T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

ELEKTRONİK BELGELERİN ARŞİVLENMESİ VE ERİŞİM

Doktora Tezi

Cengiz AYDIN

Ankara-2010

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

ELEKTRONİK BELGELERİN ARŞİVLENMESİ VE ERİŞİM

Doktora Tezi

Cengiz AYDIN

Tez Danışmanı
Doç.Dr. Fahrettin ÖZDEMİRCİ

Ankara-2010

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLGİ VE BELGE YÖNETİMİ ANABİLİM DALI

ELEKTRONİK BELGELERİN ARŞİVLENMESİ VE ERİŞİM

Doktora Tezi

Tez Danışmanı : Doç.Dr. Fahrettin ÖZDEMİRCİ

Tez Jürisi Üyeleri

Adı ve Soyadı	**İmzası**
Doç.Dr. Fahrettin ÖZDEMİRCİ	
Prof.Dr. Fatoş SUBAŞIOĞLU	
Doç.Dr. Sacit ARSLANTEKİN	
Doç.Dr. Şenol DURGUN	
Doç.Dr. Özlem BAYRAM	

Tez Sınavı Tarihi: 13/08/2010

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim.(22/07/2010)

Cengiz AYDIN

ÖNSÖZ

Bilgi teknolojilerinde yaşanan hızlı ilerleme belge yönetim yaklaşımlarında önemli değişikliklere sebep olmuştur. Bu değişime paralel olarak kurumlar artık belgelerini yoğun bir şekil elektronik ortamda üretmekte ve yönetmektedirler. Elektronik belgelerin yönetimi açısından en öneli konu elektronik belgelerin arşivlenmesi ve buna paralel olarak etkin ve hızlı erişiminin sağlanmasıdır. Bu yaklaşımla tez konusu "Elektronik Belgelerin Arşivlenmesi ve Erişim" olarak belirlenmiştir. Bu tez çalışmamsıyla kurumların elektronik belgeleri arşivlemede hangi hususları göz önünde bulundurması gerektiği ve erişim açısından nelerin öncelikle yerine getirilmesinin bir zorunluluk olduğu noktasında yol gösterici referans kaynağı oluşturulmaya çalışılmıştır. Konunun teknolojik boyutu sürekli değişen ve gelişen bir süreç olduğu için mevcut yaklaşımlar çerçevesinde çıkarımlarda bulunulmuştur. Ancak uzmanlık gerektiren bilgi teknolojileri konusunda detaya girilmemiştir. Çünkü konunun teknolojik boyutu, ayrıntıda bilgi teknolojileri uzmanlarıyla birlikte değerlendirilmesi gerekmektedir. Bu bağlamda önerilen teknolojik çözümlerin boyutu uygulamada değerlendirilmesi gereken konular arasında yer almaktadır. Bu çerçevede mesleki bir bakış açısıyla arşivleme ve erişim konusunda uygun yaklaşımlar ortaya konulmaya çalışılmıştır. Bu tez çalışmasının, kurum ve kuruluşların elektronik belge yönetimi kapsamında arşivleme ve erişim çalışma ve uygulamalarında faydalanacakları bir başvuru kaynağı olması amaçlanmıştır.

Tez çalışmam sırasında beni yönlendiren, değerli zamanlarını ayırarak bu eserin ortaya çıkmasında desteklerini esirgemeyen danışmam hocam Doç.Dr. Fahrettin Özdemirci'ye şükranlarını sunuyorum. Ayrıca tez izleme komitesinde bulunarak eserin ortaya çıkmasında katkı sağlayan değerli hocalarım Doç.Dr. Sacit Arslantekin ve Doç.Dr. Şenol Durgun'a teşekkürlerimi sunuyorum

Son olarak, bu çalışma sırasında ve hayatımın her safhasında desteklerini sürekli yanımda hissettiğim ve başarılı olmam için her türlü fedakârlığı yapan çok değerli anne ve babama sonsuz teşekkür ediyor ve bu çalışmamı onlara ithaf ediyorum.

Ankara, Temmuz 2010 Cengiz AYDIN

İÇİNDEKİLER

KISALTMALAR

AAA : Açık Anahtar Altyapısı
ARMA : American Records Management Association
ASCII : American Standard Code for Information Interchange
ASLIB : Association of Special Libraries and Information
ASP : Active Server Pages
BM : Birleşmiş Milletler
BSI : British Standards Institute
CAdES : CMS Advanced Electronic Signatures
CD : Compact Disk
CD-R : Compact Disk-Recordable
CD-ROM : Compact Disk-Read Only Memory
CD-RW : Compact Disk-Rewritable
CMS : Cryptographic Message Syntax
CRL : Certificate Revocation List
DAS : Direct Attached Storage
DES : Data Encryption Standard
DPC : The Digital Preservation Coalition
DPE : Digital Preservation Europe
DPT : Devlet Planlama Teşkilatı
DSA : Digital Signature Algorithm
DVD : Digital Versatile Disk
DVD-R : Digital Versatile Disk-Recordable
DVD-RAM : Digital Versatile Disk-Random Access Memory
DVD-ROM : Digital Versatile Disk-Read Only Memory
EBCDIC : Extended Binary Coded Decimal Interchange Code
EBYS : Elektronik Belge Yönetim Sistemi
ECSP : Electronic Certificate Service Provider
ES-A : Archival E-signature
ESHS : Elektronik Sertifika Hizmet Sağlayıcıları
FIPS : Federal Information Processing Standards

FTP **:** File Transfer Protocol

GB **:** Giga Bayt

HTML **:** Hyper Text MarkUp Language

HTTP **:** Hyper Text Transfer Protocol

IEC : International Electrotechnical Commission

ICA **:** International Council on Archives

ICR **:** Intelligent Character Recognition

IDE **:** Integrated Drive Electronics

INTERPARES: International Research on Permanent Authentic Records in Electronic Systems

IP **:** Internet Protocol

ISAD (G) **:** General International Standard Archival Description

ISO **:** International Standard Organization

IT **:** Information Technology

ITU **:** International Telecommunications Union

KB **:** Kilo Bayt

LAN **:** Local Area Network

MAC : Message Authentication Code

MAN **:** Metropolitan Area Network

MB **:** Mega Bayt

MM ESHS **:** Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı

MoReq : Model Requirements for the Management of Electronic Records

NARA **:** National Archives and Records Administration

NAS : Network Attached Storage

NIST **:** The National Institute of Standards and Technology

OCR **:** Optical Character Recognition

OECD **:** Organization for Economic Co-Operation and Development

OMR **:** Optical Mark Recognition

PC **:** Personal Computer

PDF **:** Portable Document Format

PKI **:** Public Key Infrastructure

RAID **:** Redundant Array of Independent Disk

RAM **:** Random Access Memory

RTF **:** Rich Text Format

SAA **:** Society of American Archivist

SAN : Storage Area Network

SCSI **:** Small Computer System Interface

SGLM **:** Standard Generalized Markup Language

SHA : Secure Hash Algorithm

SLL **:** Secure Socket Layer

SMTP **:** Simple Mail Transfer Protocol

TBD : Türkiye Bilişim Derneği

TCP **:** Transmission Control Protocol

TK **:** Telekominikasyon Kurumu

TODAİE : Türkiye ve Orta Doğu Amme İdaresi Enstitüsü

TSE : Türk Standartları Enstitüsü

TÜBİTAK **:** Türkiye Bilimsel Teknik Araştırma Kurumu

UEKAE **:** Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

UK **:** United Kingdom

UNCITRAL **:** United Nations Commission on International Trade Law

URL **:** Universal Resource Locator

USA : United States of America

USB **:** Universal Serial Bus

VCD **:** Video Compact Disk

VPN **:** Virtual Private Network

VTL **:** Virtual Tape Library

WAN **:** Wide Area Network

WORM **:** Write Once Read Many

XAdES **:** XML Advanced Electronic Signatures

XML **:** Extensible Markup Language

XPS **:** XML Paper Specification

TABLOLAR ve ŞEKİLLER

1. BÖLÜM
GİRİŞ

1.1.Konunun Önemi

Elektronik belgeler, genel olarak bilgisayar teknolojilerine dayalı bir yapı içerisinde üretilen, işlenen ve arşivlenen belgelerdir. Elektronik belge yönetimi de bu tür belgelerin üretimiyle birlikte tüm süreçlerinin yönetilmesini ifade eder. Elektronik belgelerin yönetiminin herhangi bir aşamasında oluşabilecek olumsuzluklar, belge yönetim süreçlerini olumsuz etkileyecek ve özellikle arşivleme ve erişim sisteminin sağlıklı işlememesi sebebiyle yönetimde doğru bilgilere hızlı bir biçimde erişimi engelleyerek yöneticilerin karar almalarında telafisi mümkün olmayan birtakım olumsuzlukların yaşanmasına neden olacaktır. Bu tip sorunlar hiç kuşku yok ki iyi bir şekilde yönetilmeyen kâğıt belge yönetim sistemlerinde de olmakta, ancak bu elektronik belgelerde daha ciddi sorunlara yol açmaktadır. Elektronik belgeler, kâğıt belgelerde olduğu gibi üretiminden arşivlenmesine ve imhasına kadar iyi bir yönetim gerektirir. Elektronik belge yönetimi prensipleri kâğıt belgelerin yönetiminden belgenin kayıt edildiği ortam özellikleri nedeniyle farklılık gösterir. Tek başına bu farklılık bile belgenin varlığını sürdürmesi açısından yeni yaklaşımların dikkate alınmasını gerektirir.

Elektronik belgelerin bulunduğu ortam gereği arşivlenmesi ve erişimi kâğıt belgelerden farklılıklar içerir. Bu farklılıklar elektronik belge yönetim sistemde dikkate alınmalı ve belgenin üretimi ile birlikte arşivleme yöntemleri, saklama süreleri belirlenmeli, güvenli erişim ve güncellemeyle ilgili konularda yetkilendirmeler yapılmalıdır. Kısaca bu çalışmalar elektronik belgelerin üretilmesine başlanmadan önce, e-belge yönetim sistemi oluşturma aşamasında planlanmalıdır.

Elektronik belgelerin arşivlenmesi konusu en önemli belge yönetim konusudur. İyi oluşturulmuş bir arşivleme sistemi beraberinde iyi işleyen bir elektronik belge yönetim sisteminin oluşmasını sağlar. Elektronik belgeler ihtiyaçları karşılamak için geri iletilebilir ve ulaşılabilir olmak zorundadır. Teknolojik altyapının ve e-belge yönetim modellemesinin yetersiz olduğu kurumlarda e-belge üretmek ve e-arşiv oluşturmaya çalışmak kurumun kendi bilgi birikimine erişimini sekteye uğratmakla kalmayıp imkânsız hale getirebilmektedir.

Erişimin sürekli olmadığı yerlerde sürekli bir bilgi akışından da söz edilemeyeceğine göre, erişim bilginin varlığını ortaya koyan temel unsur olarak karşımıza çıkmaktadır. Bu bağlamda etkin bir erişim yapılanması olmadan sağlıklı bir arşivlemenin varlığından söz etmek de mümkün değildir.

Belgelere hızlı, kolay ve güvenli erişim; hızlı, kolay, izlenebilir dağıtım ve bilgi güvenliği; kâğıtsız ortam, elektronik ortamda iş akışı ve onay ile zamandan tasarruf elektronik arşivleme ve erişim sisteminin sağlayacağı öncelikli getiriler arasında yer almaktadır. Bu çerçevede, kurumsal anlamda etkin bir arşivleme ve erişim büyük önem taşımaktadır. Tez çalışması, elektronik belgelerin arşivlemesi ve bu belgelere erişimin sağlanması noktalarında ortaya konulan yaklaşım ve önerilerle, kurum ve kuruluşların e-belge yönetim uygulamalarında arşivleme ve erişim bağlamında izlemeleri gereken yöntemler açısından yol gösterici nitelik taşıyacaktır.

1.2. Araştırmanın Amacı ve Hipotez

Elektronik belge yönetimi, bilgi teknolojilerindeki gelişmeler çerçevesinde ortaya çıkan ve bu gelişmelere paralel olarak kurumsal yapıya yansıyan bir yönetim aktivitesidir. Özellikle bilgisayar teknolojisiyle birlikte kurumlar artık yoğun bir şekilde belgelerini elektronik ortamda üretmekte ve teknolojinin ön gördüğü ağ sistemi içinde iletimini yapmaktadır. Hızlı gelişme gösteren bilgi teknolojileri belgelerin elektronik ortamda yoğun bir şekilde üretilmesini, arşivlenmesini ve erişiminin sağlanmasını da gerekli kılmaktadır. Organizasyonlar bu yeni durum karşısında etkin ve verimli çözümler üretememekte, elektronik belgeleri arşivlemede ve erişimini sağlamakta ciddi zorluklar yaşamaktadır. Elektronik belgelerin kâğıt ortamdaki belgelere göre farklı bir yapıya sahip olmaları nedeniyle, geleneksel belge yönetim anlayışıyla yönetilmesi mümkün olamamakta ve dolayısıyla elektronik belgeler için farklı yaklaşım ve yöntemlerin kullanılması gerekmektedir. Ayrıca kurumsal belgelerin bütünsel bir yapı içerisinde etkin erişimin sağlanması açısından kâğıt ortamda oluşturulmuş belgelerinde dijitalleştirilerek elektronik belge yönetim sistemine entegre edilmesi gerekmektedir. Elektronik ortamda üretilen belgeler ile elektronik ortama aktarılan belgelerin bir bütün içinde arşivlenebilmesi ve erişim sistemlerinin oluşturulması kurumların çözmeye çalıştıkları en güncel sorunlar olarak karşımıza çıkmaktadır.

Bu çerçevede tezin amacı kurum ve kuruluşların elektronik ortamda üretilen belgeler ile dijitalleştirilmek suretiyle elektronik ortama aktarılan kâğıt belgelerin arşivlenmesinde ve etkin erişimlerinin sağlanması noktasında bir yol haritası çizmek, elektronik belgelerin arşivlenmesi ve erişiminin sağlanması noktasında uygun çözümler ortaya koymaktır.

Kurum ve kuruluşlar elektronik belgelerin nasıl yönetileceği konusunda yoğun bir bilgiye ihtiyaç duymaktadır. Bu ihtiyaç değişik çalışmalarla giderilmekle birlikte, değişen bilgi teknolojilerine paralel olarak özellikle doğrudan elektronik belgelerin arşivlenmesi ve erişime yönelik çözüm önerileri üretmek önemli bir gereklilik olarak görülmektedir. Arşivleme açısında hangi ortam uygundur? Hangi formatta arşivlenmesi erişim açısından en uygundur? Kâğıt belgelerin dijitalleştirme aşamasında hangi hususlara dikkat edilmelidir? Sistemin alt yapısı için yazılım ve donanım unsurları neler olmalıdır? Elektronik belgelere erişim nasıl sağlanmalıdır? Erişim kontrolü ve güvenlik nasıl tesis edilmelidir? Erişim hakları ve doğrulama sistemleri nasıl oluşturulmalıdır? Kısaca oluşturulan elektronik belge yönetim sisteminde arşivleme ve erişim unsurları ne şekilde planlanmalı ve uygulanmalı gibi sorular önemle cevap arana sorular olarak karşımıza çıkmaktadır. Bu tez çalışmasında bu sorulara cevap aranacaktır.

Bu çerçevede araştırmanın hipotezleri şöyledir;

- Kurum ve kuruluşlar, teknolojik gelişmelerin dikkate alındığı, etkin arşivleme ve erişime sahip elektronik belge yönetim sistemine gereksinim duymaktadır.

- Kağıt belgelerin dijital ortama aktarılması ve elektronik belge yönetim sisteminde oluşturulan elektronik belgelerle birlikte entegre bir yapıda yönetilmesi için tüm belgelerin bütünsel bir yapıda arşivlenmesi ve erişiminin sağlanması gerekmektedir. Bu bağlamda standartlara uygun modeller ortaya koyan ve öneren tüm süreçleri içeren yol gösterici başvuru niteliğinde kılavuz kaynaklara ihtiyaç duyulmaktadır.

Bu yaklaşım ve öngörü ile kurum ve kuruluşların elektronik ortamda üretilen belgeler ile dijitalleştirilmek suretiyle elektronik ortama aktarılan kâğıt belgelerin arşivlenmesinde ve etkin erişimlerinin sağlanması sürecinde izlenmesi gereken yol haritası ortaya konulmuş olacaktır.

1.3. Araştırmanın Kapsamı

Tezde elektronik belgelerin arşivlenmesi ve erişimi üzerinde durulmaktadır. Tez, elektronik belgelerin arşivleme teknikleri, arşivleme ortamları, kâğıt belgelerin dijitalleştirilmesi, elektronik belgelere erişim, bu bağlamda gerekli bilgi teknolojileri altyapısının nasıl olması gerektiği çerçevesinde oluşturulmuştur. Tez çalışmasında arşivleme ve erişim konuları ele alınmakla birlikte konuya temel oluşturulması açısından elektronik belge yönetim sisteminin temel unsurlarına verilmiştir. Arşivleme ve erişim konusu herhangi bir kurum ya da kuruluş dikkate alınarak ele alınmamıştır, her kurum ya da kuruluşun kendi kurumsal yapısına göre referans alıp kullanabileceği bir çerçevede ele alınıp işlenmiştir.

1.4. Araştırma Yöntemleri

Araştırma konusu ile ilgili yerli ve yabancı kaynakları kapsayan geniş bir literatür çalışması yapılarak elektronik belgelerde arşivleme ve erişim konusu tüm boyutlarıyla değerlendirilmiştir. Bu çerçevede literatüre yansımış uygulamalar üzerinde karşılaştırmalar yapılarak en doğru çözümler ortaya konulmaya çalışılmıştır. Çalışmada geçen, tanım, açıklama ve değerlendirilmelerin yapılmasında belgesel tarama yöntemi ve betimleme yöntemlerinden yararlanılmıştır. Belgesel tarama yöntemi; var olan bilgi kaynaklarının sistemli şekilde incelenmesi yolu ile veri toplanması yöntemidir. Bu yöntem, yazılı belgeler çerçevesinde belirli bir amaca dönük olarak kaynakları bulma, okuma, not alma ve değerlendirme işlemlerini kapsar (Karasar, 1991:183). Betimleme yöntemi ise, olayların, objelerin, varlıkların, kurumların, grupların, çeşitli alanların ne olduğunun betimlenmeye ve açıklamaya çalışılmasıdır (Kaptan, 1995:59).

1.5. Araştırma Düzeni

Araştırma altı bölümden oluşmaktadır.

Girişin yer aldığı birinci bölümde, konunun önemi, araştırmanın amacı ve hipotezi, araştırmanın kapsamı, araştırma yöntemleri ile tez çalışmasında temel olarak kullanılan kaynaklar yer almaktadır.

İkinci bölümde, sonraki bölümlere temel oluşturması açısından elektronik belge yönetimiyle ilgi temel hususlar ele alınmıştır

Üçüncü bölümde, belgelerin elektronik ortamda üretilmesi ve kâğıt belgelerin elektronik ortama aktarılmasıyla ilgili hususlara değinilmiştir.

Dördüncü bölümde, elektronik belgelerin sağlıklı arşivlenmesi için gerekli hususlar ayrıntılı bir şekilde ele alınmış ve bağlantılı olarak elektronik belgelerin gerçekliği ve bütünlüğünün korunması ile ilgili konular açıklanmıştır.

Beşinci bölümde, elektronik belgelere erişim ile ilgili hususlar ele alınmış, etkin erişimin sağlayacak konular değerlendirilmiştir.

Altıncı bölümde, araştırma konusu ile ilgili genel sonuç ve yapılması gerekenler noktasında öneriler bulunmaktadır.

1.6. Kaynaklar

Konu ile ilgili literatür çalışmasında öncelikle aşağıdaki kaynaklardan yararlanılmıştır;

Açık Erişim Sistemleri ve Internet Kaynakları

- Directory of Open Access Journals
- E-prints in in Library and Information Science
- Google arama motoru
- Konu Uzmanlarının Web Sayfaları
- American Records Management Association (ARMA) (Web Sayfası)
- International Council on Archives (ICA) (Web Sayfası)
- Society of American Archivist (SAA) (Web Sayfası)
- The Digital Preservation Coalition (DPC) (Web Sayfası)
- Digital Preservation Europe(DPE) (Web Sayfası)
- InterPARES (Web Sayfası)
- International Standard Organization (ISO) (Web Sayfası)

Kataloglar

- Milli Kütüphane Kataloğu
- YÖK Tez Kataloğu

- Universite ve Araştırma Kütüphaneleri Kataloğu

Veri Tabanları

- EbscoHost Veri Tabanı
- ProQuest Central Veritabanı
- Ebrary Elektronik Kitap Veritabanı
- ProQuest Tez Veritabanı (TAM METİN)

Türkçe Dergiler

- Türk Kütüphaneciliği Dergisi
- Bilgi Dünyası Dergisi
- Arşiv Araştırmaları Dergisi

İngilizce Dergiler

- Information Management Journal
- D-Lib Magazine
- Records Management Journal
- Records Management Quarterly
- Information Syetem Management Journal
- Journal of the Society of Archivists
- Bulletin of the American Society for Information Science
- HEP Libraries Webzine
- Archival Science
- Government Information Quarterly

1.7. Terminoloji

Araştırmada yaygın olarak kullanılan ve belirtilen bazı hususların daha anlaşılır hale gelmesi açısından aşağıdaki terminoloji oluşturulmuştur.

Arşiv: Arşivsel değeri olan belgelerin muhafaza edildiği yer ya da söz konusu belgelere bakan kurum.

Ayıklama: Belgelerin saklama süreleri ve arşivsel değerleri çerçevesinde yaşam evresindeki diğer aşamaya geçmesi ya da imhasına ilişkin değerlendirmelerin yapıldığı süreçtir

Belge Yaşam Döngüsü: Belgelerin üretiminden imhasına kadar olan süreçteki aşamaların bütünüdür.

Belge: Kurumsal resmi iş aktiviteleri sonucunda oluşturulan ve her türlü iletişim ağıyla akan kaydedilmiş bilgidir.

Bütünlük: Belgenin tam olması ve kayıplar, tahrifat ve bozulma dolayısıyla üzerinde değişiklik olmaması özelliğidir.

Dijitalleştirme (Sayısallaştırma): Analog ortamda bulunan materyallerin fotoğraf ya da tarayıcılar aracılığıyla elektronik ortama aktarılması işlemidir. Tezde aynı anlamdaki dijitalleştirme ve sayısallaştırma terimlerinden dijitalleştirme terimi kullanımda tercih edilmiştir.

Doküman: Birtakım ortamlarda bulunan ancak resmi belge niteliği olmayan bilgi ya da verilerdir.

Düzenleme: Belgelerin belli bir sistem içinde sınıflandırması işlemidir.

Elektronik Belge: Elektronik araçlar vasıtasıyla üretilen, iletilen ve muhafaza edilen belgelerdir.

Envanter: Arşiv fonları meydana getiren belgelerin, sistematik bir şekilde hazırlanan sayım ve döküm listesidir.

Erişim: Belgelerin kullanılması ve geri iletimine hak ve yetkisi olma durumudur.

Felaket Kurtarma: Bir felaket sonrasında elektronik belge yönetim sisteminin eski haline getirilmesi için yapılan işlemledir.

Gerçeklik: Belgenin sahte olmaması, tahrif edilmemiş olması ve bütün unsurlarıyla delisel vasfı olması anlamına gelir.

İmha: Belgelerin daimi olarak tasfiyesini içine alan süreç

Muhafaza (Saklama): Zaman içinde gerçek belgelerin teknik ve entellektüel özelliklerini varlığını sürdürmesini sağlamaya yönelik işlemler ve faaliyetlerdir.

Provenans: Belgelerin işlem gördüğü tarihteki oluşum ve ilişkisel biçimlerine düzenlenmesi yöntemidir.

Saklama planı: Belgelerin, son işlem tarihlerinden sonra, birim ve kurum arşivlerinde ne kadar süre ile saklanacaklarına, bu süreler sonunda hangi işlemlere tâbi tutulacaklarına dair değerlendirmelerin ifade eden planlar

Tanımlama: Belgelerin gerekli üst veri elemanlarıyla niteleme işleminin yapılmasıdır.

2. BÖLÜM
ELEKTRONİK BELGE YÖNETİMİ

2.1. Belge ve Elektronik Belge Kavramı

Belge bulunduğu ortama ve türüne bakılmaksızın kurum içindeki her türlü iletişim ağıyla akan bilgidir. Belgeler iş süreçlerine ve aktivitelerine delil sağlayan önemli unsurlardır. Neyin ne zaman, nasıl ve kim tarafından yapıldığıyla ilgili bilgileri içerir. Bir başka deyişle belge; faaliyetlerin yapıldığı, sözlerin ve yükümlülüklerin yerine getirildiği konularda kişi ve kurumların ispat edebilmelerini sağlar (University of Melbourne, 2002). Bu özellikleriyle kurumsal yapının vazgeçilmez unsurlarıdırlar.

Kamu ve özel sektör belgelerinin yönetiminde başarılı uygulamaları gerçekleştirmeyi amaçlayan ve belge yönetiminde dönüm noktası olarak nitelenen ISO 15489 Uluslararası Belge Yönetim Standardı "belge"'yi İşlemlerin veya yasal zorunlulukların yerine getirilmesinde bir kişi veya organizasyon tarafından enformasyon ve delil olarak üretilen, kabul edilen (alınan) ve korunan enformasyon olarak tanımlamaktadır (Özdemirci, 2004: 193). Belge, kurumsal ya da kişisel aktivitenin tamamlanmasında ya da yürütülmesinde ve kabulünde üretilen ya da alınan belirli miktardaki bilgidir. Belge, faaliyetlerin delilini sağlamak için gerekli ve yeterli içerik, bağlam ve yapıyı ihtiva eder. Bu geçici değildir; yani, uzun, orta ve kısa dönem muhafaza için değerli bilgiler içerirler. Belgeler, gerek kurum içinde ve gerekse kurum dışında meclise, mahkemeye ve kamuoyuna karşı sorumlulukların vazgeçilmez öğeleridir. Belgeler, belli durumlarda tanımlanmış sosyal, örgütsel, yasal ya da ahlaki zorunlulukların, sorumlu kişiler ya da kurumlarca karşılanıp karşılanmadığını gösterir (Public Record Office, 1999:13).

Belge kavramı, bilgi teknolojilerindeki gelişmelere paralel olarak kavramsal ve yapı olarak doğal bir değişime uğramıştır. Bilginin yazıya dökülmesinde birincil araçlar kil tabletler iken, belgeler kilden yapılmış ortamlarda bulunuyordu. Kâğıt ve mürekkebin icadıyla, belgeler kâğıt ortamlarda oluşmaya başladı. Şimdi ise elektronik iletişim araçlarının icadı ve bilgi teknolojilerindeki gelişmelere paralel olarak, belgeler elektronik ortamda

oluşmaya başladı. Belgeler, kurumsal yapı içinden dışına doğru ya da tam tersi bir şekilde değişik iletişim araçları vasıtasıyla bir akış gösterirler (Gill, 1998: 5). Bu yüzden iletişim ağı içinde akış gösteren iş süreçleri sonucunda oluşan her türlü bilgi saklandığı ortama bakılmaksızın belge özelliğindedir. Bu çerçevede, bilgi teknolojilerindeki gelişmelere paralel olarak elektronik belge yoğun bir şekilde üretilen belge türü olmaktadır.

Birçok belge yönetim programında, belge yıllar öncesine dayanan bir kavramsal tanımlama ve faraziyeler çerçevesinde yürütülmekteydi. Bu tanımlama şöyleydi; "belge kurumun fonksiyonları gereği ürettiği fiziksel yapısı ve şekline bakılmaksızın kayıtlı bilgi demektir" (Dearstyne, 1999:8). Gelişen bilgi teknolojileriyle birlikte yeni tanımlamalar ortaya konulmaya başlanmıştır. En ileri tanımlamalardan biri 1997 yılında düzenlenen uluslar arası ICA Arşiv Konseyinde yapılan tanımlamadır; "kayıtlı bilginin yapısı ve saklandığı ortama bakılmaksızın üretilmesi ya da alınması, iletilmesi ya da kurumsal ya da kişisel bir aktivitenin tamamlanması ve bu aktivitenin delilini sağlayacak yapısal yeterlilik, içerik ve metni kapsamaktadır" (Dearstyne, 1999:8). Bu tanımda da daha önce yapılan tanımlamalarda olduğu gibi saklandığı ortama bakılmaksızın vurgusu yapılmaktadır. Bu vurgu özellikle gelişen bilgi teknolojilerinin ürettiği değişik ortamlarda bulunan ve yönetilmesi gereken belge türlerini yani elektronik belgeleri işaret etmektedir. Bu çerçevede belge kavramının yansıttığı yeni tanımlamaların test edilmesi ve geliştirilmesi gerekmektedir. Kavramsal değişimler ve yeni yaklaşımlar, görüşler ve yeni ürünler sağlamaktadır. Elektronik belge yönetimi; bu kavramsal değişim ve tanımlamaları zorunlu kılan, teknolojik ilerlemeyle paralel oluşan ve belge yönetimindeki değişimini yansıtan en önemli olgudur.

Belge kavramı tanımı içerisinde yer alan saklandığı ortama bakılmaksızın ibaresi nedeniyle günümüzde geçerliliğini sürdürmekle birlikte gelişen bilgi teknolojilerinin ortaya çıkardığı e-belgeler, belge kavramına yeni bir boyut kazandırmıştır. Yukarda bahsedilen ifadenin içeriğinin neyi kapsadığı ya da neyi tanımladığı bilgi teknolojilerindeki gelişmelerle birlikte aydınlığa kavuşmuş, belge kavramı yeni bir boyut kazanmıştır. Artık kurumsal yapıda belge yönetimi deyince sadece kâğıt belgeler söz konusu olmamakta, değişik formatlarda bulunabilen elektronik belgeler de anlaşılmaktadır. Bir başka ifade ile belge deyince kurumsal yapı içinde iş süreçleri sonucunda her türlü ortamda üretilen belge anlaşılmaktadır. Bu açıdan bilgi teknolojilerindeki gelişmelere paralel olarak belge kavramını elektronik bir anlayış içinde değerlendirme, tanımlama ve bu çerçevede yönetme zorunluluğu meydana gelmiştir. Bu çerçevede elektronik belge şöyle tanımlanabilir; bilgisayar ya da diğer elektronik cihazlar

aracılığıyla elektronik ortamda iş süreçleri sonucunda üretilen, arşivlenen, erişilen, iletilen ve imha edilen her türlü belgeye elektronik belge denir.

Elektronik belge, kurumun iş ve işlemleriyle ilgili olarak elektronik ortamdaki kayıtlı bilgileri içerir. Elektronik belge için tek kriter, kâğıt belgenin aksine bilginin makine tarafından okunabilir ortamda kaydedilmesi ve depolanmasıdır. Elektronik ortam, bilginin metin, resim ve ses gibi farklı formatlarda depolanması amacıyla kullanılır. Elektronik belgeyi tanımlamadan önce, bağlantılı bazı kavramları tanımlamak gereklidir. Bunlar veri, bilgi ve belge kavramlarıdır. Veri, işlenmemiş gerçeklerdir. Bilgi, düzenlenmiş anlamlı veridir. Belge, fiziksel biçim ve özelliğine bakılmaksızın kayıtlı bilgiyi ifade eder. Elektronik belge ise, bilginin okunması ve iletimi için elektronik sistem gerektiren fiziksel biçim ve özelliğine bakılmaksızın iş süreçleri sonucunda elektronik ortamda kaydedilmiş bilgidir (Records Management Institute, 2000:2).

Bütün kurumlar, sorumluluk alanlarıyla ile ilgili talepleri karşılamak için kararlar ve işlemlerle ilgili belgeleri saklamaya ihtiyaç duyarlar. Kamu sektöründe, elektronik belgelerin kamu belge mevzuatlarına uygunluğa ek olarak, belirli sorumluluklarla ilgili gereklilikler de bulunmaktadır. Belge, bir iş ya da işlemin delili olmak yanında sorumluluğun ne olduğunu da gösterir. Belgeler, kamudaki günlük iş aktiviteleri sonucunda ortaya çıkan resmi belge olmaları dolayısıyla, değerlerini muhafazasını sağlamak için üretilmesine, yönetilmesine ve korunmasına fonksiyonel ilişkilerle yapılandırılmış bir sistem içinde ihtiyaç bulunmaktadır. Bütün bu hususlar elektronik belge için de aynı olacak geçerli prensiplerdir.

Elektronik belgeler, uygulama yazılımları ve bilgisayar kullanımıyla dijital ortamda üretilen ve depolanan bilgisel ya da veri dosyalarıdır. Değişik manyetik ve optik depolama araçlarında depolanan bilgisayar yazılım ürünleri vasıtasıyla oluşturulurlar. Bir başka ifade ile elektronik belge " elektronik ortamda belgenin üretimi, düzenlemesi, gönderilmesi, alınması ya da depolanması olarak tanımlanabilir. Genellikle bu tanımlama, depolama ortamının tek ya da bütünleşik bir yapıda olmasına bakılmaksızın bütün elektronik belge sisteminde uygulanır (Calrim, 2002: 3).

Elektronik belgelerin, birimlerin bilgi ve sorumluluklarıyla ilgili ihtiyaçları karşılamak ve elektronik arşivlerde uzun dönem muhafaza edilmesini sağlamak aramacıyla bilgisayar sistemleri araçlarını uygulamaya konulması gerekmektedir. Elektronik belgeler, kâğıt ortama

göre daha kırılgan bir yapıdadır. Elektronik belgelerin elde edilmesi ve korunmasıyla ilgi olarak uygun faaliyetlerin yerine getirilmesi gereklidir (Public Record Office, 1999:11). Kamu kurumları, dosyaya giden her kayıt belgedir diye tanımlanan kayıtlı dosya kuralına uygun hareket etmelidir. E-belgedeki kayıtlı bilgi, kurumsal bilgi kaynağını meydana getirir; en önemlisi bu kişisel olmaktan çok kurumsal bir kaynaktır. Bu kapsamda aşağıdaki öğeler önemlidir;

- *İçerik:* E-belgenin konusunun ne olduğunu ifade eder.
- *Yapı:* E-belge bölümlerinin etiketlenmesi, tanımlanması amacıyla başlıkların ve diğer araçların kullanımı ve içerik anlamının bir bölümünü taşımak amacıyla görsel vurguların kullanımıdır.
- *Bağlam:* E-belgenin üretildiği ve kullanıldığı ortamdır. Yani, belgenin, belge gruplarıyla nasıl ilişkilendirildiğiyle ilgili durumdur.

Bu öğeler bir bütün olarak e-belgenin, belge niteliğinin tam olarak anlaşılmasına yardımcı olan unsurlarıdır. Bu öğelerden birinin eksik olması, e-belgenin amaçlanan niteliğinin tam oluşmamasına sebep olabilir.

Elektronik belgeler elektronik araçlar vasıtasıyla üretilen, iletilen ve muhafaza edilen belgelerdir. Elektronik belge ile elektronik doküman aynı değildir. Elektronik bir doküman, elektronik belge hüviyetini ancak kurumsal işlemlerde kullanıldığında ve bu işlemlerin delili olarak saklandığında kazanır. Yani resmi bir geçerliliği olmadığı sürece bu elektronik bir dokümandır. Örneğin, kelime işlemci programı kullanılarak yazılan resmi bir yazı, bütün onay süreçleri tamamlanana kadar elektronik doküman niteliğindedir. Onay süreçleri tamamlandığında ise elektronik belge hüviyetini kazanır. Doküman ise sistem içinde saklanabilir ve bir sonraki resmi yazıya temel oluşturmak için kullanılabilir. Ancak elektronik belge resmi bir nitelik kazandığı için değiştirilemez özelliktedir. Bu açıdan farklılık gösterir. Bu çerçevede elektronik belge, kurumsal, yasal ve arşivsel gereklilikler bulunduğu sürece geçerli, erişilebilir ve geri iletilebilir olmak zorundadır.

Elektronik belgeyi, kâğıt belgeden ayıran birçok karakteristik özellik vardır. Bunlar şöyle sıralanabilir;

- Kolaylıkla üzerinde yazma, silme ya da sistemdeki sorunlar nedeniyle erişilemez olabilir,
- Ortamdan bağımsızıdır
- Yazılım ve donanıma bağımlıdır
- Rastgele yerleştirilir
- Kolay bir şekilde taklit edilebilir, çoğaltılabilir
- Dayanıksız ortamlarda muhafaza edilmeleri dolayısıyla kırılgandırlar

Elektronik belgeler, kâğıt belgelerde olduğu gibi düzenleme işlemi yaptıktan sonra sadece ihtiyaç duyulduğunda işlem yapılan belgeler değildir. Zaman içinde erişilebilirliğini sürdürmek için aktif bir veri yönetimi gereklidir. Elektronik belgenin muhafaza edildiği ortam hızlı bir şekilde değişmektedir. Bu sebeple, elektronik belgelere yönelik sürekli dikkat ve özen gösterilmeli ve buna yönelik teknolojik yazılım ve donanım değişiklikleri zamanında yapılmalıdır.

Elektronik ortamda bulunan belgeler, elektronik formda olmaları dolayısıyla farklı bir statüye sahip değillerdir. Ancak elektronik belgeler arşivleme ve erişim açısından diğer belgelerden farklılık gösterir. Depomla kapasiteleri artabilir, sistem çalışamaz hale gelebilir ve yazılım güncellenemeyebilir. Artık kullanılmayan işletim sistemleri ve donanımlar yaygın problemlerdir. Kâğıt belgelerin aksine, elektronik belgelerin belli bir fiziksel ilişkileri yoktur. Dosyaya konan kâğıt belgelerin aksine, elektronik belge, disk üzerinde nerde yer varsa orda depolanır. Güvenlik, gizlilik ve güvenirlilik konularının elektronik belgelerde farklı bir şekilde gerçekleştirilmesi gerekmektedir.

2.2. Elektronik Belgelerin Yaşam Döngüsü

Elektronik belge yönetiminde en önemli husus, belgenin yaşam döngüsü boyunca yönetilebilmesidir. Temel olarak elektronik belgelerin yaşam döngüsünün yönetimi kavramı, belgelerin bütünü için geçerli olan üretim, muhafaza, kullanım, ayıklama ve imha süreçlerini kapsar. Yaşam döngüsü süreçlerinin elektronik belge yönetim sisteminin bütününde uygulanmasında aşağıdaki aşamalar takip edilmelidir;

- Yeni bir sistem oluşturmak ya da mevcut sistemde değişiklikler yapmak için gerekli politika ve programların tespit edilmesi.

- Aktif kullanımdaki elektronik belgelerin cevrim içi ya da anında erişilmesi için birincil depolama ünitelerinde muhafaza edilmesi.
- Yarı aktif ya da pasif elektronik belgelerin, daha ucuz ve daha yavaş depolama ortamlarına taşınması
- Ayıklanması, imha edilmesi ya da Devlet Arşivlerine gönderilmesi gerekli elektronik belgelerin belirlenmesi.
- Etkin erişimine yönelik çözümlerin uygulanması

Belgenin yaşam döngüsü, belgenin üretilmesinden kullanılması ve saklanmasına, aktif olmayan dosyaların saklama planları, aktif dosyalara transferi ve nihai olarak imhasını içine alan süreçtir (Gill, 1998:5). Yani belgenin üretiminden imhasına kadar sürdürdüğü yaşam evresidir. Yaşam döngüsü kavramı, belgenin yaşamının herhangi bir noktasında nerede olacağı, belgenin bulunduğu ortamın ne zaman değişeceği, ne zaman ikinci nüshasının oluşacağı, değiştirileceği, pasif hale geleceğiyle ilgili konuları içerir. Yaşam döngüsü teorisi gerçekte bilgi teknolojileri biliminde olduğu gibi bilginin ve belgenin iletimi, akışı ile ilgilidir (Sanders, 1998:74). Aslında, yaşam döngüsü kavramı elektronik bilgi ağındaki akışın bir parçası olarak değil, ama belgenin bulunabileceği herhangi bir muhafaza ortamın merkezinden imhasına kadar olan kısımla ilgilidir.

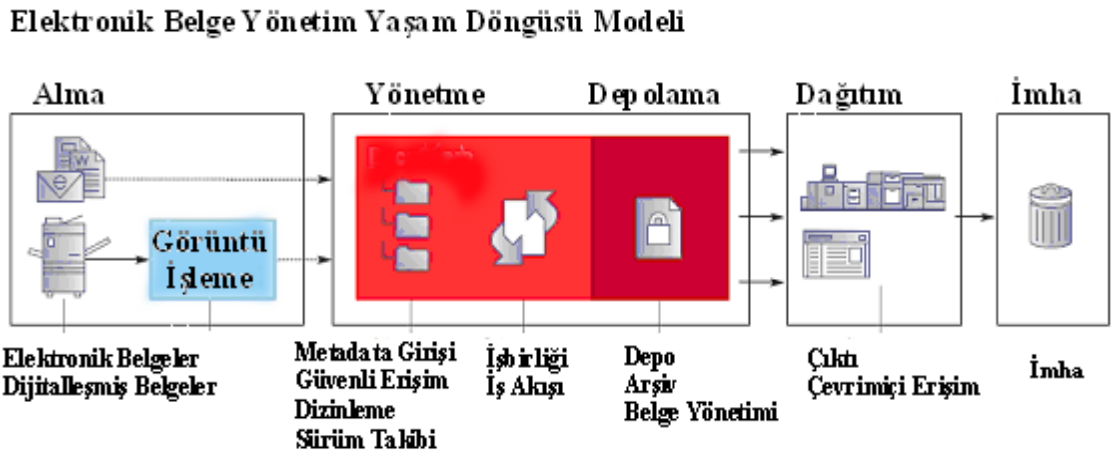
Yaşam döngüsü kavramı kâğıt belgeler için belgenin üretimi, dağıtımı, korunması, kullanılması ve imhasını içermektedir. Esasında bu tanımlamalar belge yönetiminin ta başından beri var olan bir değerlendirmedir. Ancak elektronik belge kavramının ortaya çıkmasıyla bu tanımlamaları gözden geçirmek zorunluluk haline gelmiştir. Zira bu tanımlamalar elektronik belgenin yaşam döngüsünün tam olarak karşılamamaktadır. Kâğıt belgenin yaşam döngüsü üretilmesinden itibaren başlarken, elektronik belgelerin yaşam döngüsü bilgisayara dayalı bilgi sisteminin dizayn aşamasında başlamalıdır (Kandur, 1999a:40) Bu açıdan, e-belgenin saklama süresi, imhası, sınıflandırılması ve sistem içinde akışıyla ilgili kararlar bu aşamada alınmalıdır.

Elektronik belgelerin aktif, yarı-aktif ve pasif safhalarını belirlemek oldukça zordur. Kâğıda dayalı sistemlerde belirlemek daha kolaydır. Elektronik belgelerde yarı-aktif safha gerçekte yok olur. Güvenli bir yedekleme sistemi sağlamak için elektronik belgeler ofis dışında saklanabilir. Bu durum, kâğıt belgelerin bulunduğu belge merkezleriyle benzerlik göstermektedir. Bu gibi belgeler zorunlu bir biçimde yar-aktif ya da pasif değillerdir. Belge

yöneticisi için elektronik belgelerin bir kopyasını mümkün olan en kısa zamanda elde etmek hayatidir. Çünkü elektronik belgelerin uzun süre muhafazasında önemli teknolojik sorunlar yaşanabilmektedir. Eğer yaşam döngüsü kavramı bir yönüyle kullanım sıklığıyla tanımlanıyorsa, elektronik belgelerin aynı anda aktif, yarı-aktif ve pasif safhalarda yaşamaları mümkündür (Kandur, 1999a:40). Geleneksel olarak, belgeler sık olmayan geri iletim gereksinimleriyle birlikte pasif duruma gelene kadar belge merkezinde korunurlar. Nihai olarak yasal ve fiziksel gereksinimler gereği saklama süreleri geçen e-belgeler mevcutsa, yaşam döngüsündeki son safhaya ulaşılmış demektir. Bu anlamdaki belgelerin %90-98'i fiziksel olarak imha edilir (Shepherd, 1994:41) Çok az bir belge miktarı tarihsel ve araştırma amaçlı bir değere sahiptir ve arşivde saklanmaya devam edilir.

Elektronik belgeler gerek kurum içinde ve gerekse kurum dışında üretilmiş olsun, genellikle bilgi çalışanları tarafında üretilir, alınır ve paylaşılır. Bütün yaşam döngüsü içinde elektronik belgelerin etkin yönetimi, iş sürekliliğine imkân verir, işbirliğini destekler, yasal ve idari düzenlemelere uygunluğu sağlar ve bütün maliyetlerde bir azalma oluşmasına imkân verir. Elektronik belge yönetim sistemi, belge yaşam döngüsü yönetimi ile birlikte çalışarak, kurum içinde kritik öneme sahip bilgilere ulaşmayı kolaylaştırır.

Belge yaşam döngüsü modelinde farklı yaklaşımlar olmakla birlikte, Xerox (2006:4) tarafın ortaya konulan ve genel yaklaşımlar çerçevesinde düzenlenerek şekil 1'deki halini alan elektronik belge yaşam döngüsü modeli temel aşamaları aşağıda değerlendirilmiştir;



Şekil 1. Elektronik Belgelerin Yaşam Döngüsü

- *Alma*: Belgenin kurum içinde üretilmesi ya da kurum dışından alınmasıdır. Ayrıca alınan belgeler, elektronik ya da kâğıt gibi farklı format ya da ortamlarda üretilmiş olabilir.
- *Yönetme:* Belge bir kere üretildiğinde ya da alındığında, belge hüviyeti kazanır. Ayrıca belge yönetim sistemi içinde yönetilecek, tanımlanacak ve sınıflandırılacaktır. Elektronik belge yönetim sistemi, aynı zamanda kurumun belge yönetim planını uygulayan yazılım uygulamasını da kapsar.
- *Depolama:* Belge hüviyeti kazanıldığında değiştirilmeyecek ve imha edilemeyecek güvenli bir biçimde muhafaza edilmesi önemlidir. E-belge istendiğinde ulaşılabilir ve kullanılabilir olmak zorundadır. Bunu anlamı, yeterli dizinleme işlemini belgeyi depolama sistemine teslim etmeden önce uygulanmak bir zorunluluktur. Depolama sistemi ve depolama ortamının, belgenin durumunu tehlikeye sokabilecek ortam bozukluğuna ya da kullanılmaz olmaya açık olmaması gereklidir. Depolama, büyük oranda teknolojik değişime paralel olarak belgelerin belli zaman aralıklarında bir depolama sisteminden diğer depolama sistemine aktarılmasını içerecektir. Belge yönetim sistemi buna imkân vermelidir.
- *Dağıtım(Gönderme):* Belgeler, tanımlandıktan ve güvenli bir ortamda depolandıktan sonra, kurumun normal iş akışı içinde çalışanlar için kullanıma hazır olması gerekmektedir. Bu açıdan e-belge yönetim sistemi, belgenin saklama planlarında belirtilen süreden önce silinemeyeceği ve değiştirilemeyeceğini sağlamakta önemli bir misyona sahiptir. Bu çerçevede iletim işleminin sağlıklı yürütülmesi sağlanmalıdır.
- *İmha*: Birçok kurumsal belge, belirlenen saklama planları çerçevesinde imha edilebilir. Bazı belgeler yasal saklama süreleri bittiğinde imha edilirken, bir kısmı da daha uzun süreli ya da sürekli olarak saklanacaktır. Kısaca belgelerin, saklama planlarına göre imha edilmesi büyük önem taşımaktadır. Bu imha aşaması, belge yönetim sürecinin bir parçası olarak değerlendirilmelidir

Esasında elektronik belgenin yaşam döngüsü yaşayan bir organizmayla çok benzerlik gösterir. İlk safhada belge belli standartlar ve yasal zorunluluklar gereği üretilir. İkinci safhada, birincil değerinin yüksek olduğu aktif periyoda geçer ve karar süreçlerine dahil olan kişiler tarafından aktif bir şekilde kullanılır. Bu dönem süresince, belge aktif kullanım

dolayısıyla yerinde depolanır. İkinci safhanın sonunda, belgeler için ayıklama işlemi yapılır ve saklanmasını gerektirecek bir değerlerinin olup olmadığına karar verilir. Bu durumda ya imha gerçekleşir ya da belge yarı aktif aşama olan üçüncü safhaya geçebilir. Bu safhada, belgenin kurumsal bir değeri vardır, ancak günlük karar verme süreçleri için ihtiyaç duyulacak nitelikte değildir. Sık bir geri iletim söz konusu olmadığı için kurum dışı depolama ortamlarında muhafaza edilir. Üçüncü safhanın sonunda, belgelerle ilgili olarak tekrar bir değerlendirme yapılır. Bu aşamada belgenin imhasına karar verilebilir ya da dördüncü safhaya gönderilir. Bu safha, uzun dönem arşivlenmesi gereken, arşivsel değeri olan pasif belgeler için kullanılır. Bu az sayıdaki elektronik belgeler, arşivsel amaçlı depolama ünitelerinde muhafaza edilirler. Belgelerin yaşam döngüsü aşamalarında kimin sorumlu olduğu da ortaya konmalıdır. Belge üretim ve aktif safhada, belge üreticisi birincil derecede sorumluluğa sahip kişi olarak değerlendirilmelidir. Belge yöneticisinin bütün aşamalarda etkin olması ve gerekli işlemleri yürütmesi sistemin sağlıklı çalışması açısından önemlidir.

2.3. Elektronik Belge Yönetim Standartları

Belge yönetim standartları, kurumsal yapı içinde üretilen belgelerin belli bir sistem, plan ve yöntemler çerçevesinde yönetilmesini sağlamaya yönelik olarak oluşturulmuştur. Buradaki esas amaç, uygulamada aynı standartları benimsemek ve birlikte çalışabilirliği sağlamaktır. Özellikle elektronik belge yönetimi açısından baktığımızda standartlaşma büyük önem taşımaktadır. Zira teknolojik anlamda birbirleriyle konuşamayan sistemlerin birlikte uyum içinde çalışması ve uzun dönem arşivleme açısından devamlılığın sağlanması mümkün değildir. Bu sebeple teknolojinin gerektirdiği çerçevede belli standartların ortaya konması büyük önem taşımaktadır.

Belge yönetiminde standartlaşmaya giden çalışmalar ISO ‘in ortaya koyduğu ISO 9000-9001 standardıyla önemli bir ivme kazanmıştır. Uluslararası Standartlar Örgütü (ISO*)* toplam kalite anlayışı çerçevesinde genel kalite standartlarını, “kalite sistem dokümantasyonu” adı altında, belge ve doküman *yönetimiyle* ilgili bir takım uygulama ölçütleri geliştirmiştir. Bu çerçevede ISO 9000 standartlarına uyum sağlayabilmesi için iyi bir belge yönetimi sistemine sahip olması gerekir. Çünkü kalite standardı sistem elemanlarının gerek zorunlu olan kalite prosedürlerinin hazırlanması neticesinde üretilen kalite dokümantasyonu, gerekse kalite faaliyetleri sonucunda tabii olarak üretilen kalite kayıtlarının

belirli bir disiplin altına alınması, organizasyonun standartların şart koştuğu koşulları sağlayabilmesi için göz ardı edilemeyecek bir mecburiyettir. Bu zorunluluk, her ne kadar standartlarda "Doküman Kontrolü" ve "Kalite Kayıtları" gibi başlıklarla zikredilse de ifade edilen uygulama adımlarıyla belge yönetimi fonksiyonu açıkça ortaya konulmamıştır (Çiçek, 2000: 33). Bu standart belge yönetiminin kurumlar tarafından daha dikkatle üzerinde durulması gereken bir faaliyet olduğunu ortaya koyması açısından önemlidir. Bu çerçevede belge yönetimiyle ilgili standartlarda gelişmeler kaydedilmiştir.

Uluslararası Belge Yönetim Standardı' olarak nitelendirebilecek ISO 15489 standart çalışması, belge yönetim yaklaşımının tüm yönlerini kapsamayı amaçlayan ve belge yönetiminin ana çerçevesini çizerek, belge yönetimine evrensel bir boyut kazandırmaya yönelik önemli bir doküman olarak ortaya çıkmıştır (Özdemirci, 2003:226). Bu standart, belge yönetimi politika ve prosedürlerinin standardizasyonu, standart uygulama ve prosedürler kullanılarak belgelerin gerektiği gibi muhafazasının sağlanması ve içerdikleri bilgiye ve delilsel içeriğe daha etkin ve verimli bir şekilde erişilmesini sağlanması öngörmektedir. ISO 15489 standardı başlangıç noktası olarak Avustralya Standartları AS 4390 Belge Yönetimi Standardını temel alarak belge yönetimi konusunda en iyi uluslararası uygulamaları standart hale getirme isteği ve iradesi üzerine geliştirilmiştir (Özdemirci, 2003:234). Bu standartlar elektronik belge yönetim standartlarının temelini oluşturmaktadır. Bu standartla bağlantılı olarak ISO 23081: Belge Yönetim Süreçleri- Belgeler için Üst verisi standardı (ISO, 2006) tamamlayıcı niteliktedir. Kurumsal yapılardaki ve yasal uygulamadaki farklılıklar göz önünde bulundurularak zorunlu üst veri setlerini tanımlanmamıştır. Ancak öngörülen üst veri alanlarının ISO 15489 standardına uygunluğunu sağlama ve iş süreçlerini desteklemede sağladığı faydalar ortaya konulmuştur.

Ülkemiz açısından kurumlarda elektronik belge yönetimi için gerekli bir referans kaynak olan Kandur (2006) tarafından hazırlanan "Elektronik Belge Yönetimi Sistem Kriterleri " çalışması büyük önem taşımaktadır. Öncelikle 2005 yılında Elektronik Belge Yönetimi Sistem Kriterleri Referans Modeli çalışması kamu kurumlarının görüşüne sunuldu. Bu görüşler çerçevesinde referans model oluşturuldu ve Devlet Arşivleri Genel Müdürlüğü tarafından yayınlandı. 2006 yılında Referans Model standart formatına dönüştürülerek TSE'ye sunuldu ve 2007 yılında TS 13298 Elektronik Belge Yönetim standardı olarak yayımlandı. Standart 2009 yılında revize edilmiştir. Bu standart (TSE, 2009) genel olarak aşağıdaki hususları kapsamaktadır;

- Elektronik belge yönetimi sistemi (EBYS) için gerekli sistem gereksinimleri,
- EBYS için gerekli belge yönetim teknikleri ve uygulamaları,
- Elektronik belgelerin yönetilebilmesi için zorunlu gereksinimler,
- Elektronik ortamda üretilmemiş belgelerin yönetim fonksiyonlarının elektronik ortamda yürütülebilmesi için zorunlu gereksinimler,
- Elektronik belgelerde bulunması gereken diplomatik özellikler,
- Elektronik belgelerin hukuki geçerliliklerinin sağlanması için alınması gereken önlemler,
- Erişim Kontrolü ve güvenliğinin sağlanmasıyla ilgili hususlar,
- Güvenli elektronik imza ve mühür sistemlerinin uygulanması için gerekli sistem alt yapısının tanımlanması,
- Dijital görüntüleme sistemleriyle ilgili genel konular,
- İlgili üst veri elemanları ve yapılarıyla ilgili hususları kapsamaktadır.

Dünyada çapında uygulanan elektronik belge yönetimiyle ilgili standartlar açısından Amerika Savunma Bakanlığı tarafından 1997 yılında geliştirilen ve zaman içinde gerekli güncellemeleri yapılan Elektronik Belge Yönetim Yazılım Uygulamaları Tasarım Kriterleri Standardı "DoD 5015-02-STD" önemli bir standart olarak dünyada birçok ülkede kullanılmaktadır. Bu standart, elektronik belge yönetiminde kullanılabilecek yazılımları için zorunlu ve zorunlu olmayan kurallar seti tanımlamaktadır (Kandur, 2006:104). Bu standardın, bilgi teknolojilerindeki değişimlere paralel olarak, özellikle daha üst düzeyde veri güvenliği ve elektronik belge bütünlüğü gereksinimlerini içeren yeni versiyonu 2007 yılında yayımlanmıştır. Bu standart (USA Departmen of Defence, 2007) genel olarak aşağıdaki hususları kapsamaktadır;

- Yazılım, belgelerin standartlar çerçevesinde yönetilmesini sağlaması, tarihle ilgili mantıksal tanımlamaların yapılması, geriye uyumluluk özelliğinin olması, etkin erişebilirliği desteklemesi, farklı uygulamalara uyumlu olması ve güvenliği ile ilgili genel gereklilikler,
- Dosya planlarının uygulanması, saklama planlarının gerçekleştirilmesi, belgelerin onaylanması ve dosyalanması, elektronik postaların dosyalanması, daha sonra devlet arşivlerine gönderilecek belgelerin dosyalanması, elektronik belgelerin depolanması,

- Dosyalanmış belgelerle ilgili zorunlu üst veri alanları, ilk sınıflandırma, mevcut sınıflandırma, orijinal olarak sınıflandırılmış belgeler, ikincil olarak dosyalanmış belgeler, çoklu ikincil kaynaklar, gizliliği kaldırılmış dosyalar, gizliliği kaldırılmış dosyaların depolanması, sınıflandırma rehberi, sınıflandırma rehber alanlarının planlanması, belge geçmişinin denetimi, belge geçmişi denetiminin kullanılması, erişimle ilgili ihtilaflar, sınıflandırılmış belgelerin aranması, erişimin kısıtlanması, erişim kontrolü, milli güvenlikle ilgili bilgi içeren belgelerin gizliliğinin sağlanması gibi sınıflandırılmış belgelerin yönetim gereklilikleri,
- Alan düzeyinde sınıflandırma, versiyon değişikliği bildirimin yapılması gibi seçime bağlı güvenlik özellikleri,
- Yazılım ürünü bileşimi ile ilgili hususlar,
- Elektronik belgelerin gizlilikle ve bilgi edinme hakkı yasaları çerçevesinde yönetilmesiyle ilgili hususlar,
- Elektronik belgelerin, yaşam döngüsü çerçevesinde güvenli bir şekilde transfer işlemlerinin yapılmasıyla ilgili zorunlu ve seçime bağlı hususlar,
- Standart çerçevesinde belirtilen zorunlu alanlar dışında, genel olarak bütün bir standart bağlamında seçime bağlı diğer konulardan bahsedilmiştir.

Elektronik belge yönetimi uygulama modelleri açısından "Elektronik belge yönetimi için model gereklilikler (MoReq)" çalışması önemli bir referans kaynağı olarak değerlendirilmektedir. Elektronik belge yönetim sistemi oluşturmak için gerekli teknik özelliklerle ilgili bir model ortaya koymayı amaçlayan bu standart, Avrupa komisyonu tarafından bir referans kaynak olarak kabul edilmiş ve Avrupa komisyonunun resmi yayını olarak yayımlanmıştır. Bu çalışma elektronik belge ve doküman yönetimi konusunda Avrupa'nın önde gelen danışmanlık firması Cornwell Management Consultants plc tarafından hazırlanmıştır. İlk sürümü olan MoReq1 2001 yılında yayımlanmıştır. 2008 yılında güncellenerek MoReq2 sürümü olarak yayımlanmıştır. Bu model'de ortaya konulan hususlar gerek kamu ve gerekse özel sektörde aynı şekilde uygulanabilecek niteliktedir. Kâğıt belgelerin elektronik yönetimi ve doküman yönetimi konuları kısaca ele alınmıştır. Dijitalleşme ve elektronik belge üretimimi çalışmanın dışında tutulmuştur. Model gereklilikler ortaya konurken modüler bir yaklaşım benimsenerek herhangi bir platform ya da

sektöre bağımlı kalınmamıştır. Yani, MoReq kullanıcıların kendi kurumsal yapılarına özgü hususları bu modele entegre edebilmelerine imkân vermektedir. Bununla birlikte bu model'de ortaya konulan hususların her kurumda bütünüyle uygulanacağı düşünülmemelidir. Bu model (EU, 2001) genel olarak aşağıdaki hususlarda önerileri içermektedir;

- Elektronik belgelerin elektronik dosyalar içinde nasıl organize edileceğini ve dosyalar arasındaki ilişkileri tanımlayan sınıflandırma şemalarıyla ilgili gereklilikler,
- Elektronik belgelerin güvenliğiyle ilgili erişim kontrolü bağlamında gereklilikler ve bunlarla ilişkili olarak, erişim, işlem geçmiş raporu, yedekleme ve veri kurtarma, belge hareketlerini izleme, e-belgenin gerçekliği ve güvenlik düzeyleri ilgili gereklilikler,
- Belge yönetiminin en önemli konularından olan saklama ve imha işlemleriyle ilgili süreçlerin oluşturulmasındaki gereklilikler, bu çerçevede saklama planlarının oluşturulması ve elektronik belgelerin transferi ve imhası ile ilgili gereklilikler,
- Elektronik belgelerin alınması ve kaydedilmesi ile ilgili gereklilikler, bu kapsamda, aynı yapıda ve türde gelen birden çok dosyanın transfer işlemleriyle ilgili süreçler, elektronik postaların alınması ve yönetilmesiyle ilgili gereklilikler,
- Elektronik belgelerin aranması ve geri iletimiyle ilgili süreçlerinin sağlıklı işlemesini sağlayacak gereklilikler,
- Yönetimsel fonksiyonlarla ilgili gereklilikler, bu bağlamda, sistem parametrelerinin yönetilmesi, yedeklemesi, geri yüklenmesi, sistem yönetimi ve kullanıcı yönetimiyle ilgili gereklilikleri içeren genel yönetim konuları, ayrıca raporlama, belgelerin değiştirilmesi, silinmesi ve düzeltilmesi ile ilgili gereklilikler,
- Elektronik belge yönetim sistemi içinde kâğıt belgelerin yönetimi, doküman yönetimi, iş akışı, elektronik imza ve diğer doğrulama mekanizmalarıyla ilgili gereklilikler,
- Model'de ortaya konulan gereklilikler dışında, kurumların gerekliliklerini ortaya koyarken göz önünde bulundurulması gereken hususular, bu bağlamda, sistemim kolay kullanımı, performans ve ölçeklenebilirlik, sistemin erişilebilirliği, teknik standartlar, yasal ve düzenlemelerle ilgili gereklilikler, dış kaynak kullanımı, uzun dönem koruma ve teknolojik eskimeyle ilgili gereklilikler,
- Elektronik belge yönetim sisteminde üst veri elemanlarıyla ilgili gereklilikler ele alınmıştır.

Arşiv belgelerin tanımlanmasıyla ilgii en önemli standart ICA'nin Tanımlama Standartları Koimtesi tarafından 1999 yılında ikinci sürümü hazırlanan ISAD (G) Uluslararı Arşivsel Tanımlama Standardıdır. Bu standart arşivsel tanımlamaların hazırlanmasında genel bir yol göstericidir. Mevcut ulusal standartlarla birlikte ya da ulusal standartların geliştirilmesi için bir kaynak olarak kullanılmalıdır. Arşivsel tanımlama ile ilgili bir takım kurallar içeren bu standart (ICA, 2000) genel olarak aşağıdaki hususları amaçlamaktadır;

- Tutarlı, uygun, öz açıklamalı tanımlamaların oluşturulmasını sağlamak,
- Arşivsel materyallerle ilgili bilgi değişimini ve geri iletimle ilgili hususları kolaylaştırmak,
- Yetki verisinin paylaşılabilmesini sağlamak,
- Farklı arşiv depolarından, tanımlanmamış bilgi sistemlerine tanımlamaların entegrasyonunu mümkün kılmayı amaçlamaktadır.

Elektronik belgelerin dijital korunmasıyla ilgili standartlar da önemle göz önünde bulundurulmalıdır. Bu çerçevede geçerli olan standartlar aşağıdaki gibidir;

- *ISO 12142: Elektronik Görüntüleme Hataları:* 2001 yılında ISO tarafından oluşturulan bu standart, optik disklerde depolanan verilerin doğrulanmasıyla ilgilidir. Ortam hataları görüntüleme ve raporlama ille ilgili iki düzey ve iki tekniği belirtmektedir. CD-ROM teknolojisinin uygulanmasıyla ilgili hususları kapsamamaktadır (ISO, 2001a).
- *ISO/TR 12654: Elektronik Görüntüleme*: 1997 yılında ISO tarafından oluşturulan bu standart, gerektiğinde delil olabilecek kullanılabilecek optik ortamdaki verilerin depolanmasını sağlayan elektronik depolama sisteminin yönetimiyle ilgili tavsiye niteliğindeki hususları içermektedir. Teknik bir doküman olarak bu standart, elektronik belgelerin bütünlüğünün korunarak alınması ve depolanmasıyla ilgili uygulanabilecek yöntemleri önermektedir (ISO, 1997).
- *ISO/TR 18492: Elektronik Dokümanların Uzun Dönem Korunması:* 2005 yılında ISO tarafından oluşturulan bu standart, bilgisayar yazılım ve donanımında oluşabilecek eskimeler ışığında dijital arşivlere, elektronik dokümanların muhafazası, erişimi ve gerçekliği konularında yol göstermeyi amaçlamaktadır (ISO, 2005). Dijital koruma stratejileri geliştirmek için bir çerçeve yapı ve en iyi uygulama hususunda yol haritası sağlayan teknik bir rapordur.

Elektronik belge yönetimi açısından dijital ya da sayısal imza standartları da önemlidir. Elektronik belgelerinin geçerliliğini sağlayan sayısal imza ille ilgili standartlar açısında Amerika NIST Kurumu tarafından 2000 yılında hazırlanan FIPS 186: Sayısal imza standardı önemli bir yere sahiptir. Bu standart, bilgisayar güvenliğiyle ilgili şifreleme konularını içermektedir. Bu standart, sayısal imza üretme ve doğrulama için gerekli algoritmaları belirtir. Bunlar, verinin bütünlüğünü doğrulamak için kullanılır. Böylece, veri üzerinde oynanmaması ve değişiklik yapılmaması sağlanır.

Gerçek belgelerin uzun dönem muhafazasının sağlanması için oluşturulan INTERPARES projesi elektronik belgelerin sağlıklı arşivlenmesi açısından önemli bilgiler ve çalışmalar sunmaktadır. Elektronik sistemlerdeki kalıcı gerçek belgeler üzerinde uluslar arası araştırma projesi, dijital ortamda üretilen ya da muhafaza edilen gerçek belgeleri uzun dönem arşivlenmesi için gerekli bilgileri geliştirmeyi, bu tür belgelerin uzun dönem korunmasını sağlayacak standartlar, politikalar, stratejiler ve uygulama planları gerekçelerini ve kullanıcıların bu belgelerin gerçekliğine güvenmeyi sağlamayı amaçlamaktadır (Interpares, 2006). Bu proje üç safhada geliştirilmiştir. 1999'da başlayıp 2001 yılında sonuçlanan birinci dönem, elektronik ortamda üretilen ve muhafaza edilen gerçek belgelerin arşivlenmesini sağlamayan metot ve teorilerin geliştirilmesi üzerinde durmuştur. 2002 yılında başlayan ve 2007 yılında sonuçlanan ikinci dönem de, gerçeklik konusuna ek olarak, belgenin yaşam döngüsü süresince üretiminden muhafazasına kadar güvenirliliği ve doğruluğu konuları üzerinde araştırmalar yapılmıştır. 2007 yılında başlayan üçüncü dönem ise, projenin birinci ve ikinci safhasında varılan sonuçları ile dünya çapındaki diğer dijital koruma projeleri üzerinde bina edilmiştir. Bu safhada teorik gerçekler arşivlerle çalışılarak uygulamaya konulacaktır. Bu safhanın 2012 yılında sonuçlandırılması planlanmaktadır.

Yasal durumlarda elektronik belgenin gerçekliği, bütünlüğü ve geçerliliğinin sağlanması büyük önem taşımaktadır. Bu amaca yönelik olarak Büyük Britanya standartları enstitüsü tarafından hazırlanan BSI BIP 008:2004: Elektronik olarak Depolanmış Bilginin Delilsel Ağırlığı ve Yasal Geçerliliğine Yönelik Tüzük uluslararası nitelikte önemli bir standarttır. İlk olarak 1996 yılında yayımlanmıştır. Standartta 1998 yılında teknolojik değişimlere paralel olarak bir takım güncellemeler yapıldı. Son olarak 2004 yılında yapılan değişiklikle mevcut halini almıştır. Bu standart, bir organizasyon için gerekli olacak, elektronik olarak depolanmış belgenin gerçekliği, bütünlüğü ve geçerliliğiyle ilgili kesinlik

düzeyini göstermek ile ilgilidir (BSI, 2004). Bu standart, özellikle elektronik olarak depolanmış bu bilgiler hukuk sistemi içinde ya da dışında ki ihtilaflarda delil olarak kullanılabilmesi durumlarında uygulanabilir.

Bilgi güvenliği ile ilgili standartlarda büyük önem taşımaktadır. ISO/IEC 2700 uluslararası standardı, bilgi güvenliği yönetimi standardı olarak önemle göz önünde bulundurulmalıdır. Ülkemizde bu standart ISO/TSE 27001 Bilgi Güvenliği Yönetim Sistemi olarak uygulamada kullanılmaktadır. Bu standart, kurumsal bilgi güvenliği bakış açısının her zaman bir bütün olarak kabul edilmesi gerektiğini ileri sürmektedir (ISO/IEC, 2005),. ISO/IEC 15408 ortak kriterler standardı ise, kullanılan teknolojilerin güvenlik seviyelerinin belirlenmesi, geliştirilmesi ve değerlendirilmesinin uluslar arası düzeyde kabul görmesi için oluşturulmuştur. Bu standartta güvenlik teknikleri ve bilgi güvenliği değerlendirme kriterleri bulunmaktadır.

MoReg, ISO 15489 ve US DoD gibi standartlara uygunluk, etkin bir elektronik belge yönetim sistemi oluşturma açısından bir çerçeve çizilmesinde faydalı olabilir. Bütün bu standartlar, temel bir sistem ya da genel uygulamalar için yol gösterici niteliktedir. Bu yüzden, doğrudan bir fayda ya da başarı sağlamaz (Johnston ve Bowen, 2005:136). Ancak elektronik belge yönetiminde temel noktalarda standartlaşma sağlanarak uygulamada birlikte çalışabilirlik gerçekleştirilebilir. Bu açıdan standartlarda ve model yaklaşımlarda belirtilen temel hususlar kurumsal gerçeklerde göz önünde bulundurularak uygulanmalıdır. Böylece uygulamaya dönük deneyimlenen hatalara tekrar düşülmeyecektir. Bilgi teknolojilerindeki hızlı değişim düşünüldüğünde, arşivleme ve erişim açısından standartların güncel olmasına özel önem gösterilmeli, değişiklikler takip edilmeli ve standarda dönüşmemiş güncel model uygulamalarda takip edilerek sistemin etkin işlerliği sağlanmalıdır.

2.4. Elektronik İmza

2.4.1. Elektronik İmza Kavramı

İmza, genel olarak, bir belgenin doğruluğunu göstermek amacıyla yapılan her türlü işaret olarak tanımlanabilir. İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece

imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin mevcut olduğu anlaşılır (Reed, 2000). El yazısının dolayısıyla imzanın değişmez nitelikleri vardır. Bunlar; her insanın imzasının genellikle benzersiz olması, her insanın el yazının bir bütün olması ve son olarak, her insanın yazısında değişmeyen karakterlerin bulunmasıdır (Yıldırım, 1996:57). Bu bakımdan imza, kişilere hak sağlayan, sorumluluk yükleyen bir husustur. İmzasız bir belgenin ne hak nede yükümlülük getirmesi mümkün değildir.

Elektronik ortamda üretilen ve gönderilen belgelerin hangi kuruma ya da kişiye ait olduğunu doğrulayan e-imza, mevcut kanunlar çerçevesinde ıslak imza ile eşit statüye sahip bir uygulamadır. Elektronik imza, oluşturulan güvenlik teknolojisinin verilerde değişiklik yapılmasını önleyen veya bu verilerde değişiklik yapılması durumunda bu değişikliğin gerçekleştiğinin anlaşılmasını sağlayan bir uygulamadır. Ayrıca dijital kalemle imza atılması işleminde de elektronik imzadan bahsedilebilir (Orta, 2005:42). Bu durumda söz konusu imza basit elektronik imza olarak adlandırılabilir Ancak elektronik ortamda imzadan beklenilen fonksiyonları sağlamaktan uzaktır.

Elektronik imza kavramının sayısal imzanın yerine kullanıldığı görülmektedir. Sayısal imzanın, dijital imzayla aynı şeyi ifade etmesi dolayısıyla da birbirlerinin yerine kullanılmaktadır. Ancak elektronik imza bir üst kavramdır. Yani, genel olarak elektronik imza kavramı, çok genel bir tanım olup; kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri içeren elektronik imzaları veya e-belgenin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları da içermektedir. Başka bir tanıma göre elektronik imza, ıslak imzanın fonksiyonlarını da kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır (Arıkan, 1999:151). 5070 sayılı elektronik imza kanununda ise (E-İmza Kanunu, 2004) "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmaktadır. Sayısal imza ile diğer tür elektronik imzaları birbirinden ayırmak çok önemlidir. Sayısal imza, elektronik olarak depolanmış elle atılmış imza ile aynı değildir. Bir sayısal imza, diğer tür elektronik imzalara benzemeyen güvenli bir iletişimdir. Sayısal imza, sözleşmeler, resimler, mektuplar ve buna benzer birçok elektronik belge türünün imzalanabilmesini ve kısa bir süre içinde güvenliği tehlikeye sokma korkusu olmadan başka bir birime gönderilebilmesini sağlar (Lupton, 1999). Sayısal olarak

imzalanmış bir sözleşme yasal olarak geçerlidir ve yalnızca yetkili alıcı tarafından okunabilir. Elektronik imza işlemlerinin güvenli ve sağlıklı yürütülebilmesi oluşturulan elektronik imza alt yapıyla gerçekleştirilebilir. Elektronik imza altyapısı, elektronik belgenin şifrelenmesini mümkün kılmakta, değiştirilmesini önlemekte ve ayrıca birden çok kişi ile mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek kalmadan, elektronik yoldan haberleşmeyi kolaylaştırmaktır (Alkan ve İnalöz, 2004:111).

Yukarda ifade edilen hususlar çerçevesinde elektronik imzayı, biyometrik imza ve sayısal imza olarak ikiye ayrılır. Biyometrik imza, kullanıcıların parmak izi veya retina gibi kişiye has özellikler kullanılarak oluşturulan imzadır. Dünyada daha çok sayısal imza tercih edilmektedir. Biyometrik yöntemler ise sisteme erişimde kullanılmaktadır (Orta, 2005: 42). Elektronik imza çeşitleri içinde, en çok üzerinde durulan ve kullanılan en kolay, verimli, etkin ve düşük maliyetli olabileceği belirtilen tür ise açık anahtar şifrelemesine dayanan sayısal imzadır (Orta, 2005: 41). E-imza ya da sayısal imza bir elektronik mesaj veya iletiye eklenen ve göndereni emsalsiz şekilde tanımlayan veya taklit edilmesi çok zor olan bir sayısal kod olarak ta tanımlanmaktadır. Bir elektronik imzada bulunması gereken önemli özellikler şöyle sıralanabilir (Sağıroğlu ve Alkan, 2007:54);

- Güvenirlilik
- Taklit edilemezlik
- Tekillik
- Yeniden kullanılmazlık
- İnkâr edilemezlik
- Değiştirilmezlik

E-imza ile bir belgeyi imzalamada asimetrik şifreleme yöntemi kullanılır. Bu işlemde bir asimetrik şifreleme algoritmasına, belgenin imzalanması için bir imzalama ya da onaylama algoritmasına ihtiyaç vardır. İmzalama ve onaylama algoritmasına DSA(Digital Signiture Algorithm) örnek verilebilir. Literatürde geçen imzalanmış elektronik belgenin şifre döngüsü mantığı Şekil 2'de gösterilmiştir. Şifreleme algoritması şifrelenecek metni ve şifreleme anahtarını girdi olarak alır. Çözümleme algoritması ise şifreleme algoritmasının ters yönünde çalışır. Aynı zamanda, bu işlemin sağlıklı gerçekleştirilebilmesi için bir yazılım da gerekmektedir. E-belge bütünlüğü korunması açısından, bütünlük kontrolü bir özetleme algoritması veya fonksiyonu ile yapılır. Herhangi bir uzunluktaki veriyi alıp işleyen ve bu

veriye özgü olan sabit uzunlukta bir değer çıkaran algoritmalara özetleme veya parmak izi algoritması denir (Sağıroğlu ve Alkan, 2007:70). Bu algoritmaların çıktısı, sabit uzunlukta bir değer olup, mesajın özeti olarak bilinir.

Şekil 2. E-belge Şifreleme Döngüsü

Islak imzalı belgelerde olduğu gibi, elektronik belgelerin imzalanmasında tarih ve saat damgası işleminin de sağlanması gerekmektedir. Zaman damgaları karşılaşılabilecek yasal durumlarda ve diğer olası açıklara karşı e-imza sahiplerini korumada önemli bir işleve sahiptir. Bu açıdan elektronik belgelerin düzenlendiği zamanın şüpheye yer bırakmayacak şekilde tespit edilmesinin zaman damgası fonksiyonu yerine getirir. 5070 sayılı Elektronik İmza Kanununa göre zaman damgası (E-İmza Kanunu, 2004) "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt" olarak tanımlanmıştır. Bu çerçevede elektronik belgelerde zaman damgasının bulunması bir zorunluluktur.

Bugün sanal ortamda bağlayıcı işlem yapma olanağı sağlamaya çalışan elektronik ya da sayısal imza 1998 tarihli T.C. Başbakanlık Dış Ticaret Müsteşarlığı bünyesinde faaliyet gösteren Elektronik Ticaret Koordinasyon Kurulu Elektronik Ticaret Hukuk Çalışma Grubu Raporuna göre "bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Sayısal imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini, elektronik belgenin orijinalliğini ve güvenilirliğini mümkün kılar. Gönderici için ve mesajın gönderildiği taraf için tek olan sayısal imzalar doğrulanabilir ve inkâr edilemez." Bu çerçevede sayısal imza elektronik ortamda atılan ve gönderen kişi ya da kuruma ait olduğunu garanti eden ve yasal açıdan elle atılan imza gibi bağlayıcılığı olan teknolojik uygulamaya

verilen addır. Sayısal imza teknik olarak bir yazılımdır. Sayısal imza, genel anlamıyla kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse tarafından kullanılan bir işaret veya kabul edilen herhangi bir güvenlik unsurudur (Orta, 2005:37). Sayısal imza, bir mesajın, imzalayanın açık anahtarına karşılık gelen bir özel anahtar kullanılarak oluşturulup oluşturulmadığını ve başlangıçtaki mesajın dönüşüm esnasından değiştirilip değiştirilmediğinin asimetrik şifreleme sistemi ve başlangıçtaki mesaja sahip olan kişi ve imzalayanın açık anahtarlarının tam olarak saptanabildiği bir Hash fonksiyon kullanılarak dönüştürülmesidir (Winn, 1998). Bu bağlamda sayısal imzanın esas işlevi elektronik ortamda aslında ayrılması güç olan sahte imzayı önlemek ve orijinal belgelerin olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır.

Elektronik belgeye eklenmiş bilgi bir anlamda elektronik imzadır. Elektronik İmza ve Uygulaması kitabında Orta (2005:56) elektronik imzanın gerçekleşme sürecini şöyle anlatmaktadır: Gönderilecek belgeden matematiksel yöntemler yardımıyla ve özgün bir biçimde kısaltmak suretiyle sabit uzunlukta sayısal bir bilgi elde edilir ki buna mesajın özeti veya *"hash"* adı verilir. Hash metodu ile elde edilen bilgi, geri dönüşümü olmayan bir bilgidir. İkinci adım olarak mesaj özeti gönderen tarafın özel anahtarıyla şifrelenmektedir. Bu kodlanmış olan *"hash"*, elektronik imza olarak adlandırılmaktadır. Elektronik imza belgeye eklenir ve belgeyle birlikte alıcıya gönderilir. Her mesajın farklı bir özeti vardır. Belgede en ufak değişiklik yapılması halinde şifrelenmiş olan mesaj özeti ile sonradan oluşturulan mesaj özeti arasında fark olacaktır. Fark yoksa imza geçerli bir elektronik imza demektir. Bu şekilde belge içeriğinin değişmediği ispatlanmış olur. Elektronik imza, mesaj özeti ve gizli anahtara özgüdür. Alıcı mesajı, şifrelenmiş mesaj özetini yollayan kişinin açık anahtarını kullanarak çözer. Bu iki *"hash"* aynı ise özel anahtarı sadece gönderen bildiği için bu mesajın gönderen kişiye ait olduğu ve mesajın değişmeden geldiği onaylanmış olur. Taraflar böyle bir belgeyi gönderip/almadıklarını ileri süremezler.

2.4.2. Elektronik İmza Altyapısı ve Sertifikası

Elektronik imzanın işlerlik kazanması için bir takım unsurların bulunması gerekmektedir. Bu hususların gerçekleştirilmesi sistemin sağlıklı işleyişini sağlayacaktır. Bu unsurlardan biri olan açık anahtar alt yapısı, sayısal imzanın oluşturulmasında ve kullanılmasında çok önemli rol oynamaktadır. Sayısal imzada kullanılan anahtarlar, bir kripto algoritması ile üretilir (Orta, 2005: 38). Sonucun güvenilir olması için bu sürecin belli

standartlarla desteklenmesi gereklidir. Açık anahtar altyapısında kullanılan asimetrik şifreleme yöntemlerinden biri açık anahtar diğeri özel anahtar olmak üzere bir anahtar çifti bulunmaktadır (Dönmez, 2002:12). Özel anahtar sayısal imzanın oluşturulmasında, açık anahtar ise sayısal imzanın tetkikinde kullanılır (Şenocak, 2001:99). Özel anahtarın güvenliğinin sağlanması büyük önem taşımaktadır. Özel anahtar üretildikten sonra ya bilgisayar diskinde ya da harici bir depolama biriminde tutulmalıdır. Ayrıca güvenliğinin korunması ve erişilmesini önleyici tedbirler alınmalıdır. Güvenlikle ilgili zaaflar oluşursa, imzanın özel anahtarla atıldığından ve inkâr edilemeyeceğinden bütün sorumluluk imza sahibindedir. Bu sebeple, özel anahtarın çok iyi korunması gerektiği hususunda kullanıcılar bilgilendirilmeli ve gerekli güvenlik önlemlerinin alınması sağlanmalıdır. İmzanın oluşturulmasında ve doğrulanmasında kullanılan açık ve özel anahtarlar ile açık anahtarların kime ait olduğunun belgesi sayılan elektronik sertifika ve bu elektronik sertifikanın üretilmesini, yönetilmesini sağlayan elektronik sertifika hizmet sağlayıcıları (ESHS) sayısal imzanın unsurlarını oluşturmaktadır (Orta, 2005:38). Açık anahtara herkesin ulaşabilmesi amacıyla elektronik sertifika hizmet sağlayıcıları dizinler oluştururlar. Sertifika içinde açık anahtarla birlikte kişinin kimliğini yansıtan diğer bilgiler de yer alır. Ayrıca elektronik imza sertifikalarının bir başlangıç ve bitiş süresi vardır. Bu süre genel olarak bir yıldır. Bu husus önemle göz önünde bulundurulmalıdır. Bununla beraber, ESHS'nın sertifikasının da doğal olarak bir geçerlilik süresi vardır. Bu süre azami 10 yıldır. Sertifikaların kullanım süreleri bittiğinde, sertifika içerisindeki bilgiler geçersiz hale gelir. Sertifika kullanıcılarının sertifikalarını yenilemelerini sağlayan mekanizma X.509 sertifika iptal listesidir (Alkan ve İnalöz, 2003: 42).

Elektronik sertifika, kullanıcının bilgilerini içeren bir verinin sertifika hizmet sağlayıcısı tarafından sayısal olarak imzalanması ile oluşur. Elektronik sertifika belgesinde, kullanıcının adı, soyadı, e-posta adresi gibi bilgilerin yanı sıra, kimlik belgesinin geçerlilik süresi, kullanıcının açık anahtar bilgisi gibi bilgilerde bulunur. Sertifikanın düzenlendiği tarih ve geçerlilik süresi de önemlidir (Orta, 2005:46). Elektronik sertifikada bulunması gereken bilgiler ISO ve ITU tarafından tanımlanmış olan X.509 standartlarına göre belirlenmektedir. Sertifikada zorunlu alanlar olmakla birlikte seçime dayalı alanlarda bulunmaktadır. Örneğin, sürüm numarası zorunlu olmamakla birlikte, sertifikanın seri numarası, imzalamada kullanılan algoritmanın belirteci, sertifika yayıncısının ismi, sertifikanın geçerlilik süresi zorunlu alanlardan bazılarıdır. Bu kişisel sertifikalar dışında kök ve sunucu sertifikaları da bulunmaktadır. Sertifika hizmet sağlayıcılarının kimlik bilgilerini ve açık anahtarlarını taşıyan

dosyalara kök sertifika denir. Bir başka ifade ile kök sertifika elektronik sertifika hizmet sağlayıcısının sertifikasıdır. Sertifika ile birlikte gelen açık anahtar sertifika kurumunun kimliğini doğrulamakta kullanılır. Doğrulama gerçekleştirilerek sertifikanın o hizmet sağlayıcısı tarafından onaylanmış, gerçek bir sertifika olduğu teyit edilmiş olur (Orta, 2005: 47). Hizmet sağlayıcısı sertifikaların internet tarayıcılarına yüklenmesi, kullanılabilmeleri açısından bir zorunluluktur. Bazı hizmet sağlayıcı sertifikaların kök kimlikleri Netscape ve Internet Explorer gibi popüler tarayıcılara yüklenmiş durumdadır. Sunucu sertifikaları ise, web sitesine bağlanan kullanıcılara sunulan elektronik dosyalardır.

Tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifika yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifika oluşturulması ve sertifika yaşam çevriminin yönetilmesini sağlayacak kamu sertifikasyon yapısının kurulması ve işletilmesi görev ve sorumluluğu TÜBİTAK UEKAE' ne verilmiştir. Bu çerçevede UEKAE bünyesinde Kam Sertifikasyon Merkezi 2005 yılında, 5070 sayılı Elektronik İmza Kanununa uygun olarak kurulmuş ve işletilmektedir. Kamu Sertifikasyon Merkezi 5070 sayılı kanuna uygun Nitelikli Elektronik Sertifikaları hazırlamak ve bu sertifikaları imza oluşturma verileriyle birlikte Güvenli Elektronik İmza Donanım Araçlarına yükleyerek alıcılarına teslim etmekle yükümlüdür (UEKAE, 2009). Kamu Sertifikasyon Merkezi, sertifika başvurusunda bulunan kişilerin başvuru bilgilerini toplarken, sertifikaları hazırlarken ve teslim ederken güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek, sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile yükümlüdür. Ulusal güvenlik gerekleri göz önünde bulundurulduğunda, bu yapı içinde kök sertifika hizmet sağlayıcısı ve Kamu Sertifika Hizmet Sağlayıcısı milli yazılım ürünleri kullanılmaktadır. Kamu Sertifikasyon Merkezi yalnızca kamu çalışanlarına kurumsal sertifika dağıtmakla görevlendirilmiş olmakla birlikte ilgili e-devlet projeleri çerçevesinde gerekli durumlarda kamu çalışanı olmayan gerçek kişilere de sertifika sağlanacaktır. Ancak esas olan, bu kişilere hizmet verecek özel girişim kuruluşlarının varlığı ve rekabetçi bir ortamda güçlenmeleridir. Ancak bu durum yalnızca istisnai hallerle sınırlı tutulmaktadır. Kamuya hizmet verecek TÜBİTAK-UEKAE'nün oluşturduğu Kamu Sertifika Merkezi ile özel sektöre hizmet verecek olan e-güven, e-tuğra ve TürkTrust, 5070 sayılı elektronik imza kanunun 8. maddesi uyarınca Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) olarak faaliyete geçmişlerdir. Ayrıca Mali Mühür Elektronik Sertifika Hizmet Sağlayıcısı (MM ESHS), TÜBİTAK UEKAE Kamu Sertifikasyon Merkezi (Kamu SM) tarafından, tüzel kişiler ile kurum, kuruluş ve işletmelere elektronik sertifika sağlama hizmeti vermek üzere Gelir İdaresi Başkanlığı için kurulmuş ve

işletilmektedir. MM ESHS sistemi tarafından üretilen sertifikalar, tüzel kişiler ile kurum, kuruluş ve işletmeler tarafından elektronik belge olarak oluşturulacak fatura ve diğer yasal belgelerin bütünlüğünün, kaynağının ve içeriğinin garanti altına alınması, elektronik ortamda muhataplarına iletilmesi ve elektronik ortamda saklanması sırasında güvenliğinin ve gizliliğinin sağlanması amacıyla kullanılacaktır (UEKAE, 2010). Kanunda EHSH, "elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuki tüzel kişiler" olarak tanımlanmaktadır.

6 Ocak 2005 tarih ve 25692 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Elektronik İmza Kanunun Uygulanmasına İlişkin Usul ve Esaslar Hakkındaki Yönetmelikle (TK, 2005); elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin olarak, bildirim ve sertifikasyon süreçlerine, güvenli elektronik imza oluşturma ve doğrulama verileri ile araçlarına, elektronik sertifika hizmet sağlayıcısı, Kurum, nitelikli elektronik sertifika sahibi ve üçüncü kişilerin yükümlülüklerine, denetime, faaliyetin sona erme hallerine, zaman damgasına, yabancı elektronik sertifikalara, güvenliğe, teknik ve mali hususlara ilişkin usul ve esaslar ortaya konmuştur. Bu yönetmelikte teknolojinin sürekli değişmesinden dolayı teknik hususlar ele alınmamıştır. Elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirleyen hususlar yönetmelikle aynı tarihte yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliği ile düzenlenmiştir. Tebliğde, elektronik sertifika ilkeleri ve sertifika uygulama esasları, nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yenilenmesi ve iptal edilmesi, imza oluşturma ve doğrulama verileri ile araçları, ESHS'nın işleyişi, kullandıkları sistem, cihaz, personel, güvenlik, zaman damgası ve hizmetleri düzenlemiştir.

Dünyada yapılan çalışmalar değerlendirilecek olursa; Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonunca hazırlanarak BM genel kurulunda kabul edilen UNCITRAL Elektronik Ticaret Model Kanun ilk çalışma olarak değerlendirilmektedir. Ayrıca, Avrupa Birliği tarafından 1999/93/EC sayılı ve 13 Aralık 1999 tarihli Elektronik İmzanın Müşterek Çerçeve Şartlarının Belirlenmesi Hakkındaki Avrupa Birliği Yönergesi ile 2000/31 sayılı ve 8 Haziran 2000 tarihli Elektronik Ticaret Hakkındaki Avrupa Birliği Yönergesi çıkartılmıştır (Orta, 2005:70). Avrupa Birliği ülkeleri, bu yönerge çerçevesinde iç hukuklarındaki düzenleme yoluna gitmişlerdir.

2.4.3. E-İmza Sorunları

Elektronik imzanın kullanılması beraberinde bazı sorunlar getirebilmektedir. Muhtemel sorunların göz önünde bulundurulması ve buna yönelik tedbirlerin alınması gerekmektedir. 5070 sayılı elektronik imza kanununda (E-İmza Kanunu, 2004), elektronik imzanın oluşturulmasında kullanılan anahtarlarlar ve sertifikalarla ilgili yazılım ve donanımları ifade eden güvenli elektronik imza oluşturma araçlarından bahsedilerek aşağıdaki özellikleri karşılaması şart koşulmuştur;

- Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
- İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini karşılamalıdır.

E-imza ile iş ve işlemlerin güvenli olarak yapılması sağlansa bile, sertifikaların üretiminden kullanımına kadar birçok aşamada sorunlar yaşanabilmektedir. Sertifika hizmet sağlayıcılarının yapması gerekenler kanun ve tebliğlerle belirtilmişse de yanlış ve kötüye kullanımlarda olabilmektedir. Bu kapsamda e-imza kullanımında oluşabilecek problemler şöyle sıralanabilir (Sağıroğlu, 2007:70);

- Sertifika iptallerinin bazı durumlarda duyurulması veya bunların kısa sürede duyurulmasını sağlayacak sistemlerin kullanılmasından oluşabilecek problemler,
- Kullanılacak yazılım ve kurulacak sistemlerde uyum problemlerinin yaşanması,
- Sürekli güncelleme ve dinamik bir yapı oluştuğundan maliyetin artması,
- Kurulumda ya da sistemin iletilmesinde yapılacak hataların büyük güvenlik riskleri oluşturabileceği,
- Sistemi kullananların yeterli güvenlik bilgisine sahip olmamaları dolayısıyla güvenlik zafiyetlerinin oluşabileceği,

- Anahtarların yüksek fiziksel güvenlik sağlayan ortamlarda tutulmalarının yaratacağı sorunlar,
- PIN korumalı akıllı kartların tercih edilmemesinden doğacak sıkıntılar,
- Anahtar uzunluğunun standartlara uygun olarak donanımlarda tutulmaması,
- Akıllı çubuk ve kartların fiziksel olarak güvenliğinin sağlanamamasından dolayı yaşanacak problemler,
- Sertifika yönetiminin doğru, düzenli ve hukuka uygun olarak yapılmamasından doğabilecek sıkıntılar ve kayıplar,
- E-imza kanunun bazı maddelerinin farklı yorumlanmasından kaynaklanabilecek sıkıntılar.

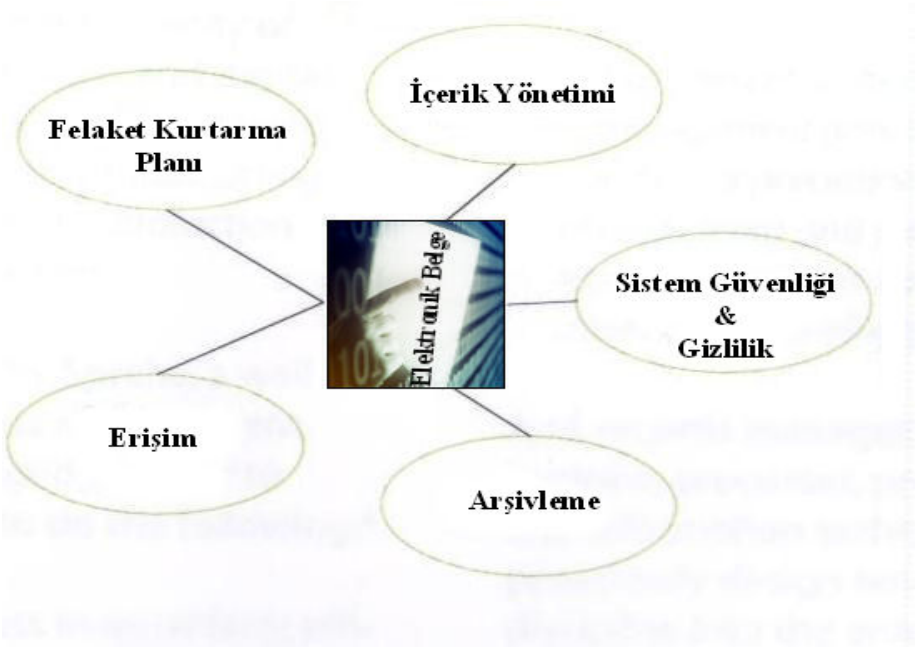
Elektronik imza; doğrulama, erişim kontrolü, bütünlük, inkâr edememe gibi fonksiyonları yerine getirerek yasal açıdan geçerli olmaktadır. Bu fonksiyonlar sayesinde, elektronik belgeyi imzalayanın kimlik bilgileri doğrulanır, gönderilen kaynaklara sadece yetkili kişiler erişir, verinin bütünlüğü korunur ve yasal durumlarda göndericinin inkâr edememesi sağlanmış olur. Bununla beraber, elektronik olarak imzalanmış e-belgenin değiştirilemeyeceği kesin olarak söylenemez. E-belge bir takım karmaşık formüllerle şifrelenmişse de imza süreci tamamlanana kadar sisteme üçüncü şahısların müdahale etme imkânı vardır. Ayrıca, sertifika sahibinin gizli anahtarı öğrenilerek, sertifika sahibinin bilgisi dışında işlemlerde bulunulabilir. Bu şekilde sertifika sahibi, iradesi dışında, üçüncü kişilere karşı sorumluluk altına girebilir.

2.5. Elektronik Belge Yönetim Sistemi

2.5.1. Sistemin Oluşturulması

Elektronik belge yönetim sisteminin geliştirilmesinde prosedürler çok önemlidir. Çünkü hayati belgeler kaybolabilir, deşebilir ya da imha edilebilir. Aynı zamanda elektronik kayıt ortamı dikkatsizlik yüzünden silinebilir ya da üzerinde yazılabilir. Bu tehlikeyle birlikte, elektronik dosyalardaki gizli ve hassas bilgilere yetkisiz erişim ihtimalinin olduğu açıktır. Elektronik belgeleri üretmek, düzenlemek, erişmek, iletmek ve imha etmek amacıyla elektronik belge yönetim sistemiyle ilgili araçları kullanan kişiler, bu araçları doğru bir şekilde kullanma ve elektronik belgeleri belirlenen prosedürler çerçevesinde yönetmeden

sorumludurlar. Bütün bu hususların elektronik belge yönetim sistemi oluşturmada ve sürdürmede önemle göz önünde bulundurulması gerekmektedir. Bununla birlikte öncelikli hususlarında ortaya konmalı ve bu çerçevede bir hareket planı belirlenmelidir. Sistemin dizaynı temel öncelikler esas alınarak yapılmalıdır. Bu temel öncelikler, felaket kurtarma, içerik yönetimi, sistem güvenliği ve gizlilik, arşivleme ve erişim olarak değerlendirilebilir. Şekil 3, belirtilen hususlar çerçevesinde elektronik belge yönetim sistemine ilişkin öncelikleri göstermektedir.



Şekil 3. Elektronik Belge Yönetiminde Öncelikler

Elektronik belge yönetim sistemi oluşturma bağlamında belge ve içerik yönetim uygulamalarında iki önemli durum bulunmaktadır (Xerox DocuShare, 2006:1). Bunlardan birincisi, elektronik belgelerin sürekli artması, gerek elektronik ortamda üretilmesi ve gerekse kâğıt belgelerin elektronik ortama aktarılması suretiyle elektronik belge yönetim sistemine entegre edilmesidir. İkinci eğilim, bu belgelerinin kontrolünün sürekliliğinde ve mevzuata uygunluğu sürdürmede ihtiyaç duyulan; yasal gereklilikler, mevzuatlar ve iş uygulamalarını destekleme sayısındaki artıştır. Bunların sonucu olarak, her kurumun en büyük öneme haiz işler listesinin en üst noktasına e-belge yönetimi ve e-belge yönetim sisteminin oluşturulması taşınmıştır. Bu çerçevede, e-belge yönetim sistemi gerekliliği değerlendirildiğinde aşağıdaki sonuçlara varılmıştır;

- E-belge yönetimi, artık küçük gruplardan oluşan e-belge yönetim uzmanları ya da memurları tarafından yönetilecek bir merkezi arka ofis faaliyeti değildir. E-belge yönetimi, bilgi çalışanı tarafından öncelikli bir iş olarak uygulanmalıdır.

- Elektronik belge yönetim sistemi, günlük iş süreçleri sonunda üretilen ve hâlihazırda var olan belgeler üzerinde kontrolü sağlamak için en uygun çözümü sunmaktadır. Halen var olan fiziksel belge dosya odaları, aslında yüzlerce masaüstü, ağ depolama araçları ve taşınabilir ortamlar olan sanal belge dosya odalarıyla değiştirilmelidir.
- Elektronik belge yönetim sistemi başarılı olmak için bir araçtır. Bununla birlikte sistemin kullanıcı dostu olması e-belge üreten bütün kişiler tarafında kolay bir şekilde kullanılması önemlidir.

Elektronik belge yönetim sistemi oluşturmada, temel bir sistem dizaynında mevcut aşamalar göz önünde bulundurulmalıdır. Bu aşamalar çerçevesinde oluşturulacak elektronik belge yönetim sistemi aşağıdaki adımlar çerçevesinde gerçekleştirilmelidir. (Smyth 2005:143);

- Mevcut durumu ortaya koyma ve hareket planını belirlemek amacıyla hazırlayıcı bir incelemenin gerçekleştirilmesi ve mevcut durumun ortaya konması.
- İş faaliyetleri ile ilgili analiz çalışmasının yapılması
- Elektronik belge gerekliliklerinin tespit edilmesi
- Mevcut sistemi değerlendirilmesi
- Elektronik belge gerekliliklerini karşılamaya yönelik stratejilerin belirlenmesi
- Elektronik belge yönetim sisteminin dizayn edilmesi
- Sistemin uygulamaya konması
- Ön uygulamaya ilişkin gözden geçirme faaliyetlerini yürütmek.
- Sistemin sorunsuz işleyişinin test edilmesi

Yukarıda belirtilen sistem yaklaşımı adımları çerçevesinde sistemi oluşturmak amacıyla daha detaylı çalışmaların yapılması gerekmektedir. Bu açıdan temel sistem yaklaşımı da göz önünde bulundurularak elektronik belge yönetim sistemi oluştururken aşağıdaki hususların belirlenmesi gerekmektedir;

- Dosyaları işlemek ve okumak için gerekeli bütün teknik hususların ortaya konması,
- Sistemin tanımlanmış bütün girdi ve çıktıların tespit edilmesi,
- Dosya ve belge içeriklerinin tanımlanması,
- Erişim ve kullanımla ilgili kısıtlamaların belirtilmesi,

- Sistemin, elektronik belgelerin fonksiyon ve amaçlarının anlaşılmasını sağlanması,
- E-belgenin silinmesi, düzeltilmesi ve eklenmesi ile ilgili güncel kuralların ve şartların ya da dönemlerin tanımlanması,
- E-belge imhasının zamanında ve yetkilendirme çerçevesinde yapılmasıyla ilgili hususların değerlendirilmesi,
- E-belgelerin etkin ve zamanında transferini sağlanmasıyla ilgili konuların açıklığa kavuşturulması gerekmektedir.

Oluşturulacak sistemde, yönetici ve çalışanların, e-belge yönetim sorumluluklarının farkında olmaları büyük önem taşımaktadır. Elektronik belgeleri kullanan yöneticilerin; çalışanlara, elektronik belgelerin üretim, kullanım ve imhasında ve bu tip prosedürlerin talimatlarda yer alması noktasında yol göstermede sorumlulukları bulunmaktadır. Bazı kurumlar elektronik belge yönetim sistemiyle ilgili donanım ve yazılımları herhangi bir talimata bağlı kalmadan her bir kullanıcının bağımsız bir şekilde kullanmasına izin verme eğilimindedirler. Bu eğilim küçük kurumlarda ciddi olmayan sonuçlar doğurabilir. Ancak büyük uygulamalara sahip kurumlarda kaosa yol açması muhtemeldir. Bu sebeple, kurumların elektronik belge yönetim sisteminin kullanımının belirli talimat ve prosedürlere bağlaması ve sistemin kullanıcıların belirlenen talimatlara aykırı davranmasına izin vermeyecek şekilde oluşturulması büyük önem taşımaktadır. Bu kapsamda belge yönetimi çalışmalarının gerektirdiği kaynaklar, sorumluluklar, düzenlemeler, araç ve gereçlerin tasarımı ve sürekliliğinin sağlanması, belge yönetimi sisteminin unsurları arasında yer almaktadır (Külcü, 2009:269)

2.5.2. Sistemin Özellikleri

Elektronik belge yönetim sistemi, elektronik belgelerin belli standartlar çerçevesinde yönetilebilir olmasını ve işlevselliğini sağlayan önemli bir husustur. Özel bir önemi olan elektronik belge yönetimi, planlama, bütçeleme, düzenleme, yönetme, eğitim ve bir bütünlük içinde belgeyi yönetme ile ilgili işlemleri kontrol etmeyi gerektirir (Calrim, 2002:2). Kâğıt ya da elektronik olsun, bütün belge yönetim sistemleri, maliyeti etkin, kolay kullanılan, ihtiyaç duyulduğunda gerekli bilgiyi sağlayan ve gerekli olduğu zaman boyunca muhafaza eden yapıda olmalıdır. Elektronik belge yönetim sistemi, fark edilmeyen değişikliklere, kayıp ya da yetkilendirilmemiş açıklamalara karşı, kâğıt ya da mikrofilm sistemlerine göre daha

hassastır. Bu hassasiyet sebebiyle, elektronik belge yönetim sistemi uygulanmadan önce, kapsamlı ve ayrıntılı bir planlama sürecini yapılması gereklidir.

Teknolojideki görünen hızlı ve sınırsız gelişmenin, e-belge yönetim sistemi tarafından kontrol edilmesi ve yönetilmesi gerekmektedir. Yeni belge türlerinin; belge ortamlarına ek olarak, elde edilmesi, düzenlenmesi, tanımlanması ve belge saklama planlarına göre depolanması gerekecektir (Xerox DocuShare, 2006:15). Bu açıdan elektronik belge yönetim sistemi kurumun bütün belge yönetim stratejileri bakımından daha önemli olmaktadır. Teknolojinin gelişmesiyle birlikte, yeni belge türleri ve ortamlarını kontrol etme çabası çerçevesinde teknolojinin yeni yönetim kuralları ve düzenlemeler geliştirmesi gerekecektir. Herhangi bir elektronik belge yönetim sistemi için anahtar kriterler; esneklik, uyumluluk ve yeni belge türleri ve ortamları bağlamında genişletebilirlik olmalıdır. Mevzuata uygunluk açısından, e-belge yönetim sistemleri, arşivlenmiş belgelerin pasif koruyucuları durumunda değillerdir. Aksine aktif bir şekilde güvenli erişime imkân vermelidir.

Kuruluşlardaki e-belge yönetim süreçleri, süreklilik arz eden değişimlere paralel olarak şekillenmeye devam edecektir. Orijinal belgeleri üretenler, temel belge yönetim kurallarıyla artan bir şekilde uyum sağlamaktan sorumludurlar. Potansiyel değişime bakıldığında, belge yönetim sistemlerinin artan bir şekilde esnek, kullanıcı dostu ve değişen çevreye uyum sağlayan bir özellikte olma zorunluluğu bulunmaktadır. Elektronik belge yönetim sistemi(EBYS), çeşitli hukuksal durumları destekleyebilmesi, yeni kural ve düzenlemelere uyarlanmak için yeterince esnek olması, elektronik belgelerdeki büyük artışı yönetebilmesi gerekmektedir. Yasal düzenlemelere uymak ve kurumsal iş aktivitelerini desteklemek zorunlu bir gereklilik iken, EBYS'nin mali açıdan da kuruma katkı sağlaması önemlidir. Finansal anlayıştaki kurumlar, satın alma kararlarını yalnız teknoloji üzerine değil aynı zamanda sistemin uygulama maliyeti ve süregitmekte olan bakım maliyetleri üzerinde de temellendirmektedir. Hukuka uygunluk, yeni bir elektronik belge yönetim sistemi için güçlü bir gerekçedir. Ancak eğer sistem kurumsal faaliyet için değer ifade edecek şekilde tasarlanmamışsa ya da bu yönde bir düşünce mevcutsa uygulamaya geçilmesi doğru olmaz. Dolayısıyla buna yönelik gerekçelerin sağlam temellendirilmesi gereklidir. Bu bakımdan, Xerox (2006:8) tarafından ortaya konulan kurumsal ihtiyaçları bütünüyle karşılayabilecek bütünleşik bir elektronik belge yönetim sisteminin içermesi gereken özellikler aşağıda değerlendirilmiştir;

- Merkezi bir sunucu ve merkezi bir yönetim anlayışıyla bütün belge yönetim fonksiyonları kullanmalıdır.
- E-belge yönetim sisteminin işin uzmanları tarafından kullanımının sağlanması ve sistemin etkin kullanımı için asgari eğitim faaliyetlerinin gerçekleştirilmesi gerekmektedir. Ayrıca, çalışanların hata oranlarını asgariye indirecek web tabanlı uygulamalar tercih edilmelidir.
- Sistem kullanımı, kullanıcıların normal rutin faaliyetlerine uygun ve kolay olmalıdır. Binlerce kullanıcısı olan büyük organizasyonlar için, yoğun eğitim ve yardım masası desteği gerektiren sistemler konuşlandırmak olanaklı değildir. Sistem, elektronik posta dahil olmak üzere bütün kullanıcı masaüstü uygulamalarıyla sorunsuz bir şekilde bütünleşmeli ve uygulama ana menüsünden ve ara yüzünden kolay bir şekilde erişilebilir olmalıdır.
- Sistem, zaman içinde oluşabilecek değişimlere kolaylıkla adapte olabilecek düzeyde esnek olmalıdır. Örneğin, yeni çalışanların gelmesi ya da çalışanların kurum içindeki rollerinin değişmesi durumlarında kullanıcı haklarının kaldırılması veya eklenmesi çok kolay olmalıdır.
- Sistem, yeni e-belge teknolojileri ve e-belge türleri konuşlandırabilecek düzeyde olması gerekmektedir.
- Sistem, e-belge gerçekliğini sağlamak için işlem geçmişi rapor verilerini paylaşmaya ve aktarmaya imkân vermelidir.
- Kullanıcı dostu ve anlaşılır bir sistemin seçilmesi ve kullanımının mümkün olduğunca basit olmasının sağlanması. Özellikle dosyalama sistemiyle ilgili kolay anlaşılır bir bakış açısının benimsenmesi.
- Sistemin kavramlar dizinine boğulmaması. Buna ilişkin karmaşık bir yapı oluşturulmaması
- Etkin bir belge yönetim anlayışının benimsenmesinin sağlanması gereklidir. Hiçbir sistem başlı başına etkinliği sağlayamaz. Bu açıdan belge yönetim prensiplerinin kurum çalışanları tarafından etkin öğrenilmesi ve buna ilişkin bilgilendirmelerin yapılması ve böylece belge yönetim prensiplerinin benimsenmesinin sağlanması gereklidir.
- Sistemin kullanımıyla ilgili eğitimlerin süreklilik anlayışı çerçevesinde gerçekleştirilmesi, sistemde oluşan değişikliklerle ilgili ek eğitimlerin verilmesinin sağlanması

Elektronik belge yönetim sisteminin ulaşmak istediği noktanın belirlenmesi ve bu çerçevede bir planlama yapılması, sistemin etkinliği açısından önemlidir. Bu bağlamda, elektronik belge yönetim sisteminin amaçları şöyle sıralanabilir (William, 2005:163);

- Takım çalışmasında dayalı bir sistemi desteklemek.
- Dosyalama, geri iletim ve arama araçlarını geliştirmek
- Dosyalama sisteminde elektronik belgelerin çıktılarının alınmasını azaltmak,
- Depolama alan ihtiyacının azaltılarak, kurum dışı depolama çözümlerinin aza indirilmesi,
- Bilgiye dayalı anlayışı benimsemek ve bunu bütün süreçlere uygulamak,
- Elektronik belgelere, doğru, uygun, hızlı ve etkin erişimin sağlanması,
- Açıklığa dayalı bir politikanın benimsenmesidir.

2.5.3. Sistemin Avantajları

E-belge yönetim sisteminin yasal ve mali faydaları yadsınamaz bir gerçektir. Karşı karşıya kalınacak muhtemel yasal yaptırım maliyetle düşünüldüğünde, e-belgenin düzenleme, tanımlama ve yönetimi maliyetinin oldukça basit kaldığı, yatırım karlılığının e-belge yönetim sistemi doğal sonucu olduğu görülecektir. Birçok kurum etkin elektronik belge yönetim çözümleri oluşturmakla hala mücadele etmektedirler. E-belge yönetiminin muhtemel yatırım kârlılığı düşünüldüğü zaman, diğer alanlar göre önemli avantaja sahip olduğu görülmektedir. Bu açıdan, belge yönetim faaliyetlerinin bütünüyle bilgi teknolojileri temelinde yürütülmesi büyük önem taşımaktadır. E-belge yönetim sistemi, belgelerin düzenlenmesi ve tanımlanmasına yönelik bedensel çalışmayı büyük oranda azaltabilir. Birçok belge basit bir bilgisayar komutuyla düzenlenebilir. Örneğin, mali ödeme dokümanları gibi rutin işler sonucunda oluşan belgeler otomatik olarak düzenlenebilir. Belge yönetimindeki en önemli öncelikli maliyet gerektiren alan, belgenin nasıl düzenleneceği ya da belge hüviyetinde olup olmadığı belirlemede belge yöneticilerinin harcadıkları zamandır. Eğer bu faaliyetler çok uzun zaman alıyorsa, belge yöneticileri, ya belgelerin tanımlanmasıyla yeterince ilgilenmeyecekler ya da işlerini düzensiz ve özensiz yapabileceklerdir. Belge yönetim sistemi olmadan, düzenlemeye tabi elektronik belge serilerinin bütünüyle tanımlanması ve korunması mümkün olmayacaktır. Belgelerin ayıklanması ve tanımlanmasının elle yapılması maliyeti

yüksek olacaktır. Bu açıdan belgelerin elektronik ortamda bir sistem içinde üretilmesi ve yönetilmesinin mali açıdan önemli getirileri olacaktır.

Elektronik belge yönetim sistemi kurumsal başarı açısından önemlidir. Özellikle mali açıdan sağladığı avantajlar sistemin oluşturulmasında önemli bir itici güç olmaktadır. Elektronik belge yönetim sisteminin finansal açıdan sağladığı avantajlar aşağıda değerlendirilmiştir;

- *Bulma Maliyeti:* E-belge yönetim sistemi, kurumların üst veri ya da tam metin aramayı kullanarak istenen belgeleri hızlı ve kolay ulaşmaya imkân tanıyarak bulma sürecini tamimiyle değiştirmiştir (Xerox DocuShare, 2006:10). Buna ek olarak, vaktinde ve sisteme dayalı imha süreçleri oluşturulabilmektedir. E- belge, oluşturulan elektronik belge yönetim sistemi içinde, pahalı olmayan bir biçimde farklı ortamlara kopyalanabilir ve istek sahibine ulaştırılabilir. Bu, bütün seviyelerde oldukça düşük bir bulma maliyeti sağlayacaktır.

- *Kâğıt Depolama Maliyeti:* Kurumlar, hala günlük iş akışları gereği oldukça büyük miktarda kâğıt çıktı almakta ve kullanmaktadır. Bunun sonucu olarak depolama maliyeti artmaktadır. Özellikle kurum dışı depolama hizmeti sunan şirketler aracılığıyla yapılırsa bu maliyet daha da artacaktır (Xerox DocuShare, 2006:11). Aynı zamanda doğru bir şekilde düzenlenmemiş ve tanımlanmamış kâğıt belgeler kurumun belge yönetim sistemi açısından büyük sorunlar yaratır. Kâğıt belgelerin, elektronik belgelerden farklı olarak üreten, üretim tarihi gibi üst veri elemanları sağlayan tanımlanabilir işlem geçmişi raporu sağlayacak bir yapısı yoktur. Bu çerçevede elektronik belge yönetim sistemine geçiş kaçınılmazdır.

- *Elektronik Belgelerin Depolanması:* Elektronik belgelerin düzenli bir şekilde yasal süreleri içinde imhasını sağlanması, kâğıt belgelerin depolamasında olduğu gibi yeni depolama ortamları ve buna bağlı donanımlar gerektirmez. Bununla birlikte, elektronik belge yönetim sistemi fazla nüshaların imhası ve gereksiz yedeklemeyle ilgili farkındalık yaratarak düzenli imha süreçlerinin oluşmasını sağlar (Xerox DocuShare, 2006:10).

3. BÖLÜM

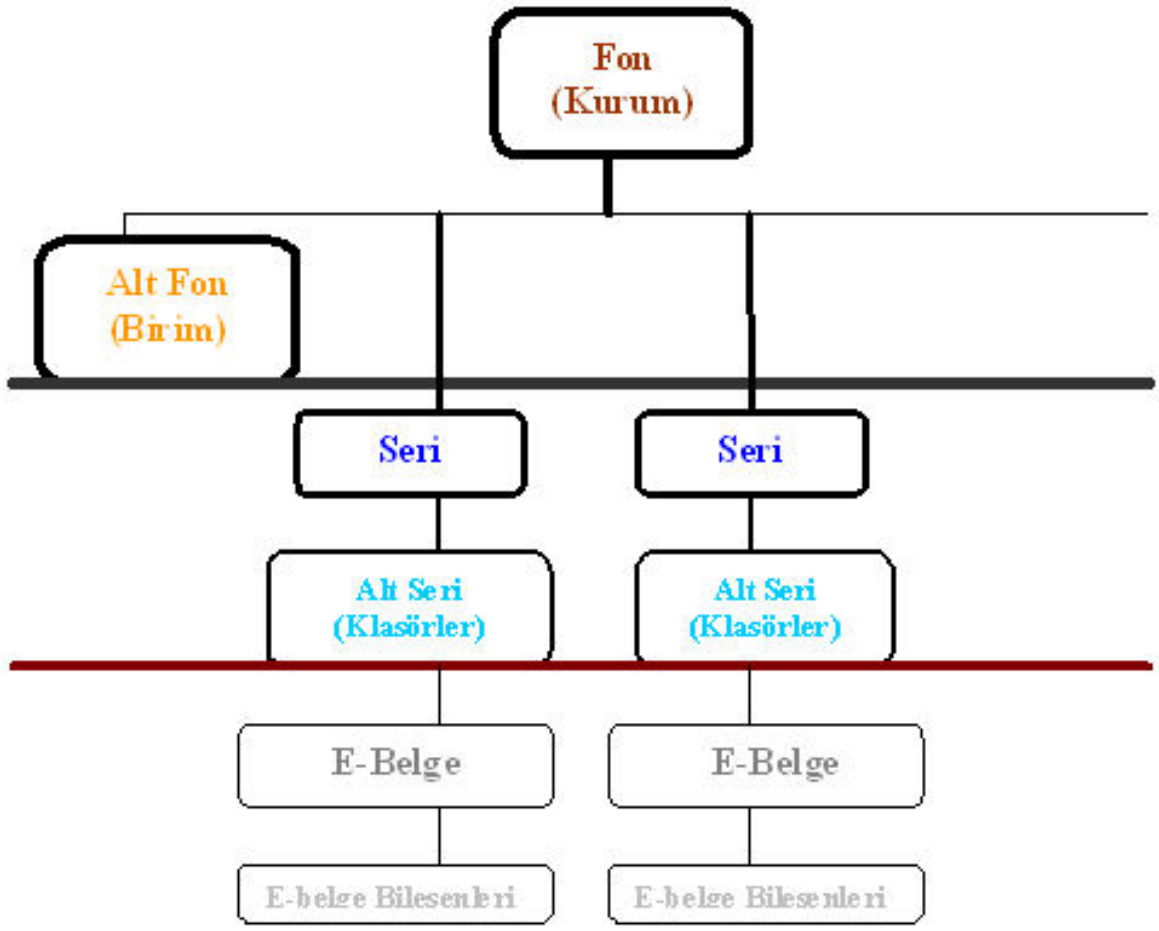
ELEKTRONİK BELGE ÜRETİMİ

3.1.Elektronik Ortamda Üretilen Belgeler

Elektronik belgeler genel olarak bilgisayar sisteminde değişik program ve yapılar içinde farklı birimlerde üretilen her türlü belgeyi kapsamaktadır. Elektronik belgeler ya tek bir uygulama programında ya da birbirine bağlı ve uyumlu birden fazla programda oluşturulabileceği gibi, bir elektronik belge birden fazla türde belge yapısı içerebilmektedir (Kandur, 1999b:16). Elektronik belgelerin üretim aşamasında kontrolü, kâğıt belgelere göre daha zor bir süreçtir. Bu sebeple e-belgeler üretilmeden önce sistem tanımlanmalı ve imhasına kadar giden süreç belirlenmelidir. Günümüz dinamik kurumsal yapılarında bilgi teknolojilerindeki gelişmelere bağlı olarak elektronik belgeler yoğun bir şekilde üretilmektedir (Menkus, 1996:3). Elektronik üretim sadece kurum içi aktiviteler sonucunda olmamakta, elektronik posta, web gibi yollarla da yapılmaktadır. Özdemirci (1996:19) belge üretimini "bir kurum ve kuruluşun işlemleri sonucu oluşacak belgelerin istenilen nitelikte ve nicelikte, istenilen zamanda ve mümkün olan en düşük maliyetle üretimini sağlayacak biçimde bir araya getirilmesidir" şeklinde tanımlamaktadır.

Belgenin nerde üretileceği ve uygun üst verilerin otomatik olarak nasıl elde edileceğini belirlemek için süreç analizinin yapılması gerekmektedir. Elektronik belgelerin, bilgisayar ortamında belge ya da veri dosyaları olarak veri tabanı yönetim sisteminde üretildiğinde, üretime ilişkin belge yönetim prensiplerinin kanuna uygunluğu sağlayan etkin belge yönetim uygulamalarını temin etmek gerekmektedir (Calrim, 2002:16). Elektronik dosyalar, büyük miktarda kâğıt dosyalar içeren dosya dolapları gibi büyük miktarda bilgisayar dosyaları içeren sabit diskte ya da ağdaki bir sabit diskte üretilir. Kâğıt dosyalar belge serileri içinde düzenlenirler. Belge serileri, aynı ya da ilgili belgeler grubuna verilen addır. Belge serisi kavramı bilgisayardaki elektronik belgelere de uygulanabilir. Kâğıt dosyalar, dosya dolapları ve dosya gömleklerindeki belge serilerince düzenlenirler. Benzer bir şekilde, elektronik dosyalar bilgisayar ortamında belge serileri şeklinde düzenlenmelidir. Elektronik ortamda üretilen belgelerin bir hiyerarşik yapı içinde düzenlenmesinin sağlanması gereklidir. Genel

olarak üretilen belgeleri, fon, seri ve dosya şeklinde üç seviyeli bir sınıflandırma yapısı içinde bulunması gereklidir. Bu seviyeler kendi içinde alt seviyelere ayrılabilirler. Bu kurum hiyerarşisi ve fonksiyonel çeşitliliğe bağlı olarak değişebilmektedir. Bu çerçevede Kandur (2006:23) tarafından ortaya konulan belge hiyerarşisi yaklaşımı ile birlikte değerlendirildiğinde Şekil 4'deki elektronik e-belge hiyerarşisi yaklaşımı benimsenmelidir.



Şekil 4. E-Belge Hiyerarşisi

Şekilde birinci düzeyde belirtilen Fon; elektronik belgeyi üreten kurumu ifade etmektedir. Alt fon ise kurum içindeki birimleri gösteren seviyedir. Kurumsal hiyerarşiye bağlı olarak fon düzeyi daha alt düzeylere ayrılabilir. Yani kurumsal yapıdaki alt birim

sayısına göre alt fon sayısı da artabilmektedir. Seri, kurumsal fonksiyonlar sonucu oluşan ancak benzerlik gösteren dosya ve klasörlerin tamamını ifade etmektedir. Alt seri ise konu ve vaka bütünlüğü olarak birlikte bulunması zorunlu elektronik belgeler bütündür. Fonksiyonlara göre seri düzeyi daha alt düzeylere ayrılabilir. Dosya tek bir işlem sonucunda oluşan elektronik belgedir. Bilgisayar literatüründeki dosya kavramı elektronik belgeye tekabül etmektedir. Dosya bileşeni ise bir elektronik belgeyi oluşturan çoklu ortam bileşenleri veya belgenin eklerini ifade etmektedir. Dosyalar klasörün içinde üretim tarihi ya da üzerinde yapılan işlem tarihine göre sıralanır. Klasör içinde bulunan dosyalar aynı fonksiyon sonucu üretilen belgelerdir. Dosya ya da klasörler uygulanan sisteme göre nümerik ya da alfa-nümerik olarak belirlenen kodlar çerçevesinde düzenlenmelidir. Bu çerçevede yapılacak bir standart düzenleme; dosyalara hızlı ve kolay erişimi, fazlalık dosyaların azalmasını, bilgi kaybının olmamasını, dosyaların hızlı ve kolay isimlendirilmesini ve etkin paylaşımı sağlayacaktır.

Elektronik belgeleri oluşturan bir takım unsurlar mevcuttur. Yani bir belgenin elektronik belge sayılabilmesi için Duranti (2001:41) bir takım elementlerin bulunması gerektiğini söylemektedir. Bunlar aşağıda değerlendirilmiştir;

- *Ortam***:** E-belgenin fiziksel taşıyıcısını ifade eder. Yani belgenin manyetik ya da optik elektronik olarak hangi ortamda bulunduğunu ifade eder
- *İçerik:* E-belgenin belirttiği, amaçladığı mesajı ifade eder. Yani e-belgenin yerine getirilen fonksiyon gereği sahip olduğu içeriktir.
- *Fiziksel ve Entelektüel Şekil ve Form:* E-belgenin iletilmesini sağlayan kurallarının bütününüdür.
- *Faaliyet:* E-belgenin hangi faaliyet sonucu oluştuğudur.
- *Arşivsel İlgi:* Her bir belgeyi öncekine ve sonrakine bağlayan ilişkiler bütünüdür.
- *Yasal ve İdari Çerçeve:* E-belgenin üretildiği yasal, yönetimsel, prosedürel çerçevedir.

Elektronik belge niteliği kazanılması için yukarıda belirtilen hususların tümünün bulunması gerekmektedir. Elektronik belge üretim safhasında bu hususlardan birinin eksik olması, e-belgenin gerçekliğini ve güvenirliliğini büyük oranda tehlikeye sokacaktır.

Elektronik belgelerin üretim safhasında FHWA (1999) tarafından ortaya konulan yerine getirilmesi gereken hususlar aşağıda değerlendirilmiştir;

- *Elektronik Belgelerin Tanımlanması***:** Elektronik belge yönetim gerekliliklerinin tanımlanmasındaki ilk aşama belge üretici ve kullanıcılarının tanımlanmasıdır. Bazı bilgiler ofis içinde farklı ortam ve uygulamalarda bulunabilir. Bu tür bilgiler elektronik belgenin nerede, nasıl, hangi ortamda ve ne kadar süreyle muhafaza edileceğinin kararının verilmesinde belirleyici faktördür.
- *Tanımlama Metotlarının Belirlenmesi***:** Tanımlamada iki metot üzerinde çalışılması gerekmektedir. Birincisi; belgenin durumunu belirlemek için her bir e-belgenin tekil olarak analiz etmektir. İkincisi ise; her bir e-belgenin aidiyetinin belirlenebileceği belge gruplarının oluşturulmasıdır.

Elektronik belge üretiminde kurum dışından resmi yazışmalar çerçevesinde gelen yazılarda değerlendirilmelidir. Bu belgelerin kurumsal e-belge üretim süreçleriyle ilişkilendirilmesi belge serilerinin bütünlüğü açısından önemlidir. Kâğıt belge olarak gelen kurum dışı yazı sonucunda oluşacak elektronik belge bir bütünlük içinde ele alınmalıdır. Burada kâğıt belge dijital ortama aktarılarak, elektronik belge üretim sürecine dahil edilmelidir. Kâğıt belgenin dijital ortama aktarılması sırasında bütünlüğünün ve gerçekliğinin korunmasına azami bir önem gösterilmelidir. Dijital ortama aktarılmış belgelerle elektronik ortamda üretilmiş belgeler arasında gerekli ilişkilendirmeler yapılmalıdır. Ayrıca gerek kurum dışından gelen ve gerek kurum dışına giden elektronik belgeler açısından birlikte işler unsurlarının sağlanması gereklidir. Elektronik belge yönetim sisteminde birlikte işlerlik önemli bir gerekliliktir. Kurumlarım elektronik belge yönetim sistemlerinin uyum içinde elektronik belge iletişimi kurmaları sağlanmalıdır. CITU (2000:15) tarafından ortaya konulan birlikte işlerlikle ilgili uyum seviyeleri aşağıda değerlendirilmiştir. Belirtilen düzeylerde bir uyumun gerçekleştirilmesi birlikte işlerliği sağlayacaktır;

- *Veri Düzeyi:* Teamüllerde ve kullanılan teknolojiler ve belge düzeyindeki üst veri standartlarında konusunda benzer yaklaşımı içermektedir.
- *Sistem Düzeyi:* Belge ve bilgi değişimine ilişkin sistem uyumu, standartlar, bilgi iletim protokolleri ve dosya formatlarının kullanımı ile taşıma stratejilerini içerir.

- *Prosedürel Düzey:* Bu düzey ortak fonksiyonlara ilişkin süreçlerdeki uyumu ifade etmektedir.

Bütün bu düzeyler de sağlanacak uyum, elektronik belge sistemlerinde alma ve gönderme işlemlerini ortak üst veri yapıları sayesinde kolaylaştıracaktır. Böylece belge üretiminde kurum dışından gelen belgeler açısından oluşabilecek olumsuzluklar önlenmiş olacaktır. Ayrıca kurumların elektronik belge yönetim sistemleri arasından birlikte işlerlik sağlıklı ve etkin gerçekleşecektir.

3.2. Kâğıt Belgelerin Dijitalleştirilmesi

Kâğıt ortamda üretilen belgelerin mevcut elektronik belge yönetin sistemine entegrasyonu, kurumun bütün belge yönetim faaliyetleri açısından büyük önem taşımaktadır. Kurum ve kuruluşların bütün belge yönetim faaliyetlerini tamamıyla sadece kâğıt ya da elektronik ortamda yürüttüğünü söylemek mümkün değildir. Ancak, iş ve işlemlerin büyük oranda elektronik ortamda yapıldığı değerlendirilirse, kâğıt ortamda üretilen belgelerinde elektronik belge yönetim sistemine entegre edilmesi gerekmektedir. Üretilen bütün kâğıt belgelerin dijitalleştirerek elektronik ortama aktarılması düşülemez. Burada yasal, idari, mali ve araştırma açıdan uzun dönem arşivlenmesi gerekli belgelerin seçilmesi ve buna ilişkin seçim kriterlerin ortaya konması gerekmektedir. Bu noktadan itibaren de belgenin bütünlüğünü, gerçekliğini ve güvenirliliğini koruyan bir dijitalleştirme faaliyetinin gerçekleştirilmesi gerekmektedir. Dijitalleştirilmiş kâğıt belgelerin, yasal açıdan gerçekliğinin olabilmesi için dijitalleşme sırasında değişime uğramadığına dair değiştirilemez bir zaman damgasının vurulması gerekmektedir. Bu işlem dijitalleştirme faaliyeti esnasında olabileceği gibi, dijitalleştirilen belgeye ayrı bir zaman damgası işlemi yapılmak suretiyle de gerçekleştirilebilir. Böylece dijital belgenin gerçekliği ve bütünlüğü korunmuş olur. Ancak yasal açıdan dijital ortama aktarılmış kâğıt belgelerin geçerliliği konusunda belirlenmiş kanuni hükümler bulunmamaktadır. Dolayısıyla kanıt niteliğine haiz olmadıkları değerlendirilmektedir. Bununla birlikte dijitalleştirilen belgelere vurulan zaman damgası elektronik belgelerle ilgili kanunlar bağlamında değerlendirilerek yasal açıdan kabul edilebilir.

3.2.1. Dijital Görüntüleme Sistemleri

Kâğıt ortamda üretilen belgelerin dijitalleştirilmesinde teknik alt yapının planlanması gerekmektedir. Görüntüleme teknolojileri, kâğıt belgelerin taramasını ve dijital ortama aktarılmasını sağlayarak elektronik doküman haline getirilmesini sağlayan sistemlerdir (Megill ve Schantz, 1999:41). Böylece diğer elektronik belgelerle birlikte bir bütünlük içinde yönetilmesi sağlanmış olur. Dijital görüntüleme işlemleri esas olarak, donanım ve yazılım bileşenlerini kullanarak görüntü yakalama, saklama, görüntüleme, işleme ve kayıtları elektronik olarak paylaşma olarak tanımlanabilir. Bir başka ifade ile dijital görüntüleme, belgelerin tarayıcılar aracılığıyla bilgisayar ortamına aktarılması ve analog formattan bilgisayar tarafından okunabilecek formata dönüştürülmesidir. Tarama işleminden sonra, belge görüntüsü farklı elektronik depolama ortamlarına aktarılabilir. Dijital Görüntüleme sistem bileşenlerini oluşturan yazılım ve donanımda teknolojiye bağımlı yaşanacak değişimler mutlaka göz önünde bulundurulmalıdır. Bu açıdan sistemde yazılımsal güncellemelerin ve donanımsal eklemelerin kolaylıkla yapılabilmesine imkân vermelidir. Sistem, verilerin taşınabilirliğini sağlamalı ve farklı yazılım ve donanım yapılarına belgelerin kolaylıkla aktarılmasını desteklemelidir. Dijital ortama aktarılan belgelerin yasal açıdan geçerliliğini sağlamak için, belgelerin güvenli bir ortamda dijital ortama aktarılmasının sağlanması gereklidir. Sistemin bunu sağladığının ve herhangi bir değişikliğe müsaade etmediğini ortaya koyması önemlidir.

Dijital görüntüleme sistemlerine bağlı teknolojinin çok hızlı bir şekilde değiştiği ve maliyetin artacağı önemle göz önünde bulundurulmalıdır. Bu çerçevede belgenin bütünlüğünü tehlikeye sokabilecek çözümlerden uzak durulmalıdır. Bu uzun dönem arşivleme ve yasal gereklilikleri karşılama açısından ciddi sıkıntılar yaratabilir. Dijital görüntüleme sistemlerini seçerken aşağıdaki hususların göz ününde bulundurulması gerekmektedir;

- *Optik çözünürlülük ve yoğunluk:* Optik çözünürlük tarayıcılarda inç başına düşen noktalar yani dpi ya da inç başına düşen piksellerdir. Dijital görüntüleme sistemleri seçerken taranacak belgenin en yüksek çözünürlülükte taranması gerektiği gerçeği göz önünde bulundurulmalıdır. Yoğunluk ise, belgenin ışıklandırılmış ve gölge alanlarını ayırt etmeden net bir şekilde görülmesini sağlar. Çözünürlülük, görüntülenen malzemenin niteliği ve kullanım amacına göre belirlenmelidir. Tarama çözünürlülüğünü belirlerken, istenen görüntü kalitesinin ve depolama kapasitesinin

Belge türü	**Çözünürlülük (minimum/optimum)**	**Notlar**
Basılı metin	400-600dpi	
Basılı fotoğraf	300-600dpi	Zenginleştirme ile 600dpi
Nadir eserler	300-500dpi	
Haritalar	200-400dpi	
Grafik ve Çizimler	300-600dpi	
Sanat eserleri	300-400dpi	
Negatif fotoğraflar, Şeffaf malzeme, vs	300-400dpi	400dpi çıktı sağlayacak tarama,
Mikro formlar	300-600dpi	Orijinal boyutta 300-400dpi

Tablo 1. Çözünürlülük Düzeyleri

- *Tonlama/Bit derinliği:* Tek bit ile temsil edilen tonlama türü olan siyah/beyaz tonlama, 8 bit ile temsil edilen gri tonlama ve genelde 24 bit ile temsil edilen renk ayrımlı tonlama türü olan renkli tonlama türü olmak üzere üç farklı tonlama vardır. Farklı malzeme türleri için tavsiye edilen tonlama şekilleri tablo 2'de gösterilmiştir (Kandur, 2006:69). Bu tonlama düzeyleri standartlarda belirtilen ve deneyimlenen hususlar çerçevesinde oluşturulmuştur. Ayrıca TSE 13298 standardında da belirtilmiştir.

Belge türü	Tonlama	Notlar
Basılı metin	S/B	
Basılı fotoğraf	Gri Tonlama ve renkli	Fotoğrafın rengine göre
Nadir eserler	Gri Tonlama ve renkli	Belgesel niteliklere göre
Haritalar	Gri Tonlama ve renkli	
Grafik ve Çizimler	Gri Tonlama	Küçültme yapılabilir
Sanat eserleri	Gri Tonlama ve renkli	Küçültme yapılabilir
Negatif fotoğraflar, Şeffaf malzeme, vs	Gri Tonlama ve renkli	Küçültme yapılabilir
Mikro formlar	S/B veya Gri tonlama	

Tablo 2. Tonlama Şekilleri

- *Hız ve bağlantı:* Sistem belgenin etkin ve hızlı bir şekilde taranmasına ve mevcut elektronik belge sistemin sorunsuz aktarılmasına imkân vermelidir.
- *Görüntüleme sisteminin belge boyutuna uygunluğu:* Görüntüleme sistem taranacak belge boyutları göz önünde bulundurularak seçilmelidir.
- *Farklı formatları kullanabilirlik:* Farklı dosya formatlarında tarama ve arşivlemeye imkân vermelidir. Görüntülenen belgenin saklama formatı gelecekte e-belgeye erişim ve teknolojik yeniliklere taşıma açısından son derece önemlidir. Seçilen dosya formatı doğrudan görüntüleme kalitesini ve dosyanın boyutunu etkiler (Minnesota Historical Society, 2004). Doğru dosya formatını seçebilmek için görüntünün nasıl kullanılacağının belirlenmesi gereklidir. Arşivleme açısından bir mastır kopyanın oluşturulması önemlidir. Bu kopyalar, erişim amaçlı kullanılan kopyalarda oluşabilecek kayıp ya da ihtilaf durumlarında birer başvuru niteliğindedirler. Bir başka ifade ile dijital mastır dosyalar, dijital ortama aktarılan belgelerin bir felaket, hırsızlık ya da bozulmaya uğrama ihtimaline karşı bir güvenlik önlemi olarak ayrıca saklanmalıdır (CDL, 2009:2). Mastır kopyalar için yüksek çözünürlülüğe sahip ve kayıpsız sıkıştırma gerçekleştirilebilen TIFF formatı en uygun formattır. TIFF formatındaki mastır kopyaların iletiminde ciddi sorunlar yaşanmakta ve yavaş bir iletim gerçekleşmektedir. Bu çerçevede erişim ve iletim hızını artırmak için PDF en uygun format olarak değerlendirilmekte ve kullanılmaktadır. Mevcut görüntü formatlarının en yaygın olanlarının özelliklerinin karşılaştırması tablo 3'de gösterilmiştir (Kandur, 2006:72). Ayrıca elektronik belge yönetim standardında kâğıt belgelerin dijitalleştirilmesine ilişkin hususların bulunduğu bölümde bu hususlar aynı şekilde belirtilmiştir.

Format adı ve versiyon	Dosya uzantısı	Tonlama	Sıkıştırma	Standart / Tescil	Renk Yönetimi
TIFF 6.0 Tagged Image File Format	.tif, .tiff	1 bit S/B 4/8 bit gri tonlama -64 bit renk	Sıkıştırmasız Kayıpsız sıkıştırma (ITU G4, LZW, vs) Kayıplı sıkıştırma (JPEG)	Resmi olmayan endüstri standardı	RGB Palette YcbCr CMYK CIE-Lab
GIF 89a Graphics Interchange Format	.gif	1-8 bit S/B, gri tonlama veya renkli	Sıkıştırmasız Kayıpsız sıkıştırma (ITU G4, LZW, vs) Kayıplı sıkıştırma (JPEG)	Resmi olmayan endüstri standardı	Palette
JPEG / JFIF Joint Photographic Expert Group JPEG File Interchange Format	.jpeg, .jpg, .jif, .jiff	8 bit gri tonlama 24 bit renkli	Kayıplı sıkıştırma (JPEG) Kayıpsız (JPEG-LS)	JPEG: ISO 10918-1/2 JFIF: Resmi olmayan endüstri standardı	YcbCr
Flashpix 1.0.2	.fpx	8 bit gri tonlama 24 bit renkli	Sıkıştırmasız Kayıplı sıkıştırma (JPEG)	Açık kaynak kodlu	PhotoYCC NIF RGB ICC
ImagePac, Photo CD	.pcd	24 bit renkli	Görsel olmayan Kayıplı sıkıştırma (Kodak Tescilli)	Marka Tescilli	PhotoYCC
PNG 1.2 Portable Network Graphics	.png	1-48 bit gri tonlama veya renkli	Kayıpsız	ISO 15948	Palette, sRGB, ICC
PDF Portable Document Format	.pdf	4 bit gri tonlama 8-64 bit renkli	Sıkıştırmasız Kayıpsız sıkıştırma (ITU G4, LZW, vs) Kayıplı sıkıştırma (JPEG)	Resmi olmayan endüstri standardı	RGB YcbCr CMYK

Tablo 3. Yaygın Görüntü Dosya Formatı

Dijital ortama aktarılan belgeler için depolama alanında kazanmak için sıkıştırma işlemi gerçekleştirilebilir. Kayıplı ve kayıpsız olmak üzere iki tür sıkıştırma işlemi yapılabilmektedir. Kayıpsız sıkıştırma işleminde herhangi bir veri kaybı söz konusu değildir. Kayıplı sıkıştırma işleminde veri kaybı bulunmaktadır. Kayba uğrayan veriler genel olarak gereksiz ya da fazla verilerdir. Sıkıştırma işleminin derecesine göre, bilgi kayıpları gözle görülmeyecek düzeyde olabilir. Dosyaların sıkıştırılması birkaç problem yaratmaktadır. İlki sıkıştırma işlemin uzun dönemdeki etkilerinin tam olarak anlaşılmaması. Sıkıştırma bilgilerin kaybolması ya da aynen aktarılması(kayıpsız) şeklinde olabilir. Bilgilerin aynen aktarılması, yani kayıpsız sıkıştırma sıkıştırılmış veriyi çözme şeklinde görüntüyü kayıpsız olarak yansıtmaktadır (Sitts, 2000:166). Bu, verinin sıkıştırılmadan önceki halinin aynısıdır. Fakat kayıplı sıkıştırmada görüntü sıkıştırıldıktan sonra açılmaktadır ve bu orijinal halinden farklıdır. Çünkü sıkıştırma işleminin bir parçası olarak bazı bilgiler kaybolmuştur. Genellikle kayıplı sıkıştırma işleminde kayıp, dosyasının sıkıştırılması gibi, gözle ayırt edilemeyecek noktalarda gerçekleşir. Ama bu durum tahmin edilemeyecek önemli sorunlara sebep olabilir. Diğer önemli bir nokta ise kayıplı ya da kayıpsız sıkıştırma işlemlerinin ikisi de dosyaları kodlama konusunda başka bir karmaşık aşama eklemektedir (Sitts, 2000:166). Bu durum gelecekte uzmanların kodlamayı çözüp dosyanın içeriğine ulaşmalarını daha da zorlaştırmaktadır. Çoğu sıkıştırma işlemi belirlenen standartlar çerçevesinde yapılsa da sıkıştırma işleminin karışıklığından dolayı ilerde okunabilir ya da kullanılabilir olmalarında önemli sorunlar yaşanacağı önemle göz önünde bulundurulmalıdır.

Dosyalarda gri tonlardan çok orijinal yapısına uygun renkli tonlar kullanılmalıdır. Renk orijinal belgenin gerekli bir parçası olduğu zaman, uygulanacak bütün sıkıştırma faaliyetleri kayıpsız olmalıdır (CDL, 2009:1). İkincil kopya dosyaları görüntülemek için kullanılan uygulamalar, zaman içinde değişebilmektedir. TIFF ITU-T.6 formatı Adobe Photo ve diğer görüntüleme programları tarafından yaygın kullanılan bir formattır. Bu format renkli belgelerin depolanmasında kullanılabilir. Bu format yüksek düzeyde ayrıntı sağlar. Kayıpsız sıkıştırma işlemi sonunda ortaya çıkan veri ile daha sonra sıkıştırma işleminin geri alınmasıyla ortaya çıkan veri hemen hemen aynıdır. JPEG formatı 24 bit kayıplı sıkıştırma formatı olarak hızlı görüntüleme için uygun bir formattır. JPEG bütün büyük bilgisayar uygulamaları tarafından desteklenmektedir. Kayıplı bir sıkıştırma işlemi yapıldığında, sıkıştırma işlemi yapılan görüntü önceki orijinal görüntüye göre görüntü kalitesi düşmüştür ve geriye dönüş söz konusu olmamaktadır. Az yer kapladığı ve kabul edilebilir bir görüntü kalitesinde olduğu için tercih edilebilir. Ancak arşivsel amaçlı olarak kesinlikle kullanılamaz.

(CDL, 2009:3). Dijital master dosyalar üzerinde filigranlama işlemi yapılmaması gereklidir. Görünebilen filigranlar görüntü kalitesini, bütünlüğünü ve birlikte işlerliği azaltmaktadır. Elektronik filigranların kullanılması görünmez olmaları dolayısıyla tavsiye edilmektedir.

Dijitalleşme işleminde kullanılacak tarayıcıların seçimi önemlidir. Bu seçimde, belgenin boyutu, belgenin renk yapısı, kâğıdın yıpranma durumu, tarayıcının sağladığı görüntü kalitesi, hızı ve desteklediği dosya formatları göz önünde bulundurulmalıdır. Bu çerçevede kâğıt belgelerin dijitalleştirilmesinde kullanılabilecek tarayıcı çeşitleri şöyle sıralanabilir;

- *Düz yatak tarayıcılar:* Kâğıt, düz fotoğraf ve diğer basılı materyalleri taramak için kullanılan bir tarayıcı türüdür. Bu tarayıcılar normal A4 boyutunda üretilen belgelerin dijital ortama aktarılmasında kullanılabilecek en uygun tarayıcılardır.
- *Geniş-format tarayıcıları:* Boyutu büyük belgeleri taramak için kullanılırlar. Mühendislik çizimleri, plan ve proje gibi büyük boyuttaki belgelerin taranmasında ciddi kolaylıklar sağlamaktadır.

3.2.2. Belge Tanıma Sistemleri

Tanıma teknolojilerinde önemli nokta belgeyi tanıma ve karakter tanımadaki güvenirlilik düzeyidir. Hayati belgeler için güvenlik düzeyi yüksek tutulmalıdır. Başarı oranının düşük olması, düzeltme maliyeti ve teknolojik maliyeti arttırır. Kâğıt ortamda üretilen belgelerin dijital ortama aktarıldıktan sonra ihtiyaca göre tanıma süreçlerinden geçirilebilirler. Dijitalleştirilen kâğıt belgeler için literatürde geçen karakter tanıma sistemleri aşağıdaki gibidir;

- *Optik Karakter Tanıma (OCR):* Optik karakter tanımada taranan belgenin görüntü analizi ve karakter görüntüleri, elektronik belge yönetim sisteminde kullanılan ASCII karakter kodlarına dönüştürülebilir. Esasında OCR farklı formatlardaki herhangi bir dosya içindeki yazıyı tanıyarak, sonradan tekrar düzenlenebilecek metin biçimine dönüştürmektedir. Bu noktada, belge üzerindeki karakterlerin baskı kalitesi, font, nokta büyüklüğü, tip ağırlığı gibi parametrelerle desteklenerek belirli bir oranda başarı ile elde edilebilir. Örneğin, JPG formatında bulunan bir belge OCR programımızla WORD ya da PDF dokümanı şekline dönüştürüp kaydedilebilmektedir. Böylece belge

- *Akıllı Karakter Tanıma (ICR):* Akıllı karakter tanıma, zayıf kalitedeki makine yazıları ile belli kurallar çerçevesindeki el yazılarının tanınmasında kullanılan bir yöntemdir. Yani, orijinal el yazısı olan belgelerin dijital ortama aktarılmasında kullanılan bir sistemdir. İşleyiş açısından, optik karakter tanıma işlemiyle benzerlik gösterir. Ayrıca, OCR ve ICR birlikte kullanılabilmektedir. ICR teknolojisi fontları ve farklı el yazısı stillerini öğrenebilmektedir. Bu ya belgeler üzerinde örnek olabilecek karakterlerin öğretilmesiyle ya da süreç içinde yeni karakter yapılarının girilerek sistemin gelişerek ilerlemesi şeklinde olabilir.

Belge üzerinde optik karakter tanıma işlemleri OCR yazılımları aracılığıyla yapılır. Tanıma işleminde yazılım önce sayfa üzerindeki metin yüzeyini analiz eder. Genelde mevcut paragraf düzeni içinde bölümlere ayırır. Daha sonra paragraf sırası belirlenerek karakterleri analiz etme işlemi başlar. Birçok OCR yazılımı, uygulama içinde bulunan sözlükle karşılaştırma yapmak suretiyle karakter gruplarına, kelimelere bakarak çalışır. Uygulama içindeki sözlükle eşleşme gerçekleşirse tanıma gerçekleşir, eğer eşleşme Gerçekleşmezse yazılım en yakın tahmini yaparak tanıma işlemini gerçekleştirir ve bu alana tam eşleşmenin gerçekleşmediğine dair işaret koyar (Sitts, 2000:130). Bazı tanıma sorunlarının olma ihtimali yüksektir. Zira hiçbir OCR yazılımı tam bir belge tanıma işlemi gerçekleştiremez. Ancak OCR yazılımının belge tanımada ki doğruluk başarısı mutlaka test edilmelidir. En yüksek düzeyde belge tanıma başarısı gösteren yazılımlar tercih edilmelidir. Burada önemli olan tanımada Türkçeye özgü (ü ğ, ç gibi), ASCII 128 dışında kalan karakterleri destekleyim desteklemediği konusudur. Eğer metin dosyalarını sadece araştırmayı desteklemek için kullanılıyorsa ve farklı formatta aynı belge bulunduğu için herhangi bir kullanım söz konusu olmayacaksa, belge tanıma işleminde doğruluk düzeyi biraz daha düşük düzeyde değerlendirilebilir.(Sitts, 2000:131).

Karakter tanıma sistemlerinin yanında doküman tanıma sistemleri de bulunmaktadır. Optik doküman tanıma sistemleri, şablon tabanlı form işleme olarak bilinir ve formların

tanınması ve belirli alanlarından verilerin okunarak bunların ilgili uygulamalara aktarılmasıdır. Özellikle nüfus sayım formları, Maliye Bakanlığının doldurulmasını istediği bildirgeler bu tür formlara örnek olarak verilebilir. Aklı doküman tanıma ise, temelinde formun yerleşimi ve yapısına bakarak tanınması ve bağlı olarak doküman künyesinin çıkarılmasına dayanır (TBD, 2009:66).

Elektronik belgelerin bütünlünü ve gerçekliği bağlamında belge tanıma sistemlerini değerlendirdiğimizde kullanımları farklılık göstermektedir. Zira belge tanıma sistemine tabi tutulmuş bir belgenin gerçekliği ve bütünlüğünden söz edilemez. Dijital ortama aktarılan bir belgeyi bütünüyle tanımlayan bir sistemde mevcut değildir. Bu açıdan belge tanıma sistemlerini daha çok belgeye erişim açısından değerlendirmek gerekmektedir. Belge tanıma sistemlerinden geçmiş belgeleri, erişim amaçlı kullanmak gerekmektedir. Yasal geçerlilik açısından her ne kadar dijital ortama aktarılmış belgenin zaman damgası olmaması durumunda geçerliliği olmasa da, arşivsel erişim amaçlı olarak belge tanıma sistemlerinden geçmemiş dijitalleşmiş belgeleri kullanmak gereklidir. Bu çerçevede dijital ortama aktarılan belgeler için gerekli ayrımın ve sınıflandırmanın yapılması gerekmektedir. Yani, erişim amaçlı ve arşivsel amaçlı kullanılacak belgeler olarak ayırmak faydalı olacaktır. Belge tanıma sistemlerinden geçmemiş belgeler de yasal açıdan geçerli olmasa da en azından orijinal belgenin kayıpsız görüntüsü görülebilecektir. Bu görüntülerin renkli çıktıları alınmak suretiyle yasal süreçlere belli oranda da olsa katkı sağlanabileceği düşünülmektedir.

4. BÖLÜM
ELEKTRONİK BELGELERİN ARŞİVLENMESİ

4.1. Arşivleme ve Dosya Türleri

4.1.1. Temel Gereklilikler

Elektronik belge yönetiminde elektronik belgelerin arşivlenmesi, büyük oranda paylaşılmış bilginin düzenlenmesi, organize edilmesi ve ulaşılabilir olmayı sağlamaya dayanmaktadır. Arşivleme sisteminin, elektronik belgeleri saklama süreleri boyunca yönetmesi gereklidir. Arşiv sistem fonksiyonları, kurum uygulamalarıyla bütünleşik ya da tamamıyla ayrı bir şekilde çalışmalıdır. Elektronik belgeler, kâğıdın saklama ortamından farklı bir saklama ortamı gerektirir. Kâğıtlar sadece okuyacak bir göze ihtiyaç duyarken, elektronik belgeler faydalı bir bilgi kaynağı olacak makinelere ihtiyaç duymaktadırlar. Rhodes (1991:16) tarafından ortaya konulan elektronik belgelerin arşivlenmesinin sağlıklı yürütebilmek tespit edilmesi gerekli öncelikli hususlar aşağıda değerlendirilmiştir;

- *Depolanan malzeme:* Ne tür malzemenin arşivleneceğinin, yani malzemelerin hangi formatta olacağının belirlenmesi gereklidir. Veri, grafik, video gibi formatlardan hangisini içereceği tespit edilmelidir.
- *Ne kadar süreyle saklanacağı ve ne kadar süreyle kullanım ihtiyacı olacağı*: Elektronik belgenin ne kadar süreyle saklanacağının ve kullanım ihtiyacının ne kadar süreceğinin belirlenmesi gereklidir. Buna göre arşivleme ortamları belirlenecektir.
- *Ne tür kullanımın olacağı:* Kullanıcıların belgeye ne şekilde ulaşacağının tespiti gereklidir. Yani çevrimiçi, anında, tam metin iletimi gibi şekillerden birinin belirlenmesi ve buna göre planlamanın yapılması gerekmektedir.
- *Belge yaşam döngüsünün hangi aşamasında dijital olacak:* Elektronik ortamda üretilmeyen belgenin yaşam döngüsünün hangi aşamasında dijital olacağının tespiti belge arşivleme aşamasının sağlıklı yürütülebilmesi için önemlidir.

- *Uzun dönem saklama kriterleri nelerdir*: Hız, fiyat, kapasite, kolay taşınabilirlik ve süreklilik gibi uzun dönem saklama kriterlerinin belirlenip, buna dönük gerekliliklerin yerine getirilmesi gerekmektedir.

Elektronik belgelerin sisteme bağımlı çalışmalarından dolayı üretildiği yazılım ve donanımın korunması ya da gelişen bilgi teknolojileri bağlamında yenilenmesi gerekmektedir (Aydın, 2003:41). Elektronik belgelerin arşivlenmesinde birinci önemli husus bağlı olduğu donanımdır. Bu yüzden elektronik ortamdaki veriler belli bir zaman sonra kullanılmaz duruma gelebilir. Optik diskler kimyasal bileşimine göre sürekliliği değişebilmektedir (Stepherd, 1994:43). Optik diskler için 10-15 yıllık bir ömür ifade edilse de, çok daha kısa bir sürede bozulmalar olmaktadır. Diğer yandan sabit diskler verileri iletemez duruma gelebilir. Değişen teknolojiler ve makinelerin nasıl hızlı bir şekilde etkilendiğini düşünülürse, geleceğin arşivlerinde e-belgelerin erişilebilirliğini sağlamak için bir makine müzesi oluşturulmasına ihtiyaç duyulacaktır. Bunun mümkün olmayacağı düşünülürse gelişen bilgi teknolojilerine paralel olarak oluşturulan elektronik belge yönetim sisteminin donanımının sürekli güncellenmesi gerekmektedir. İkinci önemli husus yazılımdır. Elektronik veriler yazılıma göre değişebilir ve yazılım yaşam döngüsünün iki yıldan daha az olduğu ileri sürülmektedir. Bu yüzden yazılımlardaki değişimler takip edilerek gelişmelere paralel olarak eski elektronik belgelerin yeni yazılımlarla uyumlu bir şekilde çalışması sağlanmalıdır.

Dijital arşivlemenin sağlıklı gerçekleştirilmesi için yapılması gerekenler noktasında Hollier (2001) tarafından ortaya konulan hususlar elektronik belgelerin arşivlenmesi açısından aşağıda değerlendirilmiştir;

- *Gerçeklik:* Elektronik belgelerin güvenirliliğini ve yasal geçerliliğini sağlanmasına yönelik teknik stratejilerin ne olduğunun ortaya konması ve buna dönük çalışmaların yapılması gereklidir.
- *Ayıklama ve Saklama Planları:* Bu süreçlerin nasıl geliştirileceği ve nasıl uygulanacağının sistem içinde tasarlanmış olması gereklidir.
- *Uzun dönem arşivlenmesi gereken belgelerin yeni sisteme taşınması:* Bu çerçevede uzun dönemde elektronik belgelerin nasıl erişilebilir ve kullanılabilir olacağına yönelik uygun planlamalar yapılmalıdır.

- *Depolama ortamı ve formatının seçimi:* Kurumsal yapı içinde depolama ortamı ve formatlarına yönelik uygun seçimlerin yapılması gereklidir
- *Üst veri:* Gerekli üst veri elemanlarının nasıl tanımlanacağı ve uygun belgelerle gerekli ilişkilendirmenin nasıl yapılacağının belirlenmesi gereklidir
- *Eğitim ve farkındalık yaratma:* İyi bir elektronik belge yönetim uygulamasını desteklemek için yürütülmesi gerekli eğitim faaliyetlerinin planlanması ve yerine getirilmesi gereklidir.

Elektronik belgelerin nasıl arşivleneceği kullanımına bağlı olarak değişmektedir. Elektronik belgelerin muhafazası, kâğıt belgelerle benzerlik gösterir. Güncel belgeler, kurumun günlük iş akışı içinde aktif bir şekilde kullanılırlar. Arşivleme gerektiğinde daha düşük bir aktivite süreci gerekebilir. Elektronik belgelerin kullanım sıklığına bağlı olarak farklı depolama araçları kullanılmaktadır. Bunlar manyetik, optik ve manyeto-optik gibi araçlardır (Calrim, 2002:28). Bu çerçevede uygun depolama araçlarının seçilmesi gereklidir.

Kurumlar, yönetimsel, iş ihtiyaçları ya da yasalarca düzenlenen en düşük kanuni saklama gerekliliklerini karşılamak için elektronik belgelerini arşivlenmesi gerekmektedir. Elektronik belgelerin uzun dönem ya da sürekli saklama gerekliliklerinden dolayı, kurum tarafından kullanılabilir ve erişilebilir formda korunmaları bir zorunluluktur. Diğer belgeler, sadece devlet arşivleri tarafından belirlenen belge imha yetkilendirmeleri çerçevesinde yasal bir şekilde imha edilebilir. Üretilen ya da alınan elektronik belgelerin bütünlüğünün muhafaza edilmesi, bir birim olarak erişilebilmesi, gösterilebilmesi ve yönetilebilmesi demektir. Elektronik belge yönetim politikalarının muhafaza edilmesi, bilgi yönetim ve depolama hususundaki kurumsal politikalarında korunması anlamına gelir. NECCC E-sign Policy Workgroup (2001:7) tarafından ortaya konulan elektronik belgele yönetim politikaların içermesi gereken arşivleme ile bağlantılı alanlar aşağıda değerlendirilmiştir;

- *Hangi elektronik belgeleri kapsayacağının belirlenmesi:* Elektronik belgeler uygun bir şekilde yönetilmelerini sağlayacak türler ya da seriler şeklinde gruplandırılmalıdır. Örneğin, bilgi türleri, ya üretildikleri iş faaliyetleri referans gösterilerek ya da grup türüne bakarak belirlenebilir. Bazı e-belgeler, kurum faaliyetleri için daha kritik olacaktır. Bu tür belgelerin erişilemez olmaları ya da kaybolmaları halinde kurumu risk altına girmesi dolayısıyla oluşabilecek yasal süreçlerde ihtiyaç duyulması

- *Dosya formatları için standartlar oluşturulması:* Politikalarda, her bir belge türü için onaylanmış veri dosya formatları belirlenmelidir. Bilgisayar sisteminde depolanmış bütün bilgilere erişmek ve göstermek için yazılım gereklidir (NECCC E-sign Policy Workgroup, 2001:8). Bu yazılım, yeni bir sürümün uygulanması, işletim sisteminde veya donanımdaki yenilemeler paralelinde değişebilir. E-belge depolamaya uygun onaylanmış ortam formatlarına yönelik politikalar, elektronik belgelerin uzun dönem erişilebilir olmalarını sağlamayı yardımcı olacaktır.
- *Bilgi yönetim fonksiyonları için sorumluluklar tanımlanması:* Etkin bir bilgi politikası, farklı bileşenlerini uygulamak için sorumlulukların tanımlanmasına ihtiyaç duyar. Elektronik belgelerde, sorumluluklar genelde programlar ve teknik personel arasında paylaşılmalıdır.
- Bütün saklama süreleri boyunca, elektronik belgelerin depolanması ve yönetimini sağlayacak prosedürlerin tanımlanması gereklidir.

4.1.2. Arşivleme

Arşivleme açısından önerilen hangi metodun belgelerin uzun vadede okunabilirliğini korumak açısından başarılı olacağını ya da daha az maliyetli olacağını tam olarak açıklığa kavuşturulamamıştır (Sproull ve Eisenberg, 2005:24). Bu açıdan, belgelerin arşivlenmesi belirli tip belgeler için uygun saklama tekniğini seçmeyi gerektirecektir. Arşivleme açısından bir elektronik belgeyi temsil eden orijinal veri akışını saklamak gereklidir. Bir arşiv farklı tür belgeler için farklı yaklaşımlar kullanabilmelidir. Aynı anda paralel olarak belirli bir türde kayıt için farklı yaklaşımlar aranması gereklidir. Elektronik belgeler, arşivcilerinin mevcut bir dizi saklama tekniğini anlaması ve hangisinin uygun olduğu ile ilgili değerlendirme yapması gerekecektir. Her bir yaklaşımının muhtemel dezavantajları ve maliyetleri olduğu için hizmetin seviyesine dayalı bazı tavizler gerekecektir (Sproull ve Eisenberg, 2005:24). Bu tavizler belirli bir kayıt ile ilgili işlevselliğin alt kümelerini korumayı kapsayabilir.

Uzun dönem arşivleme açısından, uygun standartların göz önünde bulundurulması, açık kaynak kodlu ve özel olmayan veri formatlarının kullanılması, zorunlu standartlarla

uyumlu olarak gerekli dokümantasyon ve üst verinin sağlanması büyük önem taşımaktadır (Hollier, 2001**).** Uzun dönem arşivleme açısından benimsenmiş tek bir çözüm bulunmamaktadır. Teknolojide yaşanan hızlı değişimde buna imkân vermemektedir. Ancak, ortaya konan bazı ortak yaklaşımlarda bulunmaktadır. Bilgi teknolojilerinde yaşanmakta olan hızlı değişim, temel olarak arşivlenecek olan belge türlerinde ve gelecekte etkin kullanımını sağlayacak buna bağlı teknolojik bileşenlerdeki değişimi kapsamaktadır. (Sproull ve Eisenberg, 2005:21) Teknolojik değişime yönelik planlamanın önemli unsur farklı eğilimleri ayırmak ve tanımlamaktır. Sistem değişikliği gerektiren unsurlar, sisteme ekleme gerektiren unsurlar ve sistemin değişime yönelik olarak yeterli düzeyde ölçülebilirliği sağlayan unsurlar çerçevesinde bir planlama gerçekleştirmek önemlidir.

Arşivlemede devlet arşivleri tarafından belirlenen, kamu kurumlarda tercih edilen teknik standartların ve bilgi teknolojileri mimarisinin kullanılması ve benimsenmesi gereklidir. Tercih edilen standartlar, ulusal ve uluslar arası standartlarla ilgili organlarınca tanınmış olan açık standart teknik özelliklerine uygun olmalıdır. Standartlar, benzer sistemler arasında belgelerin paylaşılması ve erişimini kolaylaştırmaya yardımcı olur. E-belgelerin, güvenlikle ilgili emirlerin öngördüğü çerçevede şifrelenmiş formda muhafaza edilmesi gereklidir. Elektronik belgeler, işlemler ve ağ üzerinden iletilmesi sırasında güvenlik amacıyla bazen şifrelenirler. Kamuya açık olmayan kişisel bilgiler içeren yüksek düzeyde hassas belgeler, verilen zaman diliminde şifreli formda arşivlenmelidir. Ancak, şifre çözme anahtarının kaybolması ya da tahrip olması, şifrelenmiş belgelere erişmede bazı kayıplara sebep olabilir. Güvenlikle ilgili böyle bir tespitin yapılması, kurumların elektronik belgeleri şifrelenmiş formda arşivlemeyi tercih etmemelerine yol açabilir. Bu açıdan şifre çözme anahtarlarının etkin muhafazasının önemi konusunda kurumda bilinçlendirme yapılmalıdır.

Elektronik belge saklama gerekliliklerini karşılayan saklama çözümleri geliştirilmesi gereklidir. Seçilen çözümlerin bazı hususları başarması gereklidir. Öncelikle, elektronik belgelerin orijinal işlevselliğini gereken düzeyde muhafaza etmesi önemlidir. Birçok e-belge, eğer orijinal ortamında sahip olduğu işlevini yerine getiremiyorsa ya da kullanılamıyorsa anlamını ve yararlılığını kaybetmiş demektir (NECCC E-sign Policy Workgroup, 2001:9). Bu açıdan, e-belgenin güncel teknolojiyle işlenebileceği ya da kullanılabileceği formatta muhafaza edilmesi önemli bir gerekliliktir. Ayrıca, elektronik belgelerin bileşenleri arasındaki bağlantının ve bağlamının korunması gereklidir. Bazı elektronik belgelerin anlamını açıklamak için, bütün gerekli dosya yapılarının ve belge bileşenleri arasındaki ilişkilerin

belgenin saklama periyodunda muhafaza edilmesi gereklidir. Örneğin, elektronik olarak imzalanmış belgeyi doğrulamak için kullanılan açık anahtarın belgenin saklama periyodunda muhafaza edilmesine ihtiyaç duyulabilir.

Elektronik belgelerin kamuda arşivlenmesinde; kanunlarda, remi kurallarda, düzenlemelerde, yönergelerde belirlenmiş gerekliliklerin de karşılaması bir zorunluluktur. Bu açıdan, resmi dokümanların değiştirilemeyeceği, taşınamayacağı, imha edilemeyeceği ya da silinemeyeceği anlamına gelen resmi belgelerin tamlık, bütünlük ve gerçekliğinin sağlanması önemli bir zorunluluktur. Ayrıca, e-belgelerin sistematik bir şekilde düzenlenen konu dosyalarıyla doğru bir şekilde birleştirmesi anlamına gelen kamu yönetiminin belge kurallarına uygunluk sağlanmalıdır. Bununla birlikte, yönetimsel süreçlerin hesap verebilirliği ve kanuna uygunluğu sağlanması gereklidir.

Kurumsal yapıda üretilen ve muhafaza edilen elektronik belgelerin imhasına yönelik etkin ve uygun yollar bulunması gereklidir Bu yollar, elektronik ortamda ayıklamaya yardımcı olmalı ve kurumların pasif elektronik belgelerinin devlet arşivlerine transferiyle ilgili zorunlulukları karşılamalıdır. İmhanın amacı, güncel işler için artık ihtiyaç duyulmayan tam, gerçek ve güvenilir elektronik belgelerin tasfiyesi olarak tanımlanır. Ancak, elektronik belgeler kâğıt belgeler gibi fiziksel birimler meydana getirmez. Sonuç olarak, beklide hiçbir zaman tam olmazlar. Buna karşılık, klasörler, hızlı bir şekilde kapanır, çünkü belli bir işlemlerin sonucunda oluşurlar. Bu yüzden, güncel işler için artık gerekli olmayan klasörler, belli bir zaman diliminden sonra seçilmeli ve uygun dosyalarla birleştirilmelidir. Böylelikle, elektronik dosyalar, dosyalama planındaki dosya seviyelerine göre düzenlenen belli zaman sürecine ait bütün tam dosyaları içerir. Elektronik dosyalardaki klasörler kronolojik olarak düzenlenebilir. Devlet arşivlerine transferinden sonra, her bir elektronik dosya bir arşivsel öğeyi ifade eder.

Saklama sürelerinin sona ermesinden sonra, elektronik dosyaların devlet arşivlerine gönderilmesi teklif edilmelidir. Bu dosyaların, işletme aktiviteleri ve işlemleriyle ilgili yönergeler ve direktifler, katılım ve onaylar, notlar, kabuller ve yorumlar gibi bütün bağlamsal bilgileri içermesi gereklidir. Bu aktivitelerle ilgili sorumluluklara ek olarak işlemlerin gelişimi, sistem tarafından belgelere otomatik ve tam olarak kaydedilmesi zorunludur. Bağlamsal bilginin, belgenin bir parçası ya da sürümü ya da eki olarak

arşivlenmesi bir zorunluluktur. Belgenin, klasörün ve dosyaların kaydedilmesi sürecinde üretilen üst bilgi ilgili objelerle birlikte de kaydedilir.

Elektronik belgelerin uzun dönem arşivlenmesi açısından zaman içindeki güvenirliliğini ve kullanılabilirliğini sağlamak için iyi tasarlanmış ve belgelendirilmiş bir plan gereklidir. Taşıma, koruma, üst veri ve XML gibi araçlar, yalnızca belgelerin korunmasına yardımcı olmaz aynı zamanda gerçek değerlerinin fark edilmesine yardımcı olur. Kurumdaki bilginin değeri bilgi teknolojilerine yapılan yatırımın ispatı niteliğindedir. Teknolojinin değişmesiyle birlikte, yazılım ve donanım eskiyip kullanılmaz hale gelecektir. O zaman zor seçimlerle karşı karşıya gelinebilir. Buradaki esas hedef, bilginin güvenirliliğinin ve yararlılığının, verimli ve etkin maliyetle korunmasıdır. Elektronik belgelerle ilgili herhangi bir koruma planı, yazılım ve donanımdaki değişiklikleri, depolama ortamlarındaki kısıtlamaları ve bilginin potansiyel kullanım değerini dikkate almak zorundadır (Minnesota Historical Society, 2004:2). Seçeneklerin keşfedilmesi aşamasında, ihtiyaçlar analizi, fiziksel depolama seçenekleri, dosya formatı seçenekleri ve dijital koruma teknikleri gibi hususların iyi bilinmesi gerekmektedir

Belgelerdeki belli verilere erişimin kanunlara dayalı olarak sınırlandırılıp sınırlandırılmadığının da tespit edilmesi önemlidir. Eğer bu durma yönelik sınırlandırmalar varsa, uzun dönem arşivleme ve erişim politikalarının bu sınırlamalara paralel olarak yapılması gerekecektir. En geniş anlamıyla, belgelerin kullanımı ve erişimimin düzenlenmesine ilişkin talepler, hangi saklama seçeneklerinin daha uygun olduğunu belirleyecek ve belgelerle birlikte üretilecek ve depolanacak üst veriyi ortaya koyacaktır. Üst veri, zaman içinde bilginin değerlendirilmesi, bulunması ve yönetilmesine imkân veren veri hakkındaki veridir.

Yaşam süresi, depolama ortam türüne bağlı olarak da değişebilmektedir. En uygun depolama ve kullanım şartları altında, optik diskler ve manyetik bantlar genellikle 5 ile 20 yıl arasında güvenli hizmet verebilmektedir (Minnesota Historical Society, 2004:4). Oysa normal şartlar altında, yaşam süresi beklentileri büyük oranda daha azdır. Çoğu belge, belirli, özel yazılım uygulamaları kullanılarak farklı dosya formatlarında üretilirler. Zaman içinde, bu uygulamaların yeni sürümleri çıkacaktır ya da üretimleri bütünüyle bitecektir. Çünkü sürümü yükseltilmiş uygulamalar, daha önce sürümde üretilmiş belgeleri okuyabilecek ya da okuyamayacaktır. Yazılımı kendi kendine korumak bir seçenek olabilir. Ancak maliyetle ilgili

soruların ötesinde ve daha önemli olarak, yazılımın zaman içinde göçmesi ve belgelere hiçbir şekilde erişilememesi riskiyle karşı karşıya bırakmasıdır. Arşivlemenin devamlılığı açısından ortak bir çözüm; yazılım ortamının sürekli değişmesiyle birlikte, dosyaların bir sürümden diğer bir sürüme ve bir formattan diğer bir formata dönüştürülmesidir.

Belgelerin elektronik versiyonunun, iyi bir şekilde muhafaza edilebilmesi ve etkin bir şekilde paylaşılması gereklidir. Belgenin genel kabul gerçekleşmende önce, belirli şartlar karşılanması gereklidir. E-belgelerin, resmi onay aşamasında gerçekliği ve değiştirilmediğinin garanti edilmesi gerekmektedir. Böylece onaylayıcının kabul etmeme durumu olmayacaktır. Buna ek olarak, belgelerin kullanılır olması zorunludur. Ayrıca, öngörülen güvenlik gereklilikleri teknik açıdan bakıldığında, elektronik belgenin arşivlenmesi için gerekli en düşük standartlardır. Aslında, uygun sistem tasarımı ve bakımı ile elektronik belgeler, kâğıt belgelere nazaran daha güvenilir ve kullanışlı olacaktır. Üstelik yedekleme elektronik belgelere erişime imkân tanırken, imha edilen ya da kayıp olan kâğıt belgeler yeniden üretilemeyecektir (Oatway, 2004:2). Belgeyi üreten birimler arasında paylaşıma açma, elektronik belgelerin diğer bir avantajıdır. Belgeleri diğer birimlerle paylaşmak, alıcı sistemin belgeyi anlamasını sağlayacak standartları karşılamasını gerektirir. Arşivlemenin sağılıklı gerçekleştirilmesi bütün bu hususları etkilemektedir.

Arşivleme de önemli hususlardan biride hata sezme ve düzeltme işlemidir. Çünkü veri bir uçtan diğer uca aktarılırken bazı bitler bozulabilir, bunun alıcı tarafından sezilmesi büyük önem taşımaktadır (Çölkesen, 2008:45). Öyle ki, veri paketinin içerisinde taşınan veri yükü bitleri bozulabileceği gibi paketin başlık kısmındaki alıcı veya gönderici adres de bozulabilir. Bu durumların sezilmesi ve mümkünse belgenin bütünlüğüne zarar vermeyecek şekilde düzeltilmesi gereklidir. Uzun dönem saklanması gereken belgelerin veri yapılarının bozulma olasılığı bulunmasından dolayı, arşivleme sisteminde hata sezme ve düzeltme teknikleri kullanılmalıdır. Hata sezmek için kullanılan tekniklerinden bazıları yalnızca hata olup olmadığını sezerken bazıları da belirli oranda hata düzeltmesi yapar. Hata sezme ve düzeltmede kullanılan teknikler; boyuna fazlalık sınaması, çevrimli fazlalık sınaması ve hamming kodlamasıdır (Çölkesen, 2008:55).

Arşivlenen ya da arşivlenecek veri ya da e-belge üzerinde bazı işlemler yapılır. Bunlar yeni veri ya da e-belge kaydetme, mevcut veriyi güncelleme, mevcut veri ya da e-belgeyi silme ve bu yapı içinde bilgi arama gibi işlemlerdir (Kurnaz, 2008:239). E-belge özelliğini kazanmış bir yapı üzerinde yukarıda bahsedilen güncelleme işleminin yapılması söz konusu

değildir. Zira yapılacak değişiklik ya da güncelleme, elektronik belgenin bütünlüğünü ve gerçekliğini ortadan kaldıracaktır. Diğer işlemlerde elektronik belge yönetim sistemi içinde belirli bir plan, program ve yetki çerçevesinde yapılır.

Hayati belgelerin korunması elektronik belge yönetiminin belge muhafaza safhasında önemli bir rol oynamalıdır (Menkus, 1996:4). Bu çerçevede hayati belgelerin korunması, devamlılık planı olarak dizayn edilmiş bir çerçevede geliştirilmelidir. Hayati belgelerin bir nüshası, kurum dışında kontrol altında güvenli bir ortamda arşivlenebilir. Bu anlamda elektronik belge saklama birimleri çevresel şartlara, elektrik ve manyetik alanlara karşı duyarlı olması sebebiyle bilginin güvenli kopyasının harici saklama birimlerine aktarılması gerekmektedir (Kandur, 1999b: 16). Bu yüzden elektronik belge arşivleme ortamları sürekli kontrol altında olmalı ve okunabilirliğini sağlayıcı önlemler alınmalıdır. Bununla birlikte teknolojik değişimlere paralel olarak yeni ürünlere transferini gerçekleştirmek gerekmektedir

4.1.3. Dosya Türleri

Genel olarak seçilen dosyanın türü arşivleme işleminin nasıl gerçekleştirileceğini belirleme açısından önemlidir. Bununla birlikte erişimin etkin ve hızlı gerçekleşmesini de doğrudan etkilemektedir. İçerdikleri bilgi türü bakımında dört ana elektronik dosya türü bulunmaktadır. Bunlar;

- Metin dosyaları,
- Görüntü dosyaları,
- Veri dosyaları
- Çoklu ortam dosyalarıdır.

Her bir dosya türü ile belge özel ya da özel olmayan formatlarda kaydedilebilir. Metin dosyaları için başlıca özel olmayan format ASCII dır. Bir ASCII metin doyası, klasör olarak da tanımlanır, zira metin özelliği ya da formatları içermez (Records Management Institute, 2000:3). Kelime işleme programları dokümana temel olarak ASCII metin dosyası kullanır ve kendi özel formatlarını metine uygularlar. Dosya uzantısı belirli bir uygulamanın özel formatını tanımlar. Başlıca kelime işleme yazılımları, dokümanların başka bir kelime işleme uygulamalarınca üretildiğini göstermek için özel bir filtre ile birlikte gelir.

Arşivleme açısından farklı formatlar kullanılır. Arşivlemede kullanılan TIFF formatı, çoğu görüntüleme sistemi tarafından desteklenen oldukça yaygın ve bozulmaz bir formattır. Genellikle veri tabanı formatında depolanan belgeler, klasörler ve dosyalarla ilgi bütün üst bilgiler, erişilebilir şekilde muhafaza edebilmek için ASCII dosya formatında gönderilmelidir. Günümüzde, bu format, dijital muhafaza açısından en iyi standartları sunuyor görünmektedir. TIFF formatı yerine, uluslar arası ISO8879 standart SGLM ve XML formatı gibi farklı alternatifler gözden geçirilmektedir. Ancak, TIFF dönüştürme işleminde standardı oluşmuş bir formattır. Ancak SGML ya da XML dönüştürme işlemi için hala özel gereklilikler sağlanmasına ihtiyaç vardır.

Uzun dönem dosya arşivleme için özel olmayan formatlar en ideal formatlar olmasına rağmen, az sayıda olmaları ve birtakım kısıtlayıcı unsurlar içermeleri dolayısıyla pek tercih edilmemektedir. ASCII ya da düz metin, veriyi yaygınlığı düşük formatta, yapıda ve fonksiyonda kayıplarla kaydedecektir. Metin dosyası olarak adlandırılan Word ve zengin metin formatı (RTF) bir Microsoft formatıdır. Bununla beraber birçok satıcı ve yazılım uygulamalarınca da desteklenmektedir. Adobe'nin ürünü PDF formatı, dosya paylaşımı ve depolanması için yaygın olarak kullanılmaktadır. Çünkü Adobe PDF özelliklerini herkesin kullanabileceği şekilde tasarlamış ve açık bir standart olarak kullanıma sunmuştur. Aslında şirketin gelecekte bu uygulamayı devam ettirme konusunda yasal bir zorunluluğu yoktur. Bunun yanında, PDF formatının geriye uyumluluk ile ilgili sorunları bulunmaktadır. Yeni sürüm genellikle eski sürümle üretilmiş dosyaları doğru bir şekilde okuyamamaktadır. Bu sorunun çözümüne yönelik olarak PDF/A olarak hâlihazırda belirlenmiş arşivsel bir sürüm geliştirilmiştir (Minnesota Historical Society, 2004: 4).

E-belge formatları, uzun dönem arşivleme ve gelecekte okunabilirlik açısından Adobe PDF'den PDF/A'ya ya da PDF arşive doğru bir gelişme göstermektedir. Benzer sorunları yaşamamak için, Microsoft, kendi açık belge format olan ASP'yi oluşturdu. Buradaki amaç, uzun dönem arşivleme ve okunabilirliktir. XPS, uzun dönem koruma gerektiren e-belgelerin depolanması için gerekli standart formatta PDF/A ile benzerlik gösterir (Xerox DocuShare, 2006:15). Bir formatın başka bir formata dönüştürülmesi kullanışlı olduğundan, diğer format standart ve sabit olduğunda görüntüleyici sonsuza kadar elverişli olacaktır. Bu tarz standart ve sabit formatların arzu edilen özellikleri genel tanımlama, geniş uygulanabilirlik, önceki versiyonlarla uygunluk ve yavaş hızda değişim gibi faktörleri kapsar. PDF/A standardı

arşivsel özelliklere sahip formatların geliştirilmesi ve kabul edilmesinin yaygınlaştırılmasına yardımcı olmaya devam etmektedir (Sproull ve Eisenberg, 2005:30). Microsoft ve Adobe birbirleriyle rekabete ederken, Sun open office gibi platform bağımsız olan açık standart tabanlı ürünleri üreten birkaç şirketlerden biridir. Kurumlar, mikrosoft'un belli bir tekel yaratan e-belge formatlarına alternatif olarak, uzun dönem arşivleme, erişim ve okunabilirlik açısından bu farklı ürünleri kullanabilmektedir.

Zaman içinde teknolojide yaşanacak tahmin edilen değişmelere rağmen, gelecekte, arşivleme için büyük zorluklar yaratacak birçok veri ve alt veri türü olacaktır. Bütün bu veri türlerini aynı düzeyde destekleyen bir sistem oluşturmak ve sürdürmek oldukça zordur. Ancak önemli belgeler XML gibi formatlarda üretilebilir (Sproull ve Eisenberg, 2005:21). Bu bağlamda, uzun dönem arşivleme ve kullanım açısından, XML şu anda en uygun format seçeneği olarak görülmektedir. 1998 yılından buyana ulusları bir standart olarak, XML hem dosya formatı ve metin tabanlı, hem de kendini tanımlayabilen, donanım ve uygulama sistemlerinden bağımsız insanın okuyabileceği işaretleme dilindedir (Minnesota Historical Society, 2004:5). Çünkü altyapından bağımsızdır. XML belgenin içeriğini yeniden tasarlama ve/veya diğerleriyle paylaşma bakımından en iyi çözümdür. XML in doğru kullanımı, belli oranda gerekli planlamanın yapılması, bunun paralelinde para ve zaman gerektirir. Ancak, yapısal niteliği dolayısıyla, gelecekte muhtemel oluşabilecek açık formatlara ilişkin takip yapabilmeye imkân tanımaktadır.

Elektronik belgelerin belirlenmiş saklama planları olması gereklidir. Saklama planları aynı zamanda elektronik depolama ortamlarının ve araçlarının etkin kullanımını da ifade eder. ASCII (American Standart Code for Information Interchange) metin dosyaları yazılım bağımlılığını azaltır ve ürün eskimesine karşı birtakım önlemler sağlar (Records Management Institute, 2000:1). Dosya sıkıştırma, sabit diskte ve yedekleme ünitesinde kullanılacak depolama alanını azaltmak ve ağdaki bilgi akışını hızlandırmak için kullanılabilir. Bununla birlikte, uzun dönem arşivleme için dosya sıkıştırma işlemini yapmamak, gelecekte oluşabilecek problemleri azaltacaktır. Belge yöneticisi her zaman ASCII metin formatını uzun dönem saklama gerektiren özel formattaki elektronik belgelerin yerine ya da birlikte göz önünde bulundurmalıdır (Records Management Institute, 2000:6). ASCII formatına dönüştüren ya da ASCII formatından orijinal formatına dönüştüren yöntemler bulunmaktadır. Metinselden kod çözme (Uudecode) ve metinsele kodlama (Uuencode) ASCII formatıyla ilgili dönüştürme işlemleri yapılmasını sağlayan yöntemlerdir. Bu yöntem yazılacak

elektronik belge yönetim yazılımı içine bir kütüphane olarak eklenebileceği gibi, ayrıca da kullanılabilir. Sadece bu işlemleri yapan yazılımlar da bulunmaktadır. ASCII formatından sadece orijinal formatına dönüştürme yapılabilmektedir. Farklı formatta bir dönüştürme yapmak mümkün değildir.

Bütün bu hususlar çerçevesinde farklı dosya türlerinin olduğu değerlendirildiğinde, dosya türünün seçiminde göz önünde bulundurulması gereken hususların mutlaka değerlendirilmesi gerekmektedir. Bunlar, aşağıdaki gibidir;

- *Erişilebilirlik:* Belgelerin erişilebilir ve görüntülenebilir formatta olması gereklidir.
- *Uzun Ömürlülük:* Dosya formatını üretenlerin uzun süre destek vermeyi sağlamları gereklidir. Eğer bu sağlanamıyorsa uzun vadede elektronik belgelerin kullanılabilirliği söz konusu değildir.
- *Esneklik:* Seçilen dosya formatı elektronik belgelerin paylaşımı ve kullanımıyla ilgili kurumsal amaçları mutlaka karşılamalıdır. Eğer seçilen dosya türü sadece belli bir yazılım ve donanım profiliyle okunabiliyorsa veya yaygın kullanımda olan bir format değilse, elektronik belgenin kullanımı ve paylaşımının sınırlı olduğu değerlendirilir.

Format seçiminde belirtilen hususlar göz önünde bulundurulduğunda PDF ve XML formatı elektronik belgelerin için kullanılan yaygın dosya formatı olarak değerlendirilmektedir. PDF formatında imzalama denildiğinde, PDF formatındaki elektronik belgenin içinde e-imzanın görsel olarak görülebilmesi anlamına gelmektedir. PDF formatında imzalamanın en büyük avantajı imzanın kullanıcı tarafından görülebilmesidir. Elektronik imza ile ilgili bilgi eksikliğinin yaygın olduğu düşünülürse görünebilirlik olumlu olarak değerlendirilebilir. XML formatında ise elektronik belgenin özellikle imza kısmı anlaşılırlıktan uzak karakterlerinden oluşmaktadır. Ancak XSL formatıyla bu durum düzeltilebilmektedir. Yukarıda belirtildiği gibi seçilen dosya formatının belgenin etkin paylaşım ve kullanımına uygun olması gereklidir. Bu durumda imzalı verilerin ne kadarının paylaşılmak istendiğinde önem taşımaktadır. XML formatındaki bir elektronik belgenin istenilen kısımlarının imzalanması ve değişik kısımlarını değişik kullanıcılara imzalattırılması mümkündür. (Yalçınkaya, 2008:64) Bu veri paylaşımında esneklik sağlayan bir yöntemdir. PDF formatında ise, elektronik belgenin bir kısmını imzalanması veya paylaşılması mümkün olmamaktadır. PDF imzalama kullanılıyorsa dosyanın tamamını paylaşmak zorunda kalınacaktır. Boyut açısından da XML formatı, düz metin tabanlı bir format olduğundan

dolayı, aynı içerik için, PDF formatına göre daha küçük boyutta olacaktır. Esneklik açısından PDF formatı XML formatına göre kullanıma daha uygundur. Zira PDF formatında imzalama ve imza doğrulama işlemleri Adobe ürünleriyle kolay bir şekilde gerçekleştirilebilmektedir. Ancak XML formatında imzalama ve imza doğrulama işlemleri XML araçları bulunsa dahi ihtiyaçlar doğrultusunda özelleştirmek gerekebilecektir XML formatına ait e-imzalama ve imza doğrulama süreci XAdes standardına net olarak tanımlanmıştır.

4.1.4. Arşivleme Mekân Özellikleri

Arşivlemenin sağlıklı yürütülmesi açısından fiziksel depolama tesislerinin oluşturulmasında ya da seçilmesinde bazı hususların göz önünde bulundurulması gereklidir. Öncelikle fiziksel depolama alanının ya da bu amaçla dizayn edilmiş alanların, elektronik belgeleri bulunduğu donanımları depolaması, operasyonel ve yasal olarak gerekli olduğu sürece etkin korumayı sağlaması gerekmektedir. Ayrıca, seçilen depolama alanına bağlı olarak depolama hizmetlerinin kullanımı ve erişimle ilgili usuller, belgelerin kontrolü, eklenmesi ve imhasının kim tarafından yapılabileceği noktasında detaylandırılmalıdır. Arşivleme hizmetleri ve usulleriyle ilgili politikalar bütün belge yönetim stratejileriyle içi içe geçmesi gereklidir. Elektronik belgelerin muhafazası için kullanılan donanımlar ve diğer ilgili ekipmanlara yönelik olarak istenen nitelikte depolama tesisi sağlamak için Minnesota Historical Society (2004:2) tarafından ortaya konulan hususlar aşağıda değerlendirilmiştir;

- *Yeterli alan*: Buna yönelik tespit edilmesi gereken hususlar şunlardır;

    1. Depolanacak elektronik materyalin miktarı,
    2. Gelecekte depolanması öngörülen materyalin miktarı,
    3. Belli bir zamanda ne kadar miktarda materyalin depolanacağını görmek amacıyla saklama planının tespiti,
    4. Farklı ortamlar için alan gereksinimlerinin belirlenmesi

- *Güvenlik:* Depolama hizmetlerine sadece yetkili kişilerin erişimine izin verilmesi gereklidir. Buna bağlı olarak aşağıdaki hususlar göz önünde bulundurulmalıdır;

    1. Kontrollü bir giriş: Güvenlik kodu ve smart kart gibi uygulamalar kullanılabilir.

2. Depolama tesisine yetkili olmayan bir kişi girmeye çalıştığında aktif hale gelecek bir alarm sistemi bulunmalıdır.

- *Uygun mekân:* Çevrimdışı depolama tesisindeki belgelere hangi sıklıkta erişimin gerekli olacağını göz önünde bulundurmak depolama tesisinin ne kadar merkezi yerde olmasına ihtiyaç duyulduğunun belirlenmesine yardımcı olacaktır. Bu çerçevede uygun depolama mekânın belirmesi gereklidir.
- *Ayarlanabilir aydınlatma:* Depolama tesisi, kullanacak kişilerin ihtiyaç duyacağı oranda yeterli aydınlatmaya sahip olması gereklidir. Ancak, kullanım olmadığında depolanan materyalleri korumak için oldukça karanlık olması sağlanmalıdır.
- *Havalandırma:* Uygun havalandırma sisteminin bulunması gereklidir.
- *Isı ve nem kontrolü:* Uygun nem ve sıcaklık, dijital ortamdaki elektronik belgeleri korumak için gereklidir. Belirlenen düzeyin üstünde ya da altında ne kadar sıcaklığın elektronik belgelerin bozulmasına sebep olduğu göz önünde bulundurulmalıdır. Öngörülen sıcaklık, 68 f +-2 f ve nem 40% +-5% olmalıdır.
- *Temiz hava kalitesi:* Depolama tesisindeki hava, kirleticilerden arındırılmış olmalıdır. Toz, özellikle dijital ortamlara zarar verebilir.
- *Tahribatı önleme:* Yangın, duman ve su akıntılarına, manyetik etkilere karşı depolama tesisi korunmalıdır.

Elektronik belgelerin arşivlendiği donanım unsurlarının bulunduğu mekânların yukarda belirtilen hususlar çerçevesinde oluşturulan fiziksel alanlarda bulundurulması etkin arşivleme açısından önemli bir husustur. Bu hususlara paralel olarak elektronik arşivlemenin sağlıklı yapılabilmesi için State of North Dakota (1998) tarafından ortaya konulan çevresel ve ortama ilişkin önlemler aşağıdaki değerlendirilmiştir;

- Depolama araçlarından her türlü yiyecek ve içeceğin uzak tutulması, bu alanlara bu şekilde girilmemesi
- Depolama disklerinin ve bantlarının dikey pozisyonda ve tozdan uzak bir ortama muhafaza edilmesi
- Depolama disklerinin ve bantlarının uygun ısı ve nemde muhafazasının sağlanması gereklidir. Isı ve nemde ani dalgalanmalar ya da değişimler, bantların bozulmasını hızlandırabilir.
- Elektronik belgelerin düzenli bir şekilde yedeklerinin alınması, böylece makine ya da insan hatasından oluşabilecek bilgi kayıpları önlenmesi sağlanacaktır

- İkincil nüshaların orijinal depolama ortamlarından farklı bir ortamda muhafazasının sağlanması
- Belli aralıklarla depolama disklerinde ya da bantlarında herhangi bir veri kaybının olup olmadığının test edilmesi, varsa düzeltilmesi ve buna ilişkin kayıpların nerden kaynaklandığının bulunması,
- Uzun dönem arşivlenen ya da sürekli arşivlenmesi gereken elektronik belgelerin bulunduğu ortamların belirli aralıklarla bir test edilmesi ve yeni depolama ortamlarına sağlıklı bir şekilde aktarımının sağlanması
- Depolama disklerinin ve bantlarının temiz muhafaza edilmesinin sağlanması
- Depolama disklerinin ve bantlarının telefon da dahil olmak üzere güçlü elektrik ve manyetik akımlardan uzak tutulması,
- Yetkisiz kişilerin elektronik belgelerin bulunduğu bilgisayarlara, bantlara, disklere ya da dokümanlara erişiminin engellenmesi sağlanmalıdır.

Yukarıda belirtilen hususlarla birlikte arşiv mekânlarıyla düzenlenmesiyle ilgili standartlar da mutlaka göz önünde bulundurulmalıdır. Bu bağlamda TSE 13212: Arşiv Mekânlarının Düzenlenmesi standardı arşiv mekânı oluşturmada değerlendirilmelidir. Ancak, arşiv mekânında elektronik belgelerin depolandığı fiziksel araçlar bulunacağı için standartta belirtilen bütün hususların uygulanması söz konusu değildir. Özellikle yapı ve iç donanım özelliklerinde, arşiv malzemelerinin korunması ile ilgili kurallarda belirtilen ilgili hususlar değerlendirilmelidir. Elektronik belgelerin depolandığı fiziksel araçlar sistem odası diye tabir edilen mekânlarda da muhafaza edilebilmektedir. Bu elektronik belge yoğunluğuna ve bunun için gerekli donanım miktarına göre değişebilmektedir. Yani, ayrı bir elektronik arşiv mekânı da duruma göre oluşturulabilmektedir. Ancak her iki durumda da temel yaklaşım, çevresel tehlikelere, kazalara ve bilinçli saldırılara karşı dayanıklı elektronik arşiv mekânlarının oluşturulmasıdır. Bunun içinde, çevresel tehlikeler olarak nitelenebilecek yangın, duman, toz, deprem, patlama, aşırı sıcaklıklar, yıldırım, titreşim, nem ve suya karşı uygun önlemlerin alınması gereklidir. Ayrıca arşiv mekânına yönelik bilinçli olarak olabilecek saldırılara karşı kapı denetimi ve alarm sistemi mutlaka oluşturulmalıdır. Bununla birlikte elektronik belgelerin arşivleneceği fiziksel mekânın ağ yapısının büyük miktarlardaki bilginin, ses, veri ve görüntü şeklinde iletim ve paylaşımını sağlayan; internet, intranet, video konferans, IP Telefonu vb. uygulamaları destekleyen yapısal kablolamaya sahip olması gereklidir. Bu elektronik belge yönetim sisteminin hızlı, sağlıklı ve problemsiz çalışmasını sağlayacaktır.

Bununla birlikte e-belgeleri depolayacak, erişilebilir yapacak ve dağıtımını gerçekleştirecek üçüncü parti arşivleme tesislerinin de kullanımı göz önünde bulundurulmalıdır. Ancak üçüncü parti depolama tesislerinin bütün operasyonel ve yasal gereklilikleri karşıladığından emin olunması önemli bir gerekliliktir.

4.2. Teknolojik Gereksinimler

Yazılım ve donanımla ilgili teknolojik bileşenler, elektronik ortamda üretilen ve depolanan bilginin okunması ve işlenmesi için gerekli teknolojik unsurlardır. E-belge, ayrıntılı bir bilgi sisteminin ve/veya kodlarının ne ifade ettiğini çözmek için bilgisayara bağlı donanımına ihtiyaç duymaktadır. Bilgiler genellikle kodlanmıştır. Bunu görmek için belirli bir yazılım sistemiyle çalışan bilgisayar programına ihtiyaç bulunmaktadır. Bu durum belirli bir donanım platformu gerektirmektedir. Buna ek olarak, e-belgeler genellikle belirli bir tip sürücünün bağlı olduğu belirli bir tip bilgisayara ihtiyaç duyan fiziksel aygıtlarda depolanmaktadır (Sitts, 2000:166). Teknolojik ürünler anlamında tek bir markaya bağımlılığı önlemek için, farklı markalarda teknolojik bileşenler alınmalı ve sistemin farklı marka ürünleri üzerinde de sağlıklı çalışması için gerekli çalışmalar yapılmalıdır (Sproull ve Eisenberg, 2005:23). Bu bağlamda bilgi teknolojileri; sistemin dizaynı ve analizi, verinin dönüşümü, bilgisayar programlama, e-belge depolama ve iletim, ses, video ve veri iletişimleri, sistem kontrolleri, simülasyon, insan ve makine arasındaki bütün etkileşim dahil olmak üzere bütün bilgisayara uyarlanmış ve otomasyonu yapılmış işlenmiş bilgi anlamına gelmektedir (Calrim, 2002:7). Bilgi teknolojilerinin yönetimi, planlama, bütçeleme, organize etme, yönetme, eğitim, değerlendirme ve bilgi teknolojileri uygulamalarıyla ilişkili diğer kontrol aktiviteleridir. Bu, toplamak, kaydetmek, işlemek, depolamak, erişmek, göstermek ve bilgiyi iletmek için dizayn edilmiş, oluşturulmuş, yönetilmiş prosedürler donanım ve yazılımları içerir. Bu aynı zamanda ilgili personel, danışman ve uygulayıcıları da içerebilmektedir. Bilgi teknolojileri bağlamında değerlendirildiğinde, e-belgelerin arşivlenmesinde, fiziksel depolama ortamları ve buna bağlı yazılım ve donanım ömürleri dolayısıyla bazı sorunlarla karşı karşıya kalınmaktadır. Aslında, bilgi hangi ortamda bulunursa bulunsun, hepsinin belli sınırlı bir yaşam süresi bulunmaktadır. Bir bilginin değeri, uzun bir depolama süresinden sonra okunabilmesine ve erişilebilir olabilmesine bağlıdır (Stamatiadis, 2005:56). Elektronik arşivleme, karmaşık ve çok yönlü teknolojik unsurları içermesi dolayısıyla, arşivleme açısından diğer ortamlar için söylenebilecek zaman sınırının dışında tutulabilmektedir.

Bilgi teknolojileri önemli bir varlık olarak yönetilmelidir. Bu prensibe uygun olarak, hizmet kalitesini arttırma, maliyeti düşürme noktasında sunduğu imkânlar sebebiyle modern bir kamu kurumu için vazgeçilmez bir araçtır. Ancak teknolojinin hızlı değişimi düşünüldüğünde esas konu araçların uzun ömürlü olması değil, teknolojik anlamda kullanılmaz hale gelmesidir. On yıl sonra hangi uygulama programı kullanılacak? Günümüzde üretilen elektronik belgelerin içindeki bilgilerin kayıtların okunmasını sağlayacak mı? Belge yönetiminin temel felsefesi olan doğu bilgiyi, doğru zamanda, doğru kişiye doğru bir şekilde ulaştırma, uzun dönemli bakışı doğrulamaktadır (Calrim, 2002:8). Bu çerçevede bilgi teknolojinin temel bileşenleri olan yazılım ve donanım bu bakış açısıyla planlanmalı ve gerçekleştirilmelidir.

4.2.1. Donanım

Donanım, elektronik ortamda belgenin üretilmesi ve depolanması için gerekli elektronik ekipmanları ifade etmektedir. Teknoloji, donanımın elektronik belgeleri kısıtlayan bir faktör olmadığı noktasına doğru gelişmektedir. Ek gelişmeler hız ve kapasiteyi arttırmaya devam ederken, iletişim, depolama ve bellekle ilgili yeni işlemci ve aygıt ortamı uygun bir başlangıç noktasıdır. Taşınabilir cihazlardaki ve kimlik denetim metotlarındaki oluşacak gelişmeler, elektronik belgelerin kabulünü arttıracaktır (Oatway, 2004:4).

Bilgisayar sistemini oluşturan unsurlardan bir tanesi olan donanım denilince anlaşılması gereken bilgisayarın fiziki yapısıdır. Yani bilgisayar kasası ve içindekiler: ana kart, RAM, ekran kartı, ekran, klavye, fare, yazıcı, tarayıcı, hoparlör, mikrofon gibi birimler bilgisayar ortamının donanım bileşenini oluştururlar. Kısaca donanım bir merkezi işlem biriminden ve birime bağlı çevre birimlerinden meydana gelir. Ayrıca çevre birimleri, giriş birimleri ve çıkış birimleri olmak üzere iki kısma ayrılır (Özen, 2007:21). Donanım teknolojisindeki gelişmeler yazılımların daha çok işlevinin olmasını sağlar, yazılım sektöründeki gelişmeler ise daha iyi bir donanıma ortam yaratır. Kısaca hem donanım hem de yazılım sektörü sürekli birbirlerinin sınırlarını zorlamaktadır. Arşivleme açısından değerlendirildiğinde depolama üniteleri en önemli donanım unsudur. Bunlar elektronik belgelerin depolandığı ünitelerdir. Birincil ve ikincil olmak üzere iki tür depolama üniteleri vardır (Capron, 1997:42). Bilgisayar hafızası birincil depolama ünitesi olarak adlandırılır Hafıza veriyi sisteme girişinden sonra, işlenmeden önce ve aynı zamanda işlendikten sonra

depolar. Hafıza aynı zamanda veriyi işlemek için gerekli programları da depolar. Hafıza veriyi geçici olarak depolar, çünkü sürekli elektrik akımına ihtiyaç duyar. Akım kesildiği zaman veri kaybolur. İkincil depolama üniteleri hafızadan ayrı depolama üniteleridir. Sabit disk, optik diskler ve manyetik bantlar bunlardan bazılardır. Bunlar disk sürücüleri vasıtasıyla okunurlar. İşte bu yüzden bilgisayarı kapatmadan önce üzerinde çalışılan dosyaları kaydetme zorunluluğu ortaya çıkmıştır. Bunlar, depolama teknolojilerini oluşturan unsurdur.

4.2.1.1. Arşivleme Ortam Seçenekleri

Elektronik belgelerin erişilebilirliğini ve bütünlüğünü koruyan kontrollü depolama ya da dosyalama sistemleri geliştirilmesi büyük önem arz etmektedir. E-belge üretildiğinde ya da alındığında, onun gerçekliğini ve bütünlüğünü sürdürebileceği kontrollü bir ortamda muhafaza edilmesine ihtiyaç vardır. Bu açıdan depolama ortamlarının özenle seçilmesi gereklidir. Depolama ortamı seçerken göz önünde bulundurulması gereken hususlar çerçevesinde, arşivleme açısından gerekli başlıca depolama araçlarını şöyle sıralanabilir;

1. **Manyetik Depolama**

Manyetik depolama üniteleri en yaygın depolama üniteleridir. Manyetik depolama uzun dönem saklama açısından riskler taşımaktadır. Disk yüzeyinin çeşitli dış etkenlere bağlı olarak bozulması sebebiyle veri kayıpları olabilmektedir. Sabit diskler ve manyetik bantlar manyetik depolama üniteleri olarak çalışma şekilleri temelde aynıdır. Bilgisayar sistemindeki disk sürücüsü bilgisayarın veri merkezidir. Sabit disk değişik türler içinde bilgisayarda kullanılan en önemli sürekli saklama ünitesidir. Sabit disk diğer tür saklama araçlarından büyüklük, hız ve süreklilik açısından farklılık gösterir. Sabit diskler genelde daha büyüktürler ve daha çok veri depolama kapasitesine sahiptirler. Hız açısından genelde daha hızlıdırlar. Süreklilik bakımından ise, genelde bilgisayara sabitlenmiştir ve kaldırılabilir değildir.

Sabit disk sürücülerinin son yirmi yılda kullanıldıkları teknoloji, kapasite, hız ve fiyat bağlamında sağlandığı ilerleme şaşırtıcıdır. Aynı zamanda, sabit diskin hızı ve kapasitesi de çarpıcı bir şekilde artmaktadır. Elektronik belgeler kurumsal yapı içinde sabit disk ortamında ve buna bağlı yedekleme ünitelerinde arşivlenir. Bu açıdan elektronik belgelerin muhafazası açısından önemlidirler. Sabit disk bilgisayar sisteminin aşağıda belirtilen hususları üzerinde önemli bir rol oynayan hususlar (PC Guide, Ağustos 2009) aşağıda değerlendirilmiştir;

- *Performans:* Sabit disk bütün sistem performansı üzerinde çok önemli rol oynar. Bilgisayarın çalıştığı ve programların işlediği hız doğrudan sabit disk hızına bağlıdır. Sabit disk performansı, birden fazla işlem yapıldığı zaman ya da grafik çalışmaları, video ve ses düzenleme ya da veri tabanlarıyla çalışmak gibi büyük miktarda verinin işlendiği durumlarda kritiktir.
- *Depolama Kapasitesi:* Daha büyük bir sabit disk daha fazla program ve veri saklanabilmesine imkân tanır. Bir zamanlar 100 MB yer çok fazla bir yer olarak düşünülüyordu. Ancak günümüzde sabit disk büyüklükleri terabayt ve petabayt büyüklüğüne kadar ulaşarak gelişme göstermiştir Sabit diskler dahili veya harici olabilmektedir. Her bilgisayarda bulunan bir sabit diskin yanı sıra USB bağlantı noktasından harici olarak bağlanan küçük boyutlu disklerde kullanılmaktadır. Günümüzde disklerin kapasiteleri yüzlerce gigabayt bilgi depolama kapasitesine sahiptir. Özel çözümleri sunan yapılar terabaytlarla ölçülebilecek depolama alanlarına sahip olabilmektedir.
- Bilgisayar artık çok değişik amaçlar için aynı anda kullanılmaktadır.
- *Yazılım Desteği:* Yeni yazılımları etkili kullanabilmek için daha fazla yere ve daha hızlı bir sabit diske ihtiyaç bulunmaktadır.
- *Güvenirlilik:* Sabit disk'in önemini anlayabilmek için, çökmesi durumunda ortaya çıkan hasarı düşünmek yeterli olacaktır. Bu bağlamda sabit disk bilgisayarın en önemli öğesidir. Yazılımlar bir şekilde tekrar yerine konabilir ama kaybolan veri tekrar yerine konamaz. İyi kalitede bir sabit disk, yedekleme ünitesiyle birlikte veri kayıplarının en aza indirilmesini sağlayabilir.

Manyetik bantlar manyetik depolama ünitelerinden biridir. Müzik kasetlerine benzer manyetik bantlar, manyetikleşebilir bir madde ile kaplanmış ince plastik bantlardır. Veri, manyetik noktalar (1) ve manyetik olmayan noktalar (0) şeklinde temsil edilir. Bir ses kasetinde istenen şarkıyı bulmak için kaseti sarmak gerektiğine benzer bir şekilde, manyetik bantlarda da istenen veriye erişmek için bantın sarılması gerekir. Bu yüzden manyetik bantlar, uzun vadeli veri yedekleme ve arşivleme amacıyla kullanılır. Büyük bilgisayarlarda bantlar, manyetik bant birimi veya makaralar halinde kullanılır. Kişisel bilgisayarlarda bantlar, görünüşü ses kasetlerine benzeyen bant kartuşları şeklinde kullanılır. Yaygın olarak kullanılan manyetik bant çeşitleri QIC, DAT ve DLT' dır. Kapasiteleri 66 GB' a kadar çıkmaktadır. Manyetik bantlar 100MB yoğunlukta veri saklayabilir. Ancak düzeltme ve kayıt için oldukça

yavaştırlar (Shamri, 1996:12). Bu yavaşlık saatlerle ölçülür. Yazılıp okunabilen makineler düşük fiyatta ve iyi korunursa kasetler veriyi yıllarca koruyabilir. Manyetik bant, bilgi başına veri saklama maliyeti en az olan harici depolama birimidir. Bantlar sıradan veri değerlendirme ve sıradan ulaşma yapılan harici veri saklama donanım araçlarıdır (Kurnaz, 2008:239). Manyetik bantta bulunan veriler sırayla değerlendirilir. Dolayısıyla kayıta erişim süresi kayıtın bulunduğu yerle doğrudan bağlantılıdır. Ancak, doğrudan erişim veri yapıları bulunan manyetik disklerde saklanan kayıtlardan herhangi birine ulaşmak için geçen süre aynıdır.

2. Optik Depolama

Bilgi taşımak için manyetik sistemlere alternatif olarak optik sistemler ortaya çıktı. İlk önce CD kullanılmaya başlandı. Yüksek kapasitesi ve mıknatıs gibi manyetik ortamlardan etkilenmemesi nedeniyle kullanımı çok yaygın hale geldi. Daha sonra DVD'ler daha fazla veri saklama kapasiteleri sebebiyle CD'lere önemli bir alternatif olarak görünmektedir. Optik depolama manyetik depolamaya göre daha dayanıklıdırlar. Ancak yüksek nem ve sıcaklık optik depolama sistemlerine zarar verir. Bu yüzden uygun nem ve sıcaklık ortamı sağlanmalıdır.

Optik diskler, genellikle 4.75, yaklaşık 12 cm çapında ve yaklaşık 1mm kalınlığında, lazer ışınlarıyla veri okuyan ya da yazan, taşınabilir disklerdir. Veri optik disklerde değişik biçimlerde saklanır. Kapasiteleri 17 GB' a kadar çıkabilir. En yaygın iki türü CD yani yoğun disk ve DVD yani sayısal çok yönlü disk veya sayısal video disk'tir. Bunların dışında bir CD çeşidi olan VCD'ler mevcuttur. VCD temel olarak hareketli resim ve ses içeren bir CD çeşididir.

CD-ROM'lar küçük noktalar ve çizgiler içeren ve her birinin bir bit'e tekabül ettiği WORM disklerdir. Bir CD genel olarak 650 MB büyüklüğündedirler ve yaklaşık 114 MB yoğunlukta veri saklayabilirler (Shamri, 1996: 12). CD biçimi en yaygın kullanılan optik disk türdür. Sadece yazılabilen CD-Romlara 100 yıl ömür biçilmektedirler. Ancak 20-25 yıl sonra içinde disk yüzeyinde bozulmalar olabileceği ileri sürülmektedir. Hem yazılıp hem silinebilen CD-romlar da ise 10–15 yıl sonra disk yüzeyinde bozulmalar olabileceği ileri sürülmektedir. Bütün bunlar elektronik belgelerin depolanmasının çok sıkıntılı bir alan olduğunu ve sürekli güncelleme gerektiğini göstermektedir. Başlıca CD türleri aşağıda belirtilmiştir;

- **CD-R** diskler: WROM yani bir yaz çok oku olarak da adlandırılır. CD-R disklere yalnız bir kez yazılabilir, üzerindeki veriler bozulmadan tekrar tekrar okunabilir. Bir kez yazdıktan sonra, üzerindeki veri silinemez veya değiştirilemez.
- **CD-RW** diskler, silinebilir optik diskler olarak da adlandırılır. Veri kaydedilirken disk yüzeyi kalıcı olarak değiştirilmediği için tekrar tekrar yazılabilir. CD-RW diskleri, genellikle veri yedekleme ve çoklu ortam çalışmalarını saklamak için kullanılır.
- **CD-I:** Görsel dosyalar için geliştirilmiştir. Bu sayede verilerin kayıpsız olarak saklanabilmesine sağlanır. Ayrıca kayıt alanı daha verimli kullanabilmektedir (Henkoğlu, 2008:160)

DVD biçimi, CD biçimiyle benzer şekildedir. Ancak, veriyi belirten deliklerin boyutu CD'lerdekinden çok daha küçük ve birbirine daha yakındır. Buna ek olarak, ışığın değişik açılarda yansıması kullanılarak veri iki değişik katman halinde saklanabilir. Ayrıca, DVD' lerin iki yüzü de kullanılabilir. Böylece kapasiteleri, 4,7 GB' dan 17 GB' a kadar ulaşılır. Tek yüzlü ve tek katmanlı DVD 4,7 GB; tek yüzlü ve çift katmanlı DVD 8,5 GB; çift yüzlü ve tek katmanlı DVD 9,5 GB; çift yüzlü ve çift katmanlı DVD 17 GB kapasitesindedir. DVD’ ye ses ve görüntü kaydı da yapılabildiği ve bir film DVD’ ye rahatça sığabildiği için, büyük oranda videoteyp teknolojisinin yerini almıştır. DVD diskler, standart disklerin 25 katı depolama kapasitesi ve 10 katı daha hızlı erişim ve veri aktarım süresi ile her gün gereksinim duyulan veri alanı ve hız sorunlarına büyük ölçüde çözüm olmaktadır (Özen, 2007:32). CD’lerde olduğu gibi, bir kez yazılabilen ve yazılıp silinebilen olmak üzere farklı DVD çeşitleri de bulunmaktadır.

3. Manyeto-Optik Depolama

İki tür depolama ünitesinin melez türüne manyeto-optik denir. Manyeto-optik disk, manyetik ve optik disk teknolojisinin en iyi özelliklerini kapsamaktadır (Capron, 1997:135). Manyeto-optik disk, optik diskin yüksek seviyedeki kapasitesine sahiptir, ancak manyetik disk gibi üzerine tekrar yazılabilir. Çalışma prensibi olarak sabit disk'lerle CD-ROM’ların bir bileşimi olarak düşünülebilir. Manyeto-Optik diske bilgi yazılmadan önce bilgi yazılacak kısmin +200 C°'ye kadar lazerle ısıtılması gerekir. Ancak bu işlemden sonra o konumda bulunan manyetik bilgi manyetik bir kafa sayesinde değiştirilebilir. Manyeto-Optik disklerin yapısı disket kabinin içine konulmuş bir CD'ye benzer. Yaklaşık 230 MB kapasiteye sahiptirler.

Optik disklerin daha az maliyetle arşivleme seçeneği sunması, manyeto-optik depolama aracının kullanımını düşürmektedir (Records Management Institute, 2000:3). Yani optik disk ve manyeto-optik diskler değerlendirildiğinde, düşük maliyetle arşivleme seçeneği sunan optik diskler tercih edilmektedir.

4. Flaş Disk ve Kartlar

Harici olarak bilgisayara takılan saklama ünitesidir. Bilgiler dijital olarak saklanmaktadır (Özen, 2007:39). Kapasiteleri gigabayt sevilerinde olabilmektedir. Bilgisayara USB bağlantı noktası kullanılarak bağlanılır. Bilgilerin bozulması ya da kaybolması CD gibi diğer saklama ortamlarına göre daha azdır.

Flaş bellek kartları veya flaş RAM'lar kredi kartı boyutunda, USB gibi bilgisayar ana kartı yuvalarına yerleştirilerek kullanılabilen devreler içeren kartlardır. Çeşitli boyutlarda bilgisayarlarda ve elektronik aygıtlarda kullanılabilmektedir. Örneğin, sayısal fotoğraf makineleri ve kameralarda kullanılarak bilgisayara veri aktarımı yapabilmektedirler. Ayrıca, MP3 müzik dosyalarını kaydetmek ve bilgisayar ile diğer aygıtlar arasında aktarımını sağlamak için de kullanılırlar. Ancak devreleri kullanıldıkça eskidiğinden dolayı ömürleri sınırlıdır.

4.2.1.2.Uygun Arşivleme Çözümlerinin Seçimi

Günümüzde e-belge depolanması için var olan birçok ürün; daha hızlı geri iletim gerektiren aktif dosyaların ve geri iletimi daha yavaş olan arşivsel dosyaların her ikisinin de karakteristiğini kapsamaktadır (Shamir, 1996: 12). Bilgisayar en önemli depolama araçlarından bir tanesidir. Bilgisayar değişik türde bilgiyi değişik yollardan saklar, bu bilginin ne olduğuna, saklama için ne kadar yer gerektiğine ve ne kadar hızlı bir ulaşım gerektiğine bağlıdır. Elektronik belgelerin depolama ortamlarını seçerken ya da bir depolama ortamından başka bir depolama ortamına aktarırken göz önünde bulundurulması gereken faktörler (State of North Dakota, 1998) aşağıda değerlendirilmiştir;

- Saklama planlarında belirlenmiş, saklanması onaylanmış belgelerin hacmi ve türü,
- Elektronik belgeleri elde bulundurmak için gerekli bakım hususları,
- Elektronik belgelere erişim ve depolama maliyeti,
- Elektronik belgelerin geri iletimi için erişim zamanı,

- Elektronik belge yönetim sistemine bağlı olarak zaman içinde elektronik belgelere erişebilirlik,
- Depolama ortamının taşınabilirliği. Yani seçilen depolama ortamının birden fazla firma tarafından önerilecek araçlarla yürütülmesi ya da aynı ürünler arasında taşınabilirliği
- Depomla ortamlarının, mevcut standartlara uygunluğudur.

Uzun dönem arşivleme açısından manyetik bant türü en uygun depolama seçeneğini sunmaktadır. Ömürleri teoride belirtilen diğer depolama seçeneklerine göre daha fazladır. Ancak erişim açısından çok yavaş oldukları önemli bir gerçektir. Uygun nem ve sıcaklık ortamında saklanılırsa 10 yıllık bir ömür biçilmektedir. Bu açıdan pasif safhada bulunan bir elektronik belge için en uygun depolama ortamıdır. Genel bir yaklaşımla, aktif elektronik belgeler için sabit disk, yarı pasif elektronik belgeler için ise harici depolama çözümler önerilebilmektedir. VTL teknolojisi etkin bir arşivleme yapılması açısından önemli bir çözüm sunmaktadır. Zira bu teknoloji, verinin nerede, ne kadar süre kalacağını ve erişileceğini noktasında depolama seçenekleri arasında etkileşimli bir yapı sunar. Bu teknoloji için önerilen dosya yapısı Samfs'dir. Sabit diskte saklanan ve belli bir süre sonra arşive aktarılması gereken belgelerin sağlıklı bir şekilde tape'lere aktarılmasını sağlar. Tabi ki buna ilişkin tanımlamaların ve göndermelerin sistem içinde yapılması gerekmektedir.

Elektronik belgelerin uzun dönem arşivlemesi açısından depolama ortamları kritik bir öneme sahiptir. Bu açıdan seçim yaparken elektronik belge yönetim sistemimin teknoloji bağlamda bütün unsurları dikkate alınmalı ve bu çerçevede bir planlama yapılmalıdır. Bu çerçevede Dollar (1999:40) tarafından ortaya konulan depolama ortamları seçerken göz önünde bulundurulması gereken kriterler mutlaka göz önünde bulundurulmalıdır. Bu kitreler aşağıda değerlendirilmiştir;

- *Büyük Çapta Depolama Kapasitesi:* Büyük çata depolama araçları fiziksel büyüklük açısından küçülmüşleridir. Bir başka deyişle daha küçük çapta bir fiziksel depolama aracı daha büyük çapta elektronik belgeleri saklayabilmektedir. Bu açıdan fiziksek olarak fazla yer kaplamayan büyük çapta depolama araçları kullanmak mümkün olmaktadır. Uzun dönem arşivleme açısından, elektronik belge üretim yoğunluğu da göz önünde bulundurularak yüksek depolama kapasitesine sahip araçlar seçilmelidir.

- *Yükse Veri Transfer Hızı:* Bir depolama aracının veri transfer hızlı; bir megabaytlık bir verinin transferi için gerekli zaman süreci olarak tanımlanmaktadır. Yüksek hızda bir veri transferi, okumak için ve verinin bir depolama aracından diğer bir depolama aracına taşınmasında daha az zaman kullanılması demektedir. Genellikte yüksek maliyetli bir disk yüksek hızda bir veri transferi demektedir. Bu açıdan seçim yaparken yüksek hızda bir depolama aracı seçilmeli, aksi takdirde uzun vadede ciddi mali ve yasal kayıpla oluşabilir.
- *Depolama Aracının Ömrü:* Dijital depolama aracının ömrünün disk yüzeyinde okumadaki ortalama ömrün üzerinde olduğu göz önünde bulundurulmalıdır. Ayrıca, dik yüzeyindeki okumadaki ortalama ömür, elektronik belgeyi işlemek ve iletmek için kullanılan yazılım uygulamasının ortalama ömründen daha uzundur. Bu açıdan elektronik belgenin kullanılabilirliğini uzatmanın tek yolu, yeni disk ve yazılımlarla desteklenmiş yeni depolama ortamlarına periyodik olarak transferinin yapılmasıdır.
- *Uygunluk:* Bu kriter, depolama teknolojisinin esas amacı ile uzun dönem erişim gereklilikleri arasındaki uygunluğu ifade etmektedir. Bütün dijital depolama araçları uzun dönem erişim açısından sağlıklı çalışmaz. Bu açıdan uzun dönem erişim açısından sunulan özel çözümler tercih edilmelidir.

Büyük çapta depolama açısından sunucu bilgisayarlar ve buna bağlı sunucu diskler büyük önem taşımaktadır. Bilişim teknolojilerinde sunucu, belirli bir servisi sunmak için üretilmiş yazılım ya da donanımı ifade eder. Bir bilgisayar ağındaki kullanıcılar işlerini yapabilmek için, dosya ve yazıcı kaynakları, veri tabanı, e-posta gibi birçok servisi kullanır. Bu servisler, sunucu adı verilen özel yazılımlar tarafından sunulur (İmamoğlu, 2008:32). Bu yazılımlar, yine sunucu olarak adlandırılan özel bilgisayarlar üzerinden sunulur. Sunucu bilgisayarlar, aynı anda birçok kullanıcıya hizmet vermek zorunda oldukları için donanımsal olarak kullanıcı bilgisayarlarından çok daha güçlü bir yapıdadır. Sunucu sistemler, aynı anda birçok bilgisayara hizmet etmek zorunda oldukları için kullanıcı isteklerine yeterli hızlarda cevap vermek zor olabilir. Özellikle elektronik belge yönetim sisteminin çalıştığı sunucular kullanıcı isteklerini cevaplarken disklerini yoğun olarak kullanmak zorundadırlar. Disklerdeki veriyi çok hızlı okuyup, yazılacak veriyi çok hızlı yazmak zorundadırlar. Bu yüzden sunucu sistemlerde yüksek performanslı hız diskler kullanılır. Bunu sağlamak için, yani veri erişim hızını arttırmak için RAID (Redundant Array of Independent Disk) çözümleri de kullanılmaktadır. RAID, birden fazla diski tek bir diskmiş gibi kullanarak, hızı ve hata toleransını arttırmak için kullanılan teknolojidir (İmamoğlu, 2008:34). RAID çözümler,

sunucu bilgisayarlara takılan disklerin tek disk gibi hareket etmesiyle hız artışı sağlar ve olası disk bozulmaları durumunda veri kayıplarını önler.

Depolama ortamının seçimiyle birlikte, depolama bağlamında kullanılan sistem yaklaşımının seçimi de önem taşımaktadır. Temel olarak üç değişik sistem seçeneği bulunmaktadır. Bunlar; DAS (Direct Attached Storage), NAS (Network Attached Storage) ve SAN (Storage Area Network) dır. Bu seçenekler bir birinin alternatifi olmayıp her birinin kendine göre kullanım alanı vardır. Saraçoğlu (2006:1) tarafından ortaya konulan depolama sistemleri aşağıda değerlendirilmiştir;

- *DAS*: Temel olarak bir veya daha fazla disk sürücüsü doğrudan bir sunucu bilgisayara bağlı olarak tanımlanabilir. Yani depolama üniteleri doğrudan sunucuya bağlanabilir. Bu sistemin gerçekleştirimi çok kolay olmakla birlikte, yüksel işletim maliyeti, mesafe kısaltması ve ölçeklenebilirlik önemli dezavantajlar olarak değerlendirilmektedir. DAS sistemi lokal bir teknoloji olduğundan sunucunun çok yakınında olmalıdır. Eğer yeni kapasite artırımı gerekiyorsa yeni sunucu eklemek gerekir. Ayrıca her sunucudaki diskler sadece o sunucu tarafından görülebildiği için sistemin etkin ve verimli kullanılması mümkün değildir
- *NAS*: Bu sistem dosya-tabanlı olup kaynaklar doğrudan yerel ağa bağlı çalışır. Veri, dosyalar halinde ağ üzerinden taşınır. Ayrıca veri depolama birimleri kolayca ağa eklenebilir. Bu sisteminde veriye erişim genel ağ trafiğine bağlı olduğu için ölçeklenebilirliğinin çok yüksek değildir. Trafik zamana ve iş artışına göre değişiklik gösterebileceği için performans ciddi şekilde olumsuz etkilenebilir.
- *SAN:* Bu sistem doğrudan sunuculara bağlanarak ağ trafiğini etkilemeden veri depolama kapasitesi sunmaktadır. Sistem ölçeklenebilirlik, kaynakların verimli kullanımı, kritik verilerin etkin şekilde korunması ve en önemlisi mevcut veri depolama kapasitesinin kolay ve esnek yönetimi özellikleri dolayısıyla önemli avantajlar sunmaktadır.

Kurumların depolama mimarisinde yapacakları seçimler sistemin bütününün etkileyebilir. Eğer yeterli yönetimsel araçlar mevcut değilse, yüksek performans gerektiren uygulamalarda bazı sunuculara çok yüklenirken diğerleri boş kalabilmektedir. Yukarıda tanımlanan depolama sistemleri arasında SAN; yüklü sunucular arasında dengeleme görevini yerine getirerek maliyetin düşmesine de katkıda bulunur. Ayrıca sistem gereksiz dosya

kopyalarını veya veri bütünlüğünü bozacak uygulamaları ortadan kaldırır. Ancak yüksek maliyet gerektirmesi sistemi en önemli dezavantajıdır. Bu tür sistemler seçilirken kurumların esneklik, kolaylık ve toplam sahip olma maliyetini düşünmeleri gerekiyor. Depolama sistemleri donanımın giderek daha da önem kazanan bir parçasıdır. Bu bağlamda yüksek güvenilirlik, ölçeklenebilirlik, performans ve çoklu platform desteği için tasarlanan depolama çözümleri tercih edilmelidir.

4.2.2. Yazılım

Yazılım, elektronik ortamda üretilen belgenin işlenmesi için kullanılan farklı programları ifade eder. Bilgisayar sistemini oluşturan unsurlarda ikincisi olan yazılım bilgisayarın kullandığı programların genel adıdır. Sistem yazılımları ve uygulama yazılımları olmak üzere iki ana yazılım kategorisi (Özen, 2007:41) aşağıda değerlendirilmiştir.

- *Sistem Yazılımları:* Bu yazılımlar, uygulama yazılımlarının belirli bir donanım grubu üzerinde pürüzsüz olarak çalışmasını temin eden zemin programlardır. Donanımlar onu çalışır hale getirecek yazılımlara ihtiyaç duyar. Uygulama programları donanımla doğrudan bağlantı kuramaz. İşletim sistemleri, uygulama programlarıyla yazılımlar arasında aracı bir hizmet sunar (Capron, 1997:42). Yani işletim sistemi bilgisayarın belleğini harekete geçirerek donanım birimleri ile merkezi işlemci birimi arasında ilişki kurar ve denetler. Bilgisayar kaynaklarını, merkezi işletim sistemini, hafızayı, disk sürücülerini, yazıcıları yönetme ve uygulama programlarını çalıştırma işletim sistemlerinin önemli görevlerinden bazılarıdır. İşletim sistemleri kişisel kullanıma imkân verdiği gibi aynı anda birden çok kullanıma da imkân vermektedir. İşletim sistemleri ve hizmet programları başlıca sistem yazılımlarıdır. İşletim sistemi, bilgisayar sisteminin yapacağı işleri yöneten programlar bütünüdür. Bir işletim sisteminin temel fonksiyonu bilgisayar kaynaklarının yönetimi ve kontrolüdür. Servis yazılımları ise genel sistem destek işlemlerini icra etmek için kullanılan sistem programlarıdır. Örneğin bir servis programı diskleri biçimlendirmek, dosyalar kopyalamak, disklerdeki programları yedeklemek, verileri sıraya dizmek ya da bir programı ASCII biçiminden EBCDIC dosya biçimine dönüştürmek için kullanılır (Özen, 2007:53). ASCII ve EBCDIC en yaygın ikili kodlama sistemlerindendir. EBCDIC ana bilgisayarlarda kullanılmak için geliştirilmiştir.

- *Uygulama Yazılımları:* Belli bir amaç için oluşturulan programlardır. Uygulama programları ısmarlama olabileceği gibi paket halinde de olabilmektedir (Capron, 1997:42). Birçok kurum kendi kurumsal ihtiyaçlarını karşılayacak uygulama programları oluşturmaktadır. Bu türe giren ısmarlama programlarını yazmak bazen çok uzun bir zaman alabilmektedir. Ismarlama programlar genel olarak kurumsal ihtiyaçları karşılamak amacıyla hazırlanırlar. Paket programlar ise genel olarak kişisel kullanıma hizmet etmektedir. Genel ve özel maçlı olmak üzere iki tür uygulama yazılımı bulunmaktadır. Genel amaçlı yazılıma, kelime işlemci programları ve dosya/veri tabanı yönetim sistemleri örnek olarak gösterilebilir. Özel amaçlı uygulama yazılımlar ise belirli bazı işleri icra etmek için geliştirilen dolayısıyla sınırlı amaçları olan yazılımlardır (Özen, 2007:43). Karar destek, analiz ya da elektronik belge yönetim yazılım programları bu guruba örnek olarak gösterilebilir.

Genel yazılım uygulamalarına bağlı olarak Calrim (2005:5) tarafından ortaya konulan elektronik belge yönetim yazılım program ilkeleri ve ayrıntılarının aşağıdaki çerçevede değerlendirilmesi ve gerçekleştirilmesi gerekmektedir;

- Kâğıt belgeler dahil olmak üzere bütün belgelerin yönetimi için kurumsal bir yazılımın geliştirilmesi ve uygulanması ile ilgili sorumlulukların belirlenmesi,
- Elektronik belge yönetiminin diğer belge ve bilgi teknolojileriyle entegrasyonunun sağlanması,
- Elektronik belge yönetim amaçlarını ve sorumluluklarını kurumsal talimatlara ya da politikalara dahil ederek kurumsal yapıda uygun bir şekilde yayılmasının sağlanması,
- Yeni bir elektronik belge sistemi kabul etmeden ya da mevcut sistemi geliştirmeden önce belge yönetim gerekliliklerinin belirlenmesi,
- Elektronik belge sistemi kullanıcılarını; koruma, yazılım ve sistemde kullanılan araçlar ve elektronik belgelerin yönetimi için gerekli eğitimin verilmesinin sağlanması,
- Bütün elektronik belge sistemleri hakkında güncel bilgilerin geliştirilmesi ve bunun sürdürülmesi,
- Kurumsal elektronik belgelerin envanterinin çıkarılması ve bu envanterin güncelliğinin korunması,

- Hayati belgelerin belirlenmesi ve korunması, uygun araçların seçilmesi ve saklama planlarını geliştirmek için kurumsal belgelerin ayıklama işlemlerinin yapılması,
- Elektronik belge saklama planlarının onayını temin ederek elektronik belge yönetiminde ve imhasında kullanım için uygulanmasının sağlanması.

Yukarıda belirtilen unsurlar çerçevesinde elektronik belge yönetim yazılımı oluşturulmalı ve uygulama safhasına konmalıdır. Yazılımlar, elektronik belge yönetimi açısından en önemli kısıtlayıcı faktördür. Mevcut sistemler, ilgili firmaya özgüdür ve birçok firma kendilerince kapsamlı çözümler sunmaya çalışmaktadır. Her bir ürünün, kullanıcı ara yüzü, veri yapıları, işlem akışı, kuruma özgü bir ürün olarak kapalı bir şekilde muhafaza edilmektedir (Oatway, 2004:4). Bu kısıtlayıcı faktörden kurtulabilmek için, kurumsal yapıya özgü yazılım çözümlerinin geliştirilmesi ve devamlılığının sağlanması gerekmektedir.

Kurumsal yazılım uygulamalarına bakıldığında kendilerine özgü gereksinimlerini karşılamamaktadır. Zaman içinde bu gereksinimler, ya özel yazılımlarla ya da ek maliyetlerle karşılanmaktadır (Arslantekin, 2005:232) Genellikle ticari amaçlı oluşturulan bu yazılımlara müdahale de söz konusu olmamaktadır. Bu açıdan gerek mali açıdan ve gerekse güvenlik açısından elektronik belgelerin başkaları tarafından oluşturulan ve arka planda tam olarak nasıl işlediği bilinmeyen yazılımlarla yönetilmesi önemli bir risk taşımaktadır. Aynı zamanda önemli bir fonksiyonun yerine getirilmesinde firma bağımlı bir çözümün kullanılması uzun vadede ciddi sorunlara sebep olabilmektedir. Alınan paket yazılımların uygulanmasında ve güncellenmesinde ek maliyetlerin oluşması kaçınılmazdır. Bu noktada tüm dünyadaki çözüm yolunda genel eğilim, özgür ve açık kaynak kodlu yazılımların kullanılması olarak görülmektedir (Arslantekin, 2005:233). Ancak burada önemli sorun sürdürülebilirliktir. Bu açıdan en önemli nokta yeterli uzman personelin bulunması ve teknolojik değişimlere paralel olarak oluşturulacak yazılımda gerekli güncelleme işlemlerinin yapılabilmesidir. Günümüz dinamik teknolojik ortamda bunu başarmak oldukça zor gözükmektedir. Ayrıca birlikte işlerlik açısından kurumsal yazılım eğilimleriyle ilgili bir değerlendirmenin de yapılması gereklidir. Bununla birlikte özgün yazılımı hazırlanması oldukça zaman almakta, yapılacak her düzeltme geçiş aşaması için ekstra bir zaman anlamına gelmekle birlikte oluşacak yazılım kurumun ihtiyacını tam anlamıyla karşılayacaktır.

Kişisel bilgisayarların yaygınlaşmasıyla yazılım; her kullanıcı ve her kullanım için ayrı geliştirilen amatör programlar yerine, benzer işleri yapan çok sayıda kullanıcının işine

yarayan, dünya çapında pazarlanan ürünlerin geliştirildiği bir teknoloji olmuştur. Bir yandan dünya çapında yaygınlaşırken, diğer taraftan da gittikçe daha ayrıntılı, daha stratejik, daha önemli işlerde, kişilerin ve kurumların yaşamındaki önem artmaktadır. Yazılım konusunda özellikle Microsoft sürekli yeni yazılımlar geliştirmektedir. Her yeni program daha güvenilir daha işlevsel bir yapı sunmaktadır. Daha önceleri MS Dos ortamında hazırlana ve çok kısıtlı bir işlem yapma imkânı sunan programlar düşünüldüğünde gelinen nokta gösterilen büyük gelişimi görmek açısından büyük önem taşımaktadır. Bu çerçevede, elektronik belge yönetimin bağlı olduğu yazılımın benzer bir gelişmeyi sağlayabileceği düşünülerek gerekli önlemler alınmalıdır. Diğer programların aksine, elektronik belge yönetim yazılımı kolay bir şekilde kurulup doğrudan kullanılamaz. Kullanıcı hesapları, güvenlik kontrolleri ve dosya planlarıyla ilgili, kullanımdan önce gerekli tanımlamaların yapılması gerekmektedir (Wojcik ve Gouin, 2003:46). Buna ilişkin eğitim faaliyetlerinin de gerçekleştirilmesi büyük önem taşımaktadır. Bu sistemin doğru bir şekilde kullanılmasını sağlayacaktır.

Elektronik belge yönetim yazılımının sistemin işleyişiyle ilgili bütün hususları içermesi gerekmektedir. Belgenin yaşam döngüsünde belirtilen aşamalar çerçevesinde elektronik belge yönetim yazılımında modüller oluşturulmalı ve bu modüllerin birbirleriyle işlerliği sağlanmalıdır. Temel olarak elektronik belge yönetim programında aşağıdaki modüllerin bulunması gereklidir;

- *Belge Üretim Modülü:* Belge üretim modülü elektronik belge üretimini sağlayacağı gibi kurum dışından gelen elektronik belgeleri de alama özelliğine sahip olmalıdır. Bu modülde yazışmaların şekil ve içerik bakımından standartlaşabilmesi için şablon ve form kullanımını desteklemelidir. Onay mekanizması kurumun hiyerarşik yapısına göre oluşturulmalı ve üretim modülüne yansıtılmalıdır. Aynı zamanda modül üst veri alanlarının otomatik ve elle girebilecek şekilde olmalıdır.
- *Akış Modülü:* Akış modülü üretilen belgelerin teşkilat içinde bir birim olabileceği gibi, bir başka kurum ile özel ve tüzel şahıslar ulaştırılması sürecidir. Modülde; kurum dışına elektronik olarak gidecek belgelerin karşı sistemin teknik gereksinimlerine uyum sağlayabilecek dönüşüm işlemleri tanımlanabilmelidir.
- *Arşivleme Modülü:* Arşivleme modülü, belge niteliği kazanmış elektronik belgelerin saklanacağı ve istendiğinde ulaşılabileceği bir yapıda oluşturulmalıdır. Burada saklanacak belgelerin sistemin kabul ettiği tüm doküman tiplerini kapsamalıdır. Arşivleme modülü belgelerin dosyalama mantığına göre tasnif edecek şekilde

- *İmha Modülü:* İmha modülü, saklama planları çerçevesinde oluşturulmalı, imha ile ilgili süreçler ve onaylar bu modülde tanımlanmalıdır. Otomatik imha işlemine kesinlikle müsaade etmemeli, imhası gelen belgeler için iki aşamalı bir onay mekanizması modülde bulunmalıdır.
- *Dijitalleştirme Modülü*: Kâğıt ortamda oluşturulan belgelerin elektronik ortama aktarılarak mevcut elektronik belge yönetim sistemine entegre etmensi sağlayacak şekilde tasarlanmalıdır. Modülde, farklı dosya türlerinde aktarım yapılabilmelidir. Ayrıca modül, elektronik ortama aktarılan belgenin gerçekliğini sağlamak amacıyla dijitalleşme sırasında zaman damgası işlemi gerçekleştirebilecek şekilde olmalıdır.

4.3. Dijital Koruma

Elektronik ortamda depolamada her gün yeni teknolojinin ortaya çıkmasına rağmen, elektronik ortamda depolanmış önemli miktarda bilgi bozulmakta ve kaybolmaktadır. Dijitalleşme çalışmalardaki sorunların ve başarısızlıkların farkına varılırken, çoğunlukla analog bilgiden farklı olarak dijital bilgilerin sonsuza dek kalacağını düşünme eğilimi bulunmaktadır. Çok büyük miktardaki dijital bilgi içinde yer aldıkları diskin bozulmasından dolayı kaybolmaktadır. Günümüzde 20 yıl önce popüler olan 8 inch lik bilgisayar diskinden bir şey okumak, hemen hemen imkânsızdır. Dolayısıyla yıllar öncesinden kalacak büyük miktardaki bilgiler kaybolma ve kullanılamama riskiyle karşı karşıya kalabilmektedir (Sitts, 2000:164). Daha fazla kaybı önlemek için dijital bilginin yaşam süresiyle ilgili konunun ciddi bir şekilde ele alınıp çözülmesi gerekmektedir.

Dijital koruma teknikleri, geçmişe ait ihtiyaç duyduğumuz bilgileri kullanılabilir kılmak için alt yapı ve veri tabanlarının iyi bir konumda tutulmasını sağlar (Sitts, 2000:165). Örneğin, eski bir kelime işlem dosyasını görmek için orijinal yazılımın kodlamasını anlayan bir yazılıma gereksinim duyulmaktadır. Ancak bu şekilde ekrana uygun olarak yansıyabilmektedir. Bu olmadan bütün görmeye çalıştıklarımız anlamsız olacaktır. Bu dosyaları uzun süre kullanılabilir tutabilmek için, onları çalıştıran bir yazılıma ya da şifreleme

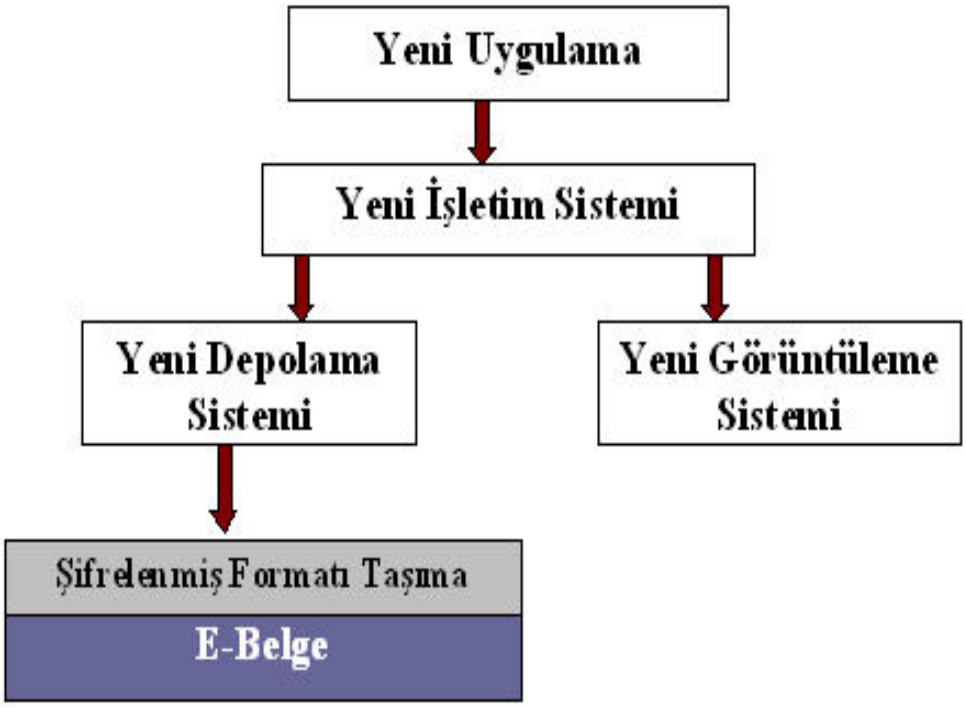
sisteminin bilgisine ihtiyaç duyulmaktadır. Dijital dosyaları uygun bir şekilde kullanabilmek için kodlama sistemini kullanan bir yazılım üretilmesi gerekmektedir.

Yazılım ve donanım versiyonlarındaki bu hızlı değişim uzun dönem arşivleme açısından ciddi bir soruna sebep olmaktadır. Bu durum dosya formatları, depolama ortamları, yazılım ve donanım sistemleriyle ilgili problemleri içermektedir (Sitts, 2000:166). Bugünün kelime işlemcisi daha eski bir versiyonla yaratılmış dosyaları okuyamamaktadır. Çoğu düzenleme sadece yıllar öncesinde yaratılmış en popüler kelime işlemci dosyasını açarken bile okuyamama riskiyle karşı karşıyadır. Aslında, bugünün popüler kelime işlemci programı, aynı kelime işlemcisinin bir önceki versiyonuyla yaratılmış dosyaları okuyamamaktadır. Bu durumda oluşturulan elektronik belgelerin yıllar sonra okunabilir ve kullanılabilir olmasında ciddi sorunların olacağı önemli bir gerçektir. Dijital korumaya karar vermede kurumlar ilk olarak çalışmalarında neye gereksinim duyduklarını tespit etmeliler. Bu bir formattan diğer bir formata dönüştürmenin çalışmalarını nasıl etkileyebileceğini anlamaları demektir. Bu, çalışmalarının sınırını, büyüklüğünü bilmek ve hangi parçaların gerçekten saklanması gerektiğini de anlamak demektir. Bununla birlikte, dijital koruma tekniklerinden taşıma ve yazılım eskimesi konuları henüz tam anlamıyla çözülmemiş sorunlardır.

4.3.1. Temel Dijital Koruma Teknikleri

Uzun dönem koruma çözümleri ortam bağımsız olmalı, çünkü ortam biçimleri ve standartları genellikle saklama periyodu boyunca değişecektir. Çözümlerin, belgelerin yönetilmesine odaklı olması gereklidir. Böylece, saklama süreleri boyunca erişilebilir ve kullanılabilir olmaları sağlanır. Uzun dönem saklama gerekliliklerinin ve elektronik belgelerin muhafazasına ilişkin hususların belirlenmesi gereklidir. Bazı elektronik belgelerin, çok uzun ve devamlı saklama gereklilikleri vardır. Bu yüzden geliştirilen saklama çözümlerinin uzun dönem erişimlerinde sürekliliğin sağlanması zorunludur (NECCC E-sign Policy Workgroup, 2001:9). Maalesef, elektronik belgelerin uzun dönem muhafazası için kolay bir teknik çözüm bulunmamaktadır. Ancak, bu problemi çözmeye yönelik bazı yaklaşımlar bulunmaktadır. Bu yaklaşımların maliyeti ve faydası kurumsal ihtiyaçlara paralel olarak ölçülmelidir. Arşivlenen elektronik belgelere uzun dönem erişimi sağlayacak dijital koruma yaklaşımları aşağıda sıralanmıştır;

- *Taşıma:* Sistem taşıma, elektronik belgelerin korunmasına yönelik çok yaygın bir şekilde üzerinde durulan çözümdür. Bu çözüm, e-belge yönetim sistemi yöneticisinin,

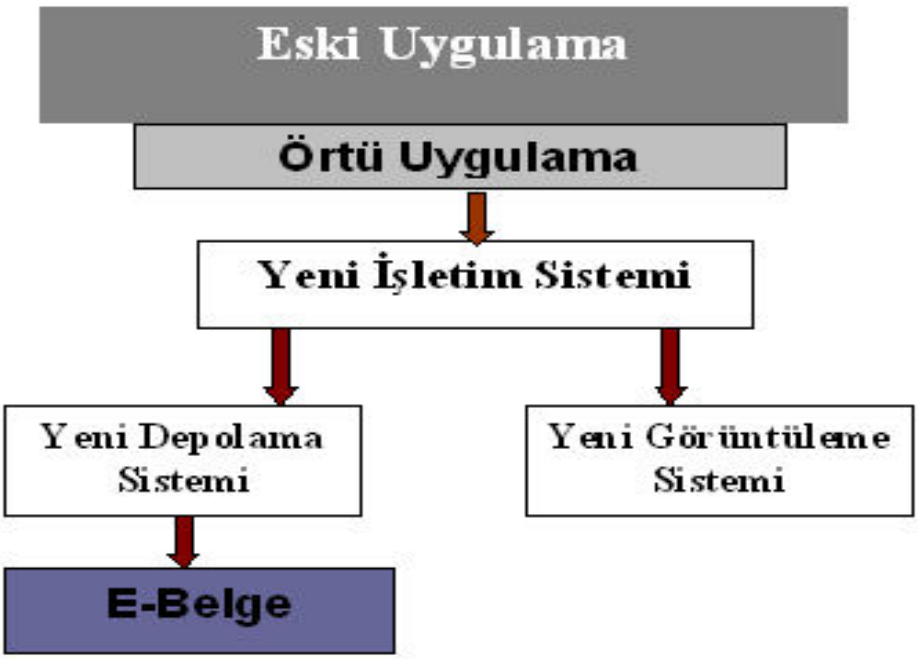


Şekil 5. Taşıma Süreci

- *Enkapsülasyon (sarma):* Sarma, taşınabilir formatta tek bir dijital obje olarak gerekli bütün üst veri elemanları ile birlikte orijinal belgenin, görüntüsünün ve hissinin alınması metoduna dayanır. Bazı açılardan, sarma standart formatların kullanımı ile sistem taşımayı birleştirir. Enkapsülasyon stratejileri, araştırmada henüz başlangıç

- *Diğer Ortamlarla Değiştirme(Dönüştürme):* Elektronik belgelerin, kâğıt ya da mikrofilm gibi dayanıklı ortamlarda çıktısını almak oldukça kolaydır. Elektronik belgeler, kâğıt olarak çıktısı alınabilir. Ayrıca mikrofilme aktarılarak kâğıt ve mikrofilm koruma kopyası olarak muhafaza edilebilir. Bu çözüm, sadece bütün gerekli üst veri elemanlarının ortam çıktısında alınabildiği ve belgenin elektronik formda kullanılması ya da erişilmesine ciddi ihtiyaç olmayacağı zaman geçerlidir.

- *Eskimiş Teknolojilerin Öykünümü (Emulation):* Öykünüm, bir bilgisayar teknolojisinin başka bir teknolojiymiş gibi hareket etmesine imkân tanımayı amaçlayan yazılım ve donanım kullanımından oluşmaktadır. Bu çözüm yazılım ve donanım değiştirirken, elektronik belgelerin orijinal dosya formatlarında kalmalarına imkân tanır. Öykünüm, herhangi bir yapay sistemde arşivlemek için karmaşık ve pahalıdır. Öykünüm çözümlerine yönelik araştırmalar devam etmektedir. Öykünüm (Emulation), antikacı niteliğine sahiptir. Öykünüm programları, diğer programların davranış, görünüm ve hisleriyle ilgili benzetim işlemini yapar. Böylece, orijinal ekipman ve yazılımların saklanmasına gerek kalmadan belgenin orijinal formatındaki işlevselliğini korunur (Minnesota Historical Society, 2004:5). Ancak, öykünüm uygulamadan çok teoride ispatlanmıştır. Bu yaklaşımı kullanarak çok az başarılı örnek mevcuttur ve maliyet oldukça yüksektir. Burada daha fazla kısıtlamalar bulunmaktadır. Teknolojiye yapılan bütün yatırımlar değerlendirildiğinde, bilginin durağan bir çerçevede korunarak değerini kısıtlanması problemli olarak görünmektedir. Öykünümde, taşımanın işaret ettiği probleme benzer konular üzerinde durulur. Fakat farklı olarak bu yaklaşım dosyaların bilgi içeriğini araştırmaktansa yazılım uygulamaları üzerine odaklanmıştır. Öykünümle uğraşanlar her tip uygulamayı taklit eden ve her çeşit formatta çalışan bir yazılım üretmeyi hedeflemektedirler. Böylece uygun bir emulatorle Word 3.0 ve Word 97'ye bugünün



Şekil 6. Öykünüm Süreci

Orijinal sistemin benzerini yapma yaklaşımı bilgiyi ilk alanda oluşturmak ya da işlemek için kullanılan orijinal çalıştırılabilir programı saklamayı içerir. İşletim sistemi ile birlikte bu program yalnızca orijinal ya da eşdeğer bir makinede çalışır. Gelecekte, programı çalıştırmanın tek yolu, bir emülatördür. Benzetme için sunulan daha önceki öneriler orijinal makine mimarisinin bütün detayları ile arşivlenmesini belirtir. Böylece gerektiğinde emülatörün yazılması mümkün olacaktır. Bu önerinin orijinal makinedeki bilgi yok olduğunda ya da orijinal makine kontrol için uygun olmadığında yürütülmesi zordur. Bu yaklaşıma bir alternatif, bilginin var olduğu zamanda bir tür emülatör belirlemesi yapmak ve bu bilgiyi hangi makinede çalıştırılacağı bilindiği zaman emülatör oluşturmak olacaktır. Diğer bir alternatif de orijinal makine bilindiği zaman, orijinal makinenin emülatörünün yazılmasına ve hataların ayıklanmasına izin veren sanal makineye güvenmektir. Gelecekte, sanal

emülatörü, bir orijinal makinenin sonrasında orijinal uygulama kodunu çalıştırmasını sağlayarak, orijinal makinenin emülatörünün çalıştırılmasını mümkün kılacaktır. Üst verinin programın nasıl çalıştırılacağına dair basit bir kullanıcı kılavuzu içermesi gerekmektedir. Orijinal programın çalıştırılmasını saklama, programın o programın hareketi ile ilgilenildiği tekrar belirtildiği zaman uygun olur ancak bu veri arşivleme için uygun değildir (Sproull ve Eisenberg, 2005:28).

Yukarıda belirtilen temel metotların dışında dijital arkeoloji, teknoloji koruma gibi metotlarda kullanılabilmektedir. Dijital arkeoloji, hasar görmüş yazılım ve donanım çevrelerinden, eskimeden ve depolama ortamındaki içeriği kurtarma ile ilgili metot ve prosedürleri kapsamaktadır. Bu metot açıkçası, acil kurtarma stratejisidir ve genellikle okunmaz duruma gelen depolama ortamından veri akışının kurtarılması ile ilgili özel teknikleri içerir. Dijital arkeoloji işlemleri genellikle bu konuda uzmanlaşmış firmalar aracılığıyla gerçekleştirilir. Ancak maliyeti yazılım ve donanım çevresinde meydana gelen hasara ve kayıp veri miktarına bağlı olarak değişmekte ve artmaktadır. Eğer yazılım ve bağlı olduğu donanım oldukça eski ise, içeriğin okunabilir ve anlaşılabilir yapılması mümkün olamayabilmektedir. Teknolojik koruma ise sistemin üzerinde çalıştığı depolama ortamı, bağlı olduğu yazılım, işletim sistemi dahil olmak üzere bütün teknik unsurların korunmasıdır. Bu yöntem teknoloji müzesi yaklaşımı olarak ta adlandırılır. Bu yöntemde bozulabilecek donanımsal ya da yazılımsal bir unsurun yerine aynı özellikte bir teknolojinin konamamasıdır. Zira teknoloji değiştikçe, eskiden kullanılan teknolojik unsurlar artık üretilmeyecektir. Bu çerçevede uzun dönemde kullanışlı değildir.

4.3.2. Uygun Dijital Koruma Tekniklerinin Seçimi

Elektronik belgelerin zaman içinde kullanılabilir kalmasını sağlamak için uygulanabilir bahsedilen dijital koruma yaklaşımları bütüncül bir yaklaşımla değerlendirmek ve uygun çözümü seçmek gereklidir. Bahsedilen yaklaşımlardan bir tanesi, belgeleri destelemek için gerekli bütün dokümantasyon, yazılım ve donanımın muhafaza edilmesidir. Bu bilgisayar müzesi yaklaşımı olarak ta bilinir, bu büyük ölçekte çok gerçekçi değildir. Çünkü yazılım ve donanım ortamının ne kadar hızlı değiştiği düşünüldüğünde, ihtiyaç duyulduğunda çalışacağı hususunda herhangi bir garantisi olmayan büyük miktarda zamanı geçmiş cihazların depolanacağı ve muhafaza edileceği gerçeği görülecektir. Elektronik

belgelerin korunmasına yönelik en yaygın yaklaşım, taşıma ve dönüştürme tekniklerinin birleştirilmesiyle ortaya çıkan tekniktir (Minnesota Historical Society, 2004: 5). Taşıma, dosyaların değerlerini korumak amacıyla dosyaların yeni ortama ya da bilgisayar platformuna nakledilmesidir. Dönüştürme, dosyaların bir formattan diğer bir formata değiştirilmesi gerektirir ve Microsoft Word gibi özel bir formattan düz metin ya da XML gibi özel olmayan formata taşınması şeklinde de olabilir. Süreçte veri kaybından korunmak için, ne tür değişiklikler olacağını ve bu değişikliklerin kabul edilebilir olup olmadığını belirlemeye yönelik başlangıç testleri ve analizler yerine getirilmelidir. Her iki taşıma ve dönüştürme ile birleştirilmiş herhangi bir üst veriye erişilebilirliğin korunmasına da özel bir dikkat gösterilmesi gereklidir. Uygun bir şekilde planlandığı ve yürütüldüğü zaman, taşıma ve dönüştürme yaklaşımı muhtemelen günümüzde geçerli olan en kolay ve maliyeti etkin koruma metodunu ifade eder. Diğeri, elektronik belgelerin korunmasında öykünüm (benzemeye çalışma) yaklaşımı elektronik belgelerin muhafazasını tam olarak karşılamamaktadır. Ayrıca bir strateji olarak da işlerliği bulunmamaktadır. Eskimiş yazılım ve donanım yapılarından uygun ortamlara aktarılmamış elektronik belgelerin onlarla birlikte yok olması muhtemeldir. Sonuç olarak, öykünüm çözümü çalıştırılsa bile elektronik belgelerin delilsel niteliğini koruyamayacaktır. Elektronik belgelerin delil olarak korunmasının gerekli olduğu durumlar içinde ciddi sorunlar yaşanabilir. Dijital bilginin gelecekte okunabilir olmasını sağlamak için uzun dönem stratejiler üzerinde dikkatle durulmalıdır (Bearman, 1999:2). Maalesef gelecekte okunabilir olmak tek başına elektronik belgelerin korunması için yeterli değildir. Elektronik belgenin delil vasfını zaman içinde kaybetmesine neyin sebep olduğunu detaylı incelmede başarısızlık, uzun vadede ciddi sorunlar yaratacaktır.

Kurumlar, uzun dönem saklamak için gerekli uygulamalarda depolanan belgeleri korumada kullanılacak taşıma stratejileri dikkatlice düşünmelidir. Belgenin ve taşıma yönteminin doğruluğu sağlanmak zorundadır (Public Records Office of Victoria, 2000:4). Taşıma, belge ya da belirli dosya türleri için bir depo olarak kullanılan araçların eskimesinden dolayı, korunmaya yönelik stratejilerdir. Ortam türü eskiyebilir ve geçerli yazılım bunla çalışmayabilir. Dosyaların geçerli biçime aktarımını ve içeriğinin korunmasını temin edecek taşıma programının uygulamaya konmasına ihtiyaç vardır. Bu, ortam türü eskimeden yapılmalıdır. Bundan dolayı, elektronik belgelerin kurumun ayrıntılı belge yönetim planında bozulmayan ortam ve dosya türlerine belirli aralıklarla taşıması yapılmalıdır (Calrim, 2002:28). Ortam ve dosya türlerinin, mevcut araç, metot ve teknolojiler kullanılarak geçerli belgelerin korunmasını ve erişilebilir olmasına yönelik güvenilir ve dayanıklı depolar

sağlaması gerekir. Çünkü ortam ve dosya türleri genellikle değişkendir. Bir taşıma stratejisi her bir ortam ve dosya türü için bir program oluşturmalıdır. Örneğin WPD dosyasının, üretilmesinden sonra dört yıl içinde güncel kelime işlemci yazılımına taşıma ve gözden geçirme gerektirebilir.

Bir format bir defalığına yeni bir formata dönüştürülebilir. Yeni formatın eskiye oranla açıklama yapmak için daha basit olması oldukça olasıdır. Diğer bir taraftan, yeni format daha az etkili olabilir. Ayrıca, her dönüştürme de hata ya da özelliklerin kaybolması riski vardır. Bu durum, elektronik belgenin bütünlüğünü önemli ölçüde tehlikeye sokar. Değiş tokuşun (dengelemenin) dikkatli bir şekilde değerlendirilmesi gerekmektedir. Ancak, bir kere dönüştürme orijinal dosyanın da saklanamayacağı anlamına gelmez. Veriyi XML'e dönüştürmek saklama problemi için bir yaklaşım olarak açığa çıkmaya başlamaktadır. Her ne kadar XML'in bilgileri saklama amacıyla etkili bir rol oynadığı doğru olsa da, tek başına bütün sorunlara çözüm için yeterli değildir. XML kendi başına veri ile ilgili ne yapılması gerektiğini belirleyemez; özellikle de verinin nasıl sunulması gerektiğini söyleyemez. Ancak etiketler her bir programın sunumunu belirlemek için XML sentakslar sağlayarak XML teknolojisi ile ilgili, diğer programlar için yollar sağlar (Sproull ve Eisenberg, 2005:29). Ancak XML damga dizgilerinin çalıştırılmasını gelecekte korumak için yardımcı olamaz.

En iyi belge yönetim uygulamaları, içerik korumada bazı belge nitelikleri taşıma sürecinin sağlıklı işlemesine imkân vermese de, belge taşımanın eninde sonunda haklı olduğunun ortaya koymaktadır. Belgenin yaşam döngüsünde uygulanan ve kullanılan belge yönetim metodolojisi, bilginin güvenliği, korunması ve muhafazası ve gelecekte ulaşılabilir olmasını sağlar (Calrim, 2002:28). Belgelerin taşınması, değerli belgelerin korunması ve uzun dönem erişiminin garanti altında alınması için gereklidir. Belgelerin taşınabilmesini temin etmek için, en iyi e-belge yönetim uygulamaları; açık sistemleri, standartlara uyumlu teknolojileri ve bütçe olanaklı teknolojik yükseltmeye, eğitim ve güvenli yazılım seçimleri yapmaya imkân tanıyabilen tedbirler içermeyi gerekli kılmaktadır.

Dijital arkeoloji ve teknolojik koruma yöntemlerinin uzun dönem arşivleme açısından kullanabilirliği söz konusu değildir. Zira dijital arkeoloji yönteminin uzun dönem arşivlenmiş ortamlarda başarı oranı oldukça düşüktür. Bu yöntem oldukça güncel uygulamalarda ve donanım çevrelerinde başarılı olmaktadır. Teknolojik koruma ise gerek felaket kurtarma stratejilerine uygun bir yöntem olmaması ve gerekse bozulan donanım ve yazılım unsurunun

yerine uzun vadede aynısını koyma imkânı olmaması dolayısıyla hiçbir şekilde kullanılabilir değildir. Ayrıca bakım ve eski donanım bulma maliyeti oldukça yüksektir. Bu açıdan uzun dönem arşivleme açısından bu yöntemlerin kullanılabilirliği oldukça düşüktür.

4.4.Saklama Planlarının Oluşturulması

Elektronik belgelerin saklama planlarının oluşturulması sistem dizayn aşamasında gerçekleştirilmelidir. Bu fonksiyonel ayıklamaya dönük yaklaşımları desteklemektedir. Bu metot, kurumsal yapı içindeki iş süreçlerinin ve bilgi akışlarının açıklığa kavuşturulmasını sağlayarak, belgelerin gerekli olduğu noktaların tespitini sağlar. Saklama planları, yasal, yönetsel, mali ya da tarihi gereksinimleri karşılamak üzere belgenin ne kadar süre ile tutulması gerektiğini belirten dokümandır (Özdemirci, Torunlar ve Saraç, 2009:259). Geleneksel belge yönetim yaklaşımında, hangi belgelerin bulunduğu noktasında bir envanter çalışması yaparak, bu çerçevede her bir belge serisinin ne kadar süreyle saklanması gerektiğini belirten bir saklama planı ortaya konur. Saklama planları genellikle belge serileri düzeyinde yapılır ve her bir birim için ayrıca düzenlenir. Bunun anlamı, bağlı faktörlerin birinin değişmesi durumunda, saklama planlarını yeniden düzenlemek gerekecektir. Elektronik belgeler için oraya konan yeni tür saklama planı yaklaşımı, kurumun, delilsel vasfı dolayısıyla hangi aktivite ve işlemleri koruyacağına yönelik kuramsal politikaları içerir (Hollier, 2001**)**. Bu gereklilikler belli bir süre geçerli kalır. Bunlar, amaçlara nasıl ulaşılacağı ve kurumsal yapı ya da teknolojik değişim gerçekleştiğinde değişikliklerin nasıl olacağıyla ilgili detayların belirtildiği uygulama adımlarıyla desteklenecektir. Esasında uygulama adımlarını belirlemede belge envanter çalışmaları hala geçerlidir.

Kurumların, e-belgelerin bilgisayar ortamında depolanmasında kullandıkları sistemlerde üretip ve muhafaza ettikleri belgelerin doğru, gerçek ve güvenilir olmasını sağlamak konusunda dikkatli olmaları bir zorunluluktur. Elektronik belgelerin doğruluğu ve bütünlüğü sadece işletmenin başarısı için önemli değildir, aynı zamanda bu belgeler hukuk davalarıyla ilgili olduğunda da ya da devlet arşivlerine gönderilmesi gerektiğinde özel bir önem taşırlar. Özellikle, saklama planlarının oluşturulması bağlamında Zanger ve Oei (1994:102) tarafından ortaya konulan elektronik belge arşivleme siteminde bulunması ve birleştirilmesi zorunlu dört gerekli element aşağıda değerlendirilmiştir;

- *Belge saklama:* Kâğıt belgeler için öngörülen saklama sürelerinin elektronik belgeler içinde uygulaması gereklidir. Bunla birlikte, vergi, yasal ya da devam eden herhangi bir iş süreci için gerekli olduğu sürece de muhafazası sağlanmalıdır. E-belgeler, sadece sistematik ve belgelendirilmiş prosedürlere göre imha edilmelidir. E-belgelerin imhasına yönelik talimatlar, sistem tasarımının bir parçası olmalı ve gizli ya da diğer hassas bilgilerin imhası gibi konuları içermelidir. E-belgeler, kurumun belge saklama planlarının bir parçası olan düzenli bir programa göre rutin bir şekilde imha edilmelidir. Rutin prosedürler önemlidir. Çünkü delilsel değerleri ve yasal gereklilikler dolayısıyla imha edilen belgelerle ilgili ortaya çıkacak herhangi bir soru işaretini ortadan kaldırmaya yardımcı olabilmektedir.
- *Veri güvenliği ve bütünlüğü:* Kurumlar elektronik belge yönetim sistemlerinin yetkisiz erişim ve veri tahrifine karşı güvenilir olduğunu gösterebilmelidir. Bu genellikle, kontrol sağlayan bir güvenlik programı geliştirmeyi ve belgelemeyi gerektirir. Bu kontrol sistemi; sadece yetkili personelin elektronik belgelere erişimini, belgelerin yedeklenmesini ve gerektiğinde kurtarılmasını sağlar. Yetkisiz değiştirme, ekleme ve silme risklerini azalmasına yardımcı olur. Elektronik belgelerin bütünlüğünü sağlamak için, depolama araçlarını elektronik belgeleri depolamak amacıyla kullanmadan önce hatalardan ve yanlışlardan arındırıldığını doğrulaması için test edilmesi gerekmektedir. Depolama araçlarının uygun ısı ve nem ortamında muhafaza edilmesi sağlamalıdır. Depolama araçlarının örnekleme suretiyle herhangi veri kaybının ya da ortam bozulmasının olup olmadığını tespit etmek için düzenli bir şekilde okuma yapılmalıdır.
- *Sistem dokümantasyonu:* E-belgeler, veri dosyalarını üreten, kullanan ya da depolayan sistemin, belgelerin teknik ve fiziksel özelliklerinin tanımını ve yeterli kaynak dokümanlarını içeren dokümantasyonla birlikte depolanmalıdır. Elektronik belgelerin, yetkili kişiler tarafından erişilmesi, korunması ve imhası işlemlerinin sağlıklı yürütülmesi için yeterli tanımlama ve indeksleme yapılmalıdır. Uygun tanımlayıcı bilgiler, dosya kodu, erişim için anahtar kelimeler, alıcı, imza sahibi, yazar, üretim tarihi, onaylanmış imha tarihi, gizlilik derecesi sınıflandırılması ve diğer ortamlardaki e-belgelerle bağı gibi hususları içermelidir. Depolama araçların etiketlenmesi de gereklidir. Etiketlemede, verilerden sorumlu birimin ve sistemin adı belirtilmelidir. Ayrıca, dosya adları, üretim tarihleri, kapsadığı tarihler, kayıt yoğunluğu, iç etiketleme tipi, karakter kodları ya da çalıştığı yazılım da belirtilebilir.

- *Arşivsel kopyaların saklanması ve erişim:* Genellikle, elektronik ortamdaki belgelerin basılı kopyaları, belli yasal ya da düzenlemeler arşivlenmesini öngörmedikçe saklanması gerekli değildir. Elektronik belgeler kolay erişilebilir olmalıdır. Bunu sağlamak için, kurumların, sistem yükseltmesi ya da değiştirilmesi durumlarında elektronik belgelerin uygun formatlara dönüştürülmesinden emin olmaları bir zorunluluktur.

Elektronik belge yönetim programının oluşturulmasında ilk aşama kurumun belge envanter işleminin tamamlanmasıdır. Belgeler, kapsamlı bir şekilde tespit edilmeli tanımlanmalı ve diğer belgelerle bağlantıları yapılmalıdır. Elektronik belge envanter çalışmasını yürütmek için en iyi ve en çok kullanılan metot, belgelerle ilişkilendirilmiş bilgi sisteminin tespiti ve analiz edilmesidir. Elektronik belgelerin genellikle belge serisi düzeyinde envanteri çıkarılır ve daha sonra program seviyesinde tanımlama yapılır (Records Management Institute, 2000:5). Envanter aşamasında, önemli elektronik belgelerin tespiti ve korunması bir zorunluluktur. Teknolojik altyapının yeterli olmadığı kurumlarda, önemli belgelerin çıktısını alarak insan okuyabilir formatta tutmak ve kurum dışında depolamak bir ihtiyatlı uygulama olarak değerlendirilir. Bütün belgeler, biçimine bakılmaksızın envanteri çıkarılmak ve saklama planları oluşturulmak durumundadır. Elektronik belgeler, kâğıt nüshalardaki gibi, benzer şekilde düzenlenmesi gerekmektedir. Saklama planları yasal gereklilikler, prosedürler çerçevesinde hazırlanır ve belge saklama planlarının güncellenmesi, onayı, gönderilmesi ve geliştirilmesiyle ilgili süreçleri kapsar.

Saklama planlarının oluşturulması için kurumsal elektronik belgelerin envanterinin tamamlanması gerekmektedir. Elektronik belgeler, manyetik depolama ortamı, çevrimiçi ya da optik disk üzerinde korunabilirler. Bilgisayarda işlenmiş bilginin kayıtlı kopyası, işlenmiş veri çıktısı ya da bilgisayar çıktısı mikrofilm biçiminde de olabilir (Calrim, 2002:12). Anabilgisayar ya da diğer bilgisayar işlemleri ile çoklu çıktısı olan veritabanları olması da mümkündür. Çıktılar, farklı birimler için üretildiklerinden dolayı birçok belge serisi yaratabilir. Bu yüzden saklama süreleri özel amaçlı kullanımdan dolayı değişebilir. Örneğin, bir kurumun müşteri bilgileri koruduğu bir veri tabanı var. Birimlerden biri bunu araştırma ve yönetsel raporlar hazırlamak için kullanır. Bunlar örneğin üç yıl saklanır ve daha sonra arşivsel değerleri açısından gözden geçirilirler. Diğer birim, aynı veritabanını yasal ihtilaflar için kullanır ve daha uzun süre saklanması gereklidir. Belgelerin her iki birimde de envanteri çıkarıldığı için, her iki belge serisi ayrıca kayıt altına alınmalıdır.

Belge saklama planları, belge yönetim programı tarafından gözden geçirilir ve onaylanır. İlgili kurum planları gözden geçirerek, arşivsel ilgilerini belirtir. Böylece onaylanmış belge saklama planı, listelenmiş belge serilerinin yönetim ve nihai imha süreçleri için resmi kaynak haline gelir (Calrim, 2002:15). Belge serilerinin kopya nüshaları, saklama planlarında belirtilmelerine gerek yoktur. Örneğin, eğer idari bir yazışmanın belge kopyası saklama planında belirtilmişse (kâğıt olarak) ve bir kopya nüshası da bilgisayarda varsa, elektronik nüshanın belirtilmesine gerek yoktur. Ancak, kopya nüshalar artık ihtiyaç duyulmuyorsa en kısa zamanda imha edilmelidirler

Onaylanmış bir belge saklama planının, mahkeme işlemleri üzerinde çok büyük bir etkisi vardır. Çünkü plan, bir saklama süresi ve belirli bir imha zamanını ortaya koymaktadır (Calrim, 2002:37). Her ne kadar istenen elektronik belge için onaylanmış saklama planı, mahkemenin onu kabul etmesini garanti etmese de, saklama planı oluşturulmuş belgenin kurumsal düzenli uygulamalar içinde üretilmiş olmasıyla ilgili koşulları karşılamada kesinlikle yardımcı olmaktadır. Mahkeme, onaylanmış belge saklama planları kapsamında elektronik belgenin imha edildiği savunmasını da kabul edecektir. Mahkemeler, güncel belge saklama planları bulunmayan ya da belgeleri uygun şekilde koruma ve yönetmek için oluşturulmuş prosedürleri takip etmede başarısız olan kurum ya da çalışanlara yönelik cezalara hükmetmesi gerekmektedir. Davaların kurum aleyhine sonuçlanmasındaki en önemli faktör, gerekli belgelerin sağlanamamasından kaynaklanmaktadır. Eğer belgeler gerektiği gibi korunmaz ya da kişiler gerekli belgeleri bulma konusunda iyi niyet gösteremezlerse, bazı uç durumlarda cezai müeyyideler öngörülmektedir (Calrim, 2002:37).

Elektronik belgelerin belirlenmiş bir saklama süreleri olması gereklidir. Saklama sürelerinin belirlenmesinde, idari, mali, hukuki ve tarihi kriterlerin göz önünde bulundurulması önemli bir zorunluluktur. Bu çerçevede oluşturulacak saklama planlarının, elektronik belgelerle ilgili aşağıdaki hususları içermesi gereklidir (Records Management Institute, 2000:6);

- Bütün e-belge serilerinin saklama süreleri,
- Bilginin depolanması için kullanılan ortam,
- E-belgenin depolandığı yer,
- E-belgenin imha tarihi ve yöntemi.

Gerektiği gibi düzenlenmiş saklama planları, imhası gerekli belgelerin arşivlenmesini engellerken aynı zamanda elektronik belgelerin uygun biz zaman diliminde kullanılmasını ve geçerli olmasını sağlar. Saklama planları, aynı zamanda elektronik depolama ortamlarının etkin kullanımını da destekleyen önemli bir unsurdur. Esasında, elektronik belge saklama kuralları, elektronik belgelerin kurum için herhangi bir değer ifade edip etmediğine yönelik tasarrufları göstermek için tasarlanır. Eğer kurum için bir değer ifade etmiyorsa imha edilir. İmha edilmemişse, pasif belge olarak arşivde kalır. Elektronik belgelerin daha önce tanımlanmış saklama kurallarına göre imha edilmesi, kurum içindeki risk yönetimine katkıda bulunur (NASCIO, 2007). Belgenin gerçek değeri, üretilmesinden çok sonra da anlaşılabilmektedir. Bu kurumsal ihtiyaçlara bağlı olarak değişebilmektedir. Arşivsel amaçlı saklanacak belgelere yönelik saklama planlarını oluştururken, yönetimsel ihtiyaçlar, yasal zorunluluklar, mali gereklilikler ve tarihsel değerleri çerçevesinde değerlendirmeler yapılmalıdır. Şekil 7, belirtilen hususlar çerçevesinde arşivsel amaçlı saklanacak elektronik belgelerle ilgili seçim kriterlerini göstermektedir. Bu kriterler çerçevesinde saklama planları oluşturulmalıdır.

Şekil 7. Arşivsel Amaçlı Elektronik Belge Seçim Kriterleri

4.5.Ayıklama ve İmha İşlemleri

Ayıklama işlemi, hangi belgelerin uzun dönem arşivlenmesi gerektiği ve hangi belgelerin imha edileceği ile ilgili karar verme sürecidir Ayıklama, belgenin üretilmesiyle ilgili unsurlar ile aktif yaşam süreçleri boyunca saklanmasına yönelik uygulanan farklı işleri ve koşulları değerlendirir. Ayıklama sürecinde, belgelerin diğer kurumlarla işlemler, organizasyon, fonksiyonlar, politikalar ve prosedürler bağlamında ilişkilerde

değerlendirilmesi gereklidir (Moore, 2004:105). Belgelerde ayıklama imha faaliyetlerinin gerçekleştirilmesi önemli oranda depolama maliyetini azaltmak için kullanılmıştır. Ancak sürekli azalan depolama maliyeti ile dijital bilgilerde bunun tersi söz konusudur. Ayrıca, belgeler elektronik olduklarında daha birbirine bağlanmış olurlar. Belge dizinleri ile ilgili bu bilgi ya da delile dayanan değer çok açık olmayabilir ama bir dizi belge diğer bir dizi belgeyi anlamak ya da kullanmak için gerekli olabilir. Bir dizi belge dikkatle incelemekten ve bir kaçını saklamak için seçmekten ziyade, daha geniş belge birimlerini muhafaza etmek daha avantajlı ve uygun olabilir (Sproull ve Eisenberg, 2005:42). Her şeyi muhafaza et yaklaşımı doğru bir yaklaşım değildir. Neyin saklanması gerektiği konusunda kriterler belirlenmeli ve buna göre işlemler yapılmalıdır.

Kurumsal belgelerin sadece küçük bir kısmı devlet arşivlerinde sürekli saklanır. Resmi belgelerin etkin ve ekonomik bir şekilde imhası için, zaten ayıklanmış sadece arşivsel değeri olan belgeler devlet arşivlerine gönderilmelidir. Bu amaca ulaşmak için Wettengel ve Engel (1999:106) tarafından tanımlanan farklı aşamalar aşağıda değerlendirilmiştir;

- İmha işlemleri kurumun dosya planına göre bir belge imha listesinin hazırlanmasıdır. İmha listesi, genel olarak arşivsel değeri olmadığı için devlet arşivlerine devredilmeyecek bütün belge ve belge serilerini içerir. Ancak kurum yasal saklama süreleri sonunda imhası gereken belgeyi muhafaza edebilir. Diğer belgeler, kurum tarafından imha edilebilir. Belgelerin otomatik olarak seçimi için, e-belge, klasör ve dosyaların üst verisinde imha et ya da arşive gönder seçeneklerini içeren imha durumu veri alanı bulunması gereklidir.
- Devlet arşivlerine gönderilmesi gereken bütün belgeler, bütün dosya ve klasörlerin üst verilerini içeren programda listelenmelidir. Program, devlet arşivlerinin bilgi teknolojileri sistemine veri tabanı tablo formatında elektronik olarak transfer edilmelidir. Programdaki her bir dosyanın, giriş işlemi sırasında otomatik olarak numaralandırılması gerekmektedir.
- Programda listelenen dosyalar bilgi teknolojilerinin yardımıyla ayıklanır. Belli bir dosyanın arşivsel değeri olup olmadığını ilişkin karar veri tabanı tablosundaki belirli veri alanına girilmelidir. Ayıklamaya ilişkin karar, belgenin üretildiği kuruma elektronik olarak raporlanmalıdır.

- Ayıklamaya ilişkin kararlara dayanarak, kurumlar arşivsel değeri olan dosyaları otomatik olarak seçmeli ve arşiv formatına dönüştürmelidir. Devir listelerine ve bütün dosya ve klasörlerin sayılmasına ek olarak, belgeler elektronik olarak devlet arşivlerine devir edilir. Devir listesi ve sayım işlemi, dağıtım işleminin doğruluğunu ve tamlığını kontrole ilişkin araç işlevi görür. Kurum, devir işleminde belgelerin gerçekliğini tasdik eden bir belgede de teslim etmelidir.

Ayıklama, belgenin değerini belirleme sürecidir. Yani, yönetsel, delilsel, bilgisel ya da araştırma değerine göre düzenlenmesi ve diğer belgelerle ilişkisine dayalı olarak belgelerin saklama sürelerinin ve imhasının belirlenmesidir. Ayıklama, envanter çalışması sırasında elde edilen bilgileri, belge serilerini analiz etme ve resmi bir belge saklama planları geliştirmek için kullanır. Elektronik belgelerin arşivleme gerekliliklerini belirlemek için ilk aşama belgenin üreticisi ve kullanıcısının tespit edilmesidir. Bunu yaparken, kurumsal yapı içindeki kişilerin ve birimlerin belgeleri farklı amaçlar için kullanabilecekleri unutmamak önemlidir. Bazı belgeler bir birimde değişik formatlarda bulunabilirler. Eğer bu gibi belgelerin, ayrı ayrı amaçları için gerekiyorsa, arşivleme gereksinimleri programı değiştirebilir. E-belge envanter çalışması sırasında belirlenen bunun gibi gereklilikler, elektronik belgelerin ne kadar süre, hangi formatta, nerde muhafaza edileceği noktasında önemli bir faktör olacaktır. E-belgelerin saklama planlarının oluşturulmasında ayıklamaya yönelik kararlar şunları içermelidir (Calrim, 2002:14);

- Her bir e-belge serisi için toplam saklama sürelerinin, yönetsel, mali, yasal, araştırma, tarihsel ya da arşivsel değerlerine dayalı olarak belirlenmesi,
- Kurumda e-belgelerin güncel, aktif kullanım sürelerinin ne kadar olacağının tespiti,
- Eğer nihai imhadan önce pasif bir kullanım süresi varsa, e-belge serilerinin ne kadar süre saklanacağının belirlenmesi,
- Her tür pasif saklama ve güncel kullanım olduğu sırada, e-belge serileri için uygun biçime karar verilmesi,
- E-belge serilerinin potansiyel arşivsel değerlerinin ortaya konması,
- Gizli ya da özel bilgilerin tespit edilmesi,
- Hayati belgelerin tespitinin yapılması.

Ayıklama süreçleri sırasında, elektronik belgelerle ilgili olabilecek her tür özel durumlar kayıt altına alınmalıdır (Calrim, 2002:14). Örneğin, elektronik ortamda potansiyel arşivsel değeri olan planlama ile ilgili e-belgeler, ilgili bütün birimlerin bir araya gelmesi suretiyle ayıklama ve imha kararları verilmelidir. Saklama planlarında tarihsel değeri dolayısıyla belirtilen ve güncel iş akışında kurumda ihtiyaç duyulmayan belgeler devlet arşivlerine gönderilmelidir. Belgelerin ayıklama, transfer ya da imhasının kontrollü bir şekilde mümkün olması gereklidir. Belgelerin, kurum tarafından belirlenmiş uygun yetkilendirmeler olmadan imha edilmemesi gerektiğinin bilinmesi önemlidir. EBYS'de, herhangi bir zamanda dosyanın kendisi değiştirilmeden, dosyaya uygulanan politikaları değiştirmek için yetkilendirmelerin yapılabilmesi ve buna ilişkin takiplerin olabilmesi gereklidir (Public Records Office of Victoria, 2000:6). Bu, dosyaları değiştirmeden, imha ile ilgili politika değişikliklerine imkân tanır.

Dosyaların kontrollü imhasının sağlanması önemli bir zorunluluktur. Dosyanın imhasının, dosya içindeki bütün belgelerin imhası anlamına geldiği unutulmamalıdır. İmha edilen belgelerle ilgili kayıtların tutulması gereklidir. Kaydedilen bilgilerin, elektronik belgelerin transfer ve imhasına onay veren kişiyle ilgili bilgileri, dosya transfer ve imha tarihini ve imha edilen dosya ile ilgili imha yetkilisi bilgilerini içermesi gereklidir. İmha işlemleriyle ilgili kayıtların tutulması, e-belgelerin akıbetlerini izlemelerini için bir işlem geçmiş raporu sağlar. EBYS, imha edilen belgeleri göstermemesi gereklidir. İmha edilen e-belgeler bir şekilde sistem içinde bulunabilir. Ancak, sistemin hiçbir şekilde bu e-belgeleri göstermemesi gereklidir. Bununla birlikte, elektronik belge yönetim sistemi istendiğinde sistem yöneticisi tarafından imha edilmiş belgeleri sistemden tamamıyla yani fiziksel olarak ta kaldırması gerekebilir. Bazı kurumlar, yasal sebeplerden dolayı imha edilmiş belgelerin fiziksel olarak sistemden temizlemeyi sağlamaya ihtiyaç duyabilirler. Sistemin, imha işlemini yerine getiren operatörün kimliği, gerçekleşme zamanı ve belge imhalarıyla ilgi gerçekleri kaydetmesi gereklidir.

E-belgelerin yaşam döngüsünün son aşaması imhasıdır. Bu kurumsal işleyişin amaçlarına yönelik kullanım değeri sona erdiğinde gerçekleşir. Bu noktada, tespit edilmiş belgeler imha edilebilir ya da sürekli saklama için arşive gönderilirler. E-belgelerin imha edilmesindeki amaç, yürürlükte süresi geçmiş belgelerin muhtemel kullanımını önlemeye yönelik olarak kalıcı bir şekilde ortadan kaldırılması, hassas ve gizli bilgilerin açığa çıkmamasını sağlamaktır (Calrim, 2002:43). İmha edilen belgeler tekrar geri

alınamamasından dolayı, belgeler imha edilmeden önce özel bir önem gösterilerek bütün yasal gerekliliklerin sağlanması gerekmektedir.

Kurumsal belgelerin imhası, belge saklama planlarına ve diğer yasal gerekliliklere uygun olarak yapılması gereklidir. Bütün tanımlanmış belge imha süreçleri resmi belgelere uygulanmalıdır. Referans ya da taslak nüshaları, artık ihtiyaç duyulmuyorsa hemen imha edilmelidir. Bazı durumlarda, taslak nüshaları gizli olabilir ve öngörülen talimatlar uygun olarak imha edilmeleri gereklidir. Ayrıca elektronik belgelerin saklandığı donanımında imhası bazı durumlarda gerekebilir. Buna ilişkin belirlenmiş parçalama süreci sağlanmalı ve yetkili kurum nezaretinde gerçekleştirilmelidir.

Kurum için önemli olan potansiyel arşivsel, tarihi, araştırma ya da tek olması sebebiyle önemli elektronik belgeleri tespit edilmesi ve işaretlenmesi gereklidir. Bu elektronik belgelerin nihai imhası kurumsal yapı ile koordineli yapılmalı veya devlet arşivlerine devredilmelidir. Devlet arşivlerine devri gereken elektronik belgeler ile ilgili işlemlerinde sağlıklı yürütülmesi gerekmektedir. Her kurum elektronik belgelerin uygun devrinin sağlanmasından ve koordinasyonundan sorumludurlar (Calrim, 2002:44). Elektronik belgelerin değişik biçimlerde olması, özel yazılımlar ve uzmanlık gerektiren donanımlar konusu sebebiyle, belgelerin devrine ya da kurumda muhafazasına ilişkin kararların devlet arşivlerinin danışmanlığında yapılması gereklidir. Eğer belge devir kararı alınmışsa, belge devir işleminin metodu, sıklığı ve biçimi kurum ve devlet arşivleri tarafından işbirliği içinde belirlenmesi gereklidir. Elektronik belgelerin fiziksel transferiyle ilgili zamanlama, saklama planları çerçevesinde belirlenmelidir. Özel koruma tedbirleri, sıklıkla elektronik belgelerin korunması için gereklidir. Uzun dönem arşivleme ve erişimi sağlamak için, elektronik belgelerin uygun farklı ortamlara aktarılması gerekebilir. Bu yüzden bütün sistem dokümantasyonunun elektronik belgelerle birlikte devrinin yapılması gereklidir. Devlet arşivlerine devir edilen elektronik belgelerin gizlilik düzeyleri ve erişim haklarına ilişkin seviyeler aynen korunur (State of North Dakota, 1998). Devlet arşivlerinin, arşivsel gerekliliklerin karşılanmasını sağlamak için süreçlere erken dahil olması gereklidir. Elektronik belgeleri korumak için çoğu zaman özel muhafaza tedbirleri gerekebilmektedir.

Elektronik belgelerin, uzun dönem erişim ve okunabilirliği sağlamak için uygun biçim ve ortamlara dönüştürülmesi gerekebilir. Uygun sistem dokümantasyonun tümünün, elektronik belgelerin devriyle birlikte gitmesi gereklidir. En düşük düzeyde bile

dokümantasyonu olmayan bir bilgisayar veritabanı kullanılabilir değildir. Çünkü içerikler okunabilir ya da açıklanabilir değildir. Dolayısıyla devir sırasında sistemin sürekliliğini sağlayacak ilgili bütün dokümantasyonunda devir edilmesi gereklidir.

Elektronik belgelerin saklama süreleri tamamlandıktan sonra ayıklama ve imha süreçleriyle ilgili yazılı prosedürler geliştirilmelidir. Belgelerin miktarı ve kurum çalışanlarının durumuna bağlı olarak, dosyaların tasfiyesi aylık, üç aylık, altı aylık ya da yıllık olarak yerine getirilebilir. Elektronik belgelerin tasfiyesi ile ilgili süreçler, elektronik belge yönetim sistemi içinde yerine getirilmelidir (Calrim, 2002:45). E-belge yönetim programı, kurumların bir imha kayıt defteri tutmalarını öngörmelidir. Kayıt defteri, belge serisi başlıklarını, ilgili tarihi, sayısı ve nihai imha tarihini göstermelidir. Elektronik belge yönetim sistem yazılımı, nihai imha kayıt defterini oluşturmalıdır. Yazılı prosedürler ya da belirlenmiş yetkilendirmeler, belgelerin nihai imhasını onaylamada kimin yetkisi ve sorumluluğu olduğunu doğrulamalıdır.

Elektronik belgeler, genellikle, silinebilir, yeniden kullanılabilir, kırılgan ve oldukça ucuz ortamlarda depolanabilir. Bu sebepten dolayı, elektronik belgelerin imhası, kurumsal işleyiş için artık gerekli olmadıklarında, mümkün olan en kısa zamanda belirlenmelidir (Calrim, 2002:46). Gizli belgeler için bazı önlemlerin alınması gereklidir. Çünkü birçok bilgisayar işletim sistemi, aslında dosya silindiğinde dosyanın tamamını silmez ve temizlemez. Sadece basit bir biçimde dosya ismini sistem dizininden kaldırır. Diskin bu bölgesi tekrar kullanımına kadar, elektronik belge değişikliğe uğramaz. Sonuç olarak silinmiş elektronik belge dosyaları, mevcut yardımcı programlar kullanılarak kurtarılabilirler. Bu sebeple imha sürecinde, fiziksel imhanın da yapılması duruma göre gerekebilecektir. Bununla birlikte, kâğıt belgelerin imhasında kullanılan shredder (kâğıt öğütme) yöntemi elektronik belgeler için de kullanılabilmektedir. Bu yöntemin genel mantığı, önce dosya yapılarının değiştirilmesi daha sonra imha işleminin gerçekleşmesine dayanmaktadır. Böylece verinin usulsüz bir şekilde tekrar geri yüklemesi gerçekleşirse ya da veri kurtarma işlemi yapılırsa, üzerinde değişiklik yapılan son veriye yani bozuk veriye ulaşılacaktır. Böylelikle imha işlemi tam anlamıyla gerçekleşmiş olacaktır. Buna ilişkin yazılımlar bulunmaktadır. Eğer mevcut yazılımlara güvenilmiyorsa, kurum kendi yazılımını yapmalıdır. Kurumun kendi yazılımını yapması bu işlemin sağlıklı ve güvenilir bir şekilde gerçekleştirilmesine imkân tanır. Elektronik belgelerin imhası ancak saklama planları çerçevesinde gerçekleştirilebilir. Belirtilen hususlar çerçevesinde imha işlemini gerçekleştirirken temel olarak bazı hususların

göz önünde bulundurulması gerekmektedir (State of North Dakota, 1998). Bu hususlar aşağıda değerlendirilmiştir;

- İmha edilmek üzere planlanmış elektronik belgelerin, imha süreçlerinde gizli ve kapalı bilgilerin korunmasını sağlayacak şekilde gerçekleştirilmesi gerekmektedir.
- Manyetik depolama ortamları kullanılarak muhafaza edilmiş, gizli ve kapalı bilgilerin bulunduğu elektronik belgelerin imhasından sonra, buna ilişkin manyetik depolama ortamlarının da bir daha kullanılmamasının sağlanması ya da fiziksel imhalarının gerçekleştirilmesi gerekmektedir.
- İmhası gerçekleştirilen elektronik belgelere ilişkin bütün yedek kopyalarının da imha edilmesi bir zorunluluktur.
- Elektronik belgelerin imhasında, o belge ile ilgili bütün üst veri elemanları da imha edilmelidir (Neale, 2004).

4.6. Arşivlemede Elektronik Belgelerin Gerçekliğinin ve Bütünlüğünün Korunması

Kurumsal yapı içinde elektronik belgenin gerçekliği, bütünlüğü, güvenliği ve erişilebilirliğini sağlanması gereklidir. Elektronik belgeler yasal, politik ve arşivsel gereksinimler, iş ihtiyaçları olduğu müddetçe, kullanılabilir, geri iletilebilir, ulaşılabilir ve geçerli olmak zorundadır. Elektronik belgeler doğaları gereği kolayca üretilebilir, düzeltilebilir ve imha edilebilirler (Dickman, 2002:54). Bununla birlikte eğer kurumlar elektronik belgeleri mahkeme sürecinde ya da denetim aşamasında delil olarak kullanacaksa, elektronik belgenin bütünlüğünün korunması bağlamında gerekli olan iki unsur sağlamalıdır. Bunlar; güvenirlilik ve gerçekliktir. Yani elektronik belgelerin, kurumsal ve yasal ihtiyaçlar çerçevesinde kullanılabilmesi için güvenilir ve gerçek olmaları gerekmektedir. Bu iki unsur bölünmez bir bütünün iki parçalarıdırlar. Güvenirlilik belgenin kapsadığı ya da sahip olduğu gerçekliği devam ettirmesidir. Yani bir elektronik belgenin üretiminden itibaren aynı içeriği ve değeri muhafaza etmesidir. Güvenirlilik iki faktöre bağlıdır (Duranti, 2001:43); bunlardan birincisi; belge formunun tamam olma derecesi yani belgenin bir bütün olarak belge şeklini taşımasıdır. Örneğin bir imza ya da terim eksikliği önemlidir. İkincisi ise; belge üretim aşamasından gösterilen kontrolün derecesidir. Bu iki faktörün yerine getirilme derecesi belgenin güvenirlilik derecesini belirler. Gerçeklik ise belge yapısının aynı şekilde korunması

ve tahrip edilmemesidir. Yani belgenin oluşturulduğu andaki içeriğini korunmasıdır. Fiziksel varlık olan belgenin üzerinde değişiklik yapılıp yapılmadığını gösteren izlere rastlamak mümkündür. Ancak elektronik ortamda bu tip izleri görmek daha zor olmaktadır.

Belgelerinin bütünlüğü ve aslına uygunluğu elektronik belge yönetiminin ilgilendiği önemli konulardan biridir. Gerçek belge, usulüne uygun olarak yetkili kişi ya da kuruluş tarafından oluşturulmuş belgedir. Bir belgenin bütünlüğü o belge üzerinde herhangi bir değişiklik yapılmaksızın korunması demektir. Kâğıt belgelerin aslına uygunluğunu ve bütünlüğünü sağlamak için, belgeyi iletenden belge kullanıcısına kadar saklama zinciri oluşturulmasını sağlayan teknikler kullanılmaktadır (Sproull ve Eisenberg, 2005:59). Aynı teknikler elektronik belgelerde de uygulansa bile, elektronik belgelerin yapısı aslına uygunluğu ve bütünlüğü sağlamak için ek tekniklerin kullanılmasını zorunlu hale getirmektedir. Dijital teknikler kâğıt belgeler için mevcut tekniklerden daha güçlü teminat vermeye elverişlidir. Ayrıca, elektronik belgeler tahrifata ve onaysız değişikliklere daha hassastır. Yetkisiz erişimin gerçekleşmesi durumunda, belgeleri bütünüyle kopyalanabilir, silebilir, değiştirebilir ya da denetim ile belirlenebilmesi zor ince değişiklikler yapabilir. Bilgi teknolojilerinde artan deneyim, elektronik belgelerin fark edilmeden nasıl kolayca değiştirilebildikleri ile ilgili farkındalık oluşturmuştur.

Elektronik belgeyi göndereni doğrulamak ve belgenin değiştirilmediğine emin olmak gereklidir. Her bir belgenin bütünlüğünü belirlemek ve göndericiyi doğrulamak için bir takım politikalar ve prosedürler belirlenmesi bir zorunluluktur. Bu politikalar ve prosedürler, kurumlar tarafından alınan farklı türdeki elektronik belgelerin bütünlüğünü ve gerçekliğini tespit etmede önemlidir. Bu politikalar, belgelerin uygun olmayan bir şekilde açıklanması ve değiştirilmesinden ortaya çıkacak maliyet ve potansiyel riskleri de içine alacak şekilde hazırlanmalıdır. Kurumlar genel devlet alt yapısına uygun internet ve e-mail politikaları geliştirmeli ve uygulamalıdır.

4.6.1. Gerçeklik ve Bütünlüğe Yönelik Tehditler

Elektronik belgelerin bütünlüğünü tehlikeye sokacak hatalar, kayıtlar doğrulandıktan sonra ya da iletildikten sonra da arşive sızabilir. Bu donanımın aksamaya uğramasından, işlemsel hatalardan, yazılım arızasından, kasıtlı saldırılardan ya da bunlara benzer başka nedenlerden kaynaklanabilir. Hatalar arşivdeki her bir dosyanın başka bir kopyası ile

kıyaslanması, dosyanın okunması, mevcut sağlamasının (hash) hesaplanması ve bu sağlamanın o dosya için korunan kopyası ile karşılaştırılması sonucu tespit edilebilir. Bu kıyaslamaları yapacak sürekli bir sürecin olması gereklidir. Böylece hataların fark edilmesi sağlanmış olur (Sproull ve Eisenberg, 2005:65). Bütünlük kontrolü başarısızlığa uğradığında, hem onarım hem de araştırma gerekli olur. İlk olarak, geçersiz veri, arşivde tasarlanan 'artık' mekanizması tarafından sağlanan yansımalardan ya da yedek kopyalarından geri alınır. İkinci olarak, hatanın nedeninin araştırılması gerekmektedir. Hatalı bütünlüğün bütün durumlarını kesin bir şekilde araştırmadaki başarısızlık, arşivi koruma konusunda da başarısızlığa neden olacaktır (Sproull ve Eisenberg, 2005:66).

Belge yeni bir ortama ya da formata aktarıldığında, yapılan işlem belgenin bütünlüğünde bir kısım değişimlere sebep olabilir. Analog ortamdan dijital ortama aktarımda yaşanan sorunların, tamamıyla dijital ortamda yapılan benzer işlemlerde yaşanmayacağı yanılgısına düşmemek gereklidir. Dijital ortamda yapılacak işlemlerde dosya formatı ve boyutu aynı gözükse de belgenin bütünlüğünü etkileyecek bir takım sorunların olması muhtemeldir (Sitts, 2000:171). Uygulamada, belgelerini aynı kelime işlemcinin bir önceki versiyonunu kullanılarak başarılı bir şekilde kopyalama yapılabilmektedir. Ancak bu işlemde, sayfa ortalama, alt çizgi, font değişiklikleri gibi formatlar ve çift tırnak gibi özelliklerini kayıp söz konusu olmaktadır. Bu emulasyon uygulamaları için doğru olabilir. Çünkü bu çalışmaların yaratıcıları uygulamanın hangi kısmını dönüştüreceğini seçer ve zaten tek tek her parçasını benzetmeye ya da dönüştürmeye çalışması mümkün değildir. Bu husus belgenin bütünlüğünü tehlikeye sokar. Bu çerçevede, yazılım ve donanım güvenirliği dahil olmak üzere sistem performansının test edilmesi gereklidir. Yazılım ve donanımın güvenirliliği, elektronik belgelerin gerçekliğini ve bütünlüğünü etkiler. Cihazların bozulması, elektronik belgelerin içeriğini değiştirebilir. Eğer elektronik belge üretme ve depolamak için kullanılan veri işleme araçları ve yazılımları güvenilir değilse, belgelerin bütünlüğü reddedilebilir.

Elektronik belgenin gerçekliği ve güvenirliliği açısından fiziksel ve çevresel güvenlik kontrollerinin sürdürülmesi gereklidir. Fiziksel ve çevresel tehditlerin, özellikle kırılgan çevrimdışı ortamlarda depolanan elektronik belgeler üzerinde etkileri vardır. Kurumsal güvenlik programı, büro mekânı, veri merkezi ya da donanım içeren odalar, sistem elektrik tesisatı, destek hizmetleri, yedekleme ortamları ve diğer sistem unsurlarında fiziksel erişim ve uygun çevresel şartları göstermelidir. Güvenlik programın aynı zamanda, yangın, kullanım hatası, yapısal göçme ve tesisatla ilgili bozulmalar gibi tehditleri de göstermesi gereklidir.

Normal imha süreçleri dışında elektronik belgelerin imhası ya da silinmesinin mümkün olmaması bir zorunluluktur. İndeksleme ya da belge bulma metoduyla bilgileri silinerek elektronik belgenin gizlenememesinin sağlanması gerekmektedir. Bir başka ifade ile elektronik belgeler bulunamaz yapılarak, erişilebilir olma engellememelidir (Public Records Office of Victoria, 2000:5). Karmaşık sistemlerin yazılım böcekleri ya da belgelendirilmemiş erişim mekanizmaları içerebilmesi dolayısıyla delilsel bütünlüğü korumak zordur. Kurumların bundan dolayı sistemi ve sistemin güvenliğini test etmek için, sistem tasarımını denetimini yapmaları gereklidir.

Yazılım uygulamalarının değişik fonksiyonları, bilgisayarda üretilen belgelerin bütünlüğünü ve durumunu etkileyebilir. Elektronik belgelerin uygun araçlarda kaydedilmesi gerekmektedir, aksi halde bilgisayarı kapatıldığında ya da uygulamadan çıkıldığında belgeyi kaybetme riskiyle karşı karşıya kalınabilir (Calrim, 2002:18). Dosyaların silinmesi ya da kopyalanmasını elektronik belgenin bütünlüğü üzerinde doğrudan etkisi vardır. Birçok bilgisayarın dosya kopyalama fonksiyonun, belgenin bütünlüğü üzerinde doğrudan etkisi olma potansiyeli problemi mevcuttur. Dosya yönetiminde problem, kopyalama süreci tesadüfen yanlış yönde oluşursa ortaya çıkabilir. Eğer kullanıcı, taşınabilir diskte yedek kopya oluşturursa ve yedek kopyayı daha sonra sabit diske aktarırsa, dosyanın önceki sürümü mevcut dosyayla yer değiştirebilir. Bu tip durumlar da belgenin bütünlüğünü tehlikeye sokar.

4.6.2. Gerçeklik ve Bütünlüğü Korumaya Yönelik Tedbirler

Dijital denetim araçları elektronik belgelerin bütünlüğünün kontrolü ve sağlanması açısından önemlidir. Belgelerin dijital denetimi temel olarak, bütünlük kontrolünü sağlamak ve belgelerin arşive ve arşivden iletilmesini güvence altına alan coğrafi ve idari olarak yayılmış kopyalara ve kriptografik tekniklerin kullanılmasına dayanmaktadır (Sproull ve Eisenberg, 2005:60). Kriptografik teknikler, asla uygunluk ve bütünlük için temel araçlar sağlar. Bunlar kriptografik algoritmalara dayanır ve bu algoritmalar sahteciliği sayısal olarak imkânsız hale getirir. Ayrıca bütünlüğü kontrole yönelikte teknikler kullanılmaktadır. Sağlama (hash) özümlemesini hesaplama tekniği bu çerçevede kullanılan bir yöntemdir. Bu teknikle, güvenli sağlama algoritması kaydı oluşturan dijital bitlerden kompakt sağlama özümlemesini hesaplanır (Sproull ve Eisenberg, 2005:60). Yaygın olarak kullanımda olan birçok algoritma vardır. Standart güvenli sağlama algoritması bunlardan biridir. Belge iletimi

sırasında, herhangi bir değişiklik olursa, bu farklık bir mesaj özümsemesiyle sonuçlanacaktır. Belge, yönetim sistemine ilk girdiği zaman hesaplanan sağlama özümsemesi, iletimden sonra oluşan değerle kıyaslanarak belgenin bütünlüğü doğrulanır. Belgenin oluşturulduğunda hesaplanan sağlama özümsemesi değişikliğin olup olmadığını tespitte kanıt niteliğindedir. Ayrıca, bu tekniğe benzer olarak, gönderilen ve alınan belgenin aynı olduğundan emin olmak için kullanılan çeşitli kriptografik teknikler vardır. Bir elektronik belge, belgeyi kullanan herhangi bir kişi tarafından doğrulanan dijital imza oluşturarak aslına uygun hale getirilebilir. Belge herhangi bir şekilde değiştirilirse, imza kontrolü başarısız olacaktır. Elektronik belgenin orijinalliğini doğrulamak için kullanıcı girdiyi aslına uygun hale getirme etiketi kabul ederek ve doğrulanmış aslını ortak anahtar kabul ederek ikinci tuşlamalı kriptografik iletim içeren algoritma gerçekleştirir (Sproull ve Eisenberg, 2005:61). Çıktı iki terimli bir değerdir, orijinalliği doğrulanmıştır ya da orijinalliği doğrulanmamıştır. Orijinalliği doğrulanmıştır terimi objenin özel anahtara sahip olan biri tarafından oluşturulduğu anlamına gelir. Kişinin, özel anahtarın varsayılan sahibinin o anahtarı koruduğuna güvenmesi gerekir, Böylece, o kişinin aslına uygunluk etiketini oluşturan kişi olduğundan emin olunur.

Belgelerin bütünlüğü açısından değerlendirildiğinde; belgelerin, üretimi, ortamı ve yönetimi belli yasal emirlere, iş ihtiyaçlarına ve geçmişteki deneyimlere bağlıdır. E-belgenin bütünlüğünün korunması değerlendirildiğinde risk yönetimi kavramı faydalı olabilmektedir. Risk yönetimi, risk analizine bağlı olarak potansiyel faydaya bağlı riskleri, riskleri belirlemek için seçenekli ölçümleri düşünmeyi ve bu analize bağlı olarak riskleri en iyi belirleyen ölçümlerin uygulamayı gerektirir. Elektronik belgelerin bütünlüğü tehlikeye sokacak risklerin tespit edilmesi ve buna ilişkin tedbirlerin alınması büyük önem taşımaktadır.

Elektronik belgelerin üretilmesinde, alınmasında ve muhafaza edilmesinde kullanılan süreçlerin ve usullerin doğruluğu ve güvenirliliği, e-belgelerin gerçekliğini, bütünlüğünü ve güvenliğini göstermede kritik faktörlerdir. Bu faktörler, e-belgelerin üretilmesi ve muhafaza edilmesi için kullanılan belirli teknolojilerden, formatı ya da ortamından çok daha önemlidir. Kurumlar, yasal ya da diğer işlemlerde elektronik belgelerinin kabul edilmesini bekliyorlarsa, bu süreçleri ve usulleri tespit etmeli, belirtmeli ve belgelendirmelidir (NECCC E-sign Policy Workgroup, 2001:5). Bu bağlamda eğitim de kritik bir öneme sahiptir. Eğitim, özellikle belgelerin üretimi ve muhafazasında kullanılan sistemin personel tarafından yeterli düzeyde devamlılığının sağlanması açısından önemlidir. Ayrıca, e-belgelere erişim ve kullanım için ihtiyaç duyulan teknolojik platform ve depolanması için kullanılan ortamın kırılganlığına

bağlı olarak ortaya çıkan belli yönetim konularından kurumsal yetkililerin haberdar olmasının sağlanması da önemlidir. Kurumsal yetkililerin, elektronik belgelerin yönetimi konusundaki sorumluluklarının farkında da olmaları gerekir. Ayrıca e-belgelerin yasal saklama sürelerinde erişilebilir ve yasal işlemlerde kabul edilebilir olmalarını sağlamları konusundaki bu sorumluluklar özenle yerine getirilmelidir.

E-belgeler erişilebilirliklerini desteklemek için uygun şekilde muhafaza edildiğinden emin olunması gerekmektedir. Elektronik belgelerin alınmasında ve iletilmesinde, belgelerin yetkisiz kişiler tarafından bozulması ve tahrif edilmesini önlemeye yönelik tedbirler alınması büyük önem taşımaktadır. Bunları yapmada başarısız olma, belgelerin gerçekliğini ve bütünlüğünü tehlikeye sokabilir. Elektronik belgelerin alınması, üretilmesi ve dosyalanmasına ilişkin net süreç ve usullerin geliştirilmesi ve belgelendirilmesi gereklidir. Politikalar ve prosedürler, hangi işlemle işin tamamlandığını belirtmekle birlikte, kabul edilebilir belge formatlarını ve belge üzerinde herhangi bir değişiklik yapılmamasını sağlayacak şekilde güvenli bir depolamayı içermelidir.

Elektronik belgelerin bütünlüğü açısından, belgenin düzenlendiği zamanın şüpheye yer bırakmayacak şekilde bilinmesi gerekmektedir. Zaman kaşesi fonksiyonu bu açıdan önemli role sahiptir. Bilgisayar işletim sistemlerindeki tarih ve saat ayarı çok kolay bir şekilde değiştirilebilmektedir. Bu nedenle onay makamları talep üzerine dijital tarihleri, bir zaman kaşesi ile birlikte bildirmeye mecburdurlar. Bu çerçevede e-belgenin alındı zamanı ve tarihinin belgelendirmeye yönelik ölçümlerin muhafaza edilmesi gereklidir. Birçok resmi işlemlerde bu bilgilerin belgelendirilmesi önemlidir. Yüksek riskli uygulamalar konusunda, güvenli ya da güvenilir zaman-tarih damgası, elektronik zaman ve tarih damgası uygulayan güvenir ve tarafsız üçüncü parti uygulamalarda kullanılabilir. Güvenilir zaman yetkilisi, bunun gibi elektronik zaman damgaları uygular. Güvenilir zaman damgası, açık şifreleme düzeni(PKI) içinde sağlanabilen diğer bir hizmettir (NECCC E-sign Policy Workgroup, 2001:6).

Bazı iş süreçleri ya da yasal gereklilikler, alınan e-belgelerin doğrulamasını gerektirir. Doğrulama, uygulamanın türüne bağlı olarak farklı formlarda yapılabilir. Yüksek güvenlikli ortamlarda, farklı bir yolla ayrı bir doğrulama tavsiye edilir. Yasal, denetim ve diğer amaçlara yönelik elektronik belgelerin kabulü, elektronik belgeleri üretmek için kullanılan sistemin sağlamlığının gösterilerek gerçekliğini ve güvenirliliğini tespiti şartına bağlıdır (NECCC E-

sign Policy Workgroup, 2001:12). Belge üreten sistemlerin, doğru ve uygun şekilde iş süreçlerinin gerçekleştirildiğini göstermeleri zorunludur. Bu amaca yönelik başarılı bir şekilde kullanılan, elektronik belgelerin güvenirlilik ve gerçekliğini korumaya yönelik çabalarda belge yöneticisine yardımcı olacak bazı öneriler geliştirilmelidir. Belge yöneticisinin, sistemin, normal iş süreçlerini uygun, doğru ve güvenilir biçimde yerine getirdiğinden emin olunmalıdır. Bunun için, sistem yönetim politika ve prosedürlerinin belgelendirilmesi ve tanımlanması gereklidir. Bu tip tanımlamalar belge bütünlüğünü destekleyecek unsurlardır.

Elektronik belgelerin bütünlüğü aşağıdaki hususlar çerçevesinde korunabilir (NECCC E-sign Policy Workgroup, 2001:13);

- Üreticinin tavsiyelerine uygun olarak, bakım yapmaya ek olarak rutin bir şekilde yazılım ve donanımın test edilmesi.
- Yazılım ve donanımın tedariki, yüklenmesi ve bakımıyla ilgili dokümantasyonların muhafaza edilmesi,
- Sistem faaliyetlerinin ve performansının güvenirliliğini belgelendirmek amacıyla işlem kayıtları ve çalıştırma planlarının muhafaza edilmesi.

Kurumlar, yüksek riskli sistemler için harici teknik değerlendirme ya da denetimi düşünmelidirler. Benzer sistemlerin bağımsız kontrolü ve denetimi, sistemin ve ürettikleri elektronik belgelerin güvenirliliğini belgelendirilmesini sağlayabilir. Sistem ya da uygulama işlemleri ve kullanıcı aktivitelerinden oluşan sistem aktivitelerini içeren işlem geçmiş raporunun muhafaza edilmesi gereklidir. Uygun araçlar ve prosedürler ile birlikte, işlem geçmiş raporu; kişisel sorumluk, yetkisiz giriş belirleme ve problem tespitleri de dahil olma üzere bazı güvenlikle ilgili konularda başarıya ulaşılmasında yardımcı olabilir. İşlem geçmiş raporunun, hangi olayların olduğun ve kimin sebep olduğuyla ilgili yeterli bilgi içermelidir. Bunlar, sistemde depolanan elektronik belgelerin bütünlüğüne ek olarak, sistemin güvenirliliğini ve sağlamlığını belgelendirmekte kullanılabilir. Eğer mümkünse işlem geçmiş raporu, belgelerin alınması, işlenmesi ve muhafaza edilmesi sırasında otomatik olarak yerine getirilmelidir. Bu kapsamda erişimle ilgili benzer uygulamalar gerçekleştirilmelidir. E-belgelerin belli metotlarla erişilebilir olabileceği göz önünde bulundurulmalıdır. Bu erişim metotlarının erişenle ilgili tanımlayıcı bilgileri ve belgede yapılan değişikliklerin içeriğini kaydettiğini ve bu erişim kayıtlarındaki bilgilerin değiştirilemeyeceğini ve silinemeyeceğini onaylayan bir rapor yazılımının geliştirilmesi ya da temin edilmesi gerekmektedir. Bu rapor,

yönetim ve idari fonksiyonları kullanan sistem yöneticilerini de kapsayacak şekilde, bütün kullanıcıların erişimlerini içermelidir.

Dijital varlıkların uzun süre korunması, arşiv depolama sistemlerinde bulunan büyük miktardaki veri yığınlarının gerçekliğini yönetecek bir mekanizma gerektirir. Arşivleme ortamları, gerçeklikle ilgili kısıtları düzenler ve alt yapıdan bağımsız çözümler oluşturarak depolama sistem teknolojilerindeki dönüşümü yönetir. Büyük arşivlerle ilgili ihtiyaçlar data grid teknolojisini kullanılarak çözüme ulaştırılır. Data gridlerin depolama ortamlarından çıkarma işlemini sağlar, firma bağımlı ürünler arasında veri taşıma işlemini mümkün kılar ve aynı zamanda arşivsel verinin gerçekliğini de temin eder (Moore, 2004:101). Data gridler, firma bağımlı depolama arşivleri ile koruma ortamları arasında ara birim özelliğinde yazılım alt yapısı sağlar.

E-belge bütünlüğünü sağlamak için, belge sayısallaştırma sistemi, belgeyi üreteni, ne zaman üretildiğini ve üretiminden itibaren değiştirilmediğini göstermesinin sağlanması gerekmektedir. Belge sayısallaştırma sisteminde, delilsel bütünlük, belge bütünlüğünü sağlayan bilgi elde edilerek arşivlenir. Bu sistem içinde, bütün bir yaşam evresinde belge bütünlüğünü sağlamak, arşiv sisteminin sorumluluğundadır (Public Records Office of Victoria, 200:2). Arşiv sistemi, delilsel bütünlüğü sağlamak için, elektronik belgenin kim tarafından ne zaman ve oluşturulmasından sonra değiştirilmediğini göstermeye imkân tanımayı sağlamak zorundadır Arşiv sisteminde, bu öncelikli gereklilikler, belge oluşturulduğunda gerekli provenans bilgileri elde edilmek suretiyle belgedeki herhangi bir değişiklik tespit edilebilir. Bu açıdan, belgenin bir faaliyet sonucunda üretilmesi ve geçirdiği evrelerin kayıt altına alınması belgenin provenansı açısından göz ardı edilmemesi gereken bir kuraldır (Özdemirci ve Yalçınkaya, 2009:8). Bu çerçevede elektronik belgelerin, hem kullanıcı ve hem de sistem yöneticisi tarafından değişikliklere karşı korunması gereklidir.

Elektronik belgelerin delil olarak kabulünde teamülün, değişik içerik ve biçimdeki belgelerin bazı mahkemeler tarafından kabul edildiğini göstermektedir. Her bir yargıç, verilen belgenin gerçekliğini, mahkemelerin bağımsız değerlendirmesine dayanarak delilleri ret etme konusunda özgürdür. Geleneksel kâğıt belgelerden farklı olarak, elektronik belgelerin sisteme dayalı zafiyetleri bulunmaktadır. Bu sebepten, güvenirlilikleri konusunda mahkemeyi ikna etmek için ek bir çaba gösterilmesi gerekmektedir. Bu yüzden bir elektronik belge yönetim sistemi, belgenin bütünlüğünün güvenirliliği konusunda mahkemeyi ikna etmeye yönelik

işlevsellikleri içermelidir. Küçük ve ana bilgisayar çevreleri için aşağıdaki öğelere itina gösterilmesi belgenin güvenirliliğini artıracaktır.

- Donanım ve yazılım güvenirliliğinin sağlanması.
- İşin normal seyrinde çıktıların hazırlanması
- Belge saklama sürelerinin tespiti

Belge içeriğinin cihaz düzgün çalışmadığında değişebilir olması, bir kurumdan belgenin üretildiği bilgisayarın güvenli bir şekilde çalıştığını gösteren delillerin istenmesini gerektirebilir. Bilgisayar çalışmasıyla ilgili herhangi bir arızanın bulunduğunu gösteren kayıt defteri genelde yeterlidir. Elektronik belgedeki bir yanlış, bilgisayar programındaki bir hatadan da kaynaklanabilir. Bir kurumdan programın testi ve geliştirilmesiyle ilgili delilleri göstermesi istenebilir. Bu konuyla ilgili bilirkişi, doğruluğu ve güvenirliliği belirlemek için genelde programları gözden geçirir. Bir kurumdan, delil amaçlı olarak elektronik belgelerin yönetimi ve verinin işlenmesinde kullanılan belirli bilgisayar program sürümelerini göstermesi istenebilir (Calrim, 2002: 36). Bir programın farklı sürümlerinden eğer sadece biri kullanılır durumda sorun yaşanmayabilmektedir. Ancak doğru sürümünün bulunmaması, elektronik belgelerin güvenilirliği ve bütünlüğü konusunda ciddi soru işaretleri meydana getirebilmektedir.

Bütün belirtilen hususlar çerçevesinde, yasal süreçlerde elektronik belgelerin delil olarak kabul edilebilmeleri için, gerçeklik, bütünlük ve orijinal formunda bulunma gibi özelliklerin sağlanması gerekmektedir.

4.6.3. Gerçeklik ve Bütünlüğü Korumada Sayısal İmza

EBYS, elektronik belge ile ilgili dijital imzayı doğrulayabilmelidir. Sistem, aynı zamanda rastgele bir belge örneğinin dijital imzasını doğruluğunu denetleyebilme özelliğine de sahip olmak zorundadır (Public Records Office of Victoria, 2000:5). Dijital imzayı doğrulamadaki hatanın belgenin değiştirildiğinin ya da sahtesinin yapıldığının göstergesi olabilmesi dolayısıyla, dijital imzayı doğrulamadaki herhangi bir hata kaydedilmek ve anında yöneticinin dikkatine sunulmak zorundadır. Elektronik belge, doğrulama hatalarında yöneticinin kabulünü de gerektirir. Eğer belge, erişim performansını artırmak için arşiv

dışında bir yerde kaydediliyorsa, hızlı bellekteki belgenin değiştirilmediğini, arşivdeki kopyasıyla aynı olduğunu otomatik olarak doğrulamaya imkân vermesi gereklidir.

Dijital imzaların koruma zinciri ya da veri bütünlüğü için uzun vadeli saklamalarda sınırlı değere sahip olduğunun farkında olunması önemlidir. İmzanın değeri, geçerlilik ile sınırlıdır. Geçerlilik zamanı, gizli anahtarın gizliliğinin ihlal edilmesi zamanı, imza algoritmasının gizliliğinin ihlal edilmesi zamanı ve açık anahtar alt yapısının eskime zamanını bağlı olarak sona erebilmektedir (Sproull ve Eisenberg, 2005:62). Örneğin, belgeler için dijital imza oluşturmak amacı ile kullanılan özel anahtar belirli bir zamanda gizliliği ihlal edilmiş hale gelirse, o tarihten sonra özel anahtarla doğrulanmış belgeler şüpheli olacaktır. Gizliliğin ihlal edilmesi doğrulanan kayıtları artık tehlikeye sokmazken, yetkisiz kullanıcının belgeyi düzenleme ya da oluşturulma gününü anahtarın geçerli olduğu dönemdeki herhangi bir güne kaydetme imkânı verir. Bir anahtarın gizliliğinin ihlal edilmesinin fark edilmesi aslında bu olayın gerçekleştiği zamandan çok sonra olabilir. Gizlilik ihlali kriptonalitik bir saldırı sonucunda da olabilir (Sproull ve Eisenberg, 2005:62). Bu nedenle dijital imzalar yeni iletilmiş verileri doğrulamak için en mükemmel yöntemdir.

Dijital imzalar, güvenli iletişim kanalı oluşturmak için diğer birçok kriptografik araçlar ile birlikte kullanılabilir. SSL Protokolü, ilk olarak Netscape tarayıcısında uygulanmıştır daha sonra İnternet Mühendislik Görev Ekibi tarafından standartlaştırılmış ve bütün Web tarayıcılarında kullanılmaktadır. Bu da güvenli kanala bir örnektir. TCP tarafından sağlanan güvensiz kanalın üstünde güvenli bir kanal kurar. Bunu da delillerin değiş tokuşu dijital imzaları kullanarak paylaşılan gizli anahtarların görüşmesi ve mesajların aslına uygunluğunu kanıtlayan MAC kodlarını değiş tokuşu ile yapar (Sproull ve Eisenberg, 2005:62). MAC'lar gerekli bir ortak ve gizli anahtar imzası mekanizmasıdır. SSL'lerin uygulanmasında gözden kaçan bir önemli adım protokol raporlarıdır. Bunlar güvenlik bağlantılarının diğer ucundadırlar. Aslına uygunluğun tamamlanması için, alıcının tanımladığı durumun beklenen durum olduğunu görmek için raporu kontrol etmesi gerekmektedir. Birçok mevcut web tarayıcı bu adımı atlamak ya da önemini azaltmak için SSL kullanmaktadır, bunun sonucunda da güvenlik kanalının aslında hiç güvenli olmadığı sonucuna varılabilir. Dolayısıyla belgenin bütünlüğü tehlikeye atılmış olur.

Uzun dönem saklamada dijital imza teknolojisi kullanılarak, belge üretiminden sonra yapılan herhangi bir değişikliğin tespit edilebilmesi sağlanır (Public Records Office of

Victoria, 200:2). Dijital teknolojinin olduğu yerde, diğer sistem kullanıcılar tarafından, kişisel anahtarların bulunmamasını sağlamak için korumaya yönelik ciddi tedbirler alınmalıdır. Buna ek olarak, sistemden üst veri sağlamaya ya da zaman ve tarih damgası gibi uygulamalara dikkat gösterilmelidir. Bilgisayar sistem saatini değiştirerek, sahte belge üretmek mümkün olmamalıdır.

4.7. Uzun Dönem Arşivlemede Elektronik İmza Sorunları ve Çözüm Önerileri

Arşivlemede yaşanabilecek elektronik imza sorunları değerlendirildiğinde, elektronik imza oluşturulurken kullanılan kriptografik algoritmalar zamanla zayıflamakta ve kırılabilir hale geldiği görülmektedir. Ayrıca, imzaya eklenen zaman damgaları da kullanılan algoritmalara bağlı olarak zamanla zayıflayabilmektedir. İmza oluşturulurken kullanılan sertifikaların ait olduğu üst köklerin de belirli geçerlilik süreleri vardır. Bu zayıflamalardan dolayı, imzanın geçerliliğini koruyabilmesi için periyodik olarak tekrar güçlendirilmesi gerekmektedir.

Arşivlenmiş e-belgelerin bütünlüğü ve kaynağının doğruluğu elektronik imza ile sağlansa bile, imzaların atılmasını sağlayan elektronik sertifikaların ömrü sınırlı olduğundan, geçerlilik kontrolü bakımından sorunların yaşanması muhtemeldir. İmzaların uzun dönemli saklanmasında yaşanacağı öngörülen sorunlara karşı tedbir alabilmek amacıyla, imzaların gerekli ek verilerle birlikte depolanması bir çözüm önerisi olarak sunulmaktadır. İmza veri yapısı standartlarına bağlı olarak bu konuda iki standart geliştirilmiştir; birincisi Kriptografik Mesaj Sözdizimi (CMS) yapısındaki imzalar için CMS ileri Elektronik imzalar (CAdES), ikincisi XML yapısındaki imzalar için XML ileri Elektronik imzalar (XAdES)dır. CAdES bünyesinde tanımlanan veri yapıları, çekirdekte yer alan imza verisinin üzerine sağlıklı bir arşivleme için gerekli verilerin katmanlar halinde eklenmesini sağlamaktadırlar (Özarar ve Kırımer, 2007:299).

Elektronik sertifika hizmet sağlayıcısının faaliyetlerinin sonlandırılması ya da kendinsin son vermesi durumunda elindeki sertifikaları başka bir kuruma teslim etmelidir. ESHS'nın nitelikli elektronik sertifika sahiplerinin zarar uğramasını engellemek için faaliyetlerine son vereceklerine ilişkin bildirimi zamanında yapmalıdır. Kullanım süresi

dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği iptal durum kayıtları bulunmaktadır. İptal durum kaydını herhangi bir kimlik doğrulamasına gerek olmaksızın ücretsiz ve kesintisiz olarak kamu erişimine açık tutulması gerekliliği elektronik imza kanununda belirtilmiştir. Faaliyetine son verilen ESHS, son iptal durum kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder, geçerlilik süresi en geç sona eren nitelikli elektronik sertifikanın geçerlilik süresi sona erene kadar iptal durum kaydı hizmetini devam ettirir ve arşivi en az yirmi yıl süreyle saklar (Orta, 2005: 133). Elektronik sertifika hizmet sağlayıcılarına duyulacak güvenin temini açısından nitelikli elektronik sertifikanın süresi dolana kadar kullanımının sağlanması gereklidir. Bunun sağlanması uzun dönem arşivleme açısından hizmet sağlayıcıları bağlamında yaşanabilecek sorunları ortadan kaldıracaktır. Ayrıca elektronik sertifika hizmet sağlayıcılarının verdiği hizmetler gereği tutacağı kayıtların saklanması hukuki ihtilafları çözmede büyük önem taşımaktadır. Bu açıdan elektronik sertifika hizmet sağlayıcılarının verdikleri hizmetlere ilişkin kayıtların saklanması kanunla düzenlenmiş, yönetmelikle bu sürenin 20 yıl olduğu hükme bağlanmıştır. Bu açıdan, bu verilerle ilgili olarak uzun dönem arşivleme açısından gerekli yedekleme ve felaket kurtarma planları yapılmalı, veri kaybını önleyici tedbirler alınmalıdır. Aynı şekilde, buna ilişkin kayıtlara sağlıklı bir şekilde tutulması uzun dönem arşivleme çerçevesinde yasal durumlarda ortaya çıkacak sorunların çözümünde büyük önem arz etmektedir. Bu açıdan bu tür kayıtların güvenli bir ortamda erişilebilir olması önemli bir zorunluluktur. Ayrıca sistemin güvenliğini korumaya yönelik uygulamalarda gerçekleştirilmelidir. Uzun dönem arşivleme açısından dijital koruma tekniklerine de ihtiyaç duyulacağı göz önünde bulundurularak, buna ilişkin planlamalar da yapılmalıdır. Daha önce bahsedilen temel dijital koruma teknikleri aynı şekilde elektronik imza içinde kullanılmalıdır.

Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım ve donanım aracı olarak tanımlanan e-imza oluşturma araçları smart kartlar, e-token veya bilgisayar yazılımları olarak uygulamada görülmektedir. Bunlara ilişkin yazılım ve donanım uyumlarının zaman içinde kontrolü ve devamlılığının sağlanması gereklidir. Yani, arşivleme teknolojisi değişse dahi arşivlenen verinin okunabilir olması gereklidir. Ayrıca imza oluşturma verisinin bulunduğu donanım aracının dışına çıkarılamayacağı gerçeği göz önünde bulundurulmalıdır. Bununla birlikte, sertifika sahibinin özel anahtarını kaybedebileceği ya da sertifikanın zaman içinde kullanılmaz hale geleceği gerçeği ışığında, elektronik sertifika

hizmet sağlayıcıların üretilen imza oluşturma verisinin bir kopyasını tutarak anahtar kurtarma işlemini yerine getirebilir (Orta, 2005:126). Bu tamamıyla istisnai durumlarda geçerlidir.

Uzun dönem arşivlemede elektronik imzaya ilişkin oluşabilecek sorunları çözme açısından arşiv elektronik imza (ES-A) büyük önem taşımaktadır. ES-A, Genişletilmiş Uzun Elektronik imza veya Zamanlı Genişletilmiş Uzun Elektronik imza formatlarına bir veya daha fazla Arşiv Zaman Damgası niteliği eklenerek oluşturulmaktadır. Bu imza formatı, uzun zamanlı imzaların arşivlenmesi için kullanılmaktadır. Zaman damgaları, tüm yapıları zayıf özet algoritmalarına veya kriptografik algoritmaların kırılmasına karşı korumaktadır (Hasırcıoğlu, 2006). Bu açıdan uzun dönem arşivleme açısından arşiv elektronik imzanın mutlaka kullanılması gerekmektedir. ES-A yapısındaki zaman damgası içerideki verilerin doğruluğunu daha uzun bir süre boyunca belgeleyebilecektir ES-A yapıları başka ES-A yapılarının üzerine yeni bir zaman damgası eklenerek de oluşturulabilirler. Bu özellik, ES-A yapılarının üzerine periyodik olarak daha kuvvetli algoritmalarla zaman damgası ekleyerek arşivleme süresini sürekli uzatma imkânını tanır (Özarar ve Kırımer, 2007:300).

Bir elektronik imzanın, oluşturulmasının üzerinden uzun bir süre geçtikten sonra doğrulanabilmesi önemli bir problem olarak karşımıza çıkmaktadır. Aradan geçen zaman nedeniyle ortaya çıkabilecek benzer sorunlara hazırlıklı olmak gerekmektedir. Bu açıdan güvenli bir elektronik arşivleme için zaman damgasının e-imza ile tümleşik şekilde kullanılması gerekir. Elektronik imzalı bir belgenin kullanım süresi zaman damgalama hizmeti ile uzatılabilir. Elektronik imzanın iletimi ve birleşik doğrulaması belli bir zamanla sınırlıdır. Ancak, birtakım dijital olarak imzalanmış belgeler orta vadeli uzun dönem arşivleme için uygundur ve bu belgelerin gerçekliği öngörülen süre kadar garanti edilmek zorundadır. Elektronik belgelerin dijital imza bağlamında geçerliliğinin uzun vadede garanti edilemeyebileceği göz önünde bulundurulmalıdır. Dijital imzalar ağırlıklı olarak teknolojiye bağımlıdır. Diğer teknolojilerle benzer bir şekilde, doğrulama teknolojileri de teknolojik eskimeye maruz kalırlar. Veri akışı ve hash kodunun şifrelenmesi belirli algoritama ve yazılımlara bağlıdır (Boudrez, 2005). Her ikisi de teknolojik eskimeye tabidir, ama elektronik imzanın uzun vadede yeniden doğrulanması için gereklidirler. Ayrıca dijital sertifikaların belli bir süresi olduğu düşünüldüğünde ve elektronik belgelerin yasal saklama sürelerinin daha uzun olacağı değerlendirildiğinde dijital imzaların doğrulanması noktasında önemli sorunlar oluşmaktadır. Eğer veri akışı bozulmamasına rağmen doğrulamada hala problemler yaşanıyorsa, teknolojik eskimeden dolayı oluşan problemleri çözmek için taşıma işleminin

yapıldığı anlaşılmalıdır (Boudrez, 2005). Elektronik belgelerin taşınması, belgenin bit ve baytının değişmesi doğal sonucunu doğuracaktır. Kaynak ve hedef dosyaları şekillendiren veri akışları birbirinden farklıdır ve farklı hash kodları üretecektir. Taşıma işleminden sonra, kaynak dosyada hesaplanmış dijital imza, hedef dosyanın doğrulanması için kullanılabilir olmayacaktır.

Gelecekte elektronik belgeleri doğrulamak için dijital imzanın kullanılmaya devam etmek için, elektronik belgeleri ve dijital imzayı tek başına korumak yeterli değildir. Doğrulama için, harici bir açık şifreleme düzeni gereklidir. Dijital sertifika ve kök sertifika dahil olmak üzere tam doğrulama zinciri geçerli kalmak zorundadır (Dumortier ve Van Deneynde, 2002). Doğrulama zinciri, uzun dönem arşivlemede imzanın geçerliliğini sağlayan unsurları kapsamaktadır. Dijital imza ile ilgili yazılım uygulamalarının yaşam evresinin oldukça kısa olduğu göz önünde bulundurulduğunda, doğrulama teknolojisinin geçerli kalacağı ile ilgili bir delili bulunmamaktadır. Gelecekte, belgelendirilmiş algoritmalar temelinde gerekli yazılımın yeninden yapılması gerçekten imkânsızdır. Ama bu oldukça pahalı ve karmaşık bir konu olacaktır. Gerekli kısımlar artık geçerli ve işlevsel değilse, doğrulama zinciri kırılmış demektir. (Boudrez, 2005). Doğrulama zinciriyle ilgili bütün öğeler, dijital arşivin kendisinde hazır vaziyette bulunması dahil olma üzere bir zorunluluktur. Dijital arşivin içinde bir sertifika arşivi de kurulması gereklidir. Bu sertifika arşivi çok iyi korunmalıdır. Böylece sertifikalar değiştirilemeyecek ya da sertifikaya herhangi bir ekleme yapılamayacaktır. Sertifikanın geçerlilik tarihi sona ermesi ya da iptal edilmesi durumunda, sertifikanın durumuyla ilgili bilgininde saklanması önemlidir. Zaman damgasının arşivlenmesi, belgelerin dijital sertifika geçerlilik süresi bitmeden ya da iptal edilmende önce özel bir anahtarla imzalandığının göstermesi açısından önemlidir. Uzun dönem arşivleme açısından dijital imzanın kendisi bir problem değildir. Ancak belgenin erişilebilirliğinin sağlamakla birlikte dijital imzanın doğrulanması bir problem olarak ortaya çıkmaktadır. Bu çerçevede, aşağıda uzun dönem arşivlemede dijital imza sorunlarını çözüm noktasında Boudrez (2005) tarafından ortaya konulan öneriler ve bazılarının henüz tam anlamıyla uygulamada kabul görmediği hususlar aşağıda değerlendirilmiştir;

- *Dijital koruma tekniklerinden taşıma işleminden sonra elektronik belgelerin yeniden imzalanması:* Elektronik belge farklı formatlara taşındığında, dijital imza onay fonksiyonunu kaybeder. Taşıma işleminden sonra, bilgisayar dosyalarının bitleri değişir, bu yüzden, taşıma işleminden sonra yapılacak herhangi bir doğrulama, hash

- *Doğrulamanın tasdik edilmesi:* Elektronik belge alındıktan hemen sonra, dijital imzanın geçerliliği kontrol edilir. Doğrulamanın sonucu, elektronik belgenin üst verisinden alıcı tarafından tasdik edilir. Bu verinin elektronik belge ile birlikte arşivlenmesi ve hilelere ve değişikliklere karşı korunması bir zorunluluktur. Dijital imza doğrulama teknolojileri çoğunlukla teknolojik çözümlerdir ve teknolojik eskimeden kaçamazlar. Üstelik doğrulama zincirinin de arşivlenmesi gereklidir.
- *Orijinal veri akışının ve doğrulama zincirinin korunması.* Doğrulama zincirinin arşivlenmesi ile ilgili çözüm önerileri aranmakta, böylece doğrulamanın uzun vadede korunması mümkün olabilecektir. Bunun için sadece orijinal veri akışının arşivlenmesi gerekli değildir, aynı zamanda belli bir doğrulama periyodundan sonra doğrulamak için gerekli dijital imza, açık anahtarla birlikte dijital sertifika, sertifika ile ilgili üst veri, zaman damgası ve ikinci tasdik imza gibi bütün açık şifreleme düzeni öğelerinin de arşivlenmesi gereklidir. Doğrulama zinciri, elektronik belge korunduğu sürece korunmalı ve işlevselliğinin devamlılığı sağlanmalıdır. Her bir dijital imza için asgari olarak, kullanılan hash algoritması, dijital imzayı hesaplamak için kullanılan algoritma, imza sahibinin adı, şifresi çözülmüş dijital imza, açık anahtar ve dijital imzanın durumu gibi hususların tasdik edilmesi bir zorunluluktur.
- *Taşıma işlemlerinin onaylanması:* Taşıma işleminden sonra oluşan doğrulama problemleri için diğer bir çözüm taşıma işlemlerinin onaylanmasıdır. Bu durumda taşınan elektronik belgeler yeniden imzalanmaz. Ancak güvenilir üçüncü kişi yetkililerce; taşıma işlemi yapılmanda önce elektronik olarak imzalanmış belgeleri doğrulanır, taşıma işlemlerinin kontrol edilir ve sertifika verilir. Bu yaklaşımla, taşınan elektronik belgelerin güvenirliliği elektronik imza ile değil verilen sertifika ile sağlanır.

Esasında dijital imzaların uzun dönem arşivlenmesinde çok az ya da hiçbir soruna sebep olmamaktadır. Ancak doğrulama fonksiyonlarının arşivlenmesi özel bir dikkat gerektirmektedir. Bu durum, dijital imzaların elektronik belgelerin uzun dönemde geçerliliğini sağlamak için dizayn edilmemiş olmaları gerçeğinden kaynaklanmaktadır. Elektronik belgelerin okunabilirliğiyle ilgili problemleri çözmeye yönelik çalışmalar dijital imzaya ilişkin sorunları arttırmaktadır. Ayrı çözümler üretmek yargısal ve arşivsel gereklilikleri karşılamaz. Ayrıca taşıma işleminden sonra yeniden imzalanan bir elektronik belge yasal açıdan mevcut yapıda geçerliliği söz konusu değildir. Bu açıdan buna ilişkin çözümler üzerinde değerlendirmeler yapılmalı ve sağlıklı sonuçlara ulaşılmalıdır.

4.8. Üst Veri Elemanları

Üst veri ile ilgili literatürde kullanılan en yaygın tanım veri hakkındaki veri tanımıdır. Üst veri, belgenin yazarı, üretim tarihi, imha tarihi gibi temel bilgileri içerir. Üst veri elemanları için herhangi bir sınırlama getirilmemeli, mümkün olan en geniş kapsamda üst veri elemanları oluşturulmalıdır. Zira bu e-belgenin erişilebilirliğini arttıran en önemli unsurdur. Farklı belge türleri için farklı üst veri elemanları tanımlanmalıdır. Sistem içinde bulunan üst veri elemanlarının belgeye ulaşımı kolaylaştıracak bir indekslemeye tabi tutulup tutulmayacağı sistem tasarım aşamasında belirlenmeli ve işlemin otomatik yapılması sağlanmalıdır. Elektronik belge yönetim üst verisinin en önemli özelliği, ona elektronik belge özelliği kazandıran belge nitelikleridir. ISO 15489 standardında üst veri (ISO, 2001b) "belgenin yapısını, içeriğini ve bağlamını tanımlayan veri ve zaman içindeki yönetimi" olarak tanımlanmaktadır. Bir başka ifade ile üst veri elektronik belgeyi tanımlayan veridir. Bu, gerek elektronik ve gerekse kâğıt belge ile ilgili tanımlayıcı bilgileri sağlar. Elektronik belge üretildiği ya da başka bir depolama ortamına aktarıldığında uygun üst veri elemanlarıyla birlikte işlem gerçekleştirilmelidir.

Kapsamlı üst veri bir elektronik belgenin erişilememe riskini minimize eden en iyi unsurdur. Uygun bir şekilde oluşturulan üst veri aşağıdaki hususların tespitini sağlar (Sitts, 2000:174);

- Belgeyi kimin ürettiğini, belgenin adını, kimin formatladığını ve diğer tanımlayıcı bilgiler,

- Kimlik tespitini ve bunun için daha fazla tamamlayıcı üst veriye gereksinim duyan organizasyonlara, klasörlere ya da veri tabanlarına bağlanmayı sağlar
- Belgeyi görüntülemek için gereken teknik gereksinimi, içerdiği uygulamaları, hangi versiyona gereksinim duyulduğunu, çalışmanın ilk durumuna getirilmesini, ona bağlanmaya gerek duyan diğer dosyalara gerekli bilgileri sağlar

Bazı üst veriler, belgelerin nasıl yapılandırıldığını, onların ne tür belgeler olduğunu, nereden geldiklerini, ne zaman oluşturulduklarını ifade eder. Hem belgelerin kurum içinde kullanılmalarını ve hem de araştırmacıların belgelere etkin ulaşmalarını sağlamak için üst veri türü bilgilere ihtiyaç bulunmaktadır (Sproull ve Eisenberg, 2005:32). İçerik üzerinde daha etkin erişim sağlayan otomatik üst veri özütleme tekniği çok çeşitli algoritmaları ve yaklaşımları kapsar ve çoğunlukla, yarım yapılanmış ya da doğal dildeki metinden bilgi ayıklamak için kullanılır. Başka bir ifade ile belge için gönderici, alıcı ve konu gibi hususlar açıkça etiketlenmemiş olsa bile özütlenmesini sağlar (Sproull ve Eisenberg, 2005:33). Üst verinin otomatik sağlanması için ilgili içerikteki gruplamaları ayırmaya yarayan kategorizasyon gibi teknikler kullanılır. Ancak bunun gibi teknikler her zaman doğru üst veriyi sağlamayabilir.

Üst veri elemanları asgari olarak aşağıdaki formatları desteklemelidir (Kandur, 2006: 76);

- Alfabetik
- Nümerik
- Alfa-nümerik
- Tarih / saat
- Mantıksal (Evet/Hayır)

Sistem tasarım aşamasında parametrik bilgiler sisteme dahil edilmelidir. Bu işleyişte ve tanımlama da farklılıkları ortadan kaldırarak standartlaşmanın oluşmasını sağlayacaktır. İlk etapta ve en kolay bir şekilde tarih ve nümerik olan alanlarla ilgili parametrik bilgiler girilmelidir. Diğer alanlarla ilgili parametrik bilgiler daha sonra uygulama safhasında oluşabilmektedir. Elektronik belgeleri tanımlayan üst verilerin manüel tanımlamalara mümkün olduğunca az başvurulacak şekilde oluşturulması gerekmektedir. Üst verinin

otomatik olarak toplanmasını sağlayacak aşağıdaki üç yolun anlaşılması faydalı olacaktır (Sproull ve Eisenberg, 2005:43);

- Üst veri doğal olarak belge oluşturulduğunda toplanabilecektir. Örneğin, kelime işlemcisi son değiştirilme tarihini tanımlayarak otomatik olarak üst veriyi eklenebilir.
- Üst veri otomatik olarak her hangi bir bilgiye başvurmadan ya da belgeyi anlamadan bir belgeden ayıklanmış olabilir.
- Üst veri, bir belgeden bilgi ayıklama ya da sınıflandırma (kategorizasyon) teknikleri kullanılarak otomatik olarak ayıklanabilir.

Bu seçeneklerin ilki, nispeten daha kolay ve daha ucuzdur. Bu yazılmış belgeler için tercih edilen yaklaşımdır. İdeal olarak kuruluş belge saklama sisteminin yerleşik otomatik yakalama özelliklerinin olması gerekir. İkinci seçenek de gereksiz yapıya sahip belgeler için daha kolay ve ucuzdur. Üçüncü seçenek yedek olarak görülmelidir. Otomatik üst veri özütleme tekniklerinin kullanılması gerekli olsa bile, içeriğe özgü teknikler kullanabilecek yapıları oluşturma işlemini daha önce yapmak sağlıklı olacaktır (Sproull ve Eisenberg, 2005:44).

Elektronik belge yönetim sistemi zorunlu üst veri alanlarının kaydedilmesine imkân tanımak zorundadır. Bunun dışında, elektronik belgelerin depolanması için, ek üst veri alanlarının oluşturulabilir. Eğer ek üst veri alanları girilecekse, kamu birimlerinin, standart belge formatlarını geliştirmeye yönelik en iyi yaklaşım üzerinde değerlendirmeler yapması önerilir. Bu kamu birimleri arasında üst veri konusunda birlikte işlerliğin sağlanmasını destekleyecektir (Public Records Office of Victoria, 200:3). Elde edilen bilginin doğruluğu artarken, elde edilen üst verinin toplam maliyetini azalmayı sağlayacak bir analiz gerçekleştirilmelidir. Mümkün olduğunca, üst veri elle değil, bilgisayar sisteminden, uygulamadan ya da diğer belgelerden otomatik elde edilmelidir. Fakat üst veriyi otomatik elde etmeyi sağlayacak yazılımın geliştirilmesine, sistemin devamlılığı ve bakımı için gerekli maliyete dikkat edilmelidir. Aslında, maliyet etkinliği, uygulamayı gerçekleştirmek için kullanılan teknolojiye ve üretilen belgenin önemine bağlı olarak değişecektir.

Elektronik belge yönetim sistemi, belge üretimi sırasında kullanıcılar tarafından girilen üst verileri kontrol edebilmelidir. Bu, veri geçerlilik teknikleri, kavramlar dizini ve sistemden zaman ve tarihin otomatik elde edilmesi kullanılarak sağlanabilir. Bu tekniklerce kullanılan

bilgilin üretilmesi ve korunmasına ilişkin maliyet analiz edilmelidir. Üst veri kontrolü yapan sistemin, kullanıcıların belgeleri doğru bir şekilde tanımlamalarını engelleyecek kadar katı olmamasına özen gösterilmelidir (Public Records Office of Victoria, 2000:4). Elektronik belgeler üretildiğinde, elektronik belge yönetim sistemi, kullanıcıların yeni üretilen belgelerle, arşivdeki eski belgeleri ilişkilendirmesine izin verecek bir yapıda olmalıdır. Bu basit bir ilişkilendirme değildir, ilişkilendirilmiş elektronik belge ile ilgili ortak üst veriyi de kapsar. Bir ilişkilendirme gerçekleştirme de, daha önce üretilen belgenin üst verisinin göz önünde bulundurulması önemlidir. En alışılmış üst veri linklerinden biri dosya atıfı olabilir. Aynı dosya atıfları olan bütün belgelerin, aynı dosyada düşünülmesi gerekmektedir.

Sistem tasarımı aşamasında üst veri elemanlarının veri kaynaklarının neler olduğu tanımlanmalıdır. EBYS üst veri elemanları için veri kaynakları şunlar olabilir (Kandur, 2009);

- İşletim sistemi
- Ağ yazılımı
- Uygulama programı
- EBYS
- Bilgisayar sistemi yöneticisi
- Bilgi ve belge yöneticisi
- Kullanıcı

İşletim sistemi, ağ yazılımı ve uygulama programlarıyla ilgili üst veri elemanları sistem tarafından otomatik olarak alınmaktadır. Bunlara müdahaleyi teknoloji mümkün kılmamaktadır. Diğer veri kaynaklarından gelecek bilgiler üzerinde mutlak kontrol sağlanmalı. Olabilecek bütün değişiklikler, daha sonra oluşabilecek yasal ve idari sorunları çözebilmek için sistem tarafından kayıt altına alınmalıdır.

Elektronik belgelerin içeriğinin anlaşılması ve erişiminin etkin bir şekilde sağlanması açısından mümkün olduğunca daha fazla üst veri kullanılmalıdır. Gelecekte görüntülenmesi kritik öneme sahip olan dosyalar için çeşitli tipteki üst veriler bugün önemsiz görülmektedir. En doğru yaklaşım korunması ve erişilmesi kolay olan her çeşit üst verinin saklanması gereklidir (Sitts, 2000:174). Sistem tasarımcısı tarafından tanımlanan sistem üst verileri, genellikle elektronik belgeleri gerektiği kadar tanımlamak için yeterli olmayabilir. Bunu göz

önünde bulundurularak değerlendirmenin yapılması ve gerekli eklemelerin gerçekleştirilmesi gerekmektedir. Üretim ve kullanımın içeriğine yönelik belgenin neden üretildiği, belgenin kullanıcısın kim olduğu ve kimin sorumluluğunda olduğuyla ilgili üst veri eksikliği önemli sorunlara yol açabilir.

Belge üst verisi, iş süreçleriyle olan ilişkisine kısmen de olsa bağlı olmalıdır. Eğer bir klasör ya da klasör bölümü ticari işlemlerle ilgili belgeler içeriyorsa, o zaman, bileşenlerin paylaşabileceği ortak üst veri elemanları olmalıdır. Belge yönetim üst veri elemanlarıyla ilgili hususlar, belgenin kaynaklarını, uygulamalarını, zorunluluk düzeylerini ve önemini ortaya koymaktadır. İngiltere Milli Arşivi (The National Archives, 2004) tarafından hazırlanan ve 2004 yılında revize edilen elektronik belge yönetim sistem gereksinimleri üst veri standartları çalışmasında belirtilen, genel kabul görmüş uluslararası Dublin Core standardı öngörülen ve Minnesota eyalet arşivi tarafından açıklanan (Minnesota Historical Society, 2004) üst veri elemanları birlikte aşağıda değerlendirilmiştir;

- *Tanımlayıcı işaret:* Sistem içinde ya da sınıflandırma şemasında belge için benzersiz tanımlayıcı işarettir. Bu belgeleri birbirinden ayıran bir kod dur. Zorunlu bir alandır
- *Başlık:* Belgeye, dosyaya ya da tanımlama düzeyine verilen başlıktır. Bir başka ifade ile bilgi kaynağını üreten tarafından verilen addır. Erişim fonksiyonu da dahil olmak üzere tanımlamayı desteklemek için önemlidir. Zorunlu bir alandır.
- *Konu:* Belgenin konusunun belirtildiği alandır. Belgenin içeriğini, konusunu tanımlayan ibare ya da anahtar kelimeler bu alanda belirtilir. Başlıkla ulaşılabilecek aramalar için daha yapılsa erişim araçları sağlar. Seçmeli bir alandır. Klasör ve dosya düzeyinde uygulanması önerilir.
- *Tanım:* Belgenin, konu, başlık gibi alanlar dışında kullanıcılar için daha faydalı olacak farklı ayrıntıları kapsamaktadır. Belgenin içeriğinin kısaca tanımlanmasıdır. Özellikle belge ve klasör düzeyinde uygulanması önerilir.
- Üretici: Belge vasfını kazanmasına kadar belgenin içeriğinden sorumlu kişiyi ifade etmektedir. Bir başka ifade ile belgeyi üreten kişi ve/veya kurumun adıdır. Bu alanda amaç, belgenin içeriğinden sorumlu kişi ve kurumların tanımlanmasıdır. Belge düzeyinde uygulanır ve zorunlu bir alandır.

- *Tarih:* İmhası hariç olmak üzere, belgenin yaşam döngüsü süresince olan faaliyetlerle ilgili tarih ve zamanla ilgili bilgileri içerir. Zorunlu bir alandır. Üretme ve alma tarihi belge düzeyinde uygulanır. Açma ve kapatma tarihleri ise klasör düzeyinde uygulanır.
- *Alıcı: B*elgenin gönderildiği kişiyi ifade eder. Belgenin alıcısının tanımlamak amacıyla kullanılan bir alandır. Bu alan elektronik posta için zorunlu ve diğer belgeler için seçime bağlı bir alandır. Belge düzeyinde uygulanması önerilir.
- *Belge Türü:* Gerek erişim ve gerekse saklama süreleri açısından farklık arz eden belge yapılarını ifade etmektedir. Belge düzeyinde uygulanması önerilir. Uygulanması gereken durumlar için zorunludur.
- *İlişki, Bağ:* Bir belgenin diğer bir belge ile olan arşivsel ilgisi ya da bir düzeyde kümelenmiş belgelerin diğer bir düzeydeki belgelerle ilgisini açıklamak için kullanılan bir alandır. Belgeler arasında ilişkilendirme yapılması gerekli durumlarda zorunlu bir alandır.
- *Kümeleme:* Belge yönetim fonksiyonlarının nerede gerçekleştiğini tanımlamak için kullanılan ölçme birimi olarak tanımlanabilir. Farklı düzeylerde hangi faaliyetlerin gerçekleştirilebileceğinin kapsamını açıklığa kavuşturmaya çalışır. Faaliyetler gerçekleştirilirken verilen izin düzeylere buna örnek gösterilebilir. Zorunlu bir alandır.
- *Dil:* Belgenin içeriğinin yazıldığı dildir. Araştırma ve diğer amaçlar için belgenin dilinin tanımlanmasını amaçlayan bir alandır.
- *Yer:* Belgenin fiziksel olarak bulunduğu yeri belirten alandır. Elektronik belgeler açısından özellikle zorunlu bir alan olduğu belirtmek gereklidir. Bu alan için yol tabiri de kullanılmaktadır.
- *Haklar:* Elektronik belge yönetim sistemi içinde arşivlenen belgelere erişimle ilgili kısıtlama ve izinleri içeren alandır. Bu haklar ve kısıtlamalar; yasal, kurumsal politikalar çerçevesinde belirlenir. Elektronik belgelerin güvenliği açısından önemlidir. Zorunlu bir alandır. Her tasnif düzeyine uygulanması önerilir. Özellikle klasör ve belge düzeyinde uygulanabilir.
- *Tasfiye(Ayıklama):* Yaşam evreleri sonunda belgelere ne olacağıyla ilgili duruma tespitiyle ilgilidir. Belge yönetim sisteminde saklama planlarının uygulanmasını sağlamayı amaçlamaktadır. Zorunlu bir alandır. Her düzeyde düzenlemeye uygulanır. Belgelerin ayıklama işlemi, yetkili kullanıcılarca denetlenmiş ayıklama programı aracılığıyla bilinçli bir şekilde yapılması gereklidir.

- *Dijital imza*: Bu alan imzanın kendisini korumaktan ziyada tarihsel imza doğrulamasının kaydedilmesiyle ilgilidir. Zorunlu bir alandır.
- *Koruma:* Belgenin yaşam evresi boyunca, belgenin tanımlanması, taşınması, sürdürülebilirliği ve koruma yönetim süreçlerinde kullanılan bilgileri içeren alandır. Zorunlu bir alandır
- *Format:* Belgeyi oluşturan elektronik bileşenlerin yazılım formatıyla ilgili alandır. Bir başka ifade ile belgenin bulunduğu ortamdır. Zorunlu bir alandır. Belge düzeyinde uygulanmalıdır.
- *Fonksiyon:* Belgenin üretildiği resmi fonksiyonla ve işlemlerle ilgili alandır. Belgelerin sınıflandırılması için ek bir takım unsurlar sağlar. Zorunlu olmayan bir alandır. Klasör düzeyinde uygulanabilir
- *Kapsam:* Belge içeriğinin kapsamı ya da büyüklüğüyle ilgi alandır. Aynı zamanda kurum ve yıl bazında bir kapsam tanımlamak için de kullanılır. Yani belgenin yasal, mekânsal ve maddi içeriğinin özellikleleriyle ilgili alandır. Birbiriyle daha ilgili belgelerin geri iletimini destekler. Faydalı olduğu düşünülen durumlarda kullanılır. Belge ve dosya seviyelerinde uygulanması önerilir.
- *Yönetim Geçmişi:* Belgelerin belge yönetim sistemi içinde üretilmesinden tasfiye işlemlerine kadar, belgeler üzerinde gerçekleştirilen bütün belge yönetim faaliyetlerinin tanımlamaları ve tarihlerini içeren alandır.
- *Emirler:* Belge yönetim gerekliliklerileyle ilgili kaynaklardır.

Üst verinin temel elemanları, belgenin değerini, yerini ve içeriğini tam ve anlaşılabilir bir şekilde tanımlamaya imkân veren yapılandırılmış format ve kontrollü sözlüktür. Üst veri herhangi bir bilgi sistemde olduğu gibi elektronik belge yönetim sisteminde de verimlilik ve etkinlik için temel bir araçtır. Üst verinin etkin bir şekilde kullanılması, kurumsal ihtiyaçlara uygun standartların anlaşılması ve uygulanması anlamına gelir. Üst verileri etkin bir şekilde üretmek, anlamak ve kullanmak için Minnesota Historical Society (2004) tarafından ortaya konulan ve detaylı bir şekilde bilinmesi gereken hususlar aşağıda değerlendirilmiştir;

- *Üst veri Fonksiyonları:* Kurumlar birçok fonksiyonu yerine getirmek için rutin olarak üst veri kullanırlar. Ancak üst veri öncelikli olarak, yasal ve kanuni sebepler, teknik sebepler, operasyonel ya da yönetimsel sebepler, kamuya, kurum personeline ya da diğerlerine hizmet vermek için kullanılır. Bütün bu bahsedilen önceliklerde, eğer üst

- *Yasal ihtiyaçlar ve kanuni emirler:* Kurumsal bir yapı olarak, temel yasal ihtiyaçların arşivlenmesine yardımcı olacak ve kanuni emirleri karşılayacak üst verilere özel bir önem gösterilmesi gerekmektedir. Yasal ihtiyaçları karşılamak için belgelerin, ne oldukları, nerede oldukları, önemlerinin ne olduğu, tasfiye işlemlerinin nasıl olacağı gibi konularda iyi tanımlanması gereklidir. Bütün bu bilgiler üst verdir.
- *Üst veri ve bilgi teknolojileri:* Üst veri, dijital ya da kâğıt ortamda depolanan bilginin yönetilmesi açısından faydalı bir araçtır. Ancak, dijital ortamdaki bilgi için kritik bir öneme sahiptir. Çünkü sadece uygun yazılım ve donanımlar kullanılarak okunabilir. Eğer bilgi teknolojileri üst veriyi gerekli kılıyorsa, üst veriyi faydalı kılan bu bilgi teknolojileridir. Özel yazılım uygulamaları, standart üst veri yapılarının üretilmesine imkân tanır. Veri tabanları, üst veri depolar ve bunlara erişimi sağlar. Birçok yazılım uygulamaları, otomatik olarak üst veri oluşturur, dosyalara gerekli ilişkilendirmeleri yapar. Örneğin bir ofis dokümanı üretildiğinde, otomatik olarak, başlık, yazar, dosya boyutu gibi birtakım üst veri unsurları otomatik olarak üretilir, ancak diğer unsurlar uyarlanabilir ya da el ile üretilebilir. Esasında, otomatik ve el ile üretilmiş bilgi kombinasyonu, tam ve uygulanabilir bir üst veri için en iyi çözümdür.
- *Üst veri Standartları:* Etkin bir şekilde çalışmak için, üst verinin tam ve anlaşılabilir olması önemli bir zorunluluktur. Kullanıcı ve üreticilerin bütününün yapılan tanımlamaların neyi ifade ettiğini anlaması gereklidir. Bu açıdan yapılan tanımlamaların ulusal ve ulusları standartlara uygunlu birlikte çalışabilirlik ve standartlaşma açısından büyük önem taşımaktadır.

Üst veri etkin kullanabilmek içi, kullanıcıların muhtemel bilgi ihtiyaçları mutlaka göz önünde bulundurulmalıdır. Ayrıca üst verini ve onu tanımlayan bilginin değerini arttırabilmek için diğer üreticiler ve konuyla ilgili sorumlu kişilerle birlikte çalışılması gerekmektedir. Eğer konuyla ilgi bütün taraflarla, üst veri standartları, araçları ve uygulamaları konusunda bir anlaşmaya varılırsa, kurumsal yapının bütünü için en faydalı çözüme ulaşılmış demektedir. Bu çerçevede seçilen standardın uygulama safhası önemli ve zorlu bir adımdır. Zira üst

verinin üretilmesi ve korunması dikkat, kaynak ve personel gerektirmektedir. Bunu için gerekli planlamanın ve yatırımın yapılması gerekmektedir. Bununla birlikte, üst verinin önemi ve uygulanması konusunda kurumsal bilincin oluşturulması gerekmektedir. Bu çerçevede üst veri uygun bir şekilde uygulandığında aşağıdaki faydaların elde edilir;

- Belge erişimini desteklenir
- Kapsamlı belge yönetim süreçlerini desteklenir
- Belge provenansını oluşturması sağlanır
- Belge bütünlüğünün tam olup olmadığını gösterilir
- Ayrı belgeler arasındaki ilişkinin varlığını açıklanır
- Belgelerin platformlar ve zaman süreçleri arasında ve teknolojik platformlarda sürekliliği ve birlikte işlerliğini desteklemek için gerekli bilgi sağlanır

Elektronik belgelerin etkin erişim sağlama açısından üst veri alanları mümkün olduğunca detaylı ele alınmalı, belgelere ilişkin detaylı tanımlamalar yapılmalıdır. Bu yaklaşım çerçevesinde, asgari üst veri elemanlarını belirtmek doğru olmamaktadır. Ancak, belgeleri tanımlamada, tanımlayıcı işaret, başlık, konu, üretici, üretim tarihi, alıcı, belge türü, dil, haklar, ayıklama, dijital imza, koruma ve format'a ilişkin bilgileri içeren alanlar tanımlamada bulunması gereken asgari zorunlu üst veri alanlar olarak değerlendirilebilir.

4.9. Felaket Kurtarma Planı ve Yedekleme

Elektronik belge yönetim sisteminde; veri yedekleme, felaket kurtarma ve acil durum işlemleri dahil olmak üzere bir acil durum planının geliştirilmesi büyük önem taşımaktadır. Acil durum planı, bir felaketten sonra elektronik belge yönetim sisteminin hızlı bir şekilde kullanılabilir hale getirilmesini sağlayacaktır. Planlar, elektronik belgelerde kaybı önlemek için veri kurtarmayı ve yedeklemeyi içermelidir. Girdi ve çıktıların zamanlılık ve doğruluğuna yönelik kontroller oluşturmak gereklidir. Sistemin girdi ve çıktılarının zamanlılık ve doğruluğu, sistem tarafından üretilen elektronik belgelerin gerçekliği ve bütünlüğünü göstermek açısından kritiktir.

Standart etiketleme ve izleme kayıtlarının tutulması gibi farklı tedbirler manyetik bantlar ve diğer ortamlar üzerinde fiziksel ve entelektüel kontrol sağlamaya imkân tanır. Felaket kurtarma planı çerçevesinde e-belgeler çevrimdışı ortamlar da, fiziksel ve çevresel

olarak kontrol edilmiş alanlarda depolanmalıdır. Ortam kontrolünün kapsamı, verinin türü, ortamın miktarı ve kullanıcı çevresinin niteliği gibi birçok faktöre dayanır. Kritik ve yüksek riskli elektronik belgelerin depolanması için kullanılan ortamlar, normal olarak diğer verirle göre daha yüksek düzeyde kontrol gerektirecektir (NECCC E-sign Policy Workgroup, 2001:14) Özellikle, veriler elektronik belgeleri oluşturuyorsa, verilerin ve yazılımların rutin yedeklenmesi kritik öneme sahiptir. Yedekleme sıklığı, verilerin ne sıklıkta değiştiğine ve bu değişikliklerin önemine bağlı olarak değişmektedir. Hangi yedekleme planının uygun olduğunu belirlemek için danışmanlık alınmasında fayda vardır. Yedek kopyalarının, felaket durumlarında sistemden uzakta bir yerde güvenli bir şekilde depolanma durumunu ve kullanılabilirliğini test edilmesi büyük önem taşımaktadır.

EBYS'nin, belge oluşturulduktan sonra e-belgeleri kaybedilmemesini sağlayacak şekilde sürdürülmesi gerekmektedir. Uygun yedekleme stratejilerinin uygulanması ve belgelerin kaybedilmesine yol açacak durumların belirlenmesi için bir risk analizinin yapılması gereklidir (Public Records Office of Victoria, 200:7). EBYS, belgenin kaydedildiği ortamı yenilenebilmesine imkân vermelidir. Doğru yenileme, e-belge içeriklerinin düzgün bir şekilde kopyalandığı ve imha edilmeyeceği belirtilen belgelerin kopyalandığının doğruluğun kanıtlanması bir zorunluluktur. Sistem, yenilemeyi ve yenilenen ortamın kimliğini kaydetmelidir. E-belgelerin arşivlenmesi, belgelerin üretildiği sistemden diğer bir sisteme ve çevrimdışı olarak transfer edilebilmesine imkân vermesi gereklidir. Sistemden e-belge alımı ve iletiminin kayıt altına alınması gereklidir. Bu işlemi yapan operatörün bilgilerinin de kaydedilmesi gereklidir. Belgelerin yeni yerleriyle ilgili göndermeler kayıt altına alınmalıdır.

Rutin elektronik belge yönetiminden başka, felaket durumlarına hazır olmaya dikkat gösterilmelidir. Acil durum planları, kurumun bütün kademelerindeki gerekli ve hayati belgelerin, tespit edilmesi, düzenlenmesi ve korunmasına yönelik çalışmaları içerir (Calrim, 2002:23). Bu anlamda; kurumların, elektronik belge yönetim faaliyetlerini ve bilgi işlem sistemlerinin devamlılığını sağlamak için önemsiz bir yıkımdan büyük felaketlere kadar acil durumlarla başa çıkmaya yönelik planlar geliştirmeye ihtiyaçları vardır. E-belge yönetim planı, felakete hazırlıklar ve kurtarma ihtiyaçları içermelidir. Bu planı bütün belge yönetim planının bir parçasına dahil edilerek değerlendirilmelidir.

Felaket kurtarma planı, farklı felaket senaryolarının e-belgelerin bütünlüğünü ve geçerliliğini nasıl tehdit edebileceğine yöneliktir. Bu çerçevede aşağıdaki sorulara verilecek etkin cevaplar büyük önem taşımaktadır (Calrim, 2002:23);

- Muhtemel bir felaket nasıl meydana gelir?
- Eğer bir felaket meydana gelirse ne yapılabilir?
- Etkilerini azaltmak için ne yapılabilir?
- Belgeleri korumak için ve felaket halinde kurtarmaya hazır olmak için ne yapılabilir?
- Riski yönetmek için, değerlendirme ve planlama amaçlı olarak proje yönetim metodolojileri nasıl kullanılır?

Acil durum, geçici bir güç kesintisinden bir birimin ve orda bulunanların tam yıkımı olarak tanımlanabilir. Her tür acil durumlara uyacak tek bir acil durum planı yoktur. Planlayıcıların beklenen durumlar için, sistemlerini bozacak muhtemel acil durum türlerinin ne olduğunu belirlemeleri, acil durum yanıt süreçlerini ve kurtarma palanlarını düzenlemeleri gerekmektedir. Bütün acil durumlar bir felaket olarak sınıflandırılmayabilir. Ancak felaket durumlarına hazırlıklı personelin, daha küçük acil durumlarla başarılı bir şekilde başa çıkabileceği önemli bir gerçektir. Genel olarak, felaket durumunun şiddetini ya da önemini tanımlayan dört seviyede bozulma meydana gelir. Bunlar şöyle sıralanabilir (Calrim, 2002:25);

- *Kısıtlı:* Herhangi bir hasar ya da kayıpla sonuçlanmayan geçici bir aksaklık bu düzeyde sınıflandırılabilir. Elektrik kesintisi ya da dalgalanması, iletişim arızası, tehditten dolayı birimi tahliye etme ya da kilit personelin mevcut olmayışı örnek olarak gösterilebilir.
- *Ciddi:* Ekipmanlardaki ya da ofis alanındaki tamir edilebilir hasar ya da kilit personel, veri, belge ya da yazılımlardaki yerine konabilir kayıplar ciddi bozulmalar olarak düşünülebilirler. Bir ekipmandaki bozulma, havalandırma sistemindeki arıza, ya da sabotajdan dolayı düşük hasar, vandalizm ya da insandan kaynaklanan hatalar örnek olarak gösterilebilir.
- *Büyük:* Ekipmanın, ofis alanının ya da verinin imhası bir büyük bozulma olarak sınıflandırılabilir. Su baskını, patlamadan dolayı ekipmanların tam kaybı ya da yapısal aksaklıklar, ya da kazara veya kasıtlı veri kaybı örnek olarak gösterilebilir.

- *Feci:* Bu kategori, ofis alanının ya da ekipmanların, verinin ya da insanların bütünüyle kaybını içerir. Ofisin tümüyle imhası ve yangın ya da doğal afetten dolayı personelin kaybı buna örnek olarak gösterilebilir.

Yukarıda belirtilen anlık acil durum seviyeleriyle başa çıkmak için felaket kurtarma planlarının, yeterince esaslı bir kapsamda olması, geçici hizmet sağlaması, elektronik belge yönetim ve bilgi işlem fonksiyonlarını normal durumlarına geri getirmesi gerekmektedir. Çünkü kurumların hızlı bir şekilde felaketlere cevap vermesi, kurtarma süreçlerine açık bir şekilde ortaya koyması gerekmektedir. Felaket kurtarma planını muhtemel yürütecek kişiler, bu planı geliştirenlerdir. Geliştiriciler, görevli çalışanların ehliyetsiz ve müteakip felaketle ilgili görevini yerine getirmede aciz olabileceklerinin muhtemel olduğunu düşünmeleri gerekmektedir. Bu nedenle, plan yazılı olmalıdır. Böylece kuruma çok alışkın olmayan diğer çalışanlar, işlemleri yürütmede gerekli bilgiye sahip olmuş olacaklardır. Kurumda ya da ekipmanlarda şiddetli bir hasar meydana getiren felaket dolayısıyla, işler onarılıncaya ve iyileştirmeler tamamlanıncaya kadar farklı bir yerde işlemlerin yürütülebilir olmasının sağlanmasını gerektirebilir. Felaket kurtarma planı içine sistemin kesintisiz çalışmasını sağlayacak bir güç kaynağının dahil edilmesi gerekmektedir (İmamoğlu, 2008:31). Kesintisiz güç kaynakları, bilgisayara gelen elektrik enerjisinin kesilmesi durumunda, sistemin geçici bir süre kesintisiz güç kaynağı(KGK) akülerinde depolanan elektrik ile beslenmesini sağlar.

Felaket kurtarma planlarında belirtilen hususların ve alınan önlemlerin çalışabilirliliği mutlaka test edilmelidir. Uzak bir yerde arşivlenen verinin sürekli güncellenmesi ve buna ilişkin senkronizasyonların yapılması büyük önem taşımaktadır. Glusetrfs sistemi öngörülen senkronizasyonu yapmada ve değişen verileri aktarmada mantıksal bir çözüm sunmaktadır. Bu sistem daha çok büyük veriler için kullanılmaktadır. Bu yapının genel işleyiş mantığı şöyledir; farklı yerlerde aynı sunucu ve depolama sistemi kuruluyor. Merkezi ünitede değişiklik olduğunda, felaket kurtarma için kurulan sisteme bütün değişiklikler otomatik olarak bu sistem sayesinde uygulanıyor. Dolayısıyla en kötü felaket senaryosunda, yani sistemin çökmesi durumunda, uzak bir yerde etkileşimli çalıştırdığımız sistem sürecin devamlılığını sağlamaya imkân vermektedir. Bu sayede elektronik belge yönetim sistemi herhangi bir sorun yaşanmadan işleyişine devam edebilmektedir. Bunun mutlaka sağlanması gerekmektedir.

Elektronik belge yönetim sistemiyle ya da onsuz, kurumlar elektronik belgelerinin felaketlerden korunmasını sağlamaya ihtiyaç duyacaklardır. Felaket kurtarma planının bir parçası da, kurumun elektronik belgelerinin planlı yedeklemesi olacaktır. Yedekleme, sabit disk bozulmalarına ya da yangın, deprem gibi doğal felaketler sonucun bilgisayar ortamında saklanan verilerin dış ortama aktarılması için kullanılır. Yedekler, kapasiteleri yüksek olan ve kaset olarak da adlandırılan manyetik bantlar üzerine alınırlar (İmamoğlu, 2008:23). Yedekleme üniteleri, IDE, SCSI ara yüzlerinden ya da paralel porttan bilgisayara bağlanabilir. Yedekleme sağlayan birçok metot, değişik düzeyde veri korumada kullanılır. Yedekleme programlarındaki en önemli faktör, düzenli yapılmasıdır. Yedeklemenin ne kadar sıklıkta yapılacağı çok yaygın bir sorudur. Cevap sübjektiftir. Ancak kesin olarak şu söylenebilir ki, yedekleme arasındaki süre, sonlandırmak istenen iş miktarıdır. Genel kullanımdaki genel geçer kural, her sekiz saatte birdir. Yedekleme sistemleri ve metodolojileri değişir, ancak çoğunluk yedekleme programlı bir şekilde otomatik olarak belirli zaman aralıklarında gerçekleştirilir (Calrim, 2002: 26). Bu yüzden, eğer bilgisayar gün boyunca kullanılıyorsa, o zaman yedekleme en az günlük. Eğer haftada sekiz saat veri üretimi varsa, o zaman yedekleme en az haftalık ve buna benzer süreler içinde yapılmalıdır. Eğer kullanıcının bilgisayarı paylaşımdaysa, dosyalarını sıklıkla yedeklenmesi teşvik edilmeli, tercihen her güncellemeden sonra yapılmalıdır. Yedekleme işlemi, eğer veri miktarı fazla uzun sürer ve performansı olumsuz etkiler. Bu sebeple yedekleme işleminin sunucu bilgisayarların çok az kullanıldığı zaman yapılması gerekmektedir. Yedeklemede temel olarak, her şeyin yedeğinin alınması, yedeği alınacak verilerin belirlenmesi ya da sistemin o anki yapılandırma bilgilerinin ve sistem dosyalarının yedeğinin alınması seçeneklerinden birinin uygulanmasıyla gerçekleştirilir. Hemen hemen düzenli yedekleme kadar, yedekleme ortamını doğru bir şekilde etiketlemede önemlidir. Sistem yenilemesi için önemli olan etiketlemede aşağıdaki bilgiler kullanılmalıdır;

- Kurumda e-belgelerden sorumlu birimin adı,
- İçeriği tanımlayıcı başlık,
- Üretim tarihi,
- Gizli ve açık bilgiler,
- Kullanılan yazılım ve donanım unsurları.

Elektronik belgelerin felaket durumlarında ulaşılabilir olması için, yedekleme araçlarının dikkatli ve planlı bir şekilde depolanması gerekmektedir. Belgeler sadece depolanmamalı ve yedeklenmemeli, kurumların aynı zamanda, sistem için gerekli olan uygulama yazılımlarının güncel sürümlerini, işletim el kitaplarını, sistem dokümanlarını, program dokümanlarını ve işletim sistemi bant ve disklerinin kopyalarını almaları gerekmektedir. Tipik bir yedekleme, verinin üç sürümü oluşturulmasından meydana gelir. Bunlar, verinin önceki hali, güncel veri ve güncel verinin kopyasıdır. Yedekleme araçları kurum dışında saklanmalıdır. Yedeklemenin, belge korumayı sağlarken, hızlı kurtarma ve belge imhası ile ilgili bilgi sağlaması gerekli değildir. Elektronik belge yönetim sistemi, belge kurtarma ve imha için en iyi çözümü sağalacaktır.

Zarar görmüş belgelerin kurtarılması için atılacak adımlar önemlidir. Eğer durum sudan zarar görmüş elektronik araçların kurtarmasını gerektiriyorsa, temizlenip kurutulmadan kullanılmamalıdır. Bu ekipmanların özellikle disk sürücülerinin zarar görmesini engelleyecektir. Islanan manyetik bantlardaki bilginin kurtarılma şansı yüksektir. Bütün iç yüzeyleri yumuşak pamuklu bir bezle silinir ve sıcak hava kurutucusuyla bant temizleyiciyi kullanarak kurutulur. Manyetik bantlar üzerinde uzmanlaşmış bir firmadan danışmanlık almak bu noktada önemlidir.

Temel olarak elektronik belge yönetim sisteminde felaket kurtarma işlemi, üst verilerin bulunduğu veri tabanını geri yüklenmesi, sistem ayarlarının geri yüklenmesi ve veri tabanından ya da elektronik depodan elektronik belgelerin geri yüklenmesini kapsar (Johnston ve Bowen, 2005:135). Gerçek bir felaket kurtarma deneyimi gerçekleştirilmeyebilir ancak, birçok felaket kurtarma testi, işin teknik boyutunun başarılı bir şekilde gerçekleştirdiğini göstermektedir. Bununla birlikte felaket senaryolarının oluşturulması ve bunların çalışabilirliğinin test edilmesi önemli bir gerekliliktir. Zira teoride bütün detaylarıyla ortaya konan bir felaket kurtarma planı uygulamada aynı sonucu vermeyebilir. Bu açıdan felaket senaryolarının test edilerek onaylanması başarılı bir felaket kurtarma planı için en önemli noktadır.

4.10. Sistem Bakımı

Elektronik belge yönetim sisteminin bağımlı çalıştığı teknolojik altyapının düzenli bakımın yapılması büyük önem taşımaktadır. Bu bağlamda gerekli yazılımsal ve donanımsal

düzenli bakımların yapılması sistemin devamlılığı açısından gereklidir. Sabit disk elektronik belgelere çevrimiçi ve anında erişim sunar. Sabit diskler çok hassastır. Küçük toz parçacıkları ya da duman diske zarar verebilir. Eğer bilgisayar kötü kullanıma maruz kalırsa veri kaybı da olabilir. Bilgi, disk sürücüsün okuma/yazma kafası tarafında sabit diske kaydedilir. Bu disk yüzeyine çok yakındır ancak yüzeyle teması olmamalıdır. Eğer disk ile okuma yazma kafası bir temas olursa, diskin kaydeden yüzeyini kaşımak suretiyle ciddi hasarlara yol açması muhtemeldir. Bu, kafa çarpması(sabit diskte veri kaybı) olarak adlandırılan sebeplerden bir tanesidir (Calrim, 2002:29). Bilgisayar her zaman dikkatle taşınmalıdır. Birçok sabit diskte, sistem taşındığında disk kafasının sabitlenmesi suretiyle kafa çarpma riskini azaltan bir düzenek vardır. Bazı sistemler, her sistem kapandığında kafanın otomatik olarak sabitler. Bilgisayarla ilgili dokümanlar, sabit disklerin taşınması sırasında korunmasına yönelik belirli talimatlar içermelidir. Sabit diskler için diğer bir potansiyel problem ufalanmadır. Günlük dosya üretim ve imhası yüzünden, sabit diskteki veri parçalara ayrılır, bu disk performansını azaltır(hız) ve nihayetinde kafa çarpmasıyla sonuçlanabilir. İşletim sistem talimatları, ufalanmayı azaltıcı süreçler içerir. Sabit diskin performansını ayarlayan(tune-up) basit ve kullanımı kolay ticari uygulamalar mevcuttur. Manyetik bant ve bant kartuşları, genellikle büyük ana bilgisayarlar ya da mini bilgisayarlar işlemleri ile ilişkilendirilirler. Bilgisayarlarda bulunan e-belgeler, artan bir şekilde yedek kopya sağlamak için büyük bilgisayarlardaki bantlara aktarılırlar. Bilgisayar manyetik bandı, kırılgan bir ortamdır, uygun olmayan kullanım ve korunmadan dolayı yüksek oranda hata riski oluşma durumu vardır (Calrim, 2002:30). Manyetik bant uygun ortamlarda korunsa bile, on yıldan fazla verinin okunabilir olması mümkün değildir.

Hız ve performansın en üst seviyede devamlılığının sağlanması büyük önem taşımaktadır. Gelişen yazılımlara bağlı olarak, donanım birimleri yenilenmekte ve buna bağlı olarak performans ihtiyacı da artmaktadır. Donanım birimlerinin hızına bağlı olarak ısınma problemleri ortaya çıkmaktadır. Sistem performansının mevcut kapasitenin üzerinde çalıştırılmak istenmesi veya bunun bir zorunluluk olması halinde işlemcinin soğutulması, kasanın soğutulması, ekran kartının soğutulması, belleklerin soğutulması, sabit disklerin soğutulması ve kart yuvalarının soğutulması gibi soğutma yöntemlerine başvurulması gerekmektedir (Henkoğlu, 2008:357). Bir sistemin düzenli ve sağlıklı çalışması açısından en önemli bileşenlerden biri olan belleğin çeşitli nedenlerden dolayı işlevini tam olarak yerine getirememesi, zaman zaman sadece performans üzerinde olumsuz etki yaratırken, bazen işletim sisteminin çökmesine veya sürekli kilitlenmelere sebep olabilmektedir. Bellek sızması

olarak adlandırılan bellek sorunları, aslında belleğin işlevini tam olarak yapmaması ve üzerindeki uygulamaların düzensiz ve gereksiz bir şekilde yer tutması anlamında gelir (Henkoğlu, 2008:389). Bu ve benzeri sorunlarla karşılaşmamak için düzen olarak sistemin bakımının yapılması gereklidir.

Fiziksel depolama mekânının düzenli bakımı da gerekmektedir. Bu depolama ortamlarının daha üzün süre kullanılabilmesini ve elektronik belgelerin bütünlüğünü destekler. Bu açıdan depolama tesisinin sürekli bakımını yapacak bir sistemin oluşturulması gereklidir. Bu çerçevede aşağıdaki hususlar yerine getirilmelidir;

- Tesise zarar vermeyecek şekilde kimyasallarda kullanarak düzenli temizleme faaliyetinin yapılması,
- Fiziksel depolama ortamlarındaki bozulmaların kontrolünün yapılmasıyla ilgili prosedürlerin tespit edilmesi,
- Elektronik içeriklerdeki bozulmaların kontrolüyle ilgili prosedürlerin belirlenmesi,
- Sürekli bakım programı oluşturulması,
- Depolama tesisi araçlarının düzenli bakımlarının yapılması gereklidir.

Sistemin belirtilen çerçevelerde düzenli bakımlarının yapılması e-belge yönetim sisteminin işlerliği ve devamlılığı açısından büyük önem taşımaktadır. Bu düzenli bakımlar, oluşabilecek donanımsal ve yazılımsal hataların önceden belirlenip önlem alınmasını sağlayacaktır. Bu önlemler sayesinde acil durumların oluşması asgariye indirilecek, bir bakıma erken uyarı vazifesi görerek muhtemel felaket durumları önlenmiş olacaktır.

5. BÖLÜM
ELEKTRONİK BELGELERE ERİŞİM

5.1. Erişim Sistemi

Elektronik belge erişim sitemi geliştirirken, temel bilgi erişim sistemleri göz önünde bulundurulmalıdır. Bilgi erişim, bilgi toplama, sınıflama, kataloglama, depolama, büyük miktardaki verilerden arama yapma ve bu verilerden istenen bilgiyi gösterme teknik ve süreci olarak tanımlanmaktadır (Tonta, 2001:200). Bilgi sistemleri genel olarak, bilginin tutarlı ve güvenli bir şekilde saklanıp, kolayca ve hızlı bir şekilde erişilmesi amacıyla geliştirilmiş sistemlerdir. Bilgi sistemlerine, veri tabanı sistemleri, uzman sistemler, soru yanıtlama sistemleri ve coğrafi ve kentsel bilgi sistemleri örnek olarak gösterilebilir. Elektronik belgelere erişim sisteminde bu temel yaklaşım çerçevesinde yürütülmesi gerekmektedir. Bu çerçevede, elektronik belge erişim sisteminin kullanımı kolay olmalı, kullanıcı bilgi ihtiyaçlarını etkin bir şekilde ifade edebilmeli ve sistem tarafından çıktı olarak ortaya konan arama sonuçları anlaşılır olmalıdır. Ayrıca, sistemdeki kullanıcı ara yüzleri yapılacak işlemleri kolaylaştıracak yapıda olmalıdır. Sistemde elektronik belgeler güvenli bir şekilde muhafaza edilmeli, belgenin gerçekliğini ve bütünlüğünü tehlikeye sokabilecek güvenlik zaaflarıyla ilgili önlemler alınmalıdır. Ayrıca belge erişim sistemi, hız bakımından yani kullanıcının bilgi ihtiyaçlarına verdiği cevap ve cevabın nitelik açısından etkinliğini sağlayacak şekilde oluşturulmalıdır.

Erişim sisteminde elektronik belgenin içeriğini yansıtmak amacıyla belirteç kümeleri kullanılmalıdır. İçerik belirteçleri, anahtar kelime ve dizin terimleri olarak adlandırılır. Arşivlenen elektronik belgelere etkin erişim sağlamak için dizinleme işleminin sağlıklı bir şekilde gerçekleştirilmesi gerekmektedir. Dizinleme işlemi insan eliyle yapılabileceği gibi, bilgisayar tarafından otomatik olarak da yapılabilmektedir. Ancak dizin terimleri açısından geniş bir çeşitlilik arz eden otomatik dizinleme işleminin yanında, ihtiyaçlar belirlenerek kontrollü dizinleme işlemi yapılması da sağlanmalıdır. Zira kontrollü dizinleme işlemi konu uzmanlarınca yapılması gerekir ve böylece dizinlerde belgenin anlamsal olarak yansıması sağlanır. Bu konuda gösterilecek hassasiyet erişim performansını doğrudan etkilemektedir.

Erişim sisteminde, önemli hususlardan biri gömü (Thesaurus)'nün kullanılmasıdır. Gömü, erişim sistemlerinde dizinleme ve erişim sırasında kullanılan ve seçilen terimlerin belli bir mantığa göre ilişkisini gösteren yapıdır (Srinisava, 1992). Bu yapı sayesinde, girilen sorgunu, bilgi ihtiyacıyla ilgili terimlerle genişletilip erişim performansı arttırılmış olacaktır. Gömüde bulunan kavramlar, belirli bir anlamsal ya da istatistiksel ilişkiye göre sınıflanır.

Bilgi erişim sistemlerinde kullanılan ve Teufel (2004:10) tarafından ortaya konulan arama metot ve modelleri, elektronik belge erişim sistemi bağlamında aşağıda değerlendirilmiştir;

- *Boolean arama:* Burada ikili karar söz konusudur. Yani bulunan belge ilgili mi değil mi ortaya konur. Ayrıca, terimlerin kesinliği eşleşme için gerekli ve yeterlidir. Aranan e-belgeyi bulmak için kullanılan bul operatörleri "ve", "veya", "değil" gibi operatörlerdir. Boolean model kesin eşleştirme yaklaşımına dayanmaktadır. Boole modelinde, belgeler sistemde dizin terimleri ya da anahtar kelime kümeleriyle tanımlanır ve kullanıcının bilgi ihtiyacı dizin terimlerinin boole kombinasyonu şeklinde sisteme sunulur. Belgelere erişim, sistemde ek olarak oluşturulan ve dizin terimlerinin hangi belgelerde geçtiğini gösteren devrin dizin üzerinde gerçekleşir. (Eroğlu, 2000:22). Bir belgenin sorguya bağlı olarak seçilebilmesi için "ve" operatörü ile bağlanan tüm terimleri içermesi gereklidir. "Veya", iki terim arasında eş anlamlılık ilişkisini kurar. Sorgu sonuçlarının aranılan terimlerin sadece birini içermesi yeterlidir. Değil operatörü ise kısıtlama amacıyla kullanılır. Boole'nin genişletilmiş bir modeli de bulunmaktadır. Bu genişletilmiş modelde, boole modelinin sorgu işleme sistemi ile vektör uzay modelinin işletimsel sistemi arasında yer alan bir modeldir. Burada sorgu yapısı korunurken aynı zamanda hem sorgu ve hem de belge terimleri ağırlıklandırılmaktadır (Eroğlu, 2000:38).
- *Vektör Uzay Modeli:* Geliştirilen çeşitli bilgi erişim modelleri içinde, sorguları ve belgeleri oluşturan terimleri ağırlıklandırılarak kullanan ve sorgu ve belgeleri birer terim vektörü biçiminde ele alan bu model kullanımı en kolay modeldir. Boole erişim modelinde terimleri ağırlıklandırmak için kullanılan değerler, bu modelde o belge için önemini gösteren sayısal bir değerdir (Eroğlu, 2000:29),
- *Sıralı Algoritmalar:* Sıralama terimin e-belgede geçme sıklık derecesi hesaba katılır. Belgede geçen bütün ilgili terimler aranmaz.

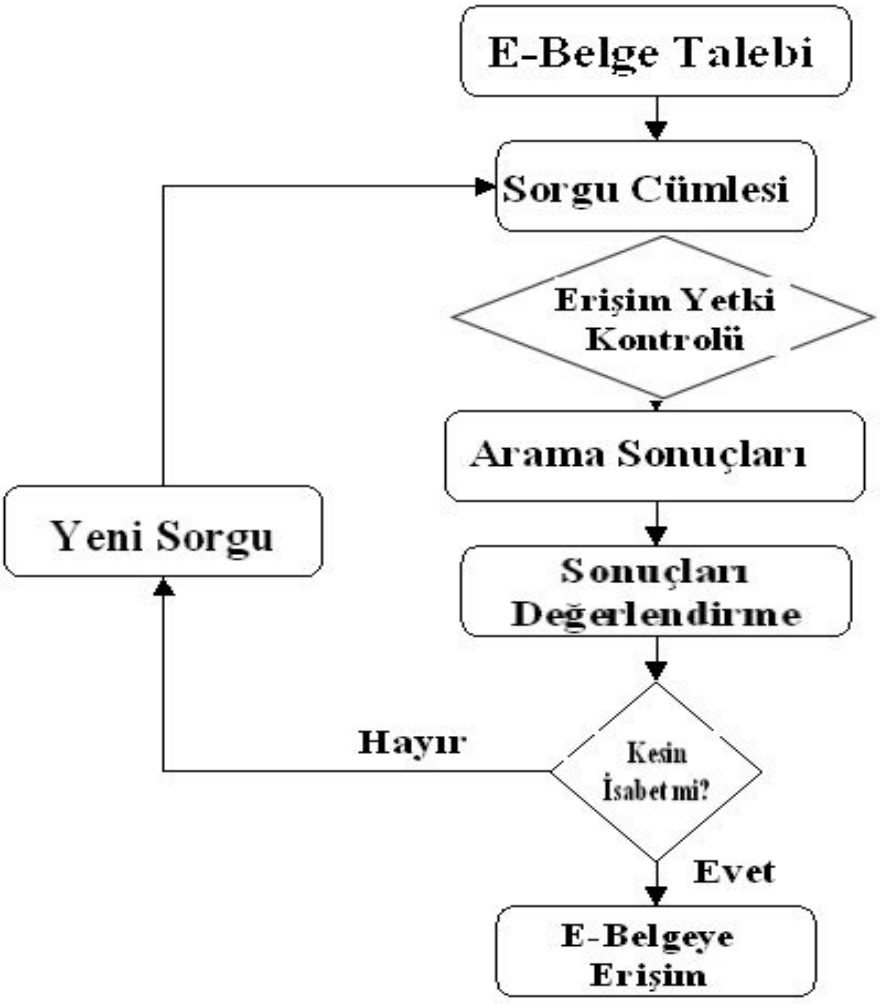
Aranılan elektronik belgeyi bulmada vektörel model yaklaşımı önemlidir. Bu modelde e-belge geniş bir tabanda alanda bir nokta olarak sunulmaktadır. Sorgu geniş bir alanı kapsamaktadır. Yüksek oranda benzerlik gösteren belgelerin seçimi yapılmaktadır. Üç boyutlu vektör alanında, birinci boyut bilgi, ikinci boyut erişim ve üçüncü boyut sistemdir (Teufel, 2004:12). Bu aşama da verilecek karar, vektörün boyutunun seçimidir. Eşleştirilen her bir terim için ağırlığın belirlemesi gereklidir. Bu bağlamda, mevcudiyet ya da yokluk terimlerin belgede geçme sıklığı gibi hususlar değerlendirilmelidir. Ayrıca yakınlık ölçümü de seçilmelidir. Yakınlık, benzerlik ya da farklılıklarla tanımlanabilir. Seçilmiş elektronik belgelere erişmek için, yazılım uygulamaları veriyi aramak için ya veri tabanı yönetim sistemindeki anahtar alanlardan ya da tam metin erişim sistemindeki kelime sıradüzeninden birine başvurur (Calrim, 2002:20).

Elektronik belge erişim sisteminin temel işlevi, bilgi ihtiyaçlarını karşılaması muhtemel ilgili belgelerin tümüne erişmek, ilgili olmayanları da ayıklamak olarak tanımlanabilir. Bu bağlamda bir erişim sisteminin bazı belgelere erişim sağlayabilmesi için aşağıda sıralanan iki koşul yerine getirilmelidir (Tonta, 2002:7);

- Eklenen her belgenin temel özellikleri geleneksel veya otomatik olarak gerçekleştirilen dizinleme işlemleri sırasında belirlenmeli ve her belge için ilgili içerik belirteçleri (dizin terimleri) oluşturulmalıdır. Bir belge için oluşturulan söz konusu içerik belirteçleri bilgi erişim sırasında belgenin tamamını temsil etmek üzere (surrogates) kullanılır.
- Kullanıcılar belgelere verilen bu içerik belirteçlerini doğru olarak tahmin edip sorgu cümlelerini ona göre oluşturmalıdırlar. Bir başka deyişle, kullanıcının bilgi ihtiyacını ifade etmek için kullandığı terimlerle belgeyi temsil eden içerik belirteçleri birbiriyle karşılaştırılır ve çakışan belgelere erişilir.

Elektronik belge erişim sisteminde ilgili belgelerin tümüne ya da sadece aranan e-belgeye erişim sağlanmalıdır. Bu bağlamda erişim kurallarından biri olan çakışma önemli bir yere sahiptir. Maron'un (1984: 155) açıkladığı bu kural elektronik belge açısından tekrar ifade edilecek olursa:"Herhangi bir resmi sorgu cümlesi için bu arama sorgusunda belirlenen belgelerin alt serisinde yer alan belgelerin tümüne ve salt bu serideki belgelere erişim sağlar. Böylece aranan belgeye, sorgu cümlesinde yazılan kavram ya da kavramlar sistem içindeki bütün ilgili terim ve belgeler karşılaştırılarak ulaşılacaktır. Burada ilgili belgelerde kast edilen

aralarından arşivsel ilgi ya da bağ bulunan bütün belgelere erişimin sağlanmasıdır. Bu e-belgeler arasından gerekli eleme işlemi, yapılacak süzme işlemiyle gerçekleştirilecektir. Sisteme eklenen bir e-belge içeriğinin otomatik olarak dizinlenebilmesi gerekmektedir. Bu belgeye erişim açısından büyük önem taşımaktadır. Sistem e-belge ile ilgili, üretim tarihi, üreten, belgenin biçimi, türü gibi bilgilere göre de aramaya imkân vermelidir. Şekil 8'de e-belge erişim sistemi için örnek bir mantıksal düzen gösterilmiştir.



Şekil 8. E-Belge Erişim Sistemi Mantıksal Düzeni

Bu düzende, elektronik belgeye erişimle ilgili süreç şöyle işlemektedir. Öncelikle kurumsal ya da kişisel olarak bir elektronik belge talebinin gerçekleşmesi gerekir. Bu talebin yasal ve idari hususlar çerçevesinde gerçekleşmesi önemlidir. Eğer elektronik belgenin sayısı ya da arşiv numarası belli ise erişim hızlı ve kolay olacaktır. Ancak burada sistem aranılan elektronik belgeye erişim hakkı ya da yetkisi olup olmadığını mutlaka kontrol etmektedir. Eğer erişim yetkisi olmayan bir belgeye erişim çabası söz konusu ise sistem bununla ilgili uyarı mesajını verecektir. Eğer aranılan belge ile ilgili tanımlayıcı çok fazla bir bilgi yok ise. O zaman bilinen hususlar çerçevesinde bir sorgu cümlesi oluşturulur, bu sorgu cümlesi belli bir tarih aralığı için sınırlandırılır. Sorgu cümlesi erişim yetkisi kontrolünden geçer ve arama sonuçlarına ulaşılır. Arama sonuçları üzerinde bir değerlendirme faaliyeti gerçekleştirilerek aranılan belgeye erişimde kesin isabet sağlanıp sağlanmadığı değerlendirilir. Eğer kesin isabet varsa aranılan elektronik belgeye erişim sağlanmış demektir. Eğer kesin isabet sağlanmamışsa, oluşturulacak yeni sorgu cümlesi ve ilgili sınırlamalarla aranılan elektronik belgeye erişim çabası devam eder. Ortaya konulan bu mantıksal düzen erişim açısından bir sürecin işleyişini ortaya koymaktadır.

Erişim sistemi, hem aramaya ve hem de dosya ve belgelerin görüntülenmesini desteklemelidir. Erişim sistemi en azından belge içinde bulunan üst verinin aranabilmesini desteklemesi gereklidir. Bununla birlikte belge içeriklerinde tam metin olarak da arama yapabilmesinin sağlanması büyük önem taşımaktadır. Sistem boolean mantığında arama yapılabilmesi özelliğine sahip olmalıdır. Ayrıca, sistem üst veri alanlarında göre sonuçların sınıflandırılmasına imkân vermesi gereklidir. Belgede kayıtlı bulunan bağlamsal bilgi anlamında elektronik belgelerin birbiriyle ilişkilendirilmesini desteklemesini sağlamalıdır. Sistem, araştırma araçlarından belgelere göz atmaya ve belge, dosya, seriler ve birim sıradüzeni vasıtasıyla göz atmayı desteklemelidir (Public Records Office of Victoria, 2000:9).

Elektronik belgelere erişimin sağlanmasında anahtar alan metodu ya da tam metin erişim metotları kullanılmalıdır. Erişim sisteminde, anahtar alan metodu belgenin başlığı gibi belirli veri alanlarının seçilmesidir. Veri sisteme yüklendiği zaman, yazılım anahtar tablolar ve dosyalar oluşturur. Bunlar depolama aracında aranan verinin nerde yerleştirildiğini ilişkin çapraz başvurular içerir. Belirli miktarında veri talebi almada, yazılım, eşleşme olup olmadığını belirlemek için anahtar tablolarda bulunan verilerle talebi karşılaştırır (Calrim, 2002:20). Tam metin erişim metodunda bütün kelimeler indekslenir. Tam metin metodu

kullanıcın istediğini bulması için, belgenin bütün içeriğinde arama yapmaya imkân tanır. Burada metin içinde geçen bütün içerik indekslenerek erişim açısından daha detaylı bir arama imkânı sağlanmış olur. Metot seçimi kurumsal yapı ve verinin kullanımına göre değişmektedir.

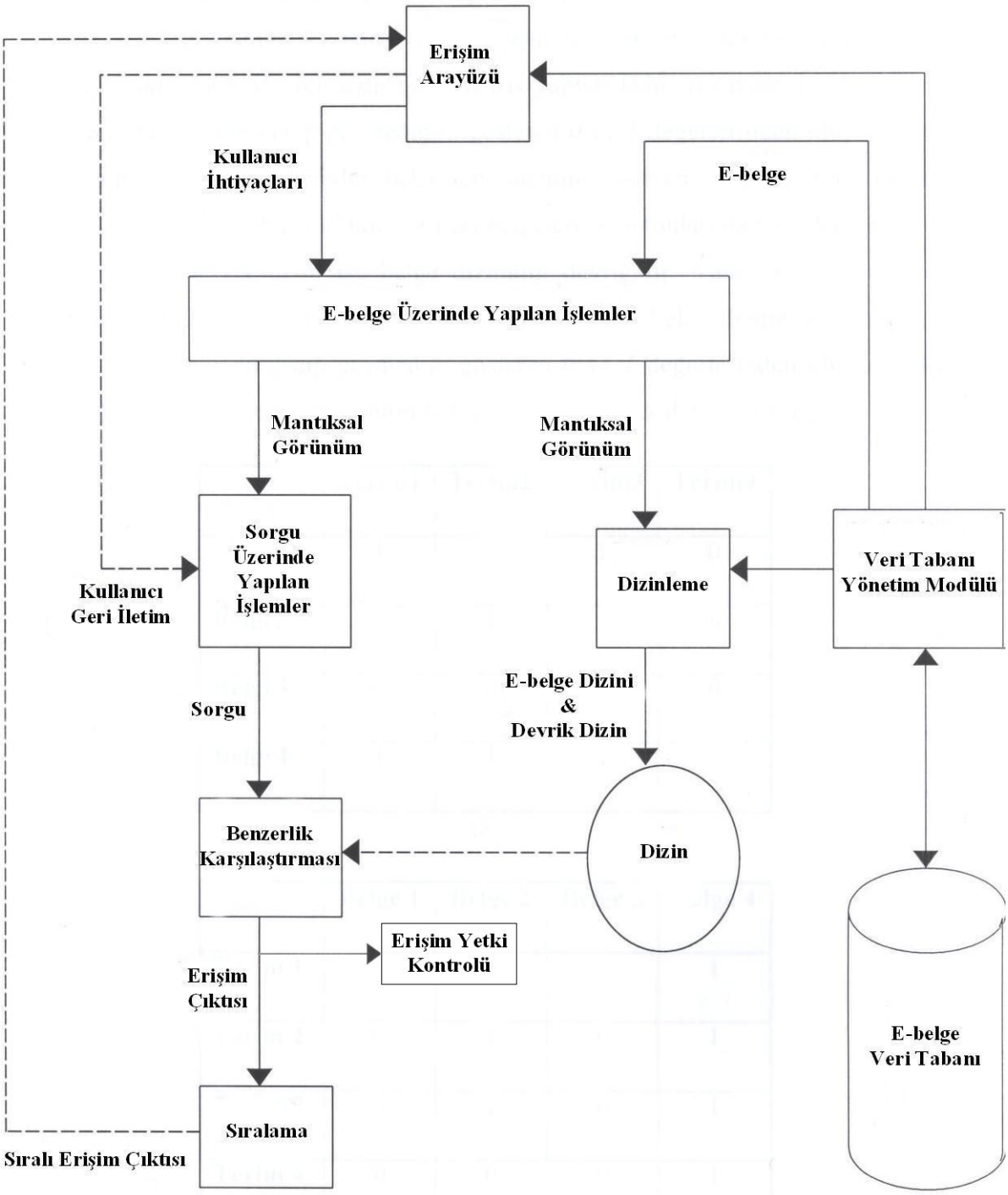
E-belge erişim sisteminde, veri kümelerinde anahtar olarak belirlenen özellikler kayıtlara ulaşmamızı sağlar. Anahtar değerler tek kaydı sorgulayabileceği gibi birden fazla kaydı da sorgulamak için kullanılabilir. Tek kaydı bulmak için kullanılan anahtar asal anahtar, bu sorgulamaya adres sorgulamada denir. Birden fazla kaydı bulmak için yapılan sorgulamaya ikincil anahtar kullanılarak yapılan sorgulama ya da içerik kullanılarak yapılan sorgulama denir. İkincil anahtar kullanılarak yapılacak sorgulamada birden fazla kayıt bulunabilir. Ancak, asal anahtar kullanılarak yapılacak sorgulamada tek kayıt bulunacaktır (Kurnaz, 2008:269). Örneğin bir e-belge yönetim sistemi içinde imha edilen e-belgeler arama açısından değerlendirilirse. İmha edilen belge ile ilgili üretim, imha, ait olduğu seri birçok bilgi kaydedilmektedir. İmha tarihi kullanılarak yapılacak sorgulamada birden çok e-belgenin imha detaylarına ulaşılacaktır. Çünkü sorgulama yapılan tarihte birçok e-belge imha edilmiştir. Ancak e-belge ile ilgili bütün özellikler kullanılarak bir sorgulama yapıldığında tek bir e-belge bulunacaktır.

Oluşturulacak sistemde arama yöntemlerinin performansı çok önemlidir. Buradaki amaç aranılan bilgi ya da e-belgeye ulaşmak için geçen süreyi olabildiğince azaltmaktır. Temelde iki arama yöntemi bulunmaktadır. Bunlar doğrusal arama yöntemi ve ikili arama yöntemidir. Doğrusal arama yönteminde, veri kümesinde bulunan bilgi fiziksel sıralarından okunur ve aranılanın bulunmasına çalışılır. Aranan bilgi oluşturulan yapının bütününde aranır. İkili arama yönteminde ise aranan bilginin yeri konusunda herhangi bir öngörü yapılmaması nedeniyle kullanımı çok etkin değildir. Bu arama yönteminde veri kümesinin küçük elemandan büyük elemana doğru sıralı olması gerekmektedir (Kurnaz, 2008:239).

Arşivlenen elektronik belgelere nasıl ulaşılacağı ve kullanıcıların isteği doğrultusunda nasıl işleneceği erişim sistemi açısından önemli bir konudur. Erişim açısından değerlendirildiğinde başlıca veri kümesi yapıları (Kurnaz, 2008:270) aşağıda değerlendirilmiştir;

- *Ardışık Veri Kümesi:* Kayıtları ard arda saklayan veri kümesidir. Bu yapı, manyetik teyp biriminin kullanımına en uygun yapıdır. Bu yapıda herhangi bir kayda ulaşılmak istendiğinde o kayıttan önceki kayıtların her birinin okunması gereklidir. Üzerinde çok sık işlem yapılmayan uzun dönem arşivlenmiş e-belgeler bu veri yapısında ve manyetik teyp depolama ortamlarında saklanmalıdır.
- *İndekslenmiş Ardışık Veri Kümesi:* Kullanıcıların daha kısa sürede daha çok ve daha etkin işlem yapmasını sağlayan yapılardır. Bu yapıda kayıtlar anahtar değerlerine göre sıralı olarak bulunur.
- *Doğrudan Erişimli Veri Kümesi:* Bu yapıda doğrudan adresleme yöntemi kullanılır. Bu sayede, bir kaydın anahtarına veya harici bir tanımlayıcının değerine göre uygun disk adresinin belirlenmesi sağlanmış olacaktır. Ancak, kayıt anahtarı dahili disk adresi tanımlayıcısı olarak kullanıldığı için anahtar sahalarının formatı ve sayısal değerlerinin aralığının mevcut disk adresiyle aynı olmak zorunda olması sebebiyle kullanımı zor bir yöntemdir. Bir kaydın adresinin değiştirilmesi veya bir kayıt ilave etmek, çıkarmak oldukça zor olup bellek sahasının kötü kullanılmasına sebep olabilir (Kurnaz, 2008:299). Bu yöntemde kayıtların anahtar değerlerinin bir dönüştürme yöntemi ile bilgisayarın bellek adresine çevrilmesi gereklidir. Burada amaç, istenen belgeye doğrudan erişimin sağlanmasıdır.

Erişim sistemi model çerçevesinde oluşturulmalı, etkinliğinin sağlanması için gerekli bütün bileşenler ortaya konmalıdır. Eroğlu (2000:15) 'nun bilgi erişim sistemi genel modeli olarak ortaya koyduğu yaklaşım, elektronik belge erişim sistemi açısından değerlendirilerek elektronik belge erişim sistemi modeli olarak Şekil 9'da gösterilmiştir.



Şekil 9. E-Belge Erişim Sistemi Modeli

Bu erişim sistemi modeli uygulanabilir bir model olarak göz önünde bulundurulmalıdır. Bu modelde öncelikle erişim faaliyetlerinin gerçekleştirileceği bir erişim ara yüzü bulunmaktadır. Bu ara yüzde erişim faaliyetini gerçekleştirmeyi sağlayan unsurlar bulunur. Bu erişim ara yüzünün arka planında esas işlemleri gerçekleştiren mekanizma

bulunmaktadır. Bu mekanizmanın temel ayaklarını elektronik belgelerin bulunduğu veri tabanı ve bu veri tabanında işlemler yapmamızı sağlayan bir veri tabanı yönetim modülü oluşturmaktadır. Veri tabanı yönetim modülüne bağlı olarak çalışan ve elektronik belgeye etkin erişimi sağlayan bir dizinleme faaliyeti gerçekleşir. Bu dizinleme faaliyeti sonucunda bir e-belge dizini oluşur. Bu kısım elektronik belgelere erişimin olmasına imkân veren yapıdır. Erişimi sistemi modelinin diğer kısmı ise kullanıcı ihtiyaçlarının karşılanmasıyla ilgili işlemlerin bulunduğu kısımdır. Burada erişim ara yüzünden kullanıcı ihtiyaçları çerçevesinde sorgular gerçekleşir ve bu sorgulara paralel geri bildirimler elde edilir. Kullanıcı ihtiyaçları çerçevesinde gerçekleştirilen sorgular oluşturulan e-belge dizinlerinde benzerlik karşılaştırması yapılmak suretiyle erişim çıktısı şeklinde ortaya çıkar. Bu erişim çıktısı erişim kontrol yetkisi çerçevesinde oluşur. Kullanıcının oluşturduğu sorgu tamamen erişim yetkileri çerçevesinde sonuçlanır. Erişim çıktıları daha önce tanımlanan, tarihine göre ya da alfabetik olarak sıralanarak sıralı bir erişim çıktısı halini alır. Bu erişim çıktısı kullanıcı ara yüzüne yansır. Bu model kendi içinde etkileşimli ve sistemin işleyişini sürekli iyileştirme temel yaklaşımı çerçevesinde oluşturulmuştur. Kullanıcıların geri bildirimleri çerçevesinde sistemin daha etkin çalışması için gerekli düzeltmeler ya da eklemeler yapılabilmektedir.

5.2. Erişim Kontrolü ve Güvenliği

Erişim kontrolü ve güvenliği sistemin sağlıklı işlemesi ve elektronik belgenin güvenliği ve bütünlülüğün korunması açısından büyük önem taşımaktadır. Elektronik belgelerin erişim açısından güvenliğini sağlamak için birçok teknik ve yaklaşım bulunmaktadır. İdeal bir seviyede güvenliği sağlamak için; gizlilik, bütünlük ve erişebilirlik temel prensip olmakla birlikte, erişim bağlamında e-belgelerin bulunduğu ortamlarla ilgili olarak kimlik kanıtlama veya doğrulama, inkâr edememe, fiziksel güvenlik, insan faktörü, güvenlik duvarları, anti-casus ve anti-virüs yazılımlar, atak tespit sistemleri, sayısal imza, şifreleme ve açık anahtar gibi çözümlerin kullanılması gerekmektedir (Sağıroğlu, 2007:14). Erişim güvenliğinin sağlanması açısından, sistemi kullanan her kullanıcıyla en az hak verme yaklaşımı benimsenmelidir. Bir kullanıcıya, bu seviyede hak vermenin karşılaşılabilecek problemleri azaltacağı göz önünde bulundurulması gereken önemli bir gerçektir. Ayrıca sistemin bağımsız kuruluşlarca içten ve dıştan sızma testleri yaptırılmalı ve güvenlik açıkları giderilmelidir. Bu çerçevede tanıma ve doğrulamanın işlemlerinin yapılması gereklidir. Bu işlemler, yetkisizi kişilerin sisteme girmesini engellemeye yönelik olarak tasarlanmış teknik

tedbirlerdir. Bunlar yalnızca ağ üzerindeki işlemlerde önemli değildir, aynı zamanda sistemin yönetiminde ve elektronik belgelerin güvenliğinin sağlanmasında da önemlidir. Sistem, kişileri kullanıcı adlarını ayırt edebilmeli ve her bir işlemlerin ilgili kullanıcıyla bağlantısını yapabilmelidir. Tanıma, sadece halen yetkilendirilmiş kullanıcılara ait olmalıdır. Doğrulama, kullanıcıların kimliklerinin gerçekliğinin sağlanmasıyla ilgili araçlardır. Tanıma ve doğrulama işlemleri sistemin güvenliği açısından çok önemlidir.

5.2.1. Erişim Kontrol Mekanizmaları

Erişim sistemine girişlerin belirli yapılar çerçevesinde kontrolünün sağlanması sistemin bütünün güvenliği açısından büyük önem taşımaktadır. Sisteme girişlerin yetkiler çerçevesinde oluşturulan kimlik doğrulamaları vasıtasıyla yapılması gereklidir. Bu sayede yetkisiz erişimler engellenerek elektronik belgelere erişim kontrol atına alınmış olur. Bu bağlamda kullanıcıların kimliklerini doğrulamaya yönelik tek başına ya da birlikte kullanılabilen üç araç bulunmaktadır (NECCC E-sin Policy Workgroup, 2001:15);

- *Sadece kişinin bildiği bir şey olan araçlar:* Bunlar oldukça gizlidir. Bu şifre, kişisel kimlik numarası ya da şifreleme anahtarı olabilmektedir. Şifrenin unutulması ya da başkası tarafından öğrenilme durumu en önemli zayıf yönüdür.
- *Kişinin sahip olduğu bir şey olan araçlar:* Bu bir atm ya da akıllı kart olabilmektedir. Kullanılan cihazın bozulması ya da kaybolması durumu en önemli zayıf yönüdür.
- *Kişinin kendisinden olan araçlar:* Bu bir biyometriktir. Biyometrik, kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimidir. Bu, kişinin sesi ya da parmak izi olabilmektedir. Parmak izi, ses, yüz ve retina gibi her insanda ayrı özellikler taşıyan fiziksel verileri elektronik tabanlı ortamlarda toplayıp sınıflandırmasıdır. Özel yazılımlar, kendiliğinden alınan biyometrik veriyi, hızlı bir şekilde veri tabanındaki verilerle karşılaştırıp, aranan kimliğin tespitine imkân vermektedir. Henüz Türkiye'de ve dünyada çok yaygın bulunmayan özel cihaz ve yazılımlar gerektiren bu yöntem kesin sonuçlar elde edilmesini sağladığı için elektronik belgelerin erişim kontrolü ve güvenliğinde önemli bir çözüm sunmaktadır. Kullanıcının biyolojik özelliğinin yanlış algılanması en zayıf yönüdür.

Bu araç ya da yöntemlerden yalnızca birinin kullanılması durumunda zayıf kimlik doğrulama gerçekleşir. Eğer bu yöntemlerden iki ya da daha fazlası kullanılırsa güçlü kimlik doğrulama gerçekleştirilmiş olur. Parola ile akıllı kart ya da jeton ve parmak izinin aynı anda kullanılması güçlü kimlik doğrulamaya örnek olarak gösterilebilir. Zayıf kimlik doğrulama yöntemi olan parolanın kullanılması, en çok istismar edilen ve güvenlik boşluk yaratan bir yöntemdir. Zira kolay hatırlamak için zayıf parolaların belirlenmesi önemli bir güvenlik sorunu yaratır. Bu yüzden parolalar belli kurallara dayalı olarak karmaşık bir yapıda belirlenmelidir. Ayrıca parolaların belirli zaman aralıklarında değiştirilmesi mutlaka sağlanmalıdır. Yukarıda belirtilen biyometrik araçlar elektronik belge depolama araçları ve sunucularının bulunduğu fiziksel alana girmede kullanılabilecek yöntemlerdir. Sistemin sadece bilgi teknolojileri bağlamında güvenliğini sağlamak yeterli değildir, aynı zamanda sistemin bağlı çalıştığı donanımların bulunduğu alana erişimlerinin de biyometrik araçlarla kontrolü büyük önem taşımaktadır. Dolayısıyla sisteme erişimle ilgili fiziksel ve teknolojik tehditlerin bir bütün içinde önlenmesi sağlanmış olacaktır.

Erişimim güvenliği açısından mantıksal erişim kontrolünün sağlanması da büyük önem taşımaktadır. Erişim, bilgisayar araçlarıyla bir şeyler yapabilmektir. Mantıksal erişim kontrolü, bazı yollardan erişimin açıkça sağlandığı ya da kısıtlandığı sistem tabanlı araçlardır. Bunlar, belli sistem araçlarına kimin erişimin olabileceğini ve izin verilen erişim türünü saptayabilir. Genelde, kurumlar erişim kontrol politikalarını en düşük erişim hakkı prensibi üzerinde temellendirmelidir. En düşük erişim hakkı, kullanıcıların yalnızca resmi görevlerini yerine getirmek için sisteme erişimlerini sağlamayı ifade eder. Örneğin, veri giriş elemanları veri tabanlarının analiz raporlarını çıkarmaya ihtiyaç duymamalıdır. Kurumlar, aşağıdaki erişim kriterleri (NECCC E-sign Policy Workgroup, 2001:15) çerçevesinde kaynaklara erişimi kontrol etmelidir. Belirtilen erişim kriterleri iç erişim mekanizmasının unsurlarıdır. Bu unsuların etkin olarak gerçekleştirilmesi iç erişim mekanizmasının sağlıklı ve güvenli bir şekilde işlemesini sağlar. Bu açıdan NECCC (2001:15) tarafından ortaya konulan erişime ilişkin hususlar aşağıdaki değerlendirmeler çerçevesinde önemle göz önünde bulundurulması gerekmektedir.

- *Kimlik (kullanıcı adı):* Kişinin sisteme erişmesini sağlamak ve kişisel sorumluluğu desteklemek için verilir. Sisteme kullanıcı adı ve buna bağlı şifresi olmayan kimsenin girememesidir.

- *Görevler:* Kişinin sistem içinde görevleri çerçevesinde verilen yetkileri ifade eder. Yani, kişilere verilen işler ya da yerine getirilen fonksiyonları belirtir. Belirlenen yetki ve sorumluluklar dışında erişim gerçekleşmemelidir.
- *Yer:* Erişim sağlanan sistemin donanımsal unsurlarının bulunduğu mekândır. Bir başka ifade ile fiziksel ya da kurumsal birimdir. Bu birime giriş çıkışlar kontrol edilmelidir.
- *Zaman:* Erişimin kısıtlandığı gün ya da zamanla ilgili hususlar. Örneğin, gizli kişi dosyalarının kullanımına yalnızca normal çalışma saatlerinde izin verilebilir. Böylece resmi çalışma saatleri dışında sistem erişim engellenmiş olur.
- *İşlem:* İşlem tamamlandığı zaman erişim yetkisinin bitmesidir. Örneğin; vaka dosyalarına erişime yalnız işlem sırasında izin verilebilir. Erişim yetkilerinin sadece işlem sırasında olması, yetkisiz erişim açısından önemli bir kontrol sağlar.

Dış erişim kontrol mekanizmasını oluşturulması da önemlidir. Sitemle dış kullanıcılar, servisler ve sistemler arasındaki etkileşimi kontrol araçları vardır. Erişim kontrolleri kurulacağı zaman, kurumların aşağıdaki mekanizmaları düşünmeleri gerekir (NECCC E-sign Policy Workgroup, 2001:15). Bu mekanizmalar sayesinde sisteme kurum dışından gelebilecek tehditler önlenebilecektir. Bunlar birbirlerini tamlayan unsurlar olarak ele alınması gereklidir.

- *Şifreleme:* Şifrelenmiş bilgiler, uygun şifreleme ile ilgi anahtara sahip olan kişi tarafından okunur ve şifresi çözülebilir.
- *Güvenli ağ geçidi ve ateş duvarları:* İki ağ arasında güvenli ağ geçidi blokları ya da filtreleri, genelde iki özel ağda ya da daha büyüğünde, internet gibi daha kamuya açık ağlar. Güvenli ağ geçitleri, iç sistemi korurken, iç kullanıcıların dış ağlara bağlanmalarına izin verir. Ağ güvenliği, doğrudan sistemin kendisine veya sahip olunan kaynaklara yetkisiz ve kötü amaçlı erişimleri engellemek ve veri aktarımı sırasında mahremiyeti sağlar (Çölkesen, 2008:317). Ayrıca, veri bütünlüğü ve doğrulama gibi gereksinimleri sağlama hususuyla da ilgilidir. Güvenlik duvarı, genel olarak bir yerel ağ içerisinde erişimleri denetlemek için kullanılır. Ancak, oluşturulacak bu denetimde elektronik belge yönetim sistemine erişimle ilgili özel yetkilendirme ve kısıtlamaların yapılması gerekmektedir.
- *Ana bilgisayar tabanlı(host-base) onaylama:* Ana bilgisayar tabanlı onaylama, istekte bulunan kullanıcının kimliği yerine, istekte bulunan bilgisayarın kimliğine dayalı

Belirtilen bütün hususlar çerçevesinde erişim kontrol mekanizmalarının etkin kullanılması sisteme yetkisiz girişleri engelleyeceği gibi, elektronik belgelerin gerçekliğini ve bütünlüğünün sağlanmasını da destekleyecektir. Bu açıdan bütün detaylarıyla sisteme uygulanmalıdır.

5.2.2. Kontrol ve Güvenliğe İlişkin Tehdit ve Tedbirler

Elektronik belge erişim sisteminin güvenli bir yapı içinde belli kurallar çerçevesinde kontrollü olarak gerçekleştirilmesi gerekmektedir. Kurum içinde ve dışından olabilecek tehditler her zaman göz önünde bulundurulmalıdır. Bilgi teknolojilerindeki gelişmelere paralel olarak tehdit türlerinde azalma beklenirken, aksine artışlar görülmektedir. Bu açıdan, erişimle ilgili tehditler tespit edilmeli ve buna yönelik çözüm önerileri geliştirilmelidir. Tehditleri en aza indirgemek için erişim kontrol mekanizmalarının etkin kullanılmaması gerekmektedir. Sağıroğlu (2007:40) tarafından ortaya konulan temel tehdit türleri elektronik belge yönetim sistemi açısından aşağıda değerlendirilmiştir;

- *İzinsiz erişim:* Pasif atak olarak da bilinen izinsiz erişim en tehlikeli tehditlerin başında gelmektedir. Bu açıdan elektronik belge yönetim sistemi bu tür erişim risklerine karşı korunaklı olması gerekmektedir.
- *Zarar Verme:* Aktif atak tiplerindendir. Karşılıklı veya tek taraflı olarak haberleşmeyi engelleme ve zarar verme, bu yaklaşımda karşılaşılan tehditlerdir. Bu tür tehditte, üretilen elektronik belgenin kullanılmaz hale gelmesi ya da değiştirilmesi mümkün olabilmektedir.
- *Değişiklik Yapma:* Bu işlemde göndericiden gönderilen bilgiler veya göndericinin bilgisayar sistemindeki bilgiler saldırgan tarafından elde edilip değiştirilebilir. Bu tehdit türünde, elektronik belgelerin bağlı olduğu yazılım ve bununla ilişkili program kodları değiştirilebilir.
- *Üretim:* Bu işlemde, saldırgan üretmiş veya oluşturmuş olduğu mesajı ya da dokümanı, alıcıya göndericiden mesaj geliyormuş gibi karşı tarafa gönderir. Bu

Yukarıda belirtilen teknolojik tehditler dışında fiziksel depolama araçlarının bulunduğu alana ilişkin yetkisiz erişim riskleri de göz önünde bulundurulmalıdır. Sistemin çalıştığı donanım araçlarına ya da sunuculara fiziksel olarak da zarar verilme riski bulunmaktadır. Bu tehdit sonucunda oluşabilecek fiziksel zararlar diğerlerine göre geri dönüşü olmayacak daha büyük sonuçlara yol açabilmektedir. Bu açıdan fiziksel alana erişime ilişkin biyometrik araçlar mutlaka kullanılmalı ve erişim kontrol altına alınmalıdır.

Arşivleme sisteminin, arşivdeki belgelere erişim kontrolünü destekleyecek politikaları içermesi bir zorunluluktur. Asgari olarak, erişim kontrol politikalarının belgelere yetkisiz erişimi ya da erişim kontrol politikalarının değiştirilmesini önleyebilme kapasitesinde olması gereklidir. Bu asgari bir gerekliliktir. Ayrıca, kurumlar ihtiyaç duyacakları erişim kontrol politikalarını dikkatli bir biçimde düşünmelidirler. Korunması gereken belgelerin türü, kontrol edilecek erişim türleri ve yetkilendirilmiş ya da engellenmiş kullanıcı sınıflarının belirlenmesi gereklidir.

EBYS, e-belge üretimi, e-belgelerin sisteme aktarımı, belgelerin sistemden başka yere aktarılması, belgelerin imhasına karar verme de dahil olmak üzere belgeyi etkileyecek her türlü olayı kaydedebilmesi gereklidir. Bu işlem geçmiş raporu, belgelerin hatalı bir şekilde kasıtlı ya da kazara imhasının izlenebilmesine imkân verir. Denetim kayıtlarının değiştirilmesinin mümkün olmaması gereklidir, aksi taktirde geçmiş işlem raporlarına yönelik bir güven oluşmayabilmektedir (Public Records Office of Victoria, 2000:7). Eğer gerekliyse, e-belgelere yapılan bütün erişimlerin kaydedilebilmesi gereklidir. Kayıt defteri, hangi belgelere erişildiğini, belgeye erişen kullanıcının kimliğini ve erişim zamanını içermelidir. Bu işlem, e-belgelere yetkisiz erişimin tespit edilmesini sağlamada büyük öneme sahiptir.

Sistemin, dosyalar, elektronik belgeler, araştırma araçları, imha planları ve erişim kontrol politikaları dahil olma üzere arşivdeki bütün nesnelerin üzerinde erişim kontrolünü desteklemesi gereklidir. Erişim kontrol politikaları en azından, kişisel dosya ve belgelerin kullanıcılar tarafından erişilip okunmasına izin verebilmesi ya da engelleyebilmesi gerekmektedir. Elektronik belge koleksiyonuna erişimin kontrolü ya da belli kullanıcı gruplarını kısıtlama gibi daha karmaşık erişim kontrolü kurumsal yapılar içinde gerekebilir.

Kurumlar, istedikleri kontrol seviyelerine ulaşmak amacıyla en uygun maliyeti belirlemek için erişim kontrol politikalarını yönetmenin idari maliyetini dikkatli bir şekilde değerlendirmeleri gerekmektedir.

Kamu otoritesi, elektronik belgelere bütün erişimlerle ilgili belge bulma sistemi işlem lisesini isteyebilir. Belge erişim sırasında kaydı tutulan bilgiler; belgeyi isteyen kullanıcının kimliği, istenilen belge, erişime müsaade edilip edilmediği ve elektronik belgenin gönderildiği sistemim hangisi olduğunun içerir (Public Records Office of Victoria, 2000:8). Sistemin güvenliğine yönelik çözümler ile erişimin kontrol altında alınması ve kaydıyla ilgili hususlar değerlendirilmelidir. Bilgisayar sisteminde üretilen, depolanan ve kullanılan elektronik belgelerin güvenliği önemli bir konudur. Hangi formatta olursa olsun belgenin korunması sağlanmalıdır. Eğer veri kişisel ya da gizli ise bu daha da ilgili bir durumdur. Ana bilgisayar sistemleri geleneksel olarak korunurlar. Ancak diğer bilgisayarlar korunmaz, çünkü bunlar genellikle tek kullanıcılı araçlar olarak düşünülür (Calrim, 2002:22). Sonuç olarak, güvenlik zafiyetleri, elektronik belgenin gizliliğini, bütünlüğünü ve geçerliliğini tehdit edebilir. Elektronik belgeleri koruma işlemi, bilgisayar donanımının fiziksel güvenliği ve erişim kontrolü ile veri güvenliği sağlanarak gerçekleştirilebilir.

Güvenlik sistemlerinin potansiyel kayıpları önleyecek şekilde dizayn edilmesi gerekmektedir. Başarılı olmak için, bilgisayar güvenliğinin, devam eden bir yönetim ilgisi olması gerekmektedir. Nem, sıcaklık ve temizlik gibi çevresel şartların elektronik belge yönetimi ve bilgi işlem sistemi bileşenleri üzerindeki etkisi, elektronik olarak korunan belgelerdeki potansiyel değiştirme ve kayıplardan dolayı bir güvenlik sorunudur (Calrim, 2002:23). Büyük bilgisayarlarda çok miktarda hassas belgelerin büyük çapta elektronik belge yönetim sistemi içinde korunması, kapsamlı bir çevresel kontrol gerektirecektir. Küçük çapta, bilgisayarlardaki kritik olmayan sistem uygulamaları, muhtemelen daha düşük bir çevresel kontrol gerektirecektir. Buna rağmen, hassas elektronik araçlardan oluşan küçük sistemlere, güvenirliliğin sürekliği için en azından en düşük düzeyde bir çevresel kontrol sağlamak gerekir.

Elektronik belgeler, kâğıt belgelere oranla gelişi güzel erişim riskine karşı daha güvenlidir ve gelişen teknoloji, erişim için gerekli kimlik doğrulama konusunda yetkililerin güvenlik sorumluluklarını azaltacaktır (Oatway, 2004:2). Erişim kontrol mekanizması oluşturulacak sistem için en kritik ve gerekli bir yapı taşıdır. Erişim kontrolü, bilgi kaynağına

ulaşımla ilgili kontrol yollarını ifade eder. Belgelerin işlenmesi ve iletimi sırasında belgelerin bütünlüğü de dahil olmak üzere elektronik belgelerin güvenli iletimine yönelik tedbirler oluşturulmalıdır. Bu tedbirler, kullanılan teknolojiye, iş gerekliliklerine risk düzeyine bağlı olarak değişecektir. Buna yönelik uygulamalar şöyledir;

- *Açık şifreleme düzeni (PKI):* Yüksek riskli işlemler için çok güçlü bir şifreleme sağlar ve elektronik imza ile web tabanlı uygulamalarda daha çok kullanılan güvenli soket katmanı(SSL) gibi güvenli iletim tedbirlerini destekleyebilir. SSL kullanıcı ve sunucu arasında doğrulanmış ve şifrelenmiş güvenli bir aktarım yapılmasını sağlayan güvenlik protokol kümesidir (Çölkesen, 2008:322).
- *Tatlı mahremiyet(PGP):* Kamusal ağ üzerinde güvenli mesaj gönderme tekniğidir
- *Sanal özel ağ(VPN):* Bu yapı, kişiye ya da kuruma ait özel e-belge ya da verinin internet gibi kurumsal bir ağ üzerinden aktarılmasını sağlar (Çölkesen, 2008:326). Kurumun, bağlı bir birimiyle güvenli bir iletişim yapacak şekilde internet üzerinden bağlanmasının sağlanması sanal ağ oluşturulmasıdır. Bu sayede kurumların taşra teşkilatlarıyla etkin ve güvenli bir e-belge akışı sağlanabilecektir.

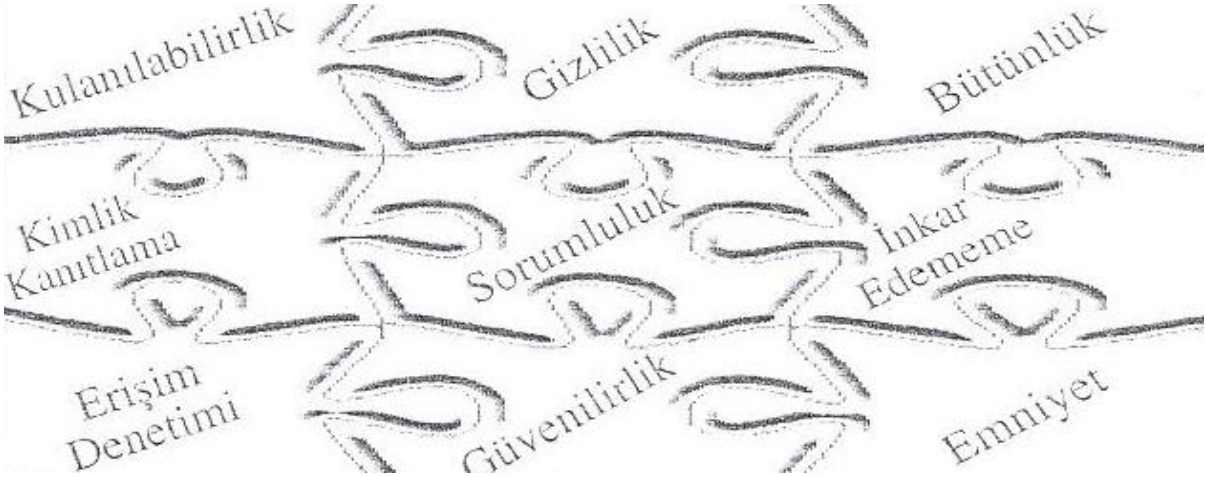
Belli teknikler, elektronik belgelerin değiştirilip değiştirilmediğini kontrol etmek amacıyla yukarda bahsedilen teknolojiler ile birlikte ya da serbestçe kullanılabilir. Bunlar, dijital imza teknolojisinde ve veri işlemede kullanılan teknikler gibi düşük düzeyde tedbirleri içerebilir (NECCC E-sign Policy Workgroup, 2001:6). Yasal gerekliliklere ve potansiyel risklere bağlı olarak göndericinin kimliğini doğrulayacak tedbirlerin muhafaza edilmesi gereklidir. Bu, belirli iş gerekliliklerine ve işlemlerin yapısına bağlı olarak değişebilir. Bazı işlemler doğrulama gerektirmez. Örnek bir doğrulama, tekil bir şifre ya da kişisel betimleme numarası kullanarak tamamlanmış olur. Ancak, yüksek riskli uygulamalar, retina taraması, parmak izi, ses doğrulama ve dinamik imza gibi biyometrik betimlemelere ya da açık şifreleme düzen(PKI*)* tabanlı elektronik imza teknolojilerine dayanabilir.

Sistem güvenliği en üst düzeyde sağlansa bile bazen, yetkisiz erişimlerde olabilmektedir. Böyle durumların olabileceği de dikkate alınarak, elektronik belgelerin kopyalanmaya karşı korumalı olması gerekmektedir. Buna ilişkin teknolojik çözümlerin kullanılması ve kopyalamanın ayrı bir güvenlik çemberi içinde gerçekleşmesinin sağlanması gerekmektedir. Bununla birlikte, sistemin kötü amaçlı yazılımlardan doğacak tehlikelere karşı koruma sağlanması gerekmektedir. Truva atları, ağ solucanları ve virüsler gibi zararlı

programların bilgisayara girmelerine engel olmak sistemi kullananların birinci önceliği olmalıdır. İkinci öncelik; bulaşma olmuşsa aktif hale gelmeden temizlemek ya da sistem yöneticisine haber vermektedir Anti-virüs programları vasıtasıyla temizleme olabilmekle birlikte, bazı durumlarda bu mümkün olmamaktadır. Güncel anti-virüs programları belleğe yerleşerek gerçek zamanlı koruma sağlar. Yani virüs sisteme bulaşmaya çalışırken fark ederek engeller (Özen, 2007:59). Sistem kullanıcıların, bu konularda bilgi sahibi olması ve sistemi tehlikeye sokacak uygulamalar konusunda dikkatli olması gerekmektedir. Sistemin güvenliği açısından, kötü niyetli yazılım ve saldırılardan korunmak için yapılması gereken temel şeyler şöyle sıralanabilir (İmamoğlu, 2008:148);

- Anti-virüs yazılımları kullanmak ve sürekli güncellemelerini takip etmek
- Kişisel güvenlik duvarı kullanarak olası saldırıları önlemek
- İnternetten ne olduğu bilinmeyen programları indirip kurmamak
- Bilinmeyen kişilerden gelen dosyaları açmamak
- Bilinmeyen kişilerden gelen e-postaları açmamak
- Bilinmeyen internet sitelerinin önerdiği ActiveX kontrollerine izin vermemek

Erişim güvenliği açısından her bir hususun yüksek seviyede bir güvenlik için önemli olduğu unutulmamalıdır. Şekil 10, bilgi güvenliği genel konseptini göstermektedir (Sağıroğlu, 2007:46).



Şekil 10. Bilgi Güvenliği Genel Konsepti

Bu konsept, kullanılabilirlik, gizlilik, bütünlük, kimlik kanıtlama, sorumluluk, inkâr edememe, erişim denetimi, güvenirlilik ve emniyet gibi hususları içermektedir. Kullanılabilirlik, erişilmek istenen elektronik belgenin sağlanabilmesidir. Gizlilik, kurumun fonksiyonları gereği ürettiği belgelerin belirlenen erişim seviyelerine göre gizlilikle ilgili hususları içerir. Bütünlük ise elektronik belgenin tam olma, delisel bütünlüğünü koruması ve bu çerçevede bir kullanımın olmasıdır. Kimlik doğrulama belirlenen sorumluluklar çerçevesinde sisteme erişimde kişini kimliğini doğrulamayı sağlamasıdır. Bu aynı zamanda yapılan işlemlere ilişkin inkâr edememe fonksiyonunun yerine getirilmesini sağlar. Belirlenen sorumluluklar çerçevesinde oluşturulan kimlik doğrulama işlemi erişim denetimini sağlar. Erişim denetiminin sağlıklı gerçekleştirilmesi sistemle ilgili güvenirlilik unsurlarını destekler. Bütün bu hususlarla birlikte, erişim faaliyeti sisteme herhangi bir zarar vermeden emniyetli bir şekilde sağlanmalıdır. Kısaca, bilgi güvenliği konseptinin bütüncül bir yaklaşım içinde alınması ve bütün unsurlarının sağlanması gereklidir. Şekilde görülen ana resmi bozacak her türlü zafiyet güvenlik açığı oluşturacaktır.

Bilgi güvenliği genel konseptine paralel olarak sistem güvenliğini sağlamak açısından mutlaka önlem alınması gerekmektedir. Bu çerçevede aşağıda sıralanan hususlar yerine getirilmelidir;

- Virüslere ve casus yazılımlara karşı gerekli güvenlik önlemleri alınmalıdır. Güvenlik duvarı yazılımları kullanılmalıdır.
- Sisteme yapılacak saldırıları tespit edecek yapılar kullanılmalıdır
- Kullanılan yazılımlar mutlak lisanslı olmalıdır. Dolayısıyla ilgili güvenlik güncellemeleri yapılabilecektir.
- Çok gizli elektronik belgeler mutlaka şifreleme algoritmaları kullanılarak arşivlenmelidir.
- Yüksek seviyede güvenlik için elektronik imza kullanılmalıdır
- Sistem güvenliğinin dinamik bir yapı olduğu sürekli güncellenmesi gerektiği mutlaka göz önünde bulundurulmalıdır.

Elektronik belge yönetim sistemi içindeki belgelerin güvenirliliği önemlidir. Genel olarak bir elektronik belge yönetim sistemi, bütün erişimleri kaydedecek denetim kayıt sistemi içermelidir. Bununla beraber, sistemin kullanılmadan önce bir risk analizinin

yapılması ve buna göre sistemin ayarlanması bir zorunluluktur (Johnston ve Bowen, 2005:135). Risk analiz çalışmalarının periyodik olarak yapılması büyük önem taşımaktadır. Zira, teknolojik ilerlemeye paralel olarak oluşabilecek yeni risk unsurları böylece tespit edilmiş olacak ve buna yönelik önlemlerin anılması sağlanacaktır. Ancak bu şekilde sisteme güvenli bir yapı içinde erişime erişimi sağlayabilir.

5.3. Erişim Hakkı ve Yetkilendirme

Erişim hakkı ve yetkilendirme ile ilgili süreçlerin belirlenmesi sistemin güvenliği ve güvenirliliği açısından büyük önem taşımaktadır. Bu çerçevede sistemi kullanacakların erişim hakları ayrı ayrı belirlenmeli, her bir kullanıcının hangi işlemleri yapmada yetkili oldukları açıkça ortaya konmalıdır. Bu, iş süreçleri çerçevesinde yapılan idari yetkilendirmelerle birlikte sistemin bütünüyle kullanımıyla ilgili süreçleri ve erişim haklarını kapsamaktadır. Kullanıcıların her birine bir kullanıcı adı ve şifresi tanımlanmalı, ilgili kullanıcı adıyla sisteme yapılan bütün giriş kaydedilmelidir. Ayrıca yapılan bütün işlemler kayıt altına alınmalıdır. Yetkisiz girişlerin ya da giriş teşebbüslerinin tespit edilmesi ve buna yönelik tedbirlerin arttırılması gerekmektedir. Elektronik belge yönetim sisteminin, sistem ve veritabanı yöneticisinin, kullanıcıların şifrelerini görmelerine izin vermeyecek şekilde tasarlanması gerekmektedir. Ayrıca aynı kullanıcı adıyla aynı anda sisteme tek bağlantının yapılabilmesinin sağlanması gerekmektedir. Sistemin kullanıcılarının değişmesi ya da kurumdan ayrılması durumunda buna ilişkin hesaplar iptal edilmeli, ancak bu kullanıcı hesaplarına ilişkin kayıtlar yasal ve idari hususlar göz önünde bulundurularak saklanmalıdır.

Kullanıcı rollerinin ayrı ayrı tanımlanması ve bunların yazılı prosedürlerle kayıt altına alınması önemlidir. Kimin neyi yapabileceği sistem içinde atanmış olsa da, sistemden kaynaklanabilecek sorunların var olabileceği göz önünde bulundurulmalıdır. Kullanıcıların, belli dönemlerde birbirlerine vekâlet edecekleri düşünüldüğünde, vekâlet edenin aynı kullanıcıyla sisteme girmesine izin vermek yerine, geçici bir vekil kullanıcı hesabı açmak daha doğru olacaktır. Zira yasal açıdan öngörülmeyecek bir takım sorunların çıkabileceği göz önünde bulundurulmalıdır. Sistemde bütün işlemler belirli bir yetki çerçevesinde yapılmalıdır. Kullanıcının belli bir işlemi yapabilmesi için kendisine daha önce bu yetkinin verilmiş olması gerekmektedir. Sistem yöneticisinin bu yetkilendirmeleri atarken resmi bir talebin olduğundan

emin olması gerekmektedir. Aksi takdirde bütün sorumluluk sistem yöneticisinde olacaktır. Sistem içinde yapılan bütün işlemler kayıt altına alınmalıdır.

EBYS, bünyesinde yer alan kullanıcılar için Kandur (2006:41) tarafından ortaya konulan en azından beş kademeli erişim hakları aşağıda değerlendirilmiştir;

- **Tasnif dışı:** İçerdiği konular itibariyle, gizlilik dereceli bilgi taşımayan, bilgi, belge, evrak, mesaj ve dokümanlardır. En alt düzeyde erişim haklarının verilmesi gereken kademedir. Bu çerçevede gerekli erişim yetkilendirmeleri yapılmalıdır.
- **Hizmete özel:** İçerdiği konular itibariyle, gizlilik dereceli konular dışında olan, güvenlik işlemine ihtiyaç gösteren ve devlet hizmetine ait özel bilgileri ihtiva eden belgelere verilen gizlilik derecesidir. Buna ilişkin erişim yetkilendirmeler belirlenen görev ve sorumluluklar çerçevesinde yapılmalıdır. Erişim hakları açısında bir üst düzeyde erişim güvenliği gerektiren kademedir.
- **Özel:** İçerdiği konular itibariyle, müsaadesiz olarak açıklandığı takdirde, milli menfaatleri olumsuz yönde etkileyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir. Bu e-belgelere erişim, yasal ve idari çerçevede belirlenmeli. Yetkisiz erişimlere müsaade edilmemelidir.
- **Gizli:** Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği, milli prestij ve menfaatlere ciddi ve önemli derecede zedeleyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir. Bu tür e-belgeler, arşivleme sistemi içinde şifreli dosyalarda saklanmalıdır. Yasal ya da idari bir gereklilik olmadığı sürece erişim hakkı verilmemelidir. Sistem yöneticisinin bu konularda çok dikkatli ve titiz olması gerekmektedir. İmha ve devir işlemlerinde çok gizli belgelere uygulanan süreçlerin uygulanması gerekmektedir.
- **Çok Gizli:** Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği büyük ölçüde tehlikeye düşürecek, devlete ve müttefiklerine büyük ölçüde zararlar verebilecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir. Bu kapsama giren e-belgeler arşivleme sistemi dışında fiziksel ya da uzaktan erişime imkân vermeyecek şekilde şifreli bir ortamda saklanmalı. Devlet arşivlerine devir işlemleri bu kapsamda yapılmalıdır. Eğer bu e-belgelerle ilgili bir imha gerekiyorsa, sistemde silmenin dışında, fiziksel depolama ünitesinin de imha edilmesi gerekmektedir. Bu işlem gerekirse diğer erişim düzeylerinde de uygulanabilir.

Yukarıda belirlenen seviyelerde erişim hakları ve rolleri belirlenmelidir. Genel bir prensip olan "bilmesi gereken" prensibi bu seviyelere uygulanmalıdır. Yetkisiz ve erişim haklı olmayan kişilerin e-belgelere ulaşmaları engellenmelidir. Gizli ve çok gizli belgelerle ilgili arşivleme ve erişim süreçleri ayrıca değerlendirilmeli. Bunlara ilişkin şifreleme ve imha süreçleri ayrı ayrı belirlenmelidir. Elektronik belge yönetim sistemi kullanıcılara tanınan erişim hakları yetkili kullanıcılar tarafından değiştirilebilmelidir. Erişim haklarında yapılan değişiklikler kayıt altına alınmalıdır. Belli bir zaman için verilen erişim haklarının, ilgili zaman diliminin bitiminde sona erdiğinden emin olunmalıdır. Sistemin bu ve benzer durumlara ilişkin uyarıları yapması gerekmektedir. E-belgelere erişimle ilgili zaman ve yasal durumlara bağlı değişimler sistem tarafından raporlanabilmelidir. Bu çerçevede erişim imkânları verilmelidir. Kullanıcıların sadece erişim hakkı olan belgeleri görmesi gereklidir. Erişim hakları olmayan e-belge ya da klasörlerle ilgili hiçbir bilgiye ulaşmamaları büyük önem taşımaktadır. Aynı çerçevede arama işlemi de, erişim hakları bulunulan e-belge ve klasörler üzerinde yapılmalıdır. Sistem bu şekilde çalışmalıdır. E-belgeleri üreten kişilerin, bunlara erişim hakkının sınırsız olduğu söylenemez. Arşivleme sistemi içinde bulunan belgeleri görüntüleme ya da kopyalama hakları, yazılı talepler çerçevesinde gerçekleştirilmelidir. Sistem, keyfi işlemlerin yapılmasına kesinlikle müsaade etmemelidir.

Kullanıcıların e-belgelere erişim sisteminde kimlik doğrulamasının sağlanması yeterli değildir. Ayrıca kaynaklar üzerinde de yetkilendirmelerin yapılması gerekmektedir. Kullanıcı sisteme giriş yaptığında sadece verilen yetkilendirmeler çerçevesinde işlem yapabilecektir. Sistem tasarımı bu farklı yetkilendirmeleri yapmaya müsait olmalıdır. Yetkilendirme daha önce girilen yönergeler çerçevesinde sistem tarafından otomatik olarak yapılmalıdır. Sistem yöneticisi kullanıcıların dosyalara güvenli bir şekilde erişmelerini sağlamalıdır. Erişim sürecinde kullanıcı kimliğinin doğrulanması, kullanıcının EBYS' deki bütün e-belgelere erişmesi anlamına gelmemektedir. Bu açıdan, her kullanıcının hangi yetkilere sahip olduğu, hangi e-belgelere hangi yetkilerle erişeceğinin açık ve anlaşılır bir şekilde belirlenmesi ve buna ilişkin olabilecek kalıcı ya da geçici değişikliklerin etkin takibinin yapılması büyük önem taşımaktadır. Bu çerçevede yetkilendirme amacıyla kullanılabilecek yöntemler (Yavaş, 2007) elektronik belge yönetimi çerçevesinde aşağıda değerlendirilmiştir;

- *İsteğe bağlı Erişim Kontrolü:* Erişim yetkisini veri sahipleri belirler. Burada resmi bir çerçevede bulunmamaktadır. Kişi ürettiği klasör ve içindeki belgeler üzerindeki erişim

- *Zorunlu Erişim Kontrolü*: Tüm belgelere erişim merkezi bir noktadan belirlenir. Yani erişim yetkileri resmi onaylar çerçevesinde sistem tarafından tanımlanır. Belgeyi üreten kişinin, erişim yetkileri üzerinde herhangi bir tasarrufu söz konusu değildir. Kullanıcının mevcut yetki seviyesinin, resmi olarak tanımlanmış yetki seviyesinin üstünde olmamasına azami önem ve dikkat gösterilmelidir. Yetkilendirmelerde yapılacak hatalar, ciddi yasal sonuçlara yol açabilir. Bu açıdan, erişim yetkilendirme konusunda bilinmesi gereken önemli bir prensip olan. "En düşük erişim hakkı", veya diğer bir tabirle "Mümkün olan en az yetki" prensibi çerçevesinde erişimde bulunan özneye kendisine atanmış olan görevlerini gerçekleştirmelerine yetecek en düşük seviyede erişim hakkı verilmelidir (Dinçer, 2007). Zorunlu erişim kontrolüne ilişkin örnek yetkilendirme, tablo 4'te gösterilmiştir. Tabloda sistemde tanımlanmış yetki seviyesinin, resmi olarak tanımlanmış yetki seviyesiyle eşit ya da daha alt düzeyde olması gerektiği vurgulanmıştır.

Kişi	**Sistemde Tanımlanmış Yetki Seviyesi**	**Resmi Tanımlanmış Yetki Seviyesi**
A	Tasnif Dışı	Tasnif Dışı
B	Gizli	Gizli
B	Gizli	Çok Gizli

Tablo 4. Zorunlu Erişim Kontrolü Yetkilendirme

- *Role Dayalı Erişim Kontrolü:* Erişim kararı, kişinin kurum içindeki rol ve sorumluluklarına dayanır. Bu yetki ve sorumluluklar kurumsal güvenlik politikalarıyla ilişkilendirilir. Kişinin görev ve sorumluluğu neyi gerektiriyorsa buna ilişkin olarak erişim haklarının verilmesi gerekliliğine dayanır. Roller ilişkin yetkilendirmeler sistem yöneticisi tarafından yapılır (Curphey, 2002).

Elektronik belge yönetim sisteminde erişim hakkı ve yetkilendirmeleri belirlerken aşağıdaki hususların mutlaka göz önünde bulundurulması gereklidir;

- EBYS'ne erişim hakkı vermek için resmi bir kullanıcı kaydı girme ve kullanıcı kaydı silme prosedürü olmalıdır. Bu prosedürler resmi bir yazıyla ortaya konmalı ve uygulama safhası bu çerçevede denetlenmelidir.
- EBYS sistem kayıtları ile ilişkilendirme ve sorumlu tutulabilme açısından kullanıcı kimliklerinin her kullanıcı için farklı olmasına dikkat ediliyor olmalıdır. Sistem içinde buna ilişkin otomatik kontrol mekanizmaları geliştirilmelidir.
- EBYS hizmetlerinin kullanabileceğine dair sistem yöneticisi kullanıcıya yetki vermiş olmalıdır. Verilen bu yetkiler, resmi onay çerçevesinde yapılmalıdır. Sözlü talepler hiçbir şekilde yerine getirilmemelidir.
- Sistemde, verilen erişim hakkı kurumsal güvenlik politikasına ve görevler ayrılığı ilkesine uygun olmalıdır. Hiyerarşiye uygun yetkilendirmeler yapılmalı ve buna ilişkin sınırlar net bir şekilde belirlenmelidir.
- Kullanıcılara erişim hakları ile ilgili yazılı belge verilmelidir. Ayrıca kullanıcılardan erişim şartlarını anladıklarına ilişkin imzalı belgenin de alınması gereklidir. Bunun için gerekli eğitim faaliyeti de gerçekleştirilmelidir.
- Görevi değişen veya kuruluştan ayrılan personelin erişim haklarının en kısa zamanda güncellenmesi büyük önem taşımaktadır. Geçiş sürecinde olabilecek yetkisizi kullanımlar ciddi sorunlara yol açabilir.
- EBYS içindeki kullanıcı parolalarının atanması ya da değiştirilmesi resmi bir prosedür uyarınca yapılmalıdır. Ayrıca kullanıcılara parolalarını saklı tutacaklarına dair bir anlaşma imzalatılmalıdır. Buna ilişkin bütün sorumluluğun kullanıcıya ait olduğu belirtilmelidir
- Dosya, dizin ve e-belgelere erişim izinlerinin gruplara verilmesi, gerekmediği sürüce kişilere özel izin verilmemesinin sağlanması gereklidir.
- EBYS'nde yetkilendirmelerin belirli aralıklarla gözden geçirilmesi, gereksinimi kalmamış yetkilerin geri alınması ya da değiştirilmesinin sağlanması gereklidir.

5.4. Kullanıcı Ara Yüzü

Ara yüzü genel bir ifade ile bilgisayar ekranından kullanıcıya yansıyan ve kullanıcının yazılımla etkileşimini sağlayan her türlü öğe olarak tanımlanabilir. Bu öğeler navigasyon butonları, yazı büyüklüğü ve karakteri, menüler, renkler, görsel ve işitsel materyaller olabilmektedir. Ara yüzün kullanılabilirliği, ara yüzün olması gereken tek niteliği değildir.

Zira kullanılabilirliğin birçok yönü vardır. Bunlar, kolay öğrenilme, etkin kullanılma, kolay hatırlanma, az hata verme ve kullanıcı açısından memnuniyet yaratmadır (Nielsen, 1993:33). Bu hususlar eğer mevcutsa, ara yüzün kullanıcı dostu olduğundan bahsedilebilir.

Nielsen (1994) kullanışlılık kontrol metotları (Usability Inspection Methods) kitabında kullanıcı ara yüzün tasarımında göz önünde bulundurulması gereken on temel prensipten bahsetmektedir. Bu prensipler aşağıda değerlendirilmiştir;

- *Sistem durumunun görünürlülüğü:* Sistem, kullanıcıyı makul bir zaman içerisinde sistemde neler olduğu konusunda geri bildirim yapmak suretiyle ile haberdar etmelidir.
- *Sistemin kullanıcıya yakınlığı:* Sistem, kullanıcılara yakın gelen terim ve ifadeler kullanılarak, kullanıcının dilinden konuşmalıdır.
- *Kullanıcı kontrolü ve özgürlük:* Kullanıcılar genellikle sistem fonksiyonlarını yanlışlıkla seçebilmektedir. Bu durumdan kolayca kurtulmayı sağlayacak acil çıkış kapıları sunmalıdır. Bu yüzden geri al ve yinele fonksiyonları sistemde bulunmalıdır.
- *Tutarlılık ve standartlar:* Kullanıcılar farklı kelime, durum ve aksiyonların aynı anlama gelip gelmediğini merak etmek durumunda kalmamalıdır.
- *Hata önleme:* Çok iyi hata mesajları yerine kullanıcıların hata yapmasını önleyen dikkatli tasarımlar gerçekleştirmek daha önemlidir. Kullanıcıların hata yapma olasılıklarını artıran durumlar ortadan kaldırılmalı veya kullanıcılardan bir faaliyeti nihayetlendirmeden önce bunu yapmak isteyip istemediğinin doğrulamasını yapmaya imkân vermelidir.
- *Hatırlanma yerini tanıma:* Kullanıcının hafıza yükünü asgariye indirecek şekilde işler objeler ve seçenekler görünür olmalıdır. Kullanıcı bir bölümden diğerine geçtiğinde bazı bilgileri hatırlamak zorunda kalmamalıdır. Sistemin nasıl kullanılacağına dair bilgiler görünür veya gerektiğinde kolayca bulunabilir olmalıdır.
- *Esneklik ve kullanım etkinliği:* Kullanıcı ihtiyaçlarını tahmin edip gerekli adımların sayısı düşürülmeli ve sistem özelleştirmeye imkân tanımalıdır.
- *Estetik ve asgari tasarım:* Bölümler, ihtiyaç duyulmayan veya alakasız bilgiler içermemelidir. Alakasız her bir bilgi, ilgili olabilecek diğer hususların önüne geçerek görünürlülüğü düşürecektir. Bu husus göz önünde bulundurulmalıdır
- *Kullanıcıların hataları tanıması, anlaması ve onlardan kurtulmasına yardım*: Hata mesajları kod içermemeli, problemi açık bir dille ifade etmeli ve yapıcı bir şekilde kullanıcıya çözüm önermelidir.

- *Yardım ve Dokümantasyon:* Sistemin herhangi bir dokümantasyona ihtiyaç duyulmadan kullanılabilmesi daha iyi olsa da, kullanıcılara yardım ve dokümantasyon sağlamak gerekebilecektir. Bu durumda, ihtiyaç duyulan bilgiler kolayca aranabilmeli, kullanıcıların görevlerine odaklanmalı, çözüme yönelik somut adımlar içermeli ve çok uzun olmamalıdır.

Ara yüz tasarımında bütün bu hususlar dikkate alınmalıdır. Bu sistemin etkin ve verimli kullanılmasını sağlayacaktır. Sistemi kullanırken oluşabilecek hataları asgariye indirecektir. EBYS'nin, kullanıcılarının elektronik belgelere, dosyalara ve araştırma araçlarına kolay erişiminin desteklenmesi gereklidir. Belge bulma sistemine erişim için bilgisayara kurulması gerekli yazılımların ve bu yazılımların etkin bir şekilde çalışabileceği donanım teknik özelliklerinin belirlenmesi gereklidir (Public Records Office of Victoria, 2000:9). Elektronik belgeleri internet aracılığıyla erişim gerekebilir. Web ara yüzü, internet aracılığıyla erişimi desteklemeli ve kamu kurumlarının kullandıkları donanım profilleri buna imkân tanımalıdır. Kullanıcı ara yüzünün dizaynında özel bir dikkat gösterilmelidir. Bu ara yüz kullanıcıların, sistemle etkileşim içinde oldukları birincil yoldur. Karışıklıklardan kaçınmak için içerik ve üst verinin sunumunda dikkat gösterilmelidir. Kullanıcı ara yüzü mümkün olduğu kadar kullanıcı dostu olmalıdır.

Kullanıcı ara yüzü basit ve işletim sistemi ile uyumlu bir şekilde çalışmalıdır. Ara yüzün, kullanıcıların kendilerine özel ayar yapmasına izin vermesi gereklidir. Yani kullanıcıların, kullanım açısından temel özellikleri kişileştirebilmesi gereklidir. Pencere ayarlar, uyarı mesajlar, renk ve font ayarları gibi kişileştirilebilecek özellikler kullanıcı profilinde saklanmalı ve sisteme girişi yapıldığında aktif hale gelmelidir. Kullanıcıların sistem içinde sık kullandıkları fonksiyonlar için kısa yol tuşları ve simgeleri tanımlanmalı, buna ilişkin olabilecek taleplere göre ara yüzde kolay değişiklikler yapılabilmelidir. Bu çerçevede temel nokta her işlem ve hizmette olduğu gibi kullanıcı hedef alınarak düzenleme yapılmasıdır (Arslantekin, 2001:39).

Etkin bir ara yüz tasarımı bağlamında, teknolojinde yaşan hızlı değişime karşı başarılı olabilmek için, modüler bir tasarımın yapılması gereklidir. Bu modüler yapı, ara yüzün genel yapısı ve teknolojik bileşenlerin ihtiyaç duyulduğunda geliştirilmesine ya da başka bileşenlerle değiştirilmesine imkân vermesi açısından kritik öneme sahiptir. Teknoloji gelişmelerden yararlanabilmek için, tek parça bir sistemi tekrar tasarlamak oldukça uzun bir

zaman alır. Modüler tasarımlar, karmaşık problemleri daha küçük parçalara ayırarak ve bu bağımsız parçaları ayrı ayrı değerlendirme imkânı sunarak kolay işlenir hale getirir (Sproull ve Eisenberg, 2005:23). Düzgün bir şekilde tasarlanmış parçalar, daha üst bir versiyonla değiştirilebilir. Böylece, diğer modüllerde ya da sistemin bütününde en alt düzeyde bir kesinti sağlanmış olur. Eğer modüller oldukça büyük olursa, bunları değiştirmek ya da değişiklik yapmak zorlaşmaktadır. Eğer ara yüz aşırı karmaşıksa, bir modülde bağımsız olarak yapılacak bir değişiklik diğer modüllerde kayıplara yol açabilir. Değişikliklerin olabileceği ihtimali göz önünde bulundurularak yapılan bir ara yüz tasarımına ek olarak, sistemde bir takım düzeltmelere gerek duyulmadan bazı değişikliklerin adapte edilebilmesine imkân verecek, geliştirilebilir bir tasarım özelliğinde olmalıdır.

Ara yüz tasarımını gerçekleştirirken karşıtlık ve simetri gibi iki temel tasarım öğesi göz önünde bulundurulmalıdır (Gürkan, 2007:19). Karşıtlık esas olarak ara yüzdeki öğeler arasındaki karşıtlığı yansıtır. Örneğin, başlıklar ile metin arasındaki farklılığı göstermek için karşıtlık kullanılabilir. Karşıtlık belirlerken vurgu düzeyine uygun karşıtlık belirlenmelidir. (Gürkan, 2007:20). Simetri ise biçimsel öğelerin başında gelmektedir. Simetri sayesinde sayfa içinde bir bütünlük ve tek düzelik sağlanabilir. Aynı özellikteki metinlerin biçimleri aynı, ayrı özellikteki metinlerin biçimleri ayrı, aynı özellikteki öğelerin biçimleri aynı olmalıdır. Bu çok iyi bir simetrinin oluşmasını sağlayacaktır. (Gürkan, 2007:21). Karşıtlık ve simetriyi uygularken çok katı bir yaklaşım sergilenmemelidir. Gerekli olabilecek durumlarda esneklik sağlanmalıdır. Ayrıca, ara yüz tasarımında kullanım kolaylığı temel yaklaşım olmalıdır. Ara yüz tasarımında renk uyumuna dikkat edilmelidir. Özellikle zemin rengi ve ilişkili menülerin renginin seçiminde dikkatli olunmalıdır. Kullanıcının gözünü yoracak parlak renklerden kaçınılmalıdır. Bu hususlar çerçevesinde, tasarım gerçekleştirirken temel olarak aşağıdaki hususları göz önünde bulundurmak faydalı olacaktır;

- Sistem içinde istenilen bölümlere kolayca ulaşılabilmesini sağlayacak bir menü yaklaşımı benimsenmelidir.
- Ara yüzde renklerin uyumlu olmasına ve gözü yormamasına önem verilmelidir
- Ara yüz kolay geliştirilebilir bir alt yapıda olmalıdır. Kolay bir şekilde ekleme ve çıkarma işlemi yapılabilmelidir.

5.5. Erişim Seçenekleri

Elektronik belgelerin saklama süreleri boyunca, bütün yasal iş amaçlarına yönelik erişilebilirliğini sağlamak için yeterli arama ve erişim kabiliyetlerini muhafaza etmelidir. Buna, belgelerin çevrimdışı ya da yarı pasif ortamlarda depolandığı dönemde erişmek de dahildir. Bu hem yeterli indeksleme ve hem de arama araçları gerektirecektir. Bu açıdan, elektronik belgelerin, iş amaçları ve bütün kamunun erişim gereksinimleri için basılı kopyaları da dahil olmak gerçek kopyalarının üretilmesi ve kullanılabilir formatta sağlanması gerekmektedir. Kâğıt belgelere bir anda sadece bir yerde bulunabilir. Elektronik belgeler ise aynı anda birçok kişi tarafından görüntülenebilir. Bu erişim açısından bir avantaj sağlar. Farklı yerlerde bulunan kullanıcılar, aynı belgeyi tartışabilir ya da farklı kullanıcılar aynı belgeyi farklı amaçlar için kullanabilir (Johnston ve Bowen, 2005:138). Kurumda bulunmayan bir kişinin, kurumsal ihtiyaçlar ve yetkilendirmeler çerçevesinde elektronik belgelere uzaktan erişebilmesi çok önemli faydalar sağlayabilir. Elektronik belgeleri saklamak için kişisel gizlilik koruma politikalarını ve erişimi geliştirmek ya da gözden geçirmek önemli bir noktadır. Bunu gibi politikalar, bilgiye erişim özgürlüğüyle ilgili yasal gerekliliklerle uyumlu olmalıdır. Kişisel gizlilik ve güvenirliliği koruyacak ve elektronik belgelere kamunun erişimini sağlayacak metotların geliştirilmesi gereklidir. Sistem dizayn edildiğinde, kurumlar güvenlik gereklilikleri ve kamu erişimi dikkate alacak erişim metotları geliştirmelidir. Elektronik belgelere kamunun erişimiyle ilgili ihtiyaçlar, kişisel gizlilik ve güvenliği korumaya yönelik kurumların yasal yükümlülükleri çerçevesinde devamlı olarak ağırlaştırılması zorunludur. Bu sebepten, kurumlar her türlü kişisel bilgileri güvenli bir şekilde korumak ve elektronik belgeleri kamuya açmadan önce güvenli bilgileri korumaya yönelik otomasyon çözümlerini gelişmeleri gerekmektedir.

Elektronik belgelere erişimin kullanıcının tercih ettiği formda sağlanması önemlidir. Bazı kurumların elektronik belgeleri kullanmak için gerekli teknolojilere erişimleri yoktur ya da belgeleri kâğıt ortamda tercih ederler. Kurumların, elektronik belge yönetim düzenlemelerinde, istendiğinde elektronik belgeleri kâğıt formda erişilebilirliğini sağlaması gerekebileceğini göz önünde bulundurmalıdır (NECCC E-sign Policy Workgroup, 2001:12). Bu, kurumların elektronik belgelerin kâğıt kopyalarını saklamasının zorunlu olduğu anlamına gelmez. Yalnız, elektronik belgenin kopyasının hem kâğıt hem de elektronik ortamda sağlayabilecek teknik altyapıya sahip olmaları gerekir.

Erişim seçenekleri açısından değerlendirildiğinde, elektronik belgeye üç temel erişim düzeyi bulunmaktadır. Bu erişim düzeyleri fiziksel depolama seçeneklerine göre değişmektedir. Bu çerçevede değerlendirme yapılmalıdır. Elektronik belgeye erişim düzeyleri aşağıdaki gibidir (Records Management Institute, 2000: 5);

- *Çevrimiçi erişim:* Elektronik belgelerin anında ve hızlı erişim için sabit diskte depolanmasıdır. Bu elektronik belgelerin sürekli bir şekilde ve anında erişilebilir olmasını sağlar. Bu çözüm sık erişim gereken belgeler için en uygun olanıdır.
- *Yarı aktif erişim:* Aktif kullanımı olmayan elektronik belgelere erişimi sağlamak için optik ortamda depolanmasıdır. Erişim çevrimiçi ye göre daha yavaştır, ancak daha güncel bilgiler için ağda daha fazla alan oluşmasını sağlar. Bu çözüm ara sıra erişim gereken belgeler için en uygun olanıdır
- *Çevrimdışı erişim:* Elektronik belgelerin, çevrimdışı erişim için taşınabilir ortamlarda depolanmasıdır. Ortama erişim, kurulum için elle müdahale gereklidir Bu çözüm çok daha yavaş bir erişim sağlar ve çok nadir kullanılan belgeler için kullanılmalıdır. (Minnesota Historical Society, 2004:3);

Eğer yarı pasif ya da çevrimdışı depolamadan biri seçilirse, hangi aracın kurumsal ihtiyaçları en iyi karşılayacak çözüm olduğu değerlendirilmelidir. Bunu yapmak için, dosyaların büyüklüğü ve ilişkili üst verilerle birlikte mevcut ya da depolanmış belgelerin tahmini miktarının analiz edilmesiyle başlanması gereklidir. Ayrıca, elektronik belge yönetim sistemi içinde erişime sunulan belgelerin yasal açıdan geçerliliği olduğu gerçeği göz önünde bulundurulmalıdır Gerek yasal süreçlerde ve gerekse araştırmaya dönük çalışmalarda delili niteliği taşımaktadır. Bu açıdan, elektronik belgeler CD, DVD ortamında ya da FTP ve internet aracılığıyla erişime sunulması gerekebilir. Benzer şekilde, elektronik belgelere erişim, internet, intranet, extranet ve oluşturulacak portallar aracılığıyla olabilmektedir.

Kurumların elektronik belgeleri resmi yazışmalarda kullanmaya başlamaları ve bu yöndeki eğilimde bir artışın olması, elektronik belgelere erişimi gerekli hale getirmektedir. Kurumsal ihtiyaçların dışında araştırma amaçlı olarak elektronik belgelere erişim sağlama konusunda istekli olunduğu söylenemez. Bu noktada önemli faktör olarak, erişime açılacak elektronik belgelerin içeriği konusunda mutlak bir hâkimiyetin söz konusu olmaması, bunun sonucu olarak birtakım yasal ve idari sorunların yaşanabileceğinin değerlendirilmesidir. Kurumsal ihtiyaçlarda elektronik belgenin formatı önemli bir faktör olmaktadır. Zira,

elektronik ortamda istenen belgenin gönderilmesinde birtakım güvenlik riskleri oluşabileceği göz önünde bulundurularak, kâğıt çıktısı da istenebilmektedir. Bu durumda artık elektronik imzalı belgenin çıktısı üzerinden, elektronik imzanın kontrol edilmesi mümkün değildir. Çünkü elektronik imzanın kontrolü, ancak elektronik şekilde gerçekleştirilebilir. Bu sebeple çıktısı alınmış bir elektronik belgede artık veri değişikliğinin tespit edilebilmesi mümkün değildir. Bu açıdan yasal gereklilik durumunda Elektronik belgelerin mahkemeye ibrazı, bir veri taşıyıcısının mahkemeye verilmesi ya da e-mail yoluyla mahkemeye elektronik belgenin gönderilmesi suretiyle olabilir. Mahkemede, elektronik belge, tekrar başka bir veri taşıyıcısı üzerine kaydedilecektir. Bu şekilde devamlılık fonksiyonu da yeterince sağlanmış olacaktır. Yani elektronik belge, bilgisayar ekranında temsil edildikten sonra ya da yazıcıdan kâğıt üzerine çıktısı alındıktan sonra yargılamaya delil olarak ibraz edilebilir. Bu hususun göz önünde bulundurulması gereklidir.

Kurumların yasal ve idari gereklilikler çerçevesinde başka kurumlara ait elektronik belgelere erişim talepleri de olabilmektedir. Bu durumda elektronik belge yönetim sistemlerinin birlikte işlerliği büyük önem taşımaktadır. Uyumlu olmayan sistemde bunu başarmak mümkün gözükmektedir. Bu açıdan Devlet Arşivlerinin belirlediği standartlar çerçevesinde bir yapı teşkil edilmelidir. Elektronik belge taleplerinin aynı şekilde elektronik ortamda yapılması en sağlıklı olanıdır. Zira, oluşturulan belgenin, fonksiyonel olarak ilgili elektronik belge yönetim sistemi içinde ilişkilendirilip arşivlenmesi kolay olacaktır. Aksi durumda, benzer işlemi yapmak uzun zaman alabilecek ve hatta gerçekleştirilmeyebilecektir. Eğer elektronik ortamdaki belgeler için talepler kâğıt ortamda gerçekleşirse, sistem içinde bu talepleri ilişkilendirmek için bir dijitalleştirme faaliyetinin yapılması ve böylece elektronik belge yönetim sistemine entegrasyonunun sağlanması gerekecektir. Bunun da ne kadar sağlıklı bir yaklaşım olduğu değerlendirilmelidir. Elektronik belgelerin arşivlenmesi konusunda dış kaynak kullanımına da başvurulabilmektedir. Bu durumda elektronik belgelere erişim için ilgili organizasyonla bağlantıya geçmek gerekecektir. Bu durumda izlenecek yol, resmi bir yapı içinde izlenecek yolla aynı olmalıdır. Bu yasal ve idari açıdan elektronik belgenin geçerliliği noktasında önemlidir.

Elektronik belge içeriklerine, kullanıcıların çevrim içi olarak yetkiler dahilinde araması ve erişmesi sağlıklı bir şekilde gerçekleştirilmelidir. Kullanıcılar, erişimin aracısız bir temelde mevcut olmasını bekleyebilmektedir. Ancak yetkili kişiler olmadan bunun sağlanmaması gereklidir. Bununla birlikte, araştırma amaçlı olarak yasalar çerçevesinde

internet aracılığıyla bazı belgelerin erişme sunulabilir. Ayrıca, kullanıcıların bunlara ücretsiz erişme gibi bir beklentisi olabilir. Araştırma amaçlı olarak erişime sunulan belgeler için bir erişim maliyeti bulunmaktadır. Araştırmacının elektronik belgeyi hangi formatta ve hangi ortamda isteyeceğine bağlı olarak bu maliyet değişebilmektedir. Buna yönelik açık bir politikanın belirlenmesi ve uygulamanın bu çerçevede yapılmasının sağlanması gereklidir (Sproull ve Eisenberg, 2005:31). Bununla birlikte kullanıcıların belgelere hızlı erişme beklentileri karşılanmalıdır. Sisteme aşırı yüklenme sonucunda erişim ciddi anlamda yavaşlayabilmekte, hatta durabilmektedir. Buna yönelik önlemler alınmalıdır. Elbette, erişimlerin hepsinin anında gerçekleştirilmesi mümkün olmayabilir. Belgeleri aramak için daha zengin veri tipleri ve daha kapsamlı yaklaşımlar daha fazla işlem süresi gerektirebilir. Özelleştirilmiş erişim yollarının bütün belge çeşitleri için elverişli hale getirilmesi mümkün olmayabilir. Ayrıca kullanıcılar, çoklu kaynak içerikleri aracılığı ile arama yapma imkânının sunulması gerekebilir. Zira kullanıcılar, belgelerin hangi kuruma ait olduğuna bakmaksızın erişmek isteyebilmektedir.

6. BÖLÜM
SONUÇ VE ÖNERİLER

E-devlet olgusunun gelişmesi ve buna paralel olarak elektronik ortamda sunulan hizmetlerin yaygınlaşmasıyla iş süreçlerini yerine getirme usullerinde değişimler olmaktadır. Bu durum bilgi teknolojilerinde yaşanan hızlı değişimin bir sonucu olarak karşımıza çıkmaktadır. Bilgi teknolojilerinde yaşanan değişime paralel olarak, kurum ve kuruluşlar işlerinin büyük çoğunluğunu ağlar aracılığıyla elektronik olarak yürütme noktasında yeni teknolojilerin sağladığı avantajları kullanmaktadır. Bununla birlikte kâğıtsız işlemleri destekleyen, coğrafi bilgi sistemleri, dijital görüntüleme ve elektronik veri değişimi gibi teknolojileri de uygulamaktadır. Bu teknolojik değişimler, kurumsal ihtiyaçları ve yasal gereklilikleri desteklemeye yönelik belge üretim, yönetim ve kullanımıyla ilgili kurumsal yeterlilikler üzerinde önemli etkisi bulunmaktadır. Bu çerçevede, organizasyonların işlemlerini elektronik ortamda yapmayı tercih ettiği görülmektedir. Bu tercihe sebep olarak, bilgiye daha hızlı erişim, daha büyük çapta paylaşabilme ve elektronik ortamda bilgiyi depolamanın maliyeti düşürmesi gösterilebilir. Bu eğilim, kâğıt belgelerin yok olacağı anlamına gelmez. Ancak, elektronik belgelerin git gide daha ön plana çıktığı önemli bir gerçektir. Belirtilen bütün hususlar e-devlet yaklaşımının ve uygulamalarının bir parçası olarak oluşmaktadır. Bu açıdan e-devlet uygulamaları çerçevesinde elektronik ortamda üretilen belgeler ve oluşan e-arşivler kurumların bilgi sistemlerinin önemli bir parçası olarak karşımıza çıkmaktadır (Özdemirci, 2009:2). E-devlette, bilginin toplanması, değerlendirilmesi, paylaşılması ve dağıtılması bilgi ve iletişim omurgası üzerinden yürütüleceği için, bu yeni iş anlayışı doğal olarak devletin kendi içinde ve sunduğu hizmetlerin biçiminde elektronik belge bağlamında değişimi gerekli kılmaktadır. Elektronik belge yönetimi uygulamaları sayesinde e-devlet hizmetleri daha hızlı ve etkin hale gelmektedir (Özdemirci ve Bayram, 2009:398). E-devlet anlayışının yerleşmesiyle resmi yazışmalar artık elektronik ortamda yerine getirilmeye başlanmıştır. Bu çerçevede elektronik belgelerin etkin arşivlenmesi ve erişiminin sağlanması da büyük önem kazanmaktadır.

Elektronik belgelerin ve dijital ortama aktarılan kâğıt belgelerin elektronik olarak yönetilmesi, belirlenen belge yönetim yaklaşımları ve prensipler çerçevesinde bilgisayar

araçları ve yazılımlarının oluşturduğu bilgi teknolojileri sistemleri aracılığıyla yapılmaktadır. Elektronik belge yönetim sisteminin uygulanması iki aşamada gerçekleşir. Birinci aşama; sistemin oluşturulmasıyla ilgili süreçlerin bulunduğu aşama, ikincisi ise; sistemi destekleyen ve sistemin kullanımını kolaylaştıran işle ilgili kuralla bütünüdür. Elektronik belgelerin arşivlenmesi bu noktada en önemli unsur olarak değerlendirilmektedir. Elektronik belgelerin arşivlemesi faaliyeti erişim de dahil olmak üzere bütün belge yönetim aktivitelerini doğrudan etkileyen bir konudur. Bu açıdan sağlıklı gerçekleştirilmesi büyük önem taşımaktadır. Eğer elektronik belgeler doğru bir şekilde yönetilmez ve arşivlenmezse, yalnız geleceğin araştırmacılarını kullanacağı arşiv kaynakları kaybolmayacak, aynı zamanda kurum yasal bir durumla karşılaşmada, mülkiyet ispatında, güncel aktiviteler için gerekli bilgileri bulmada, önemli mali kayıplarının olabileceği durumlarda gerekli belgelere erişememe gibi risklerle karşı karşıya kalınacağı gerçeği göz önünde bulundurulmalıdır.

Geleneksel olarak arşiv sistemleri, belgenin bütünlüğünü ve geçerliliğini sağlamayı amaçlar. Ancak arşiv ilk olarak bunları sağlasa da zaman içinde bütünlük kesin olarak tehlikeye girecektir. Bu açıdan, arşivsel bir bakış açısıyla, uzun dönem sosyal ve kurumsal ihtiyaçları göz önünde bulundurularak değerlendirme yapıldığında, sağlıklı bir arşivleme sistem oluşturulmazsa sürekli bir değere sahip elektronik belgelerin gerçekliğini ve bütünlüğünü tehlikeye sokacak kayıpların olabileceği ya da delilsel vasıflarını yitirebileceği göz önünde bulundurulması gereken önemli bir gerçektir. Bu çerçevede elektronik belge yönetim gereklilikleri, yönetim aşamasından değil, sistemin dizayn aşamasında belirlenmeli ve tasarlanmalıdır. Ayrıca, organizasyonlar, elektronik belge yönetim gerekliliklerinin, kurumsal uygulamalara ve iş süreçlerine entegrasyonunda yardımcı olacak anlık belirli çözümler ve araçlara ihtiyaçları bulunmaktadır (Kowlowitz ve Kelly, 1997).

Kurum ve kuruluşlar, artan miktardaki elektronik belgeleri yönetmek için gerekli araçlar ve kurumsal kabiliyetler noktasında yeterli değillerdir. Bazı organizasyonlar, kişisel bilgisayarlarda ya da yerel ağda depolanan belgelere erişim imkânını kaybetmek tehlikesiyle karşı karşıya kalmaktadır. Bazıları da, iş süreçleri sonucunda farklı formatlarda oluşan belgeleri ilişkilendirmek noktasında önemli sorunlar yaşamaktadır. Benzer yapılar içinde, birçok organizasyon da, elektronik belgelerin kurumsal delilsel ihtiyaçlarını karşılamadığını değerlendirmektedir. Bu duruma yol açan en önemli etken ise sağlıklı bir arşivleme ve erişim sisteminin oluşturulmamasıdır. Buna bağlı olarak elektronik belgelerin arşivlenmesi işleminin, kâğıt belgeye göre üzerinde değişiklik çok kolay olduğu için daha dikkatli ve

belgenin her aşamasını kontrol gerektirmektedir. Bu anlamda teknolojinin sunduğu avantajların yeterince kullanılması önemli tamamlayıcı bir faktördür.

Günümüz dünyasında gelişmelerin gerektirdiği değişim, insanlığın ihtiyaçları ve beklentileri arttırmış, yeni değişimler ve gelişmeler de dolayısıyla yeni teknolojileri beraberinde getirmiştir. Değişimin yönetilebilmesi için yönetimin değiştirilmesi, dinamik politikalar yürütülmesi ve yönetim ile karar alma süreçlerinin esnekleştirilmesi gereklidir. Dönüşüm sürecinin iyi yönetilebilmesi için klasik reflekslerin davranış biçimlerinin ve yönetim anlayışının değiştirilmesi zorunludur. Bilişim teknolojilerin yoğun bir şekilde kullanılması ile iş ve işlemleri yapış şekilleri değişmeye başlamış, verimlilik artışı sağlanmış, belgelerin üretimi, kullanımı ve yaygınlaştırılması kolaylaşmış, belgelerin depolanması, aktarımı ve tekrar elde edilmesi elektronik belge ile birlikte kolaylaşmış, işlemler hızlanmış ve sonuçta üretkenlik arttığı gibi hizmet kalitesi de doğal olarak yükselmektedir. Elektronik belgelerin kullanıma açık olması ve teknolojiye bağımlılığı sebebiyle gerçekliğinin ve güvenliğinin de sağlanması çok önemlidir. Bunun içini elektronik belgelerin bir varlık olarak karşılaşabilecek tehlikelerden her şekilde korunması ve bu korunmanın yasal olarak da desteklenmesi büyük önem taşımaktadır. Elektronik belgeyi ve bağlantılı üst veriyi ifade eden veri akışlarını sağlıklı bir şekilde depolamak ve geri iletimini sağlamak etkin bir arşivleme açısından önemli bir gerekliliktir. Genel kural olarak etkin arşivleme, orijinal verilerin ve belgenin içinde bulunan bütün bilgilerin korunması anlamına gelir. Bu işlemin sağlıklı yürütülmesi bütün sistemin işlerliği açısından önemlidir.

Elektronik belgelerin güvenli bir sistem içinde arşivlenmesi ve etkin erişiminin sağlanması büyük önem taşımaktadır. Elektronik belge yönetim sistemini kullanan kurumların buna ilişkin teknolojik altyapıyı planlamaları, güvenlikle ilgili gerekli önlemleri almaları ve birlikte işlerlik açısından ortak standartları göz önünde bulundurmaları gerekmektedir. Bu süreçte, elektronik belge yönetim standartlarının göz önünde bulundurulması, gerekli teknolojik altyapının sağlanması ve sürdürülmesi, gerekse üst veri elemanlarının sağlanması gereklidir. Ayrıca arşivlenen elektronik belgelerle ilgili saklama planlarının oluşturulması ve gerekli ayıklama ve imha işlemlerinin teknolojik çözümler çerçevesinde gerçekleştirilmesi gereklidir. Bütün bu hususlar çerçevesinde elektronik belge yönetim sisteminin işleyişiyle ilgili süreçlerin sistem dizayn aşamasında belirlenmesi ve uygulanması büyük önem taşımaktadır. Sistemin güvenliğini sağlamakta aynı seviyede öneme sahip diğer bir konudur. Elektronik belgelerin gerçekliğini ve bütünlüğünü tehlikeye sokacak risklerden sistemin

korunması, sistemin varlığını sürdürmesi ve geçerli olabilmesi açısından en önemli unsur olarak değerlendirmek gerekmektedir. Bu açıdan sistem güvenliği çok önemlidir. Eğer bu husus sağlanmazsa arşivlenen elektronik belgelerin gerek araştırma amaçlı ve gerekse yasal açıdan geçerliliğinin risk altında olacağı önemli bir gerçektir.

Tezin bütününde belirtilen hususlar çerçevesinde uygulamaya dönük arşivleme ve erişim açısından aşağıda belirtilen önerilerin göz önünde bulundurulması oluşturulacak sistemin sağlıklı işlemesi açısından büyük önem taşımaktadır. Tezde ortaya konan hususlar ve aşağıda sıralanan önerilerin bilgi teknolojilerine mutlak bağımlı olmaları dolayısıyla bilgi teknolojileri uzmanlarıyla koordineli ve etkin çalışmanın yapılması gereklidir. Teknolojik bağlamda sunulan bazı önerilerin nasıl yapılacağı konusuna, çok derinlemesine teknolojik bilgi içermesi, farklı bir uzmanlık gerektirmesi ve mevcut teknolojik çözümlerde bulunması dolayısıyla detaylı değinilmemiştir. Temel yaklaşım olarak var olan ya da oluşturulacak teknolojik çözümlerde hangi hususların önemle göz önünde bulundurulması gerektiği vurgulanmıştır. Ortay konulan öneriler, arşivleme ve erişim olarak iki ana başlık altında verilmiştir;

Elektronik belgelerin etkin arşivlenmesine yönelik öneriler;

- Elektronik belgenin üretilmesinden, kullanılması, saklanması, aktif olmayan dosyaların saklama planları, aktif dosyalara transferi ve nihai olarak imhasını içeren yaşam döngüsü süreçlerinin etkin yürütülmelidir.
- Elektronik belgelerin bilgi teknolojilerine bağımlılığı dolayısıyla üretildiği yazılım ve donanım korunmalı ya da gelişen bilgi teknolojileri bağlamında yenilenmelidir.
- Arşivlemede, elektronik belgelerin erişilebilirliğini ve bütünlüğünü koruyan kontrollü depolama ya da dosyalama sistemleri kullanılmalıdır.
- Belge yönetimiyle ilgili yasalarla uyum içinde elektronik belge saklama ve imha planlarının oluşturulmalıdır.
- Uzun dönem arşivleme açısından, uygun standartlar göz önünde bulundurulmalı, açık kaynak kodlu ve özel olmayan veri formatlar kullanılmalı ve zorunlu standartlarla uyum sağlanmalıdır.
- Kamuya açık olmayan kişisel bilgiler içeren yüksek düzeyde hassas belgeler şifreli formda arşivlenmelidir.

- Arşivleme sisteminin, elektronik belgelerin orijinal işlevselliğini gereken düzeyde muhafaza etmesi sağlanmalıdır.
- Arşivlenen elektronik belgelere erişimle ilgili kanunlara dayalı gerekli sınırlandırmalar yapılmalıdır.
- Elektronik belgenin yaşam süresini etkileyen en uygun depolama ortamı seçimi, performans, depolama kapasitesi ve güvenirlilik kriterleri çerçevesinde yapılmalı, uzun dönen arşivleme açısından manyetik bantlar tercih edilmeli ve zaman içinde gerekli taşıma işlemlerinin gerçekleştirilmelidir.
- Uzun dönem dosya arşivleme için özel olmayan formatlar en ideal format olarak tercih edilmelidir.
- Uzun dönem arşivleme ve kullanım açısından, XML, XPS ya da PDF/A formatlarından biri tercih edilmelidir.
- ASCII metin formatı, yazılım bağımlılığını azaltması ve ürün eskimesine karşı önlemler içermesi bakımından uzun dönem saklama gerektiren özel formattaki elektronik belgelerin yerine ya da birlikte göz önünde bulundurulmalıdır.
- Elektronik belgelerin arşivlenmesi için kullanılan donanımlar ve diğer ilgili ekipmanlara yönelik uygun nem ve sıcaklıkta depolama mekânlarının seçilmelidir.
- Uzun dönem saklanması gereken belgelerin veri yapılarının bozulma olasılığı bulunmasından dolayı, arşivleme sisteminde hata sezme ve düzeltme teknikleri kullanılmalıdır.
- Elektronik belge arşivleme sistemiyle ilgili düzenli yedekleme işlemleri yapılmalıdır.
- Belli aralıklarla depolama disklerinde ya da bantlarında herhangi bir veri kaybının olup olmadığının test edilmelidir.
- Depolama disklerinin ve bantlarının telefon da dahil olmak üzere güçlü elektrik ve manyetik akımlardan uzak tutulması sağlanmalıdır.
- Elektronik belge saklama birimlerinin çevresel şartlara, elektrik ve manyetik alanlara karşı duyarlı olması sebebiyle bir kopyası harici saklama birimlerine aktarılmalıdır.
- Teknolojik ürünler anlamında tek bir markaya bağımlılığı önlemek için, farklı markalarda teknolojik bileşenler alınmalı ve sistemin farklı marka ürünleri üzerinde de sağlıklı çalışması sağlanmalıdır.
- Elektronik belge yönetimi için kurumsal bir yazılımın geliştirilmeli ve uygulanmalı, kısıtlayıcı unsurlar içeren firma bağımlı yazılımlar tercih edilmemeli, kurumsal yapıya özgü yazılım çözümleri geliştirilmeli ve devamlılığı sağlanmalıdır.

- Arşivlenen elektronik belgelere uzun dönem erişimi sağlayacak taşıma, sarma, dönüştürme ve öykünüm gibi uygun dijital koruma yaklaşımları seçilmelidir.
- Elektronik belgelerin korunmasına yönelik kullanılan en yaygın yaklaşım olan taşıma ve dönüştürme tekniklerinin birleştirilmesiyle ortaya çıkan teknik kullanılmalıdır.
- Elektronik belgelerin saklama planlarının oluşturulması sistem dizayn aşamasından gerçekleştirilmeli ve buna ilişkin kurallar sisteme girilmelidir.
- Elektronik belge saklama planları yasal gereklilikler, prosedürler çerçevesinde hazırlanmalı ve belge saklama planlarının güncellenmesi, onayı, gönderilmesi ve geliştirilmesiyle ilgili süreçleri kapsamalıdır.
- Elektronik belge saklama planları kapsamında, ayıklama ve imha işlemleri gerçekleştirilmelidir. Ayrıca güncel belge saklama planları bulunmayan ya da belgeleri uygun şekilde koruma ve yönetmek için oluşturulmuş prosedürleri takip etmeyen kurum ya da çalışanlara yönelik cezai sorumluluğun olduğu göz önünde bulundurulmalıdır.
- Elektronik belgelerin saklama sürelerinin belirlenmesinde, e-belge ile ilgili yönetimsel ihtiyaçlar, yasal zorunluluklar, mali gereklilikler ve tarihsel değerler göz önünde bulundurulması gereklidir.
- Elektronik belgelerin saklama planları, e-belge serilerinin saklama süreleri, depolama ortamı, depolandığı fiziksel mekân, imha tarihi ve yöntemi gibi hususlar içermelidir.
- Ayıklama sürecinde, belgelerin diğer kurumlarla işlemler, organizasyon, fonksiyonlar, politikalar ve prosedürler bağlamında ilişkileri değerlendirilmelidir.
- Elektronik belgelerin arşivlenmesinde, her şeyi muhafaza et yaklaşımı temel yaklaşım olmamalı, neyin saklanması gerektiği konusunda kurumsal ve yasal gereklilikler çerçevesinde kriterler belirlenmeli ve buna gör işlemler yapılmalıdır.
- Elektronik belgelerin imha işlemlerinde, kurumun dosya planına göre bir belge imha listesinin hazırlanmalıdır.
- Elektronik belge imha listesi, arşivsel değeri olmadığı için devlet arşivlerine devredilmeyecek bütün belge ve belge serilerini içermeli, bunlara ilişkin üst verilerle birlikte imhası sağlanmalıdır
- Devlet arşivlerine gönderilmesi gereken bütün elektronik belgeler, bütün dosya ve klasörlerin üst verilerini içerecek şekilde, devlet arşivlerinin bilgi teknolojileri sistemine veri tabanı tablo formatında elektronik olarak transfer edilmelidir.

- Elektronik belgelerin ayıklanmasına ilişkin kararlara dayanarak, kurumlar arşivsel değeri olan dosyaları otomatik olarak seçmeli ve arşiv formatına dönüştürmelidir.
- Devir listelerine ve bütün dosya ve klasörlerin sayılmasına ek olarak, belgeler elektronik olarak devlet arşivlerine devir edilmelidir.
- Elektronik belgelerin kurum tarafından belirlenmiş uygun yetkilendirmeler olmadan imha edilmemesinin sağlanması gereklidir.
- Dosyanın imhasının, dosya içindeki bütün belgelerin imhası olması dolayısıyla imha edilen elektronik belgelerle ilgili kayıtların tutulması gereklidir. Bu kayıtların, transfer ve imhasına onay veren ve yetkili bilgileri, transfer ve imha tarihi gibi bilgileri içermelidir.
- İmha işleminde elektronik belgelerin sistemden tamamıyla silindiğinden emin olunmalı, ayrıca fiziksel imha işlemi de gerçekleştirilmelidir. Elektronik belgelerin saklandığı donanımında imhası işlemi belirlenmiş parçalama sürecini sağlanmalı ve yetkili kurum nezaretinde gerçekleştirilmelidir.
- Elektronik belgelerin imhasında, elektronik belgelere ilişkin bütün yedek kopyaları da imha edilmelidir.
- Elektronik belgelerin imha süreçlerinin gizli ve kapalı bilgilerin korunmasını sağlayacak şekilde gerçekleştirilmelidir.
- Elektronik belgelerin değişik biçimlerde olması, özel yazılımlar ve uzmanlık gerektiren donanımlar konusu sebebiyle, belgelerin devrine ya da kurumda muhafazasına ilişkin kararların devlet arşivlerinin danışmanlığında yapılmalıdır.
- Devlet arşivlerine devir edilen elektronik belgelerin gizlilik düzeyleri ve erişim haklarına ilişkin seviyeler aynen korunmalıdır.
- Arşivlemede elektronik belgelerin yasal ve kurumsal ihtiyaçlar çerçevesinde kullanılabilmesi için gerçekliği, bütünlüğü, güvenirliliğini sağlamaya yönelik gerekli önlemler alınmalıdır.
- Elektronik belgelerin bütünlüğünün kontrolü ve sağlanması bağlamında kriptografik teknikler kullanılmalıdır.
- E-belgenin bütünlüğünün korunması bağlamında gerekli risk analizi yapılmalı ve buna ilişkin önlemler alınmalıdır.
- Elektronik belgelerin üretilmesinde, alınmasında ve muhafaza edilmesinde kullanılan süreçlerin ve usullerin doğruluğu ve güvenirliliği, e-belgelerin gerçekliğini,

- Elektronik belgelerin bütünlüğünü ve gerçekliğini tehlikeye sokacak, teknolojik platform ve depolanması için kullanılan ortamın kırılganlığıyla ilgili hususlardan üst yönetim kademesinin haberdar olması ve bilgi teknolojileri uzmanlarının önerileri çerçevesinde önlemlerin alınması sağlanmalıdır.
- Elektronik belgelerin bütünlüğünü tehlikeye sokacak hataların, donanımın aksamaya uğramasından, işlemsel hatalardan, yazılım arızasından, kasıtlı saldırılardan ya da bunlara benzer başka nedenlerden kaynaklandığı göz önünde bulundurulmalıdır.
- Elektronik belgelerin bütünlüğüne yönelik hataları, arşivdeki her bir dosyanın başka bir kopyası ile kıyaslanması, dosyanın okunması, mevcut sağlamasının (hash) hesaplanması ve bu sağlamanın o dosya için korunan kopyası ile karşılaştırılması sonucu tespit edilebileceği bilinmelidir.
- Elektronik belgelerin bütünlüğü açısından, zaman damgası fonksiyonu kullanılarak belge düzenlendiği zaman şüpheye yer bırakmayacak şekilde belirtilmelidir.
- Elektronik belge yönetim sistemiyle ilgili politika ve prosedürlerinin belgelendirilmesi ve tanımlanmasının belge bütünlüğünü destekleyeceği göz önünde bulundurulmalıdır.
- Elektronik belgenin yeni bir ortama ya da formata aktarıldığında, yapılan işlemin belgenin bütünlüğünde bir kısım değişimlere sebep olabileceği bilinmelidir.
- Elektronik belge üretme ve depolamak için kullanılan veri işleme araçları ve yazılımları güvenilir olmasına önemle dikkat edilmelidir.
- Elektronik belgelerin bütünlüğü ve gerçekliği açısından kullanılan sistemin bağımsız kontrolü ve denetiminin ve gerekli belgelendirmelerin yapılmasının sağlanmalıdır.
- Elektronik belgelerin bütünlüğünü ve gerçekliğini korum açısından, yetkisiz giriş belirleme ve problem tespitleri de dahil olma üzere bazı güvenlikle ilgili konularda başarıya ulaşılmasında yardımcı olan işlem geçmiş raporu sağlanmalı ve güvenli bir şekilde muhafaza edilmelidir.
- Elektronik belgenin gerçekliği ve güvenirliliği açısından, özellikle kırılgan çevrimdışı ortamlarda depolanan elektronik belgelerin fiziksel ve çevresel güvenlik kontrolleri sağlanmalı ve çevresel tehditlere karşı gerekli önlemler alınmalıdır.
- Elektronik belgelerin bütünlük ve gerçeklik çerçevesinde arşivlenmesinde, depolama ortamlarından çıkarma işlemini sağlayan, firma bağımlı ürünler arasında veri taşıma

- Elektronik belge arşiv sisteminde, belge oluşturulduğunda gerekli provenans bilgileri elde edilmelidir.
- Elektronik belgeler, hem kullanıcı ve hem de sistem yöneticisi tarafından yapılabilecek değişikliklere karşı korunmalıdır.
- Dijital imzayı doğrulamadaki hatanın belgenin değiştirildiğinin ya da sahtesinin yapıldığının göstergesi olabilmesi dolayısıyla, dijital imzayı doğrulamadaki herhangi bir hata kaydedilmeli ve anında yöneticinin dikkatine sunulmalıdır.
- Elektronik belgenin bütünlüğündeki bir eksik ya da hata, bilgisayar çalışmasıyla ilgili herhangi bir arızadan kaynaklanabilir. Bu açıdan, yazılımsal ya da donanımsal hatalar ilgili kayıt defterleri itina ile tutulmalıdır.
- Elektronik belgelerin delil olarak kabul edilebilmeleri için, gerçeklik, bütünlük ve orijinal formunda bulunma gibi özellikleri sağlanmalıdır.
- Elektronik imza oluşturulurken kullanılan kriptografik algoritmaların zamanla zayıfladığı ve kırılabilir hale geldiği göz önünde bulundurulmalıdır.
- Uzun dönem arşivleme açısından elektronik imzaya eklenen zaman damgaları kullanılan algoritmalara bağlı olarak zayıfladığı bilinmelidir.
- Elektronik imza oluşturulurken kullanılan sertifikaların ait olduğu üst köklerin de belirli geçerlilik süreleri olması dolayısıyla, imzanın geçerliliğini koruyabilmesi için periyodik olarak tekrar güçlendirilmelidir.
- Elektronik imzaların uzun dönemli saklanmasında yaşanabilecek sorunlara karşı tedbir almak amacıyla imzaların gerekli ek verilerle birlikte depolanmalıdır.
- Elektronik sertifika hizmet sağlayıcısının faaliyetlerinin sonlandırabileceği ve nitelikli elektronik sertifikaların belli bir sürelerinin olduğu göz önünde bulundurularak, bunlara ilişkin duyurular ve iptal kayıtları takip edilmelidir.
- Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım ve donanım araçlarının zaman içinde kontrolünün ve devamlılığı sağlanmalıdır.
- Uzun dönem arşivlemede elektronik imzaya ilişkin oluşabilecek sorunları çözme açısından arşiv elektronik imza (ES-A) kullanılmalıdır.
- Elektronik imzanın, oluşturulmasının üzerinden uzun bir süre geçtikten sonra doğrulanabilmesinde yaşanabilecek sorunları çözme anlamında elektronik arşivleme için zaman damgası e-imza ile tümleşik şekilde kullanılmalıdır.

- Elektronik belgelerin arşivlenmesinde sertifikalar değiştirilemeyecek ya da sertifikaya herhangi bir ekleme yapılamayacağından emin olarak sayısal imza sertifikaları iyi korunmalı ve sertifikanın geçerlilik tarihi sona ermesi ya da iptal edilmesi durumunda, sertifikanın durumuyla ilgili bilgi de saklanmalıdır.
- Elektronik belge farklı formatlara taşındığında, dijital imza onay fonksiyonunu kaybedeceği göz önünde bulundurularak bu tip işlemler yapılmamalıdır.
- Elektronik belgelerin arşivlenmesinde gerekli dijital imza, açık anahtarla birlikte dijital sertifika, sertifika ile ilgili üst veri, zaman damgası ve ikinci tasdik imza gibi bütün açık şifreleme düzeni öğeleri de arşivlenmelidir.
- Elektronik belgelerin arşivlenmesinde üst veri elemanları için herhangi bir sınırlama getirilmemeli, mümkün olan en geniş kapsamda üst veri elemanları oluşturulmalıdır.
- Elektronik belge üretildiği ya da başka bir depolama ortamına aktarıldığında uygun üst veri elemanlarıyla birlikte işlem gerçekleştirilmelidir.
- Uygun arşivleme açısından sistem tasarım aşamasında; işleyişte ve tanımlama da farklılıkları ortadan kaldırarak standartlaşmayı sağlayan parametrik bilgiler sisteme dahil edilmelidir.
- Sistem tasarımı aşamasında, üst veri elemanlarının; işletim sistemi, ağ yazılımı uygulama programı, bilgisayar sistemi yöneticisi, bilgi ve belge yöneticisi, kullanıcı gibi veri kaynakları tanımlanmalıdır.
- Elektronik belgelerin içeriğinin anlaşılması ve erişiminin etkin bir şekilde sağlanması açısından mümkün olduğunca daha fazla üst veri kullanılmalıdır.
- Elektronik belgelerin arşivlenmesinde, tanımlayıcı işaret, başlık, konu, tanım, üretici, tarih, alıcı, belge türü, ilişki, dil, yer, haklar, dijital imza, forma, fonksiyon, kapsam, yönetim geçmişi gibi üst veri elamanları tanımlanmalıdır.
- Üst veri etkin kullanabilmek içi, kullanıcıların muhtemel bilgi ihtiyaçları mutlaka göz önünde bulundurulmalıdır.
- Elektronik belge yönetim sisteminde; veri yedekleme, felaket kurtarma ve acil durum işlemleri dahil olmak üzere bir acil durum planı gerçekleştirilmelidir.
- Felaket kurtarma planı elektronik belgelerde kaybı önlemek için veri kurtarmayı ve yedeklemeyi içermelidir.
- Felaket kurtarma planı çerçevesinde e-belgeler çevrimdışı ortamlar da, fiziksel ve çevresel olarak kontrol edilmiş alanlarda depolanmalıdır.

- Elektronik belge yönetim sisteminin işler durumda yedek kopyalarının, felaket durumlarında sistemden uzakta bir yerde güvenli bir şekilde depolanma durumu ve kullanılabilirliği test edilmelidir.
- E-belgelerin arşivlenmesi, belgelerin üretildiği sistemden diğer bir sisteme ve çevrimdışı olarak transfer edilebilmesine imkân vermeli ve taşıma işlemleri mutlaka kayıt altına alınmalıdır.
- Felaket kurtarma planı, önemsiz bir yıkımdan büyük felaketlere kadar farklı felaket senaryolarını içermeli ve buna yönelik testler yapılmalıdır.
- Felaket kurtarma planları, anlık acil durumlarla başarılı bir şekilde başa çıkmak için geçici hizmet sağlaması, elektronik belge yönetim ve bilgi işlem fonksiyonlarını normal durumlarına geri getirecek şekilde hazırlanmalıdır.
- Felaket kurtarma planlarında belirtilen hususların ve alınan önlemlerin çalışabilirliliği mutlaka test edilmelidir.
- Sistemin yedekleme işlemlerinin düzenli yapılmalı, ayrıca veri miktarı fazla olması işlemin uzun sürmesine ve performansın olumsuz etkilenmesine sebep olması dolayısıyla, yedeklemenin sunucu bilgisayarlar çok az kullanıldığı zaman yapılmalıdır.
- Yedekleme işlemlerinde, sistem için gerekli olan uygulama yazılımlarının güncel sürümlerini, işletim el kitaplarını, sistem dokümanları, program dokümanları ve işletim sistemi bant ve disklerinin kopyaları alınmalıdır.
- Elektronik belge yönetim sisteminin bağımlı çalıştığı teknolojik altyapının düzenli bakımı yapılmalıdır.

Elektronik belgelere etkin erişime yönelik öneriler;

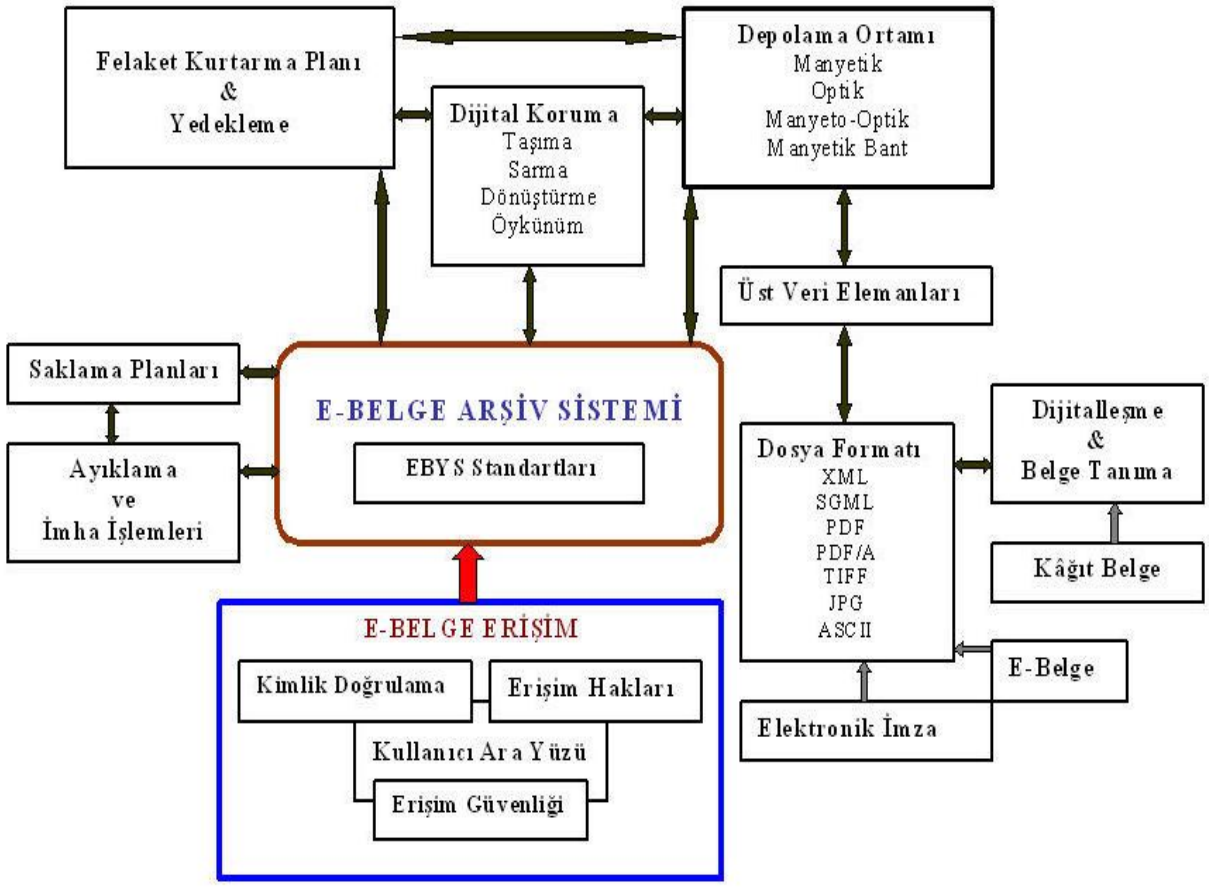
- Elektronik belge erişim sistemi, kullanıcının bilgi ihtiyaçlarına verdiği cevap ve cevabın nitelik açısından etkinliğini sağlayacak şekilde oluşturulmalıdır.
- Elektronik belge erişim sisteminde elektronik belgenin içeriğini yansıtmak amacıyla belirteç kümeleri kullanılmalıdır.
- Elektronik belgelere etkin erişim sağlamak için dizinleme işlemi sağlıklı bir şekilde gerçekleştirilmelidir.
- Elektronik belge erişim sisteminde, dizinleme ve erişim sırasında kullanılan ve seçilen terimlerin belli bir mantığa göre ilişkisini gösteren gömü (Thesaurus) kullanılmalıdır.

- Elektronik belge erişim sistemi temel arama metotlarını destekleyecek şekilde oluşturulmalıdır.
- Erişim sistemin etkin çalışması açısından uygun veri kümesi yapıları kullanılmalıdır.
- Erişim sisteminin güvenliğinin sağlanması açısından, erişim kontrol politikalarını en düşük erişim hakkı prensibi üzerinde temellendirmelidir.
- Sistemin güvenliğiyle ilgili olarak bağımsız kuruluşlara testler yaptırılmalı, bu çerçevede güvenlik açıkları giderilmelidir.
- Sistem, kullanıcıları tanıması ve gerekli doğrulamaları yapmasıyla ilgili teknik hususları içermelidir.
- Erişimde, kullanıcı işlemleriyle ilgili olarak, aynı anda birden fazla kimlik doğrulama yöntemi kullanılmalıdır. Eğer sadece parola kullanılacaksa, parolalar belli kurallar çerçevesinde karmaşık bir yapıda belirlenmelidir.
- Erişim güvenliği açısından, erişimin açıkça sağlandığı ya da kısıtlandığı sistem tabanlı araçlar kullanılarak yapılan mantıksal erişim kontrolü kullanılmalıdır.
- Mevcut sistem ile kullanıcılar, servisler ve sistemler arasındaki etkileşimi kontrol edecek dış erişim kontrol mekanizmasını oluşturulmalıdır.
- Erişim sistemi, hangi belgelere erişildiğini, belgeye erişen kullanıcının kimliğini ve erişim zamanı, yetkisiz erişim denemelerini kaydetmeli ve buna ilişkin kayıt defterleri üzerinde herhangi bir değişiklik olmaması açısından güvenle saklanmalıdır.
- Erişim sistemi, elektronik belgeler, araştırma araçları, imha planları ve erişim kontrol politikaları dahil olma üzere arşivdeki bütün nesnelerin üzerinde erişim kontrolünü desteklemelidir.
- Erişim sistem güvenliği en üst düzeyde sağlansa bile sisteme yetkisiz girişle olabilmektedir. Bu açıdan, elektronik belgeler kopyalanmaya karşı korumalı olmalıdır.
- Sistemin truva atları, ağ solucanları ve virüsler gibi zararlı programların bilgisayara girmelerine yol açan kötü amaçlı yazılımlardan doğacak tehlikelere karşı koruma sağlanmalıdır.
- Erişimle ilgili olarak, izinsiz erişim, zarar verme, değişiklik yapma ve üretim gibi temel tehditlere karşı gerekli önlemler alınmalıdır.
- Hayati belgelere yetkisiz erişimi önlemek için, elektronik belgeler mutlaka şifreleme algoritmaları kullanılarak arşivlenmelidir.

- Erişim hakkı ve doğrulama ile ilgili süreçler belirlenmelidir. Bu çerçevede sistemi kullanacakların erişim hakları ayrı ayrı tespit edilmeli ve her bir kullanıcının hangi işlemleri yapmada yetkili oldukları açıkça ortaya konmalıdır.
- Erişim sisteminde, kullanıcıların her birine bir kullanıcı adı ve şifresi tanımlanmalı, ilgili kullanıcı adıyla sisteme yapılan bütün girişler kaydedilmeli ve aynı kullanıcı adıyla aynı anda tek bir girişin yapılabilmesi sağlanmalıdır.
- Kullanıcı rollerinin ayrı ayrı tanımlanması ve bunların yazılı prosedürlerle kayıt altına alınmalıdır.
- Sistem yöneticisi, kullanıcı yetkilendirmelerini resmi yazılı talepler ve onaylar çerçevesinde yapmalı ve buna ilişkin değişikliklerin kaydedilmesini sağlamalıdır.
- Elektronik belge yönetim sistemindeki kullanıcılar için; tasnif dışı, hizmete özel, özel, gizli ve çok gizli gibi erişim hakkı düzeyleri kullanılmalı, erişim hakları ve rolleri "bilmesi gereken" prensibi çerçevesinde belirlenmelidir.
- Arşivleme sistemi içinde bulunan elektronik belgeleri görüntüleme ya da kopyalama hakları, yazılı talepler çerçevesinde gerçekleştirilmelidir.
- Erişim sisteminde, hangi e-belgelere hangi yetkilerle erişileceği gibi kaynaklar üzerinde yetkilendirmeler açık ve anlaşılır bir şekilde belirlenmeli ve buna ilişkin olabilecek kalıcı ya da geçici değişiklikler etkin bir şekilde takip edilmelidir.
- Görevi değişen veya kuruluştan ayrılan personelin erişim haklarıyla ilgili işler en kısa zamanda yapılmalı, geçiş sürecinde olabilecek yetkisiz kullanımların önüne geçilmelidir.
- Erişim ara yüzünün, kullanıcılarının elektronik belgelere, dosyalara ve araştırma araçlarına kolay erişiminin desteklenmelidir.
- Erişim ara yüzü, kullanıcıların kendilerine göre özel ayar yapmasına izin vermelidir.
- Erişim ara yüzünde kullanıcıların sistem içinde sık kullandıkları fonksiyonlar için kısa yol tuşları ve simgeleri tanımlanabilmelidir.
- Erişim ara yüz tasarımında, tasarımın genel yapısı ve teknolojik bileşenlerinin ihtiyaç duyulduğunda geliştirilmesine imkân veren modüler bir tasarımın benimsenmelidir.
- Erişim ara yüzü tasarımını gerçekleştirirken karşıtlık ve simetri gibi iki temel tasarım öğesi göz önünde bulundurulmalıdır.
- Erişimde, kişisel gizlilik ve güvenirliliği koruyacak ve elektronik belgelere kamunun erişimini sağlayacak metotlar geliştirilmelidir.
- Elektronik belgelere erişimin kullanıcının tercih ettiği formda sağlanmalıdır.

- Erişim seçenekleri, kurumsal ihtiyaç ve gerekliklere göre çevrimiçi erişim, yarı aktif erişim ve çevrimdışı erişim olarak değerlendirilmelidir.
- Kurumsal ihtiyaçların dışında araştırma amaçlı olarak elektronik belgelere erişim sağlamalı, erişime açılacak elektronik belgelerle ilgili yasal ve idari değerlendirmeler mutlaka yapılmalıdır.
- Kurumla arası elektronik belge iletimi olabileceği göz önünde bulundurularak genel kabul görmüş standartlar çerçevesinde birlikte işlerlik sağlanmalıdır.

Ortaya konulan öneriler bağlamında temel alınabilecek bir model ortaya koymak gerekmektedir. Bu çerçevede Şekil 11, oluşturulacak arşivleme ve erişim sistemi açısından genel bir model yaklaşım sunmaktadır. Bu model elektronik belge arşivleme ve erişim açısından temel öğeleri içermektedir.



Şekil 11. Elektronik Belge Arşivleme ve Erişim Sistemi Modeli

Bu model yaklaşım temel alınarak arşivleme ve erişim sistemi oluşturulmalıdır. Bu modelde, arşivleme ve erişim açısından öncelikli birbiriyle ilişkili alanlar ortaya konmuştur. Model unsurlarının birbirleriyle ilişkilerinin özelliği tek yönlü ya da çift yönlü oklarlar belirtilmiştir. Bu modelde elektronik belgenin üretiminden arşive ulaşmasına kadar geçen temel yollar ve erişim mekanizmasının temel unsurları ortaya konmuştur. Modelde belirtilen unsurların belirli bir önceliği yoktur. Sistem bütünüyle en başta tasarlanmalı ve ortaya konmalıdır. Bu temel unsurların detayları tezin bütününde ele alınmıştır. Modelin temel işleyiş mekanizması şöyledir; öncelikle belgenin türünün ne olduğu üzerinde yapılacak işlemi belirleyecektir. Eğer kâğıt ortamda üretilen belgenin elektronik belge yönetim sistemine dahil edilmesi düşünülüyorsa, öncelikle standartlarda belirtilen uygun dosya formatları çerçevesinde dijitalleştirme faaliyetinin gerçekleştirilmesi gereklidir. Kurumsal yapı çerçevesinde eğer ihtiyaç duyuluyorsa belge tanıma faaliyeti gerçekleştirilebilir. Bu işlemler çerçevesinde gerekli üst veri elemanları ile birlikte kullanım sıklıkları ve arşivsel ihtiyaçlara göre belirlenen depolama ortamlarında saklanma işlemi gerçekleştirilir. Elektronik ortamda üretilen belgeler için ise öncelikle elektronik imzaya imkân veren uygun dosya formatının seçimi ve elektronik imzanın atılması faaliyeti gerçekleştirilir. Bununla birlikte gerekli üst veri elemanları ile birlikte uygun depolama ortamlarında arşivleme işlemi gerçekleştirilir. Bu noktadan sonra yapılacak işlemler gerek dijital ortama aktarılan kâğıt belgeler ve gerekse elektronik olarak üretilen belgeler için benzerlik gösterir. Daha önce de ifade edildiği gibi belirtilen bütün unsurlar sistem kullanılmadan önce tasarlanmalı ve ortaya konmalıdır. Uygun depolama araçlarında saklanan belgeler için en kötü felaket senaryosunu da içine alan bir felaket kurtarma planı hazırlanır. Ayrıca sistemde olabilecek veri kayıplarını göz önüne alarak bir yedekleme faaliyeti gerçekleştirilir. Uzun dönem arşivlemede elektronik belgelerin gerçekliğinin ve bütünlüğünün korunmasında ciddi riskler bulunmaktadır. Bu açıdan uygun dijital koruma teknikleri kullanılarak, elektronik belgeleri gerçekliği ve bütünlüğü korunarak erişilebilirliği sağlanır. Elektronik belgelerin saklama süreleri ve imha işlemleri ile ilgili olarak sistem dizayn aşamasında, oluşturulan saklama planlarında resmi olarak belirlenen hususlar oluşturulan sisteme uygulanır. Yukarıda belirtilen bütün hususlar bu konularda mevcut standartlar göz önünde bulundurularak ve tam olarak gerçekleştirilmelidir. Bu temel unsurlar çerçevesinde elektronik belgeler sağlıklı bir şekilde arşivlenmiş ve erişime hazır hale gelmiş olacaktır. Oluşturulan arşiv sistemine erişim mekanizması Şekil 10'da ortaya konulan e-belge erişim sistemi modeli çerçevesinde işlemelidir. Ayrıca erişim sisteminin temel unsurları olan kimlik doğrulama, erişim hakkı ve erişim güvenliğine ilişkin gereklilikler

gerçekleştirilmelidir. Bu hem arşiv sisteminin güvenliğini ve hem de arşiv sistemine güvenli erişimin gerçekleşmesini sağlayacaktır. Bu modelde belirtilen ana bileşenlerin gerçekleştirilmesinde bilgi teknolojileri önemli bir yer almaktadır. Bu açıdan bir takım teknolojik hususların nasıl gerçekleştirileceği konusunda bilgi teknolojileri uzmanlarıyla sıkı ve sürekli bir işbirliğinin sağlanması sistemin sağlıklı işlemesi ve yaşaması açısından büyük önem taşımaktadır.

Şekil 11 'de belirtilen genel yaklaşımın benimsenmesi ve bu çerçevede oluşturulmuş etkin arşivleme ve erişim sistemi kurumsal elektronik belge yönetim sistemi açısından temel olarak aşağıdaki faydaları sağlar;

- Uzun dönemde elektronik belgelerin bütünlüğünü ve gerçekliğinin korunmasını sağlar.
- Güvenilir ve doğru bir e–belge erişimi temin eder ve erişim maliyetini düşürür.
- E-belgelerin yasal geçerliliği sağlanır.
- Tarihsel, yasal, kültürel ya da yönetimsel değeri olan elektronik belgelere uzun dönem erişimi sağlar.
- Vatandaşın, kamuya açık bilgiye erişimini artırır.
- Kamuya açık olmayan kişisel bilgilerin gizlilik ve güvenliğini sağlar.
- Sisteme yetkisizi girişler engeller.
- Felaket durumlarında sistemin sorunsuz ve kayıpsız çalışmasını sağlar.
- Düzenli yedekleme işlemleri gerçekleştirilerek, veri kayıplarının olması durumlarında da sistemin sağlıklı çalışmasını sağlar.
- Yasal ihtiyaçların etkin ve geçerli bir şekilde karşılanmasını sağlar.
- Elektronik belgelerin uygun dosya formatlarında oluşturulması ve muhafaza edilmesini sağlar.
- Elektronik belgelerin uygun depolama araçlarında arşivlenmesini sağlar.
- Teknolojik eskimeye yönelik dijital koruma teknikleri uygulayarak oluşabilecek veri kayıplarını önler.
- Elektronik imzaların uzun dönem arşivlemede ömrünü uzatır ve kullanılabilirliğini sağlar.
- Teknik ve fiziksel olarak sistemin düzenli bakımını sağlayarak oluşabilecek sorunları önler.

- Çok gizli ya da hayati elektronik belgelerin şifreleme algoritmaları kullanılarak arşivlenerek tam bir erişim güvenliği sağlar.
- Sistemin çalışmasıyla ilgili sürekli bir eğitim faaliyeti gerçekleştirerek kullanıcı hatalarının asgariye inmesini sağlar.
- Fiziksel depolama maliyetlerinin azaltır.
- Ayıklama ve imha işlemlerinin sistem dizayn aşamasında belirlenen çerçevede sağlıklı bir şekilde yapılmasını sağlar.
- Elektronik belge yönetim standartlarına uygunluğun sonucu olarak, kurumlar arasında birlikte işlerliği destekler.
- Bilgi teknolojilerinde yaşanan hızlı değişime uygun yazılım ve donanım değişiklikleri ve gerekli dijital koruma teknikleri uygulanarak uzun vadede sistemin sorunsuz çalışmasını sağlar.

Belirtilen bütün hususlar çerçevesinde elektronik belgelerin sağlıklı bir şekilde arşivlenmesi ve buna paralel etkin erişiminin sağlanması sistemin bütünlüğü ve başarısı açısından en önemli konulardır. Öngörülen ve önerilen hususların yerine getirilmesi kurumsal başarıyı sağlayacaktır. Ayrıca teknolojinin çok hızlı bir gelişme içinde olduğu değerlendirilerek, mevcut durumun belli aralıklarla gözden geçirilmesi ve değişime paralel olarak yenilenmesi ve yeni önerilerle daha ileriye taşınması gerekmektedir. Mevcut çözümlerin yeterli görülmemesi ve yeni çözümler içinde gerekli deneyimleme çalışmalarının yapılması önemli bir zorunluluktur. Zira mevcut durumda elektronik belgelerin gerçekliğini ve bütünlüğünü koruyacak çözümler zaman içinde geçerliliğini yitirebilecektir. Bu açıdan teknolojik perspektifte sistemle ilgili bütün unsurlar sürdürebilirlik açısından gözden geçirilmeli ve gerekiyorsa uygun çözümlerle yenilenmelidir.

TERİMLER

Bu kısım literatürde sıkça kullanılan İngilizce terimlerin Türkçe karşılıklarını vermek amacıyla oluşturulmuştur. Ayrıca kısaltmalar kısmında bulunan İngilizce sözcüklerin Türkçe karşılıkları da bu kısımda verilmiştir. Literatürün ağırlıklı olarak İngilizce kaynaklardan oluşmasından dolayı, karşılıklar İngilizceden Türkçeye verilmiştir. Buradaki esas amaç Türkçe karşılıklarda bir standardın oluşmasını sağlamaktır.

Access Control: Erişim Kontrolü
Accountability: Sorumluluk
Accuracy: Doğruluk
Active Server Pages: Aktif Sunucu Sayfaları
American Records Management Association: Amerika Belge Yönetim Derneği
American Standard Code for Information Interchange: Bilgi Alışverişi için Amerikan Standart Kodu
Appraisal: Ayıklama
Archival E-signature: Arşiv Elektronik İmza
Archival Interest: Arşivsel İlgi (bağ)
Arrangement : Düzenleme
Association of Special Libraries and Information: Özel Kütüphane ve Bilgi Merkezi Derneği
Attribute: Nitelik
Audit Trail: İşlem Geçmiş Raporu
Authentic Records: Geçerli Belge
Authenticate Identity: Kimlik Doğrulama
Authentication: Doğrulama
Authenticity: Gerçeklik
Bitstream: Veri Akışı
Certificate Revocation List: Sertifika İptal Listesi
CMS Advanced Electronic Signatures: CMS İleri Elektronik İmzalar
Communication Device: İletişim Araçı
Compact Disk: Kompakt disk
Computer System: Bilgisayar Sistemi

Confidential Records: Gizli Belge

Confidential: Gizli

Countersignature: İkinci tasdik imza

Cryptographic Message. Syntax: Kriptografik Mesaj Sözdizimi

Custody: Muhafaza

Data Processing: Veri İşleme

Database: Veri Tabanı

Decrypt: Şifre çözmek

Description: Tanımlama

Destruction of Records: Belgelerin İmhası

Digital Preservation: Dijital Koruma

Digital Signature: Dijital İmza

Digital Versatile Disk: Sayısal Çok Yönlü Disk

Direct Attached Storage: Direk Bağlanan Depolama

Disaster Recovery: Felaket Kurtarma

Disposition: Tasfiye, İmha

Electronic Certificate Service Provider: Elektronik Sertifika Hizmet Sağlayıcısı

Electronic Form: Elektronik Form

Electronic Imaging: Elektronik görüntüleme

Electronic Records Management: Elektronik Belge Yönetimi

Electronic Records: Elektronik Belge

Electronic Signature: Elektronik İmza

Encryption: Şifreleme

Evidentiary Integrity: Delilsel Bütünlük

Evidentiary: Delilsel

Extended Binary Coded Decimal Interchange Code: Genişletilmiş İkili Kodlamalı Onluk Sistem Değiştirme Kodlaması

Extensible Markup Language: Genişletilebilir İşaretleme Dili

File Transfer Protocol: Dosya Aktarım Protokolü

File: Dosya

Finding Aid: Araştırma Araçları

Flat File: Klasör

Form: Biçim

Fragmentation: Parçalara Ayrılma

Hard Drive: Sabit Disk

Hyper Text MarkUp Language: Hipermetin Belirtme Dili

HyperText Transfer Protocol: Hipermetin Transfer Protokolü

Imaging System: Görüntüleme Sistemi

Information Technology: Bilgi Teknolojileri

Information Technology: Enformasyon Teknolojisi

Information: Enformasyon

Input Device: Giriş Aygıtları

Integrated Drive Electronics: Bağlı Cihazların Elektronik Yapısı

Integrity: Bütünlük

Intelligent Character Recognition: Akıllı Karakter Tanıma

International Electrotechnical Commission: Uluslararası Elektronikteknik Komisyonu

International Council on Archives: Uluslararası Arşiv Konseyi

International Research on Permanent Authentic Records in Electronic Systems: Elektronik Sistemlerdeki Kalıcı Gerçek Belgeler Üzerinde Uluslararası Araştırma

International Standard Archival Description: Uluslararı Arişiv Tanımlama Standardı

International Standart Organization: Uluslararası Standartlar Örgütü

Internet Protocol: İnternet Protokolü

Inventory: Envanter

Least Privilege: En Düşük Erişim Hakkı

Legal Requirement: Yasal Gereklilik

Life Cycle: Yaşam Döngüsü

Life Span: Yaşam Süresi

Local Area Network: Yerel Alan İletişim Ağı

Log: Kayıt Defteri

Magnetic Tape: Manyetik Bant

Media Type: Ortam Türü

Media : Ortam

Message Authentication Code: Mesaj Doğrulama Kodu

Metadata: Üst Veri

Metropolitan an Area Network: Metropolitan Alan Ağı

Migration: Taşıma

National Archives and Records Administration: Ulusal Arşiv ve Belge Yönetimi

Network: Ağ

Network Attached Storage: Ağa Bağlı Depolama

On-line: Çevrimiçi

Operating System: İşletim Sistemi

Optical Character Recognition: Görsel Karakter Tanıma

Optical Mark Recognition: Optik işaret tanıma

Organization for Economic Co-Operatıon and Development: Ekonomik İşbirliği Organizasyonu

Output Device: Çıkış Aygıtları

Personal Computer: Kişisel Bilgisayar

Portable Document Format

Preservation: Saklama, Koruma

Pretty Good Privacy: Tatlı Mahremiyet

Privacy: Gizlilik

Public Key Cryptography: Açık Anahtar Şifrelemesi

Public Key Infrastructure: Açık Şifreleme Düzeni

Random Access Memory: Rastgele Erişimli Bellek

Receive: Alma

Records Appraisal : Belge Ayıklama

Records Management: Belge Yönetimi

Records Manager: Belge Yöneticisi

Records Retention Schedule: Belge Saklama Planları

Records Security: Belge Güvenliği

Records Series: Belge Serileri

Records: Belge

Redundant Array of Independent Disk

Refresh: Yenilemek

Reliability: Güvenirlilik

Replication: Yineleme

Retain: Saklama

Retention Schedule: Saklama Planı

Retention: Saklama

Retinal Scan: Retina Taraması

Retrieve: Geri İletim

Rich Text Format: Zengin Metin Formatı

Secure Socket Layer: Güvenli Soket Katmanı

Simple Mail Transfer Protocol: Basit Posta İletim Protokolü

Small Computer System Interface: Küçük bilgisayar Sistemi Arabirimi

Standard Generalized Markup Language: Standart Genelleştirilmiş İşaretleme Dili

Storage Area Network: Depolama Alanı Ağı

Storage Unit: Depolama Unitesi

The Digital Preservation Coalition: Dijital Koruma Koalisyonu

Time Stamp: Zaman Damgası

Transaction: İşlem

Transmission Control Protocol: İletim Kontrol Protokolü

Trustworthiness: Güvenirlilik

United Nations Commission on International Trade Law: Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu

Universal Resource Locator: Evrensel Kaynak Belirtici

Validation Chain: Doğrulama Zinciri

Version: Sürüm

Video Compact Disk: Video Kompakt Disk

Virtual Private Network: Sanal Özel Ağ

Virtual: Sanal

Vital Records: Hayati Belge

Wide Area Network: Geniş Alan İletişim Ağı

XML Advanced Electronic Signatures: XML İleri Elektronik İmzalar

XML Paper Specification: XML Kâğıt Belirtimi

KAYNAKÇA

A National Electronic Commerce Coordinating Council E-Sign Policy Workgroup (NECCC E-sign Policy Workgroup, (2001), **Electronic Records Management Guidelines for State Government: Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records**, NECCC E-sign Policy Workgroup Elektronik Adres: http://www.dir.state.tx.us/standards/NEC3-Records_Mgmt_ED.pdf, Haziran 2008.

Alkan M., İnalöz, A., 2004, "Telekomünikasyon Regülâsyonları ve Elektronik İmzanın Elektronik Ticaret Üzerindeki Etkileri", **Ankara: TBD 21. Ulusal Bilişim Kurultayı Bildiriler Kitabı içinde.**

Arıkan, S., (1999), **Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım,** Ankara.

Arslantekin, S., 2001, "Web Sayfalarının Düzenlenmesi ve Bilgi Merkezleri", **Türk Kütüphaneciliği Dergisi**, C.15, S.1, s. 31-39.

Arslantekin, S., 2005, "Özgür ve Açık Kaynak Kodlu Yazılımlar ve Bilgi Merkezlerine Etkisi", **Ankara Üniversitesi Dil ve Tarih-Çoğrafya Fakültesi Dergisi**, C.44, S.2, s. 231-246.

Aydın, C., (2003), **Bilgi Teknolojilerindeki Gelişmeler Işığında Arşivcinin Değişen Rolü,** Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi.

Bearman, D., 1999**,** "Reality and Chimeras in the Preservation of Electronic Records", **D-Lib Magazine,** C.5, S.4 .

Boudrez, F., (2005), **Digital Signatures and Electronic Records,** Elektronik adres: http://www.expertisecentrumdavid.be/docs/digitalsignatures.pdf, Aralık 2009.

BSI, (2004), **BSI BIP 008:2004: Code of Practice for the Legal Admissibility and Evidential Weight of Information Stored Electronically**, Elektronik Adres: http://www.alliancegroup.co.uk/legal-admissibility.html, Mart 2010.

Bulut, M., (2005), **Dijital İmza Rehberi,** İstanbul: İstanbul Ticaret Odası yay. N0:2005/37.

California Digital Library (CDL), (2009), **Guidelines for Digital Images**, University of California, Elektronik Adres: http://www.cdlib.org/services/dsc/tools/docs/cdl_gdi_v2.pdf, Ocak 2010.

Calrim, (2002), **Electronic records management handbook: State of California Records Management Program,** Elektronik Adres: http://www.documents.dgs.ca.gov/osp/recs/ERMHbkall.pdf, Ağustos 2008.

Capron, H.L., (1997), **Computers: Tools for Information Age**, London: Adisson Publ.

CITU, (2000), **Framework for Information Age Government: Electronic Records Management**, Elektronik Adres: http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/erm.pdf, Mayıs 2010.

Curphey, M., (2002), **A Guide to Building Secure Web Applications**, Elektronik Adres http://www.cgisecurity.com/owasp/html/ch08.html, Kasım 2009.

Çiçek, N., 2000, "ISO 9000 Kalite Güvence Sistemi Standartları'nda Evrak Üretimi ve Yönetimi", **Arşiv Araştırmaları Dergisi***,* C.2, S.1, s.7-33.

Çölkesen, R., Örencik, B., (2008), **Bilgisayar Haberleşmesi ve Ağ Teknolojileri,** İstanbul: Papatya Yayıncılık.

Dearstyne, B. W**.,** 1999, "Records Management of the Future: Anticipate, Adapt, and Succeed", **Information Management Journal**, C.4, S.33 , s. 5-8.

Dickman, J.C., 2002, "Information Preservation: Changing Role", **Information Management Journal***,* C.36, S.5, s. 54-59.

Dinçer, Ö., (2007), **Erişim Kontrol Politikası Oluşturma Kılavuzu**, Kocaeli: TÜBİTAK-UEKAE.

Dollar**,** C. M., 1999**,** "Selecting Storage Media for Long-term Access to Digital Records", **Information Management Journal**, C.33, S.3, s. 36-43.

Dönmez, C., (2002), **Regulation of Electronic Signatures and Protection of Private Keys**, UK: University of Sheffield Department of Law.

Dumortier, J., Van Deneynde, S., (2002), "Electronic Signatures and Trusted Archival Services*"*, **Proceedings of DLM Forumu , 6-8 May 2002 içinde**, s.520-524, Barcelona.

Duranti, L., 2001, "The Impact of Digital Technology on Archival Science", **Archival Science***,* C.1, S.1, s.39-55.

Elektronik İmza Kanunu, 2004, **Resmi Gazete**, 5070 (15.01.2004)

Eroğlu, M., (2000), **Gövdelemenin ve Gömünün Türkçe Bir bilgi Erişim Sistemi Üzerindeki Etkisinin Araştırılması**, Yayımlanmamış Yüksel Lisans Tezi, Ankara: Hacettepe Üniversitesi.

EU, (2001), **Model Requirement for The Management of Electronic Records,** Elektronik Adres: http://www.cornwell.co.uk/edrm/moreq.asp, Haziran 2007.

FHWA (U.S. Federal Highway Administration), (1999), **Files management and records disposition manual**, Elektronik Adres: http://www.fhwa.dot.gov/legsregs/directives/orders/m13241/13241ac4.htm, Nisan 2008.

Gill, S. L., (1998), File **Management and Information Retrieval Systems**, Colorado.

Gürkan, O., (2007), **Web Tasarım Kılavuzu,** Ankara: Nirvana Yay.

Hasırcıoğlu, I., 2006, "Elektronik İmza Oluşturma ve Doğrulama Standartları", **Ulusal Elektronik İmza Sempozyumu**, Ankara.

Henkoğlu, T., (2008), **Modern Donanım Mimarisi**, İstanbul: Pusula Yayıncılık.

Hollier, A.**,** 2001**,** "The Archivist in the Electronic Age", **HEP Libraries Webzine**, March, S.3.

İmamoğlu, F., (2008), **Sistem ve Ağ Temelleri,** İstanbul: Bilge Adam Yay.

İnalöz, A., (2003), **Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi,** Yayımlanmamış Yüksel Lisans Tezi, Ankara: TK.

ICA, (2000), **General International Standard Archival Description**, Elektronik Adres: http://www.ica.org/sites/default/files/isad_g_2e.pdf, Haziran 2009.

INTERPARES, (2006), **International Research on Permanent Authentic Records in Electronic Systems**, Elektronik Adres: http://www.interpares.org/, Ekim 2009.

ISO, (2006), **ISO 23081-1: Information and Documentation-Records Management-Metadata for Records**, Elektronik Adres: http://portal2.tcu.gov.br/portal/pls/portal/docs/769655.PDF, Mayıs 2010.

ISO, (2005), **ISO/TR 18492: Long-term Preservation**, Elektronik Adres: http://www.dcc.ac.uk/resources/standards/diffuse/show?standard_id=108, Nisan 2010.

ISO, (2001), **ISO 12142: Electronic Imaging Errors**, Elektronik Adres: http://www.dcc.ac.uk/resources/standards/diffuse/show?standard_id=115, Nisan 2010.

ISO, (2001b), **ISO 15489-1: Information and Documentation-Records Management**, Elektronik Adres: http://www.archives.org.il/UserFiles/File/119894256812.pdf, Mayıs 2010.

ISO, (1997), **ISO/TR 12654: Electronic Imaging, Management of Electronic Recording Systems**, Elektronik Adres: http://www.dcc.ac.uk/resources/standards/diffuse/show?standard_id=117, Nisan 2010.

ISO/IEC, (2005), **ISO/IEC 27001: Information Security Requirements**, Elektronik Adres. http://www.dcc.ac.uk/resources/standards/diffuse/show?standard_id=148, Nisan 2010.

Johnston, G. P., Bowen, , D.V., 2005, "The Benefits of Electronic Records Management Systems", **Records Management Journal**, C. 15, S.3, s.131-140.

Kandur, H., 2009, "Elektronik Belgelerin Standartlarla Yönetimi", **Elektronik Belge Yönetimi Bilgilendirme Toplantısı**, Devlet Arşivleri Genel Müdürlüğü, 13-17 Nisan 2009, Ankara.

Kandur, H., (2006), **Elektronik Belge Yönetimi Referans Kriterleri Referans Modeli v.2.0**, Ankara:T.C. Başbakanlık Devlet Arşivleri Genel Müdürlüğü Cumhuriyet Arşivi Daire Başkanlığ, Yayın no:29.

Kandur, H., 1999a, "Management of electronic records: Educating archivist and records managers". **Arşiv Araştırmaları Dergisi**, C.1, S.1, s.35-45.

Kandur, H., 1999b, "Elektronik arşivler ve arşivcilik mesleğinin geleceği". **"Bilgi Çağı, Bilgi Merkezler ve Bilgi Teknolojileri" Sempozyumu bildirileri, 7-8 Mayıs 1997 içinde,** Ankara: Ankara Üniversitesi, s.15-21.

Kaptan, S., (1995), **Bilimsel Araştırma ve İstatistik Teknikleri**, Ankara: Tek Işık Web.

Karasar, N., (1991). **Bilimsel Araştırma Yöntemi,** Ankara: Nobel Yayın Dağıtım.

Kowlowitz, A., Kelly, K., 1997, "Model for Action: Developing practical approaches to electronic records management and preservation", **Bulletin of the American Society for Information Science**, C.23, S.5.

Kurnaz, S., (2008), **Veri Yapıları ve Algoritma Temelleri,** İstanbul: Papatya Yayıncılık.

Külcü, Ö., (2009), "Belge Yönetiminde Program Geliştirme: Belge Yönetimi Kapasite Geliştirme Sistemi", **Bilgi Dünyası Dergisi**, C.8, S.2, s.261-285.

Lupton, W. E., (1999) "The Digital Signature: Your Identity by the Numbers, **The Richmond Journal of Information, Law and Technology**, C.6, S.2 .

Maron, M.E., 1984, "Probabilistic retrieval models", **Progress in Communication Sciences,** C.5, s. 145-176.

Megill, K.A., Schantz, H.F., (1999), **Document Management: New Technologies fort he Information Services Manager,** London: Bowker-Saur.

Menkus, B., 1996, "Defining Electronic Records", **Records Management Quarterly**, C.30, s.1-6.

Minnesota Historical Society, (2004), **Electronic Records Management Guidelines**, Elektronik Adres: http://www.mnhs.org/preserve/records/electronicrecords/erguidelinestoc.html, Nisan 2008.

Moore, R., 2004, "Preservation Enviroments" **NASA Goddard Conference**, April.

NASCIO, (2007), **Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise**, Elektronik Adres: http://www.nascio.org/publications/documents/NASCIO-RecordsManagement.pdf, Haziran 2008.

Neale, W. E.**,** 2004**, "**Managing Electronic Records", **Today,** October.

Nielsen, J., Mack, R. L., (Eds.), (1994), **Usability Inspection Methods,** New York: John Wiley & Sons.

Nielsen, J., 1993, "Iterative User Interface Design", **IEEE Computer,** C.26, S.11, s. 32-41.

Oatway, D., 2004**,** "Electronic Records in Long-term Care", **Nursin Homes,** September.

Orta, M., (2005), **Elektronik İmza ve Uygulaması**, Ankara: Seçkin Yay.

Özarar, M., Kırımer, B., 2007, "Güvenli Elektronik Arşivleme: Standartlar, Yapılar ve İşlevler", **Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık 2007 içinde,** s.298-301, Ankara.

Özdemirci, F., 2009, "E-dönüşüm Sürecinde e-Bege Yönetimi ve e-Arşivler", **Türkiye'de Arşivler ve Arşiv Uygulamaları Paneli 02 Nisan 2009**, Ankara.

Özdemirci, F., 2004, "Bir Disiplin Olarak Belge Yönetim", **Kütüphaneciliğin Destanı Uluslar arası Sempozyumu 21-24 Ekim 2004 içinde,** s.191-210, Ankara.

Özdemirci, F., 2003, "İlk uluslararası belge yönetim standardı: Ülkemiz açısından bir değerlendirme", **Türk Kütüphaneciliği,** C. 17, S. 3, s.225-246.

Özdemirci, F., (1996), **Kurum ve Kuruluşlarda Belge Üretiminin Denetlenmesi ve Belge Yönetimi**, İstanbul: Türk Kütüphaneciler Derneği İstanbul Şubesi.

Özdemirci, F., Bayram, Ö., 2009, "Approaches of E-Records Management in E-State Transformation Process in Turkey", **Second World Summit on the Knowledge Society, WSKS 2009, September 16-18 2009, Chania, Crete, Greece,** s.395-403

Özdemirci, F., Torunlar, M. ve Saraç, S., (2009), **Üniversiteler için Belge Yönetimi ve Arşiv Sistemi/İşlemleri (BEYAS) El Kitabı**, Ankara.

Özdemirci, F., Yalçınkaya, B. 2009, "Belge Yönetiminde Değişim Süreci: e-Belgelere Çok Yönlü Yaklaşım", **8. Ulusal Büro Yönetimi ve Sekreterlik Kongresi, 14-16 Ekim 2009, Ankara.**

Özen, Ü., Naralan, A., (2007), **Temel Bilgi Teknolojileri**, Ankara: Bizim Büro Yay. A.Ş.

Pc Guide, (2004), **Information Storage,** Elektronik Adres: http://www.pcguide.com/intro/works/jobsStorage-c.html, Ağustos 2009.

Public Record Office, (1999), **Management, Appraisal and Preservation of Electronic Records,** Elektronik Adres: http://www.nationalarchives.gov.uk/documents/principles.pdf, Nisan 2008.

Public Records Office of Victoria, (2000), **System Requirement for Archiving Electronic Records**, Elektronik Adres: http://www.prov.vic.gov.au/vers/standard/ver1/99-7-1.pdf, Ekim 2008.

Records Management Institute, (2000), **Understanding Electronic Records: The Basics**, Elektronik Adres: http://www.rmicanada.com/articles_understandinge-records.html#Introduction , Mayıs 2009.

Reed, C., 2000, 'What is a Signature?', **The Journal of Information, Law and Technology**, S.3.

Rhodes, S. B., 1991, "Archival and Records Management Automation", **Records Management Quarterly**, C. 25, S.1.

Sağıroğlu, Ş., Alkan, M., (2007), **Elektronik İmza ve Uygulamaları,** İstanbul: İstanbul Ticaret Odası yay. No:2007/56.

Saraçoğlu, T., 2006, " Veri Depolama Ağları ve Yeni Gelişen Teknolojiler", **İntransa**, Elektronik Adres: http://www.if.com.tr/pages/tr/yayinlar.htm, Mayıs 2010.

Sanders, R. L.,1998, "Records Management Returns to the Departments: A suggestion for the Next Century", **Records Management Quarterly**, C.32, S.1.

Shamir, H. A., 1996, New Technologies for Records Management, **Records Management Quarterly**, C.30 , S.3.

Shepherd**, E.,** 1994**,** "Managing Electronic Records", **Records Management Journal**, C.4, S.1, s. 39-49.

Sitts, M.K.(Ed.), (2000), **Handbook for Digital Projects: A Management Tool for Preservation and Access**, Northeast: Northeast Document Conservation Center.

Smyth, Z.A., 2005, "Implementing EDRM: has it provided the benefits expected", **Records Management Journal**, C.15, S.3, s.141-149.

Sproull, R. F., Eisenberg, J.(Ed.), (2005), **Building an Electrnic Records Archive at the National Archives and Records Administration: Recomendation for a Lon-Term Strategy,** Washington DC: National Academies Pres.

Srinisava, P., (1992), **Thesaurus Construction, Information Retrieval Data Stuructures and Algorithms**, New Jersey: Prentice Hall.

Stamatiadis, D., 2005, "Digital Archiving in the Pharmaceutical industry", **Information Management Journal,** July-August.

State of North Dakota, (1998), **Electronic Records Management Guidelines**, Elektronik Adres: http://www.nd.gov/itd/records/erguide.pdf, Eylül 2008.

Şenocak, Z., 2001, "Dijital İmza ve İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", **A.Ü. Hukuk Fakültesi Dergisi,** C. 50, S.2.

TBD, (2009), **Elektronik Belge Yönetimi,** Ankara: TBD.

Teufel, S., (2004), **Information Retriaval: Retriaval Models,** Elektronik Adres: http://www.cl.cam.ac.uk/users/sht25/IRIE/lec2.2.pdf, Kasım 2009.

The National Archives (UK), (2004), **Requirements for Electronic Records Management Systems: Metadata Standard,** Elektronik Adres: http://www.cabinetoffice.gov.uk/media/277297/records_management_metadata_standard_2002.pdf, Aralık 2009.

TK, 2005, "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik", **Resmi Gazete,** 25692 (06.01.2005).

Tonta, Y., 2001, "Bilgi Erişim Sorunu"**, 21. Yüzyıla Girerken Enformasyon Olgusu: Ulusal Sempozyum Bildiriler içinde**, s. 198-206, Hatay.

Tonta, Y., Bitirim, Y., (2002), **Türkçe Arama Motorlarında Performans Değerlendirme**. Ankara: Total Bilişim Ltd. Şti.

TSE, (2009), **TS:13298: Elektronik Belge Yönetim Standardı**, Ankara: TSE.

UEKAE, (2010), **Kamu Sertifikasyon Merkezi: Mali Mühür Sertifika Hizmetleri**, Elektronik Adres: http://mm.kamusm.gov.tr, Haziran 2010.

UEKAE, (2009), **Kamu Sertifikasyon Merkezi**, Elektronik Adres: http://www.kamusm.gov.tr/tr/Kurumsal/Hakkinda, Ekim 2009.

University of Melborune, (2002), **University of Melbourne Records Management Manual: Electronic Records,** Elektronik Adres: http://www.unimelb.edu.au, Nisan 2008.

USA Department of Defense, (2007), **DoD 5015-02-STD: Electronic Records Management Software Applications Design Criteria Standard**, Elektronik Adres: http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf, Nisan 2009

Wettengel, M., Engel, A., (1999), "Disposition and Archiving of Electronic Records: Concepts for Information Network Berlin/Bonn", **Proceedings of DLM Forumu, 18-19 December 1999 içinde,** s.102-108, Belgium.

Williams, D.J., 2005, "EDRM Implementation and the National Weights and Measures Laboratory", **Records Management Journal**, C.15, S.3, s.158-166.

Winn, J. K., (1998), **Couriers without Luggage: Negotiable Instruments and Digital Signatures**, Elektronik Adres: http://www.law.washington.edu/Directory/docs/Winn/Couriers%20without%20Luggage.htm, Aralık 2009.

Wojcik, C., Gouin, D., 2003, "Managing Electronic Records in the 21st Century", **Information Management Journal***,* C.37, S.6 s.44-50.

Xerox DocuShare, (2006), **Applying Electronic Records Management in the Document Management Environment: An Integrated Approach**, Elektronik Adres: http://docushare.xerox.com/pdf/docushare_RM_whitepaper.pdf, Mayıs 2008.

Yalçınkaya, B., (2008), **Elektronik İmzalı belgelerin Yönetilmesi ve Arşivlenmesi,** Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi.

Yavaş, A., (2007), **Erişim Kontrolü,** Elektronik adres: http://www.olympos.org/belgeler/erisim-kontrolu/erisim-kontrolu-129165.html, Ocak 2009

Yıldırım, N., (1996), **İmza ve El Yazısı Sahteciliği,** Yayımlanmamış Yüksek Lisans Tezi, Ankara: TODAİE.

Zanger, L.M., Oei, L.G., 1994, "Electronic-Records Storage Checklist", **IEEE Software,** C.11, S.4, s.102-103.

ÖZET

Belgeler, bilgi teknolojilerinin kurumsal yapılarda yoğun bir şekilde kullanılmasıyla birlikte elektronik ortamda yönetilmeye başlanmıştır. Elektronik belgelerin kurumsal yapı içinde yoğun bir şekilde kullanılmaya başlanması sağlıklı bir arşivlemeyi ve buna bağlı etkin erişimi zorunlu hale getirmiştir. Buna yönelik sağlıklı çözümler geliştirmek elektronik belge yönetim sisteminin ve kurumun başarısı açısından büyük önem taşımaktadır.

Bu tez çalışmasında genel olarak elektronik belge yönetimi ele alınmış, elektronik belgelerin sağlıklı arşivlenmesi için gerekli hususlar üzerinde durulmuş ve buna bağlı olarak elektronik belgelere etkin ve güvenli erişimin nasıl sağlanacağı ortaya konulmuştur. Bu genel kapsam çerçevesinde tez altı bölümden oluşmaktadır.

Girişin yer aldığı birinci bölümde, konunun önemi, araştırmanın amacı ve hipotezi, araştırmanın kapsamı, araştırma yöntemleri ile tez çalışmasında temel olarak kullanılan kaynaklar yer almaktadır.

İkinci bölümde, belge ve elektronik belge kavramı, elektronik belgelerin yaşam döngüsü, elektronik imza, elektronik belge yönetim standartları gibi temel elektronik belge yönetim hususları ile elektronik belge yönetim sistemi oluşturulmasına ilişkin konular ele alınmıştır.

Üçüncü bölümde, elektronik ortamda belge üretimi ile kâğıt belgelerin elektronik ortama aktarılması ile ilgili hususlara değinilmiştir.

Dördüncü bölümde, elektronik belgelerin arşivlenmesiyle ilgili olarak arşivleme ve dosya türleri, teknolojik gereksinimler, dijital koruma, saklama planlarının oluşturulması ve ayıklama imha işlemleri, arşivlenen elektronik belgelerin gerçekliğinin ve bütünlüğünün korunması, uzun dönem arşivlemede elektronik imza sorunları, üst veri elemanları, felaket kurtarma ve yedekleme, sistem bakımı konuları detaylı değerlendirilmiştir.

Beşinci bölümde, elektronik belgelere erişim bağlamında; erişim sistemi, erişim kontrolü ve güvenliği, erişim hakkı ve yetkilendirme, kullanıcı ara yüzü ve erişim seçenekleri konuları açıklığa kavuşturulmuştur.

Altıncı bölümde, araştırma konusu ile ilgili olarak genel değerlendirme yapılmış, yapılması gerekenler noktasında önerilerde bulunulmuş ve bir model önerisi ortaya konulmuştur.

Bu tez çalışmasıyla, elektronik belgelerin, bilgi teknolojileri bağlamda gerçekliğinden ve bütünlüğünde taviz vermeden sürdürülebilir bir şekilde arşivlenmesi için yerine getirilmesi gereken hususlar ortaya konulmuş ve önemli bir gereklilik olduğu vurgulanmıştır. Arşivlemedeki başarının, elektronik belgelere erişimle ilgili belirtilen hususlarla birlikte, erişim etkinliğini tamamlayan en önemli unsur olduğu değerlendirilmiştir.

ABSTRACT

Records have become to be managed in electronic media since information technologies used in institutional structures intensively. Commencement of the usage of the electronic records in institutional structures makes it compulsory to make a good archiving and depending on this provide efficient access to electronic records. It is significantly important to find solutions to this for the success of management system of electronic records and the institution.

In the thesis, it is concentrated on electronic record management; important issues for a good archiving and within this context, methods of efficient and reliable access to electronic records are handled. In this context, the thesis comprises of six parts.

In the initial part of the thesis, the significance of the subject, aim of the study, the hypothesis, and the context of the study, research methods and resources used in the study are explained.

In the second part, basic electronic records management issues such as record and electronic record concepts, electronic records life cycle, electronic signature, electronic record management standards and subjects of developing an electronic record management system are discussed.

In the third part of the study, developing record in electronic media and transferring paper records to electronic media are handled.

In the fourth part, issues such as regarding the archiving of the records, archiving and the types of files, technological requirements, digital preservation, preparing records retention schedule, appraisal and destruction process, preserving the authenticity and integrity of the archived electronic records, electronic signature problems in long-term archiving, metadata elements, disaster recovery and back up, system maintenance are explained in details.

In the fifth part, in the context of access to electronic records; the subjects of access system, access control and security of access, right of access and authorization, user interface and access options are discussed.

In the sixth part, general evaluation regarding research subject is performed, suggestions are given and a model proposal is developed.

With this thesis, the necessary issues in order to provide the sustainable archiving of electronic records with preserving the authenticity and integrity of them are explained and the significance of this is emphasized. The success of archiving is evaluated to be the most significant complementary factor of the issues on access to electronic records.