doğruluğunu teyid etmeye yarayan bir kontrol karakteridir. Son iki karakter ise Uluslararası Standardizasyon Örgütü (ISO) tarafından yayımlanan ISO-3166-1 (ISO, 2006)'e göre oluşturulan gönderinin çıktığı ülke kodunu ifade etmektedir. Örneğin "RR123456785TR" şeklinde oluşturulmuş bir takip numarası Türkiye'de oluşturulmuş bir kayıtlı postayı ifade etmektedir.

On üç karakterden oluşan takip numarası otomatik işlemeye imkân tanımak amacıyla bir barkod olarak gönderinin üzerinde bulunur. Diğer taraftan kayıtlı postada gönderinin takibi dışında göndericiye postayı gönderdiğine dair bir alındı belgesi verilmesi gibi özellikler de bulunmaktadır. Bu belge posta hizmet sağlayıcısı tarafından oluşturulur ve gönderici bu belgede bulunan takip numarası aracılığıyla gönderisinin takibini yapabilir. Posta hizmet sağlayıcısı teslim zincirinde gönderinin geçmiş olduğu herbir adımı kaydettiğinden göndericinin bu takibi yapması mümkün olabilmektedir.

1.1.2 Hibrit (Hybrid) kayıtlı posta

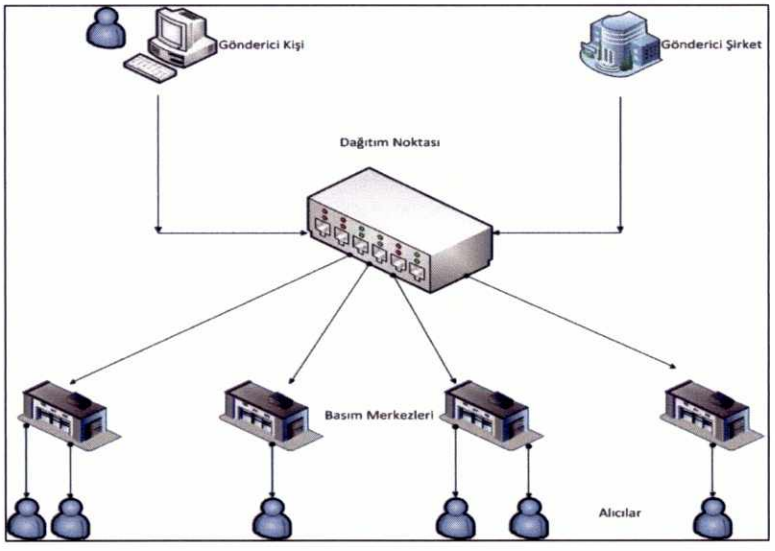
BİT'in hızla yaygınlaşmasıyla birlikte posta servis sağlayıcılar maliyetleri düşürme, katma değerli hizmetler sunma, kaliteli ve hızlı hizmet verme gibi nedenlerle fiziki ortamda yürüttükleri iş ve işlemleri elektronik ortamda yürütmeye başlamışlardır. Bu nedenle 1980'li yıllarda hibrit kayıtlı posta ortaya çıkmıştır. Maliyet ve zaman açısından sağladığı avantajlar bu hizmetin Avrupa'da ve ABD'de yaygınlaşmasını hızlandırmıştır (Cattel ve Inscore, 2001). Türkiye'de ise hibrit posta PTT tarafından 2010 yılı Ocak ayı itibariyle fiilen hizmete geçirilmiştir (PTT, 2015).

Jovanovic ve Rankov (2012)'a göre hibrit posta klasik postanın aksine gönderinin içeriğinin elektronik ortamda oluşturulduğu ve taşındığı, elektronik postaya kısmen

benzeyen bir posta sistemidir. Elektronik ortamda taşınan bu posta teslim yerine en yakın merkezde basılı hale getirilir ve paketlenerek fiziksel ortamda alıcısına teslim edilir (Jovanovic ve Rankov, 2012).

Hibrit postanın çalışma mantığı Şekil 1.1'de gösterilmektedir. Buna göre sistemde faturalar gibi çoklu gönderiler öncelikle elektronik ortamda üretilir ve daha sonra üretilen bu gönderiler elektronik ortamda posta hizmet sağlayıcısına ulaştırılır. Bu elektronik postayı alan hizmet sağlayıcısı ise postayı alıcısına en yakın basım merkezine elektronik ortamda iletmektedir. Son olarak basım merkezinde ilgili posta iletisi alıcısına fiziki ortamda teslim edilmek üzere basılıp zarflanmakta ve alıcının adresine fiziki olarak teslim edilmektedir. Sonuç olarak gönderi alıcının adresine en yakın yerde fiziki ortama aktarıldığından taşıma maliyetleri ve dağıtımla ilgili problemler önemli oranda azaltılmış olmaktadır (McMillan, 2001; Livson, 1999).

Şekil 1.1. Hibrit posta çalışma mantığı



Gönderi elektronik olarak iletilirken ne seviyede güvenlik önlemi alınırsa alınsın, sonuç itibariyle postanın basılı hale getirilme aşamasında açılması ve dolayısıyla görülebilmesine olanak sağlanması bu sistemin gizlilik açısından ciddi sıkıntıları

olduğunu ortaya koymaktadır. Bununla birlikte hibrit posta, gönderime ilişkin tüm süreçlerin elektronik ortama aktarıldığı KEP'e geçiş aşamasını oluşturmuştur.

1.2 Elektronik Posta Yapısı

Elektronik posta; internetin yaygınlaşması, her türlü verinin kolaylıkla iletilebilmesi ve düşük maliyetli olması nedeniyle ülkemizde ve tüm dünyada yoğun olarak kullanılan iletişim araçlarından biri haline gelmiştir. Günümüzde başta resmi kurumlar, ticari işletmeler ve vatandaşlar arasında her türlü bilgi ve belgenin gönderici ile alıcı arasındaki iletimi elektronik posta yoluyla gerçekleştirilebilmektedir.

Bu bölümde; genel mesaj işleme ve internet elektronik posta yapısı incelenmek suretiyle, KEP sisteminin gelişimi ortaya konularak, KEP sisteminde bulunan güvenlik hizmetleri ve özelliklerinin temelleri incelenmektedir. Bu amaçla öncelikle X.400 standardında kapsamlı bir şekilde anlatılan genel mesaj işleme mimarisi ele alınmaktadır (ITU-T, 1999a). Ayrıca, mevcut durumda yaygın olarak kullanılan ve X.400'e göre daha sade formlar sunan internet e-posta sistemlerinin kullandığı standart ve özelliklere de yer verilmektedir.

1.2.1 Elektronik postanın tarihçesi

Elektronik postanın ortaya çıkışı bilgisayar ağlarınının ortaya çıkışından da önceye dayanmaktadır (Partridge, 2008). Elektronik posta, 1961 yılında Uyumlu Zaman Paylaşımlı Sistem[1] (Compatible Time Sharing System-CTSS) adı verilen çok kullanıcılı bir sistem ile birlikte ortaya çıkmıştır. CTSS sistemi çok kullanıcılı bir sistem olmasına karşın kullanıcılar arasında doğrudan iletişim ihtiyacına cevap verememekteydi. Bu ihtiyaçtan yola çıkan CTSS kullanıcıları birbirlerine göndermek istedikleri mesajları alıcının ismini içeren ve herkesin erişimine açık bir dizine koymak suretiyle paylaşmışlardır. Ancak bu şekildeki bir paylaşım herhangi bir kullanıcının

[1] CTSS MIT bünyesinde geliştirilen, yüzlerce kayıtlı kullanıcısı bulunan, kullanıcılarının sisteme çevirmeli bağlantıya sahip terminaller ile bağlandıkları ve dosyaların çevrim içi bir diskte tutulduğu bir sistemdir (Vleck, 2013).

herhangi bir mesaja erişebilmesi nedeniyle güvenlik açısından bir takım riskler barındırmaktaydı (Vleck, 2013).

1964 yılında mesaj gönderme üzerine resmi bir sistem için ilk belgelenmiş öneri, Programlama Grup Notları 49 (Programming Staff Note 49) adı altında Louis Pouzin, Glenda Schroeder ve Pat Crisman tarafından oluşturulmuştur. Bu öneri doğrultusunda 1965 yılında Noel Morris ve Tom Van Vleck tarafından sistemin kullanıcıları arasındaki haberleşmeyi temin etmek üzere bir mesajlaşma sistemi tasarlanmış ve gerçekleştirilmiştir (Chisnall, 2015).

1971 yılına gelindiğinde CTSS sistemi üzerinde ve sadece aynı bilgisayar üzerinde mesajlaşmaya olanak sağlayan sistem, Ray Tomlison tarafından Gelişmiş Araştırma Projeleri Ajansı Şebekesi (Advanced Research Projects Agency Network - ARPANET) üzerinde farklı bilgisayarlar arası denenmiş ve bir ağ üzerinden mesaj gönderme işlemi gerçekleştirilmiştir. Tomlison bu işlemi aynı bilgisayar üzerinde posta kutusu oluşturma mantığı ile çalışan SNDMSG programı ile henüz deneysel bir dosya aktarım programı olan CPYNET'i birleştirmek suretiyle gerçekleştirmiştir. Tomlison günümüz e-posta adreslerinde de kullanılan '@' işaretini kullanıcıların yerel bir klasörden ziyade başka bir makine üzerinde olduğunu belirtmek amacıyla ilk kez kullanmıştır (Tschabitscher, 2011).

Zaman içerisinde hizmetin kullandığı protokoller, kullanım alanları ve hizmet sağlayıcılar farklılaşmış ve ihtiyaçlara göre değişimler geçirmiştir. Kullanım alanlarının artması ve kullanıcı kitlesinin genişlemesi ile birlikte, farklı platform ve uygulamalar üzerinde çalışma gereksiniminin ortaya çıkmış olması bu hizmetin verilmesinde standart bir yapı oluşturulması zorunluluğu doğurmuştur. Bu sebeple hizmetin sağlıklı bir şekilde verilebilmesini teminen birçok standart yayımlanmıştır. Hali hazırda e-posta, bu standartlar çerçevesinde işleyen bir sistem olarak geniş bir kullanım alanına sahiptir.

1.2.2 Genel mesaj işleme yapısı

Elektronik postanın gelişiminde rol oynayan standartlardan en önemlilerinden birisi Uluslararası Telekomünikasyon Birliği (ITU), Uluslararası Telgraf ve Telefon Danışma Komitesi[2] (Comité Consultatif International Téléphonique et Télégraphique-CCITT) tarafından yayımlanan X.400 standardıdır (ITU-T, 1999a; ISO/IEC, 2003a). Bu standartta, genel mesaj işleme sistemi (Message Handling System-MHS) detaylandırılmaktadır. X.400'de konu edilen mesaj işleme modeli hali hazırda kullanılan birçok elektronik posta sisteminin de temellerini oluşturmaktadır. Ancak X.400'ün öngördüğü mesaj işleme sistemi çok karmaşık ve maliyetli olduğundan, temelde birçok elektronik posta sisteminde baz olarak alınmasına rağmen kendisi yaygın bir kullanıma sahip olamamıştır. Ancak bu standart hali hazırda bazı yerel sistemlerde uygulanmaktadır.

1.2.2.1 Mimari

X.400 (ITU-T, 1999a; ISO/IEC, 2003a) ve X.402'de (ITU-T, 1999b; ISO/IEC, 2003b) yer alan MHS sisteminin genel işleyişi Şekil 1.2'de verilmiştir. Bu modelde ister MHS'ye doğrudan bağlantı sağlasın, isterse başka bir iletişim sistemi üzerinden MHS ile dolaylı bağlantı sağlasın, kullanıcı bir kişi veya sistem olabilmektedirler. Kullanıcılar mesaj gönderiminde mesajın kaynağı, mesaj alımında ise mesajın alıcısı konumundadırlar (ITU-T, 1999a). Sistem üç temel katmandan oluşmaktadır. En dış katmanda mesaj aktarım sistemini (Message Transfer System-MTS) kullanacak olan doğrudan veya dolaylı kullanıcılar bulunmaktadır. Kullanıcı konumunda bulunan dolaylı kullanıcılar diğer iletişim sistemleri olabileceği gibi fiziksel iletim servisleri de olabilmektedir.

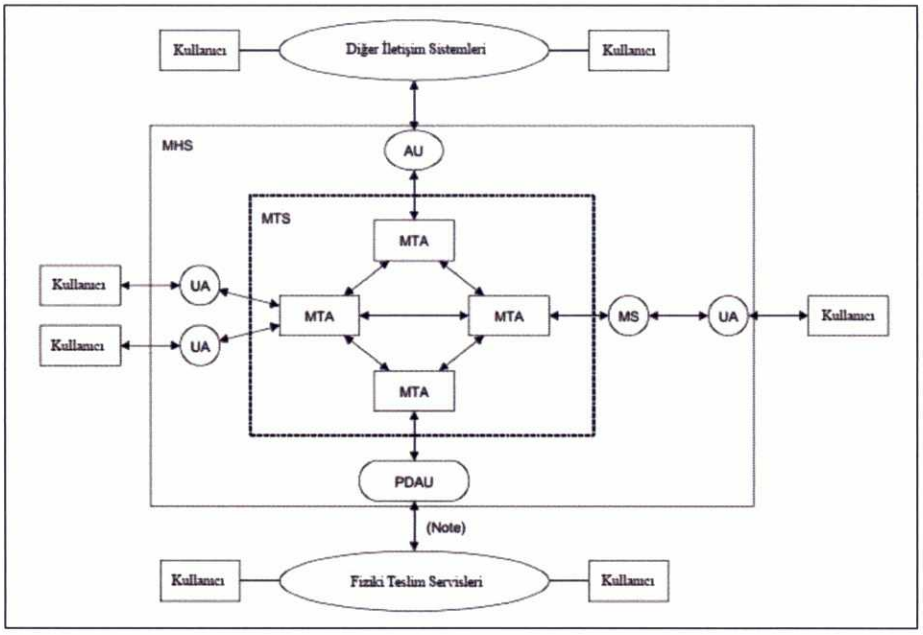
Sistemin orta katmanı olarak kabul edilebilecek olan kısımda MHS'nin kendisi ile karşılaşılmaktadır. Bu katmanda mesajın gönderici ve alıcılar arasındaki iletimine

---

[2] CCITT 1992 yılında ITU–Telekomünikasyon Standartları Sektörü (ITU-T) olarak yeniden adlandırılmıştır (ITU, 2006). ITU-T uluslararası ölçekte telekomünikasyon alanında standartlar geliştirmektedir.

ilişkin iş ve işlemler gerçekleştirilmektedir. MHS içerisinde yer alan ve en önemli bileşen olarak kabul edilen MTS ise en iç katmanda yer almaktadır.

Şekil 1.2. X.400 sistem mimarisi



Kaynak: ITU-T, 1999a

1.2.2.2 Sistemin bileşenleri

X.400 sistem mimarisi içerisinde yer alan bileşenler kullanıcılar, kullanıcı araçları (User Agent-UA), mesaj depoları (Messages Stores-MS), erişim birimleri (Access Unit-AU), fiziksel teslim erişim birimleri (Physical Delivery Access Unit-PDAU) ve mesaj aktarım araçları (Message Transfer Agent-MTA) şeklinde sıralanmaktadır. UA, MS, AU ve MTA'lar MHS'nin parçalarını oluşturmaktadırlar (ITU-T, 1999a).

1.2.2.2.1 Kullanıcılar

ITU-T'ye göre doğrudan ve dolaylı olmak üzere iki çeşit kullanıcı bulunmaktadır (1999a). Doğrudan kullanıcılar MHS ile doğrudan bağlantısı olan kullanıcılardır. Dolaylı kullanıcılar ise diğer telekomünikasyon sistemleri veya fiziki teslim servisleri

gibi bir sistem aracılığıyla MHS'ye bağlantısı olan kullanıcılar olarak tanımlanmaktadır.

1.2.2.2.2 Kullanıcı aracı

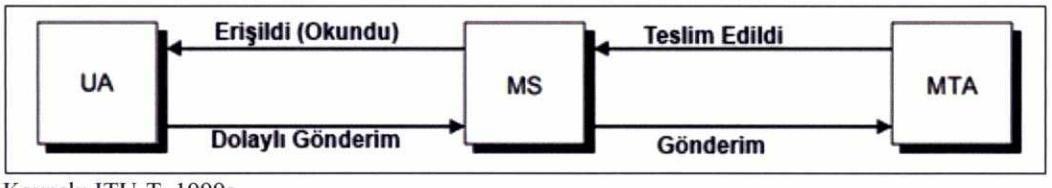
UA, mesaj göndermek ve almak için kullanılan ve son kullanıcılara hizmet veren yazılımlardır. İletinin kaynağı olan gönderici, mesajı bir UA aracılığıyla hazırlar. UA, kullanıcı adına mesajı göndermek veya almak üzere MTS veya MS ile irtibat sağlamaktadır. Bir UA, mesajı doğrudan MTS'den alabileceği gibi mesajlara bir MS aracılığıyla da erişebilmektedir. UA'nın grafik arayüze sahip olan Thunderbird gibi çeşitleri olduğu gibi, komut satırından çalışabilen çeşitleri de bulunmaktadır (Collings ve Wall, 2005).

Sistemin kullanıcı tarafından görünür kısmı UA'dır. Kullanıcılar ile MHS arasında bir katman olması nedeniyle kullanıcı MTA ve mesaj transferi kısmından soyutlanmaktadır (Collings ve Wall, 2005).

1.2.2.2.3 Mesaj deposu

MS, UA ve MTA arasındaki iletişimi sağlamak üzere tasarlanan bir birimdir. Diğer taraftan MS'nin mesajları kullanıcının erişimine sunmak üzere saklamak gibi bir görevi de bulunmaktadır. Ayrıca mesajı göndermek ve UA'ya gerekli bilgileri sağlamak da MS'nin işlevleri arasındadır. Yine mesajların gruplanması ve sınıflandırılması bu birim aracılığıyla gerçekleştirilebilmektedir. Bununla birlikte MS biriminde mesajın geçmişine ilişkin bilgileri içeren kayıtlar da tutulabilmektedir. Şekil 1.3'de bir mesajın MS kullanılarak teslimi ve mesaja erişim gösterilmektedir.

Şekil 1.3. MS kullanılarak gönderim ve alım



Kaynak: ITU-T, 1999a

1.2.2.2.4 Erişim birimi

Erişim birimleri vasıtasıyla diğer iletişim sistemleri ve fiziki iletim servisleri gibi dolaylı kullanıcıların MTS'ye bağlantısı sağlanmaktadır.

Bir AU olarak tasarlanan fiziksel erişim birimi sistemde isteğe bağlı olarak bulunmaktadır. Fiziksel iletim söz konusu olduğunda AU'lara PDAU adı verilir ve bu birimler AU'ların yaptığı işlemleri fiziki teslim kısmında gerçekleştirir.

1.2.2.2.5 Mesaj transfer sistemi ve mesaj aktarım aracı

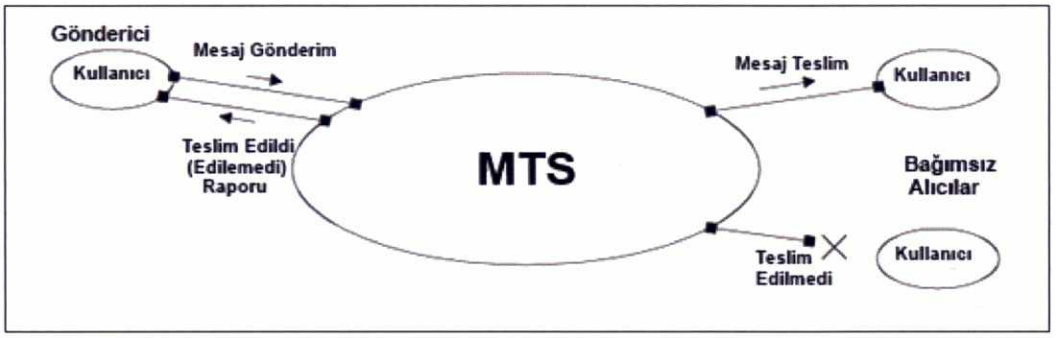
MTS, "mesaj sunum" (*message submission*), "mesaj teslim" (message delivery) ve "yönetim işlevleri" olamak üzere üç ana görevi ifa etmektedir (ITU-T, 1999c). Şekil 1.4'te bir MTS sisteminin işlevsel açıdan çalışma mantığı gösterilmektedir.

UA veya MS tarafından gönderilen mesajlar, alıcı veya alıcılarına gönderilmek üzere "mesaj sunum" tarafından teslim alınır. Bu kısım, mesaj gönderim aracı (Message Submission Agent-MSA) olarak da isimlendirilebilmektedir. MSA kendisine gelen mesaj üzerinde gerekli kontrolleri gerçekleştiren ve mesajın belirli kurallara ve standartlara uygunluğunu denetleyen kısımdır. Yapılan kontroller neticesinde; herhangi bir hata tespit edilmemiş ise mesaj alıcı veya alıcılarına iletilmek üzere MTA'ya iletilirken, herhangi bir hata tespit edilmesi halinde gönderme işlemi yarıda kesilir (Crocker, 2009).

MTA'lar tarafından taşınmış olan mesaj MS'ye iletilmek üzere mesaj teslim aracı (Message Delivery Agent-MDA) olarak da adlandırılan "mesaj teslim" tarafından alınır. MDA, bu mesajı teslim alarak ilgili alıcı veya alıcıların MS'sine ileterek mesajın saklanmasını sağlar (Crocker, 2009).

Yönetim işlevleri kısmı ise MTS'de uzun dönemli parametreleri değiştirmek amacıyla kullanılmaktadır (ITU-T, 1999c).

Şekil 1.4. MTS'nin yapısı



Kaynak: ITU-T, 1999c

MTA, mesajın alıcı ya da alıcılarının UA, AU veya MS birimlerine teslimini gerçekleştirir ve bu teslime ilişkin göndericiyi bilgilendirme işlevini yerine getirir. MTS birden fazla MTA'dan oluşmaktadır. MTA'lar sakla ve ilet mantığıyla kendi aralarındaki iletişim ile mesajın ilgili alıcıya teslim edilmesini sağlar (ITU-T, 1999a). Mesajın ilgili alıcıya iletilmesi için hangi yolun kullanılacağına da bu birim tarafından karar verilir. Kısacası MTA'ların bulunduğu bu katman iletimin omurgasını oluşturmaktadır.

1.2.2.3 Sistemin İşleyişi

Mesajlaşma sistemi yukarıda bahsedilen bileşenlerin belirli kurallar çerçevesinde birlikte çalışmasıyla ortaya çıkmaktadır.

Mesaj, gönderici tarafından UA aracılığıyla hazırlanmakta ve yine UA tarafından genellikle basit posta aktarım protokolü (Simple Mail Transfer Protocol-SMTP) kullanılarak MTS'ye iletilmektedir.

MTS'ye gelen mesaj, öncelikle standartlara ve tanımlanan kurallara uygunluk açısından değerlendirildikten sonra herhangi bir olumsuzluk tespit edilmemesi halinde alıcı veya alıcılarına iletilmek üzere MTA'ya teslim edilmektedir.

Mesajın alıcısına ulaştırılması için alıcıya ilişkin bilgilerin bilinmesi gerekmektedir. Bu nedenle MTA, Alan Adı Sistemi'nden (Domain Name System-DNS) alıcının Posta

Değişim (Mail Exchange-MX)[3] bilgilerini öğrenir. Ardından bu bilgiler doğrultusunda mesajın alıcısına ulaşması için izleyeceği yolu belirler ve mesajı alıcının MTA'sına ulaştırır. Mesajın MTA'lar arası taşıma işlemi için de yaygın olarak SMTP kullanılmaktadır.

Mesaj, alıcının MTA'sına ulaştığında alıcı taraftaki MDA tarafından tanımlı olan kontroller gerçekleştirilir ve bu mesaj alıcının MS'sine iletilir. Alıcılar UA aracılığıyla MS'ye yazılan mesajlara erişim sağlar. Mesajın MS ile UA arasında taşınması sırasında en çok Posta Ofis Protokolü (Post Office Protocol-POP) veya İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol-IMAP) kullanılmaktadır.

1.2.2.4 Adres ve mesaj yapısı

Bu kısımda elektronik posta veya mesajlaşma sistemlerinde kullanılan adres ve mesaj yapısı ITU ve elektronik posta standartları kapsamında ele alınacaktır.

1.2.2.4.1 Adres yapısı

İnternette yaygın olarak kullanılan elektronik posta sistemleri RFC 5322'de (Resnick, 2008) belirtilen adres yapısını kullanmaktadırlar. Genellikle elektronik posta aktarımı için SMTP kullanan elektronik posta sistemlerinde de kullanılan bu adres yapısı alışık olduğumuz üzere "ad.soyad@bolum.kurum.tr" şeklindedir.

X.400'de ise ITU-T X.500 (ISO/IEC, 2008) serisinde tanımlanan rehber yapısı kullanılır. Bu yapıda adres bileşenleri G=ad, S=soyad, OU=Bölüm, O=Kurum, C=TR şeklinde yer almaktadır.

Bahse konu adresleme yapıları tekil, hiyerarşik ve bileşen tabanlı bir adresleme sağlamaktadır.

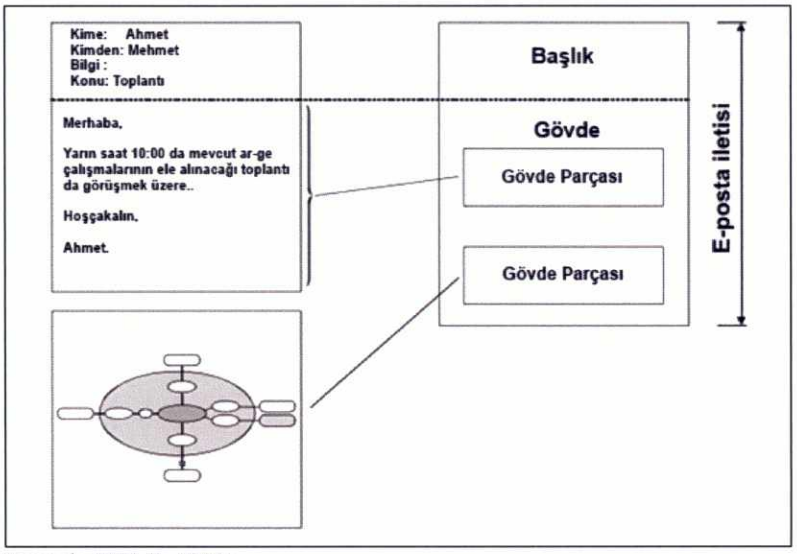
---

[3] E-posta sisteminin doğru çalışabilmesi için isim çözümleme sistemi olan DNS'ten bir e-postanın hangi adrese teslim edileceği bilgisinin elde edilmesi gerekir. Bu kayıtlar da DNS'te MX kayıtlarında tutulur. Örneğin; btk.gov.tr alan adına sahip bir e-postanın nereye teslim edileceği bilgisi bu kayıtlarda bulunmaktadır.

1.2.2.4.2 Mesaj yapısı

X.400 (ITU-T, 1999a) ve Resnick (2008)'e göre bir e-posta mesajı, mesaj başlığı ve mesaj içeriği olmak üzere iki kısımdan oluşmaktadır (Bkz. Şekil 1.5).

Şekil 1.5. Elektronik posta mesaj yapısı



Kaynak: ITU-T, 1999a

1.2.2.4.2.1 Mesaj başlığı

MTS tarafından kullanılan mesaj başlığı, mesajın doğru bir şekilde iletimi için gerekli bilgileri içerir. Mesaj başlığı içerisinde gönderici ve alıcı bilgileri ile birlikte MTA'lar tarafından, mesajın iletimi için eklenen gerekli bilgiler bulunmaktadır.

Mesaj başlığında her bilgiye tek bir satır şeklinde yer verilmekte ve kullanılan alanın adı, ':' karakteri ve sonra ilgili alanın değeri bulunmaktadır. Mesaj başlığında bulunan temel alanlar aşağıdaki şekildedir (Bautts vd., 2005; Resnick, 2008; Önal, 2009; Oppliger, 2014).

- **Gönderen (From):** Elektronik postanın kimden geldiğini gösteren başlık alanıdır. Standart elektronik posta'da çok kolay taklit edilebilen bir alan olduğundan güvenilirliği en az olan başlık alanıdır.

- **Alıcı (To):** Elektronik postanın kime gönderildiği bilgisini taşımaktadır.
- **Konu (Subject):** Elektronik postanın konusunu içermektedir.
- **Cevap Adresi (Reply-To):** Mesaja ilişkin cevabın hangi adrese gönderileceğini bildirmektedir.
- **Cevabın Ait Olduğu Mesaj (In-Reply-To):** Mesajın hangi mesaj veya mesajların cevabı olduğunu belirtmek üzere kullanılmaktadır. Bu alanda cevabın ait olduğu mesaj veya mesajların belirteçleri bulunmaktadır.
- **Geri Dönüş Yolu (Return-path):** Mesajın taşınması ve iletilmesi sırasında oluşan hata ve bilgilendirme mesajlarının hangi adrese gideceğini belirtmektedir.
- **Alındı (Recieved):** Gönderici ile MTA, MTA ile MTA arasındaki iletişim sırasında görev alan sunucu bilgilerini tutmaktadır. Elektronik postayı teslim alan bütün MTA'lar, mesaja bir alındı başlığı eklediğinden bu alan aşağıdan yukarıya takip edilerek gönderilen elektronik postanın hangi MTA'lardan geçtiği belirlenebilmektedir.
- **Mesaj Numarası (Message ID):** Elektronik postanın ilk çıktığı sistem tarafından oluşturulan ve her mesaj için tekil üretilen özel bir numaradır.
- **Tarih (Date):** Mesajın gönderildiği tarih bilgisini içermektedir.
- **X-Anything:** Bu alanın sistemlere özgü bazı ek ihtiyaçları karşılamak üzere kullanılacak bilgileri içermesi öngörüldüğünden bu alan hiçbir standartta tanımlanmamıştır.

Mesaj başlığında zorunlu olarak bulunması gerekli olan başlık alanları mesajın oluşturulma tarihi, gönderenin elektronik posta adresi ve alıcı elektronik posta adresi şeklindedir. Diğer alanlar isteğe bağlı olarak kullanılmaktadır (Resnick, 2008).

1.2.2.4.2.2 Mesaj içeriği

Mesaj içeriği asıl olarak iletilmek istenen mesaj ve eklerden oluşur (Turner ve Housley, 2008). Mesaj içeriği RFC 5322'de tanımlandığı üzere 7-bit ASCII karakterlerinden oluşmaktadır. Fakat bu şekildeki bir yapı, , metin tabanlı olmayan veya ASCII karakterlerden oluşmayan mesajların gönderilmesi ve birbirinden

bağımsız parçalardan oluşan mesajların iletilmesi gibi iki temel ihtiyaca cevap verememektedir. Bu sebeple ASCII karakterlerinden oluşmayan resim, video gibi farklı türdeki verilerin taşınması ve bağımsız bölümlerden oluşan mesajların kullanılabilmesi için Çok Amaçlı İnternet Posta Eklentileri (Multipurpose Internet Mail Extensions-MIME) geliştirilmiştir (Oppliger, 2014).

MTS mesajın aktarımı sırasında mesajın içeriği ile ilgilenmez ve bu içeriği değiştirmez. Bunun tek istisnası MTS'nin, mesaj içeriğini farklı kodlama biçimlerine dönüştürmesidir. Bu özellik sayesinde mesajın değişik kodlama biçimlerini destekleyen cihaz ve ortamlarda düzgün görüntülenme imkânı sağlanmaktadır. Bu sayede mesaj alıcının kullandığı ortamın yetenek ve özelliğine göre dönüştürülmüş olmaktadır (ITU-T, 1999a).

1.2.2.4.3 MIME

MIME elektronik posta uygulamaları aracılığıyla gönderilecek olan iletiye çeşitli türdeki içeriği eklemek için kullanılan bir internet standardıdır. MIME, SMTP'yi hem metin hem de metin olmayan (ses, görüntü, uygulama programlar gibi) birden çok içerik eklenebilecek şekilde genişletmektedir. Yani MIME, elektronik posta iletilerine resim, ses, görüntü türünde veriler eklenebilir hale gelmiştir. Diğer taraftan MIME, herhangi bir güvenlik özelliği getirmemektedir (Tracy vd., 2007; Turner ve Housley, 2008; Turner, 2010).

MIME, aşağıda listelenen dört temel özelliği içermektedir (Freed ve Borenstein, 1996; Turner ve Housley, 2008).

- Sadece US-ASCII karakterlerini göndermek üzere tasarlanan yapı diğer dilleri içerecek şekilde genişletilmektedir. Yani metin olan mesaj gövdelerinde US-ASCII karakterleri dışındaki karakterlerin de yer almasını sağlamaktadır.
- Metin olmayan ve mesaj gövdesinde yer alan içeriklerin taşınabilmesine olanak sağlamaktadır.
- Çok parçalı mesaj gövdesinin oluşturulabilmesine olanak sağlamaktadır.

- US-ASCII olmayan karakterlerin mesaj başlıklarında yer alabilmesini sağlamaktadır.

MIME, elektronik posta mesaj başlığına bir takım alanlar eklemek suretiyle gerçekleştirilmektedir. Elektronik posta mesajının oluşturulma aşamasında eklenen bu başlık bilgileri ile alıcı tarafta mesajın yorumlanması ve anlamlandırılması sağlanabilmektedir.

1.2.3 Elektronik posta protokolleri

Bilgisayarlar arası veri iletişimi protokol adı verilen standartlaştırılmış bir takım kurallar bütünüyle gerçekleştirilmektedir. Bu protokolleri oluşturan standartların ve kuralların temel amacı farklı özellik ve çalışma mimarisine sahip ortamların veya ürünlerin birbirleriyle uyumlu olarak çalışmasının sağlanmasıdır (Öztürk, 2009).

Çeşitli elektronik posta uygulamaları arasında güvenilirlik ve birlikte çalışabilirliği sağlamak üzere SMTP, POP, IMAP gibi elektronik posta protokolleri oluşturulmuştur.

1.2.3.1 SMTP

SMTP, 1982 yılında Jon Postel tarafından geliştirilmiş ve RFC 821 ile tanımlanmıştır (Postel, 1982). Bu protokol, 2001 yılında RFC-2821'in (Klensin, 2001) yayımlanması ile birlikte son halini almıştır. Protokolün amacı mesajların aktarımının daha güvenli ve verimli olarak gerçekleştirilmesi olarak tanımlanmıştır (Postel, 1982).

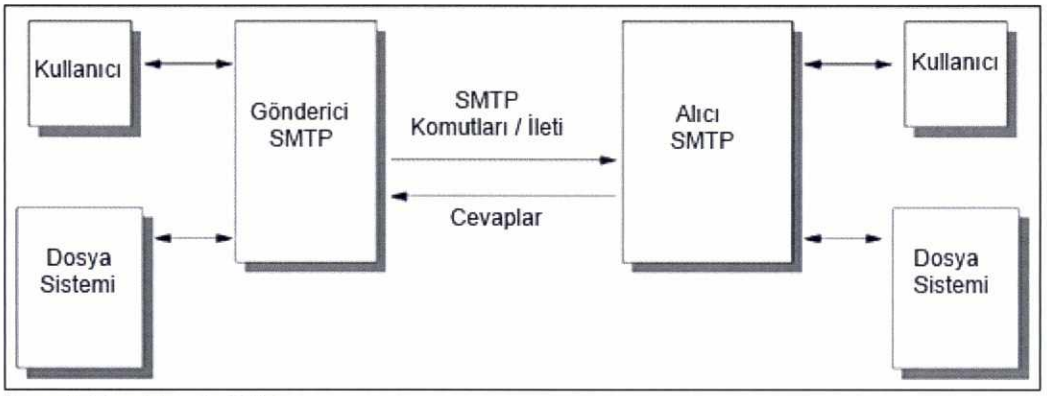
En yaygın olarak kullanılan elektronik posta aktarım protokolü SMTP'dir. SMTP protokolünün IP tabanlı iletişim ağlarında "de-facto" olarak benimsenmiş olması, geliştirilmekte olan elektronik posta uygulamalarının da bu protokolü destekleme zorunluluğunu beraberinde getirmiştir. Bu şekilde farklı işleyiş ve özelliklere sahip MTA'ların birlikte çalışabilirlikleri de sağlanabilmektedir. Diğer taraftan bu protokolü desteklemeyen ve farklı bir aktarım protokolünü çalıştıran MTA'lar sadece kendi içinde çalışabilen sistemler olarak yerel düzeyde kalmaktadırlar (Tracy vd., 2007).

SMTP ile veri iletişiminde SMTP komutları kullanılmaktadır. İstemci, sunucuya SMTP komutları göndermekte ve sunucu, istemci tarafından gönderilen ilgili komuta karşılık bir cevap vermek suretiyle protokol işletilmektedir.

Bir elektronik posta iletişiminde gönderici tarafta bulunan MTA, SMTP istemcisi, alıcı tarafta bulunan MTA ise SMTP sunucusu olarak adlandırılmaktadır.

SMTP istemcisi TCP portu üzerinden SMTP sunucusuna bağlantı sağladıktan sonra SMTP protokolü çalışmaya başlamak üzere hazır hale gelmiş olur (Oppliger, 2014). Bahse konu bağlantının kurulmasını müteakip SMTP komutları gönderilir ve bunların cevapları alınmak suretiyle iletişim gerçekleştirilir (Parziale vd., 2006; Comer, 2008).

Şekil 1.6. SMTP çalışma modeli



Kaynak: Parziale vd., 2006

1.2.3.2 POP

POP, elektronik posta sunucusu üzerindeki posta kutusunda saklanan iletilerin istemciye kopyalanma işlemlerini gerçekleştirmek üzere tanımlanan kuralları içeren bir elektronik posta alma protokolüdür. 1984 yılında geliştirilen ve hali hazırda POP3 olarak adlandırılan üçüncü sürüm RFC 1939'da detaylandırılmaktadır (Myers ve Rose, 1996).

POP'da sunucu ile istemci arasındaki iletişim, SMTP'ye benzer şekilde bağlantının sağlanması ve komutların gönderilerek cevapların alınması esasına göre sürdürülmektedir. (Kozierok, 2005).

Bu protokolde sunucu üzerindeki posta kutusundan mesaj çekildiğinde sunucu üzerindeki kopya da silinmekte ve bir başka yerden tekrar elektronik postalara erişim mümkün olamamaktadır. Bu nedenle kullanıcıların eriştikleri mesajları arşivlemesi ve elektronik postaların yerel diskler üzerinde yönetilmesi gerekliliği bulunduğu söylenebilir (Tracy vd., 2007).

1.2.3.3 IMAP

IMAP elektronik postaların kullanıcı tarafından arşivlenmesi zorunluluğunu ortadan kaldırmak ve merkezi olarak konumlandırılan sunucu üzerindeki posta kutusuna farklı istemci ve UA'lar kullanarak tekrar erişebilme özelliğini getirmek üzere geliştirilmiştir (Collings ve Wall, 2005). İlk olarak 1988 yılında geliştirilen ve günümüzde dördüncü sürümü kullanılan IMAP RFC 3501'de tanımlanmaktadır (Crispin, 2003).

IMAP temel olarak sunucu üzerinde mesajların yönetilebilmesi esasına dayanmaktadır. Ayrıca kullanıcıların, mesajların bir kopyasını yerel bilgisayar üzerinde oluşturmasına ve hem sunucuya bağlı iken hem de yerel düzeyde değişiklik yapmasına olanak sağlaması IMAP'in en önemli avantajı olarak ön plana çıkmaktadır (Parziale vd., 2006).

IMAP'de üç temel çalışma modeli bulunmaktadır. Bunlardan çevrim dışı olarak adlandırılan model POP ile aynı şekilde çalışmaktadır. Çevrim içi olarak adlandırılan modelde ise istemci sunucuya bağlanarak mesajlar üzerindeki tüm değişiklikleri sununucu üzerinde yapmaktadır. Son olarak bağlantısız (*disconnected*) olarak adlandırılan model ise çevrim içi ve çevrim dışı modellerinin karışımı şeklindedir. Bu modelde mesajın bir kopyası yerel dizine de alınmakta ve değişiklikler ister çevrim içi iken yapılsın ister çevrim dışı iken yapılsın asenkron olarak iki tarafa da

yansıtılmaktadır. Bu protokolde bulunan komut sayısı ve çeşitliliği POP'a göre oldukça fazladır.

1.2.4 Elektronik posta güvenlik servisleri

Gönderici ve alıcı arasında bir mesaj gönderimi ve alımı söz konusu olduğundan, bu iletişime yönelik potansiyel bazı tehditler söz konusu olmakta ve bu tehditlere karşı birtakım güvenlik yaklaşımları ortaya konmaktadır.

1.2.4.1 Tehditler

MHS'ye yönelik tehditler genel olarak aşağıdaki gibi tanımlanmaktadırlar (ITU-T, 1999a).

- **Erişime ilişkin tehditler:** Yetkisiz bir kullanıcının sisteme bağlanabilmesi alınabilecek tüm güvenlik önlemlerini geçersiz kılacağından geçersiz ve yetkisiz erişim temel bir tehdit olarak tanımlanmaktadır.
- **Araya girme tehditleri:** Sahte kullanıcı oluşturulması, mesaj değiştirme, yeniden mesaj gönderme (*replay attack*) ve aradaki trafiğin analiz edilmesi gibi yöntemler ile mesajlaşmaya ilişkin, mesajlaşan taraflar dışında bir taraftan gelebilecek tehditlerdir.
- **Mesajlaşmanın taraflarından gelebilecek tehditler:** Mesajlaşmanın gerçek ve yetkilendirilmiş taraflarından kaynaklanan bu tehditler gerek mesajın göndericisinin gerekse alıcısının mesajı gönderdiğini veya aldığını inkâr etmesi şeklinde gerçekleşebilmektedir. Mesajın gönderiminin veya alımının inkârı MHS kullanılarak yapılan iş ve işlemlere ilişkin ciddi problemlere yol açmaktadır.
- **Saklanan verilere yönelik tehditler:** Yönlendirme bilgilerinin değiştirilmesi ve teslim edilmek üzere MTA'da bekleyen iletilerin kopyalanması ve/veya tekrar gönderilmesi şeklindeki tehditler bu kategori içerisinde değerlendirilmektedir.

1.2.4.2 Güvenlik unsurları

X.400'de bir önceki başlık altında açıklanan MHS sistemine yönelik tehditlere ilişkin bir takım güvenlik unsurlarına yer verilmektedir. Güvenliğin sağlanması için gerekli olan bu unsurlardan KEP ile ilgili olanları bu başlık altında ele alınmaya çalışılacaktır.

X.400, mesajlaşmanın yanı sıra, mesajın kabul edilmesi ve teslim edilmesine ilişkin raporlamaları da desteklemektedir (ITU-T, 1999a). Ancak bu raporlamalar herhangi bir güvenlik süzgecinden geçirilmemektedir (Tauber, 2012). Tablo 1.1'de bu güvenlik servislerinden KEP'e ilişkin olanlarına yer verilmektedir.

Tablo 1.1. KEP ile ilgili X.400 güvenlik özellikleri

Güvenlik Servisi	**Gönderici**	**MTS**	**Alıcı**
Mesaj kaynağının kimlik doğrulaması	S	K	K
Raporların kaynağının kimlik doğrulaması	K	S	-
Teslim kanıtı	K	-	S
Gönderim kanıtı	K	S	-
İçerik bütünlüğü	S	-	K
İçerik gizliliği	S	-	K
Mesaj akış gizliliği	S	-	-
Kaynağın inkâr edilemezliği	S	-	K
Gönderimin inkâr edilemezliği	K	S	-
Teslimin inkâr edilemezliği	K	-	S
S: MHS bileşeni bu servisi sağlamaktadır. K: MHS bileşeni bu servisi kullanmaktadır.			

Kaynak: ITU-T, 1999a ve Tauber, 2012

ITU-T'de Tablo 2.2'de verilen bu güvenlik servislerinin açıklamaları şu şekilde yer almaktadır (1999a).

- **Mesaj kaynağının kimlik doğrulaması (*message origin authentication*) :** Alıcı MTA veya mesajın üzerinden geçtiği herhangi bir MTA için, mesajın göndericisinin kimliğininin doğrulanmasını sağlamaktadır.

- **Raporların kaynağının kimlik doğrulaması (*report origin authentication*):** Mesajın teslim edilip edilmediğine ilişkin göndericiye gelen raporların kaynağının kimlik doğrulamasının yapılmasını sağlamaktadır.
- **Teslim kanıtı (*proof of delivery*):** Mesajın göndericisine, ilgili mesajın MTS tarafından, alıcısı veya alıcılarına teslim edildiğine ilişkin kanıt sağlamaktadır.
- **Gönderim kanıtı (*proof of submission*):** Mesajın göndericisine, ilgili mesajın alıcısı veya alıcılarına teslim edilmek üzere, MTS tarafından teslim alındığına ilişkin kanıt sağlamaktadır.
- **İçeriğin bütünlüğü (*content integrity*):** Gönderilen mesajın orijinal içeriğinin değiştirilip değiştirilmediğinin alıcı tarafından kontrolünü sağlamaktadır.
- **İçeriğin gizliliği (*content confidentiality*):** Gönderilen mesajın içeriğine, gönderici ve alıcı dışındaki yetkisiz üçüncü taraflarca erişilememesini sağlamaktadır.
- **Mesaj akış gizliliği (*message flow confidentiality*):** Mesajın göndericisine mesajın MHS üzerindeki akışının gizliliğini sağlamak üzere imkân sunmaktadır. Mesajın akışı ile ilgili bilgilerin sadece ilgili gönderici ve alıcıda olmasını sağlamaktadır.
- **Kaynağın inkâr edilemezliği (*non-repudiation of origin*):** Mesajın alıcısı veya alıcılarına, mesajın göndericisinin kimliğine ve mesajın içeriğine ilişkin değiştirilemez kanıt sağlamaktadır.
- **Gönderimin inkâr edilemezliği (*non-repudiation of submission*):** Mesajın göndericisine, mesajın, alıcı veya alıcılara teslim edilmek üzere MTS tarafından teslim alındığına ilişkin değiştirilemez kanıt sağlamaktadır.
- **Teslimin inkâr edilemezliği (*non-repudiation of delivery*):** Mesajın göndericisine, mesajın, alıcı veya alıcılara teslim edildiğine ilişkin değiştirilemez kanıt sağlamaktadır.

1.2.5 Güvenli ve güvenilir elektronik posta yaklaşımları

Elektronik posta temel olarak iletim ile ilgilenmekte ve taraflara herhangi bir güvenlik taahhüt etmemektedir. Elektronik postada gizlilik, bütünlük, güvenilirlik ve

izlenebilirlik gibi temel güvenlik özellikleri olabileceği gibi, iletime ilişkin kanıt sağlayan KEP özellikleri de olabilmektedir.

Tasarlanan elektronik posta protokollerinde bulunan kanıt eksikliğinden dolayı, birçok gönderim ve alım mekanizmaları geliştirilmiş ve kullanılagelmiştir. Bu bölümde öncelikle gizlilik, bütünlük ve güvenilirlik gibi özellikleri sağlamak üzere tasarlanan güvenlik protokollerinden bahsedilecektir. Sonrasında ise bu protokollerin eksik kalan noktaları açıklanacak ve bu protokollerin KEP'te sağlanan delil değerini haiz olamadıkları ortaya konacaktır.

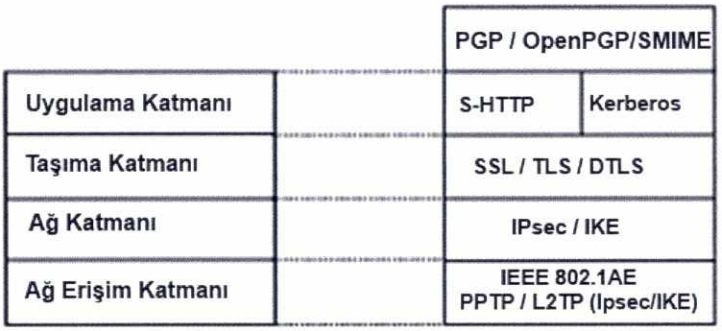
1.2.5.1 Elektronik posta güvenlik mekanizmaları

Elektronik postada gizlilik, bütünlük ve güvenilirlik özelliklerini sağlamak üzere bağlantı katmanını ilgilendiren ve bağlantının güvenliğini sağlamaya yönelik kısım ve gönderilen veriye mesajlaşmanın tarafları dışındaki üçüncü kişiler tarafından erişilmesini önlemek amacıyla kullanılan kısım olmak üzere iki farklı kısım bulunmaktadır (Bkz. Şekil 1.7).

Elektronik postanın güvenliği, hizmetin kullandığı haberleşme katmanının güvenliğiyle doğru orantılıdır. Mesajların taşınması esnasında gizlilik, Güvenli Yuva Katmanı (Secure Socket Layer-SSL) ve Taşıma Katmanı Güvenliği (Transport Layer Security-TLS) kullanılarak sağlanmaktadır.

Bununla birlikte, elektronik postanın gizlilik, bütünlük ve güvenilirlik özelliklerini kazanabilmesi amacıyla İnternet Mühendisliği Görev Gücü (Internet Engineering Task Force-IETF) tarafından standartlaştırılan ve RFC 5751 olarak yayımlanan (Ramsdell ve Turner, 2010) Güvenli/Çok Amaçlı İnternet Posta Eklentileri (Secure/Multipurpose Internet Mail Extensions-S/MIME) ve veri şifreleme/şifre çözme temellerine dayanan *Oldukça İyi Gizlilik* (Pretty Good Privacy-PGP) gibi bazı yöntemler kullanılmaktadır.

Şekil 1.7. Güvenlik yaklaşımları



Kaynak: Oppliger, 2009

1.2.5.1.1 Güvenli yuva katmanı

SSL, sunucu ve istemci arasında güvenli (şifreli) bir bağlantı kurmak için kullanılan TCP/IP tabanlı bir güvenlik protokolüdür. Protokolün temel işlevi iletişimin gerçekleştirildiği uçlar arasında özel bir kanal oluşturarak tarafların kimliklerinin denetimini, taraflar arasında gönderilen ve alınan verilerin gizliliğini ve bütünlüğü sağlamaktır (Oppliger, 2009).

İlk olarak Netscape firmasının 1993 yılında geliştirdiği protokolün üçüncü sürümü IETF tarafından iletişim güvenliği standardı olarak RFC 6101 yayımlanmıştır (Freier, 2011).

SSL'in çalışma mantığı, istemci ve sunucunun kullanılacak olan şifreleme algoritmaları üzerinde mutabakata varması üzerinde anlaşılan Açık Anahtarlı Altyapı (AAA) kullanılarak anahtar değişiminin ve sertifika doğrulamasının gerçekleştirilmesi ve bir önceki adımda elde edilen anahtar ile verilerin şifreli bir biçimde karşı tarafa aktarılması olmak üzere temelde 3 adımdan oluşmaktadır (Akleylek vd., 2011a). Bu üç adım sayesinde sunucu ve istemci arasında güvenli bir bağlantı tesis edilir. Bu aşamadan sonra istemci ve sunucu arasındaki veriler şifrelenmiş olarak gönderildiğinden ve alındığından gizlilik sağlanmış olmaktadır (Oppliger, 2009; Şimşek, 2012; Özel, 2013).

Ancak SSL ve TLS gibi protokoller sadece "noktadan noktaya" güvenlik sağlamaktadır. Birden fazla noktadan oluşan herhangi bir iletişim, bu yol üzerinde yer alan ve iletişimde bulunan noktalar arasında ayrı birer güvenli kanal kurulmasını gerektirmektedir (Urgun, 2007).

1.2.5.1.2 Taşıma katmanı güvenliği

Temelde SSL'e çok benzeyen bir yapıya sahip olan TLS protokolü, SSL'in aksine açık kaynak (*open source*) bir uygulama olarak ortaya çıkmıştır. İlk sürümü IETF tarafından TLS standardı olarak RFC-2246 ile yayınlanmıştır (Dierks ve Allen, 1999).

SSL'e benzer şekilde iki taraf arasındaki iletişimin şifrelenmesi suretiyle gizlilik ve bütünlüğü sağlamaya yönelik bir protokol olan TLS'in birinci sürümü ile SSL'in üçüncü sürümü hemen hemen aynı özelliklere sahiptir. TLS başlangıçta sadece Hiper Metin Transfer Protokolü (Hyper-Text Transfer Protocol-HTTP) trafiğini şifreleme amacıyla geliştirilmiş olsa da günümüzde TCP/IP tabanlı tüm servisleri şifreleme amaçlı kullanılmaktadır.

1.2.5.1.3 S/MIME

S/MIME güvenli elektronik posta iletişimi ve gönderilecek olan iletiye çeşitli türdeki içeriği güvenli bir şekilde eklemek için kullanılan bir internet standardıdır. S/MIME, bir elektronik posta içeriğinin nasıl düzenlenmesi gerektiğini belirten standart bir format içermektedir.

S/MIME, standart elektronik posta yapısına, sayısal imza ve şifreleme özelliklerinin eklenmiş halidir. Sayısal imza ile göndericinin kimliğinin inkâr edilemez bir şekilde tespiti ve mesaj içeriğinin bütünlüğünün korunması gerçekleştirilmektedir. Şifreleme ile mesaj içeriğine, ilgili taraflar dışında üçüncü kişilerin erişimi engellenmektedir. Ayrıca yine şifreleme ile bütünlük de sağlanabilmektedir. Böylelikle bir S/MIME mesajında digital imza ile göndericinin kimlik doğrulaması, mesaj kaynağının inkâr edilemezliği ve içeriğin bütünlüğü sağlanırken, şifreleme ile de içeriğin gizliliği sağlanmaktadır.

İmzalı bir S/MIME mesajı, mesaj içeriği ile başlık bilgileri ve imzanın doğrulanmasına ilişkin bilgiler olmak üzere iki MIME bölümünden oluşmaktadır (Turner, 2010). S/MIME yapısında şifrelenmiş mesaj da mesajın şifresini çözmek üzere kullanılacak bilgiler ve şifreli veri olmak üzere iki bölümden oluşmaktadır. S/MIME şifreleme işlemleri Kriptografik Mesaj Sözdizimi (Cryptographic Message Syntax-CMS) standardı (Housley, 2009) kullanılarak gerçekleştirilmektedir (Tauber, 2012).

1.2.5.1.4 PGP

Elektronik posta güvenliğini sağlamanın en önemli yollarından birisi posta içeriğindeki mesajların şifrelenmesidir. PGP; dosya imzalama, metin, dosya, hard disk ve dizin şifreleme gibi kullanım alanlarının yanı sıra elektronik posta şifrelemede de yaygın olarak kullanılmaktadır. PGP, veri iletişimi için kimlik doğrulama ve mahremiyeti sağlayan bir veri şifreleme ve şifre çözme yöntemidir (Poşul ve Aksoy, 2013). Günümüzde daha çok güvenli elektronik posta iletişimi için kullanılan PGP ile elektronik postaların imzalanıp şifrelenmeleri de mümkündür. Böylece şifrelenen elektronik postanın alıcısı hariç yetkisiz kişiler tarafından görülmesi engellenebilmektedir. PGP kullanımının diğer avantajı ise, kimlik denetiminin yapılmasıdır (Eryol, 2007). Elektronik posta üzerinde bulunan dijital imza vasıtasıyla kimlik doğrulama ve kaynağın inkâr edilemezliği özellikleri de sağlanmaktadır. PGP'ye alternatif ve benzer OpenPGP (Callas vd., 2007) gibi protokoller de geliştirilmiştir.

PGP kullanarak elektronik posta şifrelemede, gönderici, elektronik postanın içeriğini alıcının açık anahtarıyla şifreler ve alıcısına gönderir. Alıcı da kendi özel anahtarı ile göndericiden gelen şifreli metni çözer. Bu çözme işlemi yalnızca elektronik postanın alıcısı konumundaki kişi tarafından yapılabilmektedir (Poşul ve Aksoy, 2013).

PGP'de her kullanıcı kendisi için bir anahtar çifti üretir ve bu anahtarlardan açık anahtarı herkese açık bir açık anahtar deposunda veya web sayfasında yayımlar. Bu yapı üzerinde herhangi bir güvenilir üçüncü taraf (Trusted Third Party-TTP)

bulunmamakta ve bir kullanıcı başka bir kullanıcıyı doğrulayabilmektedir. Dolayısıyla güvenip güvenmeyeceği kişileri de seçebilmektedir (Taşkın ve Demircioğlu, 2014).

1.2.5.2 Elektronik posta alındı kayıtları

S/MIME ve PGP kullanımı ile gizlilik, bütünlük ve kimlik doğrulama gibi temel özellikler sağlanıyor olsa da gönderinin alıcısına ulaşıp ulaşmadığı veya alıcısı tarafından görülüp görülmediğine ilişkin bir delil sağlanamamaktadır. Bu eksikliğin giderilebilmesi ve alındı kayıtlarının üretilebilmesi amacıyla Mesaj Devir Bildirimleri (Message Disposition Notifications-MDNs), Teslim Durum Bildirimleri (Delivery Status Notifications-DSNs), mesaj takibi için SMTP servis eklentileri ve S/MIME alındı bildirimleri olmak üzere dört farklı mekanizma geliştirilmiştir.

1.2.5.2.1 Mesaj devir bildirimleri

MDN, elektronik postanın alıcısı tarafından üretilen bir bilgilendirme mesajıdır. Bir MDN mesajı gönderinin alıcısına teslim edildiğine ilişkin bilgi taşımaktadır. Ayrıca bu mesaj içerisinde, alınan mesaja ilişkin bazı hata bilgileri gibi verilere de yer verilebilmektedir.

Gönderici alıcıdan MDN mesajını talep etmek için gönderdiği iletinin başlık kısmına "*Disposition-Notification-To*" etiketini ekler. Alıcı ise bu mesajı aldığında mesajın teslim durumuna ilişkin bir MDN mesajı oluşturup göndericiye geri gönderir. MDN mesajları okunabilir şekilde bulunan ve gönderilen MDN raporunun bilgileri, göndericinin elektronik posta arabirimi tarafından okunacak olan bilgileri ve isteğe bağlı olan orijinal mesajın kendisi olmak üzere üç MIME bölümünden oluşmaktadır (Hansen ve Vaudreuil, 2004).

MDN mesaj yapısı ve çalışma mantığı elektronik posta alma protokollerinden POP3 için RFC 3798'de (Hansen ve Vaudreuil, 2004), IMAP için ise RFC 3503'te (Melnikov, 2003) standartlaştırılmıştır.

MDN, alıcı tarafından üretilerek göndericiye gönderilen MDN iletilerinin kimlik doğrulaması ve bütünlüğü üzerine herhangi bir güvenlik özelliği içermemektedir. Bu nedenle internet topluluğu tarafından Uygulanabilirlik Bildirimi (Applicability Statement-AS) olarak bilinen ve yapısal verilerin, XML verilerinin ve diğer verilerin güvenli bir şekilde taraflar arasında paylaşımını ele alan üç güvenli MDN mekanizması yayımlanmıştır. Yayımlanan üç AS standardında da MDN, temel "alındı üretme mekanizması" olarak kullanılmaktadır.

Bununla birlikte, AS kullanıldığında MDN cevaplarının imzalanması ve bu cevaplarda teslim alınan orijinal iletinin özet (*hash*) değerinin bulunması suretiyle alındı raporunun bütünlüğü, kimlik doğrulaması ve orijinal iletinin gerçekten doğru bir şekilde iletilip iletilmediği kontrol edilebilmektedir.

1.2.5.2.2 SMTP teslim durum bildirimleri

SMTP'nin sunduğu DSN hizmeti ile göndericilerin mesajın teslim durumuna ilişkin bilgi sahibi olmaları sağlanmaktadır.

Herhangi bir hata halinde üretilen teslim durum bildirimi ise, teslim edilememe raporu (Non-Delivery Report/Receipt-NDR) veya teslim edilememe bildirimi (Non-Delivery Notification-NDN) olarak isimlendirilmektedir. Bu olumsuz bildirimlere genel olarak yansı (*bounce*) mesajları adı verilmektedir.

DSN ile ilgili birçok RFC yayımlanmıştır. Bunlar; DSN için SMTP servis eklentisini konu edinen RFC 3461 (Moore, 2003), çok parçalı MIME rapor ileti biçimlerini tanımlayan RFC 3462 (Vaudreuil, 2003a), teslim durum kodlarını belirleyen RFC 3463 (Vaudreuil, 2003b), mesaj formatını belirleyen RFC 3464 (Moore ve Vaudreuil, 2003) ve uluslararası elektronik posta adreslerini de destekleyen (özellikle ASCII olmayan karakterleri barındıran) DSN'yi konu edinen RFC 6533 (Hansen vd., 2012) şeklindedir.

Gönderici tarafından mesaj gönderilirken başarılı teslime ilişkin bildirimin talep edilmesi gerekmektedir. Ancak olumsuz bildirimler için böyle bir şart aranmamaktadır.

Mesajın teslim edilememesine ilişkin NDR veya yansı mesajları gibi olumsuz bildirimler hemen hemen tüm posta sunucularında bulunurken ve fiili olarak kullanılırken, olumlu durumlar için üretilmesi gereken DSN mesajları birçok elektronik posta uygulamasında kullanılmamaktadır.

1.2.5.2.3 SMTP servis eklentileri

RFC 3888'de (Hansen, 2004) DSN ve MDN mekanizmaları kullanılarak yapılan mesaj takip mekanizmaları tanımlanmaktadır. Ancak herhangi bir MTA, MDN ve DSN'yi desteklemeyebilmekte veya alıcı MDN mekanizmasını devre dışı bırakmış olabilmektedir. Bu gibi durumlarda mesajın durumuna ilişkin herhangi bir bilgi elde edilememektedir.

DSN ve MDN gibi mekanizmalar ile mesaj hakkında geri dönüş alınamadığı durumlar için IETF tarafından SMTP servis eklentisi adı verilen ek bir takip mekanizması geliştirilmiştir (Draper-Gil vd., 2014).

1.2.5.2.4 S/MIME alındı bildirimleri

S/MIME alındı bildirimi, bir elektronik postanın değişmeden alındığını tespit etmek amacıyla alındı onayı istemek için kullanılan bir elektronik posta güvenlik özelliğidir. S/MIME alındı bildirimleri RFC 2634 (Hoffman, 1999)'te tanımlanmaktadır.

S/MIME alındı bildirimi, göndericiye, iletinin teslimine ilişkin kanıt sunmasının yanında, alıcının ileti üzerindeki imzayı doğruladığını da göstermektedir. S/MIME alındı bildirimi performans kaygısı nedeniyle sadece göndericinin istemesi durumunda üretilmektedir. Yani gönderici orijinal mesajı gönderirken, S/MIME alındı mesajı istediğini belirtmemiş ise alıcı bu kaydı oluşturmamaktadır. Diğer taraftan göndericinin bu alındı kaydını istemesi de tek başına yeterli değildir. Alıcının (veya

alıcının UA'sının) gönderici tarafından gönderilen bu isteği işlemesi ve ilgili alındı kaydını oluşturarak göndericiye göndermesi gerekmektedir. Bu da her zaman mümkün olmamaktadır (Draper-Gil vd., 2014).

1.2.5.2.5 Değerlendirme

Günümüzde hali hazırda kullanılan amacıyla MDNs, DSNs, SMTP servis eklentileri ve S/MIME alındı bildirimleri olmak üzere dört faklı mekanizma genel hatlarıyla incelenmeye çalışılmıştır. Bu mekanizmalar standart elektronik postaya bazı güvenlik özellikleri ekleseler de henüz ispat gücünü haiz güvenilir bir mekanizma tesis edememişlerdir. Aynı zamanda bu mekanizmaların hiçbirisinde alıcının bu mesajları dikkate alacağı ve üreteceği de garanti edilememektedir. Çünkü bahse konu mekanizmaların tamamında gönderici alındı onaylarını talep etmekte ve alıcının istenen alındı mesajını göndermesini beklemektedir. Yani gönderici, alıcının adaletli ve dürüstçe davranacağını varsaymak zorunda kalmaktadır. Bu varsayım ise internet ortamında özellikle de önemli ve hukuki sonuçlar doğurabilecek gönderimler söz konusu olduğunda kabul edilebilir değildir.

Ayrıca S/MIME alındı bildirimleri hariç diğer üç yöntemde de alındının teyidi veya mesajın takibine ilişkin kriptografik bir teknoloji kullanılmamaktadır.

Bununla birlikte MDN'nin anlatıldığı standartta, MDN'nin sağlamış olduğu teslim kanıtının inkâr edilemezlik sağlamayacağı açıkça belirtilmiştir (Hansen ve Vaudreuil, 2004). S/MIME alındı bildiriminde de her ne kadar gizlilik, bütünlük ve kimlik doğrulama mekanizmaları bulunsa da, geri bildirimin göndericiye gönderilmesi tercihinin alıcıya bırakılması inkâr edilemezliğin tam olarak karşılanmadığını ortaya koymaktadır. Yani S/MIME alındı bildiriminde de alıcı mesajı aldığını reddedebilme imkânına sahiptir.

Hali hazırda kullanılan Microsoft Outlook, Thunderbird gibi birçok ürün tarafından yukarıda anılan mekanizmalar desteklenmeye başlamıştır. Ancak MDN, DSN ve diğer mesaj takip mekanizmaları çok yoğun kullanıldığında doğru çalışmama gibi bazı

problemlerle karşılaşılabilmektir. Bu nedenle gerçekleştirilen çözümler birlikte çalışabilir ve güvenilir olmaktan uzaktır (Oppliger, 2007).

Ayrıca tüm bu ek güvenlik getiren mekanizmaların hayat bulabilmesi için yapısal değişiklikler yapılması ve mesajın iletim aşamasında bulunan ve bu mesajları yorumlaması gereken her bir bileşenin bu mesajları yorumlayabilecek şekilde değiştirilmeleri gerekmektedir. Bu yapısal değişiklikler gerçekleştirilse ve bahse konu mekanizmalar uygulanabilir hale getirilse bile internetin açık ve heterojen bir yapıda olması, henüz uygun kriptografik teknolojiler kullanılamadığından mesajların taklit/tahrif edilebilecek olması nedeniyle inkar edilemezlik sağlanamamaktadır (Tauber, 2012; Draper-Gil vd., 2014). Bununla birlikte inkâr edilemezliğin sağlanabilmesi için henüz standart olarak kullanılmayan dijital imzanın özel bir şekilde ele alınması gerekmektedir (Oppliger, 2007).

2. KAYITLI ELEKTRONİK POSTA

Elektronik posta için, bir dizi standart ve tavsiyede mesaj takip mekanizmalarına yer verilmiş olsa bile, bu mekanizmalar elektronik postaya fiziki kayıtlı posta ile eş değer delil sağlama özelliklerini kazandırmamaktadır.

Bu bölümde elektronik postanın sahip olmadığı özelliklerden yola çıkılarak KEP sistemine ilişkin mevcut ihtiyaç ortaya konularak literatürde bulunan KEP özellik ve bileşenleri ele alınmaktadır.

2.1 Mevcut İhtiyaç

Elektronik posta ile yapılan bir iletişimde gönderici, alıcının iletiyi alıp almadığına veya iletiyi okuyup okuyamadığına ilişkin sağlıklı bir bilgi edinememektedir. Bununla birlikte elektronik posta iletişiminde kötü niyetli bir alıcının iletiyi almadığına ilişkin bir iddiada bulunması veya göndericinin de benzer şekilde iletiyi gönderdiğini reddedebilmesi mümkündür. Elektronik postada iletinin gizliliği, bütünlüğü ve güvenilirliğine ilişkin bir takım güvenlik özellikleri bulunmasına rağmen, gönderinin inkâr edilemezliği özelliğine halen ihtiyaç duyulmaktadır.

KEP, temelde geleneksel kayıtlı postaya benzer şekilde taraflar arasındaki iletişimin tüm adımlarını içerecek şekilde elektronik kayıtları oluşturan ve sunan bir sistemdir. Sistemde tüm işlem ve kayıtlar tamamen elektronik ortamdadır. Bununla birlikte bu işlemlerin ve kayıtların hukuki geçerliliği elektronik imza gibi mekanizmalar kullanılarak sağlanmaktadır. Dolayısıyla KEP sisteminde gönderici, KEPHS[1] ve alıcı arasındaki iletişimin tüm aşamalarına dair doğru, tam ve güvenilir kayıtlar oluşmaktadır. Standart bir elektronik posta ile karşılaştırıldığında, KEP sistemi kimlik doğrulamaları yapılmış kullanıcılar arasındaki gönderim, alım ve teslime ilişkin sunduğu kayıtlar vasıtasıyla güvenilir ve inkâr edilemez bir iletişim sağlamaktadır. Aynı zamanda KEP sisteminde bir gönderinin iletilmesi aşamalarındaki her bir adım güvenilir metodlarla kaydedildiğinden iletinin geçtiği adımların inkâr edilemez bir

[1] Bu bölümde KEPHS'ler genel anlamda TTP olarak anılacaktır.

biçimde kanıtlanabilmesi de mümkündür. Bu nedenle KEP geleneksel kayıtlı postanın elektronik ortamdaki hali olarak da tariflenebilmektedir.

KEP'e ilişkin ihtiyacın daha iyi ortaya konulabilmesi için geleneksel kayıtlı postadaki işleyişe kısaca göz atılmasında fayda bulunmaktadır. Fiziki kayıtlı posta temel olarak imzalı bir alındı kaydının üretilmesine dayanmaktadır. Fiziki ortamda, posta hizmet sağlayıcısı adına bir çalışan, kayıtlı posta gönderisini, alındı kâğıdını imzalatmadan teslim etmemektedir. Yani geleneksel kayıtlı postada alıcının alındı kaydını imzalaması gönderinin teslim edilebilmesi için bir ön koşul olarak tanımlanmıştır. Dolayısıyla teslim sırasında alınan bu imzalı alındının göndericiye ulaştırılması veya posta servis sağlayıcısında saklanması suretiyle oluşabilecek herhangi bir ihtilaf durumunda yeterli bir delil sağlamış olmaktadır. Bu imzalı alındı kaydının gerek göndericide gerekse posta hizmet sağlayıcısında bulunmasıyla aslında göndericinin alıcıya bir posta gönderdiği ve alıcının da gerçekten gönderilen o postayı aldığı kanıtlanmaktadır.

Genelde posta hizmet sağlayıcının çalışanları tarafından alındı kaydını imzalayan kişinin kimlik doğrulaması tam olarak yapılmamakta veya yapılamamaktadır. Aslında burada garanti edilen husus ilgili adrese teslimin gerçekleştirilmiş olmasıdır. Dolayısıyla bu durumda göndericinin bir adrese içeriği tam olarak bilinmeyen veya ispatlanamayan bir gönderiyi kesin olarak kimlik doğrulaması yapılmamış bir alıcıya gönderdiği kanıtlanmış olmaktadır.

Diğer taraftan fiziki olarak imzalanan bir belge ile o belgede bulunan imza arasında zayıf bir bağ olduğu söylenebilir. Bu nedenle aslında fiziki ortamın doğasında var olan içerik ile zayıf bir bağ ile bağlı olma sorunu geleneksel kayıtlı postada söz konusudur. Elektronik ortamda ise bir önceki bölümde detaylarıyla bahsedilen bir takım takip mekanizmalarıyla mesajın gizliliği, bütünlüğü ve tarafların kimliğinin doğrulanması hususlarına ilişkin bir takım çözümler getirilmiş olsa da geleneksel kayıtlı postada sağlanan "imzalı alındı belgesinin" yerini tutacak şekilde inkâr edilemez ve adil bir gönderim söz konusu olamamaktadır.

KEP'te genel manada gerekli olduğu hususunda görüş birliğine varılmış iki özellik göze çarpmaktadır. Bunlar adillik (*fairness)* ve inkâr edilemezliktir (Ferrer-Gomilla vd., 2010).

Adil bir delil elde edilmesi amacıyla fiziki gönderimde posta hizmet sağlayıcısı çalışanının imzalı alındı kaydı olmaksızın postayı teslim etmemesi, gerektiğinde bu imzalı alındı kaydını saklaması ve alıcıya iletmesi gerekmektedir. Bu şekilde posta hizmet sağlayıcısı bir nevi TTP olarak davranmakta ve gönderici ve alıcı arasındaki iletişimin bir tarafın lehine ya da aleyhine olmayacak şekilde yapılmasını sağlamaktadır. Diğer taraftan postanın teslimi sırasında alınan imzalı alındı kaydının göndericiye iletilmesi veya posta hizmet sağlayıcıda saklanması sayesinde alıcının ilgili gönderiyi almadığını iddia etmesinin önüne geçilmektedir. Hatta teslim sırasında alıcının kimliğinin uygun yöntemlerle tespiti sağlandığında adrese teslimin ispatının yanında bizzat ilgili kişiye teslim de inkâr edilemez bir şekilde ispat edilmiş olmaktadır (Tauber, 2012).

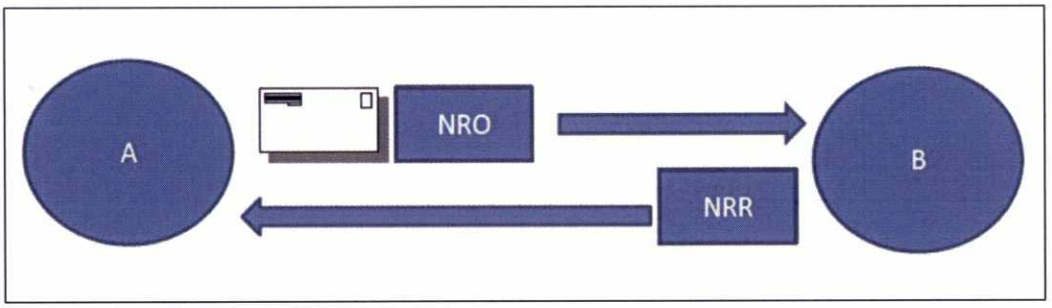
Son yıllarda fiziki ortamdaki özelliklerin elektronik ortama taşıma ve yeni özellikler bulma adına birçok çalışma yürütülmektedir. Ancak bu alanda yapılan çalışmalar incelendiğinde bir KEP sisteminin hangi özelliklere sahip olması gerektiği ve hangi ihtiyaçları karşılaması gerektiğine ilişkin çok farklı görüşler bulunduğu görülmektedir. Dolayısıyla birçok farklı KEP tanımı yapılabilmektedir.

2.2 KEP Nedir?

Ferrer-Gomilla vd.'ye göre KEP, mesaj gönderiminin yanı sıra inkâr edilemez alındı bildirimi (*Non-Repudiation of Receipt-NRR*) delili üretmek üzere mesajın kaynağının inkâr edilemezliğine (Non-repudiation of Origin-NRO) ilişkin de delil içeren sistem şeklinde tanımlanabilir (2000; 2010) (Bkz. Şekil 2.1). Diğer taraftan fiziki ortamdaki kayıtlı postanın genellikle mesajın kaynağına ilişkin bir delil sunmadığından hareketle ve KEP'in fiziki kayıtlı postanın elektronik ortamdaki karşılığı olduğu tezine dayanılarak KEP, mesaj alışverişinin sadece NRR delili üretilerek yapılması şeklinde de tanımlanmaktadır (Zhou ve Gollmann, 1996b).

KEP'te NRR delili mesaj içeriği ile ilişkilendirilebilmektedir. Yani üretilen NRR delilinin hangi mesaja ait olduğu delilin kendisine bakılarak anlaşılabilmektedir.

Şekil 2.1. KEP tanımı



Akleylek vd., 2011b

Ferrer-Gomilla vd. (2010) literatürde yer alan birçok tanıma yer vermektedir. Bu tanımlardaki ortak nokta KEP'in mesaj alışverişinin adil ve doğru bir şekilde yapılmasını sağlayan sistem olduğudur. Fakat adil bir mesaj alışverişi yanında hangi özellikleri sağlaması gerektiği konusunda bir görüş birliği bulunmadığı görülmektedir.

2.3 KEP Özellik ve Bileşenleri

Yapılan çalışmalar ve pratikte hayat bulan uygulamalarda bir görüş birliğine varılamamış olsa da bu başlık altında genel tanım ve ihtiyaçlardan yola çıkılarak literatürde karşılaşılan tüm KEP özellikleri ve bileşenleri ele alınmaya çalışılmıştır. Aynı zamanda bu özelliklerin pratik hayatta uygulanabilirliğine ve bir KEP sisteminde bulunmasının önemine ilişkin değerlendirmelere de yine bu bölümde yer verilmektedir.

2.3.1 KEP özellikleri

KEP'e ilişkin birçok özellik bulunmaktadır. Hâlihazırda mevcut uygulamalarda ve literatürde geçen herbir KEP yaklaşımında farklı özellikler ele alınmış ve öne çıkarılmıştır.

2.3.1.1 İnkâr edilemezlik özelliği

Günlük hayatta veya iş yaşamında yapılan herhangi bir işlemin inkâr edilmesi en önemli ve yaygın karşılaşılan durumlardan biridir. Bu nedenle gerçekleştirilen iş ve işlemlerin tarafları, anlaşmazlıklarda adil bir çözüm talep etmektedir. Bu ihtiyacı karşılamak üzere inkâr edilemezlik hizmetleri devreye girmektedir.

İnkâr edilemezlik servislerinin amacı iletişimin taraflarının olası kötüye kullanımlarının veya aldatma girişimlerinin önüne geçmektir. Bir mesajlaşmada gönderici mesajı göndermediğiniveya mesajı gönderenin kendisi olmadığını iddia edebilmektedir. Diğer taraftan mesajın alıcısı mesajı almadığını veya okumadığını iddia edebilmektedir. Hatta bazen TTP bile hile yapabilmekte ve yapılan bazı işlemlere ilişkin inkâr yoluna gidebilmektedir. İşte bu noktada inkâr edilemezlik hizmetleri önem kazanmakta ve bir KEP sisteminin olmazsa olmaz özelliklerinden biri haline gelmektedir. Bu özellik ile TTP dâhil olmak üzere iletişimin taraflarından herhangi birinin hile yapmasının ve yapılan işlemleri inkâr etmesinin önüne geçilmektedir.

İnkâr edilemezliğe ilişkin hizmetlerin, iletişimin tarafları arasındaki herhangi bir uyuşmazlığı çözmek amacıyla iletişime ilişkin kanıtların oluşturulması, doğrulanması, kaydedilmesi ve daha sonradan bu kanıtların erişilebilir ve tekrar doğrulanabilir olması hizmetlerinin tamamını içermesi gerekmektedir. Bu deliller anlaşmazlık ortaya çıkmadan önce kaydedilmediyse, bahse konu anlaşmazlığın çözümü de mümkün olamayacaktır (ITU-T, 1996).

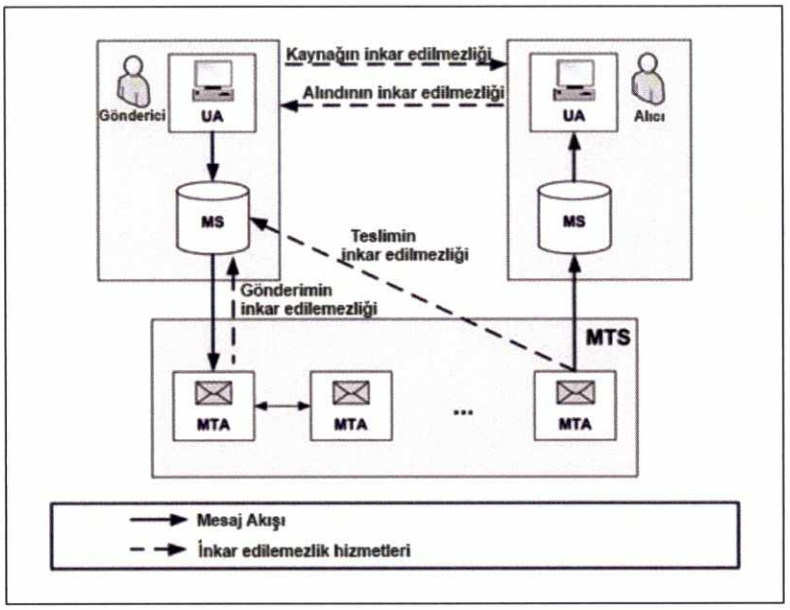
İnkâr edilemezlik hizmetleri, ISO/IEC-10181-4, ISO/IEC-13888-1, ISO/IEC-13888-2, ISO/IEC-13888-3 (ISO/IEC, 1997; 2009a; 2010; 2009b), ITU-T Recommendation X.813, ITU-T Recommendation X.400 (ITU-T, 1996; 1999a) ve RFC 2828 (Shirey, 2000) gibi birçok uluslararası standarda konu edilmiştir. Bu standartlarda temelde dört inkâr edilemezlik servisi üzerinde durulmaktadır. Bunlar:

- Kaynağın İnkâr Edilemezliği (Non-Repudiation of Origin-NRO)
- Alındı Bildiriminin İnkâr Edilemezliği (Non-Repudiation of Receipt-NRR)

- Gönderimin İnkâr Edilemezliği (Non-Repudiation of Submission-NRS)
- Teslimin İnkâr Edilemezliği (Non-Repudiation of Delivery-NRD)

şeklinde sıralanmaktadır. İnkâr edilemezlik servislerinin bir KEP sistemi içerisinde nasıl ve nerede kullanıldıkları Şekil 2.2'de gösterilmektedir.

Şekil 2.2. İnkâr edilemezlik servisleri



Kaynak: Tauber, 2012

2.3.1.1.1 Kaynağın inkâr edilemezliği

NRO; göndericinin, mesajın kaynağının kendisi olmadığına yönelik yanıltıcı girişimlerini önlemek amacıyla delil üretilmesi olarak tanımlanmaktadır. Bir başka deyişle mesajın kaynağını inkar edilemez bir biçimde ortaya koymak için kullanılmaktadır (Zhou ve Gollmann, 1996a; Onieva vd., 2008; Ferrer-Gomilla vd., 2010).

Şekil 2.2'de görüleceği üzere alıcı tarafından kullanılan NRO, genellikle dijital imzalar ile sağlanmaktadır. Bölüm 1.2.5'te detayları ile anlatılan S/MIME ve PGP mekanizmaları NRO'yu sağlamak için kullanılan standart yöntemlerdendir. Örneğin

S/MIME kullanıldığında alıcı; gönderici tarafından imzalanan mesajdaki digital sertifika vasıtasıyla mesajın, göndericinin gizli anahtarı ile imzalanıp imzalanmadığını ve mesajı gerçekten ilgili göndericinin gönderdiğini tespit edebilmektedir. Ancak burada alıcının, dijital sertifikasından doğruladığı kişinin gerçekte kim olduğunu güvenilir bir şekilde belirlemesi gerekmektedir. İşte tam bu noktada bir TTP mekanizması devreye girmektedir. Elektronik sertifika hizmet sağlayıcısı (ESHS)[2] bir TTP olarak alıcının kiminle muhatap olduğunu güvenilir bir şekilde tespit edebilmesine olanak sağlamaktadır. ESHS, açık anahtar altyapısı (Public Key Infrastructure-PKI) sunan bir TTP olarak genel erişime açık bir dizinde sertifika otoritesi (Certification Authority-CA) sertifikası, sertifika iptal listesi (Certificate Revocation List-CRL) ve çevrimiçi sertifika durum protokolü (Online Certificate Status Protocol-OCSP) cevapları gibi doğrulama için gerekli bilgileri sunarak bu doğrulamanın güvenilir bir biçimde yapılmasını sağlamaktadır.

PGP kullanılması durumunda ise merkezi bir PKI mekanizması yerine dağıtık bir mekanizma ile bu güven sorununa çözüm getirilmektedir.

Ayrıca mesajın sayısal olarak imzalanmasıyla mesajın bütünlüğü de sağlanmaktadır. Yani sayısal imza ile imzalanan mesaj arasında kuvvetli bir bağ bulunduğundan sayısal imzanın doğrulanması ile bütünlük kontrolü de yapılmış olmaktadır. Böylece hangi içeriğin imzalandığına ilişkin kanıt oluşmaktadır.

KEP sisteminin tasarımına göre değişmekle birlikte NRO delili gönderici tarafından oluşturulabileceği gibi gönderici adına bir MTA, dolayısıyla TTP, tarafından da oluşturulabilmektedir. Göndericinin sayısal imza kullandığı durumlarda imza ile birlikte NRO delili de alıcıya mesaj ile birlikte ulaştırılmaktadır. Ancak gönderici sayısal imza kullanmıyorsa bu delilin oluşturulup alıcıya ulaştırılması MTA

---

[2] Elektronik Sertifika Hizmet Sağlayıcısı tanımı 5070 sayılı Elektronik İmza Kanunu'na göre; "*Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.*" şeklindedir (T.C. Resmi Gazete, 2005).

aracılığıyla gerçekleştirilebilmektedir. Bu durumda MTA gönderici adına delili oluşturup alıcıya iletmektedir.

Son olarak fiziki postada NRO'nun karşılığının olmamasından yola çıkılarak bu delile KEP sisteminde ihtiyaç olmadığı da savunulmaktadır (Zhou ve Gollmann, 1996b).

2.3.1.1.2 Teslim alındığının inkâr edilemezliği

NRR, mesajın alıcısının mesajı almadığına ilişkin bir inkar durumuna karşı kanıt sağlamak üzere tasarlanmıştır (Zhou, 1996a; Onieva vd., 2008). Bir başka deyişle NRR ile mesajın göndericisine, mesajın alıcısı tarafından teslim alındığına ilişkin inkar edilemez bir kanıt sağlanmaktadır (Ferrer-Gomilla vd., 2010).

NRR, alıcı veya onun adına bir TTP (MTA veya MS) tarafından üretilmekte ve gönderici tarafından kullanılmaktadır. NRR'yi sağlamak amacıyla oluşturulan delil göndericiye iletilir ve gönderici tarafından saklanır.

NRR'nin fiziki postadaki alma haberinin imza ile teyidi ve alma haberli gönderim hizmetlerinin elektronik ortamdaki karşılığı olduğu söylenebilir. ISO 13888-1 standardında bu hizmet NRD olarak da isimlendirilmektedir (ISO/IEC, 2009a).

Çok çeşitli uygulamaları bulunan NRR, KEP sistemlerinde birbirinden farklı yaklaşımlarda kullanılması dikkat çekmektedir. Bazı KEP protokollerinde NRR delili oluşturulmadan önce fiziki postadakine benzer şekilde alıcıya mesaj zarfında bulunan bilgiler hakkında bilgilendirme yapılırken bazı KEP protokollerinde mesajın içeriğine ilişkin bilgiler de alıcı ile paylaşılmaktadır. Her iki yöntemde de alıcının mesajı almayı veya alındı kaydını imzalamayı reddedebilmesi gibi bazı problemler oluşabilmektedir. Örneğin icra celbi gibi kişinin istemediği veya kendisi açısından sorun yaratabileceğini düşündüğü mesajlar için mesajın göndericisine bakarak alındıyı oluşturmaması söz konusu olabilecektir (Ferrer-Gomilla vd., 2010; Tauber, 2011).

Tarafların birbirlerine güvenmedikleri durumlarda genellikle iletişim bir TTP üzerinden dolaylı olarak gerçekleştirilir. Hiçbir sistemin mükemmel olmadığı göz

önüne alındığında, TTP'nin kötüye kullanımının da ihtimal dâhilinde olması sebebiyle buna yönelik de bir takım önlemler düşünülmüştür. Bu durumda NRO ve NRR delillerinin yanı sıra TTP ve mesajlaşmanın tarafları arasındaki trafiğe ilişkin de deliller oluşturulması gündeme gelmektedir (Onieva vd., 2008).

2.3.1.1.3 Gönderimin inkâr edilemezliği

NRS, göndericiye mesajın alıcısına teslim edilmek üzere TTP'ye gönderildiğine ilişkin kanıt sağlamaktadır (Onieva vd., 2008). NRS delili genellikle gönderici ve TTP arasındaki uyuşmazlıklarda TTP'nin mesajı göndericiden aldığını kanıtlamak üzere kullanılmaktadır.

NRS, göndericinin hizmet aldığı MTA tarafından oluşturulur ve gönderici tarafından kullanılır. Fiziki kayıtlı postadaki karşılığı genellikle posta servis sağlayıcısı tarafından kayıtlı postalar için göndericiye verilen gönderi takip numarasıdır.

2.3.1.1.4 Teslimin inkâr edilemezliği

NRD, mesajın alıcısına veya alıcılarına teslim edildiğini kanıtlamak üzere kullanılmaktadır. Bu hizmet; mesajın, alıcısı tarafından gerçekten görülüp görülmediği, mesaja ulaşılıp ulaşılmadığı veya mesajın okunup okunmadığı ile ilgili bilgi sağlamamaktadır (Onieva vd., 2008).

Bu hizmetin fiziki kayıtlı postadaki karşılığı, alma haberli gönderimdir. ISO/IEC bu servisi mesaj iletiminin inkâr edilemezliği (Non-Repudiation of Transfer-NRT) olarak isimlendirmektedir (2009).

2.3.1.1.5 Deliller

Bir uyuşmazlık durumunda kullanılabilecek bilgi ve veriler delil olarak isimlendirilmektedir (Onieva vd., 2008). Delillerin ispat gücü bu kayıtlar oluşturulurken kullanılan algoritma ve parametrelerin gücü veya yapılan yasal düzenleme ile belirlenmektedir.

Bir KEP sisteminde deliller mesajlaşmanın tarafları ve/veya TTP tarafından oluşturularak saklanmaktadır. Bu delillerin formatı ise kullanılan teknoloji ile ilişkilidir. Aslında hangi format ve kriptografik teknoloji kullanılırsa kullanılsın bir KEP sisteminde deliller mesajın geçtiği adımları detaylandırmak ve bu hususlara ilişkin bilgiler sunmak amacıyla üretilmektedir.

Yapılan işlem ile bu işlemin taraflarını tanımlayan deliller genellikle delili oluşturan tarafından imzalanırlar. İnkâr edilemezlik servisleri vasıtasıyla oluşturulan deliller uçtan uca güvenilir bir sistem inşa edilmesini sağlamaktadır. İmzalı bir NRO delili göndericinin kimliğinin ispatını ve aynı zamanda da içeriğin bütünlüğünün garanti altına alınmasını sağlar.

Bu kapsamda KEP sistemindeki delillerin temel olarak;

- Olay kodu
- Olayın sebebi
- Tekil ve benzersiz delil belirteci (*identifier*)
- Delilin ait olduğu mesajın tanımlayıcısı
- Delilin hangi mesaja ait olduğununun tespitine olanak sağlayan bir parmak izi değeri veya mesajın kendisi
- Göndericinin bilgileri
- Göndericinin kimlik doğrulama verileri
- Alıcının bilgileri
- Alıcının kimlik doğrulama verileri
- Varsa gönderici veya alıcı adına hareket eden veya işlemi yapan kişi veya kurum bilgileri
- Delilin üretilme tarih ve zamanı (eğer zaman bilgisi bir zaman damgası hizmet sağlayıcısından (Time-Stamping Authority-TSA) alınıyor ise bu hizmet sağlayıcısının bilgileri)
- Delilin hangi politikaya göre oluşturulduğunu gösterir politika numaraları
- Delili oluşturan bilgileri

- Sayısal imzalar ve doğrulama verileri

gibi unsurları içermesi gerekmektedir (Onieva vd., 2008).

Delilin sistem içerisinde tekilliğini sağlamak için tekil bir belirtecin delil içerisinde bulunması gereklidir. Gönderici ve alıcıya ilişkin bilgilerin de yine delil içerisinde bulunması kaçınılmazdır.

Kullanılan düzenleyici yaklaşıma bağlı olarak değişmekle birlikte deliller genellikle elektronik imza veya güvenli zarflar (*secure envelopes*) kullanılarak oluşturulmaktadırlar. Elektronik imzada asimetrik şifreleme kullanılırken, güvenli zarfların kullanılması durumunda ise simetrik şifreleme kullanılmaktadır (ISO/IEC, 2010). Her iki yöntemin avantaj ve dezavantajları bulunmaktadır. Elektronik imza kullanımı performans açısından bir takım sıkıntıları beraberinde getirirken, simetrik şifreleme kullanımı TTP'ye bağımlılık yönünden dezavantajlar barındırmaktadır.

Simetrik şifrelemede güvenli zarflar TTP tarafından TTP'nin gizli anahtarı kullanılarak oluşturulmaktadır. TTP, delilleri oluşturan ve doğrulayan taraf olduğundan delil oluşturulması ve doğrulanması aşamasında TTP'ye çevrim içi ihtiyaç duyulmaktadır. Diğer taraftan mesaj içeriğinin değişmezliğini sağlama noktasında bu yöntemin birçok sakıncaları da bulunmaktadır. Bu yöntemin avantajı ise performans açısından elektronik imzaya nazaran daha iyi olmasıdır.

Diğer bir yöntem olan asimetrik şifrelemeye dayanan elektronik imzada, kullanılan X.509 (Cooper vd., 2008) sertifikalarının geçerlilik süreleri belli bir zaman aralığındadır. İmza doğrulanırken imzanın atılmış olduğu zamanda sertifikanın geçerli olup olmadığını güvenilir bir biçimde tespit edebilmek delilin güvenilirliğini sağlamak açısından önemlidir. Bu açıdan imzanın atıldığı zamanı, yani delilin imzalandığı zamanı, doğru ve güvenilir bir biçimde tespit edebilmek gereklidir. Bu gerekliliği sağlamak üzere delil içerisine sistem saati yazılabilmekte veya bir TSA tarafından zamanın tespit edilebilmesini sağlayan kanıtlar delil içerisine konabilmektedir. Bu sayede imza doğrulaması da güvenilir bir biçimde yapılabilmektedir.

Bir delilin oluşturulmasından uyuşmazlıklarda kullanılmasına kadarki yaşam döngüsünde; oluşturma, iletme, doğrulama, saklama, erişme ve uyuşmazlık çözümü olmak üzere altı aşama bulunmaktadır (Onieva vd., 2008). Bir KEP sisteminde bu aşamaların nasıl ve ne şekilde bulunacağı veya bulunup bulunmayacağı hususları tamamen ihtiyaca göre değiştiğinden ilgili düzenlemeler ile belirlenmektedir.

2.3.1.1.5.1 Delili oluşturma

Delilin oluşturulmasından önce delilin oluşturulmasına ilişkin talebin olması gerektiği ifade edilse de (Shirey, 2000) KEP sisteminde delillerin oluşturulması için ön talebe gereksinim olmadığı, önceden tanımlı zaman ve koşullarda delillerin üretildiği göz önüne alındığında delil oluşturmanın ilk aşama olduğu görülmektedir. Yani inkâr edilemezlik hizmetinin sağlanabilmesi için ilk koşul delilin oluşturulmasıdır.

Delilin oluşturulması, düzenleyici yaklaşıma veya delilin hangi inkâr edilemezlik servisini sağlamaya yönelik üretildiğine bağlı olarak değişmekle birlikte, delil gönderici, alıcı veya TTP tarafından üretilebilmektedir. Delilin içerisindeki alanlar ve kullanılacak algoritmalar ise tamamen düzenleyici yaklaşıma göre belirlenebilmektedir. Örneğin NRO ve NRR delilleri elektronik imza kullanılmak suretiyle gönderici ve alıcı tarafından oluşturulabilmekte iken, NRS ve NRD delilleri TTP tarafından üretilebilmektedir. Diğer taraftan tüm bu delillerin TTP tarafından oluşturulabildiği yaklaşımlar da bulunmaktadır (Onieva vd., 2008).

Başka bir yaklaşımda ise deliller, mesajlaşmaya ilişkin inkâr edilemezlik servislerini destekleyici mahiyette TTP tarafından oluşturulabilmektedir (Zhou ve Gollmann,1996a). Bu durumda TTP, mesajlaşmanın akışına karışmadan ve sadece kendisine verilen bilgileri karşılıklı olarak teyit edip delil sağlama işlevini yerine getirmektedir.

Sonuç itibariyle delillerin oluşturulma süreçleri ilgili düzenlemeler, kabul edilen yaklaşım, TTP'nin konumlandırılması ve sistemin kurgulanışına bağlı olarak farklılık gösterebilmektedir.

2.3.1.1.5.2 Delil iletimi

Delillerin ilgili taraflarla paylaşımı veya ilgili taraflara iletimi, adil bir inkâr edilemezlik mekanizması tesisi etmenin en önemli adımıdır. Delillerin ilgili taraflara iletilmesi taraflar arasındaki iletişim kanalının kalitesine doğrudan bağlıdır.

2.3.1.1.5.3 Delili doğrulama

Herhangi bir uyuşmazlık halinde delillerin yeterli olup olmadığının tespiti için bu delillerin ilgili taraflarca doğrulanabilmesi gereklidir.

Delillerin doğrulanma süreci nasıl ve hangi yöntemler kullanılarak oluşturulduklarıyla doğrudan ilgilidir. Delillerin elektronik imza kullanılarak oluşturulması halinde doğrulama ancak ESHS'lerden temin edilen doğrulama verileriyle gerçekleştirilebilir. Böyle bir doğrulama için delilin kaynağı, bütünlüğü ve geçerliliğinin kontrol edilebilir olması gereklidir. Bununla birlikte sağlıklı bir doğrulamanın ön koşulu güvenilir bir zaman damgası aracılığıyla imzanın atılma tarihi ile doğrulama için kullanılan sertifikanın geçerlilik ve iptal durumunun da kontrol edilmesidir (Onieva vd., 2008).

Diğer bir yöntem olan güvenli zarfların kullanılması halinde ise doğrulama işlemi delil oluşturma ve doğrulamada kullanılan gizli anahtarın sadece TTP'de olması sebebiyle TTP aracılığıyla yapılabilmektedir.

2.3.1.1.5.4 Delillerin saklanması

Herhangi bir uyuşmazlık halinde kullanılmak üzere geçerli delillerin saklanması ve bu delillerin ne kadar süre ile saklanacağının da ilgili düzenlemeler ile belirlenmesi gerekmektedir. Uygulamaya göre değişmekle birlikte genellikle delil saklama hizmeti TTP'ler tarafından yerine getirilmektedir.

Kritik mesajlaşmalara ilişkin delillerin uzun dönemli saklanması gerekmektedir. Elektronik ortamda delillerin uzun dönemli saklanabilmesi için farklı yöntemler kullanılmaktadır. Bu yöntemlerden birisi elektronik imza kullanılarak delillerin oluşturulması, bu delillerin uzun dönemli saklanması ve doğrulanabilmesi için belirli

işlemlerden geçirilmesidir. Elektronik imza kullanılarak oluşturulan bu delillerin oluşturulduktan sonra sadece depolanarak saklanmaları mümkün değildir. Çünkü imzanın oluşturulmasında kullanılan ve güvenliğini sağlayan algoritmalar teknolojinin gelişmesi ve yeni kriptoanaliz yöntemlerinin geliştirilmesi gibi sebeplerle güvenilirliklerini yitirebilmektedirler. Bu sebeple elektronik imza standartlarında (ETSI, 2009a; ETSI, 2009b; ETSI, 2012) bu gibi durumlarda kullanılmak üzere arşiv elektronik imza (ES-A) formatı geliştirilmiştir. Bu formata göre delillerin saklanması gereken süre içerisinde, üzerindeki imzanın belirli zamanlarda arşiv formatında güncellenmesi gereklidir. Temel olarak, bu süre, arşivleme için kullanılan zaman damgası sertifikasının süresine göre belirlenmektedir. Zaman damgası sertifikasının süresi bitmeden önce yeni bir zaman damgası sertifikası ile yeniden arşiv zaman damgası alınmaktadır. Sonuç olarak, bir dokümanın elektronik ortamda güvenli olarak saklanabilmesi için ihtiyaç duyulan süre boyunca arşiv imza ile korunması gerekmektedir (BTK, 2012a).

2.3.1.1.5.5 Uyuşmazlık çözümü ve delillerin kullanımı

Herhangi bir uyuşmazlık halinde bu uyuşmazlığın taraflarının veya yetkili mercilerin oluşturulan ve saklanan delillere ulaşım sağlamaları gerekmektedir. Bununla birlikte bu deliller yine yetkili merci tarafından doğrulanabiliyor veya doğrulattırılabiliyor olmalıdır. Bu doğrulama işlemlerinden sonra geçerliliği tespit edilen deliller uyuşmazlığın çözümü için kullanılabilir.

Bir uyuşmazlık çözümünde istenen en önemli özelliklerden birisi delillerin mesajlaşmanın taraflarından bağımsız olarak doğrulanabilir ve saklanabilir olmasıdır.

2.3.1.2 Adillik

Gönderici, gönderdiği bir mesaja ilişkin NRR delili ile kendi açısından gerekli bilgiyi edinmiş olur. Ama kötü niyetli bir göndericiye ilişkin alıcı tarafında herhangi bir koruma mevcut değilse gönderdiği mesajı inkâr eden bir gönderici karşısında alıcı dezavantajlı bir durumda olacaktır. Aynı şekilde bir alındının göndericiye

sağlanmaması durumunda da kötü niyetli alıcıya karşı gönderici dezavantajlı bir konumda bulunacaktır.

Taraflardan birinin kötü niyeti dışında farklı sebeplerle, örneğin iletişim kanallarındaki bir sıkıntı nedeniyle alındı kaydının göndericiye iletilememesi durumunda da gönderici dezavantajlı durumda olacaktır (Tauber, 2012).

Adil bir mesajlaşmada, taraflar birbirlerine karşı avantajlı veya dezavantajlı bir pozisyonda bulunmamalıdır. Bu nedenle adillik özelliğinin temel olarak bir KEP sisteminde bulunması gereklidir (Ferrer-Gomilla vd., 2000; 2010).

Fakat bu teknik, fazla maliyet ve uygun kurgulanmamış bir sistem gibi nedenlerle her zaman mümkün olmayabilir. Bu nedenle uygun kurgulanmış bir sistemde ortaya çıkabilecek olası bir uyuşmazlık durumunda taraflar arasındaki adillik sonradan da sağlanabilir olmalıdır. Örneğin bir mesajlaşmada göndericiye NRR delili teknik bir nedenle iletilmemiş olsa bile herhangi bir uyuşmazlık durumunda NRR deliline ulaşabilmesi veya uyuşmazlık sonunda taraflardan birinin mağduriyetinin engellenebilmesini sağlayacak delillerin elde edilebilmesi adil bir sistem için gereklidir.

Bir mesajlaşmada tarafların her birinin gerekli ve beklenen bilgileri alması veya talep etmesi halinde belli bir zaman içerisinde bu bilgileri temin edebiliyor olması ya da taraflardan hiçbirinin yarar sağlayacak bir bilgiyi elde edememesi durumunda bu mesajlaşma kuvvetli adil olarak tanımlanmaktadır (Asokan, 1998; Ferrer-Gomilla vd., 2010; Draper-Gil vd., 2014). Diğer taraftan hiçbir sistemin mükemmel çalışmadığı ve zaman zaman hatalar ortaya çıktığı düşünüldüğünde taraflardan birinin beklediği bilgileri elde edip diğerinin teknik veya başka bir aksaklık yüzünden beklediği bilgileri alamama durumu ortaya çıkabilecektir. Bu durumda beklediği bilgiyi alamayan tarafın buna ilişkin kanıtlara sahip olması gereklidir. Bu durumda yine koşullu olarak doğrulanabilir bir durumdan söz edilmektedir. Bu şekilde sağlanan adilliğe ise zayıf adillik ismi verilmektedir (Asokan, 1998; Ferrer-Gomilla vd., 2010).

Adil bir KEP sisteminde, göndericinin beklediği ve talep ettiği NRR delilini alıcının ise benzer şekilde mesajı ve NRO delilini alması gerekmektedir. Yani hem NRR delili hem de mesaj ve NRO delili ilgili taraflara ulaştırılmalıdır.

2.3.1.3 Sonlanabilirlik ve zaman aşımı süreleri

KEP sisteminde bulunması gereken önemli özelliklerden birisi işlemlerin adilliği bozabilecek beklemelere ve tıkanıklıklara yol açmayacak şekilde sonlandırılabilmesidir. Herhangi bir sebeple sonlandırılan bir işlem, mesajlaşmanın taraflarından birinin lehine veya aleyhine bir durum oluşturmamalıdır. Örneğin göndericinin gönderdiği mesaja karşılık alıcının imzalı alındı kaydını göndermemesi veya gönderememesi durumunda belli bir bekleme süresini müteakip iletişimin sonlandırılması gerekmektedir. Aksi takdirde KEP sistemlerinde alıcıdan gelmesi gereken alındının süresiz olarak beklenmesi gibi istenmeyen durumlar ortaya çıkabilecektir.

Günümüzde birçok KEP sisteminde işleyişin belirli noktalarında zaman aşımı süreleri belirlenmekte ve bu sürelerinin aşılması halinde de iletişim otomatik olarak sonlandırılmaktadır (Tauber, 2012). Ancak güvenilir olmayan iletişim kanalları veya kesintisiz iletişim kanallarında iletişimin tamamlanma süreleri belirsiz olduğundan bu kanallar üzerinde çalışan KEP sistemlerinde zaman aşımı sürelerini belirlemek ve uygulamak mümkün olamamakta ve bu sebeplerle taraflar arasındaki adillik özelliğini etkilenebilmektedir (Ferrer-Gomilla vd., 2010). Dolayısıyla bir KEP sisteminde zaman aşımı süreleri belirlenirken birçok parametrenin dikkate alınmasının, zaman aşımı süreleri uygulanırken karşılıklı sistem zamanlarının güncel ve güvenilir bir kaynaktan alınıyor olmasının ve bağlantı katmanının zaman aşımı sürelerine uygun olarak tasarlanmasının önem arz etmektedir.

2.3.1.4 Kayıtların saklanması

KEP sisteminde; TTP, işlevlerini yerine getirmek ve zorunlu olarak sağlaması gereken hizmetleri verebilmek için bazı bilgi ve belgeleri saklamak gerekmektedir. Ferrer-

Gomilla vd., (2010)'ya göre saklanması gereken bilgi/belgelerin durumu ve bunların saklanma süresi açısından dört farklı KEP sistemi tasarlanabilir.

Bunlardan ilki, teoride en çok tercih edilen ve en etkili yöntem olarak kabul edilen TTP'nin herhangi bir bilgi ve belge saklamasının gerekli olmadığı sistem tasarımıdır. Ancak bu şekilde bir KEP sisteminin oluşturulması mesajların büyümesi, karmaşıklık gibi dezavantajları ile birlikte teoride mümkün olsa da pratikte mümkün olamamaktadır.

İkinci yaklaşım ise, TTP'nin bazı bilgi/belgeleri tanımlı ve belirli bir zaman aralığında saklaması şeklindedir. Genel olarak dünyada üzerinde pratikte gerçekleştirilen hemen hemen tüm sistemlerin bu şekilde çalıştığı bilinmektedir (Tauber, 2012). Bu durumda bir düzenleme veya anlaşma ile verilerin ne kadar süre ile tutulacağı belirlenmekte ve belirlenen bu sürelerin sonunda TTP tarafından ilgili veriler kalıcı olarak silinmekte veya yok edilmektedir.

Üçüncü yaklaşım, TTP'nin bazı bilgi/belgeleri sınırlı bir şekilde belirli olmayan bir zaman aralığı için saklaması şeklindedir. Bu şekildeki bir yaklaşım pratik olarak anlamlı değildir. Çünkü verilerin ne kadar süre ile saklanacağının belirlenmemiş olması birçok yönden sakınca oluşturabilmektedir. Örneğin verilerin gereğinden fazla tutuluyor olması depolama alanı açısından birçok darboğaza neden olabilecektir.

Dördüncü ve son yaklaşım ise TTP'nin bilgi ve belgeleri sonsuza kadar saklaması şeklindedir ki bu en istenmeyen ve pratik olarak en zor gerçekleştirilebilecek yaklaşımdır. Bu şekildeki bir yaklaşımda hiçbir veri silinmediğinden sonsuz bir veri depolama alanı gerekliliği ortaya çıkmaktadır. Bu da böyle bir sistemin gerçekleştirilmesini olanaksız hale getirmektedir.

Bu dört yaklaşımdan gerek performans gerekse maliyetler açısından en avantajlısı birinci yaklaşım olmasına rağmen kullanımındaki ve gerçekleştirilmesindeki kolaylıklar nedeniyle en çok tercih edilenin ikinci yaklaşım olduğu görülmektedir.

2.3.1.5 Diğer özellikler

2.3.1.5.1 Gizlilik (Confidentiality)

Gizlilik genel manada bilginin veya işlemlerin, yetkili ve ilgili taraflar dışındaki kişiler tarafından erişilemez veya ulaşılamaz olmasını ifade etmektedir (ISO/IEC, 2014).

KEP sistemi için gizlilik, temel ve sağlanması gerekli bir özellik olmasına rağmen bazı yaklaşımlara göre seçimlik bir özellik olarak kabul edilmektedir. Buna göre gizliliğin sağlanması için her kullanıcı, iletmek istediği mesajın gizlilik derecesine göre doğru mekanizmaları kulanmak zorundadır. Halen kullanılan birçok KEP sisteminde, alıcının NRR delilini oluşturmasından önce mesaj içeriğine ulaşamamasını teminen mesaj içeriği şifrelenmiş durumdadır (Ferrer-Gomilla vd., 2010).

Bir KEP sisteminde gizliliğin sağlanmış olması gönderici ve alıcı hariç, TTP ve ara kademedeki herhangi bir tarafın mesaj içeriğine erişme ihtiyacının olmaması ile bağlantılıdır. Gizlilik taraflar arasındaki iletişimin herbir aşamasını kapsamaktadır. KEP sistemi içerisinde mesajın gizliliği gönderici-TTP, TTP-TTP ve TTP-alıcı arasındaki iletim sırasında mesajın şifrelenmesi ile sağlanabilmektedir. Göndericinin UA'sından başlayarak alıcının UA'sına kadar olan bu şekildeki şifreleme, noktadan noktaya şifreleme (End-to-End Encryption-E2EE) olarak adlandırılmaktadır (Tauber vd., 2012). Elektronik posta sistemlerinde E2EE, S/MIME ve PGP ile sağlanabilmektedir.

E2EE ile çalışan bir sistemde mesajlar zarflar içerisinde taşınmaktadır. Gönderici tarafından şifrelenerek bir zarf içerisine konan ileti, alıcıya iletilmekte ve alıcı tarafında da mesajdan ziyade zarfın alındığına ilişkin alındı kaydı üretilmektedir. Böylece mesajın taşınması sırasında TTP ve diğer üçüncü tarafların içeriğe ilişkin bilgi sahibi olmamaları ve orijinal mesajın gizliliği sağlanabilmektedir.

2.3.1.5.2 Bütünlük (*Integrity*)

Bütünlük, varlıkların doğruluğunun ve eksiksizliğinin (*completeness*) korunması olarak tanımlanmaktadır (ISO/IEC, 2014).

Veri bütünlüğünün korunması, mesajlaşmanın tüm aşamalarında verilerin doğruluğunun ve tutarlılığının sağlanmasıdır. Böylece iletilen veri üzerinde meydana gelen tüm değişiklikler farkedilebilmektedir.

Veri bütünlüğünde verilerin doğruluğunun yanı sıra eksiksizliği de önem arz etmektedir. Çünkü doğru fakat eksik olan bir veri yanıltıcı olabilmektedir (Boritz, 2005).

2.3.1.5.3 Güvenilirlik (*authenticity*) ve doğrulama (*authentication*)

Güvenilirlik bir tarafın gerçekten iddia edilen taraf olup olmadığını ispatlayan bir özelliktir (ISO/IEC, 2014). Bu özellik, iletişimin ve paylaşılan verilerin gerçekliğini ve orijinalliğini garanti etmek üzere kullanılmaktadır.

Doğrulama da bu kapsamda değerlendirilebilir. Bir KEP sisteminde mesajlaşmanın taraflarından olan gönderici, alıcı ve TTP'nin doğrulanabilir olması önem arz etmektedir. Çünkü herhangi bir mesajlaşmada, iletişimde olunan kişinin gerçekten istenen ve doğrulanan kişi olup olmadığı tüm yapıyı etkileyebilmektedir.

Doğrulama çok farklı seviyelerde ve farklı metodlar kullanılarak gerçekleştirilebilmektedir. Örneğin gönderici kimliği, sayısal imza kullanılarak oluşturulacak bir NRO delili ile mesaj seviyesinde doğrulanabilirken, MTS'ye bağlanma aşamasında kullanılacak SSL vasıtasıyla bağlantı katmanında da doğrulanabilir (Tauber, 2012).

KEP sisteminde kimlik doğrulama seviyesi büyük önem taşımaktadır. Bazı durumlarda yasal geçerlilik için iletişimin taraflarının kimlik doğrulamasının resmi bir yolla yapılması gerekmektedir. Bu nedenle yasal çerçevenin adresleme ve kimlik

belirlemeyi ele almak için uygun olması ve düzenlemelerin kişi ile adres arasındaki ilişkiyi net bir şekilde desteklemesi gerekmektedir. Aksi takdirde hizmetlerin sağladığı herhangi bir delil, değerini yitirilebilecektir.

Literatürde güvenlik özelliği olarak sadece gizlilik ve inkâr edilemezlik yer almaktadır. Ancak pratikte veri bütünlüğü, güvenilirlik ve doğrulama özellikleri de temel özellikler olarak karşımıza çıkmaktadır. Bahsedilen bu özelliklerin hiçbirisinin veri bütünlüğü ve gizlilik içerisinde değerlendirilmesi mümkün gözükmemektedir (Tauber, 2012).

2.3.1.5.4 Performans

KEP sistemlerinin değerlendirilmesi veya karşılaştırılmasında güvenlik özelliklerinin yanı sıra en önemli parametrelerden bir tanesi de performanstır. Performans genellikle bir mesaj döngüsünün kaç adımda tamamlandığı ile ifade edilmektedir. Örneğin iki adımda tamamlanan bir mesajlaşmada göndericinin mesajı alıcıya göndermesi birinci adım ve alıcının da mesajı aldığına dair alındı kaydını iletmesi ikinci adım şeklinde ifade edilmektedir. Fakat adil ve inkâr edilemez bir KEP sistemi için en az üç adıma ihtiyaç duyulmaktadır. Çünkü iki adımda tamamlanan yukarıdaki senaryoda alıcının alındı kaydını iletmemek suretiyle mesajı aldığını inkâr edebilmesi söz konusu olduğundan adillik sağlanamamaktadır. Bu sebeple iki adımda tamamlanabilecek bir KEP sisteminin mevcut olmadığı söylenebilir.

Diğer taraftan mesajlaşmanın gerçekleştiği sistemlerin verimini tahmin etmek ve öngörebilmek oldukça güçtür. Herhangi bir aşamada meydana gelebilecek farklı durumlar için farklı akışlar oluşabileceğinden mesajlaşmanın tamamlanması için gerekli olan adım sayısı değişebilmektedir (Tauber, 2012).

Sistem performansı işletilen adım sayısının yanında kullanılan altyapı, yazılım, donanım ve diğer faktörlere bağlıdır. Bu sebeple hangi KEP yaklaşımının en etkili yaklaşım olduğu hususunda bir yargıya ulaşabilmek oldukça güç olmakla birlikte aynı koşullar altında mesajlaşmanın hangi yaklaşım sonucunda daha hızlı yapılabildiği şeklinde bir sonuca ulaşabilmek mümkündür.

2.3.1.5.5 Düzenleme

Bir KEP sisteminin sahip olması gereken ve yukarıda sayılan özelliklerden hangilerinin ne şekilde uygulanacağı düzenlemeler vasıtasıyla belirlenmektedir. Kurulacak olan altyapı bileşenlerinin neleri içereceği, bu sistemde bulunacak özellikler ve bunların ne şekilde kullanılacağı bir düzenleme ve kurallar bütünü olarak tanımlanmaktadır. Ayrıca yine düzenleme aracılığıyla uyuşmazlık durumlarında izlenecek yollar da tanımlanmaktadır.

Her ülkenin kendi iç düzenlemesi ile ne şekilde bir TTP yapısı oluşturulacağı ve bunların yetkilendirilmesi, iletişim altyapısının ne şekilde kurulacağı, deliller, zaman aşımı süreleri gibi hususlar belirlenebilmektedir. Bu şekildeki yaklaşım "de jure" olarak adlandırılmaktadır. Diğer taraftan özel sektörde firmaların hizmet sağlayıcılarla veya müşterileri ile yapacakları bir sözleşme ve anlaşma yoluyla da kuralları "de facto" olarak da belirleyebilmesi mümkündür (Tauber, 2012).

2.3.1.5.6 Uyuşmazlık çözüm mekanizmaları

Bir KEP sisteminin pratikte uygulanabilir olması mesajlaşmanın gerçekleştiğine ve hangi koşulları içerdiğine ilişkin delil sağlaması ile mümkün olabilmektedir.

KEP'te temel olarak göndericinin iletiyi gönderdiğini inkâr etmesi ve alıcının kendisine gelen iletiyi inkâr etmesi gibi iki uyuşmazlık durumu ortaya çıkmaktadır. Literatürde bulunan ve hali hazırda kullanılan KEP yaklaşımlarının hemen hemen hepsinde bu iki duruma ilişkin çözüm getirilmiş durumdadır. Bunun tek istisnası Zhou ve Gollmann (1996b)'de bahsedilen, fiziki kayıtlı postada bu özelliğin olmadığından hareketle göndericinin kimliğini gizleme veya NRO delilin üretmeyecek şekilde tasarlanan KEP yaklaşımıdır.

Hâlihazırda tasarlanmış olan KEP sistemlerindeki uyuşmazlık çözüm mekanizmaları farklı aktörlerin yer alma gerekliliği açısından birbirinden farklılaşmaktadır. Bazı çözümlerde gönderici ve alıcı hakem konumundaki üçüncü bir tarafa başvurmakta ve bu üçüncü taraf başvuran tarafın sağladığı delilleri göz önünde bulundurarak bir

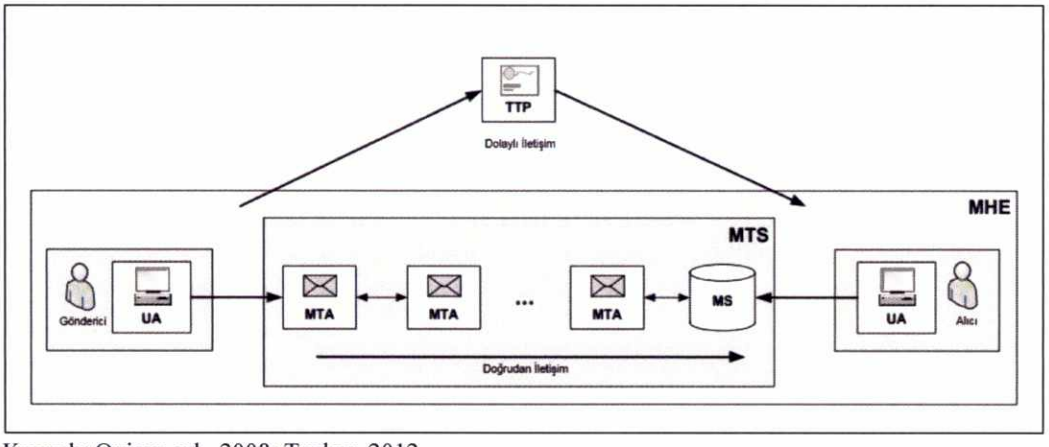
sonuca ulaşmaktadır. Bununla birlikte diğer bazı çözümlerde ise hakem konumundaki üçüncü taraf TTP'de dâhil olmak üzere diğer taraflardan deliller talep edebilmektedir. Uyuşmazlığı çözmekle görevli üçüncü tarafın uyuşmazlığı çözebilmek amacıyla sistemin işleyişinde yer alan taraflardan delilleri istemesi doğaldır. Fakat işleyişte yer alan bir tarafın uyuşmazlık çözümüne katılmayı reddetmesi durumunda sorunlar ortaya çıkmaktadır. Bu sebeple taraflardan bağımsız bir uyuşmazlık çözüm mekanizması gerekmektedir. Bu açıdan uyuşmazlığı çözmeye yetecek kadar delilin uyuşmazlığın taraflarının herbirinin elinde bulunması önem kazanmaktadır. Yani gönderici ve alıcı birbirlerinin verilerine ihtiyaç duymadan haklılıklarını ispat edebilecek yeterli delile sahip bulunmalıdır (Ferrer-Gomilla vd., 2010).

2.3.2 KEP bileşenleri

2.3.2.1 Güvenilir üçüncü taraflar

Şekil 2.3'te gösterildiği üzere taraflar arasındaki iletişimde bir hizmet sağlayıcının TTP olarak bulunmadığı doğrudan iletişime olanak sağlayan ve bir hizmet sağlayıcının TTP olarak bulunduğu dolaylı bir iletişime izin veren olmak üzere iki farklı KEP yöntemi bulunmaktadır. Düzenleme ile hangi yöntemin kullanılacağı ve kullanılan yöntemde temel gereksinimlerin nasıl karşılanacağı belirlenmektedir.

Şekil 2.3. Mesaj iletim yapısı



Kaynak: Onieva vd., 2008; Tauber, 2012

2.3.2.1.1 Doğrudan iletişim

TTP olmaksızın adil ve inkâr edilemez bir mesajlaşma doğrudan iletişim ile gerçekleştirilebilir. Doğrudan iletişimde temel olarak taraflar arasındaki adil paylaşımı sağlayabilmek için mesaj ve delillerin eşzamanlı paylaşımı esas alınmaktadır. Bu iletişimde, göndericinin mesajın tamamını alıcıya ilettiği anda kendisine gerekli olan NRR delilini elde etmesi ve böylelikle tarafların olası kötüye kullanımlarının ortadan kaldırılması esas alınmaktadır (Paulin ve Welzer, 2013).

Taraflar arasında bilgilerin aşamalı olarak paylaşılması ve mesajlaşmada karşılıklı olarak talep edilen bilgi ve belgelerin eşzamanlı olarak taraflara iletilmesi esasına dayanan bu tür yaklaşımlar (Markowitch ve Roggeman, 1999) tarafların işlem güçlerinin eşit olduğu ve sistemlerin eşzamanlı olarak çalışacakları varsayımına dayandığından pratikte anlamlı ve kullanılabilir bulunmamaktadır (Oppliger, 2004; Oppliger, 2007; Grundma ve Woß, 2008; Tauber, 2012).

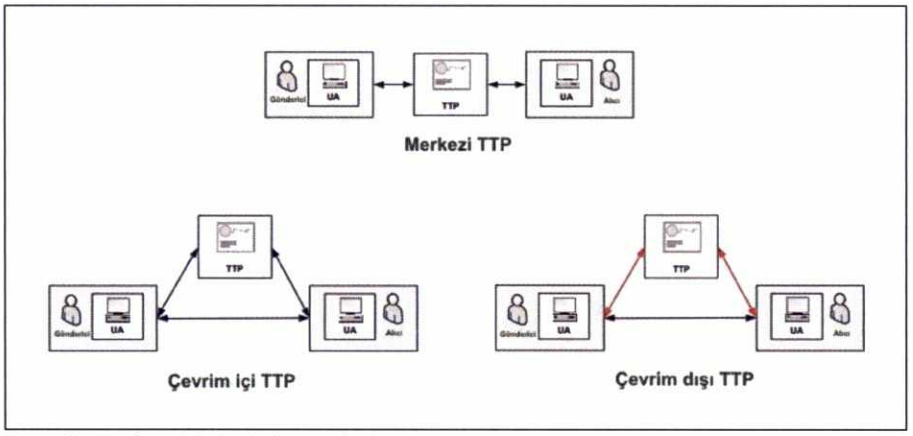
Bu nedenle TTP olmaksızın tasarlanan protokoller zayıf dahi olsa adilliği sağlamaktan uzaktırlar. Taraflar arasındaki işlem gücünden soyutlanmış protokollerde ise ancak olasılıksal bir adillik mümkün olabilmektedir (Tauber, 2012).

Bu bilgiler kapsamında bir TTP olmaksızın adil ve inkâr edilemez bir sistem oluşturulamadığı ve bu sebeple henüz uygulamada karşılığı bulunmayan bu yaklaşımın kabul edilebilir olmadığı değerlendirilmektedir (Ferrer-Gomilla vd., 2010). TTP olmaksızın gerçekleştirilecek sistemin bazı kullanım alanları olsa dahi bir KEP sistemi için bu yaklaşımın uygun olmadığı görünmektedir (Grundma ve Woß, 2008).

2.3.2.1.2 Dolaylı iletişim

Mesajlaşmanın bir TTP üzerinden yapıldığı veya mesajlaşmaya ilişkin bir ya da daha fazla adımda TTP'nin devreye girdiği dolaylı iletişimde, TTP'nin mesajlaşmada bulunduğu konum ve mesajlaşmaya müdahil olması açılarından Şekil 2.4'te görüleceği gibi üç yaklaşım bulunmaktadır.

Şekil 2.4. TTP'nin mesajlaşmadaki konumu



Kaynak: Tauber, 2012; Onieva vd., 2008

2.3.2.1.2.1 Merkezi TTP (*Inline TTP*)

Mesajlaşmanın doğrudan bir TTP üzerinden gerçekleştirildiği bir KEP sisteminde gönderici ve alıcı arasındaki iletişim tamamen TTP üzerinden gerçekleştirilmektedir. Şekil 2.4'te de görüldüğü üzere TTP iletişimin tarafları arasında yer almaktadır. Gönderilen/alınan mesaj ve deliller TTP aracılığıyla iletiliğinden gönderici ile alıcı arasında doğrudan bir bağlantı söz konusu olmamaktadır.

Bununla birlikte bu yaklaşımın birçok avantajı da bulunmaktadır. İletişim hattında bulunan ve mesaj trafiğini üzerinden geçiren TTP'nin var olması elektronik posta sistemlerindeki bileşenlerin ve altyapıların kullanılabilmesine imkân tanımaktadır. Bu da gönderici ve alıcı tarafta alışılmış yapıların kullanılabilmesi anlamına gelmektedir. Ayrıca mesajlaşma TTP üzerinden gerçekleştirildiğinden mesajlar, deliller ve akış üzerinde istenen tüm kontrol ve değişiklikler gerçekleştirilebilmektedir. Alıcı tarafından NRR delili oluşturuluncaya kadar mesajın göndericisinin gizlenmesi, şifreleme, mesajların ve delillerin saklanması bu hususa örnek olarak verilebilir.

Bu yaklaşımda tüm mesajlaşma TTP üzerinden gerçekleştirildiğinden özellikle büyük ölçekli sistemlerde performans açısından bazı problemler de ortaya çıkabilmektedir. Bu şekilde kurgulanan bir sistemde mesajlar, deliller, işlem kayıtları gibi birçok bilginin depolanması gerektiğinden TTP'nin çok fazla depolama alanına ihtiyacı

olmaktadır. Tüm trafiğin akışının sağlanması ve gerekli bilgilerin depolanması sebebiyle bu yapı TTP'nin güvenilirliği üzerine kurgulanmıştır. Ancak TTP'nin olası bir kötüye kullanımı söz konusu olduğunda tüm sistemi etkileyebilecek ve sistemi geçersiz kılabilecek büyük bir risk oluşmaktadır. Bu nedenle söz konusu riskin, çeşitli düzenlemelerle ve hizmet veren TTP'lerin denetim mekanizmalarıyla kontrol altında tutulmasıyla en aza indirilmesi gerekmektedir.

Diğer taraftan mesajlaşma TTP üzerinden gerçekleştirildiğinden mesajların içeriğinin TTP tarafından görülmesi veya değiştirilmesi gibi kötüye kullanım riskleri de mevcuttur. Bu riskin ortadan kaldırılabilmesi, mesajın gönderici ve alıcı arasındaki mahremiyetinin sağlanması ve mesajın bütünlüğünün korunması için şifreleme seçeneği kullanılmaktadır. Schneier ve Riordan (1997)'a göre göndericinin mesajı KEP sistemine sokmadan önce mutlaka şifrelemesi gereklidir. Hatta bazı metodlarda mesajın önce alıcının açık anahtarı ile şifrelenmesi, ardından TTP'nin açık anahtarı ile şifrelenerek TTP'ye iletilmesi suretiyle mesaj içeriğinin gizliliğinin sağlanması gerektiği ifade edilmektedir (Cimato vd., 2005).

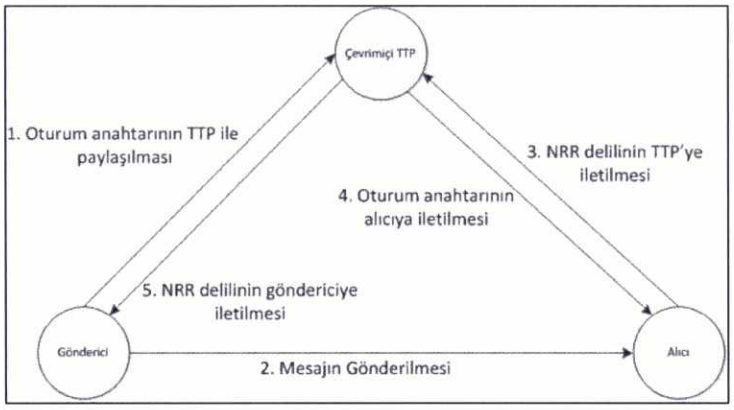
2.3.2.1.2.2 Çevrim içi TTP

Çevrim içi TTP yapısında, herbir mesajlaşmada çevrim içi olarak TTP yer almakta fakat tüm adımlar TTP üzerinden gerçekleştirilmemektedir (Ferrer-Gomilla vd., 2010). Bu yapıda TTP'nin taraflar arasındaki iletişimi sağlama görevi bulunmamaktadır. Taraflar TTP'nin devrede olması koşuluyla birbirleriyle doğrudan iletişim kurabilmektedirler (Bkz. Şekil 2.4). Çevrim içi TTP yöntemiyle merkezi TTP yönteminde yaşanması muhtemel performans problemlerinin önüne geçilmeye çalışılmıştır.

Şekil 2.5'te gösterildiği üzere çevrim içi TTP kullanılması durumunda temel olarak işleyiş; göndericinin TTP ile irtibata geçerek mesajı şifrelemek üzere kullanılacak bir oturum anahtarını TTP'ye iletmesi, göndericinin bu oturum anahtarı ile şifrelediği mesajı doğrudan alıcıya göndermesi, mesajı alan alıcının TTP ile irtibata geçerek NRR delilini TTP'ye iletmesi, TTP'nin NRR delilini almasını müteakip mesajın çözümü

için gerekli olan anahtarı alıcıya göndermesi ve TTP'nin alıcıdan almış olduğu alındı kaydını göndericiye iletmesi şekilde gerçekleşmektedir (Tauber, 2012).

Şekil 2.5. Çevrim içi TTP çalışma modeli



Aslında TTP'nin bir emanetçi pozisyonunda olduğu bu mesajlaşmada çevrim içi olarak yer alan TTP, mesajı doğrudan taşıma ve kayıtları saklama yükümlülüğünden kurtulmakta ve sadece mesaja ilişkin oturum anahtarı ile NRR delili gibi bilgileri taşımaktadır (Abadi vd., 2002; Oppliger ve Stadlin, 2004).

TTP'nin mesaj akışının bazı kısımlarından soyutlanmış olması nedeniyle bu yöntem merkezi TTP yöntemine göre daha verimli görünmektedir. Bununla birlikte mesajı göndermeme veya silme gibi bir imkâna sahip olmasa da TTP'ye güven bu yöntemde de söz konusudur. Yani bu yöntem de TTP'ye güven üzerine kurgulanmaktadır.

2.3.2.1.2.3 Çevrim dışı TTP

Çevrim dışı TTP yönteminde TTP, gönderici ve alıcı arasındaki iletişimde yer almamakta ve sadece bir uyuşmazlık ortaya çıktığında iletişime müdahil olmaktadır. Örneğin gönderici alındı kaydını almadığı yönünde bir itirazda bulunursa, alıcı mesajı almadığını iddia ederse, mesaj veya delillerin ilgililerine bazı teknik sebeplerle ulaşmazsa TTP devreye girmektedir.

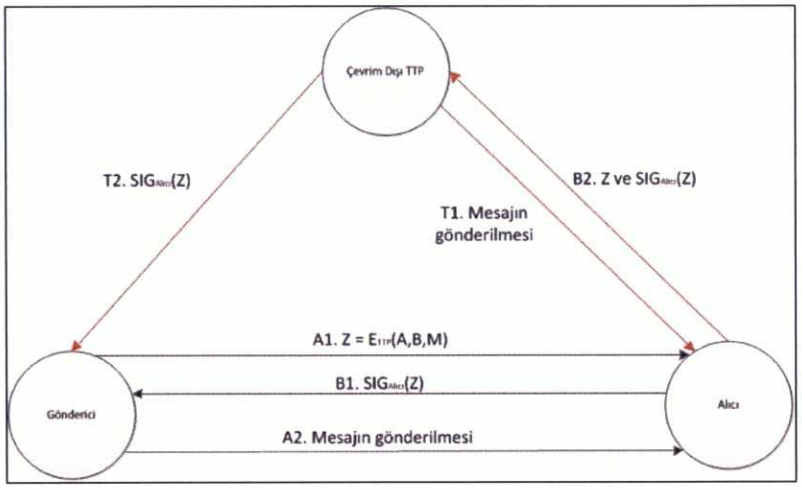
Birçok iletişimde tarafların dürüst davrandığı, hata oluşmadığı ve herhangi bir uyuşmazlığın ortaya çıkmadığı düşünüldüğünde çevrim dışı TTP modeli birçok açıdan en iyi model olarak öne çıkmaktadır. Çünkü yüksek miktardaki mesajlaşmalarda TTP iletişime hiç karışmadığından TTP kaynaklı herhangi bir darboğaz da yaşanmamaktadır (Oppliger, 2007). Bununla birlikte herhangi bir uyuşmazlık halinde çözüme ulaşmak karmaşık olabilmektedir. Örneğin, alıcının, NRR delilini gönderdiğini ve göndericinin de bu delili almadığını iddia ettiği bir uyuşmazlık durumunda tarafların kendi delillerini TTP'ye göndermesi ve TTP'nin kendinde bulunan bu delillere göre bir taraf lehine karar vermesi ve işleyişin düzeltilerek adilliğin sağlanması söz konusu olmaktadır. Bu durum TTP'nin göndericinin isteği, rızası veya yardımı olmadan mesaj içeriğine ulaşabilmesi anlamına gelmektedir.

Bunun yanında çevrim dışı TTP'nin bulunduğu sistem alışılagelmiş şekilde asenkron olarak çalışmakta olan elektronik posta sistemi için uygun değildir. Çünkü çevrim dışı yapısı senkron bir iletişim öngörmektedir. Uyuşmazlıkları iletmek için bir süre belirlenebiliyor olsa da, bu süre içerisinde taraflardan birinin aksiyon almaması halinde sıkıntılar oluşabilmektedir. Mesala alıcının gönderdiği alındı kaydını göndericinin henüz kabul etmediği bir durumda mesaj okunabilmektedir. Ayrıca mesajlaşmaya fazladan adımlar eklendiğinden mesajlaşma uzayarak mesaj boyutları artmakta ve kullanım güçleşmektedir.

TTP'ye bağımlılığı azaltan ve mesaj boyutlarını artırsa da uyuşmazlık durumları hariç protokolün işletilmesi için gereken adım sayısını üçe kadar düşüren yaklaşımlar da bulunmaktadır (Mukherjee ve Dutta, 2012).

Dünyada uygulan ve düzenlenmiş bulunan birçok KEP sisteminin merkezi TTP metodunu kullanması ve birçok avantajına rağmen çevrim dışı TTP metodunun kullanılmamasının nedeni bu modelin teorik kalması ve ticari bir model olarak henüz ortaya çıkmamış olmasıdır (Ferrer-Gomilla vd., 2010).

Şekil 2.6. Çevrim dışı TTP çalışma modeli



Micali (2003) tarafından konu edilen adil bir mesajlaşmayı ele alan ve çevrim dışı TTP kullanan KEP sistemi Şekil 2.6'da verilmiştir. Buna göre;

- Öncelikle A1 adımında gönderici TTP'nin açık anahtarı ile kendisinin ve alıcının tekil tanımlayıcısı ve mesajı şifreleyerek elde ettiği Z değerini alıcıya gönderir.
- Alıcı almış olduğu Z değerini imzalayarak göndericiye alındı kaydı olarak iletir (B1 adımı).
- Gönderici beklediği doğru alındı kaydını aldıktan sonra alıcıya mesajı açık olarak gönderir (A2 adımı).
- Alıcı gelen mesaj ile beraber kendisinin ve göndericinin tekil tanımlayıcısını TTP'nin açık anahtarı ile şifreleyerek kendisine daha önce gelen Z değeriyle karşılaştırır. Bu iki değer birbirine eşit ise protokol tamamlanmış olur. Eğer iki değer birbirine eşit değilse uyuşmazlık durumu ortaya çıkmış demektir ve bu durumda TTP devreye girer. Alıcı kendisine ilk gelen Z değerini ve Z değerinin kendi imzasıyla imzalanmış halini, yani alındı kaydını, TTP'ye gönderir (B2 adımı).
- TTP imzadan alıcıyı tanımlar ve Z'yi kendi gizli anahtarıyla açarak gönderici bilgisine, alıcı bilgisine ve mesaja ulaşır.

- TTP ulaştığı mesajı alıcıya (T1 adımı), imzalı Z değerini de göndericiye ileterek (T2 adımı) protokolün tamamlanmasını ve dolayısıyla uyuşmazlığın giderilmesini sağlamış olur.

Bu sistemlerde merkezi TTP yaklaşımındaki gibi akışa müdahale etmek ve gerekli olabilecek ek delil ve özellikler gerçekleştirmek oldukça güçtür. Diğer taraftan bazı işlemleri gerçekleştirecek ve mesajlaşmanın içerisinde yer alan bir TTP'nin bulunmayışı bu protokolün taraflarını eş zamanlı olmaya zorlamaktadır. Bu husus ise eş zamansız olarak çalışan ve bu şekilde kabul görmüş elektronik posta yapısına pek uygun görünmemektedir.

2.3.2.2 İletişim kanalı

Adil ve inkâr edilemez bir KEP sisteminin en önemli parametrelerinden bir tanesi sistemin üzerinde çalışacağı iletişim kanalının kalitesidir. Bir KEP sisteminde; gönderici, alıcı ve TTP arasındaki iletişim kanalının kalitesi ve güvenilirliği diğer tüm güvenlik özelliklerini de etkilemektedir

Genellikle tasarlanan ve kullanılan birçok KEP sisteminde iletişim kanalında meydana gelebilecek sorunlara ilişkin bir takım önlemler bulunsa da bu sorunlar sistemin istenildiği şekilde tamamlanamamasına sebep olabilmektedir.

Ferrer-Gomilla vd. (2010)'ya göre operasyonel iletişim kanalı, güvenilir olmayan (*unreliable*) iletişim kanalı ve esnek (*resilient*) iletişim kanalı olmak üzere üç çeşit iletişim kanalı tanımı mevcuttur.

2.3.2.2.1 Operasyonel iletişim kanalı

İletilecek verinin sınırlı ve belirli bir zamanda hedefine ulaşabilmesini sağlayan iletişim kanalı operasyonel olarak tanımlanmaktadır. Bu şekildeki iletişim kanalı, mesajın göndericiden alıcıya tam ve doğru bir şekilde ulaştırılabilmesini gerektirmektedir (Ferrer-Gomilla vd., 2010).

Birçok ağ teknolojisi, verileri tam ve doğru bir şekilde karşı tarafa ulaştırmayı garanti etmesine rağmen iletişimin belli bir sürede tamamlanmasını sağlayamamaktadır. Bu nedenle, gerçek hayatta operasyonel iletişim kanalı gerçekleştirilememektedir. İletişim kanalının o andaki yoğunluğu veya fiziki şartlar gibi nedenlerle sürede değişiklikler yaşanabildiğinden genellikle sürenin ayarlanabilmesi de mümkün olamamaktadır.

2.3.2.2.2 Güvenilir olmayan iletişim kanalı

İletişim kanalı üzerinden gönderilen verinin kalıcı olarak kaybolması durumu söz konusu olabiliyor ise bu iletişim kanalı güvenilir olarak kabul edilmemektedir (Ferrer-Gomilla vd. 2010). Günümüzde ek özellikler kullanılmadan doğrudan internet üzerinden yapılan iletişimler bu kategori içerisinde değerlendirilebilir. İnternet üzerinden gönderilen verilerin farklı yapılar içeren sistemlerden geçmesi ve bu sistemlerin hiçbir zaman yüzde yüz iletimi garanti etmemesi nedeniyle bahse konu iletişim güvenilir kabul edilmemektedir.

İletişim kanalında, kasıtlı veya kasıtlı olmayan sebeplerle sorunlar ortaya çıkabilmektedir. Taraflardan birinin bağlantısının; truva atı, virüs veya dağıtık servis kesintisi (Distrubuted Denial of Service-DDoS) saldırısı nedeniyle aksaması hainde mesajlar ağ üzerinde kaybolabilmektedir. Güvenilir olmayan bir iletişim kanalı üzerinde uygulanabilecek birtakım protokoller ile oluşturulan kesintisiz iletişim kanallarıyla mesaj kayıplarının önüne geçilebilmektedir (Ferrer-Gomilla vd., 2010).

2.3.2.2.3 Kesintisiz iletişim kanalı

Kesintisiz iletişim kanalı, geçici bağlantı kayıplarının ve bağlantı katmanında meydana gelebilecek aksaklıkların kalıcı mesaj kayıplarına yol açmadığı iletişim kanalı olarak tanımlanmaktadır. İletişim kanalında meydana gelen veri kayıplarının farkedilmesi ve kaybolan verilerin tekrar gönderilmesi suretiyle veri kayıplarının önlenmesi esasına dayanmaktadır (Grégr, 2011). Böylelikle mesajların karşı tarafa gecikmeli de olsa tam ve doğru gittiği garanti edilebilmektedir.

3. DÜNYADA KAYITLI ELEKTRONİK POSTA YAKLAŞIMLARI

Özellikle son yıllarda güvenli ve inkâr edilemez bir mesajlaşmanın tesisi üzerine KEP veya CEM isimleriyle anılan birçok çalışma yapılmaktadır.

Bu bölümde Almanya, İtalya, Avusturya ve Amerika Birleşik Devletleri'ndeki KEP sistemleri, uygulanan politikalar ve mevcut durum ile AB'nin yaklaşımı incelemektedir. Bununla birlikte incelenen bahse konu KEP sistemlerinin işleyişine göz atılarak değerlendirmelerde bulunulmaktadır.

3.1 Avrupa Birliği Yaklaşımı

Avrupa Parlamentosu ve Konseyi tarafından elektronik imza, elektronik mühür, elektronik zaman damgası, elektronik belge, elektronik kayıtlı iletim servisleri ve internet sayfası doğrulaması yapan sertifika hizmetleri için yasal çerçeveyi tesis etmek amacıyla 910/2014 sayılı bir tüzük yayımlanmıştır. Elektronik Tanımlama ve Güven Hizmetleri (eIDAS) Tüzüğü olarak da adlandırılan bu Tüzük 23 Temmuz 2014 tarihinde kabul edilerek 28 Ağustos 2014 tarihinde yayımlanmıştır. Tüzüğün yürürlük tarihi maddeler bazında değişmekle birlikte bu tez kapsamında ele alınan kayıtlı iletim servisleri ile ilgili kısımların yürürlük tarihi 1 Temmuz 2016 olarak belirlenmiştir.

eIDAS Tüzüğü ile; vatandaşlar, işletmeler ve kamu otoriteleri arasındaki etkileşimde ortak bir temel oluşturularak elektronik işlemlerdeki güvenin tesisi ve bu sayede AB'deki kamu/özel sektör arasındaki çevrim içi servislerin, elektronik iş ve ticaretin artırılması amaçlanmaktadır (AB, 2014).

Tüzüğün yasal çerçevesini çizdiği hizmetlerin verilmesine ilişkin nitelikli ve nitelikli olmayan hizmetler şeklinde iki farklı yaklaşımın benimsediği anlaşılmaktadır. Böylelikle tanımlanan tüm hizmetlerin nitelikli veya niteliksiz olarak verilmesinin önü açılmaktadır.

Tüzük'te KEP sisteminin karşılığı olarak elektronik kayıtlı iletim servisleri (*electronic registered delivery service*) ifadesi kullanılmakta ve KEP bir güven hizmeti olarak ele

alınmaktadır. Bununla birlikte Tüzük'te kayıtlı elektronik iletim hizmeti, üçüncü kişiler arasında elektronik olarak veri alışverişini mümkün kılan, verinin gönderildiğini ve alındığını kanıtlayan, gönderilen elektronik veriyi iletim esnasında herhangi bir kayba, yetkisiz değişikliğe, kaybolmaya veya çalınmaya karşı koruyan bir hizmet olarak tanımlanmaktadır (AB, 2014, m.3).

Tüzük'te güven hizmetlerine ilişkin yerine getirilmesi istenen tüm genel hükümler bir güven hizmeti olarak ele alınan KEP hizmetine de uygulanmaktadır (Pohar, 2015). Verilen hizmetlerin bir güven seviyesi gerektirmesi nedeniyle güven hizmetlerine ilişkin genel hükümler başlığı altında ele alınan ilk hususların tarafların yükümlülükleri ve ispat konuları olduğu görülmektedir.

Tüzük hükümlerinin ihlali halinde uygulanacak cezaların ülkeler tarafından belirlenmesi ve bu cezaların etkili, orantılı ve caydırıcı olması gerektiği hüküm altına alınmıştır (AB, 2014, m.16).

Tüzük'te güven servislerine ilişkin yer alan diğer bir husus ise denetimleri gerçekleştirmek üzere bir kurum veya kuruluşun oluşturulmasıdır. Tüzüğe göre kurulan bu denetim kuruluşunun niteliksiz güven hizmet sağlayıcıları için ex-post denetimler, nitelikli güven hizmet sağlayıcıları için ise ex-ante ve ex-post denetim faaliyetleri ile görevli olması gerektiği ifade edilmektedir. Ayrıca denetim kuruluşunun Tüzük'te belirlenen görevlerini yerine getirebilmesi için güce ve yeterli kaynağa sahip olması gerekliliği de hüküm altına alınmıştır (AB, 2014, m. 17).

Nitelikli olsun veya olmasın güven hizmeti sağlayıcıları sundukları güven hizmetlerini zafiyete uğratacak risklere karşı uygun teknik ve organizasyonel tedbirleri almalıdır. Bu tedbirler özel olarak güvenlik kazalarının sebep olduğu etkinin en aza indirgenmesine ve paydaşlara zarar vermesini engellemeye yönelik olarak alınmalıdır (AB, 2014, m. 19).

Tüzük ile; nitelikli güven hizmeti sağlayıcısının harcamalarının iki yılı geçmeyecek periyotlarda denetime tabi tutulması gerektiği, denetim kuruluşunun istediği zaman

nitelikli güven hizmeti sağlayıcısının harcamalarını denetleyebileceği veya uygunluk değerlendirmesini yapmak üzere bir uygunluk değerlendirme kurumu talep edebileceği, denetimler sonucunda eksiklik veya uygunsuzluk tespit edilmesi halinde nitelikli güven hizmeti sağlayıcısından Tüzüğün koşullarını yerine getirmede gösterdiği eksikliği düzeltmesini istediğinde hizmet sağlayıcı bunu yerine getirmezse, eksikliğin boyutu, süresi ve sonuçlarına bağlı olarak denetim kuruluşu, hizmet sağlayıcıya verilen nitelikli sıfatını veya ilgili hizmetin nitelikli sıfatını kaldırabileceği hüküm altına alınmıştır (AB, 2014, m. 20).

Nitelikli güven hizmetinin verilebilmesi için öncelikle bir yetkilendirme prosedürünün işletilmesi gerekmektedir. Bunun için ilgili firmanın bir uygunluk değerlendirme organından aldığı uygunluk değerlendirme raporuyla birlikte isteğini içeren bir bildirimle ilgili denetleyici kuruma başvuruda bulunacağı, denetleyici kurumun güven hizmeti sağlayıcılarının ve sundukları güven hizmetlerinin Tüzük ile getirilen koşulları sağlayıp sağlamadığını onaylaması gerektiği ve denetleyici kurumun nitelikli güven hizmeti sağlayıcıları ve sundukları nitelikli güven hizmetleri için olan gereklilikleri özellikle denetlemesi gerektiği yine Tüzük ile belirlenen hükümler arasında yer almaktadır (AB, 2014).

Yetkilendirmeyi müteakip her bir ülkenin sorumlu olduğu nitelikli güven hizmeti sağlayıcıları ile bunların sunduğu hizmetlerle ilgili bilgileri içeren güvenli listeleri otomatik işlemeye uygun bir formda güvenli bir şekilde elektronik imzalanmış veya mühürlenmiş bir şekilde oluşturması, yönetmesi ve yayınlaması gerekmektedir (AB, 2014, m.22). Yetkilendirilen ve herhangi bir üye devletin listesinde yer alan nitelikli güven hizmet sağlayıcıları AB güven işaretini kullanabilmektedir (AB, 2014, m.23).

AB Konseyi gerek yetkilendirme gerekse denetim esnasında akreditasyon yapısı öngörmektedir. Bu amaçla Tüzüğe göre akredite edilmiş, güven hizmeti sağlayıcısının ve sunduğu nitelikli güven hizmetlerinin uygunluk değerlendirmesini gerçekleştirmekle sorumlu bir kuruluşun bulunması öngörülmektedir. Bu kuruluş her ülke için ayrı olabileceği gibi ülkeler arası bir kuruluş da olabilmektedir (AB, 2014).

Nitelikli güven hizmet sağlayıcıların sahip olması gerekli olan şartlar Tüzük'te detaylı olarak belirlenmiştir. Bu şartlardan bazıları;

- Hizmet vereceği kişilerin kimlik doğrulamalarının uygun bir şekilde yapılması,
- İstihdam edilen veya ettirilen personel ve hizmet alınan tarafların niteliklerinin yapılan işe uygun olmasının sağlanması,
- Hasar sorumluluğu riskine istinaden yeterli kaynağın sağlanması ve/veya uygun sorumluluk sigortası alınması,
- Yetkisiz müdahaleye karşı korunmuş emniyetli sistem ve ürünlerin kullanılması,
- Kullanılan ürün ve sistemlerin sağladığı işlemlerin de güvenilir ve teknik olarak güvenli olduğundan emin olunması,
- Bilgilerin emniyetli sistemler kullanarak teyit edilebilir bir formda kaydedilmesi,
- Veri sahtekârlığı ve hırsızlığına karşı uygun önlemlerin alınması,
- Kayıtların yasal soruşturmalarda delil olarak kullanılabilmesi ve hizmetin devamlılığını sağlama amacıyla uygun bir zaman dilimi süresince saklanması ve erişilebilir tutulması

şeklindedir (AB, 2014).

Tüzük'de öncelikle kayıtlı elektronik iletim hizmetlerinin hukuki geçerliliğine ilişkin hususlara yer verildiği görülmektedir. Buna göre;

- Elektronik kayıtlı iletim hizmetleri kullanılarak gönderilen/alınan verinin nitelikli koşullarını sağlamaması durumunda hukuki geçerliliğinin ve davalarda ispatlayıcı delil olarak kabul edilebilirliğinin engellenemeyeği,
- Nitelikli bir elektronik kayıtlı iletim hizmeti kullanılarak gönderilen veya alınan verinin, bildirilen gönderici tarafından gönderildiğinin, belirtilen adrese teslim edildiğinin, gönderme/teslim alınma tarih ve saatinin doğruluğunu sağlandığının varsayılacağı

belirtilmektedir (AB, 2014, m.43).

Ayrıca nitelikli elektronik kayıtlı iletim hizmetlerinin bir ya da daha fazla güven hizmet sağlayıcısı tarafından sağlanması, göndericinin kimliğinin doğruluğunu yüksek güvenilirlik seviyesinde garanti etmesi, verinin tesliminden önce adres tanımlamasının doğruluğundan emin olması, verinin gönderilmesi veya alınması için gereken bilgilerdeki herhangi bir değişikliği göndericiye ve alıcıya açıkça bildirmesi, gönderme, alma ve verilerde meydana gelen herhangi bir değişikliğe ilişkin tarih ve zaman bilgisini nitelikli elektronik zaman damgası ile belirtmesi gerektiği hüküm altına alınmıştır. Bununla birlikte gönderilen verinin değiştirilmesi olasılığının engellenmesi amacıyla gönderilen/alınan verinin nitelikli güven hizmet sağlayıcısı tarafından sunulan gelişmiş elektronik imzayla imzalanarak veya elektronik mühürle mühürlenerek güvence altına alınması gerektiği belirtilmiştir (AB, 2014, m. 44).

Hizmet sağlayıcıların; kişisel verileri işlemeleri durumunda 95/46/EC sayılı Direktif'e uygun davranmaları, mümkün olduğu müddetçe güven hizmetleri ve bu hizmetleri sunarken kullanılan son kullanıcı ürünlerinin engelli bireyler için de erişilebilir olarak tasarlamaları gerekmektedir. Ayrıca ulusal kanunlarda verilen haklar saklı kalmak koşulu ile elektronik işlemlerde takma isim kullanımının yasaklanmayacağı da hüküm altına alınmıştır (AB, 2014).

3.2 Ülke Uygulamaları

Bu bölümde KEP sistemini kullanan ve iyi uygulama örnekleri olarak bilinen Almanya, İtalya, Avusturya ve ABD'deki KEP sistemlerinin hukuki ve teknik altyapısı, işleyişi ve bu ülkelerdeki mevcut durum incelenmektedir.

3.2.1 Almanya (De-Mail)

3.2.1.1 Hukuki altyapı

Federal yönetim tarafından Almanya'da kamu kurum kuruluşlarının, özel şirketlerin ve vatandaşların kullanımına sunulmak üzere yasal olarak geçerli, güvenilir ve

delillendirilebilen bir iletişim altyapısı oluşturmak üzere De-Mail projesi geliştirilmiştir. Bu amaçla Ekim 2009'da Friedrichshafen şehrinde bir pilot proje başlatılmıştır (Sievers, 2009).

Altı ay olarak tasarlanan bu pilot projeye dört hizmet sağlayıcısıyla birlikte test kullanıcıları olarak bankalar, çeşitli şirketler ve kamu kurumları katılmıştır. Ücretsiz olarak gönderilerin gönderildiği ve testlerin yapıldığı bu pilot proje ile farklı uygulama alanlarındaki işletmeler ve kamu kurum kuruluşları arasındaki kullanımın izlenmesi amaçlanmıştır. Bu sayede sistem devreye alınmadan önce kullanıcıların yaşadığı zorluk ve problemler tespit edilerek giderilmiş ve tanınmış bir platform sunma hedeflenmiştir (Schumacher, 2010).

De-Mail hizmetlerinin verilebilmesi için kurumsal ve yasal düzenleme getiren De-Mail Kanunu veya diğer bir ifadeyle Vatandaş Portalı Kanunu (De-Mail Act, 2011) 3 Mayıs 2011'de yürürlüğe girmiştir (Schumacher, 2014). Müteakiben üç KEPHS'nin yetkilendirilmesiyle birlikte De-Mail sistemi resmi olarak Mart 2012'de hizmete başlamıştır (Tauber vd., 2013). Hâlihazırda De-Mail'in teknik düzenlemeleri Federal Office for Information Security (Bundesamt fur Sicherheit in der Informationstechnik-BSI) tarafından gerçekleştirilmektedir (BSI, 2011).

Özellikle yaygın uygulama örneklerinden farklı olması ve Türkiye'deki KEP sistemi ile birçok benzer yanı bulunması itibariyle Almanya'daki mevzuatın değerlendirilmesi ve bilinmesi önem arz etmektedir.

De-Mail Kanunu'nun ilk kısımında De-Mail sisteminin ve servislerinin genel bir tanımı yapılmış ve uygulamadan sorumlu olarak olarak Federal İçişleri Bakanlığı ile ilişkili bir kurum olan BSI belirlenmiştir (De-Mail Act, 2011, m.2).

De-Mail Kanunu'nun ikinci kısmında De-Mail hesabının açılması, De-Mail hesap başvurusunun yapılması, posta kutusu ve gönderim servisleri, kimlik doğrulama servisleri, dizin hizmeti ve arşiv hizmetleri gibi hizmet sağlayıcılar tarafından

sunulması zorunlu ve isteğe bağlı hizmetlere yer verilmiştir (De-Mail Act, 2011, m.3-8).

De-Mail Kanunu'nun 7 maddeden oluşan üçüncü kısmında ise De-Mail servislerinin kullanım usulleri detaylandırılmaktadır. Bu kısmın altında; 9'uncu maddede kullanıcıların hesap kullanımına ve hesabın güvenliğinin sağlanmasına yönelik bilgilendirilmesine ve bu bilgilendirmenin ne şekilde ve nasıl yapılacağına, 10'uncu maddede De-Mail hesaplarının askıya alınmasına, kullanıma kapatılmasına ve tekrar kullanıma açılmasına ilişkin hususlara, 11'inci maddede hizmet sağlayıcıların faaliyetlerine son vermesine, 12'nci maddede kullanıcılarla yapılan sözleşmelerin fesihi ile ilgili hükümlere, 13'üncü maddede hizmet sağlayıcıların belgelendirme yükümlülüğüne, 14'üncü maddede gençlik ve tüketicinin korunmasına ilişkin genel hususlara, 15'inci maddede kişisel verilere ilişkin gizlilik hükümlerine ve 16'ncı maddede bilgi edinme hakkına ilişkin hükümlere yer verilmiştir (De-Mail Act, 2011, m.9-16).

De-Mail Kanunu'nun dördüncü kısmında; 17'nci maddede hizmet sağlayıcısı olmak isteyen tarafların başvuruları ve bu başvuruların değerlendirilmesine, 18'inci maddede yetkilendirme için gerekli teknik, hukuki ve finansal şartlara ve 19'uncu maddede yabancı ülkede kurulu bir hizmet sağlayıcısının Almanya'da kabul edilmesine ilişkin hükümlere yer verilerek hizmet sağlayıcıların yetkilendirme süreci belirlenmektedir (De-Mail Act, 2011, m.17-19).

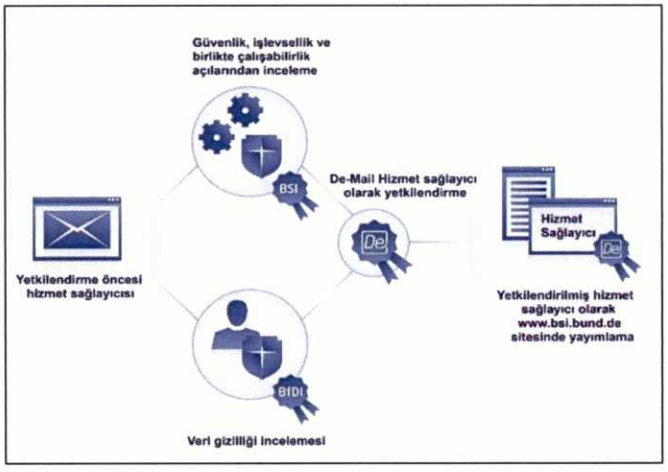
De-Mail Kanunu'nun beşinci kısmında hizmet sağlayıcıların denetimleri detaylandırılak, 20'nci maddede denetleyici önlemlerle birlikte denetimin gerçekleştirilme yöntemine, sonuçlarına ve denetim sürecinde talep edilebilecek veya edilemeyecek bilgi ve belgeleri, 21'inci maddede ise BSI'nın yetkilendirilen hizmet sağlayıcılarının listesini kamuya açık bir dizinde yayımlama yükümlülüğüne ilişkin hükümlere yer verilmektedir (De-Mail Act, 2011, m.20-21).

Son hükümler başlıklı altıncı ve son kısımda ise; yılda en az bir defa toplanması öngörülen, tüm paydaşlardan temsilcilerin yer aldığı De-Mail standardizasyon

komitesinin yapısı ve çalışması, servis sağlayıcılara verilebilecek cezalar, idari ücretler ve masraflar ele alınmaktadır (De-Mail Act, 2011, m.22-24).

De-Mail Kanunu'nun yukarıda da bahsedilen 17 ve 18'inci maddelerine göre De-Mail hizmet sağlayıcısı olarak hizmet vermek isteyen tarafların BSI'ya başvurmaları ve BSI tarafından yetkilendirilmeleri gerekmektedir. Hizmet sağlayıcısı olmak üzere başvuruda bulunan tarafların güvenlik, işlevsellik ve birlikte çalışabilirlik açılarından değerlendirilmesi BSI tarafından, veri gizliliği ve koruma hususlarına ilişkin değerlendirilmesi ise Alman Federal Veri Koruma Kurulu (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit-BfDI) tarafından gerçekleştirilmektedir. Yapılan değerlendirmeler sonucunda hizmet sağlayıcısı olmaya hak kazanan taraflar De-Mail hizmet sağlayıcı olarak yetkilendirilerek yine De-Mail Kanunu gereği kamuya açık bir dizin olan "*www.bsi.bund.de*" internet sitesinde yayımlanmaktadır (Bkz. Şekil 3.1).

Şekil 3.1. Almanya hizmet sağlayıcıların yetkilendirme süreci



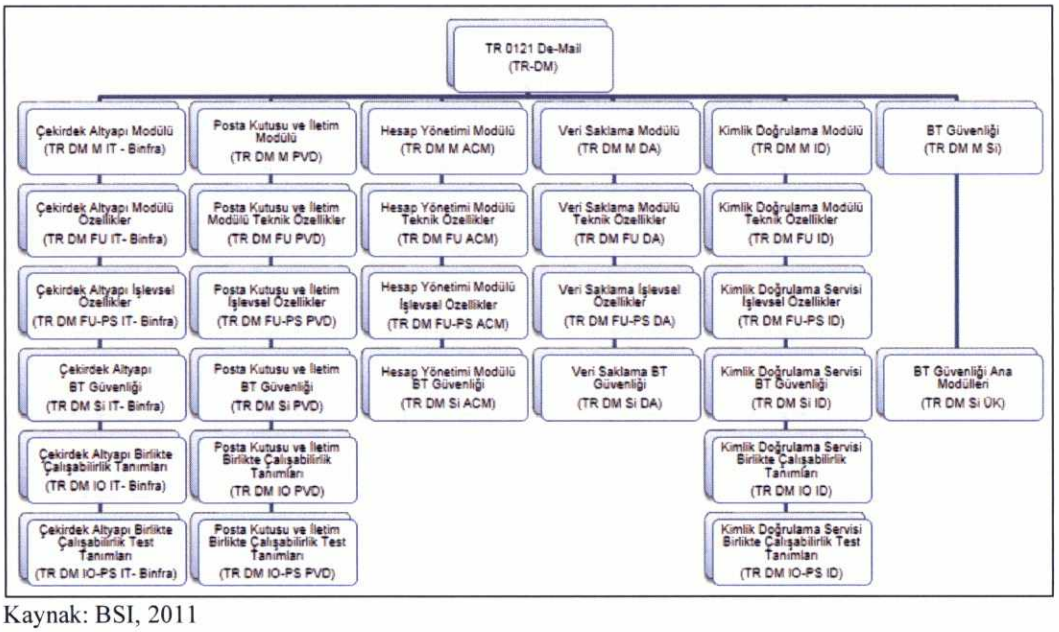
Kaynak: http://www.cio.bund.de/

Hizmet sağlayıcı olmak üzere yetkilendirme başvurusunda bulunacak olan işletmelerden, ISO 27001 sertifikasına sahip olmaları bir ön şart olarak istenmektedir. Bunun yanı sıra sunacağı hizmetler açısından teknik klavuz dokümanlarına uygunluk ve BfDI tarafından verilecek veri gizliliği sertifikasının alınması akabinde

yetkilendirme süreci tamamlanmaktadır (Schumacher, 2014). De-Mail Kanunu'na göre yetkilendirme sürelidir ve önemli bir değişiklik meydana gelmediği müddetçe üç yılda bir yenilenmek zorundadır (2011, m.17).

De-Mail Kanunu'nun hemen altında genel anlamda işleyiş ve güvenliğe yönelik teknik dokümanlardan oluşan ikincil düzenlemeler bulunmaktadır. BSI tarafından hazırlanan bu teknik düzenlemelerin yapısı hiyerarşik olarak Şekil 3.2'de verilmektedir. Buna göre sistemin işleyişi ve uyulması gereken teknik standartları belirleyen TR 01201 kodlu, "De-Mail Teknik Kılavuz" başlıklı BSI Teknik Direktifi, De-Mail sistemindeki servisler bazında modülleri ve hiyerarşide yer alan diğer dokümanlara yapılan atıfları barındırmaktadır. Ayrıca kılavuzda BSI'nın yetkilendirme çerçevesine, işlevselliğe, güvenliğe ve birlikte çalışabilirliğe ilişkin hususların teknik detayları, De-Mail sisteminin gereklilikleri, verilmesi gereken hizmetler ve bu hizmetlerin hangi teknik kriterlere uygun olması gerektiğine ilişkin hususlar ve belirlenen gerekliliklerin test gereksinimleri yer almaktadır (De-Mail Teknik Klavuz, 2014).

Şekil 3.2. BSI De-Mail teknik doküman yapısı



Kaynak: BSI, 2011

3.2.1.2 Teknik altyapı

Elektronik posta yapısı üzerine kurulan De-Mail sistemi, SMTP kullanarak mesajlaşmayı sağlamaktadır. Sistemdeki hizmet sağlayıcıları, ikinci bölümde bahsedilen gönderici ve alıcı arasında bulunan merkezi TTP şeklinde hizmet vermektedirler (Tauber vd, 2013).

Gönderici ve alıcıların De-Mail sistemini kullanabilmeleri için herhangi bir hizmet sağlayıcıdan hesap açtırmaları gerekmektedir. Sistemde bireysel, özel veya kamu tüzel kişilere hesap açılabilmekte ve bu hesapların ilk tanımlanması esnasında gerek bireysel kişiler için gerek de tüzel kişiler için katı kimlik doğrulama kuralları uygulanmaktadır. Örneğin gerçek kişiler sisteme kaydolurken kimlikleri kimlik kartı, pasaport gibi geçerli bir kimlik belgesiyle doğrulanmaktadır. Diğer taraftan tüzel kişilerin ve yetkilililerinin kimlikleri ve yetkili olduklarına dair doğrulamalar şirket kuruluş dokümanları, ticaret sicil kayıtları gibi resmi belgelere dayanılarak doğrulanmaktadır. Hatta Kanunun ilgili maddesinde hizmet sağlayıcıların gerçek ve tüzel kişilerden başvuru sırasında almaları gereken bilgi ve belgelerin neler olacağı da belirlenmiştir (De-Mail Law, 2011, m.3). Ayrıca çevrim içi ortamlarda Alman kimlik kartı olarak da kullanılan ve aynı zamanda AB elektronik imza direktifi (Avrupa Parlamentosu ve Konseyi, 1999) kapsamındaki nitelikli elektronik sertifika (Qualified Electronic Signatures-QESs) da yüklenebilen Alman eID kimlik kartı (nPA) da sisteme dâhil olmak üzere kullanılabilmektedir (Tauber vd., 2013).

Kimlikleri resmi belgelere dayanılarak doğrulanan kullanıcılar sistemde kendilerine tanımlanan hesaplarına; standart olarak adlandırılan kullanıcı adı ve şifre ya da güvenli kimlik doğrulama olarak adlandırılan kullanıcı adı ve şifrenin yanı sıra tek kullanımlık şifre (One Time Password-OTP) veya nPA kullanılmak suretiyle erişim sağlayabilmektedir (De-Mail Law, 2011, m.4).

De-Mail sisteminde farklı güvenlik özelliklerine sahip iki farklı iletişim kanalı kullanılmaktadır. Bunlardan ilki gönderici ve alıcı, yani sistemin kullanıcıları ile hizmet sağlayıcı arasındaki ve De-Mail Kanunu'na göre şifreli olması gereken

bağlantıdır (2011, m.4). Bu da SSL veya TLS kullanılmak suretiyle sağlanabilmektedir. Diğeri ise hizmet sağlayıcılar arasındaki iletişimde kullanılan, karşılıklı kimlik doğrulamayı mümkün kılacak şekilde ve şifreli olması gerektiği De-Mail Kanunu ile hüküm altına alınmış ve uçtan uca şifreleme sağlayan kanaldır (De-Mail Law, 2011, m.5).

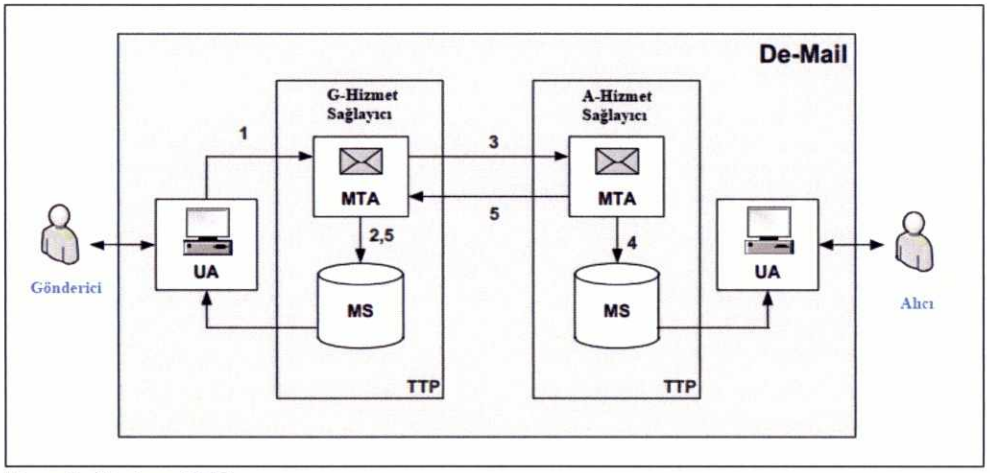
De-Mail Kanunu'nun 5'inci maddesinde sistemde bulunan inkâr edilemezlik servislerine, posta kutusu servislerine ve posta gönderim kısmına ilişkin tanımlanmalara yer verilmektedir (2011, m.5). Bu tanımlamalara göre gönderici tarafından talep edilmesi halinde göndericinin hizmet sağlayıcısının göndericinin De-Mail adresi, hizmet sağlayıcı tarafından oluşturulan zaman damgası, hizmet sağlayıcının ismi ve gönderilen mesajın özet değerini içeren NRS delilini oluşturup alıcıya göndermesi gerekmektedir. Ayrıca göndericinin hizmet sağlayıcısı NRS delilinin Alman İmza Kanunu'na uygun nitelikli elektronik sertifika ile imzalanmasından da sorumlu tutulmaktadır. Yine De-Mail Kanunu 5'inci maddesi uyarınca göndericinin talep etmesi halinde alıcının hizmet sağlayıcısı tarafından NRS delili ile aynı verileri içeren NRD delilinin oluşturulması ve göndericiye sunulması gerekmektedir. Bu NRD delilinde sadece gönderici hizmet sağlayıcının adı ve imzası yerine alıcı hizmet sağlayıcısının adı ve imzası yazılmaktadır. NRS delili mesajın alıcının posta kutusuna başarılı bir şekilde teslim edildiğini kanıtlamak üzere kullanılmaktadır (Tauber vd., 2013).

De-mail Kanunu'na göre resmi gönderilere ilişkin mevzuat ile kendilerine resmi gönderim imkânı tanınan kamu kurumları NRR delilini talep edebilme hakkına sahiptir (De-Mail Law, 2011, m.5). Bu durum alıcının yukarıda bahsedilen güvenli kimlik doğrulama mekanizması ile sisteme giriş yapmasını gerektirmektedir. NRR delili, NRD delilinde yer alan veriler ile birlikte alıcının kimlik doğrulama verilerini de içermektedir. Bu delil de yine alıcının hizmet sağlayıcısının güvenli elektronik imzasıyla imzalanmaktadır (Tauber vd., 2013).

3.2.1.3 Sistemin işleyişi

Gönderici ve alıcının farklı hizmet sağlayıcılardan hizmet aldığı bir senaryoya göre sistemin işleyiş adımlarına Şekil 3.3'te yer verilmektedir. Buna göre sistemin işleyişi aşağıdaki şekildeki gibi gerçekleşmektedir (Tauber, 2011).

Şekil 3.3. Almanya De-Mail sisteminin yapısı ve işleyişi



Kaynak: Tauber, 2011

1. Göndericinin UA'sı, kimlik doğrulamasından geçerek gönderici servis sağlayıcıya bağlanır ve mesajı güvenli bir kanal üzerinden MTA'ya iletir. Göndericinin güvenli kimlik doğrulama ile sisteme dâhil olması halinde bu durumu mesajda bir bayrak kurularak gösterilir. Ayrıca mesaj, sadece alıcının görebilmesi için uçtan uca şifrelenebilmekte (E2EE) ve/veya NRO delili için güvenli elektronik sertifika (Qualified Electronic Certificate-QEC) kullanılarak imzalanabilmektedir.
2. Göndericinin hizmet sağlayıcısı mesajda tanımlı olan alıcıların bulunup bulunmadığı, başlık bilgileri, üst veriler gibi veriler ile mesaj üzerindeki kontrollerini gerçekleştirir ve orijinal mesajın özet değerini ve zaman damgası içeren NRS delilini oluşturarak göndericinin MS'sine kaydeder. De-Mail standartları bu delilin bir donanımsal güvenlik modülü (Hardware Security Module-HSM) kullanılarak imzalanmasını önermektedir.

3. Göndericinin hizmet sağlayıcısı, mesajı, alıcının hizmet sağlayıcısının açık anahtarı ile şifreleyerek alıcının MTA'sına gönderir.
4. Alıcının MTA'sı mesajı teslim aldığında öncelikle şifresini çözer ve gerekli kontrollerini yaptıktan sonra mesajı alıcının MS'sine bırakır. Eğer gönderici mesajı kısıtlı veya gizli gönderim şeklinde işaretlemişse alıcı bu mesaja ancak ve ancak güvenli kimlik doğrulama yöntemleriyle bağlandıktan sonra ulaşabilir.
5. Son olarak alıcının MTS'si orijinal mesajın özet değerini ve zaman damgasını içerecek şekilde NRD delilini üretir ve bu delili göndericinin MTA'sına gönderir. Göndericinin MTA'sı da bahse konu delili göndericinin MS'sine koyar. De-mail Kanunu ile NRS deliline benzer şekilde NRD delilinin de alıcının hizmet sağlayıcısı tarafından HSM vasıtasıyla imzalanması önerilmektedir.

3.2.1.4 Mevcut durum

De-Mail Kanunu'nun yürürlüğe girmesi ile birlikte yetkilendirilen hizmet sağlayıcıların tamamının aynı kriterlere göre yetkilendirilip testlerden geçmeleri ve böylece Almanya genelinde sistemin tamamının aynı güvenlik düzeyinde olması sağlanmıştır. e-Devlet dönüşümü programının bir parçası olarak ele alınan bu sistem vasıtasıyla fiziki ortamdaki güvenli bilgi ve belge alışverişi elektronik ortama da taşınmıştır (Schumacher, 2014).

Güvenli ve güvenilir bir elektronik haberleşme altyapısı sunan De-Mail sisteminde, yetkilendirilen hizmet sağlayıcılar güvenlik ve güvenilirliğin temelini oluşturmaktadır. Bu sebeple hizmet sağlayıcılar BSI tarafından belirlenen yüksek güvenlik gerektiren standartlara uygunluk açısından yine BSI tarafından düzenli aralıklarla denetlenmekte ve gözden geçirilmektedirler (Schumacher, 2014). Almanya'da hali hazırda yetkilendirilen dört De-Mail hizmet sağlayıcısı bulunmaktadır (Bkz. Tablo 3.1).

Tablo 3.1. Almanya yetkilendirilen De-Mail hizmet sağlayıcılar

Hizmet Sağlayıcı	Hizmetler	Alan Adları	Yetkilendirmenin Geçerlilik Tarihi
1 & 1 De-Mail GmbH	Mailbox & Shipping Services,Directory Service	1und1.de-mail.de gmx.de-mail.de sec.de-mail.de web.de-mail.de	05.03.2016
Mentana-Claimsoft GmbH	Mailbox & Shipping Services, Directory Service	fp-demail.de mc-demail.de fpbrief.de-mail.de anwalt.de-mail.de	06.03.2015
T-Systems International GmbH	Mailbox & Shipping Services, Directory Service	de-mail-t-systems.de-mail.de	06.03.2015
Telekom Germany GmbH	Mailbox & Shipping Services, Directory Service	t-online.de-mail.de	06.03.2015

Kaynak: https://www.bsi.bund.de

Diğer taraftan sektör uzmanlarının katılımı ile kurulan ortak bir çalışma grubu vasıtasıyla De-Mail sisteminin tanıtım ve geliştirme çalışmaları sürdürülmektedir. Ayrıca sisteme giriş aşamasında kullanılan kullanıcı adı ve şifre gibi güvenli olmayan yöntemlerin nPA kullanımı gibi güvenli yöntemlerle değiştirilmesi yönünde bir takım çalışmalar da yürütülmektedir (Schumacher, 2014).

Ayrıca Almanya'da e-Devlet Kanunu (E-Government Act, 2013) ile tüm Federal Kurumların elektronik bilgi ve belge paylaşabilmek amacıyla bir De-Mail hesabı edinmeleri zorunluluğu getirilmiştir. İdari Usul Kanunu ile getirilen düzenlemeye göre de güvenli kimlik doğrulamasının yapılması şartıyla De-Mail vasıtasıyla iletilen elektronik belgeler yazılı belgelerin yerine geçebilmektedir (Schumacher, 2014).

Sistemin kullanımı ve yaygınlaştırılmasının sağlanabilmesi amacıyla ilgili bakanlık tarafından 53 kuruluşun De-mail ve eID kartlar ile ilgili 71 uygulamasının gerçekleştirimi için tavsiye ve destekler verilmiştir. 2014 yılı ilk altı ayında dört kurum De-Mail erişim noktasını açmış durumdadır. Kalan kurumlar ise bu erişim noktalarını

açmak üzere yürüttükleri projelerini tamamlamaya çalışmaktadır (Rogall-Grothe, 2014).

3.2.2 İtalya (PEC)

3.2.2.1 Hukuki altyapı

İtalyan'da kurulan Kayıtlı Elektronik Posta (Posta Elettronica Certificata-PEC) kamu ve özel sektörün kullandığı bir KEP sistemidir. Sistemin hukuki temelleri 11 Şubat 2005'te İtalyan Cumhurbaşkanlığı'nın yayımladığı 68 numaralı Kararname (İCK, 2005) ile atılmıştır (Mula, 2015). Bu kararnamede PEC sisteminin ana hedefleri, işleyişi, inkâr edilemezlik servisleri, deliller, güvenlik önlemleri gibi birçok teknik ve idari hususa yer verilmiştir (Tauber vd., 2013). Müteakiben 7 Mart 2005'te yayımlanan ve 1 Ocak 2006'da yürürlüğe giren 82 numaralı Dijital Yönetim Kanunu[1] (Digital Administration Code - Codice Dell'amministrazione Digitale) çıkarılmıştır. Bu Kanun ile söz konusu 68 numaralı Kararnameye atıf yapılmış ve PEC'e ilişkin çok temel birkaç prensip tanımlanmıştır (Notarmuzi, 2015).

İCK (2005)'de de atıf yapılan 2 Kasım 2005 tarih ve 266 sayılı mevzuat (İC, 2005a) ile PEC'nin çalışma yapısını tarifleyen teknik kurallar tanımlanmıştır. Bu mevzuatın ekinde ise elektronik dokümanların PEC ile taşınmasına ilişkin teknik tanımlamalara yer verilmiştir (İC, 2005b).

Toplam 17 maddeden oluşan ve temel mevzuat hükmünde kabul edilen İCK (2005)'de genel ifadelerle PEC'de olması gereken hususlar düzenlenmiş, uygulamaya ilişkin detaylar ise teknik kuralları içeren bir alt düzenlemeye (İC, 2005b; 2005b) bırakılmıştır.

Mevzuatın amacı, düzenlemenin "Kapsam ve Tanımlar" başlıklı birinci maddesinde kayıtlı elektronik posta aracılığıyla elektronik belge/doküman gönderme hizmetinin

[1] http://www.agid.gov.it/agenda-digitale/codice-amministrazione-digitale

tahsisini, kullanılma yöntemini ve niteliğini düzenlemek olarak ifade edilmektedir. Yine aynı maddede PEC sistemi ile ilgili taşıma zarfı, sertifikasyon verisi, KEP mesaj alanı, zaman damgası, mesaj işlem kayıtları gibi kavramların tanımlarına yer verilmektedir (İCK, 2005, m.1). İkinci maddede ise PEC sistemindeki göndericinin, alıcının ve hizmet sağlayıcısının tanımları yapılmaktadır (İCK, 2005, m.2).

Üçüncü maddede elektronik dokümanların iletimi, dördüncü maddede ise KEP sisteminin kullanımı düzenlenmiş ve yine bu maddede KEP mesaj gönderiminin hukuki bir geçerliliğe sahip olduğu hüküm altına alınmıştır (İCK, 2005, m.3-4).

Beşinci maddede mesajların iletimi ve birlikte çalışabilirliğe ilişkin hususlar ele alınmış ve bu hususlarda temel çerçeve belirlenerek detaylı düzenlemeler ikincil mevzuata (İC, 2005b; 2005b) bırakılmıştır. Sistemin temel işlevlerinden olan adillik ve inkâr edilemezliği sağlamak üzere tasarlanan delillere ilişkin hususlara altıncı ve yedinci maddelerde yer verilmiş, altıncı maddede kabul ve dağıtım alındılarının, yedinci maddede ise devir alındısının ne zaman, hangi şartlarda ve ne şekilde oluşturulacağı düzenlenmiştir (İCK, 2005, m.5-7).

Sekizinci madde, bir iletinin tesliminin yapılamaması durumunda başarısız teslimat uyarısının üretilmesine ilişkin hüküm barındırmaktadır. Dokuzuncu maddede PEC hizmet sağlayıcıların ürettikleri iletiler ve taşıma zarflarının elektronik olarak imzalanması gerektiği belirtilerek (İCK, 2005, m.8-9), teknik kuralları ele alan İC (2005b; 2005b)'de iletilerin kaynağını, bütünlüğünü ve orijinalliğini garanti etmek amacıyla güvenli elektronik imza kullanılması öngörülmüştür.

Onuncu maddede sistemdeki zaman damgası kullanımı düzenlenmiş ve hizmet sağlayıcısının her mesaja bir zaman damgası, mesaj işlem kayıtlarına ise günlük olarak bir zaman damgası eklemesi gerektiği hüküm altına alınmaktadır. Onbirinci maddede iletimin güvenliği hususu ele alınarak KEP hizmet sağlayıcılarının;

- KEP mesajını, göndericiden alıcıya iletiminin her aşamasında taşıma zarfının içinde taşıması,

- KEP mesajının iletimi esnasında meydana gelen işlem kayıtlarını tutması ve bu işlem kayıtlarını 30 ay süreyle saklaması,
- Muhafaza süresi boyunca işlem kayıtlarının gizliliğini, güvenliğini ve bütünlüğünü garanti etmek üzere en iyi teknik ve örgütsel çözümleri sağlaması

hususları hüküm altına alınmıştır (İCK, 2005, m.10-11).

Onikinci maddede virüslü bir ileti alınması durumundaki davranışa ilişkin kurallar ve onüçüncü maddede minimum hizmet seviyesi (Service Level Aggrement-SLA) zamanları belirlenerek KEP hizmet sağlayıcıların kesintisiz hizmet vermelerine yönelik önlemleri almaları zorunlu tutulmaktadır. Ondördüncü maddede ise hizmet sağlayıcılarda aranan şartlar sıralanarak, KEP hizmet sağlayıcısı olmak isteyen tarafların İtalya Dijital Ajansı'na[2] (The Agency for Italy Digital-AGID) başvurmaları ve belirli bir ödenmiş sermayeye sahip olmaları, başvuru için bankadan alınacak bir teminat mektubunun da sunulması, yönetici ve ortaklarının adli durumlarına ilişkin bazı şartların sağlanması gereklilikleri hüküm altına alınmıştır. Ayrıca hizmet sağlayıcılar faaliyeti sırasında oluşabilecek risklere ve üçüncü kişilere verilebilecek hasarlara karşı sigorta poliçesi sağlamakla, hizmetlerini güvenli bir şekilde yürütebilecek teknik ve örgütsel yapısını sunmakla, hizmetin gerektirdiği nitelikte, elektronik posta ve güvenlik prosedürleri konusunda deneyimli personel istihdam etmekle, Kanunun ve ikincil mevzuatın gereklerini yerine getirmekle, uygun prosedürleri ve yönetimsel metotları uygulamakla, elektronik imza ve uygun cihazlar kullanarak Avrupa ve uluslararası kriterlere göre bilgilerin güvenliğini sağlamakla, hizmetin bütünlüğünü ve güvenliğini garanti etmek üzere uygun tedbirleri almak ve uygulamakla, her durumda iletimin tamamlanmasını garanti etmek için acil durum hizmetlerini öngörüp uygulamakla ve kalite belgelerini almakla yükümlü kılınmaktadır (İCK, 2005, m.12-14). Yine aynı maddede yetkilendirme süreci en fazla 90 gün olarak belirlenerek düzenleyici ve denetleyici kuruma bir sınırlama getirilmektedir. Bu kapsamda AGID, 90 gün içinde hizmet sağlayıcısı olmak üzere yapılan başvuruya herhangi bir yanıt vermezse başvuru sahibi bu sürenin sonunda

[2] Kamu Yönetimi Ulusal Bilişim Merkezi (The National Centre for ICT in Public Administration-DigitPA)'nin 2012 yılında yeniden yapılandırılması ile AGID adını almıştır.

otomatik olarak yetkilendirilmiş olarak kabul edilmektedir (Falciai ve Liberati, 2006). Aynı maddede ayrıca hizmet sağlayıcıların yönetimini veya KEP hizmetini ilgilendiren herhangi bir organizasyonel veya teknik değişikliğin 15 gün içinde düzenleyici kuruma bildirilmesi gerektiği, düzenleyici kurumun kontrol yetkileri, hizmet sağlayıcının sunduğu hizmetlerde herhangi bir eksiklik tespit edilmesi halinde hizmet sağlayıcının çalışmasının durdurulması ve hizmet sağlayıcının listeden çıkarılması gibi hususları içeren hükümler de yer almaktadır (İCK, 2005, m.14).

Onbeşinci madde ile AB'nin diğer ülkelerinde bulunan hizmet sağlayıcıların bahse konu Kanun ve ilgili ikincil mevzuattaki hükümleri yerine getirmesi ve düzenleyici kurumun uygunluğu onaylaması koşuluyla İtalya'da hizmeti verebileceği belirlenmiştir.

Onaltıncı madde ile kamu kurumlarının bağımsız olarak hizmet sağlayıcısı olabilecekleri gibi Kanunla belirlenen teknik ve güvenlik kurallarına göre hizmet veren diğer bir özel veya kamu hizmet sağlayıcısından da hizmeti alabileceği hüküm altına alınırken onyedinci maddede ise teknik kuralların yer alacağı ikincil düzenlemelerin kapsamına ve bu düzenlemelerin kim tarafından yapılacağına ilişkin hususlara yer verilmiştir (İCK, 2005, m.15-17).

İtalya'da ana düzenleme haricinde teknik bir düzenleme (İC, 2005a) ile onun eki konumundaki bir başka düzenlemede (İC, 2005b) de sistemin teknik işleyişinin detayları tanımlanmaktadır.

PEC sistemine ilişkin teknik düzenlemeler, İtalyan Başbakanlığı'na bağlı bir Kurum olarak faaliyetlerini sürdüren AGID tarafından yapılmaktadır. Ayrıca PEC hizmet sağlayıcılarının yetkilendirilmesi, denetlenmesi ve teknik mevzuata uygunluklarının izlenmesi görevlerini de AGID yürütmektedir. Uygunluk izlemesi yerinde denetimi de içerecek şekilde gerçekleştirilmektedir[3].

[3] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/posta-elettronica-certificata/vigilanza-sui-gestori-pec

AGID tarafından PEC çözümünün onaylanması ve hizmet sağlayıcısının yetkilendirilmesi şeklinde iki farklı yetkilendirme yapıldığından hizmet sağlamak üzere başvuru yapan tarafların onaylı bir çözüm kullanması gerekmektedir (Ferrara, 2010).

İtalyan PEC sisteminin teknik kurallarını ve işleyişini anlatan standartların oluşturulması amacıyla AGID tarafından IETF bünyesinde bir takım çalışmalar yürütülerek bir RFC dokümanı[4] yayımlanmıştır (Petrucci vd., 2011).

3.2.2.2 Teknik altyapı

Elektronik posta mimarisini kullanan ve RFC 2822'ye (Resnick, 2001) uygun olarak çalışan PEC sistemi, mimari yapısı ve teknik özellikleri açısından De-Mail ile birçok benzer özelliğe sahiptir (Tauber vd., 2013).

PEC sistemindeki hizmet sağlayıcılar, merkezi TTP olarak gönderici ve alıcı arasındaki mesajlaşmayı gerçekleştirdiklerinden sistemde adillik ve inkâr edilemezlik özellikleri hizmet sağlayıcılar vasıtasıyla sağlanmaktadır. Diğer taraftan tüm sistemin etkinliği ve performansı da hizmet sağlayıcılara doğrudan bağlı olduğundan sistemde hizmet sağlayıcıların durumu çok kritik bir rol oynamaktadır. Bu nedenle PEC hizmet sağlayıcısı olmak üzere başvurmak isteyen işletmelerin uyması gereken kurallar ile sahip olması gereken özellikler İCK (2005, m.17)'de katı bir şekilde düzenlenmiştir (Falciai ve Liberati, 2006).

Kurgulanan yapıda, kullanıcılar ile hizmet sağlayıcılar arasında veya hizmet sağlayıcıların kendi aralarında hangi iletişim protokollerinin kullanılacağı belirlenmemiştir. Ancak güvenli bağlantı kavramına yer verilerek iletinin geçmiş olduğu her bir bağlantı için iletilen verinin gizlilik ve bütünlüğünün sağlanması öngörülmüştür[5] (Tauber vd., 2013).

---

[4] IETF RFC 6109, La Posta Elettronica Certificata - Italian Certified Electronic Mail
[5] Bu güvenlik TLS veya SSL kullanılmak suretiyle sağlanabilmektedir.

Son kullanıcıların sisteme bağlantısı büyük oranda tarayıcı üzerinden veya standart bir elektronik posta istemci programı ile sağlanmaktadır. Bu erişim birimleri için mevzuat ile zorunlu kimlik doğrulama mekanizmaları ve güvenli iletişim öngörülmüş durumdadır. Ancak mevzuatta kimlik doğrulamasının ne şekilde gerçekleştirileceğine ve hangi seviyede güvenlik içereceğine ilişkin herhangi bir tanımlamaya yer verilmemiştir. Bu nedenle kullanıcı adı ve şifre ile basit bir kimlik doğrulama mekanizması kullanılabileceği gibi, iki aşamalı kimlik doğrulama mekanizması da kullanılabilmektedir. Ayrıca eID kart ile de sisteme giriş yapılabilmektedir (Tauber vd., 2013).

PEC sisteminde, İCK (2005, m.6)'ye göre gönderici ve alıcı için NRS ve NRD delillerinin üretilmesi gerekmektedir. Göndericinin hizmet sağlayıcısı tarafından oluşturulan NRS delili, iletinin hizmet sağlayıcısı tarafından başarılı bir şekilde teslim alındığını ve doğrulandığını, alıcının hizmet sağlayıcısı tarafından oluşturularak göndericiye iletilen NRD delili ise iletinin alıcının posta kutusuna teslim edildiğini ispatlamak amacıyla kullanılmaktadır. Ayrıca hizmet sağlayıcılar arasındaki ileti alışverişinde, iletinin hizmet sağlayıcılar arasında devredildiğini kanıtlamak üzere de bir delil oluşturulmaktadır (İCK, 2005, m.7). Son olarak iletinin alıcıya teslimatının 24 saat içerisinde gerçekleşmemesi halinde teslimatın başarısız olduğuna dair bir delil üretilmektedir (İCK, 2005, m.8).

Hizmet sağlayıcıların delilleri HSM kullanarak imzalaması ve kullanılan elektronik imzaların uluslararası veya AB tarafından kabul edilebilecek şekilde üretilmiş olması esas alınmaktadır. Yani AB Elektronik İmza Direktifi kapsamında (AB, 1999) delillerin nitelikli veya ileri (*advanced*) elektronik imzalar kullanılarak imzalanması gerekmektedir (TAUBER vd., 2013).

Gönderici ve alıcının farklı hizmet sağlayıcılardan hizmet alması durumunda, sistemin doğru ve eksiksiz işleyebilmesi iki hizmet sağlayıcısının sorunsuz biçimde birlikte çalışması ile mümkün olabilmektedir. Bu nedenle İC (2005b) ile hizmet sağlayıcıların uyması gereken birlikte çalışabilirlik kuralları tanımlanmıştır (Falciai ve Liberati, 2006).

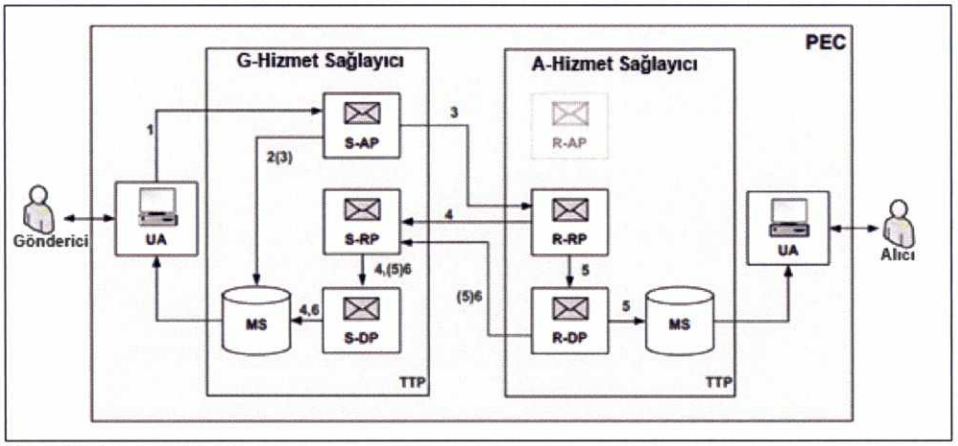
İtalya'da PEC sisteminin çalışmasını izlemek, birlikte çalışabilirliği test etmek ve teknik gelişimine ilişkin çalışmalar yapmak üzere sistemin paydaşlarının yer aldığı bir çalışma grubu faaliyet göstermektedir. Ayrıca hizmet sağlayıcıları arasında birlikte çalışabilirlik sorunlarını en aza indirmek ve birlikte çalışabilirlik eksikliğinden kaynaklanan potansiyel riskleri azaltmak amacıyla AGID tarafından bir takım kontroller gerçekleştirmektedir. Bununla birlikte hizmetlerin sürekli ve doğru bir biçimde çalışabilirliğinin sağlanması ve hizmet sağlayıcıların mevzuat ile belirlenen hizmet kalitesi ve gerekliliklerine uygunluğunun test edilmesine ilişkin çalışmaları koordine etme ve yönetme işlemleri de AGID tarafından yerine getirilmektedir. Bu çalışmaları ve teknik açıdan birlikte çalışabilirlik testlerini yapmak üzere AGID tarafından İtalya Ulusal Araştırma Merkezi yetkilendirilmiştir. Bu yetki kapsamında İtalya Ulusal Araştırma Merkezi tarafından birlikte çalışabilirliğe ilişkin teknik ve fonksiyonel tüm gereklilikleri belirleme ve test senaryolarını oluşturup uygulama görevleri icra edilmektedir. Hali hazırda bahse konu çalışmalar kapsamında 228 farklı test seneryosu tanımlanmış ve uygulanıyor durumdadır (Buzzi vd., 2014).

3.2.2.3 Sistemin işleyişi

PEC sistemi içerisinde erişim noktası (Access Point-AP), alma noktası (Reception Point-RP) ve teslim noktası (Delivery Point-DP) olmak üzere olmak üzere üç farklı servis tanımı bulunmaktadır. Gönderici tarafında bulunan AP tarafından MTA'nın diğer MTA'lara mesajı göndermesi, alıcının MTA'sında yer alan RP tarafından mesajın karşı MTA'dan alınması ve DP tarafından da mesajın alıcının MS'sine yazılması sağlanmaktadır (Tauber vd., 2013).

Gennai vd. (2005), Buzzi vd. (2014) ve Tauber (2011; 2012)'de anlatılan İtalyan PEC sisteminin çalışma mantığına Şekil 3.4'te yer verilmiştir. Buna göre sistemin işleyişi aşağıdaki gibidir (Gennai vd., 2005; Buzzi vd., 2014; Tauber, 2011; 2012).

Şekil 3.4. İtalya PEC sisteminin yapısı ve işleyişi



Kaynak: Tauber, 2011

1. Gönderici kimlik doğrulamasından geçmek suretiyle UA üzerinden sisteme giriş yapar ve orijinal iletiyi MTA üzerinde yer alan AP'ye gönderir. Orijinal ileti, NRO delilinin oluşturulması için S/MIME imza kullanılarak gönderici tarafından imzalanabilmektedir.
2. Göndericinin hizmet sağlayıcısı (veya AP'si), mesajdaki alıcıların PEC kullanıcısı olup olmadığı, mesajın RFC 2822'ye (Resnick, 2001) uygun oluşturulup oluşturulmadığı gibi geçerlilik kontrollerini gerçekleştirir. Eğer tüm kontroller başarılı ise AP tarafından NRS delili oluşturularak göndericinin MS'sine yazılır. Kontrollerden herhangi birinde hata oluşması halinde ise kabul edilmedi yani olumsuz NRS delili oluşturularak göndericinin MS'sine bırakılır.
3. Gönderici hizmet sağlayıcısı (veya AP) göndericinin orijinal iletisini, XML formatında ve bazı üst veriler eklemek suretiyle RFC 2822'ye göre oluşturulmuş yeni bir zarfa koyar ve alıcının RP'sine RFC 2821 (Klensin, 2001) ile tanımlanmış olan SMTP'yi kullanarak gönderir. Eğer alıcı tarafta bulunan RP, 12 saat içerisinde herhangi bir devir iletisi geri göndermezse gönderici tarafta bulunan AP, RP'ye teslim edilemedi delili (olumsuz NRD delili) üreterek göndericinin MS'sine koyar.
4. Alıcı tarafta bulunan RP gelen zarfın yapısını kontrol eder ve üzerindeki elektronik imzayı doğrular. Eğer gelen mesaj geçerli bir mesaj ise devir delili

üreterek göndericinin RP'sine gönderir. Sonrasında bu delil, göndericinin DP'sine iletilerek göndericinin MS'sine yazılır.

5. Alıcı tarafta bulunan RP mesajı alıcı taraftaki DP'ye iletir. İletide yapılan kontroller sonucunda virüs bulunması gibi herhangi bir sorun halinde olumsuz devir alındı üretilerek gönderici tarafında bulunan RP'ye ve oradan da DP'ye iletilmek suretiyle göndericinin MS'sine yazılır. Herhangi bir sorun olmaması durumunda ise alıcı tarafta bulunan DP, göndericinin hizmet sağlayıcısı tarafından oluşturulan zarfı açarak içerisinde bulunan orijinal iletiyi çıkarır ve alıcının MS'sine yazar.
6. Alıcının MS'sine yazma işlemi başarı ile gerçekleştirilirse NRD delili üretilir ve alıcının DP'si aracılığıyla gönderici tarafta bulunan RP'ye ve oradan da göndericinin MS'sine yazılmak üzere gönderici tarafta bulunan DP'ye iletilir. Bu durumun dışında kalan diğer durumlarda ise teslim edilemedi delili yani olumsuz NRD delili gönderici tarafa iletilir.

3.2.2.4 Mevcut durum

İtalya'da PEC sistemi 2005 yılında kurulduktan sonra KEP kullanımını yaygınlaştırmak amacıyla birçok düzenleme yapılmıştır. 7 Mart 2005'te yayımlanan 82 numaralı Dijital Yönetim Kanunu ile tüm kamu kurumlarına, PEC kullanmayı tercih ederek PEC adreslerini bildiren vatandaşlar, özel şirketler ve idareler ile iletişimlerinde PEC sistemini kullanma zorunluluğu getirilmiştir (Tauber vd., 2013).

28 Ocak 2009'da yayımlanan 2 numaralı Kanun[6] ile de tüm şirketlerin, avukatlar, mimar ve mühendisler gibi serbest meslek sahiplerinin ve kamu idarelerinin PEC sistemini kullanmaları zorunlu hale getirilmiştir. Ayrıca yeni kurulan şirketlerin kuruluş aşamasında PEC adresi edinmeleri sağlanırken Kanundan önce kurulan ve

[6] Repubblica Italiana, Legge 28 gennaio 2009, n. 2, Conversione in legge, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a amiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale, In Gazzetta Ufficiale n. 22 del 28 gennaio 2009 e Supplemento Ordinario n. 14, 2009

henüz PEC adresi edinmemiş olan şirketlerin 3 yıl içerisinde PEC adresi edinmeleri hüküm altına alınmıştır (Ferrara, 2010; Tauber vd., 2013; Mula, 2015).

6 Mayıs 2009'daki bir düzenleme[7] ile de tüm İtalyan vatandaşlara ücretsiz PEC hesabı alabilme imkânı sağlanmıştır (Tauber vd. 2013).

2010'da çıkarılan 3 numaralı Kanun ile de çalışanlar için doktorların yazdığı raporları PEC sistemi vasıtasıyla Sosyal Güvenlik Kurumu'na (National Social Insurance Agency-INPS) gönderme zorunluluğu getirilmiştir (Mula, 2015).

İtalya'da 1 Temmuz 2013 tarihi itibariyle yapılan düzenlemeler ile şirketlerle kamu kurumları arasındaki tüm iletişimin PEC vasıtasıyla yapılacağı ve fiziki ortam yani kâğıt kullanılarak yapılacak iletişimin kabul edilmeyeceği hüküm altına alınmıştır (AGID, 2015).

PEC sisteminin standart elektronik posta kullanım kolaylığına sahip olması, akıllı mobil cihazlarda kullanılabilmesi, iletilerin zamandan ve mekandan bağımsız gönderilip alınmasına imkân sağlaması, zaman ve mali tasarruf sağlaması şirketler ile kurum kuruluşlar arasındaki iletişimi artırmaktadır (Buzzi vd., 2014).

İtalya'da hali hazırda yetkilendirilmiş 25 adet hizmet sağlayıcı bulunmaktadır[8]. AGID tarafından bu hizmet sağlayıcaların isimleri ve faaliyetelerine ilişkin bilgiler ile birlikte PEC sistemi içerisinde tanımlanmış alan adı sayısı, bu alan adları altında oluşturulmuş posta kutusu sayıları ve PEC kullanılarak ulaşılan gönderim sayılarını içeren kullanım istatistikleri yayımlanmaktadır (Bkz. Tablo 3.2).

---

[7] Repubblica Italiana, Decreto del Presidente del Consiglio dei Ministri, 6 maggio 2009, Disposizioni in materiale di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini, In Gazzetta Ufficiale n. 119, 25.5.2009

[8] http://www.agid.gov.it/infrastrutture-sicurezza/pec-elenco-gestori

Tablo 3.2. İtalya 2014 yılı KEP kullanım istatistikleri

Dönem	Alan Adı Sayısı	Posta Kutusu Sayısı	Gönderim Sayısı
2014 Kasım-Aralık	251 345	7.978.341	174.561.889
2014 Eylül-Ekim	249 351	7.951.561	155.791.451

Kaynak: http://www.agid.gov.it

3.2.3 Avusturya (DDS)

Avusturya'da adli konularda hizmet veren ve resmi elektronik adalet sistemi olan yasal elektronik haberleşme sistemi (Electronic Legal Communications-ERV) ve genel amaçlı tüm kamu gönderileri için tasarlanan belge teslim sistemi (Document Delivery System-DDS) olmak üzere iki farklı KEP sistemi bulunmaktadır. Bu iki sistemden tez kapsamında olduğu değerlendirilen DDS sistemi bu bölümde irdelenmekte, UYAP benzeri bir sistem olduğu değerlendirilen ERV sistemi ise bu tez kapsamında ele alınmamaktadır.

3.2.3.1 Hukuki altyapı

Avusturya'da kamunun kullanımı için tasarlanan ve resmi KEP sistemi olan DDS'nin hukuki temelleri Resmi Doküman Hizmetleri Kanunu (RDHK) (Avusturya Cumhuriyeti, 1982) ve Avusturya e-Devlet Kanunu'na (Avusturya Cumhuriyeti, 2004) dayanmaktadır. Bu Kanunlar ile kamu kurumlarıyla iletişimin sağlanmasına ilişkin bir yasal altyapı oluşturulmuştur. DDS sistemine ilişkin teknik düzenlemeler, yönlendirmeler ve denetimler Avusturya Federal Başbakanlığı (Austrian Federal Chancellery) tarafından gerçekleştirilmektedir (Tauber, 2011; Tauber,2012, Tauber vd., 2013).

e-Devlet Kanunu'nun yürürlüğe girmesi ile aynı zamanda değiştirilen RDHK ile KEP, fiziki kayıtlı postanın yanında ikinci bir gönderim metodu olarak belirlenmiştir (Tauber vd., 2013). e-Devlet Kanunu ile e-Devlet projelerinin genel çerçevesi çizilmiş,

müteakiben elektronik gönderim ve elektronik ödeme gibi hususlara ilişkin düzenlenmeler yapılmıştır (Tanrıkulu, 2009).

DDS'nin kamuda idari ve adli her türlü dokümanın paylaşılmasını sağlayan genel amaçlı bir sistem olarak kullanıldığı görülmektedir. 2010 yılında RDHK'da yapılan bir değişiklikle kamu idarelerinin daha özel ve farklı bir sistem olan ERV sisteminde kayıtlı kullanıcılara DDS üzerinden doküman gönderebilmesinin önü açılmıştır (Tauber vd., 2013).

RDHK kapsamında dağıtım hizmetlerine ilişkin olarak çıkarılan yönetmelik ile hizmet sağlayıcılara bazı standartlar getirilmektedir. Bu standartlar dağıtım hizmetlerinin teknik ve organizasyonel yeterliliklerini ve veri koruma açısından güvenilirliklerini sağlamak üzere bir takım kurallar tanımlamaktadır. Ayrıca dağıtım hizmetlerinin yerine getirilmesinde uyulacak teknik gereksinimlere de bu yönetmelik ekinde yer verilmiştir[9].

Avusturya'da yukarıda anılan hukuki düzenlemelerle birlikte sistemin teknik alt yapısı ile ilgili olarak kapsamlı teknik dokümanlar[10] yayımlanmakta ve bu dokümanlar sürekli olarak güncel halde tutulmaktadır (Tanrıkulu, 2009).

3.2.3.2 Teknik altyapı

DDS'de, Alman De-Mail ve İtalyan PEC sisteminin aksine SMTP gibi elektronik posta iletişim protokolleri kullanılmamaktadır. Sistemde bulunan elektronik posta uyumlu MIME yapıları web servis tabanlı bir yapı ile taşınmaktadır. Bu nedenle DDS'nin hibrit bir sistem olduğunu söylemek de mümkündür. Avusturya mevzuatının göndericilerin alıcıları farklı şekillerde adreslemesine olanak sağlaması ve Avusturya kamu idareleri tarafından Avusturya'da elektronik posta adresine sahip olmayan

[9] https://www.digitales.oesterreich.gv.at/site/6514/default.aspx#a17
[10] Teknik dokümanlara http://www.bka.gv.at/site/7889/default.aspx adresinden ulaşılabilmektedir.

vatandaşlara ulusal kimlik numarası gibi tanımlayıcılarla adres oluşturulmasının talep edilebilmesi sebebiyle bu yaklaşım tercih edilmiştir (Tauber vd., 2011).

DDS'de bulunan aktörler şu şekilde sıralanabilir (Tauber, 2011; Maierhofer, 2015).

- Gönderici: Tüm kamu kurum ve kuruluşları sisteme gönderici olarak kayıt olabilmektedirler.
- Teslimat Aracı (*Delivery Agent-DA*) (Hizmet Sağlayıcı): Teslimat aracı gönderici ve alıcı arasında güçlü bir adillik sağlamak üzere merkezi TTP gibi davranmaktadır. Göndericiye MTA olarak DA hizmet verirken, alıcıya MTA tarafından gönderilen mesajları alabilmek amacıyla MS hizmet vermektedir. Her bir teslimat aracı Federal Başbakanlık tarafından yetkilendirilerek denetlenmektedir.
- Alıcılar: Tüm gerçek ve tüzel kişileri ifade eden alıcılar bir ya da daha fazla DA'ya kayıt yaptırabilmektedir.
- Merkezi arama servisi (Central lookup service-CLS): Avusturya Federal Başbakanlık tarafından tutulan ve sisteme kayıtlı tüm alıcıların adreslerinin ve hangi DA'dan hizmet aldıkları bilgilerini içeren yer aldığı bir arama hizmetidir.

Diğer sistemlerin aksine DDS'de sadece alıcıların kayıt olması zorunludur. Göndericilerin ise CLS'ye kayıt olma zorunlulukları bulunmamaktadır. Diğer taraftan tüm Avusturya vatandaşları ve tüzel kişilerin herhangi bir hizmet sağlayıcıya kayıt olabilmeleri birden fazla hesaba sahip olabilmelerinin önünde herhangi bir engel yoktur (Tauber, 2011; 2012).

Hizmet sağlayıcılara kayıt sürecindeki kimlik doğrulama işlemleri, Avusturya kimlik kartları veya standart kimlik kartları yerine kullanılabilen ve aynı zamanda AB elektronik imza direktifiyle (AB, 1999) uyumlu nitelikli elektronik imza kullanımına da imkân sağlayan ulusal eID kartları kullanılarak yapılmaktadır. Ayrıca kimlik doğrulama amacıyla mobil elektronik imza kullanımı da söz konusu olabilmektedir (Maierhofer, 2015). İletilerin okunabilmesi için alıcıların sisteme dijital imza ile giriş yapması gerekmektedir (Avusturya Cumhuriyeti, 1982, m.35).

Tüzel kişilerin sisteme kayıt olmaları için ulusal kimlik kartları ile birlikte elektronik vekâlet kullanılmaktadır. Tüzel kişiliklerin temsil işlemleri Avusturya e-Devlet stratejisi kapsamında Avusturya e-Devlet Kanunu'nun (Avusturya Cumhuriyeti, 2004, m.5) bir parçası olarak ele alınmış (Tauber, 2012) ve bu kapsamda Avusturya'da elektronik vekâlet olarak tanımlanan yasal kimlik yönetim yapısı kurulmuştur. 2010 yılında Avusturya hükümeti tarafından yasal kimlik yönetim yapısı vatandaşlık kartları ve ilgili kayıt kuruluşlarından alınan güncel verileri kullanacak şekilde kurgulamış ve eID kartlarına vekâlet bilgilerini içeren imzalanmış bir XML dosyası konulmuştur. Böylece bir şirket ya da kişiyi temsile yetkili kişinin sisteme kayıt yaptırabilmek için ilgili kişilerin adına başvuru yapabilmesi sağlanmıştır (Tauber, 2009; Maierhofer, 2015).

Göndericilerin CLS sistemine kayıt olabilmeleri için gönderici, CLS ve DA arasında kimlik doğrulama amaçlı kullanılan X.509 SSL istemci sertifikalarını bildirmiş olmaları gerekmektedir. Ayrıca bu sertifikalar içerisindeki özel bir X.509 nesne belirteci (Object Identifier-OID) alanına kamu idarelerine özgü Avusturya e-Devlet belirtecinin yazılma zorunluluğu getirilmiş ve böylece sadece kamu idarelerinin sisteme kaydolmaları sağlanmaktadır (Tauber, 2009; 2012).

Sistemin bileşenlerinden bir tanesi olan CLS, sistemde kayıtlı bulunan tüm alıcı bilgilerinin tutulduğu ve alıcılara dair güvenilir bilgilerin sağlandığı bir dizin hizmetidir. Basit nesne erişim protokolüne[11] (Simple Object Access Protocol-SOAP) dayanan sistem, alıcıları adreslemek için tekil bir belirteç kullanmaktadır. Hizmet sağlayıcılar tarafından alıcının posta kutusu bu tekil numara üzerine kurgulamakta ve bu numara ile birlikte kişilerin adı, doğum tarihi gibi bilgileri CLS'ye kaydedilmektedir (Bkz. Tablo 3.3). Avusturya kanunlarına göre göndericilerin mesaj göndermeden önce mutlaka DLS'den kişiyi sorgulaması ve akabinde gönderiyi gerçekleştirmeleri gerekmektedir (Tauber, 2009; 2011; 2012; Tauber vd., 2011).

[11] SOAP, web üzerinden kullanılmak üzere geliştirilmiş bir sistemin XML tabanlı kurallar topluluğudur. SOAP ile ilgili bütün istek ve cevaplar XML formatında iletilmektedir.

Tablo 3.3. Avusturya CLS kaydı

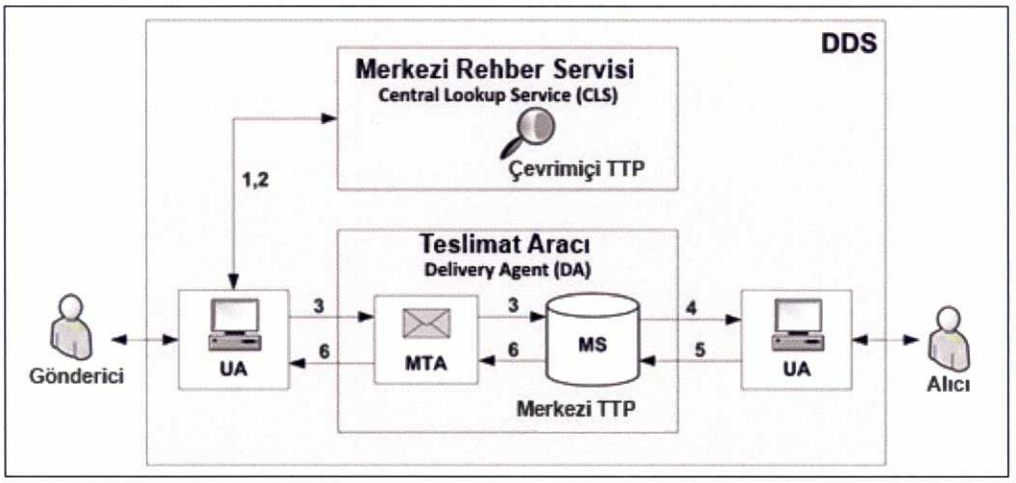
ssPIN	Ad	Doğum Günü	...	Teslimat Aracı	Belge Tipi	Şifreleme Sertifikası
ae231d34	Alice	11.1.1999		da1.delivery.at	pdf, xml, txt	----
ae231d34	Alice	11.1.1999		da2.delivery.at	pdf	MIIExjCCA66gAwIBA...
2988defd	Bob	22.2.1990		da1.delivery.at	pdf, xml, txt	----

Kaynak: Maierhofer, 2015

3.2.3.3 Sistemin işleyişi

DDS Şekil 3.5'da da görüldüğü gibi CLS ve DA olmak üzere iki ayrı alana ayrılmaktadır. CLS'nin bulunduğu alanın olmadığı bir durum Almanya ve İtalya KEP sistemleri ile birçok açıdan benzerlik göstermektedir. DA'nın yani hizmet sağlayıcının bulunduğu alanda, merkezi TTP olarak hizmet sağlayıcı güçlü bir adilliği temin etmektedir. Hizmet sağlayıcılar, göndericilerin mesaj göndermelerini sağlamak üzere MTA ve alıcıların mesajları alabilmeleri için MDA gibi hizmetleri sağlamaktadır. Göndericiler sisteme TLS/SSL kullanarak bağlanmaktadır. Bu bağlantı kayıtları hizmet sağlayıcı tarafından tutulmakta ve NRO delili bu şekilde sağlanmaktadır. Ancak üretilen bu NRO delili hizmet sağlayıcıda kalmakta ve ayrıca taraflara iletilmemektedir (Tauber vd., 2011).

Şekil 3.5. Avusturya DDS sisteminin işleyişi



Kaynak: Tauber vd., 2011

Tauber (2011; 2012) ve Tauber vd. (2011)'e göre Şekil 3.5'da verilen sistemin çalışma mantığı aşağıdaki şekildedir.

1. Gönderici; ad, doğum tarihi gibi demografik verileri veya alıcıların sektöre özel kişisel kimlik numarası[12] (ssPIN) gibi arama parametrelerini kullanmak suretiyle CLS'den sorgulama yapar.
2. CLS aranan alıcının sistemde olup olmadığı bilgisini ve varsa bu alıcının hizmet aldığı DA'ların listesini göndericiye iletir.
3. Gönderici CLS'den aldığı listeden bir DA'yı seçer ve mesajı alıcıya iletilmek üzere ilgili MTA web servisine teslim eder. Bu aşamada gönderici ilgili DA'ya SSL veya TLS kullanarak bağlanır. Alıcı tarafından talep edilmesi halinde S/MIME CMS standardı kullanılarak E2EE yapılmaktadır. Göndericinin inkâr edilemezliğini sağlamak üzere üretilen NRO delili DA tarafından gönderici ile

[12] Bu değer alıcının tekil kimlik numarası olarak da adlandırılmakta ve IdR şeklinde gösterilmektedir. IdR değeri e-devlet kapsamındaki genel ulusal tanımlama numarası (sourcePIN1) ile iki karakterden oluşan sektörü ifade eden bir harf dizisinin art arda eklenmesi ve oluşan bu birleştirilmiş ifadenin SHA-1 algoritmasına göre özet değerinin alınması sonucu oluşturulmaktadır. Aşağıda bu değerin örnek oluşturulma şekli eşitlik halinde verilmektedir.

IdR = ssPIN (CMS) = SHA-1 (sourcePIN || 'ZU')

Genellikle bu tekil tanımlama numarası Avusturya vatandaşlarının sahip olduğu eID kartlarına yüklenmektedir (Tauber vd., 2011).

arasındaki kimlik doğrulama mekanizmasına dayanılarak hazırlanmaktadır. Üretilen bu delil taraflarla paylaşılmamakla birlikte olası uyuşmazlık durumunda ilgili taraflara sunulabilmektedir. DA, mesajı almasını müteakip, mesajı ilgilinin posta kutusuna koymak suretiyle teslim eder.

4. Alıcıya posta kutusunda okunmayı bekleyen bir mesaj olduğuna ilişkin bir elektronik posta bildirimi yapılır.
5. Alıcı DA'nın web sitesi üzerinden kendi eID kartını kullanmak suretiyle sisteme giriş yapar. Bu eID kart nitelikli elektronik imza oluşturmaya imkân tanıdığından bu şekilde QES kullanılarak NRR delili de oluşturulmaktadır.
6. NRR delili bu aşamada DA tarafından gelişmiş elektronik imza ile tekrar imzalanarak göndericiye gönderilir. Bu delilin göndericiye gönderilmesi sırasında web servis veya standart elektronik posta kullanılabilmektedir.

Hizmet sağlayıcısı tarafından alıcının posta kutusuna bırakılmış olan iletiler posta kutusunda en az 14 gün kalmaktadır. Bu süre istenildiğinde artırılabilmektedir (AFC, 2011).

3.2.3.4 Mevcut durum

Avusturya'da TTP olarak hizmet veren ve diğer ülke uygulamalarına benzer şekilde güven zincirinin en tepesinde yer alan hizmet sağlayıcılar RDHK'nın (Avusturya Cumhuriyeti, 1982) 28'inci maddesinde tanımlanan gereklilikleri sağladıklarının tespiti üzerine Federal Başbakanlık tarafından yetkilendirilmektedir (Tauber vd., 2013). Hali hazırda yetkilendirilen dört adet hizmet sağlayıcının listesine ve hangi tarihte yetkilendirildiklerine ilişkin bilgiler Tablo 3.4'te yer almaktadır.

Avusturya DDS sisteminin kullanımı giderek yaygınlaşmaktadır. Özel sektörün kamu ile olan iş ve işlemlerini DDS vasıtasıyla yapmaları sayesinde sağladıkları ekonomik kazanç nedeniyle sisteme olan talep giderek artmaktadır (Tauber vd., 2011).

Tablo 3.4. Avusturya'daki hizmet sağlayıcılar

Hizmet Sağlayıcı	URL	Yetkilendirme Tarihi
Exthex GmbH	https://www.eversand.at	11.02.2014
Mail server online deliveryGmbH	https://www.postserver.at	04.09.2012
Österreichische Post AGformerly Online Post AustriaGmbH formerly Electronic Bill Presentment and Payment GmbH	https://www.meinbrief.at	25.06.2010
Federal Computing GmbH	https://www.brz-zustelldienst.at/Zustellservice/processor	03.03.2009

Kaynak: http://www.bka.gv.at

Hâlihazırda Avusturya'da DDS'nin kullanımına ilişkin bir zorunluluk bulunmamaktadır. Bununla birlikte sistemin zaman tasarrufu, maliyetleri azaltması ve 7/24 hizmet verebilmesi gibi avantajlara sahip olması sisteme olan talebi artırmaktadır (Çiftçi, 2014).

Ayrıca DDS kullanılarak sözleşme, fatura gibi resmi olmayan bilgi ve belgelerin de teslim kanıtına sahip olacak şekilde gönderilmesi mümkündür (AFC, 2011).

3.2.4 Amerika Birleşik Devletleri (RPost)

Amerika Birleşik Devletleri'nde KEP hizmeti Registered Post (RPost) isimli 2000 yılında kurulan bir firma tarafından sağlanmaktadır. Firmanın kuruluşunda fiziki ortamda sağlanan bir takım kanıt sağlama özelliklerinin elektronik ortamdaki karşılıklarının oluşturulması amaçlanmıştır (RPost, 2015a).

ABD'de KEP'e ilişkin herhangi bir mevzuat bulunmamaktadır. Sistem, gönderim ve teslime ilişkin bazı patentlerin tesciliyle fiili (*de-facto*) olarak sürdürülmektedir. Bu kapsamda 2007 yılında avukatlardan oluşan bir ekip tarafından sistem kontrol edilmiş ve sistemin Delillere İlişkin Federal Kurallar'a (*Federal Rules of Evidence*) göre ABD

mahkemelerinde kabul edilebilecek düzeyde kanıt sağladığı ortaya konmuştur. Ayrıca sistem ve sistem tarafından üretilen deliller, İngiltere'de ve ABD'nin çeşitli eyaletlerinde bulunan yirmiye yakın hukuk kuruluşu tarafından kabul edilmektedir (RPost, 2015b).

Sistem merkezi TTP metodunu kullanmaktadır. Tüm ileti trafiği RPost üzerinden geçmektedir. Sisteme göndericilerin kayıtlı olması zorunluyken alıcılar için herhangi bir kayıt şartı aranmamaktadır.

Göndericinin mesajı göndermesini müteakip sistem tarafından mesjın teslim alındığına ilişkin imzalı bir NRS delili oluşturularak göndericiye iletilmektedir. Mesaj ilgili alıcı veya alıcılara teslim edildikten sonra imzalı bir NRD delili oluşturularak göndericiye iletilmektedir. Bu NRD delili alıcının sisteme kayıtlı olma zorunluluğu bulunmaması nedeniyle RPost sunucularından alıcının posta sunucusu, MS'si veya UA'sına gönderilirken oluşan işlem kayıtlarına göre üretilmektedir. Üretilen bu NRD delili, alıcının elektronik posta sisteminin ürettiği kayıtların doğru olduğu varsayılarak üretildiğinden, bunun inkâr edilemez bir delil olmadığı kabul edilmektedir (Tauber, 2011).

Ayrıca delilleri imzalamak için kullanılan elektronik imzaların, AB çapında kabul edilebilir olan gelişmiş veya nitelikli elektronik imzaların ispat gücüne haiz olmadığı ve zaman damgalarının da ilkel düzeyde kaldığı anlaşılmaktadır.

3.2.5 Ülke uygulamalarının değerlendirilmesi

Bu bölümde yukarıda mevzuat ve işleyiş açısından incelenen uygulama örneklerinin Bölüm 2.3'te anlatılan ve literatürde yer alan KEP özellikleri ve bileşenleri kapsamında değerlendirilmesi yapılmaktadır.

3.2.5.1 Temel güvenlik özellikleri açısından değerlendirmeler

Tablo 3.5'te, bu bölümde detaylandırılan ve çalışma yapıları incelenen Almanya, İtalya, Avusturya'daki sistemlerin Bölüm 2.3'te anlatılan KEP güvenlik özellikleri

kapsamında karşılaştırması yer almaktadır. ABD'deki uygulama ise anlatılan bu üç sistemden farklı olması ve harhangi bir mevzuat altyapısına sahip olmaması nedeniyle değerlendirme dışında tutulmuştur.

Tablo 3.5. Sistemlerin KEP özelliklerine göre karşılaştırılması

Sistemin Adı	**De-Mail**	**PEC**	**DDS**
Ülke	**Almanya**	**İtalya**	**Avusturya**
İnkâr Edilemezlik Servisleri			
NRO	İ	İ	İ
NRR	K	K	U
NRS	U	U	K
NRD	U	U	K
Delillerin Paylaşılabilmesi	U	U	U
Adillik			
Güçlü Adillik	U	U	U
Zayıf Adillik	K	K	K
TTP			
Hatta TTP	U	U	U
Çevrim içi TTP	K	K	K
Çevrim dışı TTP	K	K	K
Doğrulanabilirlik	U	U	U
İletişim Kanalı			
Operasyonel	K	K	K
Güvenilir Olmayan	U	U	U
Kesintisiz	K	K	K
Kayıtların Saklanması			
Kayıt Saklanmaz	K	K	K
Sınırlı ve Belirli Zaman	U	U	U
Sınırlı ve Belirsiz Zaman	K	K	K
Sınırsız	K	K	K
Gizlilik (E2EE)	İ	İ	İ
Sonlanabilirlik	U	U	U

U= Uygulanır K= Kullanılmaz İ=İsteğe bağlı olarak kullanılabilir

İncelenen tüm KEP sistemlerinde güçlü adillik kavramının temel bir gereksinim olarak yer aldığı ve gerçekleştirildiği görülmektedir. Kullanıcılar açısından da güçlü bir

adilliğin tesisi, geleneksel kayıtlı postada olduğu gibi önemli bir etken olarak karşımıza çıkmaktadır.

Sistemlerin tamamında mesajlaşmanın TTP'ler üzerinden gerçekleşmesi ve adillik ve inkâr edilemezliğin TTP'ler aracılığıyla sağlanması dikkat çekmektedir. Teorik olarak en çok tercih edilenin çevrim dışı TTP yöntemi olmasına rağman hemen hemen tüm sistemlerde pratik hayatta kendine yer bulmuş olan "merkezi TTP" yapısının kullanılması önemli bir husus olarak karşımıza çıkmaktadır.

Teoride "merkezi TTP" yönteminin tercih edilmeme sebepleri arasında tüm mesajlaşmanın TTP üzerinden yapılması nedeniyle iletişimsel veya işlemsel nedenlerle oluşabilecek darboğaz gösterilmektedir. Ancak pratikte hangi miktarda olursa olsun herhangi bir veri uygun altyapıların kurulmasıyla işlenebilmektedir. Google, Facebook gibi siteler buna örnek olarak gösterilebilir. Diğer taraftan KEP sistemlerinin mali sebeplerle belirli limitler içerisinde olması yani gönderimlerin ücretlendirilmesi sebebiyle gereksiz kullanılmaması ve e-posta trafiğinin %90'ını oluşturan istenmeyen elektronik postaları içermemesi nedeniyle yüksek verinin getireceği bant genişliği sıkıntısıyla pratikte karşılaşılmamaktadır. Karşılaşılsa dahi basit ve maliyet açısından kabul edilebilir sınırlar dâhilinde bu problem çözülebilmektedir. Diğer taraftan kriptografik işlemlerin bolca kullanılması nedeniyle, TTP tarafında işlemsel bir güce sahip olmak gerekebilmektedir. Ancak gelişmiş HSM makinalarının yaygın olarak kullanılması sayesinde günlük bazda milyonlarca KEP iletisinin işlenebilmesi ve gönderilebilmesi mümkün olabilmektedir (Tauber 2011; 2012; Tauber vd., 2013).

Teoride bu yapıyı kullanmama eğilimi veya çevrim içi, çevrim dışı TTP yönteminin tercih edilme sebeplerinden diğer bir tanesi ise TTP'ye yüklenen güven miktarının düşürülme çabası olarak karşımıza çıkmaktadır. Pratikte ise düzenlemeler yoluyla TTP'lerin teknik ve organizasyonel olarak bir akreditasyona tabi olmaları bu hususa yönelik endişeleri azaltmaktadır. Birçok durumda bu hususa yönelik olarak ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nin (Information Security Management System-ISMS) (ISO/IEC, 2014) sertifikasının alınmasının zorunlu tutulduğu da görülmektedir.

Diğer taraftan mesajlaşmanın TTP'ler üzerinden yapılmasının birçok avantajı da bulunmaktadır. Bu yöntemin tercih edilmesinde en büyük etmen tüm mesaj akışı üzerinde tam bir kontrolün sağlanabilmesi ve bu hususun uygulamayı oldukça kolaylaştırmasıdır. Ayrıca bu yöntem ile sonlanabilirlik prensibi açısından da bazı zaman aşımı sürelerinin oluşturulabilmesindeki ve uygulanabilmesindeki kolaylık bir avantaj olarak değerlendirilmektedir. Bunların yanında en önemli etmen olarak geleneksel posta ve elektronik postada olduğu gibi tarafların eşzamanlı olarak bulunma zorunluluğunun olmamasıdır. Tarafların eşzamanlı olarak karşılıklı bulunma gereksinimi sistemin pratik olarak kullanılabilmesinin önündeki en büyük engeli oluşturmaktadır. "Merkezi TTP" metodunda sistemin gönderici ve alıcıyı birbirinden bağımsız ele alması ve eşzamanlı bulunmayı gerektirmeyecek şekilde tasarlanmış olması sayesinde bu yöntem kullanılabilirlik açısından da öne çıkmaktadır.

Son olarak sistemde oluşması gereken tüm delillerin TTP tarafından oluşturulması ve imzalanması sayesinde gönderici ve alıcının herhangi bir kriptografik araca sahip olmadan da işlemlerini kolaylıkla gerçekleştirebilmeleri önemli bir avantaj olarak düşünülmektedir. Bu durumda sistemin kullanıcıları yapılan işlemlerin karmaşıklığından uzak bir şekilde sadece bir internet tarayıcısı veya bir istemci program kullanmak suretiyle işlemlerini yapabilmektedirler. Böylece kullanıcı tarafında altyapı ihtiyacının en düşük seviyede kalması sağlanabilmektedir.

İnkâr edilemezlik servisleri açısından sistemlerin ortak bir yaklaşım içerisinde olmadıkları görülmektedir. NRO delili tüm sistemlerde zorunlu olarak tanımlanmamış ve isteğe bağlı bir delil olarak tasarlanmıştır. İncelenen sistemlerde göndericiler tarafından sisteme bir kimlik doğrulama metoduyla giriş yapılması, sistemde NRO'yu sağlamak için yeterli görülmektedir. Böyle bir durumda oluşan NRO delili TTP sistemlerinde kalmakta ve taraflarla paylaşılamamaktadır.

NRS delili ise PEC ve De-Mail gibi mesajın ilk aşamada göndericinin hizmet sağlayıcısına teslim edildiği sistemlerde temel bir delil olarak ele alınmaktadır. DDS'de ise mesaj doğrudan göndericinin hizmet sağlayıcısına teslim edildiğinden

böyle bir delil anlamını yitirmektedir. Ancak NRS delilinin kullanımı noktasında bir fikir birliği bulunmaktadır.

"Merkezi TTP" metodunun kullanıldığı sistemlerde NRR delili olmazsa olmaz özelliğini yitirmektedir. Çünkü TTP'nin arada bulunmasıyla, mesajın alıcıya, NRD delilinin de göndericiye iletilmesi sayesinde güçlü bir adillik sağlanması söz konusudur. Temelde NRR delili NRD delilinin bir sonraki ve daha kuvvetli bir aşaması olarak görülebilir. Avusturya'da bu delilin oluşturulması gerektiğine yönelik bir düzenleme yapıldığı görülmektedir. NRR delili noktasında uzlaşıya varılamamış bir diğer husus ise oluşturulan NRR delilinin mesajın içeriğine göre mi yoksa geleneksel kayıtlı postada olduğu gibi zarfına yönelik mi oluşturulacağıdır.

Hangi delillerin oluşturulacağının yanı sıra oluşturulan delillerin paylaşılabilir olması da önemli bir ihtiyaç olarak karşımıza çıkmaktadır. İncelenen tüm sistemler bu amaçla elektronik imza kullanmaktadırlar. Elektronik imzada bulunan uzun dönemli arşiv özelliğinin yanı sıra paylaşılabilir delillerin oluşturulabiliyor olması sisteme olan güveni artırmaktadır.

Yine tüm resmi KEP sistemlerinde ortak olarak bulunan diğer bir özellik ise sonlanabilirlik özelliğidir. Bu konuda tüm sistemlerde delillerin TTP tarafından belirli bir zaman içerisinde oluşturulması gerekliliği bulunmaktadır. Bu sayede belirlenmiş zaman içerisinde delilleri alamayan taraf bu delilleri yeniden talep edebilmekte veya işleyişi adilliği etkilemeyecek bir şekilde sınırlı ve belirli bir zaman zarfında sonladırabilmektedir. Ancak bu sürelerin bir düzenleme ile belirlenmesi gerektiğinden ve ülke ihtiyaçları farklı farklı olabileceğinden standartlarda bu duruma yönelik hususlar yer almamaktadır (Tauber, 2011).

Bir diğer özellik olan E2EE de tüm sistemlerde isteğe bağlı bir özellik olarak ele alınmaktadır (Tauber, 2011; 2012).

İncelenen tüm sistemler iletişim kanalı olarak internet ortamını kullanmaktadırlar. Bazı gerçekleştirimlerde bu kanalın kullanımı sırasında ek güvenlik önlemlerinin de alınabildiği görülmektedir.

Son olarak kayıtları saklama açısından bir değerlendirme yapılacak olursa hemen hemen tüm sistemlerin kayıtları sınırlandırdığı ve belirli bir zaman aralığında sakladığı anlaşılmaktadır.

3.2.5.2 Diğer özellikler açısından değerlendirmeler

KEP'e ilişkin sistemlerin karşılaştırılmasında; hangi protokollerin kullanıldığı, mesajlaşma altyapılarının ne olduğu, kullanılan imza formatları ve düzenlemenin var olup olmadığı gibi hususlar dikkate alınmalıdır.Tablo 3.6'te seçilen sistemlerin yukarıda sayılan açılardan mevcut durumları verilmiştir.

Tablo 3.6. Sistemlerin diğer özellikleri

Sistemin Adı	**De-Mail**	**PEC**	**DDS**
Ülke	**Almanya**	**İtalya**	**Avusturya**
Kullanılan Protokol			
HTTP	K	K	U
SMTP	U	U	K
Mesajlaşma Altyapısı			
SOAP	K	K	U
E-Posta	U	U	K
Kullanılan İmza Formatı			
AdES	U	U	U
QES	U	K	U
Düzenleme Yaklaşımı			
Düzenlenmiş (de-jure)	K	K	K
Fiili Uygulama (de-facto)	U	U	U

U= Uygulanır K= Kullanılmaz İ=İsteğe bağlı olarak kullanılabilir

İtalya PEC ve Almanya De-Mail gibi sistemleri mesajların transferi için SMTP'ye dayanan elektronik posta altyapısını kullanmaktadır. İkinci alternatif ise Avusturya DDS'de de benimsenen servis tabanlı mimaridir (Service Oriented Architecture-SOA). Avusturya'da mesajlar ve delillerin taşınmasında HTTPS üzerinden SOAP

kullanılmaktadır. Sistemlerin mesajların transferi için tercih ettikleri yaklaşım, kurulan tüm altyapının farklılaşmasına neden olduğundan bu özellik sistemleri sınıflandırmada kullanılmaktadır.

Sistemleri kıyaslarken hangi tür imza kullandıkları hususu önem arz etmektedir. Sistemlerin hangi tür imza kullandıkları onları birbirlerinden ayıran bir özellik olarak karşımıza çıkmaktadır. Hemen hemen tüm sistemlerde AdES ve QES'nin desteklenmektedir. Avusturya DDS'de QES'in zorunlu ve AdES'in ise isteğe bağlı olarak kullanım alanları bulunmaktadır. İtalyan PEC sisteminde kullanılacak imzanın formatı belirtilmemiş olmasına karşın kullanılacak imzanın AB ve uluslararası alanda tanınması şartı konarak dolaylı olarak Direktif'te (AB, 1999) yer alan imza formatlarının kullanılması sağlanmışır. De-Mail sisteminde ise delillerin tamamının QES ile imzalanması öngörülmektedir. Bunun haricinde kalan durumlarda daha düşük kalitede imza kullanılabilmesi de mümkün kılınmıştır.

4. TÜRKİYE'DEKİ MEVCUT DURUM VE DEĞERLENDİRMELER

Elektronik ortamda bilgi ve/veya belge paylaşımının ülkemizde bir sorun olması nedeniyle 2007 yılının ikinci yarısından itibaren bu sorunu çözmek amacıyla BTK'da bazı çalışmalar yapılmaya başlanmıştır. 2008 yılı Şubat ayında Sabancı Üniversitesi, Lostar Bilgi Güvenliği A.Ş. ve müşteri kurum olarak BTK'nın işbirliği ile "Kayıtlı Elektronik Posta Sistemi Konusunda Araştırma, Geliştirme ve Uygulamalar" konulu bir proje geliştirilerek, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) 1007 No'lu Kamu Kurumları Araştırma ve Geliştirme Projelerini Destekleme Programı kapsamında TÜBİTAK'a sunulmuş, ancak birtakım sebeplerle projenin geliştirilme imkânı olmamıştır.

e-Dönüşüm Türkiye İcra Kurulu'nun 26/12/2008 tarihli ve 26 sayılı toplantısında ele alınmış ve BTK'nın, Başbakanlığın ve Adalet Bakanlığı'nın KEP konusunda üzerinde birlikte çalışmalar yapması kararlaştırılmıştır. e-Dönüşüm Türkiye İcra Kurulu'nun 15/07/2009 tarihli ve 28 sayılı Kararı ile KEP sistemi konusunda düzenleyici çerçevenin oluşturulması amacıyla çalışmalar yapmak üzere BTK görevlendirmiştir (E-DTR, 2009).

2009 yılı Ağustos ayında görüşe açılan e-Devlet ve Bilgi Toplumu Kanunu Tasarısı'nın 17'nci maddesi ile kamu kurumları ile gerçek ve tüzel kişiler arasında elektronik ortamda belge, bildirim, ihtar, ihbar ve benzeri hukuki sonuç doğuran beyan ve yazışmaların ortak e-devlet hizmeti olarak, KEP sistemi vasıtasıyla yapılacağı ve kamuda KEP kullanılarak yürütülen idari işlemlere ilişkin esasların BTK tarafından yapılacak düzenlemeler dikkate alınarak aynı kanunla kurulması öngörülen Ajans tarafından çıkarılacağı belirlenmiştir (T.C. Başbakanlık, 2009). Ancak e-devlet hizmetlerinin yürütülmesine ilişkin usul ve esasları belirlemek, bilgi toplumuna dönüşüm sürecini planlamak ve koordine etmek amacıyla Bilgi Toplumu Ajansı'nı kurmak üzere hazırlanan bahse konu Taslak, değerlendirilmek üzere bakanlıklara gönderilmiş ancak daha sonra çeşitli sebeplerle beklemeye alınmıştır (BT Haber, 2010).

Müteakiben Ulaştırma Bakanlığı'nın teklifi üzerine Bakanlar Kurulu'nda imzaya açılan 11/03/2010 tarihli Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı'nda KEP sistemine ilişkin BTK tarafından hazırlanan hükümlere yer verilmiş ve söz konusu Tasarı ile KEP sistemi konusunda ikincil düzenlemeleri hazırlama ve denetleme yapma görevinin BTK'ya verilmesi öngörülmüştür (T.C. Ulaştırma Bakanlığı, 2010). e-Devlet konusunda önemli düzenlemeleri içeren ve kamuoyunda "Torba Kanun Tasarısı" olarak bilinen tasarı halen TBMM Adalet Komisyonu'nda beklemektedir.

KEP'e ilişkin BTK'nın çalışmaları devam ederken 14/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu'nun 18'inci ve 1525'inci maddeleri ile KEP'in Ülkemizdeki hukuki dayanağı oluşturulmuştur.

Bu bölümde 6102 sayılı Kanun kapsamında BTK tarafından hazırlanan ikincil düzenlemeler ile birlikte KEP'e ilişkin ülkemizdeki mevcut durum incelenmektedir. Bu kapsamda düzenleme düzleminde yapılması gerekenler ile birlikte değerlendirmelere yer verilecektir. Ayrıca teknik ve idari anlamda sistemin yapısı incelenirken KEPHS'lerin denetimlerinde uygulanacak esaslar da ortaya konmaktadır.

4.1 Hukuki Altyapı

Bu bölümde hâlihazırda ülkemizde KEP sisteminin hukuki altyapısını oluşturmak üzere hazırlanan düzenlemeler ele alınmaktadır. Bununla birlikte KEP sistemi ilgili olduğu düşünülen diğer düzenlemelere de yer verilmektedir.

4.1.1 Kanun

KEP sistemine ilk atıf 13/01/2011 tarihinde kabul edilen, 14/02/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanan 6102 sayılı Türk Ticaret Kanunu (TTK)'nda yapılmıştır. Aynı Kanun'un 18'inci maddesinin üçüncü fıkrasında 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." hükmü ile KEP sisteminin hukuki dayanağı oluşturulmuştur (T.C. Resmi Gazete, 2011b). Bu hüküm ile tacirler arasında elektronik ortamda gerçekleştirilecek olan diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarların veya ihtarların sayılan diğer yöntemler veya KEP sistemi vasıtasıyla yapılması gerektiği belirlenmiştir. Bununla birlikte yine aynı Kanun'un 1525'inci maddesinin 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. Yönetmelik bu Kanunun yayımı tarihinden itibaren beş ay içinde yayımlanır.

hükmü ile BTK'ya KEP sistemi ile ilgili ikincil düzenlemeleri hazırlama ve bu kapsamda KEPHS'leri yetkilendirme ve denetleme görevi verilmiştir (T.C. Resmi Gazete, 2011b).

4.1.2 Yönetmelik

KEP sisteminin hukukî ve teknik yönlerini belirlemek üzere 6102 sayılı Kanun kapsamında hazırlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik (KEP Yönetmeliği) 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanmıştır (T.C. Resmi Gazete, 2011c).

KEP Yönetmeliği ile; KEP, "*elektronik iletilerin, gönderimine, teslimatına ve kullanımına ilişkin hukukî delil sağlayan elektronik postanın nitelikli şekli*", KEP delili de "*belirli bir işlemin belirli bir zamanda meydana geldiğini gösteren, KEP sisteminde üretilen ve KEPHS'nin işlem sertifikası ile imzalanmış veri*" olarak tanımlanmıştır. Böylece KEPHS'nin aslında nitelikli elektronik sertifika ve zaman damgası kullanarak imzalayacağı verilere hukuki geçerlilik kazandırılmıştır (T.C. Resmi Gazete, 2011c).

Aynı Yönetmeliğin 15'inci maddesinin birinci fıkrasında "*KEPHS'nin KEP sistemi üzerinden sunduğu hizmetlere ilişkin olarak oluşturduğu kayıtlar ile KEP delilleri senet hükmündedir ve aksi ispat edilinceye kadar kesin delil sayılır.*" hükmüne yer verilerek (T.C. Resmi Gazete, 2011c) KEPHS tarafından KEP sisteminde oluşturulan kayıtlar ile bu sistem vasıtasıyla gönderilen iletilerin hukuki niteliğinin kesin delil[1] olduğu belirtilmiştir (Güneli, 2012).

KEP Yönetmeliği'nde KEPHS'lerin, KEP hesap sahibinin ve BTK'nın yükümlülüklerine yer verilmiştir. Bununla birlikte KEPHS'nin, Sakla ve İlet (Store and Forward-Sİ) ve Sakla ve Bildir (Store and Notify-SB) çalışma modellerinden birisiyle veya her ikisiyle hizmet vermesi gerektiği belirlenmiştir (T.C. Resmi Gazete, 2011c).

KEP Yönetmeliği ile KEPHS'ye, vermiş olduğu KEP hizmetinin güvenliğini, gizliliğini ve bütünlüğünü sağlama ve KEP sisteminde gerçek ve tüzel kişilere ait bütün bilgilerin korunması için gerekli tedbirleri alma yükümlülüğü getirilmiştir. Bununla birlikte, KEP sisteminin en önemli özelliğinin gönderici ve alıcının kimliğinin kesin olarak tespitinin sağlanması olduğundan KEPHS, güvenilir bir kimlik doğrulama mekanizması tesis etmekle, KEP sisteminin tüm süreçlerine ilişkin işlem kayıtları ile KEP hesabının ve bu hesap üzerinden verilen hizmetlerin güvenliğini, gizliliğini ve bütünlüğünü sağlamakla ve kayıt altına almakla ve KEP sisteminin tüm süreçlerine ve işleyişine ilişkin bilgi, belge ve elektronik verileri en az 20 yıl süreyle saklamakla yükümlü kılınmıştır (T.C. Resmi Gazete, 2011c).

KEP sisteminin devamlılığının sağlanabilmesi ve hesap sahiplerine sunulan hizmetin kalitesinin artırılabilmesi amacıyla KEPHS, KEP hesabının iptaline ilişkin kesintisiz hizmet sunmakla ve KEP rehberini tüm hesap sahipleri ve işlem yetkililerinin erişimine 7 gün 24 saat kesintisiz açık bir şekilde ve güncel tutmakla, KEP iletilerini ve KEP delillerini ilgili KEP hesabına anlaşılabilir ve okunabilir bir şekilde iletmekle

---

[1] Medeni usul hukukunda deliller kesin ve takdiri olmak üzere iki şekilde yer almaktadır. Hukuk Muhakemeleri Kanunu'nun 198. maddesi hâkimin, kanuni istisnalar dışında delilleri serbestçe değerlendireceğini hüküm altına alınmıştır. Kesin delil, hâkimi bağlayıcı nitelikte olduğundan, hâkimin bu deliller üzerinde takdir yetkisi bulunmamaktadır (Güneli, 2012).

ve hesap sahibinin KEP hesabına bir ara yüz üzerinden erişilebilmesini, iletilerin okunabilmesini ve gönderilebilmesini sağlamakla yükümlü kılınmıştır (T.C. Resmi Gazete, 2011c).

Güvenlik kriterlerine ilişkin olarak KEP Yönetmeliği'nde KEPHS'nin ortakları, yöneticileri ve istihdam ettiği veya ettirdiği personelin adli siciline ilişkin bir takım isterler yer almaktadır. Ayrıca KEPHS'nin, bilgi güvenliği, veri tabanı yönetimi, bilgisayar ağları ve veri koruması gibi alanlarda konusunda yeterli meslekî deneyime sahip ya da ilgili alanlarda eğitim almış yeteri kadar teknik personel istihdam etmesi ve güvenli sistem ve cihazlar kullanarak bu sistem ve cihazlar ile bunların bulunduğu bina veya alanın korunmasını sağlaması gerekmektedir (T.C. Resmi Gazete, 2011c).

4.1.3 Tebliğler

Bu bölümde KEP sistemine ilişkin teknik detayların yer aldığı ve BTK tarafından yayımlanan tebliğlere yer verilmektedir.

4.1.3.1 Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

Yönetmeliğin "*Teknik hususlara ilişkin tebliğ*" başlıklı 25' inci maddesinin birinci fıkrasında yer alan; "*KEP sisteminin tüm süreçlerine ve işleyişine, KEPHS'nin faaliyetleri için kullandığı sistemlere ve cihazlara, fizikî güvenliğe ve personeline ilişkin uyulması gereken teknik kriterler Tebliğ ile belirlenir.*" hükmü kapsamında KEP sistemine ilişkin süreçleri ve teknik kriterleri düzenlemek amacıyla hazırlanan Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Teknik Kriter Tebliği) 25/08/2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanmıştır (T.C. Resmi Gazete, 2011d).

KEPHS'nin işleyişinin bütün aşamalarında altı ana ve üç alt bölümden oluşan ETSI TS 102 640 standardına uyması gerektiği Teknik Kriter Tebliği'nin 5'inci maddesi ile belirlenmiştir (T.C. Resmi Gazete, 2011d).

Ayrıca aynı Teknik Kriter Tebliği'nin 6'ncı maddesi ile de KEPHS'ye elektronik imza, işlem sertifikası ve özetleme algoritmalarına ilişkin 06/01/2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 6'ncı maddesinin birinci fıkrasının (b) ve (c) bendleri ile belirlenen algoritma ve parametreleri kullanma sorumluluğu yüklenmiştir (T.C. Resmi Gazete, 2011d).

Teknik Kriter Tebliği'nin 8'inci maddesi ile KEPHS'nin güvenlik kriterlerine ilişkin olarak;

- KEP sistemnin genel yapısını belirleyerek, KEP sisteminin işleyişi, sistemi oluşturan bileşenler, arayüzler ve delil oluşturma kurallarının belirlenmesi, farklı KEP sistemlerinin birlikte çalışabilirliklerinin sağlanmasına, KEP yönetim alanında elektronik imzanın kullanılmasını, KEP yönetim alanı için gerekli olan Bilgi Güvenliği Yönetim Sistemi (BGYS) ile karşılanması gereken minimum gerekliliklerin belirlenmesi, farklı KEPHS'lerin yönetim alanlarının birlikte çalışabilirliklerinin SMTP'ye göre belirlenerek ETSI standartlarını uygulayan KEPHS'ler arasındaki birlikte çalışabilirliğin sağlanmasını amaçlayan ETSI TS 102 640 standardına,
- Temel amacı, kurumun bilgi varlıklarının korunması için, bir bilgi güvenlik sisteminin kurulması, gerçekleştirilmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürüdürülmesi ve geliştirilmesi amacı ile kullanılan Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin kurulması ve sürdürülmesi olan TS ISO/IEC 27001 veya ISO/IEC 27001 standardına (ISO/IEC, 2013),
- Etkin bir kişisel veri yönetimi için bir plan oluşturulmasını, bu verilerin depolanması ve korunmasını iyileştirmek ile ilgili süreçlerin belirlenmesini sağlamak amacıyla BS10012 standardına (BS, 2009),
- BİT hizmetlerinin güvenliği ve önceden tanımlanmış kabul edilebilir seviyede sürekliliğinin sağlanabilmesi için organizasyonun olay ve kesintilere karşı tepki ve müdahaleyi planlamayı, uygulamayı, kontrol etmeyi ve sonuçlara göre aksiyon almayı hedefleyen ISO/IEC 27031 standardına (ISO/IEC, 2011)

uyum sağlaması gerektiği belirlenmiştir (T.C. Resmi Gazete, 2011d).

Son olarak mezkur tebliğ ile; engelli ve dezavantajlı kişilerin de KEP sisteminden yararlanmalarını sağlamak amacıyla KEPHS'ye tüm arayüzlerini W3C'nin Web erişilebilirlik girişim yönergesine (Web Content Accessibility Guidelines) uygun hazırlama yükümlülüğü getirilmiştir (T.C. Resmi Gazete, 2011d).

Ayrıca Teknik Kriter Tebliği uyarınca KEPHS ilgili tarafları bilgilendirmek amacıyla hazırlayacağı, sistemin tüm işleyişine ve iş süreçlerine ilişkin detaylara yer vereceği KEP uygulama esaslarını ETSI TS 102 640 standardına uygun olarak hazırlamak ve internet sitesinden yayımlamak zorundadır (T.C. Resmi Gazete, 2011d).

4.1.3.2 Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ

13/01/2011 tarihli ve 6102 sayılı Türk Ticaret Kanununun 1525 inci maddesine dayanılarak hazırlanan 25/8/2011 tarihli ve 28036 sayılı Resmî Gazete'de yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 9'uncu maddesinin altıncı fıkrasında yer alan *"KEP hesabı adreslerine ilişkin usul ve esaslar Kurum tarafından belirlenir."* hükmü ile 24'üncü maddesinin dördüncü fıkrasında yer alan *"KEP rehberine ilişkin usul ve esaslar Kurum tarafından belirlenir."* hükmü uyarınca hazırlanan Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ (KEP Hesap Adresleri Tebliği) 16/05/2012 tarihli ve 28294 sayılı Resmi Gazete'de yayımlanmıştır.

KEP Hesap Adresleri Tebliği, KEP hesabı adreslerinin yapısına ve KEP rehberinin oluşturulmasına, güncellenmesine, işletilmesine ve kullanılmasına ilişkin usul ve esasları belirlemek amacı ile hazırlanmıştır (T.C. Resmi Gazete, 2012a).

KEP Hesap Adresleri Tebliği'ne göre KEP hesap adreslerininin IETF RFC 2821 (Klensin, 2001) ve IETF RFC 2822 (Resnick, 2001) uygun oluşturulması gerekmektedir. KEP hesabı adresleri "kullanıcı-tarafı@alan-adı-tarafı "formatında belirlenmektedir. Kullanıcı tarafı gerçek kişiler için "ad.soyad.sayı" şeklinde belirlenirken, tüzel kişiler için "tüzelkişiadı", "tüzelkişiadı.X", "MERSİS No" ya da

"MERSİS No.X" formatlarından biri ile oluşturulmaktadır. "X" alfa nümerik olacak şekilde isteğe bağlı olarak başvuru sahibi tarafından belirlenebilmektedir. Alan adı tarafının ise gerçek kişiler için "hsY.kep.tr" ve tüzel kişiler için "hsY.kep.tr" veya "TüzelKişiAdı.hsY.kep.tr" formatlarından biri ile oluşturulacağı hüküm altına alınmıştır (T.C. Resmi Gazete, 2012a).

KEP Hesap Adresleri Tebliği'nde ayrıca KEP rehberinde gerçek ve tüzel kişiler için bulunması zorunlu ve isteğe bağlı alanlara yer verilmiştir. KEPHS'nin, gerçek kişinin rehber kaydına, hesap sahibinin onayını alarak, tüzel kişinin ise rehber kaydına, tüzel kişinin onayını almaksızın KEP rehberinde yer vereceği hüküm altına alınmıştır. Ayrıca her KEP hesabı için sadece bir tane rehber kaydı oluşturulabilecektir (T.C. Resmi Gazete, 2012a). Mezkûr Tebliğ ile ayrıca rehber sorgularının ne şekilde gerçekleştirileceğine, bu sorgu sonuçlarının ne şekilde cevaplanacağına ve bu sorguların ne kadar süre içerisinde tamamlanması gerektiğine ilişkin detaylı düzenlemelere yer verilmektedir.

4.1.4 Usul ve esaslar

Bu bölümde KEP sisteminin işleyişine ve bazı teknik detaylara ilişkin BTK tarafından yayımlanan kurul kararlarına yer verilmektedir.

4.1.4.1 Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul Esaslar

KEP Yönetmeliği'ne göre, KEPHS olmanın şartlarından biri ESHS veya elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve altyapısını işleten şirketlerden olmamaktır. Bu kapsamda KEPHS, elektronik imza ve zaman damgası için harici bir ESHS'den hizmet almak zorundadır. KEP Yönetmeliği gereği KEPHS'nin dâhili bir elektronik sertifika hizmeti vermesi mümkün değildir (Güneli, 2012).

Bununla birlikte Yönetmeliğin 16'ncı maddesinin birinci fıkrasının (m) bendi ile KEPHS'ye KEP sistemindeki tüm imzalama süreçlerinde ESHS'ler tarafından kendileri için oluşturulan işlem sertifikasını kullanma yükümlülüğü getirilmiş ve işlem sertifikası; "*KEPHS'nin hizmetlerine ilişkin işlem verilerini imzalamak için kullanacağı elektronik sertifika*" olarak tanımlanmıştır. İşlem sertifikası 5070 sayılı Elektronik İmza Kanunu (EİK)'nun 9'uncu maddesi ile düzenlenen (T.C. Resmi Gazete, 2004) nitelikli elektronik sertifikadır. Bu nedenle işlem sertifikasıyla oluşturulan elektronik imzalar da elle atılan imza ile aynı hukukî sonucu doğuran ve aynı ispat gücünü haiz olan güvenli elektronik imzadır. KEP sistemi ve KEPHS'ler açısından önemli olan ve KEP'in hukuki geçerliliğini sağlayan işlem sertifikasının ESHS'ler tarafından oluşturulması, iptali ve yenilenmesi ile KEPHS'ler tarafından bu işlem sertifikasının kullanılmasına ilişkin usul ve esasları belirlemek üzere hazırlanan Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul ve Esaslar 06/06/2012 tarihli ve 2012DK-15259 sayılı Kurul Kararı ile yayımlanmıştır (BTK, 2012b).

Usul esas ile işlem sertifikasının geçerlilik süresinin en fazla bir yıl olacağı, ESHS'ler tarafından sertifika oluşturulurken sertifika içerisinde; KEPHS'in açık ismine, "*Bu sertifika, kayıtlı elektronik posta hizmet sağlayıcısının hizmetlerine ilişkin işlem verilerini imzalamak için kullanılır.*" ibaresine ve sertifikanın kullanılacağı işlemler için para limitinin sıfır "0" TL olduğuna ilişkin ibareye yer vermesi gerektiği belirlenmiştir. Yine aynı usul ve esasa göre KEPHS tarafından işlem sertifikası ile imzalamanın, onaltı saatte en az bir kez sertifika sahibi tarafından erişim verisinin kullanılması suretiyle gerçekleştirilmesi gerekmektedir (BTK, 2012b).

4.1.4.2 Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar

KEPHS'lerin altyapıları, mevzuatta atıf yapılan standartlara uygun olarak oluşturulmasına rağmen bu standartların kesin olarak belirlemediği bazı alanların farklı kullanımından dolayı sorunlar yaşanmaya başlamıştır. Bu nedenle, KEPHS'lerin birlikte çalışabilirliğine ilişkin teknik kriterleri ve ilgili usul esasları belirlemek üzere

"Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar Esaslar (Birlikte Çalışabilirlik Usul ve Esası)" hazırlanmış ve 09/09/2014 tarihli ve 2014/DK-BTD/447 sayılı Kurul Kararı ile yayımlanmıştır (BTK, 2014).

Sekiz bölüm ve yirmidokuz maddeden oluşan Birlikte Çalışabilirlik Usul ve Esası ile KEP sisteminde ileti akışının nasıl gerçekleşeceği, kullanılan güvenli elektronik imzaların formatları, KEP servis adresleri, KEP sistemlerinde hangi işlem kayıtlarının ne kadar süreyle tutulacağı, işlem yetkililerinin başka bir işlem yetkilisi tanımlama süreçleri ve her KEPHS'nin kurumsal internet sitesinde yayımlayacağı "Bilgi Deposu"'nun yapısı belirlenmiştir. Bununla birlikte Birlikte Çalışabilirlik Usul ve Esas'ta orijinal ileti, KEP paketi ve KEP iletisi başlık bilgilerine, KEP hesabı arayüzlerine, KEP delili içeriğine ve gösterimine ilişkin düzenlemelere yer verilmiştir (BTK, 2014).

4.1.5 İlgili diğer mevzuat

4.1.5.1 Elektronik tebligat

11/01/2011 tarihli ve 6099 sayılı Tebligat Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 1'inci maddesi ile 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanunu'nda değişiklik yapılmış ve tebligat göndermeye yetkili merciler tek tek ve sınırlı olarak sayılmıştır. Mezkûr kanunla yargı mercileri, belediyeler, köy tüzel kişilikleri, barolar ve noterler, genel ve katma bütçeli daireler, 5018 sayılı Kanunun 3'üncü maddesine göre merkezî yönetim kapsamında kabul edilen kamu idareleri, sosyal güvenlik kurumları, il özel idareleri, belediyeler, köy hükmî şahsiyetleri tebligat göndermeye yetkili kurumlar olarak belirlenmiştir. Bununla birlikte aynı maddede yer alan *"... tarafından yapılacak elektronik ortam da dâhil tüm tebligat, bu Kanun hükümlerine göre PTT veya memur vasıtasıyla yapılır."* ifadesi ile de tebligatın elektronik veya fiziki usullerle yapılacağı genel olarak belirlenmiştir (T.C. Resmi Gazete, 2011a).

6099 sayılı Kanun'un 2'nci maddesi ile 7201 sayılı Tebligat Kanunu'na eklenen "*Elektronik tebligat*" başlıklı 7/a maddesiyle;

> Tebligata elverişli bir elektronik adres vererek bu adrese tebligatyapılmasını isteyen kişiye, elektronik yolla tebligat yapılabilir.
> Anonim, limited ve sermayesi paylara bölünmüş komandit şirketlere elektronik yolla tebligat yapılması zorunludur.
> Birinci ve ikinci fıkra hükümlerine göre elektronik yolla tebligatın zorunlu bir sebeple yapılamaması hâlinde bu Kanunda belirtilen diğer usullerle tebligat yapılır.
> Elektronik yolla tebligat, muhatabın elektronik adresine ulaştığı tarihi izleyen beşinci günün sonunda yapılmış sayılır.

hükümleri getirilmiştir (T.C. Resmi Gazete, 2011a).

Bu madde ile bugüne kadar yapılan fiziki tebligata elektronik tebligat yöntemi de ilave edilmiş ve tebligat gönderecek taraflara fiziki tebligat ya da elektronik tebligat yöntemlerinden istediğini seçme imkânı sağlanmıştır. Bununla birlikte tüzel kişilere elektronik yolla tebligat yapılması zorunlu hale getirilmiş, kendisine tebligat yapılmasını isteyen şahıslara tebligata elverişli bir elektronik adres vermesi şartıyla elektronik tebligat yapılabileceği belirlenmiş ancak, elektronik tebligata elverişli adresin nereden temin edilebileceğine yer verilmemiştir.

Mezkûr maddenin son fıkrasında yer alan "*Bu maddenin uygulanmasına ilişkin usûl ve esaslar yönetmelikle belirlenir*" ifadesi ile elektronik tebligatın hangi yöntemle yapılacağının belirlenmesi görevi Adalet Bakanlığı'na verilmiştir.

Bu görev çerçevesinde Adalet Bakanlığı tarafından hazırlanan ve 19/01/2013 tarihli ve 28533 sayılı Resmi Gazete'de yayımlanan Elektronik Tebligat Yönetmeliği ile muhataba ve tebligatı çıkaran merciye ait elektronik tebligata elverişli adresin, KEP adresi olacağı yani elektronik tebligat gönderiminde KEP altyapısının kullanılacağı hüküm altına alınmıştır. Bu hükümle KEP adreslerinin aynı zamanda elektronik tebligat adresi olarak da kullanılabilmesi sağlanmıştır (T.C. Resmi Gazete, 2013).

Ayrıca Elektronik Tebligat Yönetmeliği'nde; tebligat çıkaran mercilerin, elektronik tebligat adresi almak için idareye, yani PTT'ye başvuruda bulunarak elektronik tebligat mesajını İdare tarafından kendisine verilen KEP adresi vasıtasıyla gönderebileceğine, elektronik tebligat hizmetinden yararlanacak muhatabın, elektronik tebligata elverişli KEP adresini faaliyette olan herhangi bir KEPHS'den edinebileceğine ve anonim, limited ve sermayesi paylara bölünmüş komandit şirketlere, elektronik yolla tebligat yapılmasının zorunlu olduğuna ilişkin hükümlere yer verilmiştir (T.C. Resmi Gazete, 2013).

4.1.5.2 e-Yazışma Projesi ve Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik

28/07/2006 tarihli ve 26242 sayılı Resmî Gazete'de yayımlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararı ile uygulamaya konan Bilgi Toplumu Stratejisi eki Eylem Planı'nda yer verilen 73 no'lu "*Ortak Hizmetlerin Oluşturulması*" eylemi kapsamında kamu kurum ve kuruluşları arasındaki resmi yazışmaların elektronik ortamda yürütülmesini sağlayacak ortak kurallar setinin geliştirilmesini amaçlayan "e-Yazışma Projesi" Kalkınma Bakanlığı tarafından 16/02/2011 tarihinde başlatılmıştır. Bu Projede, kamu kurum ve kuruluşlarının kendi aralarında ve/veya gerçek ve tüzel kişilerle yaptıkları resmi yazıyı taşıyan paketin (e-Yazışma Paketi) gönderici kurumda oluşturulması, alıcı kurumda alınıp açılması işlemlerine odaklanılmış ve kamu kurum ve kuruluşlarının, elektronik belge yönetim sistemi çözümlerinde uymaları gereken teknik özellikler belirlenmiştir.

e-Yazışma Projesi ile kamu kurum ve kuruluşlarındaki bilgi ve belgelerin elektronik ortamda hukuki geçerliliğe sahip bir şekilde oluşturulması, tasnif edilmesi, arşivlenmesi ve resmî yazıyı taşıyan paketin belirlenen teknik kriterlere uygun oluşturulması sağlanmıştır. Bununla birlikte e-Yazışma Projesi kapsamında gerçekleştirilecek entegrasyon çalışmalarına ilişkin genel bilgi vermek ve Proje kapsamında geliştirilen e-Yazışma paketi tasarımını detaylı bir şekilde anlatmak amacıyla hazırlanan e-Yazışma Teknik Rehberi'nin "*KEP Entegrasyonu*" başlıklı 3.2'nci maddesinde e-Yazışma Paketinin hukuki geçerliliğe sahip ve güvenilir bir

biçimde taraflar arasında paylaşımında KEP altyapısının kullanılacağı belirlenmiştir (T.C. Kalkınma Bakanlığı, 2014).

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 02/02/2015 tarihli ve 29255 sayılı Resmi Gazetede yayımlanması ile birlikte e-Yazışma Projesinin hukuki dayanağı tamamlanmış ve aynı Yönetmelik ile e-Yazışma Projesi kapsamında resmi yazışmalarını elektronik ortamda gerçekleştirecek kamu kurum ve kuruluşlarının Kalkınma Bakanlığı tarafından hazırlanan e-Yazışma Teknik Rehberi'ne uyumu zorunlu hale getirilmiştir. Böylece kamu kurum ve kuruluşları arasında e-Yazışma Paketinin taraflar arasında paylaşımı için KEP altyapısının kullanılabileceği hüküm altına alınmıştır (T.C. Resmi Gazete, 2015).

4.1.5.3 Ticaret Şirketlerinde Anonim Şirket Genel Kurulları Dışında Elektronik Ortamda Yapılacak Kurullar Hakkında Tebliğ

29/08/2012 tarihli ve 28396 sayılı Resmi Gazete'de Gümrük ve Ticaret Bakanlığı tarafından yayımlanan Ticaret Şirketlerinde Anonim Şirket Genel Kurulları Dışında Elektronik Ortamda Yapılacak Kurullar Hakkında Tebliğ'de KEP'e atıf yapılmıştır. Bu Tebliğ ile; sermaye şirketlerinin yönetim kurulu ve müdürler kurulu toplantılarına, kollektif, komandit, limited ve sermayesi paylara bölünmüş komandit şirketlerin ortaklar kurulu veya genel kurul toplantılarına katılma hakkı bulunanların elektronik ortamda toplantıya katılma talepnamesini, toplantı tarihinden bir gün öncesine kadar güvenli elektronik imza ile imzalayarak şirketin KEP hesabına iletmesi gerektiği ve iletilen bu talepleri alan şirketin de talepte bulunan kişinin toplantı anında Elektronik Toplantı Sistemine erişmesi için gerekli tanımlamaları yaparak hak sahibinin KEP hesabına bu durumu bildirmesi gerektiği belirlenmiştir (T.C. Resmi Gazete, 2012b).

4.1.5.4 Maliye Bakanlığı'nın düzenlemeleri

03/07/2009 tarihli ve 27277 sayılı Resmî Gazete'de yayımlanan 5904 sayılı Gelir Vergisi Kanunu ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun ile 21/07/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında

Kanun'un 77'nci maddesine "*...Tahsil dairelerince düzenlenen haciz bildirileri, alacaklı tahsil dairelerince ya da alacaklı amme idaresi vasıtasıyla, posta yerine elektronik ortamda tebliğ edilebilir ve bu tebligata elektronik ortamda cevap verilebilir. Elektronik ortamda yapılacak tebliğe ve cevapların elektronik ortamda verilebilmesine ilişkin usul ve esasları belirlemeye Maliye Bakanlığı yetkilidir.*" fıkrası eklenmiştir.

01/08/2010 tarihli ve 27659 sayılı Resmi Gazete'de yayımlanan 6009 sayılı Gelir Vergisi Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun ile 04/01/1961 tarihli ve 213 sayılı Vergi Usul Kanunu'na "*Elektronik Ortamda Tebliğ*" başlıklı 107/A maddesi;

> Bu Kanun hükümlerine göre tebliğ yapılacak kimselere, 93 üncü maddede sayılan usullerle bağlı kalınmaksızın, tebliğe elverişli elektronik bir adres vasıtasıyla elektronik ortamda tebliğ yapılabilir. Maliye Bakanlığı, elektronik ortamda yapılacak tebliğle ilgili her türlü teknik altyapıyı kurmaya veya kurulmuş olanları kullanmaya, tebliğe elverişli elektronik adres kullanma zorunluluğu getirmeye ve kendisine elektronik ortamda tebliğ yapılacakları ve elektronik tebliğe ilişkin diğer usul ve esasları belirlemeye yetkilidir.

şeklinde eklenmiştir. Bu madde ile vergi tebligatlarının elektronik ortamda yapılmasına ilişkin yetki Maliye Bakanlığı'na verilmiştir.

28/06/2014 tarihli ve 29044 sayılı Resmî Gazete'de yayımlanan Türk Ceza Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 11/10/2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanuna 9'uncu maddesinden sonra gelmek üzere aşağıdaki madde eklenmiştir.

> Bu Kanun ve 07/02/2013 tarihli ve 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanunun uygulanması kapsamında yapılacak tebligatlar, 11/02/1959 tarihli ve 7201 sayılı Tebligat Kanununun 7/A maddesinde düzenlenen elektronik tebligata ilişkin usullere bağlı olmaksızın, elektronik ortamda tebliğ edilebilir ve tebligata elektronik ortamda cevap verilmesi istenebilir. Bu şekilde yapılan tebligatlar karşı tarafa ulaştığında tebliğ edilmiş sayılır.
> Başkanlık, elektronik ortamda yapılacak tebligatla ilgili her türlü teknik altyapıyı kurmaya veya kurulmuş olanları kullanmaya, tebliğe elverişli

> elektronik adres kullanma ve cevapların elektronik ortamda verilmesi zorunluluğu getirmeye, elektronik ortamda tebliğ yapılacaklar ile elektronik ortamdaki tebligata ilişkin diğer usul ve esasları belirlemeye yetkilidir.

Maliye Bakanlığı tarafından yukarıda yer verilen Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un 9'uncu maddesinin uygulanmasına ilişkin olarak Mali Suçları Araştırma Kurulu Başkanlığı'nın (MASAK) tarafından hazırlanan Elektronik Tebligat Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik 30/03/2015 tarihli ve 29311 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

4.1.6 Düzenlemelerin değerlendirilmesi

4.1.6.1 Kanuni düzenlemelerin değerlendirilmesi

Bölüm 3'te detaylarına yer verilen Almanya, İtalya ve Avusturya örneklerinde yaşanan süreçte, KEP uygulamasının kamu sektöründe başladığı ve bazı zorunluluklarla birlikte özel sektöre yayıldığı görülmektedir. Bahse konu ülkelerde KEP'in e-dönüşüm ve e-devlet kapsamında ele alındığı ve vatandaş-devlet, özel sektör-devlet arasındaki iletişimi kolaylaştırmak amacını güttüğü anlaşılmaktadır. Ülkemizde ise ilk kanuni düzenleme teşebbüsleri bu yönde olsa da, bu düzenleme teşebbüslerinin bir şekilde yasalaşamaması neticesinde KEP sistemine ilişkin düzenlemelerin TTK'da yer bulduğu ve tek bir madde ile tüm KEP sistemine ilişkin ikincil düzenlemeleri yapma görevinin BTK'ya verildiği görülmektedir.

TTK ile KEP'in ilk kullanım alanı olarak tacirler arasındaki işlemler seçilmiştir. Kanun ile KEP kullanılarak yapılabilecek işlemlerin belirtildiği hükümlerin uygulanabilmesi için iki tarafı bulunan işlemlerde taraflar arasında bir anlaşmanın varlığının ön şart olarak bulunması ve seçimlik olarak sunulması gibi hususlar AB ülkelerinde genel olarak kabul gören yaklaşımlardır (Akbulak, 2012). Ancak ilk kullanım alanının bu şekilde belirtilmiş olması sistemin gelişimi ve yaygınlaşması açısından olumsuz bir husus olarak değerlendirilmektedir.

KEP'e ilişkin bir yasal düzenlemenin yapılması, sanılanın aksine, hem teknik ve hem de yasal alanda ayrıntılı çalışma gerektiren oldukça karmaşık bir husus olarak karşımıza çıkmaktadır. Bu düzenlemeler hazırlanırken karşılaşılan problemlerin en başında kişisel verilere yapılacak olan olası hukuka aykırı müdahaleler gelmektedir. Bu problemlerin birçoğu anayasada yer alan hakları doğrudan ilgilendirmektedir. Örneğin sistem adil yargılanma hakkını doğrudan ilgilendiren elektronik tebligat gibi bir alanı da kapsadığından söz konusu yasal korumanın önemi ve boyutu daha da belirginleşmektedir (Tanrıkulu, 2009).

Ancak ülkemizde KEP'e ilişkin düzenlemelerin daha önce incelenen ülke düzenlemeleri ile kıyaslandığında oldukça kısa ve genel hükümler içerdiği görülmektedir. Bu düzenlemelerde gönderimlerin elektronik ortamda **yapılabileceği belirtilmekte fakat elektronik ortamda yapılacak işlemlerin ne şekilde yapılacağı, teknik ve güvenliğe ilişkin alt yapının nasıl olması gerektiği gibi konulara temas edilmemektedir.** İşin nasıl yapılacağının ikincil düzenlemelere bırakıldığı görülmektedir. Oysa KEP ile ilgili hususların gerek Anayasa'nın 13'üncü maddesi ve gerekse özel hayatın dokunulmazlığı başta olmak üzere, adil yargılanma hakkı ve diğer bazı temel hak ve hürriyetlere müdahale imkânı verecek konular olması nedeniyle, yapılan yasal düzenlemelerde esas çerçevesinin iyi çizilmesi gerekmektedir (Tanrıkulu, 2009).

Diğer taraftan bugüne kadar farklı yasalarda ve yasa tasarılarında yapılan KEP ve elektronik tebligat ile ilgili düzenlemelerde değişik kurum ve kuruluşlara ikincil mevzuat yapma görevi verilmiş ve konuya bütüncül bir şekilde yaklaşılmamıştır. Mevzuattaki dağınıklığın ve bu durumun doğurabileceği hukuki belirsizliğin giderilebilmesi için, yukarıda yer verilen mevzuat hükümlerini ortak esaslara bağlayan yasal düzenlemeler yapılması gerekmektedir. Ayrıca düzenleme ihtiyacının yönetmeliklerle değil yasa ile doldurulmasının hukuk güvenliği, idarenin öngörülebilirliği ve kanuniliği ilkeleri çerçevesinde daha isabetli olacağı ifade edilmektedir (Dalkılıç, 2014).

Bununla birlikte konunun özellikle kamu kurum ve kuruluşları ile koordinasyon gerektirmesi nedeniyle hukuki boyut ve kullanım alanları açılarından Başbakanlık gibi tek ve üst bir kurum tarafından ele alınması gerekmektedir. Diğer taraftan Avusturya, İtalya ve Almanya örneklerinde olduğu üzere teknik düzenleme ve denetleme işlevlerinin BTK gibi teknik ve düzenleyici bir otorite tarafından gerçekleştirilmesi yerinde olmuştur. Bu kapsamda hâlihazırda BTK tarafından yapılmış detay teknik düzenlemelerin varlığı bir avantaj olarak değerlendirilmektedir.

Bu kapsamda TTK'da yer alan KEP'e ilişkin Kanun hükümlerinin içerik olarak yetersiz olduğu değerlendirilmektedir. Böyle önemli bir konuda KEP tanımı bile yapılmaksızın tek bir madde ile tüm işleyişin ikincil düzenlemelere bırakılması şeklinde bir yaklaşım uygun görünmemektedir. Diğer taraftan Maliye Bakanlığı örneğinde olduğu gibi farklı kurum ve kuruluşlara farklı kanunlarda bu konuda yetki verilmektedir.

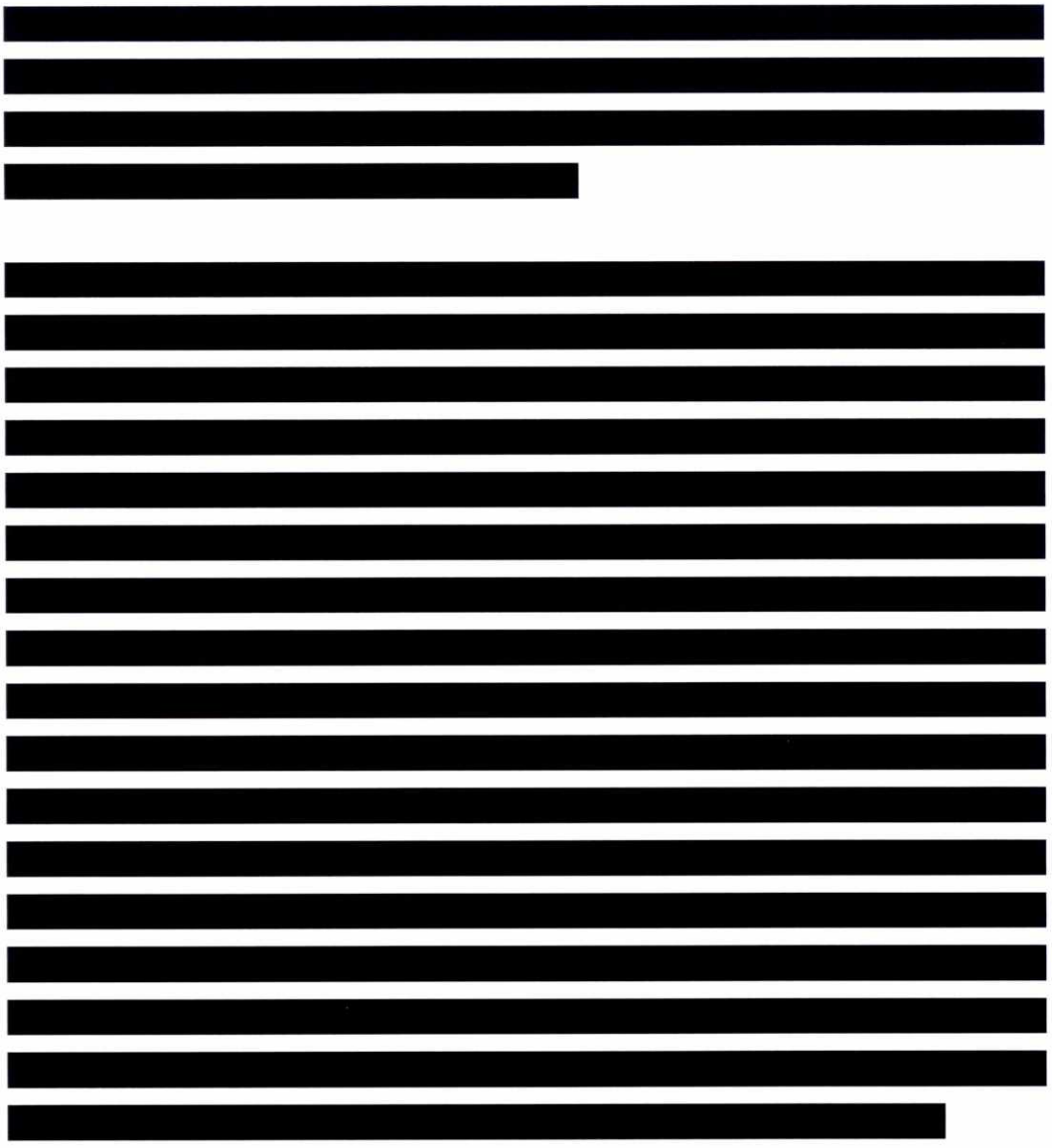
KEP sisteminde, verilerin üçüncü kişiler veya bizzat KEPHS çalışanları tarafından çeşitli şekillerde kötüye kullanılması halinde kişisel verilerin kaydedilmesi (TCK m.135) ve yayılması (TCK m.136), nitelikli dolandırıcılık (TCK m.158/1-f) ve hırsızlık (TCK m.142/2-e) gibi suçların işlenebileceği değerlendirilmektedir. KEP'in güvenli elektronik imzada olduğu gibi özel bir yasa ile düzenlenmeyişi ve 5070 sayılı EİK'de olduğu gibi KEP hesaplarının sahte üretimi ve kötüye kullanımı gibi eylemlerin diğer benzer suç tiplerinden farklılığı gözetilmeden bunlar için özel suç tiplerinin oluşturulmaması eksikliklere örnek olarak gösterilebilir. KEP hesaplarının izinsiz kullanımı ya da oluşturulması eylemlerinin ayrı suçlar olarak düzenlenmesi suretiyle bu alandaki ceza hukuku korumasının güçlendirilmesi daha yararlı olacaktır (Dülger, 2014). Hâlihazırda gerekli ve yeterli önlemleri almamak suretiyle kasten veya bilmeyerek böyle bir kötüye kullanıma sebebiyet veren KEPHS çalışanı ve sahiplerine ancak idari para cezası veya faaliyet durdurma cezası verilebilmektedir. Bu hususun da önemli bir yasa boşluğuna sebep oluduğu değerlendirilmektedir.

Bu kapsamda KEP'e ilişkin tanımların ve hukuki görev ve sorumlulukların da yer alacağı bir kanuni düzenlemeye gidilmesine ihtiyaç duyulduğu aşikârdır. Bununla

birlikte KEP uygulamalarının yaygınlaşması ile hukuken geçerli güvenli elektronik arşiv hizmetlerine ilgi giderek artmaya başlanmıştır. Bu nedenle elektronik arşiv hizmetlerine ilişkin ilave düzenlemelere ihtiyaç bulunmaktadır.

4.1.6.2 Yönetmeliklerin değerlendirilmesi

4.1.6.2.1 KEP Yönetmeliği



Yine KEP Yönetmeliği'nde KEP hesabı başvurularını düzenleyen maddeler, KEPHS'nin temel işlevlerinden olan kimlik tespiti ve doğrulama mekanizmalarına

değinmektedir. KEP sisteminde yer alan tarafların sisteme dâhil olmadan önce uygun kimlik tespit ve doğrulama adımlarından geçirilmesi sistemin genel güvenliğine ve güvenilirliğine etki edecek bir husus olarak karşımıza çıkmaktadır. KEP Yönetmeliği'nde, gerçek kişilerin kimliklerinin "*nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve kimlik yerine geçen geçerli resmî belgelerle veya güvenli elektronik imza ile*" tespit edilmesi, tüzel kişilerin sundukları bilgi ve belgelerin "*MERSİS vasıtasıyla MERSİS No ile*" tespit edilmesi öngörülmektedir. [redacted]

Ayrıca tüzel kişilerin adına hesabı kullanabilecek işlem yetkililerinin bildirilmesi de işin diğer bir boyutunu oluşturmaktadır. Yine KEP Yönetmeliği'ne göre tüzel kişiler, işlem yetkilisi olarak belirledikleri kişilerin kimlik bilgilerini ve yetkili olduklarını gösteren bilgi ve belgeleri başvuru sırasında KEPHS'ye bildirmekle yükümlüdürler. KEP hesabı açılması ve yönetilmesine dair tüm süreçlerin elektronik ortama aktarılabilmesinin önündeki en büyük engel tüzel kişiliği temsile yetkili kişi bilgilerinin elektronik ortamda sağlanamıyor olmasıdır. Süreçlerin tamamının elektronik ortama aktarılabilmesi için noterliklerden veya ilgili kurumdan elektronik ortamda temsile yetkili kişi bilgilerinin temin edilebilir olması gerekmektedir.

[redacted]

[redacted]

4.1.6.2.2 Elektronik Tebligat Yönetmeliği

Elektronik ortamda tebligatın gerçekleştirilmesine ilişkin ayrıntılı hükümler içeren Elektronik Tebligat Yönetmeliği, birtakım eksikliklerle birlikte açıklığa kavuşturulması gereken belirsiz hükümler de içermektedir. Mezkûr Yönetmelik ile elektronik tebligata elverişli hesabın KEP hesabı olduğu belirlenmiş olsa da KEP ve Elektronik Tebligat Yönetmeliği arasında bazı uyumsuzluklar bulunmaktadır. Bu uyumsuzluklar ve problemler genel hatları ile aşağıda yer almaktadır. Bu tez kapsamında sadece elektronik tebligatın KEP ile ilgili olan alanlarına değinilerek bunun dışında kalan elektronik tebligata ilişkin değerlendirmelere ise yer verilmemektedir.

Olay Kayıtları

Elektronik Tebligat Yönetmeliği'nin 9'uncu maddesinin dördüncü fıkrası "*Hizmet sağlayıcılar, muhatabın adresine elektronik tebligatın iletilip iletilmediğine ve gecikme oluşmuşsa bu gecikmeye ilişkin kayıtlar da dâhil tüm süreçlerin olay kayıtlarını tutar, bu bilgileri İdarenin sistemi vasıtasıyla tebligatı çıkaran merciye derhal bildirir.*" hükmünü içermektedir. Aynı Yönetmelik de olay kaydı; "*elektronik tebligat hizmetinin verilmesi esnasında meydana gelen ve mevzuat gereği kaydının tutulması zorunlu olan tüm bilişim sistemi işlem kayıtları*" şeklinde tanımlanmaktadır. KEP sisteminde ise olay kaydının karşılığı olarak deliller ve işlem kayıtları bulunmaktadır. Deliller mesajlaşmanın tarafları ile paylaşılırken, KEPHS'lerin sistemlerinde tutulan işlem kayıtları taraflarla paylaşılmamaktadır. Zaten KEPHS'ler tarafından tutulan işlem kayıtlarının yapıları gereği taraflarla paylaşıma uygun

olmadığı ve delillerin paylaşımı yeterliyken işlem kayıtlarının paylaşımının zorunlu hale getirilmesinin işin doğasına da aykırı olduğu düşünülmektedir.

Kayıtların Saklanma Süreleri

Elektronik Tebligat Yönetmeliği'nin 9'uncu maddesinin beşinci fıkrası "*Olay kayıtları günde en az bir defa olmak üzere zaman damgası eklenerek güvenli elektronik imzayla imzalanır ve erişilebilir şekilde arşivlerde otuz yıl süreyle saklanır.*" hükmünü amirdir. KEP Yönetmeliği'nde ise; "*KEPHS'ler, KEP sisteminin tüm süreçlerine ve işleyişine ilişkin elektronik verilerle, işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kayıtları gizliliğini, bütünlüğünü ve erişilebilirliğini koruyarak en az yirmi yıl süreyle saklamakla*" yükümlü kılınmıştır.

Elektronik Tebligat Hizmeti Alanlar Listesi

Elektronik Tebligat Yönetmeliği'nin 6'ncı maddesinin beşinci fıkrasında anılan "*Elektronik Tebligat Hizmeti Alanlar Listesi*" ile KEP düzenlemelerinde yer alan KEP rehberinin farklı yapılar olduğu değerlendirilmektedir. Elektronik Tebligat Yönetmeliği'nde bahse konu listenin kim tarafından tutulacağı ve bu hususa ilişkin KEPHS'lerin yükümlülükleri net olarak belirlenmemiştir. Bununla birlikte bu listedeki kayıtların MERSİS numarası ile eşleştirilmesine ilişkin hüküm, tüm ticari işletmelerin hâlihazırda MERSİS numarasına sahip olmamaları nedeniyle uygulanamamaktadır.

Delil, Zaman Damgası ve İşlem Sertifikası

Elektronik Tebligat Yönetmeliği'nin 9'uncu maddesinin birinci fıkrası ile elektronik tebligat mesajının sadece zaman damgası ile ilişkilendirileceği belirlenirken, KEP mevzuatıyla elektronik tebligat mesajının karşılığı olan KEP paketinin KEPHS'nin işlem sertifikası ve ESHS'den alacağı zaman damgası ile ilişkilendirileceği belirlenmektedir.

Ayrıca, Elektronik Tebligat Yönetmeliği'nin 9'uncu maddesinin ikinci fıkrasında yer alan "*İdare ve hizmet sağlayıcılar, zaman damgası bilgisini ve mesaj özetini muhataba*

iletmez, sisteminde tutar." ifadesinin de KEP sisteminde tutulan ve taraflarla paylaşılan delillerin içeriğinde mesaj özetinin bulunması hususu ile çelişmektedir.

Muhatabın Elektronik Tebligatı Alma Usulü

Elektronik Tebligat Yönetmeliği'nin 12'nci maddesinin birinci fıkrası ile elektronik tebligat hesabına erişim için elektronik imza veya kullanıcı adı, parola ve tek kullanımlık şifre yöntemlerinin kullanılabileceği belirlenmiştir. Ancak KEP'e ilişkin düzenlemelerde böyle bir zorunluluk bulunmamaktadır. Bu durum hem elektronik tebligat hem de KEP almak üzere hesabını kullanacak kişiler açısından karışıklığa sebep olabilmektedir. Bununla birlikte web servis ile yapılan kurumsal entegrasyonlarda bu hükmün uygulanmasında teknik güçlükler bulunmaktadır.

Elektronik Tebliği Almaya Yetkili Olan Kişi

Elektronik Tebligat Yönetmeliği'nin 12'nci maddesinin ikinci ve üçüncü fıkraları ile gerçek veya tüzel ayrımı yapılmaksızın elektronik tebliğat almaya yetkili kişi veya kişilerin; hesap sahibi, hesap sahibinin vekili veya kanuni temsilcisi olabileceği belirlenmiştir. KEP ile ilgili düzenlemelerde ise gerçek kişiler için vekâlet kavramına yer verilmemiş, tüzel kişiler için ise sadece işlem yetkilisi tanımı yapılmıştır.

Elektronik Tebligat Hesabının Kullanıma Kapatılması

Elektronik Tebligat Yönetmeliği'nin 13'üncü maddesin yedinci fıkrası ile; kendilerine elektronik tebligat yapılması zorunlu olan muhatapların elektronik tebligata elverişli KEP hesaplarının kullanıma kapatılması için başvuruda bulunamayacakları hüküm altına alınırken, KEP mezuatında açılan bir hesaba ilişkin yapılan kapatma taleplerinin derhal işleme alınması gerektiği hüküm altına alınmıştır. Ayrıca Elektronik Tebligat Yönetmeliği'nin 13'üncü maddesinin altıncı fıkrası ile elektronik tebligat adresinin kapatılması için yapılan fiziki başvurularda kapatılma işleminin 5 gün içerisinde

gerçekleştirileceği, KEP ile ilgili yasal düzenlemelerde ise kapatma taleplerinin derhal gerçekleştirilmesi gerektiği belirlenmiştir.

Mesajların Saklanması

Elektronik Tebligat Yönetmeliği'nin 14'üncü maddesinin yedinci fıkrasında elektronik tebligat mesajının iki ay süre ile erişime açık tutulması ve bu sürenin sonunda hizmet sağlayıcı ile muhatap arasında başka bir anlaşma yok ise silinmesi öngörülmektedir. Tanımlanan iki aylık sürenin minimum süre şeklinde değerlendirilmesi gerektiği düşünülmektedir. Ancak KEP mevzuatında KEPHS'lerin mesajları tutma veya hesap sahibinin kendisinin silmesi durumu hariç silme gibi bir işlevleri bulunmamaktadır. Hâlihazırdaki karışıklığı önlemek amacıyla hesap sahipleri ile yapılacak sözleşmelere bu yönde bir madde konulması suretiyle bu maddedeki zorunluluğun ortadan kaldırılabileceği değerlendirilmektedir.

4.1.6.3 Diğer düzenlemelere ilişkin değerlendirmeler

[redacted]

[redacted]

[redacted]

4.2 Teknik Altyapı

Türkiye'deki KEP sistemi Sİ ve SB olmak üzere iki farklı modelde çalışabilmektedir. Sİ modelinde, gönderilen elektronik posta ve bu postaya ilişkin üretilen deliller kullanıcılara doğrudan gönderilmektedir. SB modelinde ise bir depolama alanına konulan orijinal iletiye erişim için oluşturulan referans alıcıya gönderilmektedir. Hâlihazırda Türkiye'de tüm KEPHS'ler Sİ modeli ile hizmet vermektedir.

Bu bölümde öncelikle Türkiye'de uygulanan KEP sisteminin özellikleri, bileşenleri ve işleyişi ele alınarak İkinci Bölüm'de incelenen KEP özelliklerini karşılama açısından sistemin genel bir değerlendirmesine yer verilmektedir.

4.2.1 Sistemin bileşenleri

4.2.1.1 Kullanıcılar

KEP sisteminin kullanıcıları; göndericiler, alıcılar veya yetkili üçüncü taraflardır. KEP Yönetmeliği'nde gönderici; "*Orijinal iletinin alıcısı durumundaki hesap sahibini veya işlem yetkilisi*", alıcı ise "*Orijinal iletinin göndericisi durumundaki hesap sahibini veya işlem yetkilisi*" olarak tanımlanmıştır. Diğer taraftan ETSI (2011a)'da özel

amaçlarla KEP sistemindeki verilere erişebilecek kişi veya kişileri ifade eden üçüncü taraf tanımına Türkiye'deki KEP mevzuatında yer verilmemiştir.

Aynı Yönetmelik'te gönderici ve alıcı tanımlarında yer alan hesap sahibi; "*adına KEP hesabı tahsis edilen gerçek kişiyi veya kamu veya özel hukuk tüzel kişisini*", işlem yetkilisi ise "*hesap sahibinin tüzel kişi olduğu durumlarda ilgili KEP hesabına ilişkin işlemleri tüzel kişi nam ve hesabına yapan gerçek kişi veya kişileri*" şeklinde tanımlanmıştır. Bu tanımlamalara göre; gerçek kişiler için kullanıcı kişinin kendisi oluyorken, hesap sahibinin tüzel kişi olduğu durumda kullanıcı ilgili tüzel kişinin nam ve hesabına işlemleri yürüten bir gerçek kişi olmaktadır.

Burada dikkat çeken husus hesap sahibinin sahibinin, gerçek kişi olmadığı durumda, kamu veya özel hukuk tüzel kişisi olarak tanımlanmasıdır. Bu tanım sebebiyle devlet teşkilatında var olan ve kamu hukuku tüzel kişiliğine sahip olmayan kurum ve kuruluşlarının KEP hesap sahibi olamayabilecekleri düşünülmektedir (Yayla, 2010).

Ayrıca sistemin kullanıcıları olan KEP hesap sahipleri sisteme bir uygulama programı, internet sayfası veya bir servis (örn; web servisi) şeklide de gerçekleştirilebilen UA aracılığıyla bağlanmaktadır.

4.2.1.2 Orijinal ileti

Orijinal ileti, gönderici tarafından üretilen ve göndericinin güvenli elektronik imzasını taşıyan ileti olarak tanımlanmaktadır (BTK, 2014). Orijinal ileti MIME şeklinde oluşturulan elektronik posta iletisinin ETSI (2012)'de tanımlanan CMS gelişmiş elektronik imza (CAdES) ile imzalanarak S/MIME haline getirilmiş şeklidir.

Göndericinin nitelikli elektronik imzasıyla imzalanan orijinal ileti, bir bakıma NRO delilini de içermektedir. Alıcılar, bu ileti üzerindeki elektronik imza sayesinde göndericinin kimliğinden emin olabilirler. Ayrıca orijinal ileti üzerindeki göndericinin imzası mesajın bütünlüğünü de sağlamaktadır.

4.2.1.3 KEP iletisi

KEP iletisi, KEPHS tarafından üretilen KEP delilini içeren ve KEPHS'nin işlem sertifikası ile imzalanmış iletiyi ifade etmektedir (BTK, 2014).

Teknik olarak KEP iletisi, KEPHS tarafından oluşturulan ve ekinde elektronik imzalı KEP delilini taşıyan MIME yapısının, KEPHS'nin işlem sertifikasıyla ETSI (2012)'de tanımlanan arşiv özellikli CMS gelişmiş elektronik imza (CAdES) formatı ile imzalanarak S/MIME haline getirilmiş şeklidir (BTK, 2014).

4.2.1.4 KEP Paketi

KEP paketi, orijinal iletiyi içeren ve KEPHS'nin işlem sertifikası ile imzalanmış iletiyi ifade etmektedir (BTK, 2014). KEP paketi bir anlamda sistemde orijinal iletiyi taşıyacak bir zarf işlevi görmektedir.

Teknik olarak KEP paketi, KEPHS tarafından oluşturulan ve ekinde elektronik imzalı orijinal iletiyi taşıyan MIME yapısının, ETSI (2012)'de tanımlanan arşiv özellikli CMS gelişmiş elektronik imza (CAdES) formatına uygun biçimde KEPHS'nin işlem sertifikasıyla imzalanarak S/MIME haline getirilmiş şeklidir (BTK, 2014). Burada bir S/MIME yapısının başka bir S/MIME içerisinde taşınması söz konusudur. Yani sistem üzerinde iletileri taşınyan KEP paketleri üzerinde iki adet elektronik imza olduğunu söylenebilir.

4.2.2 İnkâr edilemezlik servisleri ve deliller

Bir uyuşmazlık durumunda tarafların, yapılan iş ve işlemlere ilişkin hukuki geçerlilik ifade eden kayıtlar elde edebilmeleri KEP sisteminin temelini oluşturmaktadır. KEP sisteminde deliller, ikinci bölümde anlatılan temel KEP özelliklerinden birisi olan inkâr edilemezliği sağlamak üzere üretilmektedir.

Bu bölümde; Türkiye'de KEP sisteminde kullanılan deliller ile bu delillerin ne zaman, ne şekilde, kim tarafından ve hangi alanları içerecek şekilde oluşturulacakları incelenmektedir.

4.2.2.1 Olaylar ve KEP delilleri

Türkiye'de KEP sisteminde 11 farklı olay sonucunda oluşturulan deliller Tablo 4.1'de yer almaktadır.

Tablo 4.1. KEP sisteminde oluşturulan deliller

Tetikleyici Olay	Delilin Adı	Oluşturan Taraf	Geçerli Olduğu Model
Gönderim Kabul	Gönderici KEPHS Kabul (SubmissionAcceptanceRejection:Acceptance)	Gönderici KEPHS	Sİ ve SB
Gönderim Red	Gönderici KEPHS Red (SubmissionAcceptanceRejection:Rejection)	Gönderici KEPHS	Sİ ve SB
Aktarım Kabul	Alıcı KEPHS Kabul (RelayToREMMDAcceptanceRejection:Acceptance)	Alıcı KEPHS	Sİ ve SB
Aktarım Red	Alıcı KEPHS Red (RelayToREMMDAcceptanceRejection:Rejection)	Alıcı KEPHS	Sİ ve SB
Aktarım Hata	Alıcı KEPHS'ye belirli bir süre sonunda teslim edilemedi (RelayToREMMDFailure)	Gönderici KEPHS	Sİ ve SB
Mesaj Erişim	Alındı, Erişildi (RetrievalNonRetrievalByRecipient:Retrieval)	Alıcı KEPHS	Sİ
Belli bir süre içinde alınmadı, erişilmedi	Alıcı tarafından belirli bir süre içinde alınmadı, erişilmedi (RetrievalNonRetrievalByRecipient:RetrievalExpiration)	Alıcı KEPHS	Sİ
Teslim	Alıcıya Teslim Edildi (DeliveryNonDeliveryToRecipient:Delivery)	Alıcı KEPHS	Si ve SB
Teslim edilemedi	Alıcıya belirli bir süre içinde teslim edilemedi (DeliveryNonDeliveryToRecipient:DeliveryExpiration)	Alıcı, Gönderici KEPHS	Sİ ve SB
İndirildi	Alıcı tarafından indirildi (DownloadNonDownloadByRecipient:Download)	Alıcı	SB
Belirli bir süre içerisinde indirilmedi	Alıcı tarafından belirli bir süre içerisinde indirilmedi (DownloadNonDownloadByRecipient:DownloadExpiration)	Alıcı	SB

Tablo 4.2. KEP delillerinin zorunluluk durumları

Delilin Adı	ETSI (2011a)	BTK (2014)
Gönderici KEPHS Kabul (SAR) (SubmissionAcceptanceRejection:Acceptance)	Zorunlu	Zorunlu
Gönderici KEPHS Red (SAR) (SubmissionAcceptanceRejection:Rejection)	Zorunlu	Zorunlu
Alıcı KEPHS Kabul (RAR) (RelayToREMMDAcceptanceRejection:Acceptance)	Gerekli	Zorunlu
Alıcı KEPHS Red (RRAR) (RelayToREMMDAcceptanceRejection:Rejection)	İsteğe Bağlı	Zorunlu
Alıcı KEPHS'ye belirli bir süre sonunda teslim edilemedi (RRF) (RelayToREMMDFailure)	Gerekli	Zorunlu
Alıcı tarafından Alındı, Erişildi (RNRR) (RetrievalNonRetrievalByRecipient:Retrieval)	İsteğe Bağlı	Zorunlu
Alıcı tarafından Belirli bir süre içinde alınmadı, erişilmedi (RNRR) (RetrievalNonRetrievalByRecipient:RetrievalExpiration)	İsteğe Bağlı	Zorunlu
Alıcıya Teslim Edildi (DNDR) (DeliveryNonDeliveryToRecipient:Delivery)	Zorunlu	Zorunlu
Belirli bir süre içinde KEP paketi alıcıya teslim edilemedi (DNDR) (DeliveryNonDeliveryToRecipient:DeliveryExpiration)	Zorunlu	Zorunlu
Alıcı tarafından indirildi (DLNDLR) (DownloadNonDownloadByRecipient:Download)	Zorunlu	Zorunlu
Belirli bir süre içerisinde indirilmedi (DLNDLR) (DownloadNonDownloadByRecipient:DownloadExpiration)	Zorunlu	Zorunlu

BTK (2014)'te tamamı zorunlu olarak tanımlanan delillerin bir kısmı Tablo 4.2'de de görüleceği üzere ETSI (2011a)'de isteğe bağlı olarak belirtilmiştir. KEP sisteminde oluşturulan bu deliller ve detayları aşağıdaki şekilde tanımlanabilecektir (ETSI 2011a; BTK, 2014).

- **Gönderici KEPHS ileti kabul delili:** Göndericinin hizmet aldığı KEPHS'nin, göndericinin kimlik doğrulamasını yaptıktan sonra iletilmek istenen orijinal iletiyi başarılı bir şekilde teslim aldığını kanıtlar. Bu delil NRS delili olarak nitelendirilebilir. Bu delil hem Sİ hem de SB modeli için geçerlidir.
- **Gönderici KEPHS ileti red delili:** Göndericinin hizmet aldığı KEPHS'nin, göndericinin kimlik doğrulamasını yaptıktan sonra orijinal iletiyi başarılı bir

şekilde teslim aldığını ancak orijinal iletinin KEPHS tarafından belirli bir sebeple kabul edilmediğini kanıtlamaktadır. Bu delil olumsuz NRS delili olarak değerlendirilebilir.

- **Alıcı KEPHS ileti kabul delili:** Gönderici KEPHS tarafından gönderilen bir KEP paketinin, alıcı KEPHS tarafından başarılı bir şekilde teslim alındığını ve iletilmek üzere kabul edildiğini kanıtlamaktadır. Göndericinin ve alıcının farklı KEPHS'lerden hizmet aldığı durumda üretilmektedir. İletinin KEPHS'ler arası devrine ilişkindir. Bu delil alıcı KEPHS tarafındaki NRS delili olarak kabul edilebilir.
- **Alıcı KEPHS ileti red delili:** Gönderici KEPHS tarafından gönderilen bir KEP paketinin, alıcı KEPHS tarafından başarılı bir şekilde teslim alındığını fakat KEP paketinin KEPHS tarafından belirli bir sebeple kabul edilmediğini kanıtlamaktadır. Bu delil alıcı KEPHS tarafındaki olumsuz NRS delili olarak kabul edilebilir.
- **Alıcı KEPHS'ye belirli bir süre sonunda teslim edilemedi delili:** Alıcı KEPHS'den KEP paketinin belirli bir süre (altı saat) içinde alındığına veya herhangi bir sebeple reddedildiğine ilişkin bir delil gelmezse, gönderici KEPHS dört kez daha gönderim işlemini tekrarlar ve bu denemeler sonucunda hala alıcı KEPHS'den bir yanıt alınamazsa iletinin alıcı KEPHS'ye teslim edilemediğini kanıtlamaktadır.
- **Teslim edildi:** KEP paketinin alıcının KEP hesabına teslim edildiğini kanıtlamaktadır. Bu delil NRD delili olarak sistem içerisinde yer almaktadır.
- **Belirli bir süre içinde teslim edilemedi:** KEP paketinin, belli bir süre içinde herhangi bir sebeple alıcının KEP hesabına teslim edilemediğini kanıtlar. Bu süre BTK (2014)'te altı saat olarak belirlenmiştir. Altı saat içinde teslimin gerçekleştirilememesi halinde işlem dört defa tekrar edilmektedir. KEP paketi bu denenme işlemlerinin sonucunda da teslim edilemezse teslim edilemedi delili üretilmektedir. Gönderici KEPHS tarafından ise "Alıcı KEPHS ileti kabul delili" alındıktan sonra 24'üncü saat sonrası bu delil üretilmektedir. Bu delilin alıcının hizmet aldığı KEPHS tarafından üretilmesi gerekirken herhangi

bir hata halinde söz konusu süreler beklendikten sonra göndericinin hizmet aldığı KEPHS tarafından da üretilebilmektedir.

- **Alındı (okundu, erişildi) delili:** BTK (2014)'ya göre Alıcının KEP hesabına teslim edilen KEP paketinin, alıcı tarafından okunduğunu kanıtlamaktadır. ETSI (2011a)'ye göre bu delil alıcının posta kutusuna erişimini ispatlamak amacıyla isteğe bağlı olarak kullanılırken ülkemizdeki mevzuata göre zorunlu olarak üretilmesi gerekmektedir.
- **Belirli bir süre içinde alınmadı (okunmadı, erişilmedi) delili:** Alıcının KEP hesabındaki KEP paketinin, alıcı tarafından belirli bir süre içinde okunmadığını kanıtlamaktadır. Yönetmeliğin 12'nci maddesinin ikinci fıkrası uyarınca bu delilin KEP paketinin alıcıya teslim edilmesini takip eden iş günü saat 23:59'da üretilmesi gerekmektedir. Bir önceki delile paralel olarak BTK (2014) ile ETSI (2011a) arasında bir yorum farkı bulunmaktadır.
- **Alıcı tarafından indirildi delili:** KEP paketinin alıcı veya işlem yetkilisi tarafından belirli bir süre içinde indirildiğini kanıtlamaktadır. Bu delil sadece SB modelinde üretilmektedir.
- **Belirli bir süre içerisinde indirilmedi delili:** KEP paketinin belirli bir süre içinde alıcı KEPHS'nin depolama alanına erişilmek suretiyle indirilmediğini kanıtlamaktadır. Bu delilin, KEP Yönetmeliği'nin 12'nci maddesinin ikinci fıkrası uyarınca KEP paketinin alıcıya teslim edilmesini takip eden iş günü saat 23:59'da üretilmesi gerekmektedir. Bu delil sadece SB modelinde üretilmektedir.

Tüm bu delillerin yanı sıra ETSI (2011a)'de yer alan fakat Türkiye'de kullanılmayan deliller;

- Geleneksel kayıtlı posta ile teslim için basılı hale getirilmesi işlemine ilişkin delil
- Geleneksel kayıtlı posta ile teslimi için basılı hale getirilmesinin başarısız olduğuna ilişkin delil
- Standart elektronik postaya gönderime ilişkin delil

- Standart elektronik postaya gönderimin başarısız olduğuna ilişkin delil
- Standart elektronik postadan ileti alındığına ilişkin delil

olarak sayılmaktadır (ETSI 2011a; 2011d).

Bu delillerden iletilerin basılı hale getirilip geleneksel kayıtlı posta ile gönderilmesine yönelik olan delillerin ülkemizde de kullanılmasının önünde herhangi bir engel bulunmamaktadır. Sektörden gelebilecek talepler doğrultusunda özellikle yerleşik posta hizmet sağlayıcısı olan PTT'nin, bu hizmeti verebileceği değerlendirilmektedir. Çünkü bu delilin elektronik tebligat kapsamında yaygın bir kullanım alanı bulunmaktadır.

4.2.2.2 KEP delil içerikleri

ETSI (2011b)'de sistem içerisinde oluşturulacak delillerde bulunması zorunlu ve isteğe bağlı tüm bileşenler tanımlanmaktadır (Bkz. Tablo 4.3).

Tablo 4.3'te yer alan bu bileşenlerden bazıları bir delil için kullanılırken başka bir delilde kullanılmamaktadır. Bu husus söz konusu delilin neyi ve ne şekilde kanıtlamak üzere üretildiği ile ilgilidir. Hangi alanların hangi delillerde bulunabileceğine ilişkin bilgilere Tablo 4.4'te yer verilmektedir. Örneğin sadece gönderenin hizmet sağlayıcısında bulunan ve gönderici kimlik doğrulama verilerini içeren "I04" bileşeni sadece gönderici KEPHS tarafından üretilen "Gönderici KEPHS Kabul" delili içerisinde yer almaktadır.

Ayrıca bir bileşenin alması gereken değer de deliller arası farklılıklar gösterebilmektedir. Örneğin olay türleri ve sebep kodları hemen hemen tüm delillerde farklı değer kümesinden seçilerek kullanılmaktadır. Bu nedenle ETSI (2011b)'de bileşenlerin alması gereken değerlere ve bunların açıklamalarına yer verilmektedir. Hatta bu değerler delillerin hangi formatta (ASN, XML veya PDF) oluşturulacağına göre de farklılaşabilmektedir.

Tablo 4.3. Delil bileşenleri

		ID	BİLEŞEN AÇIKLAMASI
KEP DELİL BİLEŞENLERİ	Temel Bileşenler	G00	KEPHS tarafından oluşturulan tekil delil tanımlayıcısı
		G01	Delil Tipi
		G02	Delili tetikleyici KEP Olayı
		G03	Delili tetikleyen olay sebep kodu
		G04	Delil sürüm bilgisi
		G05	Delili tetikleyen olay zamanı
		G06	İşlem log bilgileri (Transaction log information)
	KEPHS ile İlişkili Bileşenler	R01	Delili oluşturan politika tanımlayıcısı (policy identifier)
		R02	Delili oluşturan bilgileri
		R03	Delili oluşturan KEPHS'nin imzası
	Kimlik Bilgileriyle İlişkili Bileşenler	I00	Gönderici bilgileri
		I01	Alıcı bilgileri
		I02	Alıcıya vekâlet eden vekilin bilgileri
		I03	Delilin ilgili olduğu alıcı bilgisi
		I04	Gönderici kimlik doğrulama bilgileri
		I05	Alıcı kimlik doğrulama bilgileri
	Mesajlaşmaya İlişkin Bileşenler	M00	KEP Paketi/KEP İletisi bilgileri
		M01	Cevap adresi
		M02	Bildirim olup olmadığına ilişkin etiket
		M03	Mesaj gönderim zamanı (Message submission time)
		M04	Gönderilen dış sistem (standart e-posta vb. gibi)
	Diğer	Enn	Sonradan eklenmesi muhtemel alanlar

Kaynak: ETSI, 2011d

Tablo 4.4. Delillerde bulunan bileşenlerinin kullanımı

		DELİLLER					
		SAR	RRAR	RRF	DNDR	RNRR	DLNDLR
BİLEŞENLER	G00	Z	Z	Z	Z	Z	Z
	G01	Z	Z	Z	Z	Z	Z
	G02	Z	Z	Z	Z	Z	Z
	G03	Z	Z	Z	Z	Z	Z
	G04	Z	Z	Z	Z	Z	Z
	G05	Z	Z	Z	Z	Z	Z
	G06	İ	İ	İ	İ	İ	İ
	R01	Z	Z	Z	Z	Z	Z
	R02	Z	Z	Z	Z	Z	Z
	R03	Z	Z	Z	Z	Z	Z
	I00	Z	Z	Z	Z	Z	Z
	I01	Z	Z	Z	Z	Z	Z
	I02	-	-	-	Z	Z	Z
	I03	-	Z	Z	Z	Z	Z
	I04	Z	-	-	-	-	-
	I05	-	-	-	-	Z	Z
	M00	Z	Z	Z	Z	Z	Z
	M01	Z	-	-	-	Z	-
	M02	-	Z	Z	Z	Z	-
	M03	Z	Z	Z	Z	Z	Z
	M04	-	-	-	-	-	-

Z: Zorunlu, İ: İsteğe Bağlı, -: Kullanılmaz

4.2.2.3 Delil formatları

Türkiye'deki KEP sisteminde deliller ASN.1, PDF veya XML formatlarından biri ile oluşturulabilmektedir. Bu formatlar ile deliller içerisinde bulunması gerekli olan alanların ne şekilde ve nasıl kullanılacağı hususları detaylandırılmaktadır (ETSI (2011b).

KEP delilleri ile bu delillerin içeriklerinin, KEPHS'ler arası birlikte çalışabilirliğe doğrudan etki eden unsurlar olduğundan KEPHS'ler tarafından oluşturulan delillerde farklı formatların tercih edilmesi halinde bazı sıkıntıların oluşabileceği değerlendirilmektedir. Çünkü bir KEPHS'nin farklı formatta delil oluşturması diğer KEPHS'nin bu delilleri doğrulaması açısından bazı problemler ve ek maliyetler getirebilecektir. Diğer taraftan KEPHS'lerin denetimleri gerçekleştirilirken bu formatların da kontrol edilmesi için ayrı bir çaba ve kaynak harcanması gerekecektir.

4.2.2.4 Delillere ilişkin değerlendirme

Türkiye'deki KEP sisteminde yer alan tüm deliller KEPHS tarafından oluşturularak imzalanmaktadır. Sistemde oluşturulan deliller, Bölüm 2.3.1.1'de verilen bilgilere göre değerlendirildiğinde aşağıdaki sonuçlara ulaşılmaktadır.

- NRO, gerek KEPHS tarafından sağlanan delil içerikleri gerekse orijinal iletinin gönderici tarafından imzalanması ile sağlanabildiği değerlendirilmektedir. Bununla birlikte delil içerisinde bulunan alanlar ile sağlanan NRO'nun güvenilirliğinin göndericinin sisteme giriş esnasında kullandığı kimlik doğrulama yönteminin güvenilirliği ile doğru orantılı olduğu da görülmektedir.
- NRS ve olumsuz NRS'yi sağlamak üzere birden fazla delil olduğu görülmektedir. Göndericinin hizmet aldığı KEPHS'ye iletiyi gönderdiğini kanıtlayan SAR delili, KEPHS'ler arası iletilerin gönderimine ilişkin üretilen RRAR ve RRF delilleri bu amaçla üretilmektedir.

- NRD ise sistemde DNDR ve DLNDLR delilleri ile sağlanmaktadır. Ayrıca alıcıların posta kutusuna teslim edilen iletileri okuduğunda üretilen RNRR delili ise DNDR delilinin bir üst aşaması olarak kabul edilmektedir.
- NRR sistem içerisinde doğrudan bir delil olmamakla birlikte gerek DNDR gerekse RNRR delillerinde yer alan alıcının kimlik doğrulama mekanizmalarına ilişkin bileşenler yardımıyla gerçekleştirilebilmektedir. Bu durumda alıcının iletilere erişmek ve okumak üzere sisteme bağlanmak için kullandıkları kimlik doğrulama mekanizmasının önemi artmaktadır. Üretilen bahse konu delillerin NRR'yi sağlama durumu alıcıların sisteme bağlantıda kullandıkları kimlik doğrulama mekanizmasının güvenilirliği ile doğru orantılıdır.

KEP sisteminde deliller bir HSM vasıtasıyla KEPHS'nin işlem sertifikası kullanılarak imzalandıktan sonra ilgili taraflar ile paylaşılmaktadır. Bu açıdan delillerin paylaşılabilir ve KEPHS'ye ihtiyaç olmaksızın doğrulanabilir olduğu söylenebilir.

Delil içeriklerinin ise uluslararası kabul gören ve Bölüm 2.3.1.1.5'te belirtilen içeriklere fazlasıysa sahip olduğu görülmektedir.

4.2.2.5 İşlem kayıtları

Türkiye'deki KEP sisteminde taraflar ile paylaşılabilen ve paylaşılamayan deliller olmak üzere iki farklı delil tipi bulunmaktadır. Taraflar ile paylaşılabilen deliller Bölüm 4.2.1.2'de anlatılan ve ETSI (2011a; 2011d)'de tanımlanan ve "xml" olarak üretilip KEPHS tarafından nitelikli elektronik sertifikayla imzalanan delillerdir. Taraflar ile paylaşılamayan deliller ise, ancak bir uyuşmazlık durumunda kullanılabilecek olan ve KEPHS'lerin tüm süreçlerine ilişkin tutmuş olduğu işlem kayıtlarıdır. Bu kayıtlar da yine KEPHS'ler tarafından işlem sertifikası kullanılarak imzalanmaktadır. Sistemde delillerin tamamı KEPHS'ler tarafından oluşturulmaktadır.

KEP sisteminde tutulması gereken işlem kayıtları, bu kayıtlarda bulunması gereken alanlar ve bunların ne kadar süre ile ne şekilde tutulacağına ilişkin hususlar mevzuat ile belirlenmiştir. Buna göre 20 yıl saklanması öngörülen işlem kayıtları aşağıdaki şekildedir (BTK, 2014, m.24).

- **Uygulama işlem kayıtları:** KEP sisteminde iletim ve delil üretilmesinden sorumlu uygulamalar, rehber servisi vb. gibi uygulamalar tarafından üretilen, bilgilere ve verinin iletimine yönelik kayıtlar
- **Kullanıcı ve operatör erişim işlem kayıtları:** Kullanıcıların/operatörlerin müşteri yönetimi, web mail, web başvuru ekranları vb. üzerinden gerçekleştirdikleri işlemlere ilişkin işlem kayıtları
- **İptale ilişkin ses kayıtları**: KEP hesaplarının iptaline ilişkin çağrı merkezi ses kayıtları
- **KEP altyapısında bulunan sistem bileşenlerinde yönetimsel amaçlı yapılan işlemlere ilişkin işlem kayıtları:** KEP altyapısında bulunan sistem bileşenlerinde kullanıcılar, operatörler ve yöneticiler tarafından gerçekleştirilen bütün işlemlere ilişkin işlem kayıtları

Diğer taraftan KEPHS, KEP sisteminde tuttuğu yukarıda sayılan işlem kayıtlarını üç saatte bir işlem sertifikasıyla imzalayarak belirlenen süre kadar saklamakla yükümlü tutulmaktadır (BTK, 2014).

4.2.3 Elektronik imza kullanımı

KEP sisteminde elektronik imza; güvenilirlik, bütünlük ve kimlik doğrulama gerektiren tüm aşamalarda kullanılmaktadır. KEP sisteminde elektronik imzanın kullanım alanları ve imzalamada kullanılacak imza formatları Tablo 4.5'te yer almaktadır.

Tablo 4.5. Türkiye'de kullanılan imza formatları

İMZALANACAK VERİ	İMZA FORMATI
KEP Delilleri	XAdES-A
KEP İletileri	S/MIME formatında üzerinde imza CadES-A
KEP Paketi	S/MIME formatında üzerinde imza CadES-A
İşlem Logları	CAdES-A
Orijinal İleti	S/MIME formatında üzerinde imza CadES-BES
E-İmza ile Kimlik Doğrulama (Login)	CadES-BES
Sözleşme veya taahhütname	CadES-A veya PadES-A

Kaynak: BTK, 2014

BTK (2014) ile KEP sisteminde kullanılacak imza formatlarının;

- CAdES olması durumunda imzalamanın ETSI TS 101 733 (ETSI, 2012),
- XAdES olması durumunda imzalamanın ETSI TS 101 903 (ETSI, 2009a),
- PAdES olması durumunda imzalamanın ETSI TS 102 778-3 (ETSI, 2009d), ETSI TS 102 778-4 (ETSI, 2009b), ETSI TS 102 778-5 (ETSI, 2009e)

dokümanlarına uygun olarak oluşturulması gerektiği belirlenmiştir.

Ayrıca arşiv imza olarak belirlenen formatlarda kullanılacak imzalarda BTK (2012a)'da yer alan P4 profiline uygun olarak oluşturulması gerektiği hüküm altına alınmıştır (BTK, 2014).

Sistem içerisinde kullanılan tüm elektronik imzalar 5070 sayılı Elektronik İmza Kanunu kapsamında tanımlanan nitelikli elektronik sertifikalar (NES) kullanılarak oluşturulmaktadır. Bu açıdan kullanılan imzalar, sistemin geneline ilişkin hukuki geçerlilik sağlama adına temel yapı taşlarındandır. Bu nedenle sistemdeki imzaların mevzuata ve mevzuatla belirlenen standartlara uygun ve doğru oluşturulması büyük önem arz etmektedir.

Diğer taraftan KEP sisteminde kullanılan imzalar KEPHS'ler arası birlikte çalışabilirliğe en fazla etki eden unsurlardan biri olarak karşımıza çıkmaktır. Sistem

içerisindeki KEP iletileri, KEP paketleri ve delillerin üzerlerindeki imzaların KEPHS'ler arası doğrulanabilmesi sistemin sağlıklı ve doğru çalışabilmesi için gereklidir. Gönderilen bir KEP iletisi veya KEP paketi alıcı KEPHS tarafından imza kontrolüne tabi tutulmaktadır. Bu kontrol sonucunun başarısız olması durumunda işlem sonlandırılmaktadır.

Bu sebeple gerek yetkilendirilme aşamasında gerekse de hizmet vermeye başladıktan sonra KEPHS'lerin oluşturdukları elektronik imzaların doğruluğunun ortaya konabilmesi ve testlerden geçirilmesi gerekmektedir. Tablo 4.5'te de gösterilen sistem içerisinde oluşturulan imzalardan S/MIME üzerindeki CAdES-A ve XAdES-A formatları yaygın olarak kullanılmadığından piyasada bulunan elektronik imza doğrulama yazılımları tarafından doğrulamaları yapılamamaktadır.

4.2.4 Bağlantı katmanı ve güvenliği

KEP sisteminde; Gönderici G-KEPHS, Alıcı A-KEPHS ve KEPHS'ler arası olmak üzere üç farklı iletişim kanalı bulunmaktadır. Tüm bu iletişim kanallarının güvenli ve şifreli olması sistemin bütünü için çok önemlidir.

Türkiye'de KEP sisteminde gönderici ve G-KEPHS arasındaki bağlantının gizliliği temin edecek uygun bir yöntem kullanılarak gerçekleştirilmesi gerekliliği belirtilmiş olmakla birlikte kullanılacak yöntem KEPHS'ye bırakılmıştır (ETSI, 2011e). KEPHS'ler tarafından bu aşamadaki güvenli bağlantı genellikle TLS veya SSL üzerinden SMTP kullanılarak gerçekleştirilmektedir.

Benzer şekilde alıcı ve A-KEPSH arasındaki bağlantıda da bağlantının, gizliliği temin edecek uygun bir yöntem kullanılarak gerçekleştirilmesi gerekliliği belirtilmiştir (ETSI, 2011e). KEPHS'ler tarafından bu aşamadaki güvenli bağlantı ise TLS veya SSL üzerinden IMAP kullanılarak gerçekleştirilmektedir.

Birlikte çalışabilirliğin temelini oluşturan bağlantı katmanındaki en önemli kısım KEPHS'ler arasındaki bağlantıdır. KEPHS'ler arası bağlantı sağlam, güvenli ve güvenilir olmadığında alınabilecek diğer tüm önlemler anlamlarını yitirebilmektedir.

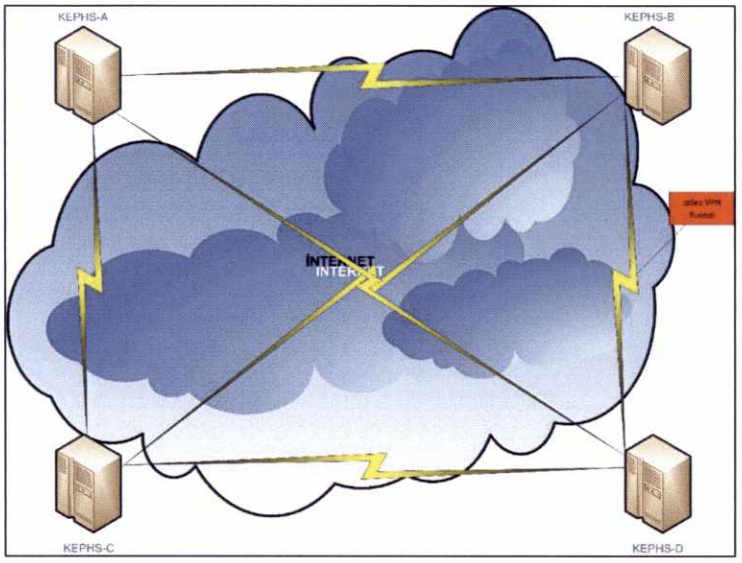
ETSI (2011e) ile KEPHS'ler arası ileti gönderimlerinin TLS üzerinden SMTP ile sağlanması zorunlu hale getirilmektedir. BTK (2014) ile de KEPHS'ler arasında bütünlük, kimlik doğrulama ve gizlilik içerecek şekilde kapalı bir ağ yapısı oluşturulması amacıyla IPSec VPN yapısının kullanılması zorunlu hale getirilirken [redacted]

Bu şekildeki bir bağlantıyı gösteren Şekil 4.1'deki yapıya göre herbir KEPHS diğer KEPHS'ler ile tek tek VPN kurulumları gerçekleştirmek suretiyle bağlantı sağlamaktadır. Bu durumda sisteme yeni dâhil olan bir KEPHS'nin tüm KEPHS'lerle irtibat kurarak parametreleri belirlemesi ve kurulumu gerçekleştirmesi gerekmektedir. Az sayıda KEPHS'nin bulunduğu bir sistem için bu yapı, zorluklarına rağmen yönetilebilir ve ölçeklenebilirken, KEPHS sayısının arttığı durumlarda yönetilebilir ve sürdürülebilir olmaktan uzaklaşmaktadır. Ayrıca Şekil 4.1'de anlatılan IPSec VPN yapısının benzerinin canlı ortam öncesi test ortamlarında da gerçekleştirilmesi gerekmektedir.

Sektöre yeni girecek olan bir KEPHS'nin hizmet vermeye başlaması önünde kurulumun bir engel oluşturması ve yerleşik KEPHS'lerin bu entegrasyon konusunda ağır davranabilmeleri rekabeti engelleyici bir husus olarak karşımıza çıkmaktadır. Ayrıca bu bağlantının yedeğinin bulunmaması nedeniyle de var olan KEPHS'ler arası zaman zaman bağlantı problemlerinin yaşanması muhtemeldir.

Tüm bu dezavantajlar nedeniyle KEPHS'ler arası bağlantının yedekli bir şekilde benzer güvenlik özelliklerine sahip, erişim tekniklerinden bağımsız, gerek kullanım kolaylığı gerekse güvenilirliği yüksek bir yapıda oluşturulmasına ihtiyaç duyulmaktadır.

Şekil 4.1. Türkiyede'ki KEPHS'ler arası bağlantı



4.2.5 KEP güven zinciri

KEP sisteminde güvenin tesis edilmesi ve TTP olarak yetkilendirilen hizmet sağlayıcıların genele açık bir dizinde yayımlanması önem arz etmektedir.

Türkiye'de KEPHS'ler TTP olarak KEP hizmetini vermek üzere yetkilendirildiklerinde BTK internet sayfasından ilan edilmektedirler. ETSI (2011a)'ye göre bu yayımlama işlemi ETSI (2009c)'de detaylandırılan güvenilir hizmetler durum listesi (Trust-service Status List-TSL) kullanılarak da yapılabilecektir. Ülkelerde kurulu KEP sistemlerinin milletlerarası birlikte çalışabilirliği söz konusu olduğunda bu husus kaçınılmaz bir hal alabilecektir. Yapılan işlemlere ilişkin hukuki geçerlilik sağlayan kritik bir husus olması dolayısıyla yayımlama işlemi titizlikle yerine getirilmelidir.

4.2.6 Kayıtların saklanması ve arşivlenmesi

ETSI (2011c)'de KEP hizmetlerinin sağlanmasında oluşturulan işlem kayıtları ve delillerin sistemin kurulu bulunduğu ülkede mevzuatla belirlenen süre kadar

saklanması ve bu sürenin sonunda uygun bir yöntemle imha edilmesi öngörülmüştür. Bu kapsamda KEP Yönetmeliği'nde KEP sisteminde KEP hizmetlerinin verilmesi ile ilişkili işlem kayıtları ve delillerin 20 yıl süre ile saklanması hükmü getirilmiştir. Elektronik Tebligat Yönetmeliği'nde ise bu süre 30 yıl olarak belirlenmiştir.

KEPHS'ler kuracakları sistemde bahse konu kayıtları belirlenen süreler kadar gizlilik, bütünlük ve erişebilirlik açılarından uygun bir yöntem ile depolamakla yükümlüdürler. Bu nedenle sistem içerisinde kritik öneme haiz bu verilerin saklanmasına yönelik özel önlemler alınması gereklidir.

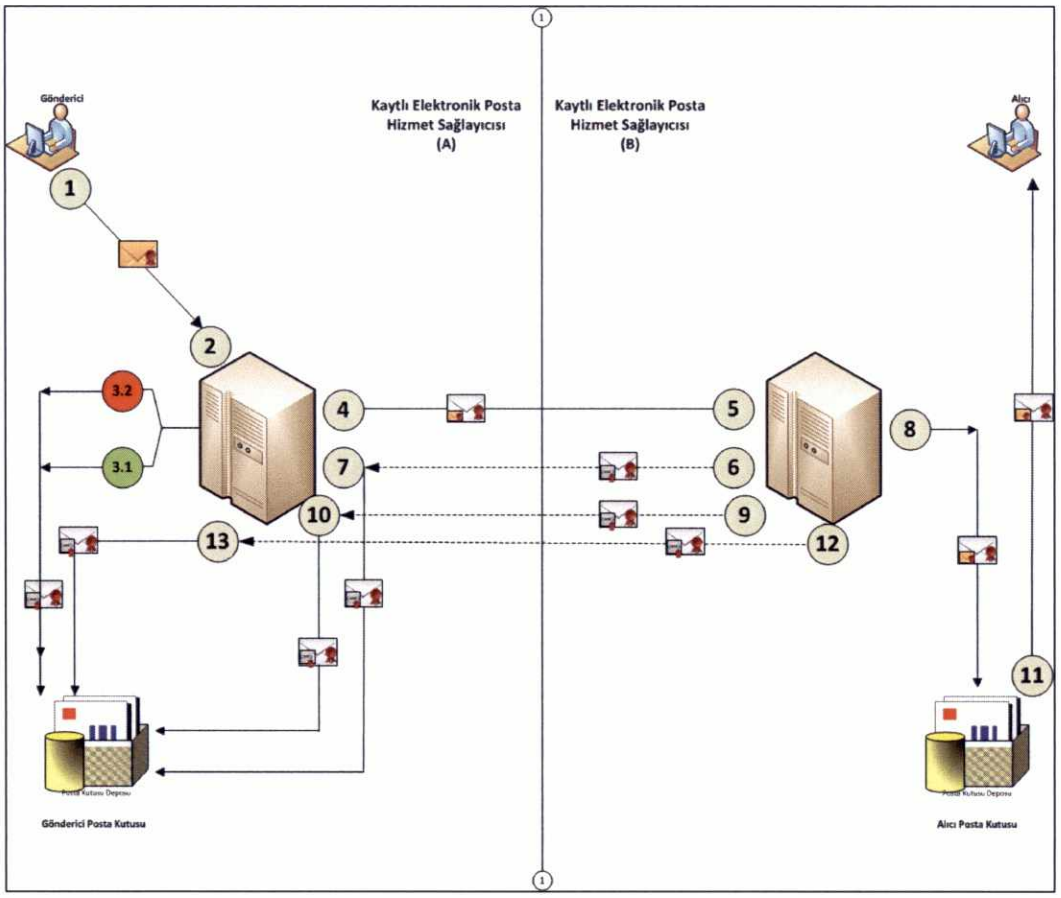
Uzun dönemli saklanması gereken elektronik imzalı delillerin ve işlem kayıtlarının elektronik imzanın doğası gereği saklama süreleri içerisinde tekrar imzalanması gerekmektedir. Tekrar imzalama periyodu, imzalamada kullanılan algoritmaların veya anahtarların artık güvenli kabul edilmediği ve imzanın veya zaman damgasının kökünün süresinin dolduğu durumlarda gerçekleştirilir. Bu işlem önceden oluşturulmuş imza dosyalarına zaman damgası alınması yoluyla gerçekleştirilmekte ve tekrar imzalama işlemi yani arşivleme gerektikçe tekrarlanmaktadır (Topcan, 2011).

Mevzuatta arşiv özelliğine sahip olması gerektiği belirtilen (Bkz. Tablo 4.5) ve KEPHS'nin arşivlemekle yükümlü olduğu kayıtlar için bu yöntemin uygulanması gerekecektir.

4.2.7 Sistemin işleyişi

Şekil 4.2'te Türkiye'de kullanım alanı bulan Sİ çalışma modeli detaylandırılmaktadır. Buna göre sistemin çalışma adımları şu şekildedir:

Şekil 4.2. Türkiye KEP çalışma modeli



1. Gönderici, kullandığı UA veya istemci uygulama aracılığıyla orijinal iletiyi MIME formatında oluşturur ve bu iletiyi güvenli elektronik imzasıyla imzalamak suretiyle S/MIME hale getirerek hizmet aldığı KEPHS'ye gönderir.
2. Göndericinin hizmet aldığı KEPHS (G-KEPHS), gönderici tarafından gönderilen orijinal iletiyi güvenli elektronik imza doğrulama, format kontrolü, varsa virüs tarama gibi kontrollerden geçirir.
3. İkinci adımdaki kontroller sonucunda G-KEPHS aykırı bir durum tespit;

   3.1. Etmemesi halinde orijinal iletinin gönderiminin kabul edildiğine dair SAR (SAR:Acceptance) delilini üretip, KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak göndericiye gönderir.

3.2. Etmesi halinde olumsuz SAR (SAR:Rejection) delilini üretip KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak göndericiye gönderir ve süreci sonlandırır.

4. G-KEPHS, orijinal iletiyi zarflayarak bir KEP paketinin ekine koyar ve bu KEP paketini imzalayarak alıcının hizmet aldığı KEPHS (A-KEPHS)'ye gönderir.
5. A-KEPHS kendisine gelen KEP paketini imza doğrulama, format kontrolü, alıcıların kontrolü, varsa virüs tarama gibi kontrollerden geçirir.
6. A-KEPHS, beşinci adımdaki kontroller sonucu herhangi bir uygunsuzluk tespit etmemiş ise olumlu RRAR (RRAR:Acceptance) delilini üretip bir KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak G-KEPHS aracılığıyla göndericiye gönderir. Beşinci adımdaki kontroller sonucu bir uygunsuzluk tespit etmiş ise olumsuz RRAR (RRAR:Rejection) delilini üretip bir KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak G-KEPHS aracılığıyla göndericiye gönderir ve süreci sonlandırır.
7. G-KEPHS, göndericiye ulaştırılmak üzere iletilen ve ekinde RRAR delilini içeren KEP iletisi üzerinde gerekli kontrolleri gerçekleştirir ve KEP iletisi ekindeki delili alıcıya ilişkin bir depolama alanına sonradan erişmek üzere yazar. G-KEPHS bu işlemlerin tamamlanmasından sonra ilgili KEP iletisini göndericiye iletir.
8. A-KEPHS kendisine gelen KEP paketini ilgili alıcı veya alıcılarına teslim etmeye çalışır. A-KEPHS'nin KEP paketini teslim etmesi veya alıcının olmaması gibi kalıcı bir nedenden dolayı edememesi halinde bir sonraki adıma geçilir. A-KEPHS KEP paketini geçici bir süre için teslim edememesi durumunda teslim etme işlemini, 24 saat boyunca en az 6 saat aralıklarla tekrar dener. Bu süre sonunda hala teslim edilemiyorsa bir sonraki adıma geçilir.
9. A-KEPHS KEP paketini alıcısına teslim ettiyse olumlu DNDR (DNDR:Delivery) delilini, teslim edemediyse olumsuz DNDR (DNDR:DeliveryExpiration) delilini üreterek bir KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak G-KEPHS aracılığıyla göndericiye gönderir.
10. G-KEPHS, göndericiye ulaştırılmak üzere iletilen ve ekinde DNDR delilini içeren KEP iletisi üzerinde gerekli kontrolleri gerçekleştirir ve KEP iletisi ekindeki delili alıcıya ilişkin bir depolama alanına sonradan erişmek üzere

yazar. G-KEPHS bu işlemlerin tamamlanmasından sonra ilgili KEP iletisini göndericiye iletir.

11. Alıcı posta kutusuna erişerek KEP paketine erişir ve okur.
12. A-KEPHS alıcının KEP paketine erişmesi veya okuması ile birlikte RNRR, ertesi iş günü sonuna kadar erişmemesi veya okumaması ile birlikte ise zamanaşımı RNRR (RetrievalExpiration) delilini üreterek bir KEP iletisinin ekine koyar ve bu KEP iletisini imzalayarak G-KEPHS aracılığıyla göndericiye gönderir.
13. G-KEPHS, göndericiye ulaştırılmak üzere iletilen ve ekinde RNRR delilini içeren KEP iletisi üzerinde gerekli kontrolleri gerçekleştirir ve KEP iletisi ekindeki delili alıcıya ilişkin bir depolama alanına sonradan erişmek üzere yazar. G-KEPHS bu işlemlerin tamamlanmasından sonra ilgili KEP iletisini göndericiye iletir.

KEPHS'lerin; iletileri, göndericiden veya diğer KEPHS'lerden teslim alma, alıcılara veya diğer KEPHS'lere teslim etme ve bu olaylarla bağlantılı delilleri oluşturma aşamaları arasındaki bağları iyi kurmaları büyük öneme haizdir. Özellikle sistemin birkaç noktasında meydana gelen olay ve bu olaylara ilişkin üretilen delillerin birbirlerine bağlı bir şekilde gerçekleştirilmesi gerekmektedir. Önlem alınmayan hatalar taraflar arasındaki adilliği zedeleyecek durumların oluşmasına neden olmaktadır. Bunun en bariz örneği bir iletinin A-KEPHS tarafından alıcısına teslim edilmesi ve DNDR delilinin oluşturulması aşamasıdır. A-KEPHS tarafından iletinin alıcının posta kutusuna teslim edilmesini müteakip DNDR delilinin oluşturulması aşamasına geçilmektedir (Bkz. Şekil 4.2). Ancak bu delilin oluşturulma ve işlem sertifikası ile imzalanma aşamalarında meydana gelebilecek bir hata halinde ileti teslim edilmiş fakat buna ilişkin delil oluşturulamamış olacaktır. KEPHS'nin buna ilişkin uygun bir mekanizma oluşturarak ilgili delilin oluşturulma ve imzalanma sürecinin tamamlanması ile eş zamanlı olarak iletiyi alıcı tarafından erişilebilir kılması ve bu işlemlerden birinde bir hata meydana gelmesi durumunda hatayı ele alacak mekanizmaları tesis etmesi gerekmektedir. KEPHS'nin böyle bir durumda uygun kuyruk (queue) veya tetikleme mekanizmaları yoluyla delillerin oluşturulmaması gibi bir olasılığı ortadan kaldırması gerekmektedir.

Benzer şekilde iletinin G-KEPHS tarafından gönderiminin kabul edilmesi ve buna ilişkin delilin oluşturulması, iletinin KEPHS'ler arasındaki devrinin kabul edilmesi ve buna ilişkin delilin oluşturulması aşamalarında da gerek donanımsal gerekse de yazılımsal olarak uygun yöntemlerin gerektiği değerlendirilmektedir.

4.2.8 Hesapların KEPHS'ler arası taşınabilirliği

KEP Hesap Adresleri Tebliği ile KEP hesaplarının alan adı tarafında KEPHS isminin doğrudan yer almaması şeklinde bir yaklaşım benimsenmiştir. Bahse konu Tebliğ'e göre tüm hesap adreslerinin alan adı tarafı "hsY.kep.tr" şeklindedir. Alan adında bulunan "hs" KEPHS'yi ifade etmek üzere kullanılan bir kısaltma ve "Y" ise, KEPHS'nin yetkilendirilme tarihine göre BTK tarafından belirlenen ve sadece KEP hizmetlerinde kullanılacak alan adında yer almak üzere KEPHS'ye verilen 01-99 arasında bir sayıdır (T.C. Resmi Gazete, 2012a). KEP hesaplarının KEPHS'ler arası taşınması söz konusu olduğunda taşınan adres içerisinde KEPHS'nin isminin geçmiyor oluşu sistemde oluşabilecek yanlış algılamaların önüne geçebilmek adına oldukça isbetli olmuştur.

Hesapların KEPHS'ler arası taşıma işleminin gerçekleştirilebilmesi için iletilerin KEPHS'ler arası yönlendirilmesi yönteminin değiştirilmesini gerektirmektedir. Hâlihazırda iletilerin doğru adrese gönderilebilmesini teminen DNS yapısı kullanılmaktadır. Ancak bir hesabın alan adı kendisine ait olmayan başka bir KEPHS'ye taşınması durumunda bu yapı çalışamayacaktır. Bu sebeple iletinin doğru adrese yönlendirilebilmesini teminen merkezi bir yapıda "Hesap Taşıma Sistemi" kurulması gerekmektedir. Bu sistemde temelde hangi hesabın hangi KEPHS'de bulunduğuna ilişkin bilgi yer alacaktır. Sistemin etkin bir şekilde kullanılabilmesi için bu sistemin bir yedek kopyasının güncel bir şekilde tüm KEPHS'lerin yerel sistemlerinde de bulunması gerekmektedir.

Diğer taraftan taşınan hesaplara ilişkin kayıt ve delillerin taşınıp taşınmayacağına, taşınacaksa bu işlemlerin ne şekilde gerçekleştirileceğine, "Hesap Taşıma

Sistemi"'nin nasıl kurulacağına ve işletileceğine, taşıma başvuru ve işlemlerinin gerçekleştirilme detaylarına ilişkin detaylı düzenlemeler yapılması gerekmektedir.

4.2.9 Sonlanma ve zaman aşımı süreleri

KEP sisteminde güçlü adilliği tesis etmek üzere Bölüm 2.3.1.3'te de bahsedilen sonlanma ve zaman aşımı sürelerinin tanımlanması gereklidir. Herbir delilin, özellikle zamanaşımı delillerinin, üretilmesi aşamasında tanımlanacak süreler önem kazanmaktadır. Bu sebeplerle Türkiye'deki KEP sisteminde mesajlaşmanın taraflarının belirsiz süre beklemesinin önüne geçilebilmesi için bazı noktalarda zamanaşımı sürelerinin tanımlanması gereklidir.

Türkiye'deki KEP sistemi için BTK (2014)'da;

- Alıcı KEPHS'ye belirli bir süre sonunda teslim edilemedi (RRF),
- Alıcıya belirli bir süre içinde teslim edilemedi (DNDR:DeliveryExpiration),
- Alıcı tarafından okundu kabul edildi (RNRR:RetrievalExpiration),
- Alıcı tarafından indirildi kabul edildi (DLNDLR:DownloadExpiration)

delilleri üretilmeden önce bazı zaman aşımı ve bekleme süreleri tanımlanmıştır. Bu düzenleme ile tanımlanan zaman aşımı ve bekleme süreleri aşağıdaki şekildedir (BTK, 2014).

- G-KEPHS, KEP paketini alıcıya iletilmek üzere A-KEPHS'ye gönderdikten sonra olumlu veya olumsuz RRAR delili beklemektedir. Bu delil G-KEPHS tarafından alınamazsa veya A-KEPHS'ye KEP paketi hiç ulaştırılamıyor ise gönderim asgari altı saatlik periyotlarla en az 4 kere daha dener ve bu gönderimlerin de başarısız olması durumunda RRF delili üretir.
- A-KEPHS KEP paketininin alıcıya geçici bir sebeple teslimini gerçekleştiremiyorsa, bu paketin teslimini yine asgari altı saatlik periyotlarla en az 4 kere daha dener ve bu süre sonunda hala teslim edemiyorsa DNDR:DeliveryExpiration delilini üretir. Dolayısıyla G-KEPHS RRAR

delilini aldığı bir KEP paketi için en fazla 24 saat DNDR delilinin gönderilmesini bekler ve 25'inci saatte kendisi paketin teslim edilemediğine ilişkin DNDR:DeliveryExpiration delilini üretir. Böylece G-KEPHS ve göndericinin belirli bir süre sonunda tüm delilleri elde etmesi sağlanmaktadır.

- RNRR:RetrievalExpiration ve DLNDLR:DownloadExpiration delilerinin, Yönetmeliğin 12'nci maddesinde yer alan "Mücbir sebep hâlleri dışında KEP hesabına erişilmemesi durumunda o işgünü içinde gelen iletinin ertesi işgünü hesap sahibine ulaştığı ve okunduğu kabul edilir." hükmü uyarınca, KEP paketinin alıcının posta kutusuna teslimini izleyen iş günü sonunda 23:59'da toplu olarak üretilmesi öngörülmüştür.

[redacted]

[redacted]

4.3 Güvenlik Yaklaşımları

KEP kullanıcıları özellikle KEPHS tarafından sunulan delillerin doğru ve güvenilir bir şekilde oluşturulduğundan ve saklandığından emin olabilmelidir. KEPHS'nin bu güveni sağlayabilmesi ise iş süreçlerinin uygun bir şekilde yönetilebilmesine bağlıdır. Bu sebeple KEPHS'lerin yönetim sistemlerini kurup, belirlenen standartlar bağlamında yönetebilmeleri önem arz etmektedir (ETSI, 2011c).

KEPHS'nin sahip olduğu bilgi sistemleri ve ağ hizmetleri bilgisayar destekli dolandırıcılık, casusluk, sabotaj, terör, delillerin yetkisiz değiştirilmesi, personelin kötüye kullanımları da dâhil olmak üzere geniş bir kaynak yelpazesinden genel

güvenlik tehditleri ile karşı karşıyadır. KEPHS'nin içinden olabileceği gibi dışarıdan da olabilecek bu tehditlerin bir kere bile gerçekleşmesi ve bir bilgi güvenliği ihlalinin yaşanması, tüm sisteme duyulan güvene zarar verecektir (ETSI, 2011c).

KEP Yönetmeliği'nin 16'ncı maddesi ile KEPHS; vermiş olduğu hizmetlerin güvenliğini, gizliliğini ve bütünlüğünü sağlamakla yükümlü kılınmıştır. Mevzuat ile belirlenen standartlar kapsamında KEPHS'ler ilk olarak ISO/IEC 27001'de belirtildiği gibi dokümante edilmiş bir BGYS'yi KEP hizmetleri bağlamında karşılaştığı tüm riskleri içerecek şekilde kurmalı, gerçekleştirmeli, işletmeli, izlemeli, gözden geçirmeli ve geliştirmelidir. Diğer taraftan BGYS'nin kurulması ve işletilmesi ile beraber bahse konu standardın Ek-A'sında yer alan;

- Bilgi güvenliği politikaları,
- Bilgi güvenliği organizasyonu,
- İnsan kaynakları güvenliği,
- Varlık yönetimi,
- Erişim kontrolü,
- Kriptografi,
- Fiziksel ve çevresel güvenlik,
- İşletim güvenliği,
- Haberleşme güvenliği,
- Sistem temini, geliştirme ve bakımı,
- Tedarikçi ilişkileri,
- Bilgi güvenliği ihlal olayı yönetimi,
- İş sürekliliği yönetiminin bilgi güvenliği hususları,
- Uyum

kontrol maddelerine uygun bir yapı oluşturulması gerekmektedir (ISO/IEC, 2013).

Bu kontrollerden bir kısmı ETSI (2011c) standardında da zorunlu olarak tanımlanmış ve ISO/IEC 27001 standardının uygulama dokümanı olarak yayımlanan ISO/IEC 27002 (ISO/IEC, 2005) dokümanına da atıflar yapılmıştır.

BİT hizmetlerinin iş sürekliliğinin sağlanması için bazı kavram ve prensipler ortaya koyan ISO/IEC 27031'de Teknik Kriterler Tebliğ'i ile uyulması zorunlu olarak belirlenen diğer bir standarttır (ISO/IEC, 2011). Bu zorunluluk gereği KEPHS'lerin ISO/IEC (2011) standardında kurulması öngörülen iş sürekliliği yönetim sistemini (ISYS) kurmaları ve işletmeleri gerekmektedir.

Teknik Kriterler Tebliğ'i ile uyulması zorunlu olarak belirlenen diğer standart ise etkin bir kişisel veri yönetimi için bir plan oluşturulmasını, bu verilerin depolanması ve korunmasını iyileştirmek ile ilgili süreçleri belirleyen BS10012 (BS, 2009)'dir. Bu standart uyarınca KEPHS'lerin bir kişisel bilgi yönetim sistemini (KBYS) kurmaları ve gerçekleştirmeleri gerekmektedir.

4.4 Kayıtlı Elektronik Posta Hizmet Sağlayıcıları

KEP hizmeti, TTP olarak kabul edilen KEPHS tarafından verilen bir hizmettir. Tüm KEP ileti ve delillerinin KEPHS tarafından oluşturulduğu ve hesap sahiplerine iletildiği göz önüne alındığında, KEPHS'nin sistemin en önemli bileşeni olduğu söylenebilecektir.

KEP Yönetmeliği'nde KEPHS,

> 13/01/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu kapsamındaki yetkilendirme çerçevesinde elektronik iletişim platformları aracılığıyla gerçekleşen, gönderildi ve alındı onayları da dâhil olmak üzere KEP iletilerinin tüm süreçlerine ilişkin KEP delili oluşturulması, güvenli bir şekilde kimlik tespiti yapılması, KEP hesabı, KEP rehberi ve arşiv hizmetleri verilmesi gibi işlevlere sahip KEP sistemini kurmak ve işletmek için kurulan anonim şirket ile başvuru yapması ve gerekli koşulları sağlaması hâlinde 11/02/1959 tarihli ve 7201 sayılı Tebligat Kanununun hükümlerine göre elektronik ortamda tebligat yapmaya yetkili kılınmış idare

olarak tanımlanmıştır. Bu tanımdan da anlaşılabileceği üzere, KEPHS olmanın temel şartı KEP sistemini kurmak ve işletmek amaçlarına özgülenmiş bir anonim şirket olunmasıdır. Diğer taraftan yine aynı Yönetmeliğin 6'ncı maddesinin dördüncü fıkrasında yer alan;

> ESHS olarak veya 05/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında işletmeci olarak faaliyet gösterenler KEPHS olmak için başvuruda bulunamaz.

hükmü ile de hizmeti verebilecek şirketlere ilişkin bir kısıtlama getirilmiştir.

KEPHS olmak amacı güden anonim şirketlerin, KEP Yönetmeliği'nin 6'ncı, 7'nci ve 8'inci maddelerinde belirlenen usule göre KEPHS olma talebini içeren dilekçeyi ve Yönetmelik Ek'inde yer verilen bilgi ve belgeleri eksiksiz olarak BTK'ya sunması gerekmektedir. BTK, öncelikle kendisine sunulan bilgi ve belgeler üzerinden bu başvuruyu değerlendirmeye almak zorundadır. Bu değerlendirmenin sağlıklı, nitelikli ve objektif bir şekilde yapılabilmesi için bir kontrol listesine ihtiyaç duyulmaktadır.

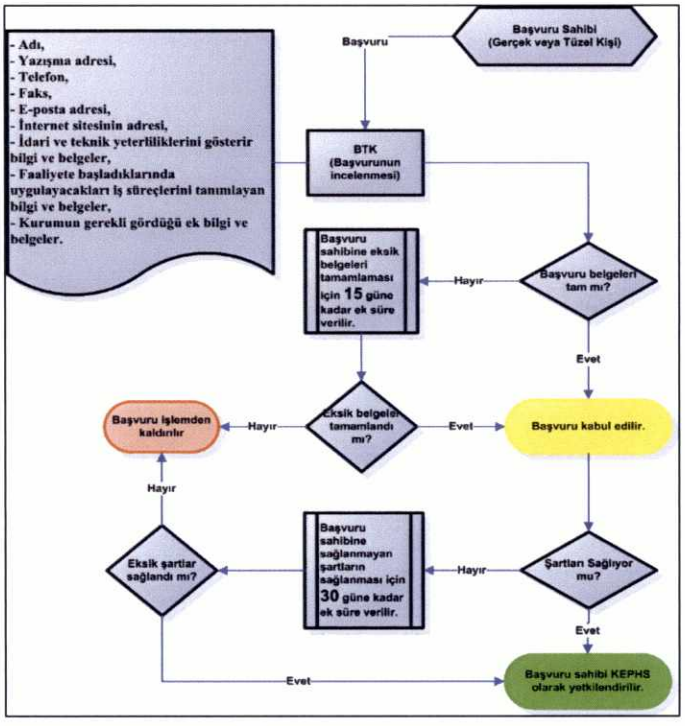
Yapılan değerlendirme sonucunda herhangi bir eksiklik tespit edilmezse başvuru derhal incelemeye alınır. Ancak bahse konu başvuruda herhangi bir eksiklik tespit edilirse bu eksikliklerin tamamlanabilmesi için BTK tarafından ilgili tarafa süre verilir ve tespit edilen bu eksikliklerin giderilmesi hâlinde başvuru kabul edilir.

BTK tarafından kabul edilen başvuru incelemeye alınır ve inceleme iki ay içinde sonuçlandırılır. Bu iki aylık süre içerisinde BTK tarafından hem sunulan bilgi ve belgeler üzerinden hem de ilgili tarafın idari ve teknik merkezlerinde oluşturulan altyapının mevzuat ile belirlenen standartlara uygun olup olmadığına ilişkin inceleme yapılır. Yapılan inceleme sonucunda belirlenen hususları eksiksiz olarak yerine getirdiği belirlenen başvuru sahipleri KEPHS olarak yetkilendirilir. Ancak yapılan inceleme sonucunda başvuruda istenen bilgi ve belgelerde yer alan hususlardan bir veya birkaçının eksikliği veya yerine getirilmediği tespit edilirse, durum gerekçeleriyle birlikte başvuru sahibine bildirilir ve bu eksikliklerin giderilmesi için bir ay süre verilir. Bu sürenin sonunda belirlenen eksiklikleri giderdiği belirlenen

başvuru sahibi BTK tarafından KEPHS olarak yetkilendirilirken, bu sürenin sonunda BTK tarafından belirlenen eksiklikleri gidermeyen başvuru sahibinin başvurusu yine BTK tarafından işlemden kaldırılır (Bkz. Şekil 4.3).

Mevzuata göre BTK bu sürecin her aşamasında başvuruyu işlemden kaldırmaya yetkilidir. Başvuru sahibi de işlemden kaldırılan başvuruya ilişkin eksiklikleri tamamlayarak tekrar KEPHS olma başvurusunda bulunabilir. Bununla birlikte KEPHS faaliyetinin devamı sırasında yapmış olduğu bildirimde meydana gelen değişiklikleri BTK'ya bildirmek zorundadır.

Şekil 4.3. Başvuru ve KEPHS olarak faaliyete başlama



KEP mevzuatına göre BTK'ya KEPHS olma başvurusunda bulunan bir başvuru sahibi asgari iki ay azami üçbuçuk ay içerisinde KEPHS olarak yetkilendirilir. Aksi takdirde başvuru BTK tarafından işlemden kaldırılır. Bu süreç çerçevesinde BTK tarafından yetkilendirilen ve hâlihazırda faaliyetleri devam eden KEPHS'lere ilişkin bilgiler Tablo 4.6 'da yer almaktadır.

Tablo 4.6. Türkiye'de yetkilendirilen KEPHS'ler

Hizmet Sağlayıcı	Alan Adları	Başvuru Tarihi	Yetkilendirmenin Geçerlilik Tarihi
Posta ve Telgraf Teşkilatı A.Ş. (PTT)	hs01.kep.tr	03/05/2012	10/09/2012
TNB Kayıtlı Elektronik Posta Hizmet Sağlayıcılığı ve Ticaret A.Ş.	hs02.kep.tr	28/09/2012	28/12/2012
TÜRKKEP Kayıtlı Elektronik Posta Hizmet Sağlayıcılığı ve Ticaret A.Ş.	hs03.kep.tr	28/11/2012	25/02/2013
İntertech Bilgi İşlem ve Pazarlama Ticaret A.Ş.	hs04.kep.tr	02/07/2014	14/11/2014
efinans Elektronik Ticaret ve Bilişim Hizmetleri A.Ş.	hs05.kep.tr	29/09/2014	05/02/2015

Kaynak:http://www.btk.gov.tr/bilgi_teknolojileri/kayitli_elektronik_posta/kephs.php

Gerek KEP Yönetmeliği gerekse Teknik Kriter Tebliği ile uyulması zorunlu olarak belirlenmiş ETSI (2011a; 2011d)'de KEPHS'nin bir takım işlevleri tanımlanmıştır.

KEP Yönetmeliği'nde KEPHS'nin yerine getirmesi zorunlu ve isteğe bağlı işlevleri belirlenmiştir. KEPHS'nin zorunlu işlevleri, KEP hesabı açmak ve iptal etmek, hesap sahibi ve BTK'ya karşı bilgilendirmede bulunmak, hesap sahibinin güvenli bir şekilde ileti gönderebilmesi için güvenli teknoloji ve sistemler sunmak, KEP rehberi hizmetini vermek, KEP hesabı için posta kutusu ve gönderi hizmetleri sağlamak ve bu kapsamda gönderilecek iletilere ilişkin süreçleri güvenli elektronik imza ve zaman damgası ile kayıt altına alıp delil oluşturmaktır. İsteğe bağlı işlevleri ise, kimlik doğrulaması ve arşiv hizmetleridir (Keser Berber, 2013).

ETSI (2011a; 2011d)'de ise KEPHS'nin yerine getirmesi zorunlu ve isteğe bağlı işlevler listelenmiştir (Bkz. Şekil 4.4). Buna göre MTA, MS ve delil oluşturma hizmetlerini vermek KEPHS'nin yerine getirmesi gereken zorunlu işlevleri, delil doğrulama, mesaj geçit, mesaj arşiv ve veri deposu hizmetleri isteğe bağlı işlevler olarak tanımlanmaktadır. Ayrıca imza oluşturma ve uzun dönemli saklama hizmetleri başka üçüncü taraflardan sağlanabilecek hizmetler olarak sayılırken, sertifika ve

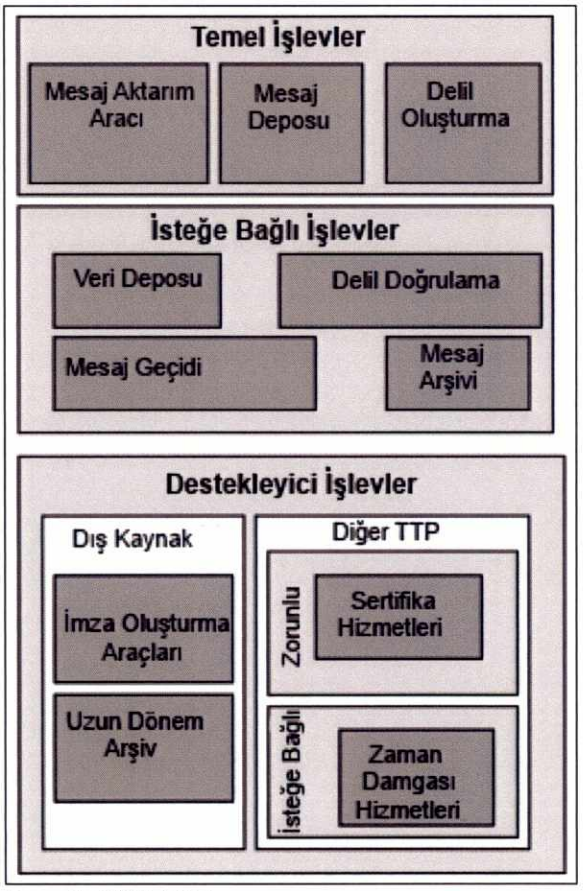
zaman damgası hizmetleri başka TTP'lerden (ESHS'lerden) alınması gerekli olan hizmetler olarak tanımlanmıştır.

Diğer taraftan ETSI (2011a; 2011d)'de isteğe bağlı olarak tanımlanan zaman damgası kullanımı KEP Yönetmeliği ile zorunlu hale getirilmiştir.

Ayrıca KEPHS, KEP Yönetmeliği'nin 14'üncü maddesine göre;

> KEP sistemi içerisinde bir elektronik iletinin gönderilmesi ve alınması dışında elektronik belgelerin saklanması, güvenli iletişim ve elektronik ortamda güvenilir üçüncü taraf hizmetleri gibi katma değerli hizmetler sunabilir.

Şekil 4.4. KEPHS zorunlu ve isteğe bağlı işlevleri



Kaynak: ETSI, 2011

4.5 Mevcut Pazarın Durumu ve Öngörüler

Ülkemizde ilk KEPHS Eylül 2012'de yetkilendirilmiştir. Dolayısıyla ilk KEP hesapları 2013 yılından itibaren verilmeye başlamıştır. 2013 yılında 5.572 bireysel, 6.882 kurumsal olmak üzere toplam 12.454 KEP hesabı oluşturulmuştur (BTK, 2015a). 2014 yılına gelindiğinde oluşturulan KEP hesabı sayısının yaklaşık 90 bine ulaştığı ve bu sayının 13.255'inin bireysel, 3519'unun Kamu Kurum ve Kuruluşlarına, 65.588 özel tüzel kişilere ait hesaplardan oluştuğu görülmektedir (Bkz. Ek-3). Oluşturulan KEP hesaplarının büyük bir kısmının tebligata elverişli olarak açılması nedeniyle KEP hesaplarının büyük oranda tebligat alma amacıyla kullanılacağı anlaşılmaktadır.

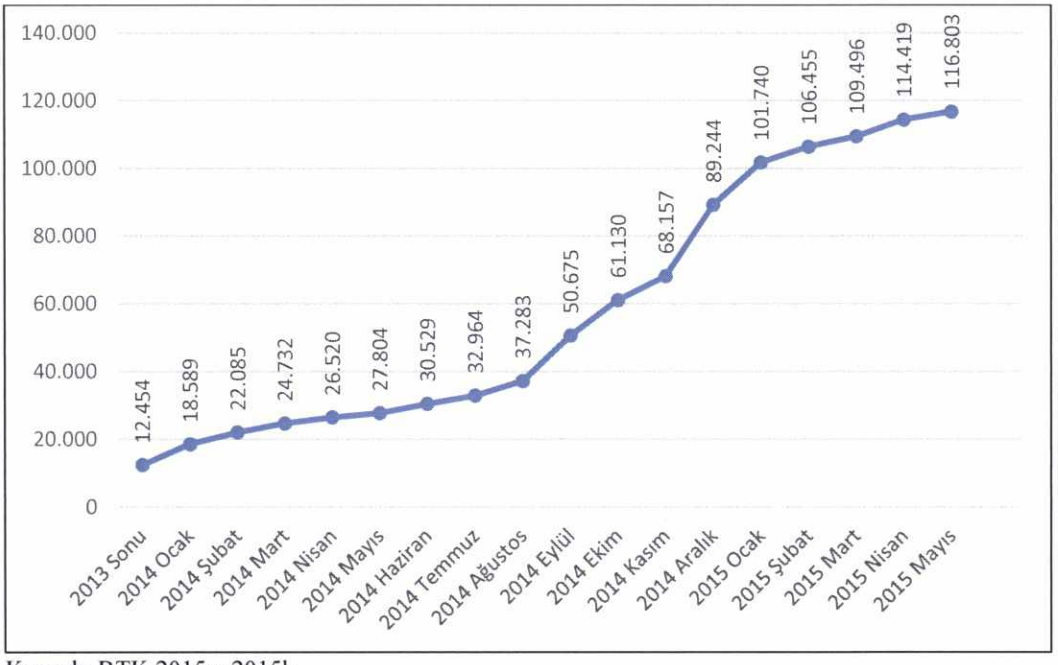
2015 yılının Mayıs ayı itibariyle KEP hesabı sayısının 116.803 olarak gerçekleştiği (Bkz. Ek-4), 2014 yılı ile kıyaslandığında artış eğiliminin devam ettiği ve tebligat amacıyla kullanım oranının değişmediği görülmektedir. Her ne kadar Kamu Kurum ve Kuruluşları yaptıkları tebligatları elektronik ortamda yapabilir hale gelemeseler de elektronik tebligata ilişkin KEP hesabı alma zorunluluğu nedeniyle şirketlerin KEP hesabı edindikleri anlaşılmaktadır.

Gerek tezin üçüncü bölümde yer verilen dünya uygulamalarından gerekse de bu bölüm içerisinde yer verilen değerlendirmelerden anlaşılacağı üzere sistemin gelişmesi ve kullanımının yaygınlaşması kamu kurum ve kuruluşlarının kullanımına bağlıdır. Hatta sistemi uygulayan ülkelerin, sistemi başlangıçta devlet-vatandaş ve devlet-özel sektör arasındaki iletişimi kolaylaştırmak bağlamında ele aldıkları, uygulamanın yaygın olarak kullanıldığı İtalya örneğinde, getirilen kanuni zorunluluklar ve kamu otoritelerinin uygulamayı kullanmaya başlaması ile birlikte hesap ve gönderilen ileti sayılarının arttığı ifade edilmektedir (Buzzi vd., 2014).

Türkiye'de de elektronik tebligat ile birlikte bir zorunluluk getirilmiş olmasına karşın henüz kapsamlı bir uygulamanın başlatılamamış olması ve getirilen zorunluluğun uygulanmamasına yönelik bir yaptırım öngörülmemiş olması sonucunda kullanımın yaygınlaşamadığı değerlendirilmektedir.

Türkiye'deki KEP hesap sayılarının artış grafiklerine bakıldığında en önemli artışların yaşandığı ayların 2014'ün Eylül ve Aralık ayları olduğu görülmektedir (Bkz. Şekil 4.5). Bu artışların nedeni, İstanbul Gümrük ve Ticaret Bölge Müdürlüğü'nün, müşavirliklere veya firmalara yapılacak tebligatları elektronik ortamda gönderilebilmesi için muhatap müşavirlik veya firmaların KEP adresine ihtiyaç duyması ve KEP adreslerinin İstanbul Gümrük ve Ticaret Bölge Müdürlüğü Evrak Kayıt Servisi'ne yazılı dilekçe ile 30 Eylül 2014 tarihine kadar bildirmesini istemesi, daha sonra bu sürenin 31 Aralık 2014 tarihine kadar uzatılmasıdır (GMD, 2014). Sadece bir Gümrük ve Ticaret Bölge Müdürlüğü'nün kullanıma başlayacağını duyurması ve buna ilişkin bir bildirim yapmasının sektörü olumlu yönde etkilediği bu örnekte açıkça görülmektedir.

Şekil 4.5. Toplam KEP hesap sayıları artış grafiği



Kaynak: BTK 2015a; 2015b

Halihazırda KEP kullanan kurum ve uygulamaların profilinden hareketle önümüzdeki yıllarda kamu kurumlarının elektronik tebligat gönderimine başlayacağı, elektronik yazışma uygulamalarının hayata geçeceği, özellikle finans sektöründe iş ve işlemleri

kolaylaştırıcı uygulamaların hayata geçirileceği, KEPHS'lerin katma değerli KEP hizmetleriyle müşterilerinde derinleşme sağlayacağı ve kurumlarda insan kaynakları ve iş paydaşları ile iletişim içeren uygulamaların artacağı ve böylelikle KEP kullanımının yaygınlaşacağı değerlendirilmektedir (Bkz. Tablo 4.7). Bununla birlikte ülkemizde KEP kullanımının yaygınlaştırılabilmesi için bazı kanun hükümlerinde değişikliklerin yapılması gerekmektedir. Bu kapsamda 2004 sayılı İcra İflas Kanunu'nun 68/b maddesinde;

> Borçlu cari hesap veya kısa, orta, uzun vadeli kredi şeklinde işleyen kredilerde krediyi kullandıran taraf, krediyi kullanan tarafın kredi sözleşmesinde belirttiği adresine, borçlu cari hesap sözleşmesinde belirtilen dönemleri veya kısa, orta, uzun vadeli kredi sözleşmelerinde yazılı faiz tahakkuk dönemlerini takip eden onbeş gün içinde bir hesap özetini noter aracılığı ile göndermek zorundadır

hükmü bulunmaktadır. Sözkonusu maddede anılan "hesap özetinin" sadece "noter aracılığı ile" gönderilebileceği belirlendiğinden bu kapsamda KEP ile gönderim yapılamamaktadır. Bu işlemlerin KEP ile yapılması halinde KEP sistemi ve uygulamalarının hızlıca yaygınlaşmasına ve yoğun kullanımına çok önemli katkı yapacağı değerlendirilmektedir. Bu kapsamda İcra İflas Kanunu 68/b maddesinde "...noter aracılığıyla ***veya kayıtlı elektronik posta ile***..." şeklinde değişiklik yapılması ve maddenin bu değişikliğe göre güncellenmesi gerekmekdir. Aynı Kanun'un 150/ı, 240, **269/c ve 309/o** maddelerinde benzer değişiklikler yapılmalıdır.

Tablo 4.7. KEP kullanan kurum ve uygulamalar

Kurum/Uygulama	**Yıl (Uygulamanın Başladığı Yıl/Ay)**
E-tebligat	Ocak 2013
E-yazışma	Mart 2014
Belediyeler	Şubat 2014
Üniversiteler	Nisan 2014
Finans	Nisan 2014

Kaynak: BTK, 2015a

Benzer şekilde 4857 saylı İş Kanunu'nun 109'uncu maddesinde yapılacak "*Bu Kanunda öngörülen bildirimlerin ilgiliye yazılı olarak imza karşılığında* ***veya kayıtlı elektronik posta ile*** *yapılması...*" şeklindeki bir değişiklik ile bordro ve izin formu gibi İş Kanunu kapsamında çalışanlara yapılacak tüm bildirimlerin KEP ile yapılması sağlanmış olacaktır.

6098 sayılı Türk Borçlar Kanunu'nun 241'inci maddesinde "*Satıcı veya alıcı, satış sözleşmesinin yapıldığını ve içeriğini önalım hakkı sahibine noter aracılığıyla* ***veya kayıtlı elektronik posta ile*** *bildirmek zorundadır.*" şeklinde, 6570 sayılı Gayrimenkul Kiraları Hakkında Kanun'un 7'nci maddesinin (a) fıkrasında "...yazı **veya kayıtlı elektronik posta** ile bildirilmiş...".ve (e) fıkrasında "iki defa yazılı **veya kayıtlı elektronik posta ile** ihtar yapılan" şeklinde yapılacak değişikliklerin KEP kullanımının yaygınlaştırılmasına önemli katkıları sağlayacaktır.

4.6 KEPHS'ler Arası Birlikte Çalışabilirlik

KEPHS'ler arası KEP iletileri ve KEP paketlerinin gönderilip alınabilmesi, gönderilip alınan ileti ve paket eklerinde yer alan delil ve orijinal iletilerin doğru ve güvenilir biçimde yorumlanabilmesini kapsayan birlikte çalışabilirlik sistemin işleyişi açısından çok önemli ve karmaşık bir konu olarak karşımıza çıkmaktadır.

KEPHS'ler faaliyete başladıklarında altyapılarını mevzuatla belirlenen standartlara uygun olarak oluşturmalarına rağmen standartların ihtiyari bıraktığı bazı alanların farklı kullanılması nedeniyle birlikte çalışabilirliğin sağlanmasında teknik ve idari sorunların yaşanması kaçınılmaz hale gelmektedir.

Sistemin düzgün çalışması ve sürdürülebilir olması, KEPHS'ler arası birlikte çalışabilirliğin hem mevcut KEPHS'ler hem de yeni yetkilendirilecek KEPHS'ler için sağlanmasıyla mümkün olacaktır. Bunun sağlanabilmesi ve devam ettirilebilmesi için bir takım testlerin gerek yetkilendirme denetimlerinde gerekse de periyodik yapılan denetimlerde gerçekleştirilmesi gerekmektedir.

Önceki bölümlerde anlatılan İtalya ve Almanya uygulamalarında birlikte çalışabilirliğin sağlanması ve sürdürülebilmesi amacıyla ciddi çalışmalar yapılmaktadır. Örneğin İtalya'da hizmet sağlayıcıları arasında birlikte çalışabilirlik sorunlarını en aza indirmek ve birlikte çalışabilirlik eksikliğinden kaynaklanan potansiyel riskleri azaltmak amacıyla AGID tarafından bazı kontroller gerçekleştirilmektedir. Bu bağlamda hizmetlerin sürekli ve doğru çalışmasının sağlanması ve hizmet sağlayıcıların mevzuatta belirlenen hizmet kalitesine ve zorunluluklara uygunluğunun test edilmesi amacıyla 228 adet test geliştirilmiştir ve bu testler uygulanmaktadır (Buzzi vd., 2014).

Diğer taraftan Almanya ve İtalya örneklerinde de olduğu gibi sistemlerin çalışmasını izlemek, birlikte çalışabilirliği test etmek ve teknik gelişimine dair çalışmak üzere sistemin paydaşlarının yer aldığı bir çalışma grubu faaliyet göstermektedir. Bu çalışma grubunun kurulmasının gerek sistemin işleyişini izlemek gerekse ihtiyaç bulunan teknik ve idari yeni gereksinimlerin belirlenip hayata geçirilmesi bağlamında önemli bir fonksiyonu icra edeceği değerlendirilmektedir.

KEPHS'ler arası birlikte çalışabilirlik; bağlantı katmanı, KEP delilleri, KEP iletileri ve KEP paketlerinin zarf yapıları, elektronik imzalar, ileti akışı ve sistemin işleyişi, rehber yapısı ve işleyişi olmak üzere temelde altı unsura dayanmaktadır.

Birlikte çalışabilirliğe ilişkin ilk unsur KEPHS'ler arası güvenli ve güvenilir bir bağlantının kurulmasıdır. Bu hususa 4.2.4'üncü bölümde detaylarıyla ele alınmaktadır.

KEP delilleri de birlikte çalışabilirliğe ilişkin önemli bir unsur olarak karşımıza çıkmaktadır. Delillerde bulunması gerekli olan ve 4.2.2'de detayları verilen alanların doğru zamanda ve şekilde oluşturulup oluşturulmadığı hususlarının test edilmesi gerekmektedir. ETSI (2011f)'de delillerin doğru bir şekilde oluşturulup oluşturulmadığına ve oluşan delillerin üzerlerindeki alanlara ilişkin hangi testlerin yapılması gerektiği belirtilmektedir. Örneğin "Gönderici KEPHS tarafından kabul edildi (SAR)" delilinin doğru bir şekilde oluşturulup oluşturulmadığını test etmek için altı farklı test senaryosunun oluşturulması gerekmektedir (ETSI, 2011f).

KEP iletileri ve KEP paketlerinin SMTP protokolü ve mevzuatta yer verilen yapıya uygun oluşturulması birlikte çalışabilirliğin diğer bir unsurunu oluşturmaktadır. Bu hususa yönelik olarak paket içerikleri ve başlık bilgilerinin doğru ve eksiksiz bir biçimde oluşturulması ve kullanılması önem arz etmektedir. Bir KEP paketi veya iletisi A-KEPHS tarafından alındığında KEPHS tarafından oluşturulan zarflar üzerinden otomatik işlemeye tabi tutulduğundan bu veriler sistemin doğru çalışabilmesi için önemlidir.

Birlikte çalışabilirlik açısından sistemin diğer önemli unsurlarından olan ektronik imzalara, ileti akışına, sistemin işleyişine ve rehber sorgularına ilişkin hususlar tezin önceki bölümlerinde ele alınmıştır.

4.7 Kayıtlı Elektronik Posta Hizmet Sağlayıcıların Denetimi

6102 sayılı TTK'nın 1525'inci maddesinin ikinci fıkrasında yer alan KEPHS'lerin denetlenmelerine ilişkin usul ve esasların BTK tarafından bir yönetmelik ile düzenleneceğine ilişkin hüküm çerçevesinde KEP Yönetmeliği'nin 21'inci, 26'ncı ve 27'nci maddelerinde BTK'nın, KEPHS'lerin Yönetmelik ile belirlenen şartlara uygun hizmet verip vermediğini re'sen veya şikâyet üzerine Elektronik Haberleşme Kanunu'nun 6'ncı ve 59'uncu maddelerine dayanılarak hazırlanan Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Usul ve Esaslar Hakkında Yönetmelik uyarınca denetleyebileceği veya denetletebileceğini hüküm altına alınmıştır. Ayrıca bu maddeler ile Yönetmeliğe ve ilgili mevzuat hükümlerine uygun faaliyette bulunmayan KEPHS'lere Kurum tarafından bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanabileceği veya bunların faaliyetine de son verilebileceği hüküm altına alınmıştır.

Böylece KEPHS'lerin denetiminin nasıl ve ne şekilde gerçekleştirileceği ve gerçekleştirilen denetimler sonucunda uygulanılabilecek idari yaptırımların çerçevesi çizilmiştir.

Söz konusu hükümler uyarınca BTK, KEPHS'lerin denetimi konusunda yetkili kılınmıştır.

Yukarıda yer verilen hükümler çerçevesinde KEPHS'lerin uymaları gereken usül ve esaslara ilişkin bir kanuni düzenlemenin yapılmadığı görülmektedir. KEPHS'lerin uyacakları kurallar, alacakları hukuki ve teknik tedbirlerin neler olduğu ve ne şekilde alınacağı KEP Yönetmeliği, bu Yönetmeliğe dayanılarak çıkarılan tebliğler, BTK tarafından yayımlanan usul esaslar ve Teknik Kriterler Tebliği'nin atıfta bulunduğu standartlardan oluşan KEP mevzuatında belirtilmektedir. Bu düzenlemelerde yer alan hükümler denetim esaslarını, Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Usul ve Esaslar Hakkında Yönetmelik'teki düzenlemeler denetim usullerini teşkil etmektedir.

Denetim usulleri bu tez kapsamında olmamakla birlikte, denetimin esasları genel hatlarıyla bu bölümde ele alınmaya çalışılmıştır. Bu kapsamda KEPHS'lerin KEP mevzuatı yanı sıra Teknik Kriterler Tebliği'nin atıfta bulunduğu ETSI TS 102 640, ISO 27031 ve BS 10012 standartlarına uyma zorunluluğu ve ISO/IEC 27001 standardına uygunluğunu yetkili kurum veya kuruluşlardan alınan belgelerle belgelendirme gerekliliği bulunmaktadır. ISO/IEC 27001 hariç diğer standartlara ilişkin bir belgelendirme kuruluşunun bulunmayışı nedeniyle bu standartlarda zorunlu olarak belirtilen alanların denetim çalışmaları sırasında kontrol edilmesi gerekmektedir. Diğer taraftan her ne kadar KEPHS, ISO/IEC 27001 standardına uygunluğunu belgelendirmiş olsa da bahse konu standartta geçen ve KEPHS'nin işleyişinde önemli rol oynayan bazı hususların aynı zamanda ETSI 102 640 kapsamında da olması nedeniyle bu standardın denetim çalışmaları sırasında dikkate alınmasının gerekli olduğu değerlendirilmektedir.

SONUÇ VE ÖNERİLER

Geleneksel posta geçmişten günümüze belge, mektup, kartpostal, koli veya diğer posta gönderilerini iletmek üzere kullanılmaktadır. Bu tür gönderimlerde, postaların posta hizmet sağlayıcısına teslim edilmesiyle alıcısına teslim edileceği varsayılır. Bu durumda alıcının, göndericiye gönderinin teslimi ile ilgili bir geri dönüş gerçekleştirmesi durumu dışında, gönderici, postanın alıcısına ulaşıp ulaşmadığına dair bilgi sahibi olamamaktadır.

Hassas ve değerli gönderilerin daha yüksek güvenlik ve güvenilirlik seviyesinde taşınmasına ihtiyaç duyulabilmektedir. Özellikle daha yüksek güvenlik, güvenilirlik ve teslim alındığına dair bildirim gerektiren değerli gönderiler söz konusu olduğunda birtakım özel hizmetlerin verilmesi gündeme gelmiştir. Posta hizmet sağlayıcısına bağlı olarak değişmekle birlikte bu servisler kayıtlı posta, kayıtlı gönderi, güvenli gönderim veya taahhütlü posta olarak adlandırılmaktadır.

BİT'in hızla yaygınlaşmasıyla birlikte posta servis sağlayıcılar maliyetleri düşürme, katma değerli hizmetler sunma, kaliteli ve hızlı hizmet verme gibi nedenlerle fiziki ortamda yürütülen iş ve işlemleri elektronik ortamda yapmaya başlamışlardır. Bu kapsamda gönderime ilişkin bir takım süreçlerin elektronik ortama aktarıldığı farklı hizmetler ortaya çıkmış ve bu hizmetler gönderime ilişkin tüm süreçlerin elektronik ortama aktarıldığı KEP'e geçiş aşamasını oluşturmuştur.

Günümüzde insanlar iletişim anlamında geleneksel yöntemleri terk ederek elektronik ortamları tercih eder hale geldiğinden elektronik posta giderek artan oranda kullanılmaya başlanmıştır. Ancak elektronik posta iletişime dair ispat özellikleri açısından zayıf kalmaktadır. Tasarlanan elektronik posta protokollerinde bu zayıflık nedeniyle birçok gönderim ve alım mekanizması geliştirilmiş ve kullanılagelmiştir. Bir elektronik posta sisteminde gizlilik, bütünlük ve güvenilirlik özelliklerini sağlamak üzere iki farklı kısım bulunmaktadır. Bunlardan ilki TLS veya SSL gibi yöntemler kullanılmak suretiyle bağlantının güvenliğini sağlamaya yönelik kısımdır. Diğeri ise S/MIME veya PGP gibi yöntemler ile gönderilen verinin göndericisi ve

alıcısı dışındaki üçüncü kişiler tarafından erişilmesini önlemek amacıyla kullanılan kısımdır.

Standart elektronik postada gizlilik, bütünlük ve kimlik doğrulama gibi temel özellikler kısmen sağlanıyor olsa da gönderinin alıcısına ulaşıp ulaşmadığı veya alıcısı tarafından görülüp görülmediğine ilişkin bir delil sağlanamamaktadır. Bahse konu eksikliğin giderilebilmesi ve alındı kayıtlarının üretilebilmesi amacıyla tezin ikinci bölümünde detaylandırılan MDN, DSN, SMTP servis eklentileri ve S/MIME alındı bildirim mekanizmaları geliştirilmiştir. Bu mekanizmalar iletişime dair bazı kayıtların üretilmesini sağlasa da üretilen bu kayıtların delil olma özelliği bulunmamaktadır (Tauber, 2012). Bahse konu mekanizmaların hiçbirisinde alıcının bu mesajları dikkate alacağı ve üreteceği garanti edilememektedir. Ayrıca gerçekleştirilen bu çözümler birlikte çalışabilir ve güvenilir olmaktan da oldukça uzaktır (Oppliger, 2007).

Geliştirilen tüm bu mekanizmalar elektronik postaya, fiziki kayıtlı posta ile eş değer delil sağlama özelliklerini kazandırmamaktadır. Özellikle kişiler ve kurumlar üzerinde hukuki sonuçlar doğurabilecek mahkeme celpleri, icra takipleri, ödeme emirleri, sözleşmeler gibi gönderiler söz konusu olduğunda gönderime ilişkin inkâr edilemezlik ve diğer güvenlik özelliklerine ihtiyaç duyulmaktadır. Dolayısıyla geleneksel kayıtlı postada var olan güven ve güvenilirliğin elektronik ortamda da bulunması gerekmektedir.

Bu kapsamda ortaya çıkan KEP, temelde geleneksel kayıtlı postaya benzer şekilde taraflar arasındaki iletişimin tüm adımlarına dair delilleri de içeren elektronik kayıtları oluşturan ve sunan bir sistemdir. Sistemdeki tüm işlem ve kayıtlar tamamen elektronik ortamdadır ve elektronik imza gibi mekanizmalar kullanılarak bu kayıtların hukuki geçerliliği sağlanmaktadır. Dolayısıyla KEP geleneksel kayıtlı postanın elektronik ortamdaki hali olarak da tanımlanabilir.

Genel anlamda KEP'te gerekli olduğuna ilişkin görüş birliğine varılmış adillik ve inkâr edilemezlik gibi iki özellik göze çarpmaktadır (Ferrer-Gomilla vd., 2010). Bu özelliklerin yanı sıra KEP içerisinde bulunabilecek veya bazı durumlarda bulunması

zaruri olan güvenilir üçüncü taraflar, iletişim kanalı, sonlanabilirlik ve zaman aşımı süreleri, kayıtların saklanması, gizlilik, bütünlük, güvenilirlik, performans, düzenleme ve uyuşmazlık çözümü gibi hususlar da öne çıkmaktadır. Tüm bu özellik ve bileşenler başta ispat olmak üzere birçok gereksinimin KEP ile ne şekilde karşılanabileceğinin ortaya konması açısından önemlidir.

Özellikle son yıllarda güvenli ve inkâr edilemez bir mesajlaşmanın tesisi üzerine farklı ülkelerde KEP veya CEM isimleriyle anılan birçok çalışma yapılmaya başlamıştır. KEP sistemini düzenlemiş ve hayata geçirmiş olan Almanya örneği incelendiğinde sistemin özel bir kanun ile düzenlendiği ve bu kanun ile sistemin hukuki boyutunun açık bir şekilde ortaya koyulduğu ve müteakiben detaylı teknik düzenlemelerin yapıldığı dikkat çekmektedir. İncelenen diğer bir uygulama olan İtalya örneğine bakıldığında KEP'in bir kanuni düzenlemeye konu edildiği ve akabinde bir takım zorunluluklar getirilmek suretiyle sistemin kullanımının oldukça yaygınlaştırıldığı görülmektedir. Avusturya örneğinde ise sistemin tek taraflı olarak kamu idareleri ile vatandaş ve şirketler arasındaki iletişimi kapsadığı anlaşılmaktadır. Avusturya'daki sistemin yapısı teknik anlamda diğer ülke uygulamalarından farklı olsa da hukuki açıdan kapsamlı düzenlemelerin yapıldığı görülmektedir. Konunun e-Devlet kapsamında ele alınması ve sistemi öncelikle kamu kurum ve kuruluşlarının kullanımlarının öngörülmesi hususları tüm bu ülke uygulamalarının ortak özellikleri olarak dikkat çekmektedir.

Türkiye ile diğer ülke uygulamaları karşılaştırıldığında KEP sisteminin KEPHS olarak faaliyet gösteren merkezi bir TTP aracılığıyla güçlü bir adillik sağladığı söylenebilmektedir. KEP hizmetinin diğer ülke uygulamalarıyla benzer şekilde internet üzerinden sağlandığı, hizmetin verilmesi esnasında oluşturulan kayıtların belirli ve sınırlı bir süre saklandığı, sonlanabilirliğin bulunduğu ve zaman aşımı sürelerinin tanımlandığı anlaşılmaktadır. Diğer bir özellik olan ve tüm ülke uygulamalarında isteğe bağlı olarak yer alan E2EE'nin ise KEPHS'ler tarafından sunulan bir özellik olmamakla birlikte kullanıcıların kendilerinin mesajı KEPHS'ye iletmeden hemen önce şifreleyip gönderebilme imkânına sahip olmaları nedeniyle isteğe bağlı bir özellik olarak KEP sisteminde yer aldığı söylenebilir. İnkâr edilemezlik

servisleri ve deliller açısından ise Türkiye'deki sistemde delillerin ihtiyacı karşılayacak şekilde belirlendiği ve kullanıldığı görülmektedir. Hatta Türkiye'de KEP sistemindeki deliller diğer ülke uygulamalarıyla kıyaslandığında delillerin hem sayı hem nitelik açısından daha kapsamlı olduğu değerlendirilmektedir. Ayrıca sistem tarafından oluşturulan ve işlem sertifikası adı verilen nitelikli bir elektronik sertifika ile imzalanan deliller taraflar ile paylaşılabilmektedir. Aynı zamanda bu deliller üçüncü taraflarca da doğrulanabilmektedir.

Türkiye'deki KEP sisteminde Almanya ve İtalya uygulamasına benzer şekilde SMTP protokolüne dayanan elektronik posta altyapısının kullanıldığı görülmektedir. Elektronik imzalar bakımından Türkiye'deki sistemin her aşamasında EİK'ya göre elle atılan imza ile aynı hukuki sonucu doğuran ve AB (1999) ile uyumlu QES imza formatı kullanılmaktadır (T.C. Resmi Gazete, 2004). Bu yönüyle sistem hukuki anlamda büyük bir güvence sağlamaktadır.

Türkiye'de KEP sistemine ilişkin kısa bir kanuni düzenlemenin yanında standartlara dayanan detaylı teknik düzenlemeler de bulunmaktadır. Diğer ülke uygulamarındaki kanuni düzenlemeler ile kıyaslandığında Türkiye'de oldukça kısa bir kanuni düzenleme bulunduğu söylenebilir.

Tez kapsamında Türkiye'deki mevcut durumun aktarılmasının yanı sıra ele alınan hususlar detaylarıyla değerlendirilmiştir. Yapılan detaylı inceleme ve değerlendirmeler neticesinde KEP düzenlemelerine, KEPHS denetimlerine ve ilgili diğer konulara ilişkin tavsiye edilen önerilere aşağıda yer verilmektedir.

Düzenlemelere İlişkin Öneriler:

- Ülkemizde gerçekleştirilen düzenlemelerin tamamı üçüncü bölümde detaylarına yer verilen ülke örneklerine bakıldığında oldukça kısa ve genel hükümler olarak karşımıza çıkmaktadır. İşin nasıl yapılacağının ikincil düzenlemelere bırakılmış olduğu görülmektedir. Oysa KEP ile ilgili hususların gerek Anayasa'nın 13'üncü maddesi ve gerekse özel hayatın gizliliği başta olmak üzere, adil yargılanma hakkı

ve diğer bazı temel hak ve hürriyetlere müdahale imkânı verecek konular olması nedeniyle, yapılan yasal düzenlemelerde esas çerçevesinin iyi belirlenmesi gerekmektedir.

- TTK ile KEP'in ilk kullanım alanı olarak tacirler arasındaki işlemler seçilmiştir. İncelenen ülke uygulamalarında konunun e-Devlet kapsamında ele alındığı ve sistemin öncelikli kullanıcılarının kamu kurum ve kuruluşları olarak beirlendiği görülmektedir. Ülkemizde ilk kullanım alanının tacirler arasındaki işlemler olarak belirlenmiş olması sistemin gelişimi ve yaygınlaşması açısından olumsuz bir husus olarak karşımıza çıkmaktadır. Bu sebeple konunun, e-Devlet kapsamında değerlendirilmesi, özellikle kamu kurum ve kuruluşları ile koordinasyon gerektirmesi nedeniyle hukuki boyut ve kullanım alanları açılarından Başbakanlık gibi tek ve üst bir kurum tarafından ele alınması gerekmektedir.

- Değişik yasalarda ve yasa tasarılarında yapılan KEP ve elektronik tebligat ile ilgili düzenlemelerde değişik kurum ve kuruluşlara ikincil mevzuat yapma görevi verilmiş ve konuya bütüncül olarak yaklaşılmamıştır. Mevzuattaki dağınıklığın ve bu durumun doğurabileceği hukuki belirsizliğin giderilebilmesi için, konuyla ilgili mevzuat hükümlerini ortak esaslara bağlayan yasal düzenlemeler yapılması gerekmektedir. Ayrıca düzenleme ihtiyacının yönetmeliklerle değil yasa ile doldurulmasının hukuk güvenliği, idarenin öngörülebilirliği ve kanuniliği ilkeleri çerçevesinde daha isabetli olacaktır. Bu sebeplerle bugüne kadar gerçekleştirilen yasal düzenlemelerin yeniden gözden geçirilmesine ve gerekli değişikliklerin acilen yapılmasına ihtiyaç duyulmaktadır. KEP'in elektronik imzada olduğu gibi bütüncül yaklaşımla çıkarılacak bir kanun kapsamında ele alınarak gerekli ve yeterli detayda kanuni düzenlemelerin yapılması gerekmektedir.

- AB yaklaşımı da göz önünde bulundurularak KEP'e ilişkin olarak yapılacak kanun çalışmalarında;

  - Uygulamada yaşanan ve ilerde yaşanması muhtemel karışıklığı ortadan kaldırmak ve KEP'e ilişkin tüm uygulamalarda yeknesaklık sağlamak amacıyla; KEP, KEPHS, hesap sahibi, gönderici, alıcı gibi tanımlamalara,

  - EİK'de olduğu gibi kimlerin KEPHS olarak faaliyet gösterebileceğine ve KEPHS'lerin yetkilendirilmesine,

  - Sistemin güvenilirliği anlamında KEPHS'lerin hizmeti ne şekilde vereceğine,

  - KEPHS'lerin KEP hizmeti sunmak için gerçek ve tüzel kişilerden talep ettiği bilgileri BTK tarafından belirlenen usule uygun ve güvenilir bir biçimde tespit etmesine,

  - Sisteminin güvenliğini sağlanmasına, güvenli ürün ve sistemlerin kullanılmasına, hizmeti güvenilir bir biçimde yürütülmesine, hizmetlerin belirlenen kalitede sunulabilmesini teminen gerekli idarî ve teknik imkân ile kabiliyetlere sahip olunmasına, bilgi güvenliğinin sağlanmasına,

  - Kullanıcı haklarının korunması, rekabetin sağlanması amacıyla KEPHS'lere bazı yükümlülükler getirilmesine,

  - KEPHS'nin KEP hizmetine ilişkin yükümlülüklerini yerine getirmemesi hâlinde doğacak zararın boyutlarının KEPHS'lerin mali açıdan yıkımına sebebiyet verebilecek olması nedeniyle malî sorumluluk sigortası yaptırma yükümlülüğü getirilmesine,

  - KEPHS'lere belirli bir mali güce sahip olma veya bir teminat mektubu sunma gibi yükümlülükler getirilmesine,

- KEPHS'lerin usulüne uygun olarak oluşturduğu kayıtların hukuki geçerliliğinin belirlenmesi ve bu kapsamda KEPHS'lerin, KEP sistemi üzerinden sunduğu hizmetlere ilişkin kayıtların BTK tarafından belirlenen usule uygun bir şekilde oluşturulması halinde senet hükmünde olacağına ve aksi ispat edilinceye kadar kesin delil sayılacağına,

- KEPHS'lerin sunduğu hizmetler gereği tuttukları delil ve kayıtları saklaması hukukî ihtilafların çözümünde önem arz ettiğinden KEPHS'lerin bu kayıtları ne şekilde ve ne kadar süre ile saklayacağına,

- KEP sisteminin zorunlu olarak kullanılacağı iş ve işlemler konusunda, sistemin öncelikle devlet-vatandaş, devlet-devlet ve devlet-özel işletmeler arasındaki iletişimi düzenleyecek şekilde ele alınmasına ve bu alanlarda bir takım zorunlulukların getirilmesine,

- KEP sisteminin ihtiyari olarak kullanabileceği diğer iş ve işlemlere ilişkin olarak resmî veya ticarî bilgi ya da belge paylaşımı, ilgili taraflar arasında bildirim, ihtar, ihbar ve benzeri hukukî sonuç doğuran beyan ve yazışmaların, KEP sistemi vasıtasıyla yapılabileceği hususunda hükümlere yer verilmesine,

- Özellikle sistemin kamu tarafından benimsenmesini ve kullanımını kolaylaştırmak üzere idari işlemlere ilişkin yetkili olacak Başbakanlık gibi bir üst otoritenin belirlenmesine,

- Almanya, İtalya ve Avusturya'da olduğu gibi kamuda KEP kullanılarak yürütülen idari işlemlere ilişkin esaslar, belirlenecek bu otorite tararından düzenlenirken, teknik hususlara ilişkin düzenleme ve denetlemenin BTK tarafından gerçekleştirilmesine,

- Kişisel verilerin korunması gerek kişisel haklar gerekse ticari ilişkiler açısından büyük önem taşıdığından KEP sistemindeki kişisel verilerin korunmasına,

- Etkin ve sürdürülebilir rekabetin sağlanması amacıyla faaliyetleri devam eden KEPHS'lere, sektöre yeni girecek taraflarla gerekli bilgi ve belgeleri paylaşma zorunluluğu getirilmesine,

- KEPHS'lerin kullanacakları işlem sertifikasının ESHS'lerde olduğu gibi KEPHS'nin tüzel kişiliği adına olmasına,

- İdari yaptırımların tam olarak uygulanabilmesi için yasaların ilgili idareye açıkça yaptırım yetkisi vermiş olması gerektiğinden KEPHS'lerin mevzuata aykırı davranmaları halinde uygulanacak idari yaptırımların belirlenmesine,

- Yetkilendirilmeden KEPHS gibi faaliyet gösterenlere ilişkin bir cezai müeyyide öngörülmesine,

- EİK'dekine benzer şekilde KEP hesaplarının izinsiz kullanımı ya da oluşturulması eylemlerinin ayrı suçlar olarak düzenlenmesi suretiyle bu alandaki ceza hukuku korumasının güçlendirilmesi için hükümlere yer verilmesine,

- EİK'de olduğu üzere işlenen suçların KEPHS çalışanları tarafından işlenmesi durumda bu cezaların yarısına kadar artırılacağına, bu suçlar nedeniyle oluşan zararın ayrıca tazmin ettirileceğine,

ilişkin hususlara yer verilmesi gerekmektedir.

- KEP uygulamalarının yaygınlaşması, kullanımın artırılabilmesi, yüksek oranda tasarruf ve verimlilik sağlanabilmesi amacıyla; 2004 sayılı İcra İflas Kanunu, 4857 saylı İş Kanunu, 6098 sayılı Türk Borçlar Kanunu ve 6570 sayılı Gayrimenkul Kiraları Hakkında Kanun gibi bazı kanunlarda değişiklik yapılması uygun olacaktır.

- KEP iletilerinin, delillerin ve elektronik belgelerin saklanması hizmetlerinin KEPHS'ler tarafından hukuken geçerli ve güvenli bir şekilde verilebilmesi için,

elektronik arşiv hizmetlerine ilişkin ilave ayrıntılı düzenleme yapılması gerekmektedir.

[redacted]

[redacted]

[redacted]

- KEP'e ilişkin tüm süreçlerin elektronik ortama aktarılabilmesi için noterlikler veya ilgili bakanlık tarafından kanuni temsilcilerin, tüzel kişilikleri temsile yetkili olduklarına dair bilgi ve belgeleri elektronik ortamda temin edebilmelerine yani elektronik vekâlet sistemine yönelik çalışmalara başlanmalıdır.

[redacted]

- Elektronik Tebligat Yönetmeliği'nde sadece elektronik tebligatın nasıl yapılacağına ve cevapların ne şekilde verileceğine ilişkin usullerin düzenlenmesi gerektiği ve altyapıya ilişkin hükümlere yer verilmeksizin KEP mevzuatına atıf yapılmasının uygun olacağı değerlendirilmektedir.

[redacted]

- Elektronik Tebligat Yönetmeliği'nde yer alan olay kayıtlarının paylaşımına ilişkin maddelerin KEP Yönetmeliği ile uyumlu olacak şekilde değiştirilmesi gerekmektedir.

- Kayıtların saklanma sürelerine ilişkin Elektronik Tebligat Yönetmeliği ile KEP Yönetmeliği'nde yer alan hükümler uyumlu hale getirilmelidir.

- Elektronik Tebligat Yönetmeliği'nde oluşturulması öngörülen "elektronik tebligat alanlar listesinin" kim tarafından ne şekilde tutulacağı ve KEPHS'lerin bu konudaki yükümlülüklerinin neler olacağı ayrıntılı bir şekilde belirlenmelidir.

- Elektronik Tebligat Yönetmeliği'nde yer alan ileti ve kayıtların zaman damgası ile ilişkilendirilmesine ve mesaj özetlerinin kullanılmasına ilişkin hükümler ile KEP Yönetmeliği'nde bu hususlara yönelik hükümler uyumlu hale getirilmelidir.

- Elektronik Tebligat Yönetmeliği'nde kurumsal entegrasyonun yapılmasının önündeki engellerin kaldırılması ve bu entegrasyonun nasıl olması gerektiğine ilişkin hükümlere yer verilmesi gerekmektedir.

- Elektronik Tebligat Yönetmeliği'nde bulunan elektronik tebligat yapılması zorunlu olan muhatapların elektronik tebligat hizmetinin kullanıma kapatılması için başvuruda bulunamayacağına ilişkin hüküm, KEP Yönetmeliği ile uyumlu hale getirilmelidir.

- Mesajların belirli bir süre sonra silinmesi hususunda Elektronik Tebligat Yönetmeliği ve KEP Yönetmeliği'nde yer alan farklı hükümler ele alınmalı ve değiştirilmelidir.

[redacted]

[redacted]

- KEP rehberinin daha kolay, hızlı ve etkili kullanılmasını sağlamak üzere merkezi bir rehber yapısının kurgulanması gerekmektedir.

- KEP sistemini zorunlu olarak kullanmaları öngörülen tarafların KEP adreslerine daha kolay ulaşılmasını teminen bahse konu KEP adreslerini kendi internet sitesinde yayımlama zorunluluğu getirilmesi uygun olacaktır.

- KEPHS'ler arası hesapların taşınabilmesini teminen hesap taşıma altyapısının kurulabilmesi için gerekli teknik ve idari hazırlıklara başlanması gerekmektedir.

- ETSI TS 102640-4'de göre sistem içerisinde üretilebilecek delillerden "iletilerin basılı hale getirilip geleneksel kayıtlı posta ile gönderilmesine ilişkin delillerin" kullanılmasının faydalı olacağı değerlendirilmektedir.

[redacted]

[redacted]

[redacted]

[redacted]

- Delillerin taşınmasında kullanılan KEP iletilerinin, KEPHS'ler arası gönderim ve alımlarında; bu iletilerin karşı tarafa ulaşıp ulaşmadığına ilişkin olarak MDN, DSNs, SMTP servis eklentileri veya S/MIME alındı bildirimleri yöntemlerinden bir tanesinin seçilerek kullanılması faydalı olacaktır.

- TTP olarak yetkilendirilen KEPHS'lerin listesinin BTK tarafından genele açık bir dizinde otomatik işlemeye uygun bir formatta TSL kullanılarak yayımlanmasının gerek kullanım kolaylığı gerekse uluslararası birlikte çalışabilirlik açısından faydalı olacağı değerlendirilmektedir.

- Sistemin sağlıklı bir şekilde işleyebilmesi ve güçlü adilliğin tesisi için KEPHS'lerin; iletilerin kontrollerinde, S/MIME ve delillerin oluşturulmasında, iletilerin aktarılmasında ve delilerin gönderilmesinde yaşanabilecek kayıpları ortadan kaldırmak amacıyla uygun kontrolleri kurgulaması gerekmektedir. Bu hususlara yönelik, taraflar arası adilliği de sağlayacak şekilde, uygun tedbirleri alma görevi düzenlemeler ile KEPHS'lere verilmeli, bu hususlar sıkı bir biçimde kontrol edilmeli ve denetimler sırasında da göz önünde bulundurulmalıdır.

- KEPHS'ler arası bağlantının yedekli bir şekilde çok noktalı ağdan çok noktalı ağa bağlantıya erişim tekniklerinden bağımsız bir şekilde izin veren özel MPLS VPN çözümü ile gerçekleştirilmesi gerektiği değerlendirilmektedir. Bu kapsamda Türkiye'deki KEP sisteminin iletişim omurgasını oluşturacak ve KEPNET olarak da adlandırılabilecek bir yapıya ihtiyaç duyulmaktadır. [redacted]

- KEPHS'ler arası birlikte çalışabilirliğin sağlanması ve sürdürülebilmesi, hizmetlerin sürekli ve doğru bir biçimde çalışmasını temin etmek üzere hizmet sağlayıcıların mevzuatta tanımlanan gerekliliklere uygunluğunu değerlendirmeyi de içerecek şekilde testler tanımlanmalı ve uygulanmalıdır. Bu kapsamda ETSI

TR 103 071'de yer verilen detaylı test senaryolarının uygulanması yerinde olacaktır.

- KEPHS'lerin kullanmış oldukları yazılımlar sistemin temelini oluşturduğundan yapılacak olan yazılım değişikliklerinde belirlenecek testlerin uygulanması ve bu testleri geçemeyen yazılımların sisteme dâhil olmalarının engellenmesi gerekmektedir.

- KEPHS'ler tarafından sunulan arayüzlerin daha sade ve anlaşılabilir olmasını teminen bir takım teknik hususlar belirlenerek zorunlu hale getirilmelidir.

- Almanya ve İtalya örneklerinde de yer alan sistemlerin çalışmasını izlemek, birlikte çalışabilirliği test etmek ve teknik gelişimine dair çalışmak üzere sistem paydaşlarının yer aldığı bir çalışma grubunun kurulması gerektiği değerlendirilmektedir. Ayrıca bu grup tarafından KEP kullanımını artırabilecek uygulamaların belirlenmesi ve bu uygulamalar ile ilgili mevzuatın araştırılarak gerekli düzenleme önerilerinin oluşturulması fayda sağlayacaktır.

- Etkin ve süredürülebilir rekabetin tesis edilebilmesini teminen KEPHS'ler ile koordineli olacak şekilde fiyatlandırmaya ilişkin düzenlemeler yapılmalıdır.

KEPHS'lerin Denetimlerine İlişkin Öneriler:

- KEP hizmeti, TTP olarak kabul edilen KEPHS tarafından verilmektedir. Tüm KEP iletilerinin ve delillerin KEPHS tarafından oluşturulduğu ve hesap sahiplerine iletildiği göz önüne alındığında KEPHS'lerin sağladığı tüm bilgiler doğru kabul edilmektedir. Ancak bu konuda karşılaşılacak yanlış bir bilgi sisteme olan güveni büyük ölçüde zedeleyecektir. Bu sebeple KEPHS'ler sıkı bir biçimde kontrol edilmeli ve denetlenmelidir. Bu konuda denetleme ve düzenleme görevi BTK'ya ait olduğundan Kurum'un teknik bilgi düzeyi yüksek ve yeterli sayıda uzman personeli bulunmalıdır.

- KEPHS olmak isteyenlerin, BTK'ya sunduğu KEPHS olma talebini içeren dilekçe ve KEP Yönetmeliği ile belirlenen bilgi ve belgelerin ilk incelemesinin Ek-1'de yer alan kontrol listesine göre yapılmasının uygun olacağı değerlendirilmektedir.

- KEPHS'lerin bağlı olduğu kurallar, almaları gereken hukuki ve teknik tedbirler ile bu tedbirlerin ne şekilde alınacağı KEP Yönetmeliği, tebliğler, BTK tarafından yayımlanan usul esaslar ve Teknik Kriterler Tebliği'nin atıfta bulunduğu standartlardan oluşan KEP mevzuatında belirtilmektedir. Bu düzenlemelerde yer alan hükümler denetim esaslarını, Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Usul ve Esaslar Hakkında Yönetmelik'teki düzenlemeler ise denetim usullerini teşkil etmektedir. Söz konusu mevzuatta yer alan ve dördüncü bölümde detaylarıyla ele alınan hususların KEPHS tarafından yerine getirilip getirilmediğinin kontrol edilebilmesi amacıyla Ek-2'te yer alan "Denetim Rehberi" hazırlanmıştır. Denetim rehberi, bahse konu mevzuat hükümleri ve mevzuat ile atıf yapılan standartlarda belirtilen KEPHS'nin uymakla yükümlü olduğu hususları içermektedir. KEPHS'ler arası adilliği de içerecek şekilde etkin ve sürdürülebilir rekabetin sağlanması için BTK tarafından yapılan tüm KEPHS denetimlerinde bahse konu "Denetim Rehberi"'nin kullanılması önerilmektedir.

- Yeni teknolojik gelişmeler ve düzenlemeler ışığında denetime konu olan hususların zamanla değişebileceğinden, yeni oluşan şartlara uygun olarak denetim rehberinin gözden geçirilmesinin ve güncellenmesinin gerekli olduğu düşünülmektedir.

- KEPHS'lerin KEP hizmetini verirken kullandıkları işletim sistemleri, veri tabanları, ağ sistem ve cihazları, veri depolama sistemleri, HSM ve imzalama sunucuları, uygulama sunucuları, izleme ve alarm sistemleri, güvenlik ve loglama sistemleri, kullanıcı yönetim sistemleri, erişim kontrol sistemleri, yedekleme sistemleri, yazılım altyapısı, çağrı merkezi, değişiklik yönetim sistemleri, felaketten kurtarma merkezi (FKM), veri merkezi ve FKM fiziki altyapısı, yazılım yaşam döngüsü gibi hususlarında belirlenmiş olan isterleri karşılayıp

karşılamadığı KEPHS'lerin denetimlerinde kullanılmak üzere hazırlanan "Denetim Rehberi" kapsamında değerlendirmeye tabi tutulmalıdır.

Genel Öneriler:

- KEP kullanımının yaygınlaştırılması için daha fazla sektörel tanıtım etkinliği yapılması, sektörde farkındalık yaratılması çalışmaları ile birlikte katma değerli özel projeler geliştirilmesine ağırlık verilmesi gerektiği değerlendirilmektedir. Bu kapsamda KEP kullanımının özendirilmesi ve yeni uygulama alanları yaratılması gerekmektedir.

- BTK'nın işletmeciler ve hizmet sağlayıcılar ile olan yazışma ve iletişiminde KEP sistemini aktif olarak kullanmasının gerek hız gerekse kullanım kolaylığı açısından büyük faydalar sağlayacağı değerlendirilmektedir. Bu kapsamda Kurumumuzun göndereceği yazıların yanında Kurumumuza yapılacak başvuruların ve cevabi yazıların da KEP ile yapılabilmesi için gerekli çalışmalara başlanmalı ve en kısa sürede tamamlanmalıdır.

- Kurumsal olarak KEP kullanacak kurum ve kuruluşlara altyapı desteği sunan elektronik belge yönetim sistemi (EBYS) sağlayıcılarının, sundukları EBYS'lerde KEP entegrasyonunu yapmaları yönünde özendirilmeleri ve teşvik edilmeleri gerekmektedir. Bu hususta KEPHS'ler ile ilgili firmaların koordineli şekilde çalışmalarının temini yoluna gidilmelidir.

- Yetkilendirilen KEPHS'lerin gerçek kişilerin kimliklerini doğrulama sırasında MERNİS sistemini, tüzel kişilerin kimliklerinin doğrulamasında ise MERSİS sistemin kullanmaları için gerekli çalışmalar yapılmalıdır.

- Vatandaşların ve şirketlerin KEP hizmetini e-Devlet kapısı üzerinden alabilmeleri yönünde çalışmaların yapılmasının faydalı olacağı değerlendirilmektedir.

İlerde Yapılabilecek Çalışmalar:

- Bu tez çalışması sırasında ortaya çıkan ve ileriye dönük yapılabilecek çalışmalar kapsamında sürekli değişen KEP sektöründe teknik gelişmelere paralel yeni düzenlemelerin yapılması gerekmektedir. Sistemin yaygınlaşması ile birlikte pazara girmek isteyen şirketlerin sayısında da artış olması beklenmektedir. Bu kapsamda bu tezi takiben KEPHS'ler arası birlikte çalışabilirlik esaslarını detaylı bir şekilde ortaya koymak ve gerekli birlikte çalışabilirlik test senaryo ve verilerini oluşturabilmek amacıyla birtakım çalışmaların yapılabileceği düşünülmektedir.

Bu tez kapsamında incelenen dünya uygulamalarından elde edilen bilgiler ve yapılan değerlendirmeler sonucu oluşturulan önerilerin, ülkemizde henüz emekleme döneminde olduğu kabul edilen KEP sistemine ilişkin düzenlemeler ile uygulamaların gelişmesine, BTK tarafından gerçekleştirilen yetkilendirme ve rutin denetimlerin etkin ve etkili bir şekilde gerçekleştirilmesine katkı sağlaması beklenmektedir.

KAYNAKLAR

ABADI Martin vd., 2002, Certified Email with a Light On-line Trusted Third Party: Design and Implementation, In Proceedings of the 11th International World Wide Web Conference, Cilt 2, s. 387–395. ACM Press

AGID, 2015, Certified Mail, http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/posta-elettronica-certificata, (04.04.2015)

AKBULAK Yavuz, 2012, Kayıtlı Elektronik Posta Sistemine İlişkin Esaslar, Mali Çözüm Dergisi / Financial Analysis, Sayı 114, s. 179-187. Business Source Complete, EBSCOhost, (12.01.2015)

AKLEYLEK Sedat vd., 2011a, Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta, Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri, Malatya

AKLEYLEK Sedat vd., 2011b, Kayıtlı Elektronik Posta, http://ab.org.tr/ab11/sunum/Kriptoloji-Egitim/KEP/kep-s2.pdf, Malatya, 4 Şubat 2011, Sunum

ASOKAN N., 1998, Fairness in Electronic Commerce, Ph.D. thesis, University of Waterloo, Computer Science

AFC (Austrian Federal Chancellery), 2011, Administration on the Net-Federal Platform Digital Austria, The ABC guide of eGovernment in Austria, ISBN 978-3-200-02352-9, Vienna

AB, 1999, Directive 1999/93/EC of the European Parliament and of the Council on a community framework for electronic signatures, Official Journal of the European Communities, 19.01.2000

AB, 2014, Regulation (EU) No: 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Communities, 28.08.2014, 257/73

Avusturya Cumhuriyeti, 1982, Federal Resmi Doküman Hizmetleri Kanunu, Austrian Federal Law Gazette No. 200/1982 as amended by: Federal Law Gazette s. 33/2013, https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1982_200/ERV_1982_200.pdf, (02.03.2015)

Avusturya Cumhuriyeti, 2004, Federal Avusturya e-Devlet Kanunu, Austrian Federal Law Gazette, Bölüm I, Sayı 10/2004, http://www.a-sit.at/pdfs/e-govg_engl.pdf, (02.03.2015)

BAKER Greg, BOWEN Tom, 2003, First Byte: Using Information and Communication Technology, Oxford University Press, 5th Ed., ISBN 0195517768

BAUTTS Tony vd., 2005, Linux Network Administrator's Guide, O'Reilly, Third Edition, ISBN 0-596-00548-2, USA

BORITZ J. Efrim, 2005, IS Practitioners' Views on Core Concepts of Information Integrity, International Journal of Accounting Information Systems, Cilt 6, Sayı 4, s.260–279, Elsevier, doi:10.1016/j.accinf.2005.07.001

BS, 2009, British Standard, BS 10012:2009 Data protection-Specification for a personal information management system

BSI, 2011, Technische Richtlinie De-Mail

BT Haber, 2010, e-Devlet İçin Arayışlar Sürüyor, http://www.bthaber.com/e-devlet-icin-arayislar-suruyor, (19.03.2015)

BTK, 2012a, Elektronik İmza Kullanım Profilleri Rehberi Sürüm 1.0, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, http://www.btk.gov.tr/bilgi_teknolojileri/elektronik_imza/dosyalar/Elektronik_Imza_Kullanim_Profilleri_Rehberi.pdf, (26.01.2015)

BTK, 2012b, Kayıtlı Elektronik Posta Sisteminde Kullanılan İşlem Sertifikasına İlişkin Usul ve Esaslar, Tarih: 06.06.2012, Sayı: 2012DK-15259, Kurul Kararı

BTK, 2014, Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar, Tarih: 09.09.2014, Sayı: 2014/DK-BTD/447, Kurul Kararı

BTK, 2015a, KEP 2013-2014 Yılı Pazar Verileri, BTK, Ankara

BTK, 2015b, KEP 2015 Yılı Aylık Pazar Verileri, BTK, Ankara

BUZZI Marina vd., 2014, E-Government Services Italian Certified Electronic Mail, 13th International Conference WWW/INTERNET, Porto

CALLAS J., vd., 2007, OpenPGP Message Format, Internet Engineering Task Force (IETF), RFC 4880

Canada Post, 2015, Registered Mail, http://www.canadapost.ca/tools/pg/manual/PGregister-e.asp#1386476, (21.03.2015)

CATTEL Rick, INSCORE Jim, 2001, 2EE™ Technology in Practice: Building Business Applications with the Java™ 2 Platform, Enterprise Edition, http://www.informit.com/articles/article.aspx?p=24236, (23.03.2015)

CHISNALL David, 2015, Electronic Messaging, http://www.swansea.ac.uk/iss/archive-and-research-collections/hocc/theinternetandcommunications/electronicmessaging/, (09.03.2015)

CIMATO Stelvio vd., 2005, Design and Implementation of an Inline Certified E-mail Service, Cryptology and Network Security, Desmedt YvoG vd.(der.), Springer Berlin Heidelberg, s. 186-199, ISBN 978-3-540-30849-2

COLLINGS Terry, WALL Kurt, 2005, Red Hat Linux Networking and System Administration, Wiley Publishing, 3rd Ed., Hoboken, N.J.

COMER Douglas E., 2008, Computer Networks and Internets, Fifth Edition, Prentice Hall, San Jose, CA, ISBN 10: 0-13-606127-3

COOPER D. vd., 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force (IETF), RFC 5280

CROCKER D., 2009, Internet Mail Architecture, Internet Engineering Task Force (IETF), RFC 5598

CRISPIN M., 2003, Internet Message Access Protocol - Version 4rev1, Internet Engineering Task Force (IETF), RFC 3501

ÇİFTÇİ Mehmet Emin, 2014, Dünyada Kayıtlı Elektronik Posta, http://www.icttele.com/index.php/component/k2/itemlist/user/53-mehmeteminciftci, (25.02.2015)

DALKILIÇ Elvin Evrim, 2014, Elektronik Tebligatın İdari İşlemler Bakımından Değerlendirmesi, Hacettepe HFD, 4 (1) 2014, s. 107–124

De-Mail Act, 2011, Bundesrepublik Deutschland, Bundesgesetzblatt Jahrgang, b. 1, s. 666, http://www.gesetze-im-internet.de/de-mail-g/index.html#BJNR066610011BJNE000301311, (23.02.2015)

De-Mail Teknik Klavuz, 2014, BSI TR 01201 – Technische Richtlinie, Versiyon 1.1.1, https://www.bsi.bund.de/DE/Themen/EGovernment/DeMail/TechnischeRichtlinien/TechnischeRichtlinien.html, (24.03.2015)

DIERKS T., ALLEN C., 1999, The TLS Protocol Version 1.0, Internet Engineering Task Force (IETF), RFC 2246

DRAPER-GIL Gerard vd., 2014, Towards a Certified Electronic Mail System, In Architectures and Protocols for Secure Information Technology Infrastructures, Antonio Ruiz-Martinez, Rafael Marin-Lopez, Fernando Pereniguez-Garcia (Ed.), s. 46-70

DÜLGER Murat Volkan, 2014, Türk Borçlar Kanunu, Türk Ticaret Kanunu ve Hukuk Muhakemeleri Kanunu'ndaki Bilişim Alanına İlişkin Düzenlemelerin Ceza Hukukuna Yansımaları, Ankara Barosu Dergisi, 2014/1, s. 114-144

E-DTR, 2009, E-Dönüşüm Türkiye İcra Kurulu KEP sistemi kararı, http://www.bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/090715_IcraKuruluIKararNo28.pdf, (19.03.2015)

E-Government Act, 2013, Germany Act to promote electronic government, Federal Law Gazette, no. 43, published in Bonn on 31 July 2013, pp. 2749 - 2760, Germany

ERYOL Gökhan, 2007, E-Posta Şifrelemede OpenPGP Kullanımı, Ulusal Akademik Ağ ULAKNET Bilgisayar Olaylarına Müdahale Ekibi ULAK-CSIRT blogu, http://blog.csirt.ulakbim.gov.tr/?p=43, (13.01.2015)

ETSI, 2009a, ETSI TS 101 903 V1.4.1 - XML Advanced Electronic Signatures (XAdES)

ETSI, 2009b, ETSITS 102 778-4 - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile

ETSI, 2009c, ETSI TS 102 231 V3.1.2 - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

ETSI, 2009d, ETSI TS 102 778-3 V1.1.2 - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles

ETSI, 2009e, ETSI TS 102 778-5 V1.1.1 - Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures

ETSI, 2011a, ETSI TS 102 640-1 V2.2.1 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture

ETSI, 2011b, ETSI TS 102 640-2 V2.2.1 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM

ETSI, 2011c, ETSI TS 102 640-3 V2.1.2 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains

ETSI, 2011d, ETSI TS 102 640-4 V2.1.2 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles

ETSI, 2011e, ETSI TS 102 640-5 V2.1.2 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles

ETSI, 2011f, ETSI TR 103 071 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Test suite for future REM interoperability test events

ETSI, 2012, TS 101 733 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

FALCIAI Roberta, LIBERATI Laura, 2006, Italian Certified E-Mail System, Digital Evidence and Electronic Signature Law Review, Cilt 3, s. 50-54, DOI: http://dx.doi.org/10.14296/deeslr.v3i0.1773

FERRARA Umberto, 2010, PEC in Italy, Meeting Exentrica / Aruba PEC / BTK, İtalya, 19 Kasım 2010, Sunum

FERRER-GOMILLA Josep Lluis vd., 2000, An Efficient Protocol for Certified Electronic Mail, Proceedings of the Third International Workshop on Information Security, LNCS 1975; s. 237–248

FERRER-GOMILLA Josep Lluis vd., 2010, Certified electronic mail: Properties revisited, Computers & Security, 29(2), s. 167–179, ISSN 01674048, Elsevier

FREED N., BORENSTEIN N., 1996, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, Internet Engineering Task Force (IETF), RFC 2045

FREIER A., 2011, The Secure Sockets Layer (SSL) Protocol Version 3.0, ISSN: 2070-1721, Internet Engineering Task Force (IETF), RFC 6101

GENNAI Francesco vd., 2005, A Certified Email System for the Public Administration in Italy, In Proceedings of the IADIS International Conference on WWW/Internet, 2005, Cilt 2, s. 143-147

GMD, 2014, Kayıtlı Elektronik Posta (KEP) Sistemi Bildirim Süresi Uzatıldı, Gümrük Müşavirleri Derneği, http://www.igmd.org/tumhaber/gumruk-ticaret-bakanligi/47637-kayitli-elektronik-posta-kep-sistemi-bildirim-suresi-uzatildi.html, (05.04.2015)

GRÉGR Matěj, 2011, Resilient Network Design, Brno University of Technology, Faculty of Information Technology

GRUNDMA Michael, WOß Andreas, 2008, Certified Mail, the Next Step in Electronic Communication?, Seminar aus Netzwerke und Sicherheit, Johannes Kepler University Linz

GÜNELİ Nihan, 2012, Kayıtlı Elektronik Posta: Bir Uygulama Örneği Olarak Elektronik Apostil, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, Yüksek Lisans Tezi, İstanbul

HANSEN T., 2004, Message Tracking Model and Requirements, Internet Engineering Task Force (IETF), RFC 3888

HANSEN T., VAUDREUIL G., 2004, Message Disposition Notification, Internet Engineering Task Force (IETF), RFC 3798

HANSEN T. vd., 2012, Internationalized Delivery Status and Disposition Notifications, Internet Engineering Task Force (IETF), RFC 6533

HOFFMAN P., 1999, Enhanced Security Services for S/MIME, Internet Engineering Task Force (IETF), RFC 2634

HOUSLEY R., 2009, Cryptographic Message Syntax (CMS), Internet Engineering Task Force (IETF), RFC 5652

ISO, 2006, International Standard ISO 3166-1, Codes for the representation of names of countries and their subdivisions

ISO/IEC, 1997, ISO/IEC 10181-4 Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework

ISO/IEC, 2003a, ISO/IEC 10021-1 - Information technology - Message Handling Systems (MHS) – Part 1: System and service overview

ISO/IEC, 2003b, ISO/IEC 10021-2 - Information technology – Message Handling Systems (MHS): Overall architecture

ISO/IEC, 2005, ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management

ISO/IEC, 2008, ISO/IEC 9594-1 - Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services.

ISO/IEC, 2009a, ISO/IEC 13888-1 - Information technology - Security techniques - Non-repudiation Part 1: General

ISO/IEC, 2009b, ISO/IEC 13888-3, Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques

ISO/IEC, 2010, ISO/IEC 13888-2 - Information technology - Security techniques - Non-repudiation Part 2: Mechanisms using symmetric techniques

ISO/IEC, 2011, ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

ISO/IEC, 2013, ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements

ISO/IEC, 2014, ISO/IEC 27000 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en, (20.02.2015)

ITU, 2006, 50 Years of Excellence 1956-2006, http://www.itu.int/ITU-T/50/docs/ITU-T_50.pdf, (31.12.2014)

ITU-T, 1996, X.813 - Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Non-repudiation Framework

ITU-T, 1999a, F.400/X.400 - Message handling system and service overview

ITU-T, 1999b, X.402 - Message Handling Systems: Overall Architecture

ITU-T, 1999c, X.411 - Message Handling Systems: Message Transfer System: Abstract Service Definition und Procedures

İCK (İtalya Cumhurbaşkanlığı Kararnamesi), 2005, Kayıtlı Elektronik Posta Kullanım Kuralları, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpr_11-feb-2005_n.68.pdf, (25.02.2015)

İC (İtalya Cumhuriyeti), 2005a, İtalya Cumhuriyeti - KEP Oluşturma, İletim, Doğrulama ve Zaman Servislerine İlişkin Teknik Düzenleme, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dm_2-nov-2005.pdf, (26.02.2015)

İC (İtalya Cumhuriyeti), 2005b, İatlya Cumhuriyeti- Elektronik Dokümanların KEP ile Gönderilmesine İlişkin Teknik Kurallar, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/pec_regole_tecniche_dm_2-nov-2005.pdf, (26.02.2015)

JOVANOVİC Mihailo, RANKOV Siniša, 2012, Cost Optimization Model And Economic Effects Of The Integration Of Registered Electronic And Hybrid Mail Systems, Megatrend Review 9, Sayı 1, s. 329-354. Business Source Complete, EBSCOhost, (09.09.2014).

KESER BERBER Leyla, 2013, Yeni Türk Ticaret Kanunu Çerrçevesinde Kayıtli E-Posta Hizmet Sağlayıcıların Posta Kutusu ve Gönderim Hizmetleri ile Kimlik Doğrulama İşlevleri, http://arslanlibilimarsivi.com/sites/default/files/makale/Leyla-Keser-Berber-Kayitli-e-Posta.pdf, (20.03.2015)

KLENSIN J., 2001, Simple Mail Transfer Protocol, Internet Engineering Task Force (IETF), RFC 2821

KOZIEROK Charles M., 2005, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, No Starch Press

LIVSON Ben, 1999, Business Modelling for Integrated Messaging and Postal Services, Hybrid Messaging Workshop, www.bal.com.au/patent/hybrid/ws.ppt, (23.12.2014)

MAIERHOFER Christian, 2015, The Austrian Governmental eDelivery System, Workshop on registered electronic mail policies and implementation, Ankara, 16-17 March 2015, Sunum

MARKOWITCH Olivier, ROGGEMAN Yves, 1999, Probabilistic Non-Repudiation without Trusted Third Party, In Proceedings of 1999 Conference on Security in Communication Networks

MELNIKOV A., 2003, Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP), Internet Engineering Task Force (IETF), RFC 3503

MCMILLAN P., 2001, Hybrid mail - from a print service to e-messaging, In Proceedings of the International Conference on Mail Technology: Evolution to e-Revolution, s. 121–131

MICALI Silvio, 2003, Simple and Fast Optimistic Protocols For Fair Electronic Exchange, In Proceedings of the twenty-second annual symposium on Principles of distributed computing (PODC '03), ACM, New York, NY, USA, 12-19, DOI=10.1145/872035.872038, http://doi.acm.org/10.1145/872035.872038

MOORE K., 2003, Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs), Internet Engineering Task Force (IETF), RFC 3461

MOORE K ve VAUDREUIL G., 2003, An Extensible Message Format for Delivery Status Notifications, Internet Engineering Task Force (IETF), RFC 3464

MUKHERJEE Ranadeep, DUTTA Ambar, 2012, An Improved Certified Email Protocol using an Offline TTP, IEEE 2012 Third International Conference on Emerging Applications of Information Technology (EAIT), 30 Kasım 2012-1 Aralık 2012, IEEE, s.425-428, ISBN: 978-1-4673-1828-0

MULA Davide, 2015, Rem Country Practice in Legal İnfrastructure, Operations, Interoperability, Usage Areas, Security Approaches, Accreditation and Supervision Of REMSPs - Italy, Workshop on registered electronic mail policies and implementation, Ankara, 16-17 Mart 2015, Sunum

MYERS J., ROSE M., 1996, Post Office Protocol - Version 3, Internet Engineering Task Force (IETF), RFC 1939

NOTARMUZI Carlo, 2015, The Digital Administration Code, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan035410.pdf, (25.02.2015)

ONIEVA Jose A. vd., 2008, Secure Multi-Party Non-Repudiation Protocols and Applications, Advances in Information Security, e-ISBN-13: 978-0-387-75630-1, Springer

OPPLIGER Rolf, 2004, Certified Mail: The Next Challenge for Secure Messaging, Communications of the ACM, 47(8), s. 75–79, ISSN 07364679

OPPLIGER Rolf, 2007, Providing Certified Mail Services on The İnternet, IEEE Security And Privacy 5, Sayı 1, s. 16-22, ISSN 15407993

OPPLIGER Rolf, 2009, SSL and TLS Theory and Practice, Artech House, London, ISBN-13 978-1-59693-447-4

OPPLIGER Rolf, 2014, Secure Messaging on the Internet, Artech House

OPPLIGER Rolf, STADLIN Peter, 2004, A Certified Mail System (CMS) for the Internet, Computer Communications, Cilt: 27, Sayı: 13, s. 1229-1235, ISSN 0140-3664, http://dx.doi.org/10.1016/j.comcom.2004.04.006

ÖNAL Huzeyfe, 2009, E-posta (Mail) Başlık Bilgileri E-posta Başlıklarından Bilgi Toplama, http://www.bga.com.tr/calismalar/mail_headers.pdf, (10.02.2015)

ÖZEL Abdurrahim, 2013, SSL' de Araya Girme Saldırıları ve Güvenlik Önlemleri, https://www.bilgiguvenligi.gov.tr/ag-guvenligi/ssl-de-araya-girme-saldirilari-ve-guvenlik-onlemleri.html, (21.03.2015)

ÖZTÜRK Özgür, 2009, E-Postalarda Spam Sorunu ve Çözüm Önerileri, Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi, Ankara

PARTRIDGE Craig, 2008, The Technical Development of Internet Email, IEEE Annals of the History of Computing, IEEE Computer Society, Cilt 30, Sayı 2, s. 3-29

PARZIALE Lydia vd., 2006, TCP/IP Tutorial and Technical Overview, IBM International Technical Support Organization, Eighth Edition

PAULIN Alois, WELZER Tatjana, 2013, A Universal System For Fair Non-Repudiable Certified E-Mail Without A Trusted Third Party, Computers & Security, Cilt: 32, s. 207-218, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2012.11.006

PETRUCCI C. vd., 2011, La Posta Elettronica Certificata - Italian Certified Electronic Mail, Internet Engineering Task Force (IETF), RFC 6109

PTT, 2015, Birleşik Posta nedir?, http://www.birlesikposta.com.tr/nedir/Hybrid-Mail-Nedir, (22.03.2015)

POHAR Mark, 2015, REM within the Scope of eIDAS Regulation, Workshop on registered electronic mail policies and implementations - ETT 57074, Ankara, 16.3.2015 – 17.3.2015, Sunum

POSTEL Jonathan B., 1982, Simple Mail Transfer Protocol, Internet Engineering Task Force (IETF), RFC 821

POŞUL Abdulkadir, AKSOY Cihan, 2013, Pretty Good Privacy (PGP) Şifreleme, TÜBİTAK-BİLGEM-SGE, https://www.bilgiguvenligi.gov.tr/gizlilik/pretty-good-privacy-pgp-sifreleme.html, (13.01.2015)

RAMSDELL B., TURNER S., 2010, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, Internet Engineering Task Force (IETF), RFC 5751

RESNICK Pete, 2001, Internet Message Format, Internet Engineering Task Force (IETF), RFC 2822

RESNICK Pete, 2008, Internet Message Format, Internet Engineering Task Force (IETF), RFC 5322

ROGALL-GROTHE Cornelia, 2014, Improved Securıty For Citizens, Security in focus, BSI Magazine 2013/14, BSI, Germany

RPost, 2015a, RPost Registered Email Services, http://www.rpost.com/registered-email, (01.04.2015)

RPost, 2015b, Corporate Overview, http://www.rpost.com/about-rpost/corporate-overview, (01.04.2015)

SCHNEIER Bruce, RIORDAN James, 1997, A Certified E-mail Protocol, In Proceedings of ACSAC '97: the Annual Computer Security Applications Conference, San Diego, IEEE Computer Society Press, s. 232–238

SCHUMACHER Astrid, 2010, De-Mail - as Simple as E-Mail and as Secure as Conventional Mail, Improving IT Security, BSI Annual Report 2008/2009, Germany

SCHUMACHER Astrid, 2014, Tools for Online Use, Security in focus, BSI Magazine 2013/14, Germany

SIEVERS Florian, 2009, Legally binding electronic correspondence, http://www.t-systems.fr/umn/uti/140838_1/blobBinary/72_30_DEMAIL_0109_E_WEB.pdf?ts_layoutId=486498, (21.02.2015)

SHIREY R., 2000, Internet Security Glossary, Internet Engineering Task Force (IETF), RFC 2828

ŞİMŞEK Umut, 2012, HTTP - Nass oluyor da oluyor? HTTPS - HTTP over SSL, http://umut-simsek.blogspot.com.tr/2012/06/http-nass-oluyor-da-oluyor-https-http.html, (21.03.2015)

TANRIKULU Cengiz, 2009, Türk ve Avusturya Hukukunda Elektronik Tebligat, TBB Dergisi, Sayı 85, s. 315-331

TAŞKIN Halil Kemal, DEMİRCİOĞLU Murat, 2014, Siber Güvenlikte Kriptoloji Kullanımı ve Uçtan Uca Şifreleme, TBD 31. Bilişim Kurultayı, Bildiriler Kitabı, Ankara

TAUBER, Arne, 2009, Requirements for Electronic Delivery Systems in Egovernment - an Austrian Experience, In Software Services for E-Business and E-Society, GODART Claude vd. (der.), 305, 123-133, Springer Berlin Heidelberg

TAUBER Arne, 2011, A Survey of Certified Mail Systems Provided On The Internet, Computers & Security, 30(6-7), s. 464–485, ISSN 01674048

TAUBER Arne vd., 2011, A Shared Certified Mail System for the Austrian Public and Private Sectors, In Electronic Government and the Information Systems Perspective, ANDERSEN KimNormann vd. (der.) , 6866, s. 356-369, Springer Berlin Heidelberg

TAUBER Arne, 2012, Cross-Border Certified Electronic Mailing, A Scalable Interoperability Framework for Certified Mail Systems, Ph.D. Thesis at Graz University of Technology, Graz

TAUBER Arne vd., 2012, An Interoperability Standard for Certified Mail Systems, Computer Standards & Interfaces, Cilt 34, Sayı 5, s. 452-466, ISSN 0920-5489, http://dx.doi.org/10.1016/j.csi.2012.03.002

TAUBER Arne vd., 2013, Cross-border Certified Electronic Mailing: A European Perspective, Computer Law & Security Review, Cilt 29, Sayı 1, s. 28-39, ISSN 0267-3649, http://dx.doi.org/10.1016/j.clsr.2012.11.002

T.C. BAŞBAKANLIK, 2009, E-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı, http://www.basbakanlik.gov.tr/Forms/_Article/pg_Article.aspx?Id=571665de-a535-49cf-9255-32ece5b6ac62, (19.03.2015)

T.C. KALKINMA BAKANLIĞI, 2014, e-Yazışma Teknik Rehberi, Mart 2014, Sürüm 1.1, http://www.bilgitoplumu.gov.tr/2014/e-yazisma-teknik-rehberi-guncellendi/, (24.03.2015)

T.C. Resmi Gazete, 2004, 5070 sayılı Elektronik İmza Kanunu, 23 Ocak 2004 tarihli ve 25355 sayılı Resmi Gazete

T.C. Resmi Gazete, 2005, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 6 Ocak 2005 tarihli ve 25692 sayılı Resmi Gazete

T.C. Resmi Gazete, 2011a, 6099 sayılı Tebligat Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, 19 Ocak 2011 tarihli ve 27820 sayılı Resmi Gazete

T.C. Resmi Gazete, 2011b, 6102 sayılı Türk Ticaret Kanunu, 14 Şubat 2011 tarihli ve 27846 sayılı Resmi Gazete

T.C. Resmi Gazete, 2011c, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2011, 25 Ağustos 2011 tarihli ve 28036 sayılı Resmi Gazete

T.C. Resmi Gazete, 2011d, Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 2011, 25 Ağustos 2011 tarihli ve 28036 sayılı Resmi Gazete

T.C. Resmi Gazete, 2012a, Kayıtlı Elektronik Posta Rehberi ve Kayıtlı Elektronik Posta Hesabı Adreslerine İlişkin Tebliğ, 2012, 16 Mayıs 2012 tarihli ve 28294 sayılı Resmi Gazete

T.C. Resmi Gazete, 2012b, Ticaret Şirketlerinde Anonim Şirket Genel Kurulları Dışında Elektronik Ortamda Yapılacak Kurullar Hakkında Tebliğ, 29 Ağustos 2012 tarih ve 28396 sayılı Resmi Gazete

T.C. Resmi Gazete, 2013, Elektronik Tebligat Yönetmeliği, 2013, 19 Ocak 2013 tarihli ve 28533 sayılı Resmi Gazete

T.C. Resmi Gazete, 2015, Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, 2 Şubat 2015 tarih ve 29255 sayılı Resmi Gazete

T.C. ULAŞTIRMA BAKANLIĞI, 2010, Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı, http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_no=81976, (19.03.2015)

TOPCAN Ferda, 2011, E-İmza Oluşturma ve Doğrulama, TODAİE Sunumu, http://bidb.beun.edu.tr/wp-content/uploads/2011/11/2-E-imzaOlusturmaVeDogrulama.pdf, (03.04.2015)

TRACY Miles vd., 2007, Guidelines on Electronic Mail Security, National Institute of Standards and Technology, Special Publication 800-45 Version 2, US

TSCHABITSCHER Heinz, 2011, The First Email Message Who sent it, and when?, http://email.about.com/cs/emailhistory/a/first_email.htm, (09.03.2015)

TURNER Sean, 2010, Secure/Multipurpose Internet Mail Extensions, IEEE Internet Computing 14, No. 5, s. 82-86. Scopus®, EBSCOhost

TURNER Sean, HOUSLEY Russ, 2008, Implementing Email and Security Tokens: Current Standards, Tools, and Practices, Wiley Publishing, ISBN: 978-0-470-25463-9

UPU (Universal Postal Union), 1996, Data definition and encoding standards, S10c-5 Identification of postal items - Part C : 13 character identifier for special letter products

URGUN Bedirhan, 2007, Web Uygulama Güvenliği Kılavuzu, Tübitak-Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Doküman Kodu: BGT-4001

VAUDREUIL G., 2003a, The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages, Internet Engineering Task Force (IETF), RFC 3462

VAUDREUIL G., 2003b, Enhanced Mail System Status Codes, Internet Engineering Task Force (IETF), RFC 3463

VLECK Tom Van, 2013, The History of Electronic Mail, http://www.multicians.org/thvv/mail-history.html, (09.03.2015)

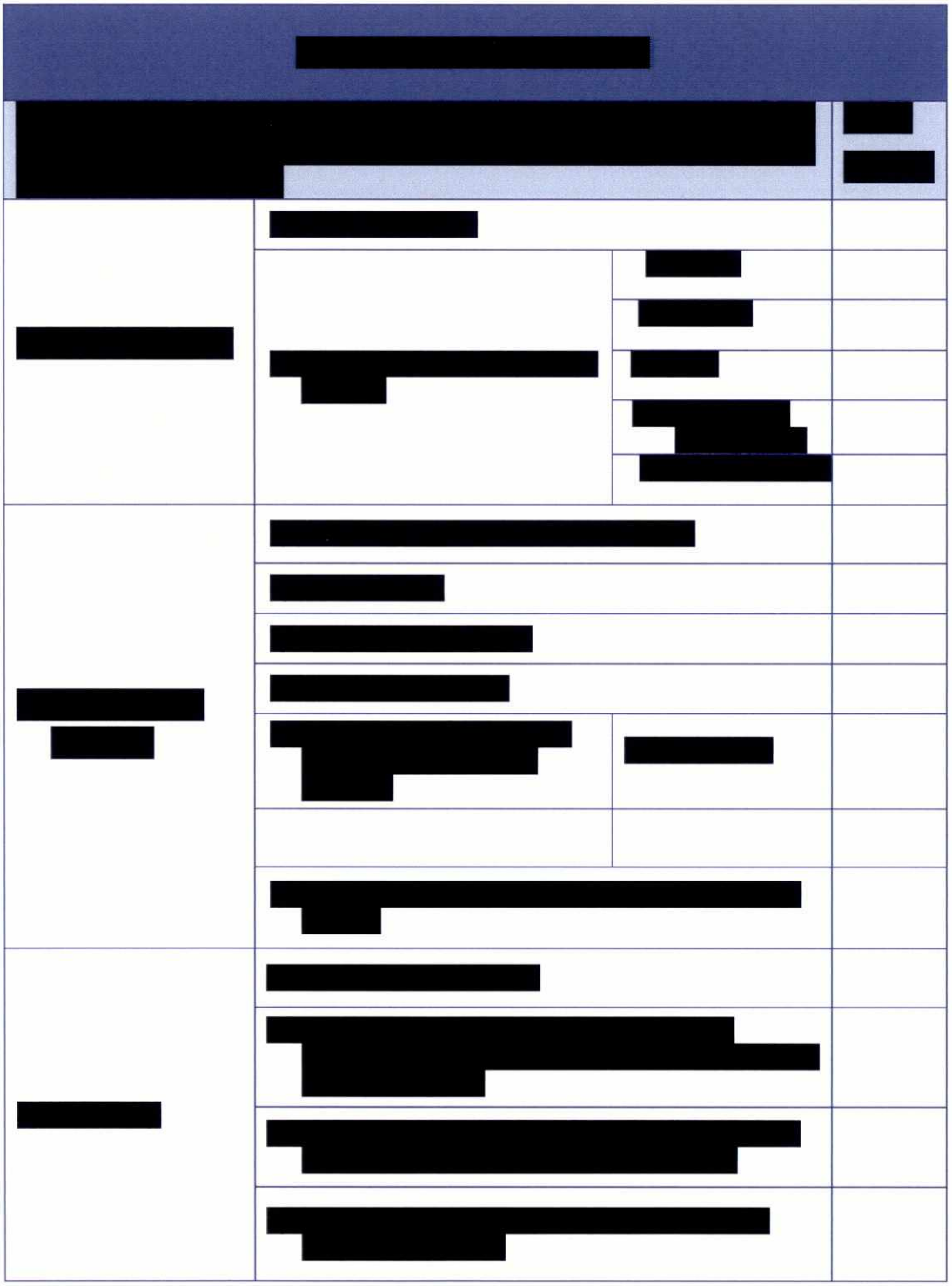
YAYLA Yıldızhan, 2010, İdare Hukuku, Beta Yayınları, İstanbul

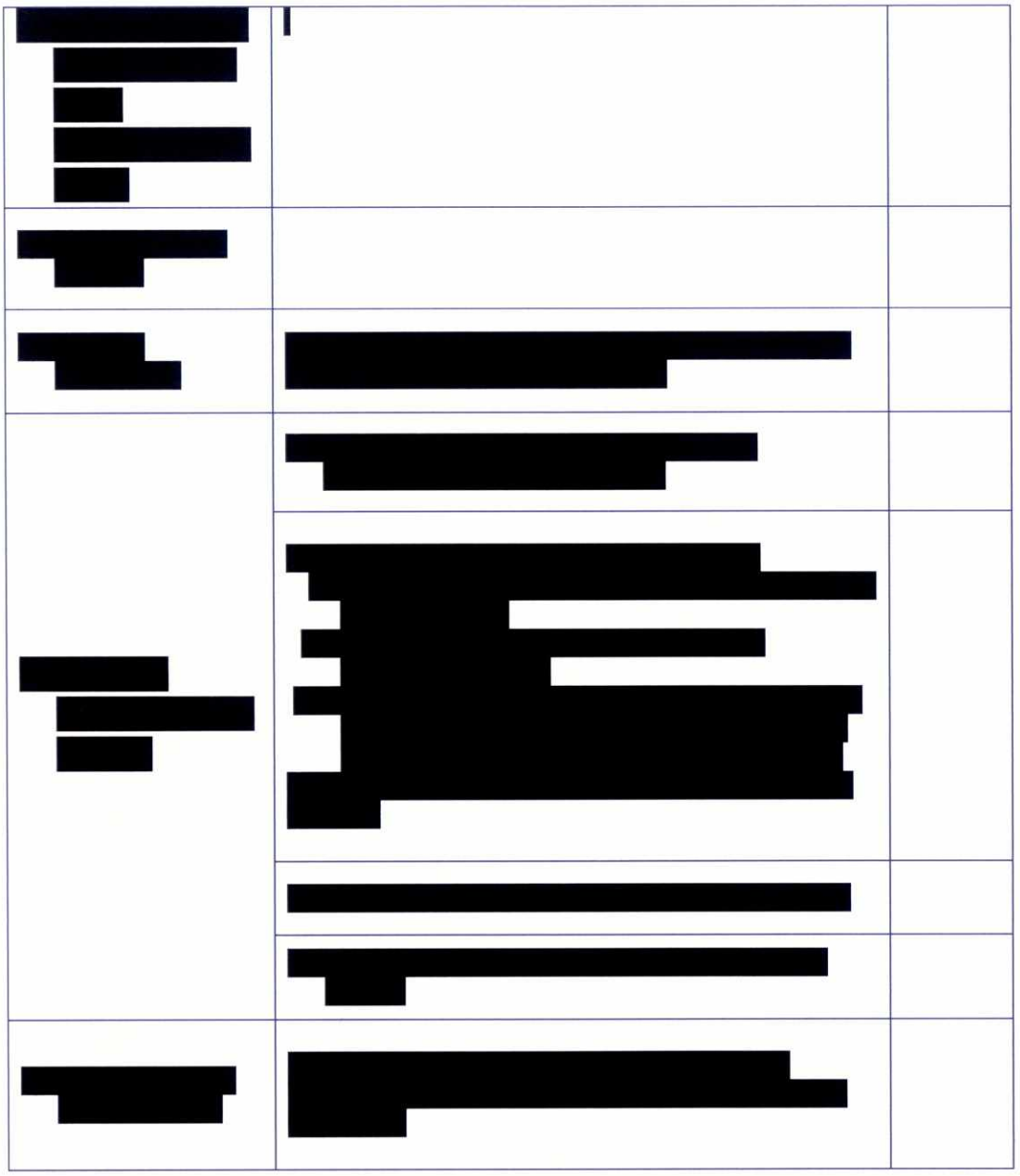
ZHOU Jianying, GOLLMANN Dieter, 1996a, A Fair Non-Repudiation Protocol, In Proceedings of the 1996 IEEE Symposium on Security and Privacy SP96, s. 55–61. ISBN 0-8186-7417-2

ZHOU Jianying, GOLLMANN Dieter, 1996b, Certified Electronic Mail, In Proc European Symp on Research in Computer Security ESORICS, s. 3–19, Citeseer

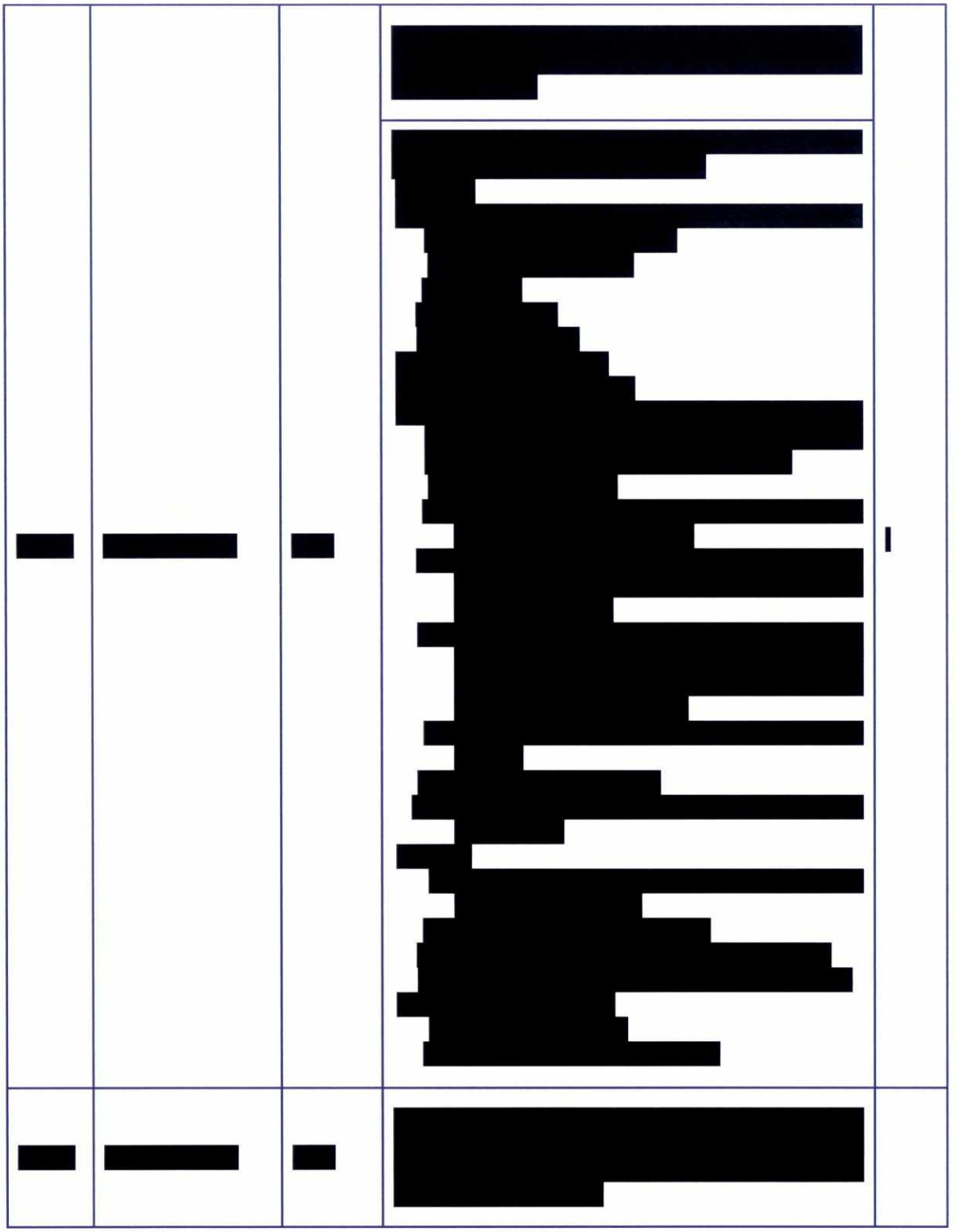
EKLER

Ek-1 Başvuru Dosyası Belge İnceleme Kontrol Listesi





Ek-2 KEPHS Denetim Kontrol Listesi



Ek-3 2013-2014 KEP Hesabı Sayıları

2013-2014 KEP SAYILARI																	
	Gerçek Kişi					Tüzel Kişi											
						Kamu Kurum ve Kuruluşları					Diğer Tüzel Kişiler						
	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Alıcı	Gönderici /Alıcı	Gerçek Kişi Toplam	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Alıcı	Gönderici /Alıcı	Kamu Toplam	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Alıcı	Gönderici /Alıcı	Diğer Tüzel Toplam	Tüzel Toplam	Toplam
2013 Sonu	-	-	-	-	5.572	-	-	-	-	-	-	-	-	-	-	6.882	12.454
Ocak	900	421	984	337	1.321	90	13	21	82	103	586	4.125	811	3.900	4.711	4.814	6.135
Şubat	398	456	613	241	854	72	26	3	95	98	164	2.380	401	2.143	2.544	2.642	3.496
Mart	20	257	79	198	277	56	13	0	69	69	113	2.188	258	2.043	2.301	2.370	2.647
Nisan	50	146	31	165	196	2	35	0	37	37	140	1.415	144	1.411	1.555	1.592	1.788
Mayıs	16	126	24	118	142	103	34	3	134	137	82	923	76	929	1.005	1.142	1.284
Haziran	46	350	160	236	396	1.166	36	3	1.199	1.202	56	1.071	104	1.023	1.127	2.329	2.725
Temmuz	146	287	142	291	433	4	8	1	11	12	194	1.796	195	1.795	1.990	2.002	2.435
Ağustos	130	472	201	401	602	5	11	0	16	16	195	3.506	408	3.293	3.701	3.717	4.319
Eylül	150	723	183	690	873	22	18	1	39	40	461	12.044	1.976	10.503	12.479	12.519	13.392
Ekim	184	513	159	538	697	1	21	0	22	22	479	9.364	1.192	8.544	9.736	9.758	10.455
Kasım	156	593	98	651	749	1	17	1	17	18	342	5.979	653	5.607	6.260	6.278	7.027
Aralık	253	890	281	862	1.143	1.745	20	4	1.761	1.765	523	16.673	1.903	16.276	18.179	19.944	21.087
2014 TOPLAM	2.449	5.234	2.955	4.728	13.255	3.267	252	37	3.482	3.519	3.335	61.464	8.121	57.467	65.588	75.989	89.244

Kaynak: BTK, 2015a

Ek-4 2015 Mayıs Ayı Sonu KEP Hesabı Sayıları

KEP HESABI SAYILARI																	
2015	Gerçek Kişi					Tüzel Kişi											
						Kamu Kurum ve Kuruluşları					Diğer						
	Alıcı		Gönderici/Alıcı		Gerçek Kişi Toplam	Alıcı		Gönderici/Alıcı		Kamu Toplam	Alıcı		Gönderici/Alıcı		Diğer Toplam	Tüzel Toplam	Genel Toplam
	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı		Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı		Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Tebligata Elverişli Olmayan KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı	Tebligata Elverişli KEP Hesabı Sayısı		
Ocak	3.029	3.704	1.736	4.783	13.252	35	12	3.283	337	3.667	955	8.451	4.260	71.155	84.821	88.488	**101.740**
Şubat	3.063	3.731	1.790	5.080	13.664	40	13	3.286	363	3.702	1.000	9.075	4.367	74.647	89.089	92.791	**106.455**
Mart	3.076	3.828	1.818	5.303	14.025	42	14	3.288	405	3.749	1.032	9.181	4.456	77.053	91.722	95.471	**109.496**
Nisan	3.175	3.898	1.861	5.548	14.482	42	14	3.288	421	3.765	1.034	9.359	4.591	81.188	96.172	99.937	**114.419**
Mayıs	3.224	3.980	1.888	5.706	14.798	43	14	3.300	521	3.878	1.022	9.453	4.675	82.977	98.127	102.005	**116.803**

Kaynak: BTK, 2015b

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 Yönetmeliğine 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.

13.06.2015

Emrah GÜNEL

ÖZGEÇMİŞ

15/12/1983 tarihinde İstanbul Kadıköy'de doğdu. İlköğrenimini Ambarlı İlkokulu'nda, orta öğrenimini Avcılar Mareşal Fevzi Çakmak İlköğretim Okulu'nda ve lise öğrenimini Avcılar Süleyman Nazif Lisesi'nde tamamladı. 2008 yılında Hacettepe Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. 2015 yılında Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Hukuku'nda yüksek lisansını tamamladı. Halen Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Adli Bilimler Ana Bilim Dalı'nda doktora yapmaktadır. 2008-2009 yılları arasında özel bir firmada yazılım mühendisi olarak, 2009-2012 yılları arasında ise Türkiye Radyo ve Televizyon Kurumu Bilgi Teknolojileri Dairesi'nde mühendis olarak çalıştı. 2012 yılı Ocak ayında Bilişim Uzman Yardımcısı olarak çalışmaya başladığı Bilgi Teknolojileri ve İletişim Kurumu'nda halen Bilgi Teknolojileri Dairesi'nde görev yapmaktadır.